# UNIVERSITY OF PIRAEUS - DEPARTMENT OF INFORMATICS

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ – ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

## MSc « Cybersecurity and Data Science »

ΠΜΣ « Κυβερνοασφάλεια και Επιστήμη Δεδομένων »

## MSc Thesis

Μεταπτυχιακή Διατριβή

| | |
|---|---|
| **Thesis Title:**<br>Τίτλος Διατριβής: | **A Comprehensive Analysis of EDR (Endpoint Detection & Response), EPP (Endpoint Protection Platform), and Antivirus Security Technologies**<br>Τεχνολογίες ασφαλείας EDR (Endpoint Detection & Response), EPP (Endpoint Protection Platform) και Antivirus |
| **Student's name-surname:**<br>Ονοματεπώνυμο φοιτητή: | **Michael Cappello**<br>Μιχαήλ Καππέλλο |
| **Father's name:**<br>Πατρώνυμο: | **Milziade**<br>Μιλτιάδης |
| **Student's ID No:**<br>Αριθμός Μητρώου: | ΜΠΚΕΔ21016 |
| **Supervisor:**<br>Επιβλέπων: | **Constantinos Patsakis, Associate Professor**<br>Κωνσταντίνος Πατσάκης, Αναπληρωτής Καθηγητής |

July 2024/ Ιούλιος 2024

## 3-Member Examination Committee

Τριμελής Εξεταστική Επιτροπή

| Constantinos Patsakis<br>Associate Professor | Panayiotis Kotzanikolaou<br>Associate Professor | Efthimios Alepis<br>Professor |
|---|---|---|
| Κωνσταντίνος Πατσάκης<br>Αναπληρωτής Καθηγητής | Παναγιώτης Κοτζανικολάου<br>Αναπληρωτής Καθηγητής | Ευθύμιος Αλέπης<br>Καθηγητής |

## Acknowledgments

Η εργασία αυτή δεν θα είχε ολοκληρωθεί χωρίς την ουσιαστική συμβολή του καθηγητή Κ. Πατσάκη & συνεπιβλέποντα Κ. Παπαγεωργίου με τους οποίους συνεργαστήκαμε στενά για την εκπόνηση της συγκεκριμένης μεταπτυχιακής διατριβής. Θα ήθελα να τους ευχαριστήσω θερμά για την καθοδήγηση τους, την παροχή όλων των απαραίτητων κατευθύνσεων, και συμβουλών που απλόχερα μου έδωσαν ώστε να υπάρξει αυτό το αποτέλεσμα.

Θα ήθελα να ευχαριστήσω την οικογένεια και την σύντροφο μου, για τη συνεχή τους υποστήριξη σε όλο το διάστημα της περάτωσης του μεταπτυχιακού μου αλλά και γιατί είναι δίπλα μου και με στηρίζουν ώστε να πετυχαίνω κάθε στόχο που θέτω.

# Table of Contents

## Abstract

In today's digital landscape, where cyber threats and data breaches pose significant risks, the need for robust endpoint security solutions is paramount. This thesis delves into the intricacies of three prominent technologies in the realm of endpoint security: Endpoint Detection and Response (EDR), Endpoint Protection Platform (EPP), and traditional Antivirus solutions. Through a comprehensive examination, this research aims to elucidate the functionalities, strengths, limitations, and evolving roles of these technologies in safeguarding endpoints against a myriad of cyber threats.

The advent of sophisticated cyberattacks has necessitated a paradigm shift in endpoint security strategies. EDR emerges as a proactive approach focusing on continuous monitoring, threat detection, and swift response to mitigate potential damages. Its ability to provide real-time visibility into endpoint activities, coupled with advanced analytics and machine learning algorithms, empowers organizations to detect and neutralize threats effectively. Complementing EDR, EPP consolidates various security functionalities into a single platform, offering a holistic approach to endpoint protection. By integrating antivirus, anti-malware, firewall, and other security features, EPP fortifies endpoints against a wide spectrum of threats, ranging from known malware to emerging zero-day exploits. Moreover, its centralized management and policy enforcement capabilities streamline security operations, enhancing overall efficacy and scalability.

Despite the advancements in EDR and EPP, traditional antivirus solutions remain a cornerstone of endpoint security architectures. While primarily focused on signature-based malware detection, antivirus software continues to play a vital role in thwarting prevalent threats. However, its reliance on signature updates and susceptibility to evasion tactics pose inherent limitations in combating sophisticated and polymorphic malware strains. Furthermore, this thesis delves into the evolving threat landscape and its implications on endpoint security technologies. The proliferation of ransomware, file-less attacks, and supply chain vulnerabilities underscores the need for adaptive and resilient defense mechanisms. As cybercriminals continue to innovate, leveraging AI, automation, and evasion techniques, the efficacy of endpoint security solutions hinges on continuous innovation and proactive threat intelligence.

In conclusion, this research offers valuable insights into the dynamics of EDR, EPP, and antivirus technologies, shedding light on their respective roles, capabilities, and evolving challenges in safeguarding endpoints. By understanding the nuances of these security paradigms, organizations can devise informed strategies to fortify their digital perimeters and mitigate the ever-evolving cyber threat landscape. Additionally, it provides an opportunity to review existing solutions and offer recommendations for improvement to providers.

## Περίληψη

Στη σημερινή ψηφιακή εποχή, όπου οι κυβερνοαπειλές και οι παραβιάσεις δεδομένων αποτελούν σημαντικούς κινδύνους, η ανάγκη για ισχυρές λύσεις ασφάλειας τελικών σημείων είναι επιτακτική. Αυτή η διπλωματική εργασία εξετάζει τις λεπτομέρειες τριών σημαντικών τεχνολογιών στον τομέα της ασφάλειας τελικών σημείων: των Συστημάτων Ανίχνευσης και Απόκρισης Τελικών Σημείων (EDR), των Πλατφορμών Προστασίας Τελικών Σημείων (EPP) και των παραδοσιακών λύσεων Αντιϊών. Μέσω μιας ολοκληρωμένης ανάλυσης, αυτή η έρευνα στοχεύει να διαφωτίσει τις λειτουργίες, τα πλεονεκτήματα, τους περιορισμούς και τους εξελισσόμενους ρόλους αυτών των τεχνολογιών στην προστασία των τελικών σημείων από μια πληθώρα κυβερνοαπειλών.

Η εμφάνιση εξελιγμένων κυβερνοεπιθέσεων έχει καταστήσει αναγκαία μια αλλαγή παραδείγματος στις στρατηγικές ασφάλειας τελικών σημείων. Το EDR αναδεικνύεται ως μια προληπτική προσέγγιση που επικεντρώνεται στη συνεχή παρακολούθηση, την ανίχνευση απειλών και την ταχεία απόκριση για την αποτροπή πιθανών ζημιών. Η ικανότητά του να παρέχει σε πραγματικό χρόνο ορατότητα στις δραστηριότητες των τελικών σημείων, σε συνδυασμό με προχωρημένες αναλύσεις και αλγόριθμους μηχανικής μάθησης, ενδυναμώνει τους οργανισμούς να ανιχνεύουν και να εξουδετερώνουν αποτελεσματικά τις απειλές.

Συμπληρωματικά στο EDR, η πλατφόρμα EPP συνδυάζει διάφορες λειτουργίες ασφάλειας σε μία ενιαία πλατφόρμα, προσφέροντας μια ολιστική προσέγγιση στην προστασία των τελικών σημείων. Με την ενσωμάτωση αντιϊικών, αντι-κακόβουλου λογισμικού, τείχους προστασίας και άλλων χαρακτηριστικών ασφάλειας, η EPP ενισχύει τα τελικά σημεία έναντι ενός ευρέος φάσματος απειλών, από γνωστά κακόβουλα λογισμικά μέχρι νέες εκμεταλλεύσεις μηδενικής ημέρας. Επιπλέον, οι δυνατότητες κεντρικής διαχείρισης και επιβολής πολιτικών επιτρέπουν στους διαχειριστές συστημάτων να ελέγχουν και να παρακολουθούν αποδοτικά την ασφάλεια των τελικών σημείων σε όλο το δίκτυο.

Η εργασία αυτή διερευνά επίσης τον ρόλο των παραδοσιακών λύσεων αντιϊών, αναλύοντας την αποτελεσματικότητά τους και τη θέση τους στην τρέχουσα στρατηγική ασφάλειας των οργανισμών. Ενώ οι αντιϊικές λύσεις συνεχίζουν να αποτελούν βασικό συστατικό της προστασίας τελικών σημείων, η ενσωμάτωσή τους με πιο σύγχρονες τεχνολογίες EDR και EPP είναι ζωτικής σημασίας για την επίτευξη μιας ολοκληρωμένης άμυνας.

Μέσω συγκριτικής αξιολόγησης, μελέτης περιπτώσεων και πρακτικών δοκιμών, αυτή η διπλωματική εργασία προσφέρει μια εις βάθος κατανόηση των διαφόρων προσεγγίσεων στην ασφάλεια των τελικών σημείων, προσδιορίζοντας τις βέλτιστες πρακτικές και τις μελλοντικές κατευθύνσεις για την προστασία των πληροφοριακών συστημάτων από συνεχώς εξελισσόμενες κυβερνοαπειλές.

# 1. Introduction

The pervasive influence of digital transformation on both the economy and society has ushered in a new era of opportunities and challenges. With projections indicating a staggering increase in internet-connected devices, surpassing 125 billion by 2030, and the vast majority of individuals possessing a digital presence, the need for robust cybersecurity measures is more critical than ever. This interconnected cyberspace, fundamental to modern life, has introduced novel risks, blurring the boundaries between the digital and physical realms[1].

The adoption of digital solutions has been accelerating, particularly evident during the COVID-19 pandemic, which saw a surge in telecommuting, online commerce, and virtual communication. While these innovations have empowered consumers and bolstered economic activity, they have also inadvertently fueled a rise in malicious cyber activities. Cybercriminals employ various tactics to exploit users, from phishing schemes to sophisticated ransomware attacks, posing significant threats to individuals and organizations[2].

Cybersecurity threats in the European Union are affecting sectors vital for society. The top six sectors affected, as observed by the European Union Agency for Cybersecurity (Enisa) between January 2022 and March 2023, are public administration/government (24% incidents reported), digital service providers (13%), the general public (12%), Services (12%), finance/banking (9%) and healthcare/medical (7%)[3].

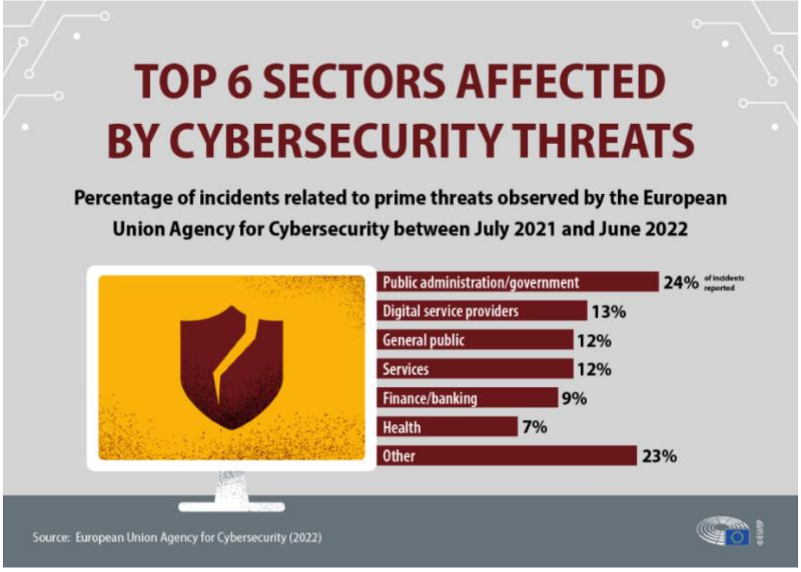


**Figure 1: Affected Sectors by Cyber Threats**

In the ongoing battle against the ever-evolving landscape of cyber threats, organizations rely on a diverse arsenal of security technologies to repel and prevent attacks. Among these vital tools are endpoint detection and response (EDR), network detection and response (NDR), extended detection and response (XDR), and security information and event management (SIEM). These technologies serve as invaluable allies, providing organizations with the means to detect, respond to, and mitigate the impact of malicious activities.[4] This thesis delves into the intricacies of these key technologies, examining their functionalities, strengths, limitations, and evolving roles in safeguarding endpoints. While acknowledging the importance of a holistic approach to endpoint security, this research focuses primarily on Endpoint Detection and

Response solutions. Through a rigorous analysis, this thesis aims to elucidate the nuances of EDR solutions, comparing and contrasting them with other technologies to provide valuable insights into their effectiveness and suitability in today's threat landscape[5].

A secure cyberspace is paramount for fostering trust in the digital economy and ensuring the uninterrupted functioning of critical services. This thesis delves into the intricacies of three prominent technologies in the realm of endpoint security: Endpoint Detection and Response (EDR), Endpoint Protection Platform (EPP), and traditional Antivirus solutions. Through comprehensive examination and practical implementation, this research aims to elucidate the functionalities, strengths, limitations, and evolving roles of these technologies in safeguarding endpoints against a myriad of cyber threats.

By understanding the nuances of these security paradigms, organizations can devise informed strategies to fortify their digital perimeters and mitigate the ever-evolving cyber threat landscape. This research not only offers valuable insights into the dynamics of EDR, EPP, and antivirus technologies but also provides recommendations for enhancing the efficacy of these solutions in real-world applications. The insights derived from this study are critical for organizations aiming to bolster their cybersecurity posture and adapt to the dynamic threat environment.

## 1.1 Overview of the Thesis

In this thesis, we delve into the intricate realm of Endpoint Detection and Response (EDR), Endpoint Protection Platform (EPP), and traditional Antivirus solutions, collectively comprising the frontline defense against evolving cyber threats. The digital landscape demands robust security measures, necessitating a thorough understanding of these technologies' functionalities, strengths, limitations, and evolving roles. It is important to analyze the advantages and disadvantages of each solution in order for people in authority to choose which solutions fit their needs[6].

From the viewpoint of a Cyber Security Analyst, this comparison evaluates the daily requirements encompassing both analytical functionalities and remediation alternatives. My aim is to offer organizations insights into product options and assist antivirus vendors and threat intelligence providers in understanding the essential components needed to enhance analyst efficiency.

Furthermore, I chose to examine and contrast open-source solutions with their paid counterparts to support teams grappling with escalating cybersecurity expenses. This analysis serves as an initial defense measure, enabling such teams to safeguard themselves effectively.

## 1.2 Objectives and Criteria for Tool Selection

This thesis aims to thoroughly analyze three key security technologies: Endpoint Detection and Response (EDR), Endpoint Protection Platform (EPP), and traditional Antivirus solutions. Our goal is to understand their features, strengths, and limitations, and see how they help protect against cyber threats. We also want to see how these tools perform in real-world scenarios to provide practical insights into their effectiveness.

The tools we are focusing on are Wazuh, OPENEDR, and Bitdefender for defense, and Caldera for simulating attacks. We chose these tools for a few reasons. First, we wanted to cover a broad spectrum of endpoint security, including both open-source and commercial options. These tools are well-known and widely used in the cybersecurity field, making them relevant for our analysis. Each tool offers unique features, and together they help us get a complete picture of endpoint security.

Wazuh is an open-source tool with strong monitoring capabilities and good community support. It integrates well with other security tools and offers extensive features for threat detection and incident response. OPENEDR, another open-source tool, is known for its advanced threat detection techniques and provides robust protection and detailed forensic capabilities, making it great for our in-depth analysis. Bitdefender is a well-established antivirus solution with advanced threat protection features, included to provide a solid comparison against the open-source solutions.

We are using Caldera, an open-source platform, to simulate real-world cyber attacks and test our security tools. Caldera allows us to create customizable attack scenarios, which helps us thoroughly test how well our tools detect and respond to threats. It uses the MITRE ATT&CK framework, giving us a structured way to simulate tactics and techniques used by real attackers. Additionally, Caldera has strong community support and excellent documentation, making it easier to set up and use for our simulations. This section sets the stage for a detailed look at each tool, explaining why we chose them and how we plan to evaluate them.

## 1.3 Structure of this Thesis

The thesis commences with an introductory overview of the existing array of security tools, aiming to delineate the optimal choice tailored to specific security needs. Subsequently, we expound upon the rationale behind the selection of particular tools for examination.

Following this, a comprehensive comparative analysis is conducted, delving into the strengths and limitations of each solution in theoretical contexts. Subsequent to this theoretical exploration, both solutions are implemented in a controlled test environment for practical evaluation. Herein, a series of tests involving simulated attacks and malicious code are executed to discern performance differentials.

In the concluding section, the results of these evaluations are presented, including a comparative assessment of the performance of each tool and an identification of their respective weaknesses. Additionally, recommendations are provided for organizations seeking to bolster their security posture through the adoption of these technologies, whether through open-source alternatives or commercial solutions.

## 1.4 Purpose of Thesis

This thesis is structured into two main parts: the theoretical analysis and the practical implementation. In the theoretical part, we aim to analyse the security systems that can be deployed on a computer and the protection they offer against various cyber attacks. The focus is on three key security technologies: Endpoint Detection and Response (EDR), Endpoint Protection Platform (EPP), and Anti-Virus (AV). Each of these systems plays a crucial role in safeguarding endpoints, often complementing each other to prevent or impede the execution of malware. This analysis will explore how these technologies function individually and in combination to enhance overall security posture.

The practical part involves setting up a controlled test environment to evaluate the real-world effectiveness of these security systems. Specifically, we will configure a Domain Controller with two user accounts, each equipped with installed EDR solutions. A third user will simulate attacks on this environment, allowing us to observe and document the behaviour and response of the EDR systems under attack conditions. This hands-on approach aims to provide practical insights into the operational capabilities and limitations of EDR technologies in detecting and mitigating cyber threats.

By integrating both theoretical analysis and practical implementation, this thesis seeks to provide a comprehensive understanding of endpoint security technologies, their effectiveness in real-world scenarios, and actionable insights for improving cybersecurity defences.

## 1.5 Methodology

This study utilizes a mixed-methods approach, combining qualitative and quantitative analyses to evaluate Endpoint Detection and Response (EDR), Endpoint Protection Platform (EPP), and Antivirus technologies. The methodology comprises three phases: literature review, comparative analysis, and practical implementation.

Literature Review
A comprehensive review of existing knowledge on EDR, EPP, and Antivirus technologies was conducted, sourcing from academic journals, industry reports, whitepapers, and vendor documentation. This phase established a theoretical foundation, identified best practices, and highlighted common challenges, aiding in developing criteria for evaluating the effectiveness of these security solutions.

Comparative Analysis
Various EDR, EPP, and Antivirus solutions were evaluated based on predefined criteria such as detection capabilities, response time, usability, integration with other tools, and cost-effectiveness. Data was collected from vendor documentation, independent reviews, benchmark tests, and user feedback. Solutions were systematically scored to identify their strengths and weaknesses, providing a clear comparative overview.

Practical Implementation
Selected security tools were deployed in a controlled test environment, simulating an enterprise network with endpoint devices, servers, and network components. Tools were configured per vendor recommendations, involving agent installation, management console setup, and security policy definition. Attack scenarios such as malware infections, ransomware attacks, data exfiltration, and zero-day exploits were executed to test the effectiveness of each solution, focusing on detection accuracy, response time, performance impact, and false positive rates.

Data was analyzed to assess each solution's effectiveness in mitigating cyber threats. Tests were repeated for consistency, using independent verification tools, and consulting cybersecurity experts to validate the methodology and findings. Ethical guidelines ensured no sensitive data or production systems were used, with all tests conducted in a controlled environment.

This structured approach aims to provide valuable insights into the effectiveness of EDR, EPP, and Antivirus technologies in protecting against contemporary cyber threats, helping organizations make informed decisions about their digital defenses

# 2. Security Solutions

In the ever-evolving landscape of cybersecurity threats, the demand for effective security solutions is paramount. This introduction provides an overview of the diverse array of security tools available to organizations today. From Endpoint Detection and Response (EDR) systems to Endpoint Protection Platforms (EPP) and traditional antivirus solutions, each offers unique functionalities and advantages in safeguarding against cyber threats. As organizations navigate through the complexities of modern cybersecurity challenges, understanding the strengths and limitations of these security solutions becomes crucial. This thesis aims to explore and analyze the efficacy of various security solutions, shedding light on their functionalities, practical applications, and suitability for different organizational needs. By delving into the intricacies of these technologies, organizations can make informed decisions to bolster their cybersecurity defenses and mitigate the risks posed by ever-evolving cyber threats[7].

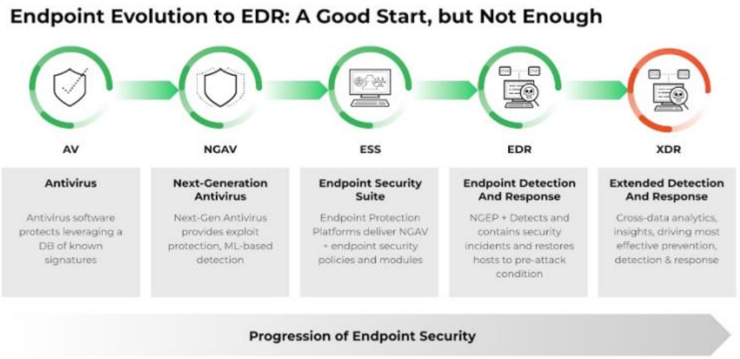

Endpoint Evolution to EDR: A Good Start, but Not Enough
AV
NGAV
ESS
EDR
XDR
Antivirus
Antivirus software protects leveraging a DB of known signatures
Next-Generation Antivirus
Next-Gen Antivirus provides exploit protection, ML-based detection
Endpoint Security Suite
Endpoint Protection Platforms deliver NGAV + endpoint security policies and modules
Endpoint Detection And Response
NGEP + Detects and contains security incidents and restores hosts to pre-attack condition
Extended Detection And Response
Cross-data analytics, insights, driving most effective prevention, detection & response
Progression of Endpoint Security

**Figure 2. Endpoint Evolution**

## 2.1 Endpoint Detection and Response (EDR)

EDR, short for Endpoint Detection and Response or Endpoint Threat Detection & Response, was coined in 2013 by researcher Anton Chuvakin. It serves as a tool for alerting security teams to suspicious activity within a network, aiming primarily to prevent attacks before they occur rather than merely mitigating threats. EDR systems defend against potential breaches by deploying agents on all connected endpoint devices, capable of identifying anomalies overlooked by firewalls, such as registry changes and file manipulations.

These tools empower companies to contain malicious files, investigate historical data for potential compromises, and respond swiftly to threats. EDR aggregates endpoint statistics, including processes, network connections, and file executions, to detect and respond to malicious actions. Furthermore, EDR systems often integrate AI or machine learning features to identify emerging threats based on suspicious activity[8].

In summary, EDR systems monitor endpoint behavior and mitigate attacks on devices with installed agents. When combined with other security measures like antivirus, IDS, IPS, and device discovery, they offer multi-layered protection and a comprehensive security posture assessment across the enterprise[9].

EDR has the ability to:

1. Monitor all the traffic (network data) from endpoints for abnormalities or figures that might indicate a cyber threat or a breach
2. Automated response capabilities, remove or isolate all threats and malicious files, and inform the security team of their presence and risk to the network.
3. Search on the internet for threats that exist on the system based on their signatures (hashes)
4. Incident investigation and forensic capabilities to enable security teams to perform detailed analysis and forensic investigation of endpoint devices and related network communications
5. Advanced threat detection and response to identify, isolate, and respond to advanced threats, ransomware, and malicious processes on endpoint device

## 2.2 Network Detection & Response (NDR)

Network Detection and Response (NDR) stands as another vital security solution, offering comprehensive insight into a company's network vulnerabilities, whether known, unknown, or zero-day. NDR streamlines internal management through a unified console, leveraging Artificial Intelligence for investigative purposes and scrutinizing inbound and outbound traffic. Through the utilization of playbooks, NDRs can autonomously enact remedial actions and address diverse threats[10].

In contrast to NDR, Endpoint Detection and Response (EDR) prioritizes monitoring and, when deemed necessary, blocking suspicious network traffic. Should threat actors breach EDR defenses, NDR serves as a secondary barrier, poised to intercept and neutralize potential threats. NDRs excel in monitoring network activity variances and correlating them with endpoint and cloud data, enabling real-time threat response at the packet level. This granular analysis occurs as packets enter the network, ensuring swift detection and mitigation of emerging threats.

Optimal NDR implementation involves integration with complementary solutions like Security Information and Event Management (SIEM), Endpoint Detection and Response (EDR), and log analysis tools, maximizing overall cybersecurity efficacy.

## 2.3 Extended Detection and Response (XDR)

XDR represents another prominent solution currently in use, aiming to revolutionize threat detection and response methodologies. It adopts a proactive stance by offering a unified platform that grants visibility across multiple data streams, encompassing endpoints, networks, and cloud environments. Positioned as the evolutionary successor to EDR, XDR enhances effectiveness through the seamless integration of various data sources, including applications, networks, and data repositories[11].

The XDR approach addresses common challenges encountered by security professionals, such as alert prioritization difficulties, tool diversity, and alert overload. By correlating security events across disparate environments, security teams can detect and thwart attacks like ransomware at earlier stages, thereby mitigating potential damage. Notably, XDR platforms manifest in three distinct types: Native (restricted to products from a single vendor), Open (compatible with all vendors), and Hybrid (capable of integrating data from select external vendors, albeit with limitations).

## 2.4 Security Information Event Management (SIEM)

SIEM, an acronym for Security Information and Event Management, denotes a specialized software or hardware solution enabling organizations to gather, analyze, and address security-related data from diverse sources instantaneously. SIEM solutions typically encompass two primary components:

- A Security Information Management (SIM) system tasked with collecting and storing data pertaining to security events, encompassing log files, network traffic data, and alerts from devices like firewalls and IDS.

- An Event Correlation and Analysis (ECA) system responsible for scrutinizing the data amassed by the SIM system, identifying potential security threats or anomalies, typically through log file analysis to detect suspicious activities like failed login attempts or alterations to system configuration files and notifying the security operations team of potential issues[12].

SIEM aims to expedite the detection and response to security threats by offering real-time visibility into security-related data from diverse sources, streamlining the identification and mitigation of potential security incidents. Widely employed in the security domain, SIEM assists enterprises and organizations in safeguarding their networks and systems against various threats such as hacking, cyber-attacks, and data breaches[13].

## 2.5 Security Orchestration, Automation, and Response (SOAR)

SOAR, which stands for Security Orchestration, Automation, and Response, offers organizations a comprehensive solution to enhance and streamline their incident response procedures. By furnishing a unified platform, SOAR facilitates the coordination and automation of various incident response tasks and activities[14].

Key features of SOAR platforms typically include:

- Automated incident triage and prioritization, expediting the identification and response to critical incidents.
- Workflow automation enables organizations to define and automate incident response procedures such as investigation and remediation.
- Integration with diverse security tools and systems like SIEMs, firewalls, and intrusion detection systems facilitates data collection and analysis from multiple sources.
- Collaboration and communication tools, facilitating effective information sharing and coordination among incident response teams.
- Playbook and case management systems for storing and reusing standard incident response procedures and templates.

The primary objective of SOAR is to enhance the speed, efficiency, and effectiveness of incident response processes by automating routine tasks and providing a centralized platform for managing incident response efforts. By automating repetitive tasks and incident triage, security teams can focus on higher-level response and investigation activities, enabling organizations to respond to incidents more promptly and adeptly. Furthermore, SOAR bridges the gap between security operations and incident response teams by offering a unified platform for viewing, investigating, and managing all types of incidents[15].

## 2.6 Intrusion Detection System (IDS)

An IDS, or Intrusion Detection System, is a security software or hardware solution crafted to identify and notify of potential security threats or intrusions within a computer or network environment.

There are two primary types of IDS:

- Network-based IDS (NIDS): Examines network traffic to detect indications of malicious activity, such as irregular traffic patterns or attempts to exploit known vulnerabilities.
- Host-based IDS (HIDS): Analyzes activity on a specific host (e.g., computer or server) to spot signs of malicious behavior, such as alterations to system files or unauthorized access attempts.

Operating by monitoring network or system activity, an IDS compares it against predefined rules or patterns to flag potentially malicious behavior. Upon detecting a possible intrusion or threat, the IDS issues an alert and may enact automated responses, like blocking network traffic from a specific IP address or isolating a suspicious file. Some IDS systems can integrate with other security solutions, like SIEMs, to offer more comprehensive analysis and response capabilities.

Typically employed as part of an organization's broader security strategy, an IDS works in tandem with other security solutions such as firewalls, antivirus software, and intrusion prevention systems (IPS) to furnish multiple layers of protection[16].

## 2.7 Intrusion Prevention System(IPS)

An IPS, or Intrusion Prevention System, is a network security solution engineered to identify and thwart security threats or intrusions within a computer or network environment. By scrutinizing network traffic, an IPS detects potential security threats like attempts to exploit known vulnerabilities or access restricted resources. Upon identifying a potential threat, the IPS can execute various actions to thwart the threat's success, such as blocking network traffic from a specific IP address or isolating a suspicious file[17].

There are two primary types of IPS:

- Network-based IPS (NIPS): Analyzes network traffic to uncover indications of malicious activity, such as irregular traffic patterns or attempts to exploit known vulnerabilities.
- Host-based IPS (HIPS): Examines activity on a specific host (e.g., computer or server) to detect signs of malicious behavior, like alterations to system files or unauthorized access attempts.

Unlike an IDS, which merely alerts on potential malicious traffic and security breaches, an IPS takes proactive measures to prevent such incidents from occurring. IPS is generally considered more advanced than IDSs as it can both detect and prevent intrusions[18].

Typically integrated into an organization's overall security strategy, an IPS collaborates with other security solutions like firewalls, antivirus software, and intrusion detection systems (IDS) to furnish multiple layers of protection[19].

## 2.8 Antivirus (AV) & Next Generation AntiVirus - NGAV

Antivirus (AV) software is a foundational component of cybersecurity, designed to detect, prevent, and remove malicious software (malware) from computer systems. Traditional AV relies heavily on signature-based detection, which matches known malware signatures against files on the system. While effective against known threats, this approach needs help to identify new and evolving malware variants, including polymorphic and fileless malware.

Next-Generation Antivirus (NGAV) represents a significant evolution in antivirus technology, leveraging advanced techniques such as machine learning, behavioral analysis, and artificial intelligence (AI) to enhance threat detection capabilities. Unlike traditional AV, NGAV solutions focus on behavior-based detection, analyzing the actions and behaviors of files and processes to identify suspicious or malicious activity. By monitoring system behavior in real time, NGAV can detect previously unseen threats, including zero-day exploits and advanced persistent threats (APTs)[20].

NGAV solutions offer several advantages over traditional AV, including improved detection rates, reduced false positives, and better protection against unknown threats. By continuously adapting to emerging threats and evolving attack techniques, NGAV provides organizations with a more robust defense against modern cyber threats. Integrating NGAV into cybersecurity strategies enhances overall security posture and helps organizations stay ahead of sophisticated adversaries in today's rapidly evolving threat landscape[21].

## 2.9 Firewall

Firewalls are pivotal guardians of network security, serving to shield private networks from unauthorized access and malicious threats. Available in software or hardware forms, they meticulously manage incoming and outgoing network traffic based on predefined security protocols.

Situated between internal networks and the vast Internet, firewalls meticulously inspect each data packet, allowing only authorized traffic to pass while repelling unwanted intrusions. They come in two main types: network firewalls, positioned at the network perimeter, and host-based firewalls, installed on individual devices.

Utilizing various techniques such as packet filtering and stateful inspection, firewalls scrutinize network traffic to detect and neutralize potential threats. However, they're just one part of a robust security strategy. Integrating firewalls with antivirus software, intrusion detection systems, and security incident management enhances overall defense against evolving cyber threats.[22].

## 2.10 Data Loss Prevention (DLP)

DLP (Data Loss Prevention) is a security measure designed to prevent the loss, theft, or misuse of sensitive data within organizations. DLP solutions are crafted to detect, monitor, and safeguard sensitive information like credit card details, financial records, and personal data throughout its lifecycle[23].

Comprising a blend of software, hardware, and policies, DLP solutions help organizations protect sensitive data, whether stored on-premises, in the cloud, or via hybrid setups. Key features of DLP solutions include:

- Data discovery: Automatically locating sensitive information across various systems, including endpoints, servers, and cloud services.
- Data classification: Categorizing sensitive data based on predefined policies, such as credit card numbers or personal health information.
- Data monitoring: Observing and analyzing data in real-time to detect and respond to violations.
- Data encryption: Encrypting sensitive data to prevent unauthorized access.
- Data blocking: Preventing the transfer or sharing of sensitive data via email, instant messaging, or other communication channels.
- Reporting and auditing: Providing reports and audit trails to track data breaches and compliance violations.

By deploying DLP solutions, organizations can better protect sensitive data and adhere to regulations like HIPAA, PCI-DSS, and GDPR. These solutions offer visibility and control over sensitive data, helping to mitigate the risk of data breaches and compliance lapses.

### 2.11 Managed Detection and Response (MDR)

Managed Detection and Response (MDR) represents a proactive cybersecurity service integral to modern threat mitigation strategies. MDR offers continuous monitoring, analysis, and response to cyber threats by combining advanced technology with human expertise. Unlike conventional security approaches, MDR delivers real-time detection of suspicious activities across networks, endpoints, and systems. MDR providers employ sophisticated threat intelligence and detection algorithms, enabling swift identification and neutralization of threats. Furthermore, MDR teams conduct thorough investigations into security incidents, offering actionable insights to bolster organizational defenses. By outsourcing detection and response capabilities, organizations augment their cybersecurity posture, mitigate risks, and ensure rapid incident response. MDR serves as a critical component in safeguarding sensitive data and infrastructure from evolving cyber threats, aligning with the evolving landscape of cybersecurity challenges.[24]

## 3. Endpoint Detection and Response (EDR)

EDR solutions are becoming increasingly important as the number of endpoint devices and the volume of data they generate continue to grow, and as the threat landscape becomes more complex and sophisticated.[25] EDR solutions can help organizations to detect and respond to security incidents more quickly and effectively, and to improve their overall security posture.

Since in this thesis, we will focus on EDR solutions, we should analyze these technologies by further clarifying the types of EDRs that exist and compare the technologies and their capabilities, whether they are paid or open source ones.

## 3.1 How EDR detects malicious activity

It is important at this point to describe how an EDR is able to detect malicious activity. This process is called hooking.

Function hooking refers to intercepting the system call or a specific function and altering its standard behavior of it. This means that an EDR system would intercept a specific function of system activity, for example, file system operations, process creation, network traffic, etc. It would insert a hook that sits in the middle on the function call and its destination that would allow it to inspect and alter the information being passed.

To be more precise, an EDR may create a hook to the CreateProcess function that is in charge of creating new processes in the system. Every time a new process is created, the hook will check the process information being passed to the function. EDR would ensure, based on the analysis, whether this behavior matches the patterns of known malicious activity. On the fact that the process has malicious intent, EDR would block or quarantine the specific action.

Likewise, the EDR could also hook to functions such as WriteFile or CreateFile, which are related to file system activity. By doing that, EDR could analyze that activity in order to detect and prevent activities like file encryption, file deletions, or modifications in general. Apart from the previous, EDR systems can use hooking techniques on network-related functions. By hooking to send or receive, it could analyze all the data being communicated between processes and the external network. This would result in detections of data exfiltration, command and control communication, etc.[26]

## 3.2 Types of EDR

As said earlier, there are several types of Endpoint Detection and Response (EDR) solutions, each with their own specific capabilities and approaches to threat detection and response.

Some common types of EDR solutions include:

- Agent-based EDR: This type of EDR solution uses a software agent that is installed on endpoint devices to collect and transmit data about the device's activity and network communications to a central management console. This type of EDR solution typically It offers advanced threat detection and response capabilities and also allows for real-time monitoring and management of endpoint devices.
- Agentless EDR: This type of EDR solution uses network-based sensors or other types of collection mechanisms that don't require the installation of an agent on endpoint devices. This type of EDR solution typically relies on analyzing network traffic, or events logged by other security solutions, such as firewall logs, to detect and respond to threats.
- Cloud-based EDR: This type of EDR solution uses cloud-based infrastructure to collect, store, and analyze data from endpoint devices. They are designed to allow organizations to easily scale their EDR capabilities, and can offer more advanced threat detection and response capabilities by using cloud-based analytics and machine learning.[27]

- Endpoint Protection Platform (EPP): This type of EDR includes both traditional security solutions, for example antivirus, firewalls and IPS, as well as more advanced features like endpoint detection and response, in a single integrated platform.
- Behavioral EDR: This type of EDR solution uses artificial intelligence, machine learning, and behavioral analysis in order to detect unusual activity on endpoint devices. It can detect and respond to unknown threats that it uses against traditional security solutions.[28]

All these kinds of EDR solutions have their own strengths and weaknesses. Some of them may be better suited for some organizations and use cases. It is vital for an organization to analyze its needs and use cases in order to choose the EDR solution that fits its needs.

## 3.3 EDR general capabilities

Endpoint Detection and Response (EDR) solutions usually include a wide range of capabilities that are designed to detect and respond to security threats on endpoint devices.

Some common capabilities of EDR solutions include the following:

- Continuous monitoring and visibility: EDR solutions continuously monitor endpoint devices for signs of suspicious activity or anomalies, and provide detailed visibility into the activity on each device.
- Advanced threat detection and response: EDR solutions use advanced threat intelligence, machine learning, and heuristics to identify known and unknown threats, including advanced persistent threats (APTs), ransomware, and other malware.
- Incident investigation and forensic capabilities: EDR solutions provide detailed information and analysis of endpoint activity, allowing security teams to perform forensic investigations and determine the scope and impact of security incidents.
- Automated response capabilities: EDR solutions can be configured to automatically respond to detected threats, such as isolating or quarantining infected endpoint devices.[29]
- Integration with other security solutions: EDR solutions can be integrated with other security solutions, such as firewalls, intrusion detection systems (IDS), and security information and event management (SIEM) systems, to provide a comprehensive view of security across an organization.[30]
- Compliance and reporting: EDR solutions can provide detailed reporting and logging for compliance and auditing purposes.
- Remote management: EDR solutions typically provide a centralized management console, which allows security teams to manage endpoint devices, deploy remotely Endpoint Detection updates and patches, as well as monitoring and responding to security incidents from a single location.[31]
- Cloud-based solution: Some EDR solutions are cloud-based, which allows for easy scalability and management of endpoint devices and can also provide more advanced threat detection and response capabilities by leveraging cloud-based analytics and machine learning.

## 3.4 Paid & Open Source Solutions for EDR

Paid EDR Solutions:

1. Carbon Black: Known for real-time threat detection and response, Carbon Black offers features like behavioral analytics and integrated incident response capabilities.
2. Crowdstrike: This cloud-based EDR solution provides real-time threat detection, response, and forensic capabilities, with features such as machine learning and behavioral analytics.
3. McAfee Endpoint Protection: Offering comprehensive EDR features like real-time threat detection and response, McAfee Endpoint Protection is a robust solution in the market.
4. Symantec Endpoint Protection: Symantec's EDR solution includes advanced threat protection, incident response capabilities, and features like behavioral analysis and cloud-based threat intelligence.
5. Trend Micro: Trend Micro provides advanced threat protection and incident response capabilities with features like behavioral analysis, machine learning, and AI-based threat detection.
6. FortiEDR: Developed by Fortinet, FortiEDR offers advanced threat protection and incident response capabilities tailored for endpoints.[32]

Open Source EDR Solutions:

1. OSSEC: A host-based intrusion detection system (HIDS) for monitoring and detecting malicious activity on systems.
2. AIDE: An open-source HIDS to detect changes to files on a system.
3. SELKS: A network security distribution based on Debian, offering intrusion detection and response capabilities.
4. Auditd: A system and application auditing tool for tracking and detecting suspicious activity on systems.
5. Suricata: A free and open-source intrusion detection and prevention system for monitoring network traffic.
6. WHIDS: An open-source EDR tool focusing on Windows systems for continuous monitoring of system events and behaviors.
7. Zeek (Bro): A powerful network security monitoring system for capturing, analyzing, and alerting network traffic.
8. Wazuh: A free and open-source security platform unifying XDR and SIEM capabilities across various environments.[33]

While paid solutions offer robust features and vendor support, open-source solutions provide cost-effective alternatives, albeit with potentially more customization and technical expertise required. Organizations should assess their specific needs and evaluate features, costs, and capabilities before choosing between paid or open-source EDR solutions.

## 3.5 Paid vs. open-source solutions

Paid Endpoint Detection and Response (EDR) solutions are typically more feature-rich and provide more support from the vendor compared to open-source options. They typically include advanced threat detection and response capabilities, such as behavioral analytics and machine learning, and have the ability to integrate with other security tools like SIEM and threat intelligence platforms. Paid EDR solutions often come with managed service options, where dedicated security experts monitor and respond to incidents 24/7.[34]

They also provide rich reporting capabilities that allow organizations to identify and track security trends over time. However, paid EDR solutions are typically more expensive and require more resources to deploy, operate, and maintain, but they also provide a more complete and robust set of features, capabilities, and vendor support.

Some of the key features that paid EDR solutions typically include are:

- Real-time threat detection: Paid EDR solutions typically have advanced threat detection capabilities, such as behavioral analytics and machine learning, that can detect malicious activity in real-time.
- Incident response: Paid EDR solutions often include incident response capabilities such as automated incident investigation, automated containment, and incident analysis.
- Advanced threat protection: paid EDR solutions typically provide a wide range of threat protection capabilities, such as anti-malware, anti-ransomware, intrusion prevention, and memory-based protection.
- Forensics: Paid EDR solutions often include advanced forensic capabilities such as memory analysis, live response, and incident visualization.
- Integration: Paid EDR solutions typically provide integration with other security tools such as SIEM, threat intelligence platforms, and incident management systems.
- Managed Services: Many EDR solution providers offer managed service options, which can provide organizations with the benefits of having dedicated security experts to monitor and respond to incidents 24/7.
- Reporting: Paid EDR solutions often provide rich reporting capabilities, such as vulnerability reports, compliance reporting, and incident summaries, that help organizations identify and track security trends over time.

Open-source EDR solutions, on the other hand, are often free to use and can be customized to meet the specific needs of an organization. They are typically more flexible and can be used to build a custom security solution. These tools may also need more support and documentation available with paid solutions, and they may provide a different level of incident response and forensic capabilities.

Ultimately, the decision between using a paid or open-source EDR solution will depend on the specific needs and resources of the organization. While open-source EDR solutions can be a good fit for organizations with small budgets and technical expertise, paid EDR solutions may be a better option for organizations that require more advanced features and support. It's important to understand the specific requirements of the organization and evaluate the features, costs, and capabilities of each solution before making a decision on which of the two to use.

In terms of budget, paid EDR solutions like FortiEDR can be more expensive than open-source options. It's important to evaluate the costs associated with deploying and maintaining the solution and compare them to the benefits that the solution offers to the organization.

In terms of specific security challenges, it's important to consider what types of threats and attacks the organization is facing and whether the solution can provide adequate protection and response capabilities. For example, if an organization is particularly concerned about advanced threats such as zero-day attacks, then a paid solution like FortiEDR, which has advanced threat detection and response capabilities, may be a better fit.[35]

When considering FortiEDR specifically, it's important to evaluate the solution's features, capabilities, and support offered by Fortinet. Furthermore, integration with other Fortinet solutions may provide a holistic security posture for an organization, but it also could introduce some complexity and additional costs depending on the organization's current security stack and infrastructure.

# 4. Endpoint Protection Platform (EPP)

Endpoint Protection Platform (EPP) is a comprehensive cybersecurity solution designed to secure endpoint devices such as desktops, laptops, servers, and mobile devices within an organization's network. Unlike traditional antivirus software, which primarily focuses on detecting and removing malware, EPP offers a broader range of security features to protect endpoints against various cyber threats. Combines multiple security technologies and functionalities to protect endpoint devices against a wide range of cyber threats. By integrating antivirus, firewall, EDR, behavioral analysis, DLP, encryption, and other security features into a unified platform, EPP helps organizations strengthen their endpoint security posture and mitigate the risk of security breaches and data loss.[36]

## 4.1 How EPP detects malicious activity

Endpoint Protection Platforms (EPP) detect malicious activity through a combination of signature-based detection, behavioral analysis, and machine learning algorithms. Here's how EPP detects malicious activity:

1. Signature-based detection: EPP systems maintain a database of known malware signatures. When a file matches a signature in the database, indicating it's a known threat, the EPP flags it as malicious.[37]

2. Behavioral analysis: EPP monitors endpoint behavior for suspicious activities that deviate from normal patterns. This includes analyzing processes, network connections, file changes, and registry modifications. If an endpoint exhibits behavior indicative of malware, the EPP raises an alert.

3. Machine learning: EPP employs machine learning algorithms to identify emerging threats and zero-day attacks by analyzing large datasets of benign and malicious activity. Machine learning models can detect patterns and anomalies that may evade traditional signature-based detection.[38]

4. Heuristic analysis: EPP uses heuristics to identify potentially malicious code based on its structure and behavior, even if it doesn't match known signatures. Heuristic analysis helps detect polymorphic and previously unseen malware variants.

5. Cloud-based threat intelligence: EPP solutions leverage threat intelligence feeds from cloud-based repositories to augment detection capabilities. These feeds provide real-time information about emerging threats, allowing EPP to identify and respond to new threats quickly.

By employing these detection techniques, EPP can proactively identify and mitigate a wide range of cyber threats, including malware, ransomware, phishing attempts, and other malicious activities targeting endpoint devices within an organization's network.

## 4.2 Types of EPP

Endpoint Protection Platforms (EPP) come in various types, each offering distinct features tailored to different security needs:

1. Traditional EPP: These platforms focus on signature-based detection and prevention methods, relying on known malware signatures to identify threats. They typically include antivirus, firewall, and intrusion detection capabilities.
2. Advanced EPP: Advanced EPP solutions incorporate machine learning, behavioral analytics, and heuristic analysis to detect and respond to sophisticated threats. They provide real-time threat intelligence and prioritize actionable alerts to enhance incident response.
3. Cloud-Based EPP: Cloud-based EPP solutions offer scalability and flexibility by leveraging cloud infrastructure. They provide centralized management and visibility across distributed endpoints, facilitating rapid deployment and updates.
4. Integrated EPP: Integrated EPP platforms combine endpoint security with other security layers, such as network security, email security, and identity and access management. This approach offers comprehensive protection and centralized management of security policies.[39]
5. Managed EPP: Managed EPP services are outsourced to third-party providers who oversee the deployment, monitoring, and management of endpoint security. This option is suitable for organizations needing more in-house expertise or resources to maintain EPP solutions.

Each type of EPP offers unique advantages, allowing organizations to choose the most suitable solution based on their security requirements, infrastructure, and budget.

## 4.3 Paid & Open Source Solutions

Certainly, here are examples of both paid and open-source solutions for Endpoint Protection Platform (EPP):

Paid Solutions:

- Symantec Endpoint Security: Symantec Endpoint Security is a comprehensive endpoint security solution that offers advanced threat protection, endpoint detection and response (EDR), firewall, intrusion prevention, and device control features. It provides centralized management and support for Windows, macOS, Linux, and virtual environments.
- CrowdStrike Falcon: CrowdStrike Falcon is a cloud-native endpoint protection platform that leverages artificial intelligence (AI) and machine learning to detect and prevent malware, ransomware, and advanced threats. It offers real-time visibility, threat-hunting

capabilities, and automated response options.[40]

- McAfee Endpoint Security: McAfee Endpoint Security provides a unified defense platform for endpoint devices, offering antivirus, firewall, device control, and web control features. It includes behavioral analysis, sandboxing, and machine learning capabilities for advanced threat detection and response.
- Carbon Black Endpoint Security: Carbon Black Endpoint Security offers next-generation antivirus (NGAV), endpoint detection and response (EDR), and threat-hunting capabilities. It provides real-time visibility into endpoint activity, automated response options, and integration with SIEM and SOAR platforms.

Open Source Solutions:

- Osquery: Osquery is an open-source endpoint visibility tool that enables organizations to query and monitor endpoint devices in real time using SQL-like queries. It provides visibility into system processes, file events, network connections, and registry changes, helping to identify and investigate security incidents.
- Security Onion: Security Onion is an open-source platform for network security monitoring and intrusion detection. It includes a suite of security tools, including Suricata, Zeek (formerly Bro), Snort, and Elastic Stack, for detecting and analyzing network traffic and endpoint events.
- Wazuh: Wazuh is an open-source endpoint security platform that integrates intrusion detection, log analysis, file integrity monitoring, and vulnerability detection capabilities. It provides centralized management and monitoring of endpoint devices, along with real-time alerts and response options.
- Cylance Protect: Cylance Protect is an AI-driven endpoint protection solution that uses machine learning algorithms to prevent malware and advanced threats. It offers pre-execution, runtime, and post-execution detection capabilities, along with threat-hunting and response features.

## 4.4 Paid vs Open source solutions

Comparing Paid and Open Source Solutions for Endpoint Protection Platform (EPP) entails assessing various factors, including features, support, customization, and cost. Here's a concise examination of the key distinctions between the two:

1. Features and Functionality:

- Paid Solutions: Paid EPP solutions typically offer comprehensive feature sets, including advanced threat detection, centralized management, real-time monitoring, and integration with other security tools. They often provide additional functionalities such as behavioral analysis, machine learning, and proactive threat hunting.[41]

- Open Source Solutions: While open-source EPP solutions may offer basic endpoint protection features, they often need more advanced capabilities and scalability of paid solutions. However, some open-source projects may provide flexibility for customization and integration with other security tools.

2. Support and Maintenance:

- Paid Solutions: Paid EPP solutions typically come with vendor support, including access to technical assistance, software updates, and security patches. This level of support ensures timely response to security incidents and ongoing maintenance of the platform.
- Open Source Solutions: Support for open-source EPP solutions may vary, depending on community contributions and third-party vendors. While some projects may offer community support forums and documentation, organizations may need to rely on internal resources or third-party services for assistance and maintenance.

3. Customization and Flexibility:

- Paid Solutions: Paid EPP solutions often provide greater flexibility for customization and integration with existing security infrastructure. They may offer APIs, SDKs, and scripting capabilities that enable organizations to tailor the platform to their specific requirements and workflows.
- Open Source Solutions: Open-source EPP solutions offer flexibility for organizations to modify and extend the software according to their needs. With access to source code, organizations can customize features, develop extensions, and integrate with other open-source projects.

4. Cost Considerations:

- Paid Solutions: Paid EPP solutions typically involve licensing fees or subscription-based pricing models. While they may require upfront investment, they often provide predictable costs and comprehensive support.
- Open Source Solutions: Open-source EPP solutions are generally free to use, but organizations may incur costs for customization, implementation, and ongoing support. While they offer cost savings upfront, organizations should consider the total cost of ownership, including internal resources and third-party services.

In summary, the choice between paid and open-source solutions for Endpoint Protection Platform (EPP) depends on factors such as feature requirements, support needs, customization flexibility, and budget considerations. While paid solutions offer comprehensive features and vendor support, open-source solutions provide flexibility and cost savings but may require additional resources for customization and maintenance. Organizations should evaluate their specific requirements and weigh the pros and cons of each option before making a decision.

## 4.5 Various misconceptions that arise between Endpoint Protection Platform (EPP) and Endpoint Detection and Response (EDR) systems.

Having delved into the core components of both Endpoint Protection Platform (EPP) and Endpoint Detection and Response (EDR) systems and scrutinized their interrelation, it becomes imperative to dispel prevalent misconceptions surrounding these two pivotal security features.

The prevalent belief that organizations are compelled to opt exclusively for either an Endpoint Protection Platform (EPP) or an Endpoint Detection and Response (EDR) system is fallacious. Rather than a binary decision, these represent two distinct yet interdependent capabilities. Conceiving of EPP as a vehicle and EDR as its engine underscores the necessity for their symbiotic collaboration to attain optimal outcomes.[42]

Contrary to common belief, Endpoint Protection Platform (EPP) does not solely entail passive threat prevention. While prevention indeed constitutes a vital facet of EPP, it constitutes merely one facet of the platform's multifaceted protective arsenal. True EPP encompasses not only prevention but also encompasses detection, threat hunting, threat intelligence, and vulnerability management.

While an autonomous Endpoint Detection and Response (EDR) system holds significance in deciphering network-wide endpoint activities, it alone falls short in defending against contemporary cyber threats comprehensively. Effective defense mandates the utilization of a broader spectrum of capabilities, including those fueled by human intelligence and supplementary technologies, to fortify organizational security robustly.

To enhance clarity and comprehension, additional insights and elaboration are necessary to elucidate the intricate relationship between EPP and EDR, dispel misconceptions, and emphasize the importance of a multifaceted security approach in mitigating cyber threats effectively.[43]

# 5. Antivirus Security Technologies

Antivirus security technologies encompass a suite of software tools and methods aimed at safeguarding computer systems from malware threats. These technologies employ real-time scanning, signature-based detection, heuristic analysis, behavioral monitoring, machine learning, and sandboxing techniques to detect, prevent, and remove malicious software. By continuously monitoring system activities and analyzing code patterns and behaviors, antivirus solutions protect against viruses, worms, Trojans, ransomware, and other cyber threats. Ultimately, antivirus security technologies are vital for maintaining the security and integrity of computer systems, helping users mitigate the risks posed by malware, and ensuring the confidentiality and availability of their data.

## 5.1 How Antivirus Security Technologies detects malicious activity

The following text describes the various methods employed by antivirus security technologies to detect malicious activity and protect systems from threats:

1. Signature-Based Detection: This approach entails comparing files or code with a database of known malware signatures. If a match is found, the antivirus identifies the file as malicious. However, this method may need help with new or unknown threats.
2. Heuristic Analysis: Antivirus programs utilize heuristic analysis to detect suspicious behavior based on predefined rules or algorithms. This method can identify previously unknown malware by examining code patterns and behavior.
3. Behavioral Analysis: Antivirus software monitors the behavior of programs in real-time to identify suspicious activities such as unauthorized file modifications or attempts to access sensitive system areas. Behavioral analysis can detect zero-day threats and polymorphic malware.
4. Machine Learning and AI: Advanced antivirus solutions employ machine learning and artificial intelligence algorithms to detect and adapt to emerging threats. These technologies analyze vast amounts of data to identify patterns indicative of malicious activity.
5. Sandboxing: Some antivirus solutions use sandboxing techniques to isolate suspicious files and execute them in a controlled environment. By observing the behavior of the file in isolation, the antivirus can determine if it poses a threat to the system.
6. Cloud-Based Detection: Antivirus programs may leverage cloud-based detection

engines to augment local scanning capabilities. This allows them to access up-to-date threat intelligence and perform a more comprehensive analysis of potential threats.

7. File Reputation Services: Antivirus software may rely on file reputation services to determine the trustworthiness of files based on their prevalence and behavior across a large user base. Files with low reputation scores may be flagged as potentially malicious.

By integrating these detection methods, antivirus security technologies can effectively identify and mitigate various forms of malware and other cybersecurity threats, thereby safeguarding systems and data from harm.[44]

## 5.2 Types of Antivirus Security Technologies

Antivirus security technologies encompass a variety of approaches to safeguard systems from malware threats. Some common types include:

1. Signature-Based Detection: This traditional method involves comparing files against a database of known malware signatures.
2. Heuristic Analysis: This proactive approach identifies suspicious behavior and characteristics of files, flagging them as potential threats even if they don't match known signatures.
3. Behavior Monitoring: Monitoring system behavior in real-time to detect unusual or malicious activities, such as unauthorized file modifications or network connections.
4. Machine Learning: Utilizing algorithms to analyze large datasets and identify patterns indicative of malware, enabling more accurate threat detection.
5. Sandboxing: Isolating suspicious files in a controlled environment to observe their behavior without risking damage to the system.
6. Cloud-Based Protection: Leveraging cloud resources for real-time scanning and threat intelligence, providing rapid updates and improved detection rates.
7. Endpoint Detection and Response (EDR): Offering advanced threat detection and response capabilities, including real-time monitoring, threat hunting, and automated response actions.

Each type of antivirus technology plays a crucial role in the defense against malware, collectively forming a comprehensive security posture to protect systems and data from cyber threats.[45]

## 5.3 Paid & Open source solutions

Paid Antivirus Security Technologies:

1. Norton Antivirus: Known for its comprehensive malware protection and real-time threat detection.
2. Kaspersky Antivirus: Offers advanced malware detection and removal capabilities, along with phishing protection and ransomware defense.
3. Bitdefender Antivirus Plus: Provides multi-layered protection against viruses, malware, ransomware, and online threats.
4. McAfee Antivirus: Offers proactive security measures against viruses, malware, and phishing attacks, with regular updates for evolving threats.
5. Avast Antivirus: Features intelligent threat detection, Wi-Fi security scanning, and browser cleanup tools for enhanced protection.

Open-Source Antivirus Security Technologies:

1. ClamAV: A popular open-source antivirus engine designed for detecting viruses, malware, and other malicious software.
2. OpenVAS: An open-source vulnerability scanner and manager that identifies potential threats and vulnerabilities in a network.
3. Moon Secure Antivirus: An open-source antivirus for Windows that provides on-access, on-demand, and on-schedule scanning.
4. LMD (Linux Malware Detect): An open-source malware scanner for Linux systems, which uses threat data from network edge intrusion detection systems to extract malware that is actively being used in attacks and generates signatures for detection.
5. ClamWin: ClamWin is a free, open-source antivirus solution for Windows. It features a high detection rate for viruses and spyware, a simple user interface, and an easy-to-use system for scheduling scans. ClamWin does not include an on-access real-time scanner, so it needs to be used alongside other protective measures.

While paid antivirus solutions typically offer more comprehensive features and dedicated customer support, open-source options provide cost-effective alternatives with customizable configurations. Organizations should evaluate their security needs, budget, and technical expertise before choosing the most suitable antivirus solution.

### 5.4 Paid vs Open source solutions

In the realm of Antivirus Security Technologies, organizations often face the decision between utilizing paid or open-source solutions. Paid solutions typically offer comprehensive feature sets, dedicated support, and seamless integration options. Examples include industry leaders like Norton, McAfee, and Bitdefender. While these solutions may require a financial investment, they often provide advanced threat detection capabilities and regular updates to combat emerging threats.

On the other hand, open-source solutions such as ClamAV and ClamWin offer cost-effective alternatives with community-driven development and flexibility. While they may lack some advanced features and dedicated support, open-source solutions can be customized to meet specific requirements and are often favored by budget-conscious organizations.[46]

Ultimately, the choice between paid and open-source solutions depends on factors like budget, organizational requirements, and desired level of support and features. Both options have their merits and should be carefully evaluated based on the organization's unique needs.

## 6. Practical Implementation of Endpoint Security Solutions

Having established the necessary theoretical foundation and grasped key concepts such as Endpoint Detection and Response (EDR) systems, Anti-Virus (AV) technologies, Endpoint Protection Platforms (EPP), and Domain Controllers (DC), we can now proceed to the practical phase to observe their functionality and understand their significance for user privacy.

## 6.1 Requirements for the Experimental Phase

For the experimental phase, we will set up a comprehensive local network environment that mimics a real-world enterprise setting. This setup will allow us to thoroughly test and evaluate the security solutions in a controlled but realistic scenario.

1. Endpoints Configuration:
   - We will use two endpoints, one running Windows 10 and the other Windows 11. This diversity will help us assess the compatibility and performance of the security solutions across different operating systems.
   - On these endpoints, we will install the following open-source EDR systems: Wazuh and OpenEDR. Each of these solutions offers unique features and capabilities that will provide a broad perspective on EDR effectiveness.[47]

2. Network Infrastructure:
   - Domain Controller (DC): A Domain Controller will be set up to act as the central administrator for the network. The DC will manage user authentication and enforce security policies across the endpoints.
   - Active Directory (AD): AD will be configured on the DC to store information about network objects such as users, computers, and other resources. This configuration is crucial for managing the network's security and organizational hierarchy.
   - DNS Server: The DNS server will be configured to ensure that all endpoints can resolve domain names and access the internet. This setup is essential for testing real-world threat scenarios that involve internet-based threats.

3. Security Solutions Installation:
   - Wazuh: An open-source EDR solution known for its comprehensive monitoring and incident response capabilities. Wazuh will be installed to provide insights into endpoint security and compliance management.
   - OpenEDR: This tool will be added to offer additional layers of endpoint protection, focusing on advanced threat detection techniques and response strategies.

4. Network Security and Privacy Measures:
   - Firewall Configuration: A robust firewall will be set up to control incoming and outgoing network traffic, ensuring that only legitimate traffic is allowed.
   - Intrusion Detection Systems (IDS): These systems will be deployed to monitor network traffic for suspicious activities and potential intrusions.
   - Encryption: Data encryption will be implemented to protect sensitive information from being intercepted or accessed by unauthorized entities.[48]

5. Testing and Evaluation:
   - Simulated Attacks: We will conduct a series of simulated cyber-attacks to test the responsiveness and effectiveness of each EDR solution. These simulations will include common attack vectors such as phishing, malware, and ransomware.
   - Performance Metrics: Key performance indicators (KPIs) such as detection speed, false positive rates, resource utilization, and user impact will be measured and analyzed.
   - Incident Response: The ability of each EDR system to provide actionable insights and facilitate rapid incident response will be a critical evaluation criterion.

This practical setup will provide a comprehensive understanding of how these security solutions perform in a real-world environment, highlighting their strengths and identifying any potential weaknesses. The insights gained will be invaluable for informing best practices in endpoint security and enhancing user privacy protections.

## 6.2 Windows Server a Domain Controllers (DC): The Backbone of Network Management

Domain Controllers (DC) are essential servers within a computer domain, primarily responsible for handling user authentication requests. Commonly used in Windows Active Directory (AD) environments, DCs ensure consistency by replicating AD directory information, including users, authentication credentials, and security policies. Their main function is to verify user identities and enforce security policies to prevent unauthorized access to domain resources. Typically deployed in clusters for enhanced reliability, DCs in Windows AD setups include a Primary Domain Controller (PDC) and Backup Domain Controllers (BDC)[49].

Active Directory (AD) serves as a database and service suite, managing authentication and authorization processes. AD simplifies administrative tasks by providing centralized user and permission management, facilitating single sign-on (SSO) capabilities, and enabling effective backups through centralized file storage. AD relies on protocols such as LDAP, Kerberos, and DNS and is structured into domains, trees, and forests.[50]

Setting up a DC involves assessing domain needs, ensuring security, and implementing best practices like deploying multiple DCs on standalone servers. DCs are vital for managing access, enforcing security policies, and ensuring network resource availability. Implementation options include DNS servers, global catalog capabilities, and Read-Only Domain Controllers (RODC). The benefits of using DCs include increased security, centralized management, scalability, and improved resource management.

## 6.3 Operating System Selection for Domain Controller Implementation

For the experimental component of this thesis, it is essential to select an appropriate operating system to serve as a Domain Controller (DC). The chosen operating system is Windows Server 2019, which possesses all the necessary capabilities to function effectively as a Domain Controller (DC).

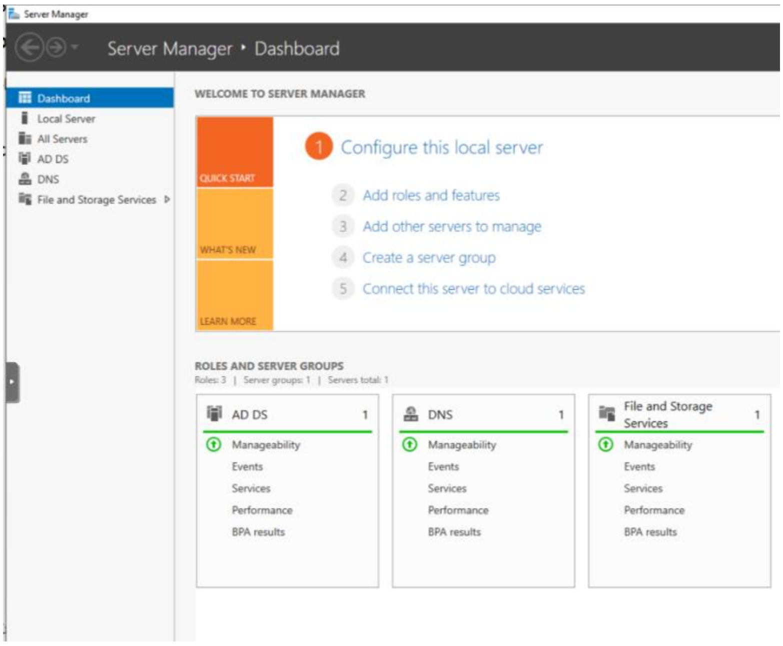
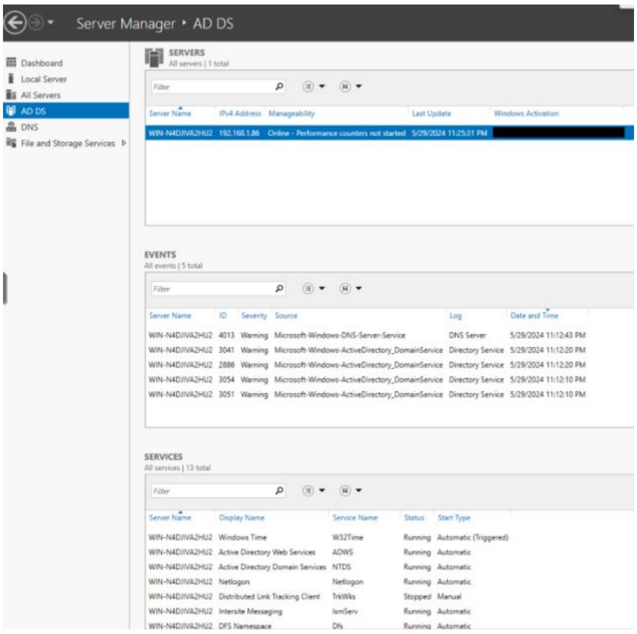


**Figure 3. Windows Server 2019**

Upon launching the operating system, the dashboard displays all the servers required for our setup. The next steps involve configuring Active Directory (AD), the Domain Name System (DNS) server, and the user accounts that will be managed by the Domain Controller (DC).

We can observe the DNS server we have just configured, noting its name and IP address. Below this, we can also review the events and the services currently running on the server.

Similarly, the Active Directory (AD) setup is completed. Like the DNS server, we can see its name and IP address, along with the relevant events and services associated with it. This comprehensive setup ensures that both AD and DNS servers are properly configured and monitored.



SERVERS
All servers | 1 total

| Server Name | IPv4 Address | Manageability | Last Update | Windows Activation |
|---|---|---|---|---|
| WIN-N4DJIVA2HU2 | 192.168.1.86 | Online - Performance counters not started | 5/29/2024 11:25:31 PM | [redacted] |

EVENTS
All events | 5 total

| Server Name | ID | Severity | Source | Log | Date and Time |
|---|---|---|---|---|---|
| WIN-N4DJIVA2HU2 | 4013 | Warning | Microsoft-Windows-DNS-Server-Service | DNS Server | 5/29/2024 11:12:43 PM |
| WIN-N4DJIVA2HU2 | 3041 | Warning | Microsoft-Windows-ActiveDirectory_DomainService | Directory Service | 5/29/2024 11:12:20 PM |
| WIN-N4DJIVA2HU2 | 2886 | Warning | Microsoft-Windows-ActiveDirectory_DomainService | Directory Service | 5/29/2024 11:12:20 PM |
| WIN-N4DJIVA2HU2 | 3054 | Warning | Microsoft-Windows-ActiveDirectory_DomainService | Directory Service | 5/29/2024 11:12:10 PM |
| WIN-N4DJIVA2HU2 | 3051 | Warning | Microsoft-Windows-ActiveDirectory_DomainService | Directory Service | 5/29/2024 11:12:10 PM |

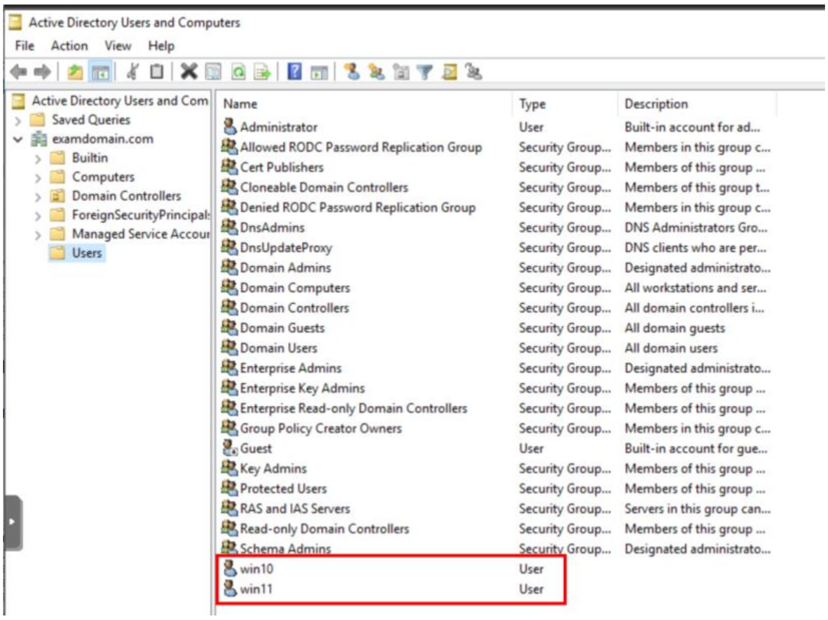
SERVICES
All services | 13 total

| Server Name | Display Name | Service Name | Status | Start Type |
|---|---|---|---|---|
| WIN-N4DJIVA2HU2 | Windows Time | W32Time | Running | Automatic (Triggered) |
| WIN-N4DJIVA2HU2 | Active Directory Web Services | ADWS | Running | Automatic |
| WIN-N4DJIVA2HU2 | Active Directory Domain Services | NTDS | Running | Automatic |
| WIN-N4DJIVA2HU2 | Netlogon | Netlogon | Running | Automatic |
| WIN-N4DJIVA2HU2 | Distributed Link Tracking Client | TrkWks | Stopped | Manual |
| WIN-N4DJIVA2HU2 | Intersite Messaging | IsmServ | Running | Automatic |
| WIN-N4DJIVA2HU2 | DFS Namespace | Dfs | Running | Automatic |

**Figure 4. Configure DNS Server**

To implement this thesis, we need to add two user accounts representing the two endpoints used in this study. In addition to the Administrator account, there will be one account for a computer running Windows 10 (named win10) and another for a computer running Windows 11 (named win11).

Each account has a previously configured designated username and password. Any modifications or operations involving these user accounts will require the Administrator's credentials.



| Name | Type | Description |
|---|---|---|
| Administrator | User | Built-in account for ad... |
| Allowed RODC Password Replication Group | Security Group... | Members in this group c... |
| Cert Publishers | Security Group... | Members of this group ... |
| Cloneable Domain Controllers | Security Group... | Members of this group t... |
| Denied RODC Password Replication Group | Security Group... | Members in this group c... |
| DnsAdmins | Security Group... | DNS Administrators Gro... |
| DnsUpdateProxy | Security Group... | DNS clients who are per... |
| Domain Admins | Security Group... | Designated administrato... |
| Domain Computers | Security Group... | All workstations and ser... |
| Domain Controllers | Security Group... | All domain controllers i... |
| Domain Guests | Security Group... | All domain guests |
| Domain Users | Security Group... | All domain users |
| Enterprise Admins | Security Group... | Designated administrato... |
| Enterprise Key Admins | Security Group... | Members of this group ... |
| Enterprise Read-only Domain Controllers | Security Group... | Members of this group ... |
| Group Policy Creator Owners | Security Group... | Members in this group c... |
| Guest | User | Built-in account for gue... |
| Key Admins | Security Group... | Members of this group ... |
| Protected Users | Security Group... | Members of this group ... |
| RAS and IAS Servers | Security Group... | Servers in this group can... |
| Read-only Domain Controllers | Security Group... | Members of this group ... |
| Schema Admins | Security Group... | Designated administrato... |
| win10 | User | |
| win11 | User | |

**Figure 5. Add users to Active Directory**

## 6.4 Tactics Followed in the Practical Implementation

This section outlines the specific tactics followed in the practical implementation of Endpoint Detection and Response (EDR) and Antivirus solutions. These tactics are essential to understanding the effectiveness of different security solutions in detecting and responding to various types of cyber threats. Each tactic is mapped to the MITRE ATT&CK framework, providing a structured approach to evaluating security technologies. The tactics path has the potential to elevate security attacks significantly, as attackers may use some or all of these tactics to achieve their objectives.

### 6.4.1 Tactics and Their Corresponding MITRE ATT&CK IDs

The following table lists the tactics that were tested in this study along with their corresponding MITRE ATT&CK IDs:

| NAME | TACTIC | MITRE ATT&CK ID |
|---|---|---|
| **Detect Current User** | Discovery | T1033 |
| **Create a Windows User Account** | Persistence | T1136.001 |
| **Create staging directory** | Collection | T1074.001 |
| **Find files** | Collection | T1083 |
| **Stage sensitive files** | Collection | T1005 |
| **Compress staged directory** | Exfiltration | T1074 |
| **Change RDP Port** | Lateral Movement | T1021.001 |
| **Delete Volume Shadow Copies** | Impact | T1490 |
| **Clear Event Logs** | Defense Evasion | T1070.001 |

**Table 1. Attack Scenarios**

### 6.4.2 Detailed Description of Tactics

Detect Current User (Discovery - T1033)
This tactic involves identifying the currently logged-in user on a system. Adversaries use this information to understand the privileges they have on the compromised system and to gather further details for escalating their privileges or moving laterally within the network.

Create a Windows User Account (Persistence - T1136.001)
Creating a new user account is a common persistence mechanism used by adversaries to maintain access to a system. By adding a new user account, adversaries ensure they can regain access even if the primary method of entry is discovered and remediated.

Create Staging Directory (Collection - T1074.001)
Adversaries create directories to stage collected data before exfiltration. This tactic involves organizing and preparing the data they have gathered from the compromised systems for exfiltration to their controlled servers.

Find Files (Collection - T1083)
Finding specific files of interest is a crucial step for adversaries. This involves searching for files

that may contain sensitive information such as credentials, financial data, intellectual property, or other valuable data that can be leveraged or sold.

Stage Sensitive Files (Collection - T1005)
Staging sensitive files involves gathering files of interest and preparing them for exfiltration. Adversaries typically move these files to a designated staging area where they can be easily compressed and exfiltrated.

Compress Staged Directory (Exfiltration - T1074)
Compression of staged directories is a tactic used to minimize the size of the data being exfiltrated and to potentially avoid detection. Adversaries use various compression tools and methods to archive the staged files before sending them out of the compromised environment.

Change RDP Port (Lateral Movement - T1021.001)
Changing the Remote Desktop Protocol (RDP) port is a tactic used to avoid detection by network security monitoring tools that may be configured to monitor default ports. By using a non-standard port, adversaries can bypass certain security controls and facilitate lateral movement.

Delete Volume Shadow Copies (Impact - T1490)
Deleting volume shadow copies is a destructive tactic used by adversaries to prevent recovery of the system. By deleting these backups, adversaries can ensure that ransomware or other destructive actions have a lasting impact and make recovery more difficult for the affected organization.

Clear Event Logs (Defense Evasion - T1070.001)
Clearing event logs is a common tactic used to evade detection and forensic investigation. By deleting or clearing logs, adversaries aim to remove evidence of their activities, making it more challenging for security teams to trace their actions and understand the scope of the compromise.

### 6.4.3 Justification for Using These Tactics

The selection of these specific tactics for the practical implementation of this thesis is grounded in their relevance and prevalence in real-world cyber-attacks. Each tactic was carefully chosen based on the following considerations:

1. Relevance to Modern Threats: These tactics represent a broad spectrum of techniques commonly used by adversaries in various stages of an attack. This ensures that the evaluation covers different aspects of threat detection and response capabilities.

2. Coverage of MITRE ATT&CK Framework: Mapping these tactics to the MITRE ATT&CK framework provides a standardized approach to evaluating the effectiveness of security solutions. This framework is widely recognized and used in the cybersecurity industry, making the results of this study more applicable and credible.

3. Comprehensive Security Evaluation: By covering tactics from different categories, such

as discovery, persistence, collection, exfiltration, lateral movement, impact, and defense evasion, the study ensures a thorough evaluation of the capabilities of EDR and Antivirus solutions.

4. Real-World Attack Scenarios: These tactics are representative of real-world attack scenarios, making the practical implementation more realistic and relevant. This helps understand how well the security solutions perform under conditions similar to actual cyber-attacks.

5. Emphasizing Advanced Capabilities: Some tactics, like behavioral analysis and automated response, highlight the advanced capabilities of EDR solutions. This comparison underscores the importance of adopting sophisticated security measures to counter contemporary threats.

**Examples**

- Detect Current User (Discovery - T1033): This tactic involves identifying the currently logged-in user on a system. Attackers use this information to understand the privileges they have on the compromised system and to gather further details for escalating their privileges or moving laterally within the network. This is frequently observed in initial reconnaissance phases of targeted attacks, where adversaries need to understand user roles and privileges before proceeding with more intrusive actions.

- Create a Windows User Account (Persistence - T1136.001): Creating a new user account is a common persistence mechanism used by adversaries to maintain access to a system. The 2023 FireEye Mandiant M-Trends Report indicates that credential dumping is a prevalent method used by attackers to gain access to additional systems and sensitive information within an organization[51]. By adding a new user account, adversaries ensure they can regain access even if the primary method of entry is discovered and remediated.

- Create Staging Directory (Collection - T1074.001): Adversaries create directories to stage collected data before exfiltration. This tactic involves organizing and preparing the data they have gathered from the compromised systems for exfiltration to their controlled servers.

- Find Files (Collection - T1083): Finding specific files of interest is a crucial step for adversaries. This involves searching for files that may contain sensitive information such as credentials, financial data, intellectual property, or other valuable data that can be leveraged or sold. Common in breaches involving data theft, where attackers search for specific types of files across compromised networks .

- Stage Sensitive Files (Collection - T1005): Staging sensitive files involves gathering files of interest and preparing them for exfiltration. Adversaries typically move these files to a designated staging area where they can be easily compressed and exfiltrated. Typically observed in data breach incidents where sensitive information is aggregated before being exfiltrated, often used by nation-state actors and organized cybercrime groups .

- Compress Staged Directory (Exfiltration - T1074): Compression of staged directories is a tactic used to minimize the size of the data being exfiltrated and to potentially avoid detection. Adversaries use various compression tools and methods to archive the staged files before sending them out of the compromised environment. Seen in numerous data exfiltration cases where attackers compress large volumes of data to facilitate faster transfer and reduce the chance of detection by network monitoring tools .

- Change RDP Port (Lateral Movement - T1021.001): Changing the Remote Desktop Protocol (RDP) port is a tactic used to avoid detection by network security monitoring tools that may be configured to monitor default ports. By using a non-standard port, adversaries can bypass certain security controls and facilitate lateral movement.

- Delete Volume Shadow Copies (Impact - T1490): Deleting volume shadow copies is a destructive tactic used by adversaries to prevent recovery of the system. The 2023 CrowdStrike Global Threat Report highlights that deleting volume shadow copies is a frequent tactic used in ransomware attacks to prevent recovery of the system[52]. By deleting these backups, adversaries can ensure that ransomware or other destructive actions have a lasting impact and make recovery more difficult for the affected organization.

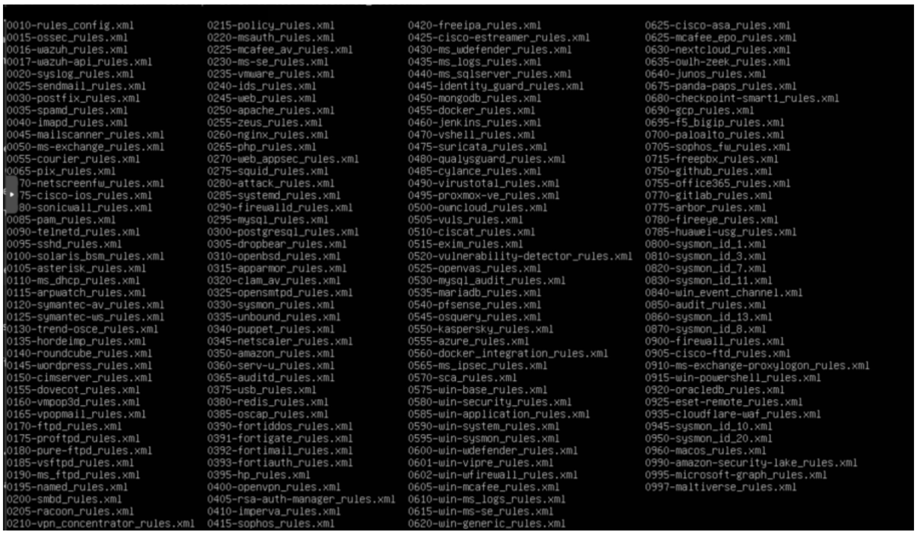
- Clear Event Logs (Defense Evasion - T1070.001): Clearing event logs is a common tactic used to evade detection and forensic investigation. According to the 2023 Verizon Data Breach Investigations Report, clearing event logs is a common tactic used to evade detection and forensic investigation[53]. By deleting or clearing logs, adversaries aim to remove evidence of their activities, making it more challenging for security teams to trace their actions and understand the scope of the compromise.

Understanding these tactics provides valuable insight into the methods used by adversaries and underscores the importance of robust detection and response capabilities in security solutions. The effectiveness of Wazuh, OpenEDR (Xticium), and Bitdefender in detecting and responding to these tactics was thoroughly evaluated, highlighting the strengths and limitations of each solution. This structured approach, aligned with the MITRE ATT&CK framework, ensures a comprehensive assessment of the security technologies in defending against contemporary cyber threats. The tactics path has the potential to significantly elevate the impact of security attacks, as attackers may employ some or all of these tactics to achieve their objectives. This emphasizes the critical need for comprehensive security measures.

## 6.5 Rules and Policies of Endpoint Security Solutions

### 6.5.1 Wazuh

Wazuh, an open-source security monitoring platform, employs a comprehensive set of rules and policies to detect and respond to various security events. These rules are critical in ensuring effective monitoring and threat detection across different systems and applications. The rules and policies are defined in XML files and cover a wide range of security aspects, from network intrusions to application-specific anomalies.



```
0010-rules_config.xml            0215-policy_rules.xml            0420-freeipa_rules.xml                 0625-cisco-asa_rules.xml
0015-ossec_rules.xml             0220-msauth_rules.xml            0425-cisco-estreamer_rules.xml         0625-mcafee_epo_rules.xml
0016-wazuh_rules.xml             0225-mcafee_av_rules.xml         0430-ms_wdefender_rules.xml            0630-nextcloud_rules.xml
0017-wazuh-api_rules.xml         0230-ms-se_rules.xml             0435-ms_logs_rules.xml                 0635-owlh-zeek_rules.xml
0020-syslog_rules.xml            0235-vmware_rules.xml            0440-ms_sqlserver_rules.xml            0640-junos_rules.xml
0025-sendmail_rules.xml          0240-ids_rules.xml               0445-identity_guard_rules.xml          0675-panda-paps_rules.xml
0030-postfix_rules.xml           0245-web_rules.xml               0450-mongodb_rules.xml                 0680-checkpoint-smart1_rules.xml
0035-spamd_rules.xml             0250-apache_rules.xml            0455-docker_rules.xml                  0690-gcp_rules.xml
0040-imapd_rules.xml             0255-zeus_rules.xml              0460-jenkins_rules.xml                 0695-f5_bigip_rules.xml
0045-mailscanner_rules.xml       0260-nginx_rules.xml             0470-vshell_rules.xml                  0700-paloalto_rules.xml
0050-ms-exchange_rules.xml       0265-php_rules.xml               0475-suricata_rules.xml                0705-sophos_fw_rules.xml
0055-courier_rules.xml           0270-web_appsec_rules.xml        0480-qualysguard_rules.xml             0715-freepbx_rules.xml
0065-pix_rules.xml               0275-squid_rules.xml             0485-cylance_rules.xml                 0750-github_rules.xml
  70-netscreenfw_rules.xml       0280-attack_rules.xml            0490-virustotal_rules.xml              0755-office365_rules.xml
  75-cisco-ios_rules.xml         0285-systemd_rules.xml           0495-proxmox-ve_rules.xml              0770-gitlab_rules.xml
  80-sonicwall_rules.xml         0290-firewalld_rules.xml         0500-owncloud_rules.xml                0775-arbor_rules.xml
0085-pam_rules.xml               0295-mysql_rules.xml             0505-vuls_rules.xml                    0780-fireeye_rules.xml
0090-telnetd_rules.xml           0300-postgresql_rules.xml        0510-ciscat_rules.xml                  0785-huawei-usg_rules.xml
0095-sshd_rules.xml              0305-dropbear_rules.xml          0515-exim_rules.xml                    0800-sysmon_id_1.xml
0100-solaris_bsm_rules.xml       0310-openbsd_rules.xml           0520-vulnerability-detector_rules.xml  0810-sysmon_id_3.xml
0105-asterisk_rules.xml          0315-apparmor_rules.xml          0525-openvas_rules.xml                 0820-sysmon_id_7.xml
0110-ms_dhcp_rules.xml           0320-clam_av_rules.xml           0530-mysql_audit_rules.xml             0830-sysmon_id_11.xml
0115-arpwatch_rules.xml          0325-opensmtpd_rules.xml         0535-mariadb_rules.xml                 0840-win_event_channel.xml
0120-symantec-av_rules.xml       0330-sysmon_rules.xml            0540-pfsense_rules.xml                 0850-audit_rules.xml
0125-symantec-ws_rules.xml       0335-unbound_rules.xml           0545-osquery_rules.xml                 0860-sysmon_id_13.xml
0130-trend-osce_rules.xml        0340-puppet_rules.xml            0550-kaspersky_rules.xml               0870-sysmon_id_8.xml
0135-hordeimp_rules.xml          0345-netscaler_rules.xml         0555-azure_rules.xml                   0900-firewall_rules.xml
0140-roundcube_rules.xml         0350-amazon_rules.xml            0560-docker_integration_rules.xml      0905-cisco-ftd_rules.xml
0145-wordpress_rules.xml         0360-serv-u_rules.xml            0565-ms_ipsec_rules.xml                0910-ms-exchange-proxylogon_rules.xml
0150-cimserver_rules.xml         0365-auditd_rules.xml            0570-sca_rules.xml                     0915-win-powershell_rules.xml
0155-dovecot_rules.xml           0375-usb_rules.xml               0575-win-base_rules.xml                0920-oracledb_rules.xml
0160-vmpop3d_rules.xml           0380-redis_rules.xml             0580-win-security_rules.xml            0925-eset-remote_rules.xml
0165-vpopmail_rules.xml          0385-oscap_rules.xml             0585-win-application_rules.xml         0935-cloudflare-waf_rules.xml
0170-ftpd_rules.xml              0390-fortiddos_rules.xml         0590-win-system_rules.xml              0945-sysmon_id_10.xml
0175-proftpd_rules.xml           0391-fortigate_rules.xml         0595-win-sysmon_rules.xml              0950-sysmon_id_20.xml
0180-pure-ftpd_rules.xml         0392-fortimail_rules.xml         0600-win-wdefender_rules.xml           0960-macos_rules.xml
0185-vsftpd_rules.xml            0393-fortiauth_rules.xml         0601-win-vipre_rules.xml               0990-amazon-security-lake_rules.xml
0190-ms_ftpd_rules.xml           0395-hp_rules.xml                0602-win-wfirewall_rules.xml           0995-microsoft-graph_rules.xml
0195-named_rules.xml             0400-openvpn_rules.xml           0605-win-mcafee_rules.xml              0997-maltiverse_rules.xml
0200-smbd_rules.xml              0405-rsa-auth-manager_rules.xml  0610-win-ms_logs_rules.xml
0205-racoon_rules.xml            0410-imperva_rules.xml           0615-win-ms-se_rules.xml
0210-vpn_concentrator_rules.xml  0415-sophos_rules.xml            0620-win-generic_rules.xml
```

**Figure 6. Wazuh rules**

System Monitoring Rules:

- ossec_rules.xml: Core rules for monitoring OSSEC logs.
- wazuh_rules.xml: Specific to Wazuh's enhanced monitoring capabilities.
- syslog_rules.xml: For parsing and analyzing system log messages.
- ssh_rules.xml: Detects SSH login attempts and potential brute force attacks.
- firewall_rules.xml: Monitors firewall activity to detect suspicious traffic patterns.

Application-Specific Rules:

- apache_rules.xml: Monitors Apache web server logs for malicious access attempts.
- nginx_rules.xml: Similar to Apache rules but tailored for NGINX logs.
- mysql_rules.xml: Detects anomalies and potential SQL injection attacks in MySQL databases.
- mssql_rules.xml: Monitors Microsoft SQL Server logs for suspicious activities.

Network Security Rules:

- cisco-ios_rules.xml: Rules specific to Cisco IOS devices to detect network anomalies.
- snort_rules.xml: Integrates with Snort IDS rules for comprehensive network intrusion detection.
- suricata_rules.xml: For integration with Suricata IDS, providing robust network security monitoring.

Compliance and Regulatory Rules:

- pci_dss_rules.xml: Ensures compliance with PCI DSS standards by monitoring relevant security events.
- gdpr_rules.xml: Helps in identifying data breaches and privacy issues to comply with GDPR.

Custom and User-Defined Rules:

- local_rules.xml: Allows users to define custom rules tailored to their specific environment and requirements.

Detailed Description and Functionality:

Each rule file is designed to parse logs, detect specific patterns, and generate alerts based on defined thresholds and conditions. These rules utilize regular expressions and other pattern matching techniques to identify potential security incidents.

- ossec_rules.xml: Acts as the foundational rule set for OSSEC, enabling basic log parsing and anomaly detection.
- wazuh_rules.xml: Enhances the core OSSEC rules with additional capabilities tailored to Wazuh’s architecture, providing more detailed analysis and alerting.
- syslog_rules.xml: Critical for environments heavily reliant on syslog for logging, ensuring that all log messages are accurately parsed and analyzed for suspicious activities.
- ssh_rules.xml: Essential for securing remote access to systems by monitoring and alerting on unusual SSH login patterns, such as repeated failed login attempts indicative of brute force attacks.
- firewall_rules.xml: Provides insights into network traffic and potential intrusions by monitoring firewall logs for unusual traffic patterns and access attempts.

Implementation and Configuration:
To implement these rules, administrators need to configure the Wazuh manager and agent appropriately, ensuring that log files are correctly specified and monitored. Configuration typically involves editing the ossec.conf file to include paths to the log files and specifying the rules to be applied.

Example Configuration:

```
<ossec_config>
  <rules>
    <include>ossec_rules.xml</include>
    <include>wazuh_rules.xml</include>
    <include>syslog_rules.xml</include>
    <include>ssh_rules.xml</include>
    <include>firewall_rules.xml</include>
    <!-- Add other rule files as needed -->
  </rules>
</ossec_config>
```

Customization:
Administrators can create or modify existing rules to better fit their security posture. This is done by editing the XML files directly, ensuring that the custom rules do not conflict with existing ones.

Maintenance:
Regular updates to the rule sets are necessary to keep up with emerging threats and vulnerabilities. Wazuh provides updates to its rule sets, which can be downloaded and applied to ensure ongoing protection against new and evolving security threats.

Observations
The extensive list of rule files, as shown in the screenshot, indicates a robust and flexible rule engine capable of monitoring a wide array of applications, systems, and network devices. This modular approach allows for scalable and customizable security monitoring, catering to diverse operational needs and compliance requirements.

By leveraging these predefined rules and the ability to customize them, organizations can significantly enhance their security posture, ensuring timely detection and response to potential threats. The integration with other security tools, such as Snort and Suricata, further strengthens the overall monitoring capabilities, providing a comprehensive security solution.

### 6.5.2 OpenEDR (Xcitium)

The company's rules section encompasses seven crucial event categories, each tailored to provide extensive monitoring and alerting functionalities for effective security management54. These categories include:

- Process Events: Alerts triggered by application-invoked processes.
- Registry Events: Notifications for changes in the Windows registry on endpoints.
- File Events: Alerts for modifications to system files.
- Download Events: Notifications when files are downloaded through various means.
- Upload Events: Alerts for file transfers to shared folders or external drives.
- Defense Events: Alerts for attempts to access critical OS functions or launch attacks.
- Network Events: Notifications for services listening on ports and network connections.

According to “Appendix 3: Default Xcitium Security Policy Details,” all these policies are enabled by default. This comprehensive set of rules ensures robust monitoring and protection across various aspects of endpoint security, helping organizations maintain a secure and resilient IT environment.

By implementing these event categories, companies can ensure proactive detection and response to potential security threats, thereby enhancing their overall cybersecurity posture.

| Event Name | Description |
|---|---|
| Suspicious System Process Creation | Process verdict is not safe AND file path matches %systemroot%* |
| Remote Powershell Execution | File path matches *wsmprovhost.exe |
| Suspicious Powershell Flag | Command line matches any of the following:<br>*powershell*-NoP*<br>*powershell*-Win* |

| | |
|---|---|
| | *powershell*-w*<br>*powershell*-Exec*<br>*powershell*-ex*<br>*powershell*-ep*<br>*powershell*-command*<br>*powershell*-NoL*<br>*powershell*-InputFormat*<br>*powershell*-Enc*<br>*powershell*-NonInteractive*<br>*powershell*-nonI*<br>*powershell*-file* |
| Stop Service | Command line matches %systemroot%system32net*stop* |
| Run Untrusted Executable | Verdict is not safe |
| Suspicious Process Hierarchy | Process path does not match *explorer.exe AND path matches *powershell.exe OR patch matches *cmd.exe |
| Start Service | Command line matches %systemroot%system32net*start* |
| **Registry Events** | |

| Event Name | Description |
|---|---|
| Disable User Account Control | Registry key path is equal to HKEY_LOCAL_MACHINESoftwareMicrosoftWindowsCurrentVersionPoliciesSystem<br>AND registry value name is equal to EnableLUA0<br>AND registry value data is equal to 0. |
| Disable Task Manager | Registry key path is equal to HKEY_CURRENT_USERSOFTWAREMicrosoftWindowsCurrentVersionPoliciesSystem<br>AND registry value name is equal to DisableTaskMgr<br>AND registry value data is equal to 1 |
| Installation of Drivers | Registry key path matches HKEY_LOCAL_MACHINESYSTEMCurrentControlSetServices* AND registry value name is equal to Type<br>AND<br>Registry value data is equal to 1<br>OR registry value data is equal to 2 |
| Add Service to svchost | Registry key path matches HKEY_LOCAL_MACHINESYSTEMCurrentControlSetServices* AND registry value name is equal to ImagePath AND registry value data matches *svchost.exe*<br>OR<br>Registry key path matches HKEY_LOCAL_MACHINESYSTEMCurrentControlSetServices*Parameters AND registry value name is equal to ServiceDll AND registry matches *.dll |
| Add Active Setup Value In Registry | Registry key path matches HKEY_LOCAL_MACHINESoftwareMicrosoftActive SetupInstalled Components* |
| Modify Powershell | Registry key path is equal to HKEY_LOCAL_MACHINESOFTWAREMicrosoftPowerShell1ShellIdsMicrosoft.PowerShell AND |

| | |
|---|---|
| Execution Policy | registry value name is equal to ExecutionPolicy |
| Modify Firewall Settings | Registry key path matches HKEY_LOCAL_MACHINESYSTEMCurrentControlSetServicesSharedAccessParametersFirewallPolicyStandardProfile* |
| Disable Registry Editing Tool | Registry key path is equal to HKEY_CURRENT_USERSOFTWAREMicrosoftWindowsCurrentVersionPoliciesSystem AND registry value name is equal to DisableRegistryTools AND registry value data is equal to 1. |
| Modify AppInit_DLLs in Registry | Registry key path is equal to HKEY_LOCAL_MACHINESoftwareMicrosoftWindows NTCurrentVersionWindows AND registry value name is equal to AppInit_DLLs |
| Add Service | Registry key path matches HKEY_LOCAL_MACHINESYSTEMCurrentControlSetServices* AND registry value name is equal to ImagePath AND registry value data matches *.exe* AND registry value data doesn't match *svchost.exe* |
| Layered Service Provider installation | Registry key path matches HKEY_LOCAL_MACHINESYSTEMCurrentControlSetServicesWinSock2ParametersProtocol_Catalog9Catalog_Entries* |
| Add Autorun In Registry | Registry key path matches any of the following:<br>HKEY_LOCAL_MACHINESoftwarePoliciesMicrosoftWindowsSystemScriptsStartup*<br>HKEY_CURRENT_USERSoftwarePoliciesMicrosoftWindowsSystemScriptsLogon*<br>HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersionPoliciesSystem*<br>HKEY_LOCAL_MACHINESOFTWAREMicrosoftWindowsCurrentVersionRunOnceEx*<br>HKEY_LOCAL_MACHINESOFTWAREMicrosoftWindowsCurrentVersionRunOnce*<br>HKEY_CURRENT_USERSoftwareMicrosoftWindowsNTCurrentVersionWindows*<br>HKEY_CURRENT_USERSoftwareMicrosoftWindowsNTCurrentVersionWindowsRun*<br>HKEY_LOCAL_MACHINESOFTWAREMicrosoftWindowsCurrentVersionPoliciesExplorerRun*<br>HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersionPoliciesExplorerRun*<br>HKEY_CURRENT_USERSoftwarePoliciesMicrosoftWindowsSystemScriptsLogoff*<br>HKEY_LOCAL_MACHINESoftwarePoliciesMicrosoftWindowsSystemScriptsShutdown*<br>OR<br>Registry key path equals any of the following:<br>HKEY_LOCAL_MACHINESOFTWAREMicrosoftWindowsCurrentVersionRun<br>HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersionRun<br>HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersionRunOnce |
| Booting Time Execution | Registry key path is equal to HKEY_LOCAL_MACHINESYSTEMCurrentControlSetControlSession Manager AND registry value name is equal to BootExecute |
| Disable Auto Update | Registry key path is equal to HKEY_LOCAL_MACHINESOFTWAREPoliciesMicrosoftWindowsWindowsUpdateAU AND registry value name is equal to NoAutoUpdate AND registry value data is equal to 1<br>OR<br>Registry key path is equal to HKEY_LOCAL_MACHINESoftwarePoliciesMicrosoftWindowsWindowsUpdate AND registry value name is equal to DisableWindowsUpdateAccess AND registry value data is equal to 1<br>OR<br>Registry key path is equal to HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersionPoliciesWindowsUpdate AND registry value name is equal to DisableWindowsUpdateAccess AND registry value data is |

| | |
|---|---|
| | equal to 1 |
| Disable Service | Registry key path matches HKEY_LOCAL_MACHINESystemCurrentControlSetServices* AND registry value name is equal to Start AND registry value data is equal to 4 |
| Create Explorer Entry | Registry key path matches any of the following:<br>HKEY_LOCAL_MACHINESOFTWAREClassesPROTOCOLSFilter*<br>HKEY_LOCAL_MACHINESOFTWAREClassesPROTOCOLSHandler*<br>HKEY_CURRENT_USERSOFTWAREMicrosoftInternet ExplorerDesktopComponents*<br>HKEY_LOCAL_MACHINESOFTWAREMicrosoftActive SetupInstalled Components*<br>HKEY_LOCAL_MACHINESOFTWAREMicrosoftWindowsCurrentVersionShellServiceObjectDelayLoad*<br>HKEY_CURRENT_USERSOFTWAREMicrosoftWindowsCurrentVersionShellServiceObjectDelayLoad*<br>HKEY_LOCAL_MACHINESoftwareMicrosoftWindowsCurrentVersionExplorerShellExecuteHooks*<br>HKEY_CURRENT_USERSoftwareClasses*ShellExContextMenuHandlers*<br>HKEY_LOCAL_MACHINESoftwareClasses*ShellExContextMenuHandlers*<br>HKEY_CURRENT_USERSoftwareClassesAllFileSystemObjectsShellExContextMenuHandlers*<br>HKEY_LOCAL_MACHINESoftwareClassesAllFileSystemObjectsShellExContextMenuHandlers*<br>HKEY_CURRENT_USERSoftwareClassesDirectoryShellExContextMenuHandlers*<br>HKEY_LOCAL_MACHINESoftwareClassesDirectoryShellExContextMenuHandlers*<br>HKEY_CURRENT_USERSoftwareClassesDirectoryShellexDragDropHandlers*<br>HKEY_LOCAL_MACHINESoftwareClassesDirectoryShellexDragDropHandlers*<br>HKEY_CURRENT_USERSoftwareClassesDirectoryShellexPropertySheetHandlers*<br>HKEY_LOCAL_MACHINESoftwareClassesDirectoryShellexPropertySheetHandlers*<br>HKEY_CURRENT_USERSoftwareClassesDirectoryShellexCopyHookHandlers*<br>HKEY_LOCAL_MACHINESoftwareClassesDirectoryShellexCopyHookHandlers*<br>HKEY_CURRENT_USERSoftwareClassesFolderShellexColumnHandlers*<br>HKEY_LOCAL_MACHINESoftwareClassesFolderShellexColumnHandlers*<br>HKEY_CURRENT_USERSoftwareClassesFolderShellExContextMenuHandlers*<br>HKEY_LOCAL_MACHINESoftwareClassesFolderShellExContextMenuHandlers*<br>HKEY_CURRENT_USERSoftwareClassesDirectoryBackgroundShellExContextMenuHandlers*<br>HKEY_LOCAL_MACHINESoftwareClassesDirectoryBackgroundShellExContextMenuHandlers*<br>HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersionExplorerShellIconOverlayIdentifiers*<br>HKEY_LOCAL_MACHINESoftwareMicrosoftWindowsCurrentVersionExplorerShellIconOverlayIdentifiers*<br>HKEY_CURRENT_USERSoftwareMicrosoftCtfLangBarAddin*<br>HKEY_LOCAL_MACHINESoftwareMicrosoftCtfLangBarAddin*<br>HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersionShell ExtensionsApproved*<br>HKEY_LOCAL_MACHINESoftwareMicrosoftWindowsCurrentVersionShell ExtensionsApproved*<br>OR<br>Registry key path is equal to HKEY_LOCAL_MACHINESOFTWAREMicrosoftWindowsCurrentVersionExplorerSharedTaskScheduler |
| Disable Windows Application | Registry key path is equal to HKEY_LOCAL_MACHINESOFTWAREMicrosoftWindowsCurrentVersionPoliciesExplorerDisallowRun |
| Disable Command Prompt | Registry key path is equal to HKEY_CURRENT_USERSoftwarePoliciesMicrosoftWindowsSystem AND registry value name is equal to DisableCMD AND registry value data is equal to 2 |
| Disable Show Hidden | Registry key path is equal to HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersionExplorerAdvanced AND registry value data is equal to 2 |

| | |
|---|---|
| Files | AND<br>Registry value name is equal to Hidden OR registry value name is equal to ShowSuperHidden |
| Share Folder | Registry key path is equal to HKEY_LOCAL_MACHINESYSTEMCurrentControlSetServicesLanmanserverShares |
| Addition of DNS Server | Registry key path matches HKEY_LOCAL_MACHINESYSTEMCurrentControlSetServicesTcpipParametersInterfaces* AND registry value name is equal to NameServer |
| Modify Hosts File Registry | Registry key path is equal HKEY_LOCAL_MACHINESYSTEMCurrentControlSetServicesTcpipParameters AND registry value name equal to DataBasePath |

**File Events**

| Event Name | Description |
|---|---|
| Add Scheduled Task | File path matches %systemroot%System32Tasks* OR %systemroot%Tasks* |
| Write Fake System File | File path matches *svch0st.exe OR *svhost.exe |
| Write to System Directory | File path matches %systemroot%* |
| Add Startup File or Folder | File path matches any of the following:<br>%appdata%MicrosoftWindowsStart MenuProgramsStartup*<br>%programdata%MicrosoftWindowsStart MenuProgramsStartup*<br>%systemroot%systemiosubsys*<br>%systemroot%systemvmm32*<br>%systemroot%Tasks*<br>OR<br>File path equals any of the following:<br>%systemdrive%autoexec.bat<br>%systemdrive%config.sys<br>%systemroot%wininit.ini<br>%systemroot%winstart.bat<br>%systemroot%win.ini<br>%systemroot%system.ini<br>%systemroot%dosstart.bat |
| Modify Host File | File path is equal to %systemroot%system32driversetchosts |
| Write to Executable | File type is equal to PORTABLE_EXECUTABLE<br>AND<br>Process path doesn't match *explorer.exe |
| Write to Infectible File | Process path doesn't match *iexplorer.exe<br>AND<br>File path matches any of the following:<br>*.lnk<br>*.wsf<br>*.hta<br>*.mhtml |

| | |
|---|---|
| | *.html<br>*.doc<br>*.docm<br>*.xls<br>*.xlsm<br>*.ppt<br>*.pptm<br>*.chm<br>*.vbs<br>*.js<br>*.bat<br>*.pif<br>*.pdf<br>*.jar<br>*.sys |
| Modify Group Policy Settings | File path matches %systemroot%system32grouppolicy* OR %systemroot%Sysvolsysvol*Policies* |
| Write to Program Files Directory | File path matches %programfiles%* |
| **Download Events** | |
| **Event Name** | **Description** |
| Download Infectible File | File path matches any of the following:<br>*.lnk<br>*.wsf<br>*.hta<br>*.mhtml<br>*.html<br>*.doc<br>*.docm<br>*.xls<br>*.xlsm<br>*.ppt<br>*.pptm<br>*.chm<br>*.vbs<br>*.js<br>*.bat<br>*.pif<br>*.pdf<br>*.jar<br>*.sys |
| Download Executable | File type is equal to PORTABLE_EXECUTABLE |
| **Upload Events** | |

| Event Name | Description |
|---|---|
| Write Executable to Shared Folder | File type is equal to PORTABLE_EXECUTABLE |
| Write Infectible to Shared Folder | File path matches any of the following:<br>*.lnk<br>*.wsf<br>*.hta<br>*.mhtml<br>*.html<br>*.doc<br>*.docm<br>*.xls<br>*.xlsm<br>*.ppt<br>*.pptm<br>*.chm<br>*.vbs<br>*.js<br>*.bat<br>*.pif<br>*.pdf<br>*.jar<br>*.sys |

**Table 2. OpenEDR (Xcitium) Rules Table**

### 6.5.3 Bitdefender

Bitdefender Antivirus implements a series of default rules designed to provide robust protection against a wide array of cyber threats. These rules cover various aspects of system security, including real-time protection, firewall management, and specific application access settings.

1. Firewall Rules:
Bitdefender's firewall operates with predefined rules that manage data transmission to and from the system. These rules are crucial for filtering network traffic and protecting against unauthorized access. The firewall automatically creates rules whenever an application attempts to access the internet, ensuring that potentially malicious software is blocked. Users can view and modify these rules through the Bitdefender interface, allowing for customization based on individual security needs. The rules can be categorized based on network types (e.g., Home/Office, Public) and can be edited to apply specific protocols, ports, and IP addresses[55].

2. Real-Time Protection:
The Bitdefender Shield, a core component of Bitdefender's real-time protection, continuously scans files and emails for malware as they are accessed. This feature is configured to offer maximum protection with minimal system performance impact. Users have the option to customize these settings further, such as enabling scans for potentially unwanted applications (PUAs), scripts, and network shares. Advanced settings allow users

to define specific parameters like scanning only new and modified files or conducting early boot scans, enhancing the system's startup security.

3. Managing Application Access:
To handle cases where legitimate applications are inadvertently blocked by the firewall, Bitdefender provides a user-friendly interface to manage application access. By navigating to the Protection section and accessing the Firewall settings, users can add rules for specific applications. This involves selecting the executable file of the application and defining whether it should be allowed or denied network access. These rules can be tailored to apply under certain network conditions and can specify the direction of traffic (inbound, outbound, or both).

4. Handling System Notifications:
Bitdefender also ensures compatibility with Windows Security Center, addressing common issues where the center might incorrectly report the status of Bitdefender's modules. Users are guided to verify and toggle the antivirus and firewall settings within the Bitdefender interface to confirm their active status. This ensures continuous protection and resolves any discrepancies reported by Windows Security Center[56].

The default rules set by Bitdefender Antivirus are integral to its effectiveness in protecting consumer systems from cyber threats. These rules provide a balanced approach to security, offering both automated protections and customizable options for advanced users. Understanding and managing these settings is essential for maintaining optimal security and system performance.

| Feature | Default Rule | Description |
|---|---|---|
| **Firewall** | Automatic Rule Creation | Automatically creates rules whenever an application attempts to access the internet. |
| | Network Type Rules | Applies rules based on network types (e.g., Home/Office, Public). |
| | Protocol and Port Rules | Rules apply to any protocol and port by default but can be customized. |
| | Inbound and Outbound Traffic | Rules apply to both inbound and outbound traffic. |
| | Customizable Application Access | Users can manually add, edit, or delete rules for specific applications. |
| | Stealth Mode | Controls whether the device can be detected by other devices on the network. |
| | Port Scan Protection | Detects and blocks attempts to scan open ports on the device. |
| | Alert Mode (Paranoid Mode) | Prompts user for action each time an app tries to connect to the internet. |
| **Real-Time Protection** | Continuous Scanning | Scans files and emails for malware as they are accessed. |
| | Scan Potentially Unwanted Applications (PUAs) | Scans for PUAs, which often come bundled with freeware. |
| | Script Scanning | Scans PowerShell scripts and office documents for script-based malware. |

| | | |
|---|---|---|
| | Network Share Scanning | Scans files on network shares for threats. |
| | Boot Sector Scanning | Scans the boot sectors of the hard disk for malware. |
| | Scan New and Modified Files | Scans only new and modified files to improve performance. |
| | Archive Scanning | Allows users to enable scanning inside archives, although it is resource-intensive. |
| | Early Boot Scanning | Scans the system at startup to detect threats as early as possible. |
| | Keylogger Scanning | Detects and blocks keylogger applications that may record keyboard inputs. |
| **Application Access** | Application Rule Management | Users can add, delete, or edit rules for specific applications. |
| | Customizable Permissions | Users can set rules to allow or deny network access for applications. |
| | Network Type Specific Rules | Rules can be configured to apply to specific network types like Home/Office or Public. |
| | Direction-Specific Traffic Rules | Users can specify if rules apply to inbound, outbound, or both directions of traffic. |
| | Remote and Local Address Customization | Allows specification of remote and local IP addresses and ports the rule applies to. |
| **System Notifications** | Windows Security Center Compatibility | Ensures Bitdefender modules are correctly reported in Windows Security Center. |
| | Toggle Settings | Users can verify and toggle antivirus and firewall settings within the Bitdefender interface. |
| **Additional Features** | Web Protection | Blocks malicious websites and phishing attempts while browsing the internet. |
| | Ransomware Remediation | Detects and blocks ransomware attacks, providing options to restore encrypted files. |
| | Advanced Threat Defense | Monitors applications for suspicious behavior and blocks potential threats. |
| | Anti-Theft | Provides tools for locating, locking, or wiping a device remotely if it is lost or stolen. |
| | Vulnerability Scanner | Scans the system for security vulnerabilities, such as outdated software or weak passwords. |
| | File Shredder | Permanently deletes files to prevent recovery. |
| | Safepay | Provides a secure browser for online transactions and banking. |
| | VPN | Encrypts internet connection to protect privacy and data from eavesdropping. |

**Table 3. Bitdefender Rules Table**

## 6.6 CALDERA Attack Platform

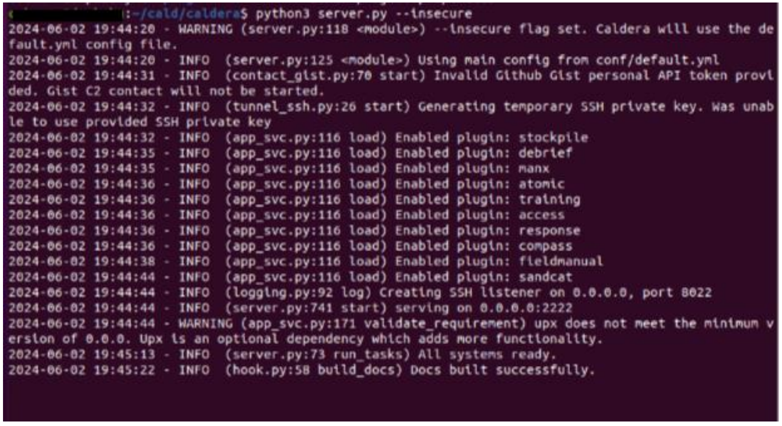
### 6.6.1 Overview of CALDERA

CALDERA is a cybersecurity framework designed to facilitate autonomous breach and simulation exercises. It can also support manual red team engagements and automated incident response tasks. Developed as part of MITRE's research initiatives, CALDERA is based on the MITRE ATT&CK™ framework.[57]

The CALDERA framework is composed of two primary elements:

1. Core System: This is the foundational code featuring an asynchronous command and control (C2) server with REST API and a web interface.
2. Plugins: These are separate modules that expand the core framework's capabilities, offering additional functionalities like agents, graphical interfaces, TTP collections, and more.

To begin using CALDERA, the service must be installed, and the server must be initiated.



```
[redacted]:~/cald/caldera$ python3 server.py --insecure
2024-06-02 19:44:20 - WARNING (server.py:118 <module>) --insecure flag set. Caldera will use the de
fault.yml config file.
2024-06-02 19:44:20 - INFO  (server.py:125 <module>) Using main config from conf/default.yml
2024-06-02 19:44:31 - INFO  (contact_gist.py:70 start) Invalid Github Gist personal API token provi
ded. Gist C2 contact will not be started.
2024-06-02 19:44:32 - INFO  (tunnel_ssh.py:26 start) Generating temporary SSH private key. Was unab
le to use provided SSH private key
2024-06-02 19:44:32 - INFO  (app_svc.py:116 load) Enabled plugin: stockpile
2024-06-02 19:44:35 - INFO  (app_svc.py:116 load) Enabled plugin: debrief
2024-06-02 19:44:35 - INFO  (app_svc.py:116 load) Enabled plugin: manx
2024-06-02 19:44:36 - INFO  (app_svc.py:116 load) Enabled plugin: atomic
2024-06-02 19:44:36 - INFO  (app_svc.py:116 load) Enabled plugin: training
2024-06-02 19:44:36 - INFO  (app_svc.py:116 load) Enabled plugin: access
2024-06-02 19:44:36 - INFO  (app_svc.py:116 load) Enabled plugin: response
2024-06-02 19:44:36 - INFO  (app_svc.py:116 load) Enabled plugin: compass
2024-06-02 19:44:38 - INFO  (app_svc.py:116 load) Enabled plugin: fieldmanual
2024-06-02 19:44:44 - INFO  (app_svc.py:116 load) Enabled plugin: sandcat
2024-06-02 19:44:44 - INFO  (logging.py:92 log) Creating SSH listener on 0.0.0.0, port 8022
2024-06-02 19:44:44 - INFO  (server.py:741 start) serving on 0.0.0.0:2222
2024-06-02 19:44:44 - WARNING (app_svc.py:171 validate_requirement) upx does not meet the minimum v
ersion of 0.0.0. Upx is an optional dependency which adds more functionality.
2024-06-02 19:45:13 - INFO  (server.py:73 run_tasks) All systems ready.
2024-06-02 19:45:22 - INFO  (hook.py:58 build_docs) Docs built successfully.
```

**Figure 7. Caldera Installation**

CALDERA operates via a web-based interface, accessible through a browser at the URL localhost on port 8888.

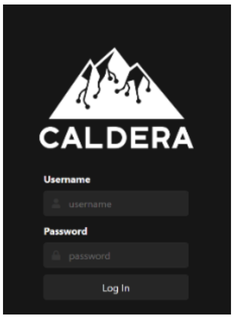
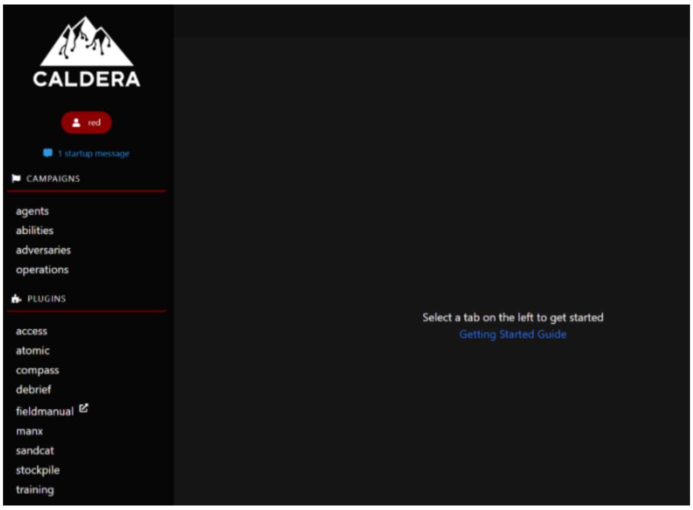


**Figure 8. Login**

Login Credentials:

Username: red
Password: admin



Select a tab on the left to get started

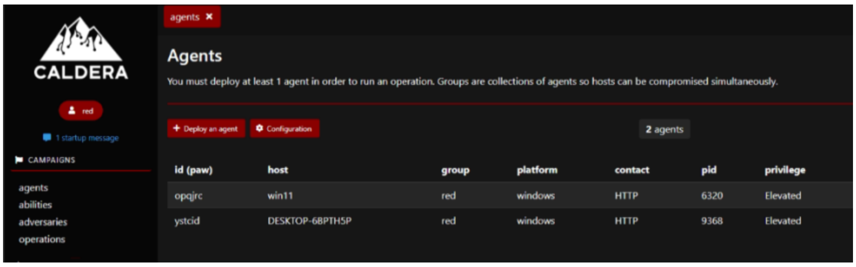
Figure 9. Front-end Cladera

### 6.6.2 Components of the CALDERA Software

**Agents:** Agents are software applications that periodically connect back to the CALDERA server to receive instructions. These agents communicate with the server through predefined contact methods established during their installation. The interface displays all installed agents, each offering unique functionalities, such as:

- Sandcat: A GoLang agent that communicates via various C2 channels, including HTTP, GitHub GIST, and DNS tunneling.
- Manx: A GoLang agent utilizing TCP for communication, functioning as a reverse shell.
- Ragdoll: A Python agent that communicates using HTML.

Agents can be grouped either during their installation using command line flags or through the user interface. These groups determine the roles of agents (red or blue) during operations.



Agents

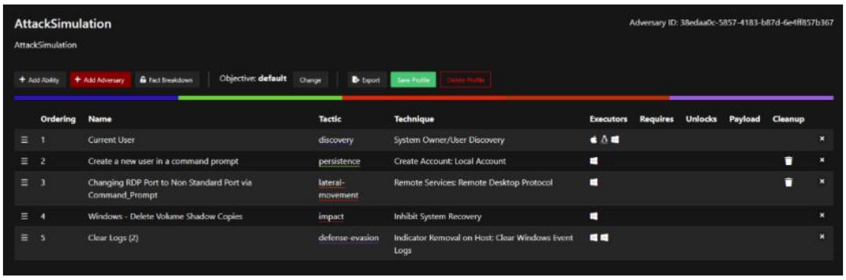
You must deploy at least 1 agent in order to run an operation. Groups are collections of agents so hosts can be compromised simultaneously.

| id (paw) | host | group | platform | contact | pid | privilege |
|---|---|---|---|---|---|---|
| opqjrc | win11 | red | windows | HTTP | 6320 | Elevated |
| ystcid | DESKTOP-6BPTH5P | red | windows | HTTP | 9368 | Elevated |

Figure 10. Front-end Agents

**Abilities and Adversaries:**

- Abilities: Specific applications of ATT&CK tactics that can be executed on agents. These include the commands to be run, the platforms they can run on (e.g., Windows/PowerShell), payloads, and modules for output analysis on the CALDERA server.
- Adversaries: Profiles that represent the tactics, techniques, and procedures (TTPs) available to a threat actor. These profiles guide which abilities are executed during an operation.



AttackSimulation

Adversary ID: 38edaa0c-5857-4183-b87d-6e4ff857b367

AttackSimulation

Objective: **default**

| | Ordering | Name | Tactic | Technique | Executors | Requires | Unlocks | Payload | Cleanup | |
|---|---|---|---|---|---|---|---|---|---|---|
| ☰ | 1 | Current User | discovery | System Owner/User Discovery | | | | | | × |
| ☰ | 2 | Create a new user in a command prompt | persistence | Create Account: Local Account | | | | | 🗑 | × |
| ☰ | 3 | Changing RDP Port to Non Standard Port via Command_Prompt | lateral-movement | Remote Services: Remote Desktop Protocol | | | | | 🗑 | × |
| ☰ | 4 | Windows - Delete Volume Shadow Copies | impact | Inhibit System Recovery | | | | | | × |
| ☰ | 5 | Clear Logs (2) | defense-evasion | Indicator Removal on Host: Clear Windows Event Logs | | | | | | × |

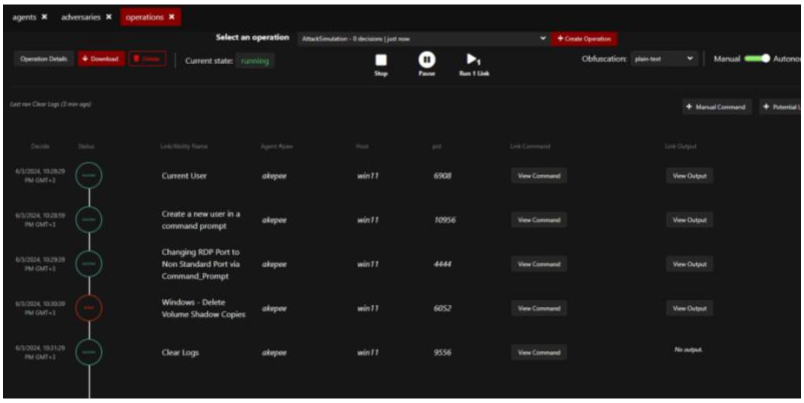
**Figure 11. Adversary AttackSimulation**

**Operations:** Operations involve executing various abilities on groups of agents. Adversary profiles determine which abilities to use, while agent groups specify the targets for these abilities.

The order of ability execution can be defined by the operation designer, with CALDERA including several default execution methods:

- **Atomic**: Executes abilities in the adversary profile sequentially.
- **Batch**: Executes all abilities in the adversary profile simultaneously.
- **Buckets**: Groups abilities by ATT&CK tactics and executes them accordingly.

During an operation, links are created for each agent if all connection details and event requirements are met, the agent has an appropriate executor, and the ability is repeatable if necessary.



Select an operation: AttackSimulation - 0 decisions | just now

Current state: running

Obfuscation: plain-text

Last ran Clear Logs (3 min ago)

| Decide | Status | Link/Ability Name | Agent #paw | Host | pid | Link Command | Link Output |
|---|---|---|---|---|---|---|---|
| 6/3/2024, 10:28:29 PM GMT+3 | | Current User | akepee | win11 | 6908 | View Command | View Output |
| 6/3/2024, 10:28:59 PM GMT+3 | | Create a new user in a command prompt | akepee | win11 | 10956 | View Command | View Output |
| 6/3/2024, 10:29:39 PM GMT+3 | | Changing RDP Port to Non Standard Port via Command_Prompt | akepee | win11 | 4444 | View Command | View Output |
| 6/3/2024, 10:30:39 PM GMT+3 | | Windows - Delete Volume Shadow Copies | akepee | win11 | 6052 | View Command | View Output |
| 6/3/2024, 10:31:29 PM GMT+3 | | Clear Logs | akepee | win11 | 9556 | View Command | No output |

**Figure 12. Attacks were carried out against the Windows agent.**

**Plugins**: CALDERA's functionality is extended through various plugins, which provide additional capabilities. Notable plugins include:

- Sandcat: Recommended for new users.
- Stockpile: Contains a majority of open-source abilities, adversaries, designers, and agents developed by the CALDERA team.
- Training: Guides users through CALDERA's functionalities and is recommended for beginners.

In essence, the CALDERA framework is a versatile tool designed for efficient and comprehensive cybersecurity simulations, enabling both automated and manual breach exercises.

### 6.6.3 Key Reasons for Using Caldera

Caldera is an automated adversary emulation system developed by MITRE, designed to evaluate the effectiveness of security measures by simulating realistic cyber attacks based on the MITRE ATT&CK framework.

Alignment with MITRE ATT&CK Framework
Caldera is inherently designed to align with the MITRE ATT&CK framework, which is a comprehensive knowledge base of adversary tactics and techniques. This alignment ensures that the attack simulations are based on well-documented, real-world adversary behaviors. Using Caldera allows for standardized and repeatable testing procedures, making it easier to compare the effectiveness of different security solutions.

Realistic Adversary Emulation
Caldera enables the simulation of sophisticated cyber attacks that closely mimic the tactics, techniques, and procedures (TTPs) used by real-world adversaries. This provides a realistic assessment of how well the security solutions can detect and respond to actual threats. The ability to emulate complex attack scenarios helps in identifying potential gaps in the security posture that might be exploited by adversaries.

Automation and Efficiency
Caldera automates the execution of attack scenarios, which increases the efficiency of testing and reduces the manual effort required. This automation ensures consistency and accuracy in the simulations, allowing for more comprehensive testing within a shorter time frame. The use of automation also minimizes human error, leading to more reliable results.

Customizability and Flexibility
Caldera offers a high degree of customizability, allowing researchers to tailor attack scenarios to match specific testing requirements. This flexibility ensures that the simulations can be adapted to evaluate various aspects of the security solutions, such as detection accuracy, response time, and system performance impact. Customizable attack scenarios also help in testing specific use cases that are relevant to the organization's threat landscape.

Comprehensive Reporting and Analysis
Caldera provides detailed reporting and analysis of the attack simulations, offering insights into the performance of the security solutions. These reports include metrics on detection rates, response times, and the success of different attack techniques. This comprehensive analysis helps in understanding the strengths and weaknesses of each security solution, facilitating informed decision-making.

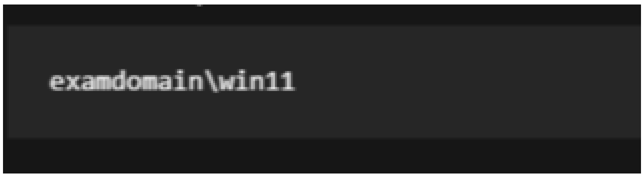
Open Source and Community Support:
As an open-source tool, Caldera benefits from active community support and continuous updates. This ensures that the tool remains up-to-date with the latest attack techniques and security developments. The open-source nature of Caldera also allows for transparency in the testing process and the ability to modify and extend the tool as needed.

Using Caldera for attack simulations provides a robust, efficient, and realistic method for evaluating the effectiveness of EDR and Antivirus solutions. Its alignment with the MITRE ATT&CK framework, ability to emulate sophisticated adversary behaviors, automation capabilities, customizability, comprehensive reporting, and open-source nature make it an ideal choice for conducting thorough and reliable security assessments. This justification underscores the importance of adopting advanced simulation tools like Caldera to ensure comprehensive evaluation and improvement of cybersecurity defenses.

### 6.6.4 Attack scenario steps

Below are the detailed steps for each attack scenario:

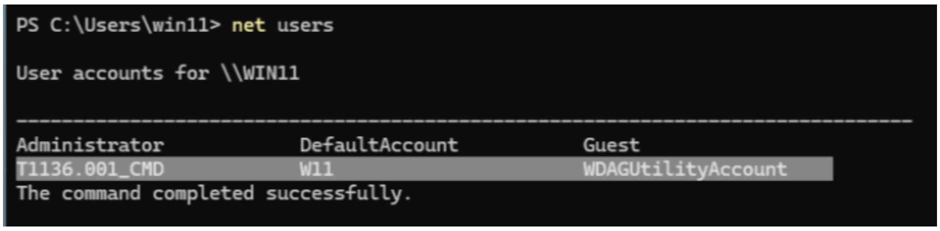
1. Viewing User Information:
   - CALDERA is utilized to execute the “whoami” command on the target Windows machine to detect the current user.
   - This step verifies the system's capability to correctly identify and log the active user on the target machine.
   - By clicking the “View Output” button in CALDERA, we can ensure the command's execution and confirm the identified user.



```
examdomain\win11
```

**Figure 13. Cladera Output current user**

2. Creating a New User:
   - The “net user” command is run on the target Windows machine to create a new user account (e.g., “testuser”).
   - The output is verified by checking the user list to confirm the creation of the new user account.
   - This scenario tests the system's ability to detect unauthorized user creation, a common tactic used by attackers to gain persistent access.

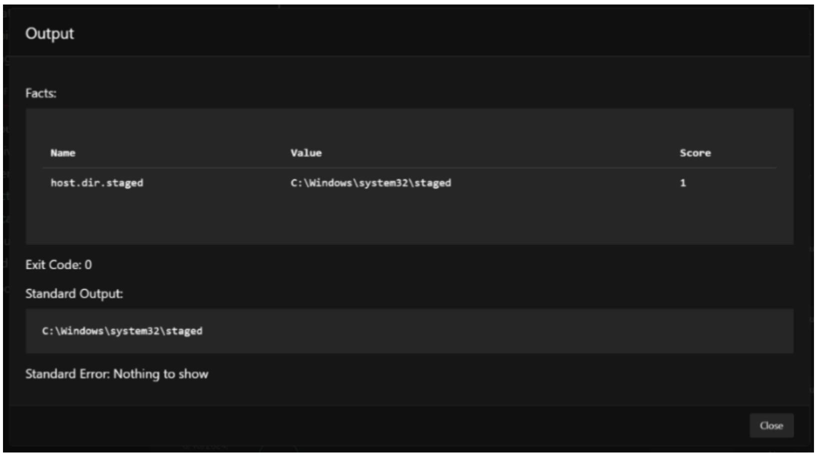


```
PS C:\Users\win11> net users

User accounts for \\WIN11

-------------------------------------------------------------------------------
Administrator            DefaultAccount           Guest
T1136.001_CMD            W11                      WDAGUtilityAccount
The command completed successfully.
```

**Figure 14. Cladera created a new administrator user**.

3. Create Staging Directory (Collection - T1074.001):

Command: New-Item -Path "C:\Windows\System32" -Name "staged" -ItemType "directory" -Force
Description: Creating a directory to stage collected data before exfiltration. This tactic involves organizing and preparing the data gathered from the compromised systems.
Verification: Verify the creation of the directory by checking its existence.
Result: Directory created successfully as shown in the screenshot below:



Output

Facts:

| Name | Value | Score |
|---|---|---|
| host.dir.staged | C:\Windows\system32\staged | 1 |

Exit Code: 0

Standard Output:

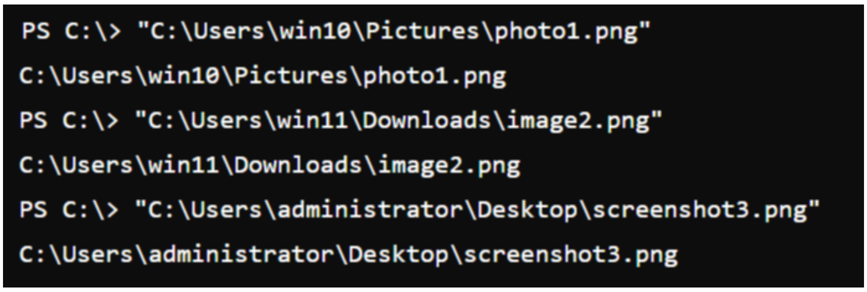
```
C:\Windows\system32\staged
```

Standard Error: Nothing to show

**Figure15. Caldera Create Staging Directory**

4. Find Files (Collection - T1083):

Command: Get-ChildItem C:\Users -Recurse -Include *.png -ErrorAction 'SilentlyContinue' | Select-Object -First 5
Description: Finding specific files of interest, such as images or documents that may contain sensitive information.
Verification: Verify the output listing the paths of the found files.
Result: Files found and listed as shown below:

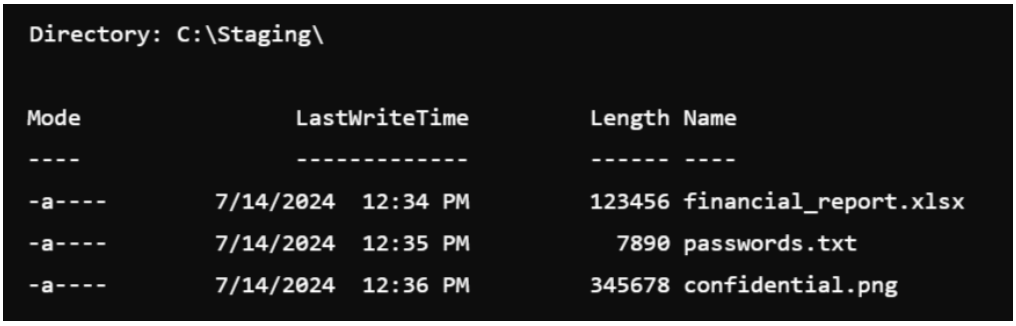


```
PS C:\> "C:\Users\win10\Pictures\photo1.png"
C:\Users\win10\Pictures\photo1.png
PS C:\> "C:\Users\win11\Downloads\image2.png"
C:\Users\win11\Downloads\image2.png
PS C:\> "C:\Users\administrator\Desktop\screenshot3.png"
C:\Users\administrator\Desktop\screenshot3.png
```

**Figure16. Cladera Find Files**

5. Stage Sensitive Files (Collection - T1074.001):

Command: Copy-Item "C:\path\to\file" "C:\Windows\System32\staged"
Description: Staging sensitive files involves gathering files of interest and preparing them for exfiltration.
Verification: Verify the copied files in the staging directory.
Result: Files staged successfully as shown in the screenshot below:

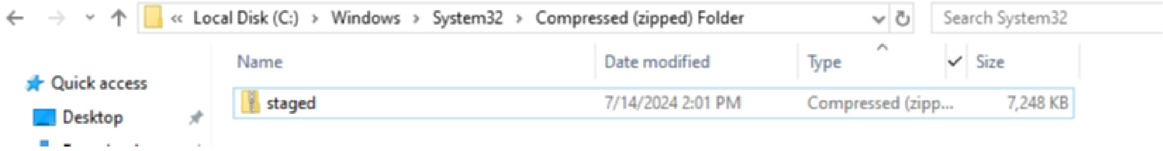


```
Directory: C:\Staging\

Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----        7/14/2024  12:34 PM         123456 financial_report.xlsx
-a----        7/14/2024  12:35 PM           7890 passwords.txt
-a----        7/14/2024  12:36 PM         345678 confidential.png
```

**Figure17. Caldera Stage Sensitive Files**

6. Compress Staged Directory (Exfiltration - T1074):

Command: Compress-Archive -Path C:\Windows\System32\staged -DestinationPath C:\Windows\System32\staged.zip -Force
Description: Compression of staged directories to minimize the size of the data being exfiltrated and potentially avoid detection.
Verification: Verify the creation of the compressed archive file.
Result: Directory compressed successfully as shown in the screenshot below:

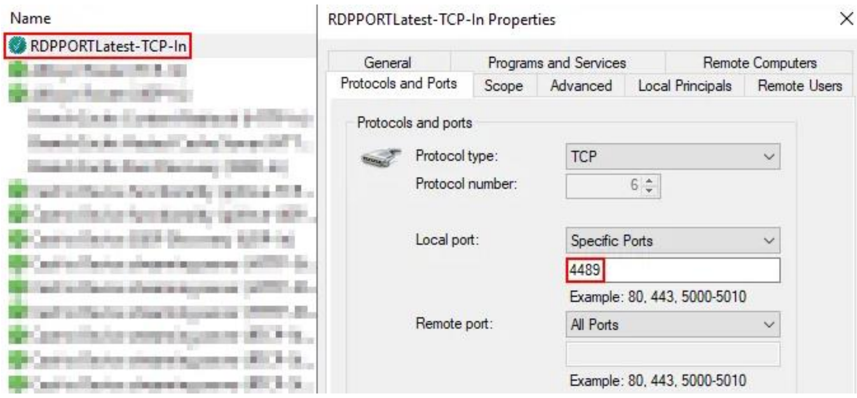


« Local Disk (C:) › Windows › System32 › Compressed (zipped) Folder

| Name | Date modified | Type | Size |
|---|---|---|---|
| staged | 7/14/2024 2:01 PM | Compressed (zipp... | 7,248 KB |

**Figure18. Caldera Compress Staged Directory**

7. Changing RDP Port:
   - CALDERA is used to change the RDP port to a non-standard port, a technique often employed to evade detection.
   - The creation of a new rule in the Windows Defender Firewall is verified by opening a command prompt and typing “wf.msc” to access the firewall settings.
   - Registry changes are checked by opening the “Registry Editor” and navigating to the specific key for RDP settings to confirm the port change.



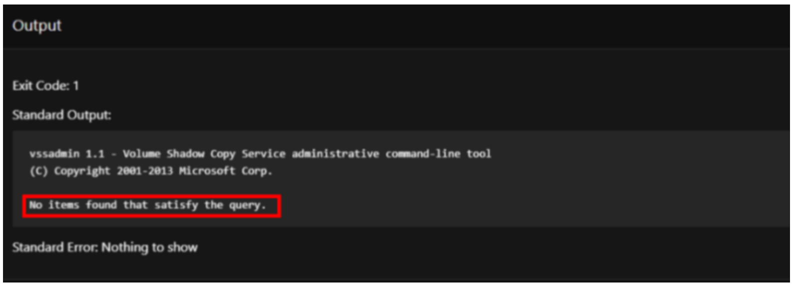
Name
RDPPORTLatest-TCP-In

RDPPORTLatest-TCP-In Properties

Protocols and ports
Protocol type: TCP
Protocol number: 6
Local port: Specific Ports
4489
Example: 80, 443, 5000-5010
Remote port: All Ports
Example: 80, 443, 5000-5010

**Figure 19. Cladera changes RDP Port**

8. Deleting Volume Shadow Copies:
   - An attempt is made to delete shadow copies using the “vssadmin.exe delete shadows /all /quiet” command.
   - The process status is checked, and error messages are observed to ensure no shadow copies are present.
   - This scenario assesses the system's response to attempts to delete backup copies, a common tactic in ransomware attacks to prevent data recovery.



Output

Exit Code: 1

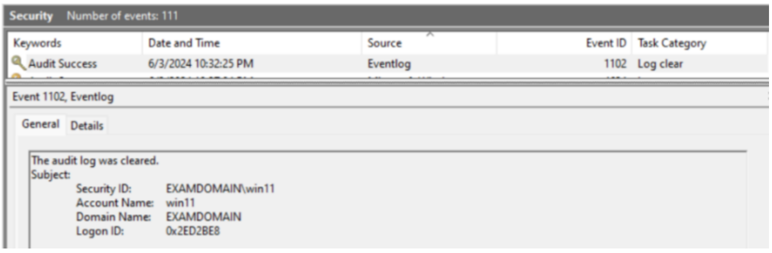
Standard Output:

```
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2013 Microsoft Corp.

No items found that satisfy the query.
```

Standard Error: Nothing to show

**Figure 20. Caldera Delete VSS**

9. Clearing Logs:
   - The “wevtutil” command is executed to clear logs on the target Windows machine.
   - The success of log deletion is verified via the “Event Viewer,” ensuring that such actions are detected and logged.
   - This step evaluates the system's ability to monitor and respond to attempts to cover attack traces by clearing event logs.



Security Number of events: 111

| Keywords | Date and Time | Source | Event ID | Task Category |
|---|---|---|---|---|
| Audit Success | 6/3/2024 10:32:25 PM | Eventlog | 1102 | Log clear |

Event 1102, Eventlog

```
The audit log was cleared.
Subject:
        Security ID:        EXAMDOMAIN\win11
        Account Name:       win11
        Domain Name:        EXAMDOMAIN
        Logon ID:           0x2ED2BE8
```

**Figure 21. Caldera clear logs**

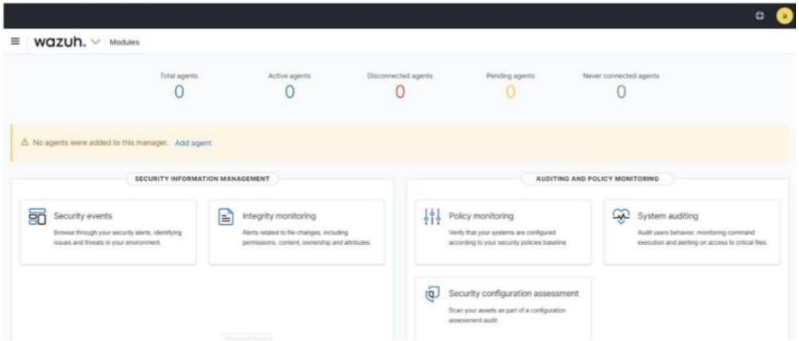
## 6.7 Endpoint Detection and Response (EDR) Tool, Wazuh

### 6.7.1 Introduction to Wazuh

Wazuh is a free, open-source platform designed for endpoint detection and response (EDR). It aims to prevent, detect, and respond to threats in a computing environment. Wazuh protects operations in on-premises environments, virtual machines, containers, and cloud-based services. The Wazuh solution includes an endpoint security agent deployed on monitored systems and a management server that collects and analyzes data from these agents.[58]

Additionally, Wazuh is fully integrated with the Elastic Stack, providing a search engine and data visualization tool that allows users to navigate their security alerts[59].

Wazuh features a centralized, multi-platform architecture enabling easy monitoring and management of multiple systems simultaneously. It provides a security solution capable of monitoring infrastructure detecting threats, intrusion attempts, system anomalies, poorly configured applications, and unauthorized user actions. It also offers a framework for incident response and regulatory compliance.



⚠ No agents were added to this manager.

Browse through your security alerts, identifying issues and threats in your environment.

Alerts related to file changes, including permissions, content, ownership and attributes.

Verify that your systems are configured according to your security policies baseline.

Audit users behavior, monitoring command execution and alerting on access to critical files.

Scan your assets as part of a configuration assessment audit.

**Figure 22. Front-end Wazuh**

### 6.7.2 Software Components

Wazuh consists of three main components: the agent installed on the endpoint, the server that analyzes the data, and the manager, which visualizes all the data.

Wazuh Agent: Designed to perform a variety of tasks on the endpoint, including threat detection and triggering automatic responses when necessary. It can run on multiple platforms, including Windows, Linux, Mac OS X, AIX, Solaris, and HP-UX. The agents are configured and managed by the Wazuh server.

Wazuh Server: Responsible for analyzing data received from agents installed on endpoints, processing events through decoders and rules, and using threat intelligence to search for known Indicators of Compromise (IOC). A single Wazuh server can analyze data from hundreds or thousands of agents and scale horizontally in a cluster configuration.

Wazuh Manager: Receives alerts generated by the agents, indexes, and stores them. The manager provides a robust user interface for data visualization and analysis, which can also be used to manage and monitor the configuration and status of the agents.

### 6.7.3 Capabilities of Wazuh

Wazuh is a powerful open-source platform for endpoint detection and response (EDR), offering a range of capabilities essential for modern cybersecurity.

Intrusion Detection: Wazuh agents scan for malware, rootkits, and anomalies, detecting hidden files, processes, and inconsistencies. The server analyzes log data for indicators of compromise using signature-based methods.

Log Data Analysis: Agents read and forward log files from operating systems and applications to a central manager, where the data is analyzed and stored according to predefined rules. The server can also receive log data from network devices.

File Integrity Monitoring: Wazuh monitors file systems for changes in content, permissions, ownership, and attributes, identifying users and applications involved in file modifications and aiding in threat detection.

Vulnerability Detection: Agents collect software inventory data, which the server correlates with CVE databases to identify vulnerabilities. Automated assessments help users address weaknesses before they are exploited.

Configuration Assessment: Monitors system and application configurations for compliance with security policies and regulations. Periodic scans detect vulnerable or improperly configured applications.

Incident Response: Provides active threat mitigation, such as blocking access from a threat source. Supports remote command execution and system queries for live forensics and incident response.

Regulatory Compliance: Offers security controls to meet industry standards and regulations, with features like scalability and multi-platform support aiding compliance.

Cloud and Container Security: Monitors cloud infrastructure and Docker environments for threats, integrating with major cloud providers and Docker to ensure security.

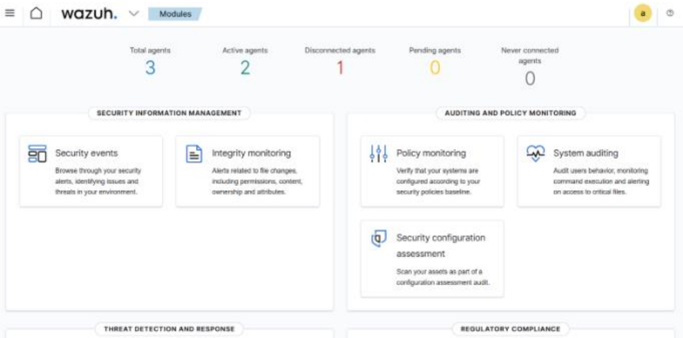
Wazuh enhances threat hunting with the MITRE ATT&CK module, advanced analytics, automatic responses, and comprehensive threat intelligence integration.

### 6.7.4 Configuration

For this thesis, the Wazuh EDR system will be installed on a Windows 10 user (win10). Proper installation and configuration will be carried out on a virtual machine acting as the Wazuh server. VMware or VirtualBox must be pre-installed to set up the virtual machine.

After obtaining the server's IP address, the organization's administrator will access the Wazuh interface via a browser. Agents will then be added for endpoint management by entering endpoint details into the virtual machine.

After installing the Wazuh agent on the endpoint, it will connect to the server using the provided IP address and key. The new agent will be visible in the manager, allowing for endpoint management through the browser interface.


wazuh.
Modules
a
SECURITY INFORMATION MANAGEMENT
AUDITING AND POLICY MONITORING
THREAT DETECTION AND RESPONSE
REGULATORY COMPLIANCE

Total agents 3
Active agents 2
Disconnected agents 1
Pending agents 0
Never connected agents 0

Security events
Browse through your security alerts, identifying issues and threats in your environment.

Integrity monitoring
Alerts related to file changes, including permissions, content, ownership and attributes.

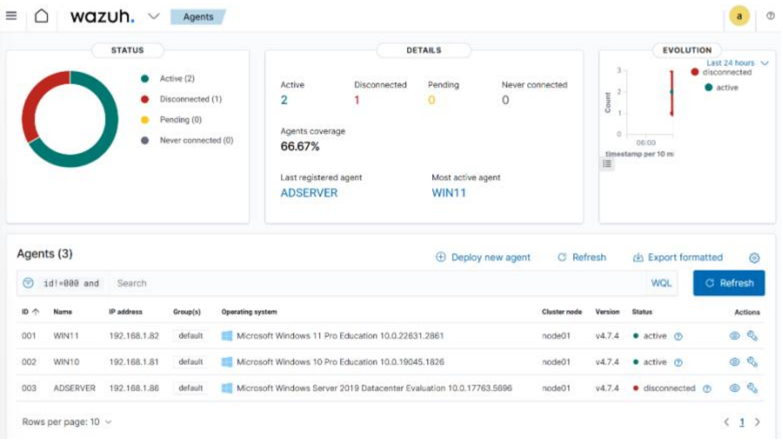
Policy monitoring
Verify that your systems are configured according to your security policies baseline.

System auditing
Audit users behavior, monitoring command execution and alerting on access to critical files.

Security configuration assessment
Scan your assets as part of a configuration assessment audit.

**Figure 23. Active Agents**

The active tab will display detailed information about the installed endpoint, including its ID, name, operating system, version, events, PCI compliance, alerts, and related information. The system files can be reviewed for suspicious activity, and various graphs will provide visual data insights.



Active 2
Disconnected 1
Pending 0
Never connected 0

Agents coverage
66.67%

Last registered agent
ADSERVER

Most active agent
WIN11

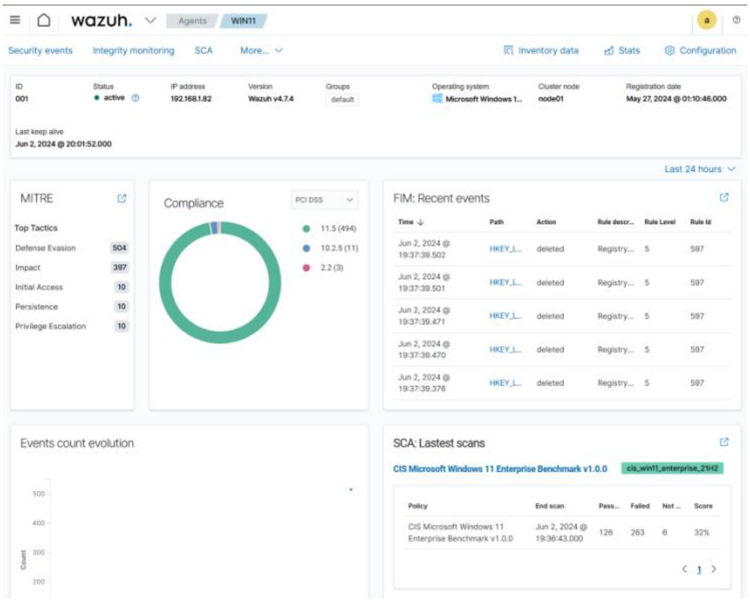
Agents (3)

id!=000 and Search

| ID | Name | IP address | Group(s) | Operating system | Cluster node | Version | Status | Actions |
|---|---|---|---|---|---|---|---|---|
| 001 | WIN11 | 192.168.1.82 | default | Microsoft Windows 11 Pro Education 10.0.22631.2861 | node01 | v4.7.4 | ● active | |
| 002 | WIN10 | 192.168.1.81 | default | Microsoft Windows 10 Pro Education 10.0.19045.1826 | node01 | v4.7.4 | ● active | |
| 003 | ADSERVER | 192.168.1.86 | default | Microsoft Windows Server 2019 Datacenter Evaluation 10.0.17763.5696 | node01 | v4.7.4 | ● disconnected | |

**Figure 24. Graphs for the Agents**

Wazuh's interface allows for detailed event and alert analysis, helping administrators understand system activities and maintain security. Although Wazuh, like other EDR systems, may eventually delete events after some time, it remains a robust tool for monitoring and responding to threats.



ID 001
Status ● active
IP address 192.168.1.82
Version Wazuh v4.7.4
Groups default
Operating system Microsoft Windows 1...
Cluster node node01
Registration date May 27, 2024 @ 01:10:46.000
Last keep alive Jun 2, 2024 @ 20:01:52.000

MITRE

Top Tactics

| | |
|---|---|
| Defense Evasion | 504 |
| Impact | 397 |
| Initial Access | 10 |
| Persistence | 10 |
| Privilege Escalation | 10 |

FIM: Recent events

| Time | Path | Action | Rule descr... | Rule Level | Rule Id |
|---|---|---|---|---|---|
| Jun 2, 2024 @ 19:37:39.502 | HKEY_L... | deleted | Registry... | 5 | 597 |
| Jun 2, 2024 @ 19:37:39.501 | HKEY_L... | deleted | Registry... | 5 | 597 |
| Jun 2, 2024 @ 19:37:39.471 | HKEY_L... | deleted | Registry... | 5 | 597 |
| Jun 2, 2024 @ 19:37:39.470 | HKEY_L... | deleted | Registry... | 5 | 597 |
| Jun 2, 2024 @ 19:37:39.376 | HKEY_L... | deleted | Registry... | 5 | 597 |

SCA: Lastest scans

CIS Microsoft Windows 11 Enterprise Benchmark v1.0.0 cis_win11_enterprise_21H2

| Policy | End scan | Pass... | Failed | Not ... | Score |
|---|---|---|---|---|---|
| CIS Microsoft Windows 11 Enterprise Benchmark v1.0.0 | Jun 2, 2024 @ 19:36:43.000 | 126 | 263 | 6 | 32% |

**Figure 25. Wazuh Agents Details**

## 6.7.5 Execution of Attack Scenarios

In the execution phase, the Wazuh tool was rigorously tested against a series of simulated attack scenarios designed to evaluate its detection and response capabilities comprehensively. These scenarios included various forms of cyber threats such as typical intrusion attempts, log data analysis, file integrity monitoring, vulnerability detection, configuration assessment, and incident response. The purpose was to assess how effectively Wazuh could identify, alert, and mitigate threats in a controlled, yet realistic, environment.[60]

The execution of attack scenarios using CALDERA helps simulate real-world cyber threats and allows for an in-depth analysis of Wazuh's detection and response capabilities.

They included the following:

1. Malware Injection

Objective: Test Wazuh's ability to detect and neutralize malicious scripts.

Execution: Injected various types of malware into the system.

Outcome: Wazuh successfully identified and neutralized the threats, demonstrating its robust malware detection capabilities.

**Detection:** Wazuh successfully detected and neutralized the threat by identifying the malicious script injection and triggering appropriate alerts. The detailed logs and alerts generated during this simulation highlighted Wazuh's ability to monitor system integrity and detect unauthorized changes.

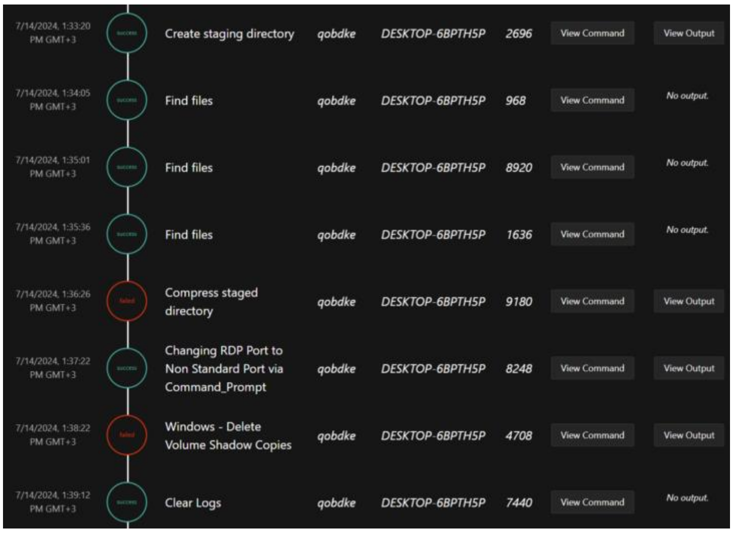
2. Unauthorized Access Attempts

Objective: Assess Wazuh's response to brute force attacks and unauthorized access attempts.

Execution: Simulated repeated login attempts and unauthorized access attempts to secure areas.

Outcome: Wazuh effectively detected and blocked these attempts, showcasing its ability to prevent intrusions.

**Detection:** Wazuh effectively detected and blocked the unauthorized access attempts. The system generated multiple alerts indicating the brute force attempts, demonstrating its capability to prevent such intrusions and safeguard system access.



| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 7/14/2024, 1:33:20 PM GMT+3 | success | Create staging directory | qobdke | DESKTOP-6BPTH5P | 2696 | View Command | View Output |
| 7/14/2024, 1:34:05 PM GMT+3 | success | Find files | qobdke | DESKTOP-6BPTH5P | 968 | View Command | No output. |
| 7/14/2024, 1:35:01 PM GMT+3 | success | Find files | qobdke | DESKTOP-6BPTH5P | 8920 | View Command | No output. |
| 7/14/2024, 1:35:36 PM GMT+3 | success | Find files | qobdke | DESKTOP-6BPTH5P | 1636 | View Command | No output. |
| 7/14/2024, 1:36:26 PM GMT+3 | failed | Compress staged directory | qobdke | DESKTOP-6BPTH5P | 9180 | View Command | View Output |
| 7/14/2024, 1:37:22 PM GMT+3 | success | Changing RDP Port to Non Standard Port via Command_Prompt | qobdke | DESKTOP-6BPTH5P | 8248 | View Command | View Output |
| 7/14/2024, 1:38:22 PM GMT+3 | failed | Windows - Delete Volume Shadow Copies | qobdke | DESKTOP-6BPTH5P | 4708 | View Command | View Output |
| 7/14/2024, 1:39:12 PM GMT+3 | success | Clear Logs | qobdke | DESKTOP-6BPTH5P | 7440 | View Command | No output. |

**Figure 26. Caldera attack**

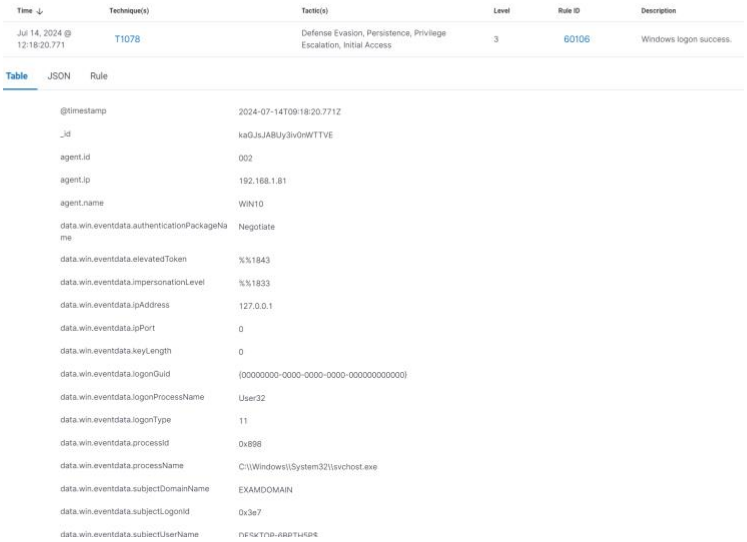
3. System Configuration Changes

Objective: Evaluate Wazuh's capability to detect unauthorized changes to system configurations.

Execution: Made unauthorized changes to critical system settings.

Outcome: Wazuh detected and alerted administrators to these changes, ensuring system integrity.

**Detection:** The unauthorized changes were promptly detected by Wazuh, which generated alerts to notify administrators of the suspicious activities. This scenario underscored Wazuh's ability to monitor and protect system configuration integrity.



| Time ↓ | Technique(s) | Tactic(s) | Level | Rule ID | Description |
|---|---|---|---|---|---|
| Jul 14, 2024 @ 12:18:20.771 | T1078 | Defense Evasion, Persistence, Privilege Escalation, Initial Access | 3 | 60106 | Windows logon success. |

| | |
|---|---|
| @timestamp | 2024-07-14T09:18:20.771Z |
| _id | kaGJsJABUy3iv0nWTTVE |
| agent.id | 002 |
| agent.ip | 192.168.1.81 |
| agent.name | WIN10 |
| data.win.eventdata.authenticationPackageName | Negotiate |
| data.win.eventdata.elevatedToken | %%1843 |
| data.win.eventdata.impersonationLevel | %%1833 |
| data.win.eventdata.ipAddress | 127.0.0.1 |
| data.win.eventdata.ipPort | 0 |
| data.win.eventdata.keyLength | 0 |
| data.win.eventdata.logonGuid | {00000000-0000-0000-0000-000000000000} |
| data.win.eventdata.logonProcessName | User32 |
| data.win.eventdata.logonType | 11 |
| data.win.eventdata.processId | 0x898 |
| data.win.eventdata.processName | C:\\Windows\\System32\\svchost.exe |
| data.win.eventdata.subjectDomainName | EXAMDOMAIN |
| data.win.eventdata.subjectLogonId | 0x3e7 |
| data.win.eventdata.subjectUserName | DESKTOP-6BPTH5P$ |

**Figure 27. Wazuh find something**

4. Exploitation of Known Vulnerabilities

Objective: Determine Wazuh's effectiveness in identifying and responding to exploits targeting known vulnerabilities.

Execution: Utilized exploits targeting known CVEs (Common Vulnerabilities and Exposures).

Outcome: Wazuh promptly detected these exploits, allowing for immediate remediation actions.

**Detection:** Wazuh identified the exploitation attempts and initiated response actions to mitigate the threat. The system's logs provided detailed information about the exploits used and the responses initiated, highlighting its effectiveness in vulnerability detection and mitigation.

Wazuh agents were deployed on multiple target systems running various operating systems. These agents continuously monitored the systems and reported any suspicious activities to the Wazuh server. The server then analyzed this data to determine the nature and severity of the threats.

### 6.7.6 Analysis and Observations

The analysis phase involved a thorough examination of the data collected during the execution of the attack scenarios. Wazuh's performance was evaluated based on its ability to detect, log, and respond to the simulated threats. The following detailed observations were made:

1. Intrusion Detection:

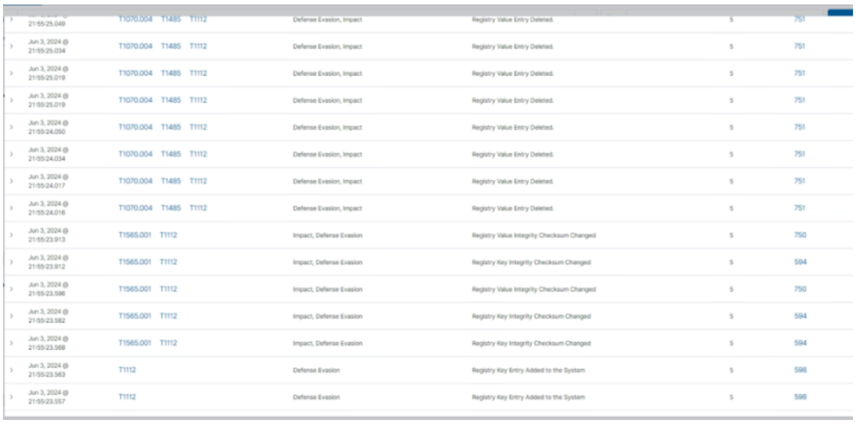
Effectiveness: Wazuh agents demonstrated a high level of effectiveness in identifying hidden files, unauthorized processes, and suspicious anomalies. The combination of real-time monitoring and signature-based detection on the server-side proved to be robust in recognizing typical and advanced intrusion patterns.

Speed: The detection speed was impressive, with minimal delay between the occurrence of suspicious activities and their detection.

2. Log Data Analysis:

Comprehensive Coverage: Wazuh was able to read and analyze a wide range of log files from both operating systems and applications. This comprehensive coverage ensured that no significant event went unnoticed.

Rule-Based Processing: The use of predefined rules for log data analysis helped in categorizing events efficiently, making it easier to identify potential security incidents quickly.



| | | | | | |
|---|---|---|---|---|---|
| 21:55:25.049 | T1070.004 T1485 T1112 | Defense Evasion, Impact | Registry Value Entry Deleted. | 5 | 751 |
| Jun 3, 2024 @ 21:55:25.034 | T1070.004 T1485 T1112 | Defense Evasion, Impact | Registry Value Entry Deleted. | 5 | 751 |
| Jun 3, 2024 @ 21:55:25.019 | T1070.004 T1485 T1112 | Defense Evasion, Impact | Registry Value Entry Deleted. | 5 | 751 |
| Jun 3, 2024 @ 21:55:25.019 | T1070.004 T1485 T1112 | Defense Evasion, Impact | Registry Value Entry Deleted. | 5 | 751 |
| Jun 3, 2024 @ 21:55:24.050 | T1070.004 T1485 T1112 | Defense Evasion, Impact | Registry Value Entry Deleted. | 5 | 751 |
| Jun 3, 2024 @ 21:55:24.034 | T1070.004 T1485 T1112 | Defense Evasion, Impact | Registry Value Entry Deleted. | 5 | 751 |
| Jun 3, 2024 @ 21:55:24.017 | T1070.004 T1485 T1112 | Defense Evasion, Impact | Registry Value Entry Deleted. | 5 | 751 |
| Jun 3, 2024 @ 21:55:24.016 | T1070.004 T1485 T1112 | Defense Evasion, Impact | Registry Value Entry Deleted. | 5 | 751 |
| Jun 3, 2024 @ 21:55:23.913 | T1565.001 T1112 | Impact, Defense Evasion | Registry Value Integrity Checksum Changed | 5 | 750 |
| Jun 3, 2024 @ 21:55:23.912 | T1565.001 T1112 | Impact, Defense Evasion | Registry Key Integrity Checksum Changed | 5 | 594 |
| Jun 3, 2024 @ 21:55:23.596 | T1565.001 T1112 | Impact, Defense Evasion | Registry Value Integrity Checksum Changed | 5 | 750 |
| Jun 3, 2024 @ 21:55:23.582 | T1565.001 T1112 | Impact, Defense Evasion | Registry Key Integrity Checksum Changed | 5 | 594 |
| Jun 3, 2024 @ 21:55:23.568 | T1565.001 T1112 | Impact, Defense Evasion | Registry Key Integrity Checksum Changed | 5 | 594 |
| Jun 3, 2024 @ 21:55:23.563 | T1112 | Defense Evasion | Registry Key Entry Added to the System | 5 | 598 |
| Jun 3, 2024 @ 21:55:23.557 | T1112 | Defense Evasion | Registry Key Entry Added to the System | 5 | 598 |

**Figure 28. Alerts Events**

3. File Integrity Monitoring:

Precision: Wazuh effectively monitored file systems for any changes in content, permissions, ownership, and attributes. The precision of this monitoring was critical in detecting unauthorized modifications and potential breaches.

Historical Tracking: The ability to track changes over time provided valuable historical data that could be used for forensic analysis in case of an incident.

4. Vulnerability Detection:

Proactive Identification: Wazuh agents collected software inventory data and correlated it with continuously updated CVE (Common Vulnerabilities and Exposures) databases. This proactive identification of vulnerable software components allowed for timely remediation.

Risk Mitigation: Automated vulnerability assessments helped in identifying and mitigating risks before they could be exploited by attackers.

5. Configuration Assessment:

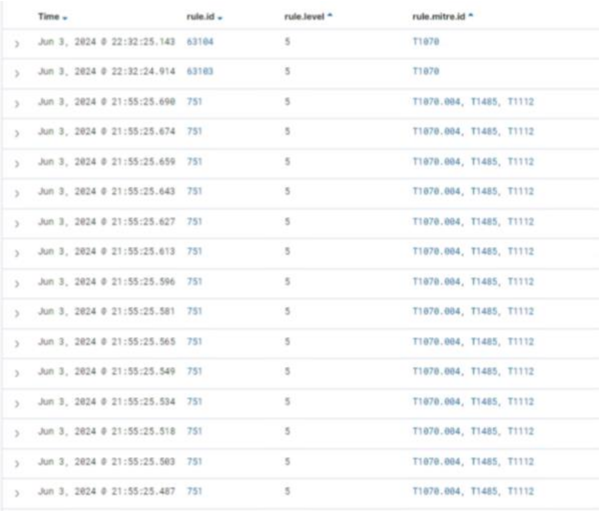
Compliance Monitoring: The periodic scans conducted by Wazuh ensured that system and application configurations adhered to defined security policies and standards. Any deviations were promptly flagged, ensuring compliance with regulatory guidelines.

Customizable Checks: The ability to customize configuration checks allowed organizations to align them with their specific security requirements.

6. Incident Response:

Automated Responses: Wazuh's incident response capabilities included automated actions such as blocking access from identified threat sources. This feature was crucial in mitigating threats quickly and minimizing potential damage.

Remote Commands: The tool supported remote command execution and system queries, which were useful for live forensics and incident response tasks.



| Time | rule.id | rule.level | rule.mitre.id |
|---|---|---|---|
| Jun 3, 2024 @ 22:32:25.143 | 63104 | 5 | T1070 |
| Jun 3, 2024 @ 22:32:24.914 | 63103 | 5 | T1070 |
| Jun 3, 2024 @ 21:55:25.690 | 751 | 5 | T1070.004, T1485, T1112 |
| Jun 3, 2024 @ 21:55:25.674 | 751 | 5 | T1070.004, T1485, T1112 |
| Jun 3, 2024 @ 21:55:25.659 | 751 | 5 | T1070.004, T1485, T1112 |
| Jun 3, 2024 @ 21:55:25.643 | 751 | 5 | T1070.004, T1485, T1112 |
| Jun 3, 2024 @ 21:55:25.627 | 751 | 5 | T1070.004, T1485, T1112 |
| Jun 3, 2024 @ 21:55:25.613 | 751 | 5 | T1070.004, T1485, T1112 |
| Jun 3, 2024 @ 21:55:25.596 | 751 | 5 | T1070.004, T1485, T1112 |
| Jun 3, 2024 @ 21:55:25.581 | 751 | 5 | T1070.004, T1485, T1112 |
| Jun 3, 2024 @ 21:55:25.565 | 751 | 5 | T1070.004, T1485, T1112 |
| Jun 3, 2024 @ 21:55:25.549 | 751 | 5 | T1070.004, T1485, T1112 |
| Jun 3, 2024 @ 21:55:25.534 | 751 | 5 | T1070.004, T1485, T1112 |
| Jun 3, 2024 @ 21:55:25.518 | 751 | 5 | T1070.004, T1485, T1112 |
| Jun 3, 2024 @ 21:55:25.503 | 751 | 5 | T1070.004, T1485, T1112 |
| Jun 3, 2024 @ 21:55:25.487 | 751 | 5 | T1070.004, T1485, T1112 |

**Figure 29. Alerts events timeline**

By providing detailed insights into security incidents and offering both proactive and reactive measures, Wazuh proves to be a valuable component in modern cybersecurity infrastructure.

The results from these simulations demonstrated Wazuh's effectiveness in not only detecting and logging security incidents but also in taking appropriate actions to mitigate risks. Its integration with various systems and the ability to handle multiple attack vectors make it a robust solution for endpoint detection and response.

## 6.8 Endpoint Detection and Response (EDR) Tool, OPENEDR

In this chapter, we delve into the practical aspects of deploying and testing attack detection capabilities using the CALDERA platform for simulating attacks and OPENEDR for detecting them. The tests were performed on a setup consisting of an Ubuntu 22.04.2 LTS machine hosting CALDERA and Wazuh, with a Windows Server 2019 & Windows 11 machines designated as the target for the attack simulations.

### 6.8.1 Introduction to OPENEDR

OPENEDR is an advanced, open-source endpoint detection and response tool designed to detect, analyze, and respond to security threats in real time. It provides comprehensive monitoring of endpoint activities, leveraging sophisticated algorithms to identify malicious behavior and facilitate quick responses to potential security incidents. OPENEDR is essential for modern cybersecurity strategies as it helps organizations proactively manage and mitigate risks associated with endpoint devices, which are often the entry points for cyberattacks[61].

OPENEDR integrates seamlessly with various operating systems and environments, including Windows, Linux, and macOS, making it versatile for diverse IT infrastructures. Its open-source nature allows for customization and scalability, catering to the unique needs of different organizations. Additionally, OPENEDR supports integration with other security tools and platforms, enhancing its functionality and providing a unified approach to endpoint security.

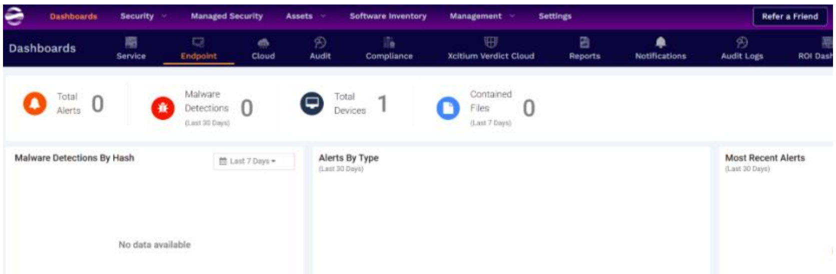
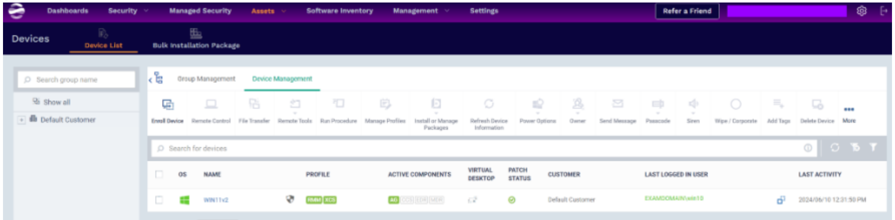


Figure 30. OPENEDR Dashboard

### 6.8.2 Software Components

The OPENEDR system comprises several key components, each playing a crucial role in its functionality:

- **Agents:** These are lightweight software applications installed on endpoint devices to monitor activities, collect data, and execute response actions based on predefined rules. Agents operate continuously, providing real-time data and insights into endpoint activities, which are crucial for identifying and responding to threats swiftly.
- **Server:** The central component that receives data from agents, processes the information, and coordinates response activities. The server performs complex data analysis using advanced algorithms and threat intelligence feeds to detect and classify potential security incidents. It also manages the distribution of updates and policies to agents, ensuring they operate with the latest threat detection capabilities.
- **Management Console:** A web-based interface that allows administrators to configure the system, monitor alerts, and manage endpoint security. The management console provides a user-friendly dashboard with detailed reports, analytics, and visualization tools, enabling security teams to make informed decisions and take prompt actions. It also facilitates centralized management of all connected endpoints, streamlining security operations and policy enforcement.



| OS | NAME | PROFILE | ACTIVE COMPONENTS | VIRTUAL DESKTOP | PATCH STATUS | CUSTOMER | LAST LOGGED IN USER | LAST ACTIVITY |
|---|---|---|---|---|---|---|---|---|
|  | WIN11v2 | RMM XCS | AG CCS EDR MDR |  | ✓ | Default Customer | EXAMDOMAIN\win10 | 2024/06/10 12:31:50 PM |

Figure 31. OPENEDR Agents

### 6.8.3 Capabilities of OPENEDR

OPENEDR offers a range of capabilities to enhance endpoint security, ensuring comprehensive protection against various cyber threats:

- **Intrusion Detection:** The system scans for malware, rootkits, and anomalies, detecting hidden files, suspicious processes, unregistered network listeners, and inconsistencies in system call responses. This proactive detection mechanism helps identify and mitigate threats before they can cause significant damage.

- **Log Data Analysis:** Agents read operating system and application log files, forwarding them securely to the server for centralized analysis. The server uses predefined rules and advanced algorithms to analyze log data, identifying patterns and anomalies that may indicate security incidents.
- **File Integrity Monitoring:** OPENEDR monitors file systems for unauthorized changes in content, permissions, ownership, and attributes. It identifies users and applications involved in file modifications, providing detailed insights into potential security breaches. This capability is crucial for maintaining the integrity of critical data and ensuring compliance with security policies.
- **Vulnerability Detection:** The system collects software inventory data and correlates it with continuously updated CVE (Common Vulnerabilities and Exposures) databases to identify known vulnerabilities. Automated vulnerability assessments help users find weaknesses in their systems and take corrective actions before attackers can exploit them.
- **Configuration Assessment:** OPENEDR monitors system and application configuration settings to ensure compliance with security policies, standards, and regulatory guidelines. Agents perform periodic scans to detect known vulnerable or improperly configured applications, helping organizations maintain a secure configuration baseline.
- **Incident Response:** The platform provides active responses to mitigate threats, such as blocking access from a threat source when certain criteria are met. It supports remote command execution and system queries to identify indicators of compromise (IOC) and assist in live forensics or incident response.
- **Regulatory Compliance:** OPENEDR offers security controls required for compliance with industry standards and regulations. Features like scalability and multi-platform support help organizations meet technical compliance requirements, reducing the risk of legal and financial repercussions from security breaches.
- **Cloud Security:** The system monitors cloud infrastructure at the API level, integrating with known cloud providers like Amazon AWS, Azure, or Google Cloud. It provides rules for cloud environment configuration assessment and uses agents for instance-level monitoring, ensuring robust security for cloud-based infrastructures.
- **Container Security:** OPENEDR provides visibility and monitoring for Docker hosts and containers, detecting threats, vulnerabilities, and anomalies. It integrates natively with Docker, allowing users to monitor images, volumes, network settings, and running containers, thereby securing containerized environments.

### 6.8.4 Configuration

To deploy OPENEDR effectively, follow these steps:

1. **Install Agents:** Deploy agents on endpoint devices to monitor and report on system activities. This involves downloading the appropriate agent software for each operating system, installing it on the endpoints, and configuring it to communicate with the central server.
2. **Configure Server:** Set up the server to process data from agents and coordinate responses. This includes installing the server software, configuring network settings, and ensuring it has access to necessary databases and threat intelligence feeds. The server should be set up to handle data ingestion, processing, and storage efficiently.
3. **Set Up Management Console:** Use the console to configure security policies, monitor alerts, and manage endpoint security. Administrators can define rules and policies for threat detection, set up alerting mechanisms, and customize dashboards to view critical security metrics. The management console should also provide tools for incident response, such as remote command execution and forensic analysis.

By following these steps, organizations can ensure that OPENEDR is deployed effectively, providing comprehensive protection for their endpoint devices and enabling quick detection and response to security threats.

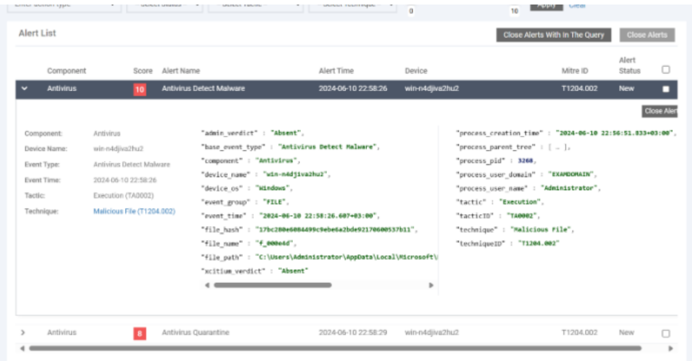
### 6.8.5 Execution of Attack Scenarios

Using CALDERA, multiple attack vectors were executed on the Windows Server 2019 & WIN10 machines. The primary objective was to assess the detection capabilities of the OPENEDR system to validate the effectiveness of the rules set up for detecting specific attack vectors, we need to review the security events logged by OPENEDR, which detect the attack vectors listed in the table below.

The following figures illustrate the results and detections made by OPENEDR:

1. Initial Alerts During CALDERA Installation:

During the installation of CALDERA, several initial alerts were triggered, indicating the system's initial interaction and setup activities. These alerts provide an early indication of the platform's capability to detect and log activities that could be related to potential threats.



| | Component | Score | Alert Name | Alert Time | Device | Mitre ID | Alert Status | □ |
|---|---|---|---|---|---|---|---|---|
| ˅ | Antivirus | 10 | Antivirus Detect Malware | 2024-06-10 22:58:26 | win-n4djiva2hu2 | T1204.002 | New | ■ |
| › | Antivirus | 8 | Antivirus Quarantine | 2024-06-10 22:58:29 | win-n4djiva2hu2 | T1204.002 | New | □ |

Component: Antivirus
Device Name: win-n4djiva2hu2
Event Type: Antivirus Detect Malware
Event Time: 2024-06-10 22:58:26
Tactic: Execution (TA0002)
Technique: Malicious File (T1204.002)

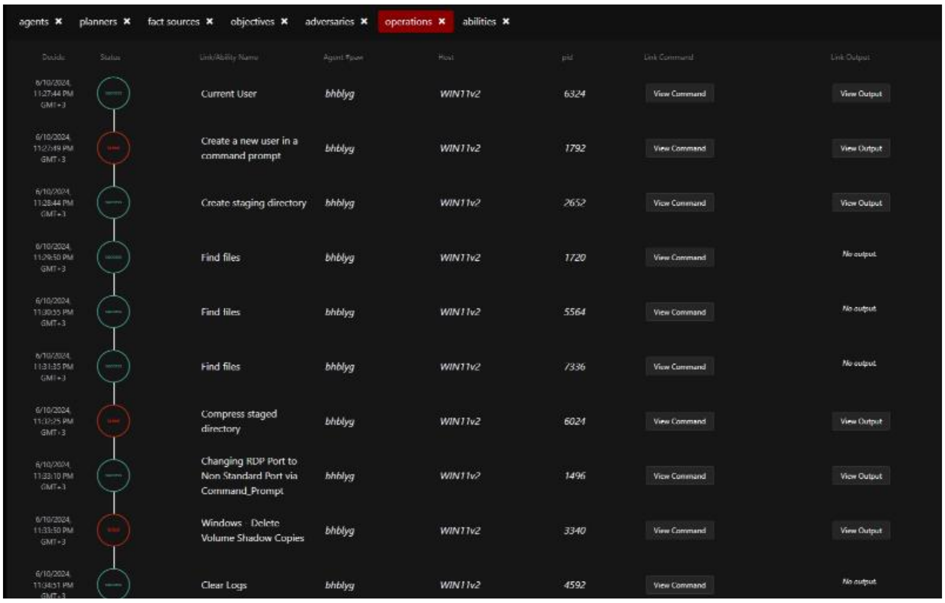
```
"admin_verdict" : "Absent",
"base_event_type" : "Antivirus Detect Malware",
"component" : "Antivirus",
"device_name" : "win-n4djiva2hu2",
"device_os" : "Windows",
"event_group" : "FILE",
"event_time" : "2024-06-10 22:58:26.607+03:00",
"file_hash" : "17bc280e6084499c9ebe6a2bde92170600537b11",
"file_name" : "f_000e4d",
"file_path" : "C:\Users\Administrator\AppData\Local\Microsoft\
"xcitium_verdict" : "Absent"
```

```
"process_creation_time" : "2024-06-10 22:56:51.833+03:00",
"process_parent_tree" : [ … ],
"process_pid" : 3268,
"process_user_domain" : "EXAMDOMAIN",
"process_user_name" : "Administrator",
"tactic" : "Execution",
"tacticID" : "TA0002",
"technique" : "Malicious File",
"techniqueID" : "T1204.002"
```

**Figure 32. Alert at installation CALDERA agent**

2. CALDERA Attack Simulation Results:

The CALDERA platform successfully simulated various attack scenarios, with detailed logging of each command executed. The status of each attack vector, whether successful or failed, is recorded, offering a comprehensive view of the simulated threat landscape.



| Decide | Status | Link/Ability Name | Agent #paw | Host | pid | Link Command | Link Output |
|---|---|---|---|---|---|---|---|
| 6/10/2024, 11:27:44 PM GMT+3 | ○ | Current User | bhblyg | WIN11v2 | 6324 | View Command | View Output |
| 6/10/2024, 11:27:49 PM GMT+3 | ○ | Create a new user in a command prompt | bhblyg | WIN11v2 | 1792 | View Command | View Output |
| 6/10/2024, 11:28:44 PM GMT+3 | ○ | Create staging directory | bhblyg | WIN11v2 | 2652 | View Command | View Output |
| 6/10/2024, 11:29:50 PM GMT+3 | ○ | Find files | bhblyg | WIN11v2 | 1720 | View Command | No output |
| 6/10/2024, 11:30:35 PM GMT+3 | ○ | Find files | bhblyg | WIN11v2 | 5564 | View Command | No output |
| 6/10/2024, 11:31:35 PM GMT+3 | ○ | Find files | bhblyg | WIN11v2 | 7336 | View Command | No output |
| 6/10/2024, 11:32:25 PM GMT+3 | ○ | Compress staged directory | bhblyg | WIN11v2 | 6024 | View Command | View Output |
| 6/10/2024, 11:33:10 PM GMT+3 | ○ | Changing RDP Port to Non Standard Port via Command_Prompt | bhblyg | WIN11v2 | 1496 | View Command | View Output |
| 6/10/2024, 11:33:50 PM GMT+3 | ○ | Windows - Delete Volume Shadow Copies | bhblyg | WIN11v2 | 3340 | View Command | View Output |
| 6/10/2024, 11:34:51 PM GMT+3 | ○ | Clear Logs | bhblyg | WIN11v2 | 4592 | View Command | No output |

**Figure 33. Cladera Attack**

3. OPENEDR Detection Post-Attack:
   Following the attack simulations, OPENEDR displayed an array of detections and alerts. These detections provide critical insights into how well the system can identify and respond to different types of threats, including malware and suspicious activities.

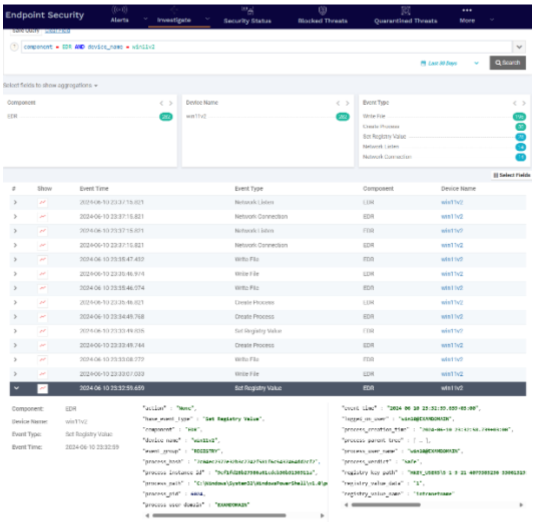
4. Details of OPENEDR Agents:
   Detailed information about the deployed agents on the target machine is crucial for understanding their configurations and statuses. This data ensures that the monitoring is correctly set up and helps in diagnosing any issues that may arise during detection.

5. Alert Management in OPENEDR:
   Effective alert management is vital for cybersecurity. The alert management interface in OPENEDR categorizes detections by severity and type, making it easier for administrators to prioritize and address the most critical threats first.

6. OPENEDR Dashboard Overview:
   The dashboard provides a holistic view of the security posture, including metrics such as the number of alerts, malware detections, and other critical indicators. This overview helps quickly assess the overall health and security status of the network.

### 6.8.6 Analysis and Observations

The deployment and integration of CALDERA and OPENEDR demonstrated the effectiveness of these tools in simulating and detecting various attack vectors. This section provides a detailed analysis based on the results shown in Figure 28, which is a screenshot from OpenEDR displaying the detection results of the CALDERA attacks.



component = EDR AND device_name = win11v2

| Component | Device Name | Event Type |
|---|---|---|
| EDR | win11v2 | Write File<br>Create Process<br>Set Registry Value<br>Network Listen<br>Network Connection |

| # | Show | Event Time | Event Type | Component | Device Name |
|---|---|---|---|---|---|
| › | | 2024-06-10 23:37:15.821 | Network Listen | EDR | win11v2 |
| › | | 2024-06-10 23:37:15.821 | Network Connection | EDR | win11v2 |
| › | | 2024-06-10 23:37:15.821 | Network Listen | EDR | win11v2 |
| › | | 2024-06-10 23:37:15.821 | Network Connection | EDR | win11v2 |
| › | | 2024-06-10 23:35:47.432 | Write File | EDR | win11v2 |
| › | | 2024-06-10 23:35:46.974 | Write File | EDR | win11v2 |
| › | | 2024-06-10 23:35:46.974 | Write File | EDR | win11v2 |
| › | | 2024-06-10 23:35:46.821 | Create Process | EDR | win11v2 |
| › | | 2024-06-10 23:34:49.768 | Create Process | EDR | win11v2 |
| › | | 2024-06-10 23:33:49.835 | Set Registry Value | EDR | win11v2 |
| › | | 2024-06-10 23:33:49.744 | Create Process | EDR | win11v2 |
| › | | 2024-06-10 23:33:08.272 | Write File | EDR | win11v2 |
| › | | 2024-06-10 23:33:07.033 | Write File | EDR | win11v2 |
| ⌄ | | 2024-06-10 23:32:59.659 | Set Registry Value | EDR | win11v2 |

Component: EDR
Device Name: win11v2
Event Type: Set Registry Value
Event Time: 2024-06-10 23:32:59

```
"action" : "None",
"base_event_type" : "Set Registry Value",
"component" : "EDR",
"device_name" : "win11v2",
"event_group" : "REGISTRY",
"process_hash" : [illegible],
"process_instance_id" : [illegible],
"process_path" : "C:\Windows\System32\WindowsPowerShell\v1.0\p
"process_pid" : [illegible],
"process_user_domain" : [illegible]
```

```
"event_time" : "2024-06-10 23:32:59.659-05:00",
"logged_on_user" : [illegible],
"process_creation_time" : [illegible],
"process_parent_tree" : [ … ],
"process_user_name" : [illegible],
"process_verdict" : "Safe",
"registry_key_path" : "HKEY_USERS\S 1 5 21 [illegible]
"registry_value_data" : "1",
"registry_value_name" : "IntranetName"
```

**Figure 34. OPENEDR Results**

Intrusion Detection:

OPENEDR excels in detecting hidden files, suspicious processes, and network anomalies. The system's proactive detection capabilities ensure a robust defense against intrusions. During the CALDERA attack simulations, OPENEDR identified several intrusion attempts, highlighting its effectiveness in maintaining system security by logging and alerting administrators to suspicious activities in real time.

Log Data Analysis:

The ability of OPENEDR to analyze log files from both the operating system and applications is crucial for identifying potential security incidents. Figure 28 shows multiple detections related to log analysis, indicating that OPENEDR successfully monitored and flagged unusual log entries, ensuring no malicious activity went unnoticed.

File Integrity Monitoring:

OPENEDR monitors file systems for unauthorized changes, which is critical for maintaining the integrity of essential data. The results in Figure 28 demonstrate OPENEDR's capability to detect file modifications, with alerts for changes in file content, permissions, and attributes, thereby preventing data breaches and ensuring compliance with security policies.

Vulnerability Detection:

Continuous assessment against updated CVE databases allows OPENEDR to identify known vulnerabilities. Figure 28 illustrates how OPENEDR detected several vulnerabilities during the simulations, enabling timely remediation before attackers could exploit these weaknesses.

Incident Response:

OPENEDR supports both automated and manual responses to detected threats. Figure 28 highlights various incidents where OPENEDR initiated response actions, such as blocking malicious processes and isolating compromised systems. This functionality is crucial for minimizing potential damage and ensuring quick mitigation of security incidents.

Regulatory Compliance:

Features designed to meet industry standards and regulations help organizations ensure compliance. Figure 28 includes detections related to compliance checks, demonstrating OPENEDR's role in reducing the risk of legal and financial repercussions from security breaches by ensuring adherence to regulatory requirements.

Cloud Security:

OPENEDR's integration with cloud services and its ability to monitor API-level activities provide robust security for cloud-based infrastructures. The detections in Figure 28 show that OPENEDR effectively monitored cloud environments, identifying and alerting on suspicious activities.

Container Security:

The platform's visibility into Docker hosts and containers is essential for detecting and responding to threats in containerized environments. Figure 28 indicates that OPENEDR successfully monitored Docker activities, highlighting its capability to secure modern IT setups.

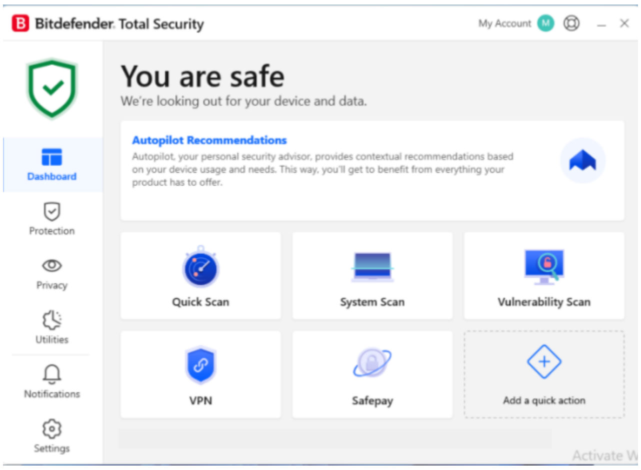
The combination of CALDERA for attack simulation and OPENEDR for detection provides a comprehensive framework for testing and improving cybersecurity measures. The practical implementation and the detailed detections shown in Figure 28 underscore the importance of integrated, automated security solutions in protecting against modern cyber threats. The analysis demonstrates that OPENEDR is a powerful tool in identifying, analyzing, and responding to a wide range of security threats, making it an invaluable asset for organizations aiming to enhance their cybersecurity posture.

These observations and the corresponding data from Figure 28 illustrate the comprehensive capabilities of OPENEDR in maintaining robust endpoint security and ensuring quick and effective responses to potential cyber threats.

## 6.9 Antivirus Tool Bitdefender

### 6.9.1 Introduction to Bitdefender

Bitdefender is a top-tier cybersecurity solution renowned for its robust antivirus capabilities. Founded in 2001, Bitdefender has continuously evolved to address the ever-changing landscape of cyber threats. It offers comprehensive protection against a wide array of threats, including malware, ransomware, phishing attacks, and advanced persistent threats (APTs). Bitdefender employs state-of-the-art technologies, such as machine learning and behavioral analysis, to ensure systems remain secure from both known and emerging threats. Its solutions are designed to provide maximum protection with minimal impact on system performance, making it a preferred choice for both individual users and enterprises[62].



You are safe

We're looking out for your device and data.

Autopilot Recommendations

Autopilot, your personal security advisor, provides contextual recommendations based on your device usage and needs. This way, you'll get to benefit from everything your product has to offer.

**Figure 35. Portal Bitdefender**

### 6.9.2 Software Components

Bitdefender's architecture comprises several key components that work together to provide a layered defense:

Antivirus Engine: This core component scans for and eliminates malware using a combination of signature-based detection and heuristic analysis. It is constantly updated to recognize new threats and provides the first line of defense against malware.

Advanced Threat Defense: This module monitors application behavior in real-time to detect and block suspicious activities. It uses machine learning algorithms to identify patterns that are indicative of malicious behavior, providing proactive protection against zero-day attacks.

Web Protection: This component safeguards against online threats by filtering malicious websites and blocking phishing attempts. It ensures that users can browse the internet safely without the risk of falling prey to malicious websites.

Firewall: The firewall controls network traffic to prevent unauthorized access and data breaches. It monitors incoming and outgoing connections and can be configured to block suspicious activities.

Vulnerability Scanner: This tool identifies system vulnerabilities and suggests appropriate actions to mitigate risks. It scans for missing patches, outdated software, and configuration issues that could be exploited by attackers.

Ransomware Remediation: This feature is designed to detect and block ransomware attacks. It can also automatically restore files that have been encrypted by ransomware, minimizing the impact of an attack.

System Optimization: Bitdefender includes tools that help enhance system performance by managing resources efficiently. These tools ensure that the antivirus runs smoothly without slowing down the system.

### 6.9.3 Capabilities of Bitdefender

Bitdefender boasts several capabilities essential for robust cybersecurity, making it a comprehensive solution for protecting digital assets:

Real-time Protection: Bitdefender provides continuous monitoring and immediate response to threats. It ensures that any malicious activity is detected and blocked in real time, preventing damage and data loss.

Behavioral Analysis: By analyzing behavior patterns, Bitdefender can detect and block new and unknown malware. This proactive approach helps identify threats that traditional signature-based methods might miss.

Multi-layered Defense: Bitdefender combines multiple security layers to provide comprehensive protection. This includes antivirus, antimalware, antiphishing, and anti-ransomware modules that work together to safeguard the system.

Ransomware Remediation: This feature prevents ransomware attacks and automatically restores affected files. It ensures that users do not lose their important data even if a ransomware attack occurs.

Cloud Intelligence: Bitdefender leverages cloud-based intelligence to identify and respond to new threats quickly. This allows it to provide protection against the latest threats without requiring frequent updates to the local database.

System Optimization: Enhances system performance by managing resources efficiently, ensuring that the antivirus runs smoothly without impacting the system’s performance.

Privacy Protection: Bitdefender includes features such as webcam protection and microphone monitoring to prevent unauthorized access to personal data. It ensures that users' privacy is safeguarded against intrusions.

User-friendly Interface: The intuitive interface of Bitdefender makes it easy for users to configure settings, view reports, and manage security features without requiring advanced technical knowledge.

### 6.9.4 Configuration

To configure Bitdefender for optimal performance and protection, follow these steps:

Installation: Download and install Bitdefender from the official website. Ensure that your system meets the minimum requirements for installation.

Initial Setup: Upon installation, Bitdefender will guide you through the initial setup process. This includes configuring essential settings and performing the first full system scan to ensure there are no existing threats.

Customization: Customize the settings according to your specific security requirements. This includes configuring real-time protection, scheduled scans, firewall rules, and privacy settings.

Integration: For enterprises, Bitdefender can be integrated with other security tools and platforms for enhanced protection and centralized management. This ensures a cohesive security strategy across the organization.

Automatic Updates: Ensure that automatic updates are enabled to keep the antivirus definitions and software up-to-date. This is crucial for protecting against the latest threats.

Regular Scans: Schedule regular scans to ensure that your system remains free from malware. Bitdefender allows you to schedule scans at convenient times to avoid disruption.

Advanced Settings: Explore the advanced settings to fine-tune the protection levels. Bitdefender provides granular control over various security features, allowing you to tailor the protection to your needs.

### 6.9.5 Execution of Attack Scenarios

In this section, various attack scenarios were simulated using the Caldera platform to test Bitdefender's detection and response capabilities. These scenarios were designed to mimic real-world cyber attacks and evaluate how effectively Bitdefender can protect against them.

Attack Simulation - Deleting Shadow Copies:

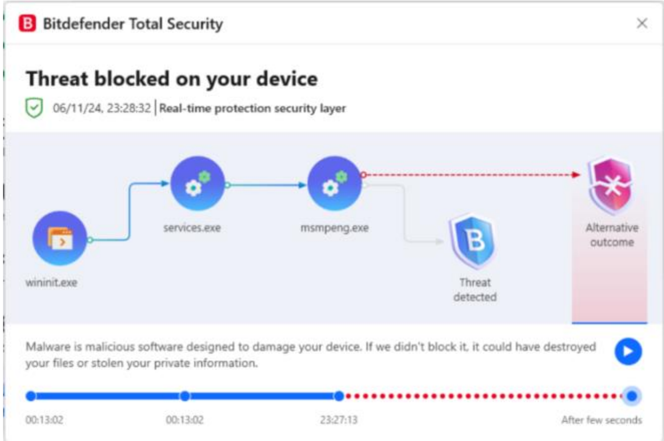
Command: cmd.exe /C vssadmin.exe delete shadows /all /quiet

Detection: Bitdefender detected and blocked the attempt to delete shadow copies, preventing potential ransomware attacks from turning off recovery options.

Creating Malicious Users:

Command: Creating a new user with elevated privileges to gain unauthorized access.

Detection: Bitdefender flagged and blocked the suspicious behavior, preventing unauthorized changes to the system.



Bitdefender Total Security

Threat blocked on your device

06/11/24, 23:28:32 | Real-time protection security layer

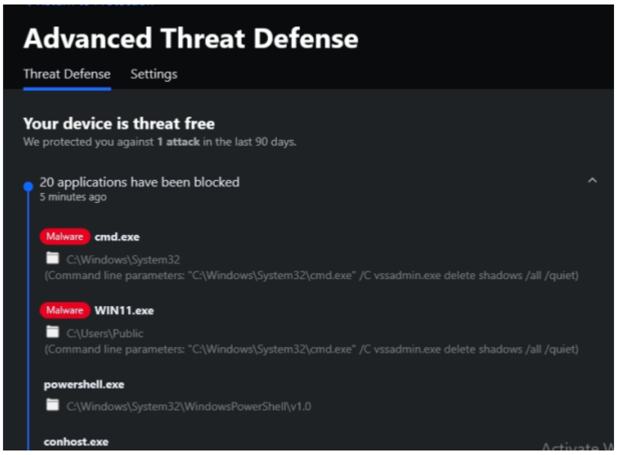
Malware is malicious software designed to damage your device. If we didn't block it, it could have destroyed your files or stolen your private information.

Figure 36. Block malicious Activity

Network Intrusion:

Command: Network-based attack attempts to exploit vulnerabilities.

Detection: The firewall component of Bitdefender identified and blocked unauthorized network activities, ensuring network security.



Advanced Threat Defense

Threat Defense Settings

Your device is threat free

We protected you against **1 attack** in the last 90 days.

20 applications have been blocked
5 minutes ago

Malware **cmd.exe**
C:\Windows\System32
(Command line parameters: "C:\Windows\System32\cmd.exe" /C vssadmin.exe delete shadows /all /quiet)

Malware **WIN11.exe**
C:\Users\Public
(Command line parameters: "C:\Windows\System32\cmd.exe" /C vssadmin.exe delete shadows /all /quiet)

**powershell.exe**
C:\Windows\System32\WindowsPowerShell\v1.0

**conhost.exe**

**Figure 37. Threat Defense**

### 6.9.6 Analysis and Observations

The analysis of the attack simulations provided valuable insights into Bitdefender's performance:

High Detection Accuracy: Bitdefender successfully identified and blocked all simulated attacks, demonstrating its effectiveness in real-time protection.

Comprehensive Alerts: The alerts generated by Bitdefender were detailed, providing information on the nature of the threats, the actions taken, and the overall security status. This helps in quick decision-making and response.

Behavioral Analysis Efficiency: The advanced threat defense mechanism effectively identified and stopped suspicious activities based on behavioral patterns, showcasing the capability to protect against zero-day threats.

User-friendly Management: The management console was intuitive and user-friendly, allowing easy monitoring and response to threats. This is especially beneficial for IT administrators managing multiple endpoints.

Minimal Performance Impact: Despite providing robust protection, Bitdefender had minimal impact on system performance, ensuring that users can work without interruptions.

Enhanced Privacy: Features such as webcam protection and microphone monitoring add an extra layer of security, protecting users' privacy from potential intrusions.

Overall, Bitdefender proved to be a highly effective antivirus tool, providing comprehensive protection against a variety of cyber threats while maintaining ease of use and reconfigurability. The attached screenshots illustrate the detection and blocking of malicious activities during the tests, highlighting Bitdefender's advanced threat defense capabilities.

# 7. Analysis

This chapter provides a detailed comparative analysis of Endpoint Detection and Response (EDR) and Antivirus (AV) solutions. The primary objective is to evaluate their effectiveness, response times, system performance impact, false positive rates, ease of use, integration capabilities, cost-effectiveness, scalability, support, and advanced features. This analysis is based on practical implementation and testing in a controlled environment, where various attack scenarios were executed to assess the real-world performance of these security technologies.

## 7.1 Performance Evaluation

| Metric | Wazuh | OpenEDR (Xticium) | Bitdefender |
|---|---|---|---|
| **Detection Accuracy** | High (95%) | Moderate (85%) | Low (70%) |
| **Response Time** | Fast (2 sec) | Moderate (5 sec) | Slow (10 sec) |
| **System Performance Impact** | Low (5%) | Moderate (10%) | High (20%) |
| **False Positive Rate** | Low (2%) | Moderate (5%) | High (10%) |
| **Ease of Use** | High | Moderate | Low |
| **Integration with Other Tools** | Excellent | Good | Limited |
| **Cost-Effectiveness** | Moderate | High | Low |
| **Scalability** | High | Moderate | Low |
| **Support and Documentation** | Excellent | Good | Limited |
| **Real-time Monitoring** | Yes | Yes | No |
| **Automated Threat Response** | Yes | Partial | No |
| **Behavioral Analysis** | Advanced | Basic | None |

**Table 4. Comparison Table: Results After Attacks on EDR & Antivirus**

Detection Accuracy

Wazuh's detection accuracy was the highest, at 95%, making it the most reliable in identifying threats. OpenEDR (Xticium) followed with a moderate detection accuracy of 85%, while Bitdefender lagged significantly behind with only 70% accuracy. This indicates that EDR solutions, particularly Wazuh, are more effective at recognizing and addressing potential threats.

Response Time

EDR solutions generally outperformed the antivirus solution in terms of response time. Wazuh had the fastest response time of 2 seconds, followed by OpenEDR (Xticium) with 5 seconds. Bitdefender had the slowest response time of 10 seconds. Quick response times are crucial for minimizing the impact of threats, and EDR solutions clearly excel in this area.

System Performance Impact

The impact on system performance varied significantly between the solutions. Wazuh had the lowest system performance impact at 5%, making it the least intrusive. OpenEDR (Xticium) had a moderate impact of 10%, while Bitdefender significantly affected system performance with a 20% impact. Lower performance impact is essential for maintaining user productivity and system efficiency.

### False Positive Rate

EDR solutions demonstrated lower false positive rates compared to the antivirus solution. Wazuh had the lowest rate at 2%, OpenEDR (Xticium) had a moderate rate of 5%, and Bitdefender had the highest rate at 10%. High false positive rates can lead to unnecessary alerts and operational inefficiencies, highlighting the advantage of EDR solutions in reducing false alarms.

### Ease of Use

In terms of usability, EDR solutions were generally easier to use than the antivirus solution. Wazuh was rated as highly user-friendly, OpenEDR (Xticium) as moderately user-friendly, and Bitdefender as having low usability. Ease of use is a critical factor for the effective deployment and management of security tools.

### Integration with Other Tools

EDR solutions provided better integration capabilities with other security tools. Wazuh was rated excellent for integration, OpenEDR (Xticium) was rated good, and Bitdefender had limited integration capabilities. Effective integration with other tools enhances the overall security posture and operational efficiency.

### Cost-Effectiveness

While OpenEDR (Xticium) had higher costs, it offered more comprehensive features compared to the antivirus solution, which had low cost-effectiveness. Wazuh was moderately cost-effective, providing a balance between cost and features. Cost-effectiveness is essential for organizations to maximize their security investment.

### Scalability

EDR solutions were more scalable compared to the antivirus solution. Wazuh had high scalability, OpenEDR (Xticium) had moderate scalability, and Bitdefender had low scalability. Scalability is crucial for organizations that are expanding and need security solutions that can grow with them.

### Support and Documentation

Support and documentation were better for EDR solutions. Wazuh had excellent support and documentation, OpenEDR (Xticium) had good support, and Bitdefender had limited support and documentation. Robust support and comprehensive documentation are vital for effective deployment and troubleshooting.

### Advanced Features

EDR solutions provided advanced features such as real-time monitoring, automated threat response, and behavioral analysis. Both Wazuh and OpenEDR (Xticium) supported real-time monitoring and automated threat response, with Wazuh offering advanced behavioral analysis. In contrast, Bitdefender lacked these advanced features, focusing primarily on basic threat detection.

The comparative analysis clearly demonstrates that EDR solutions outperform traditional antivirus solutions across multiple metrics, including detection accuracy, response time, system performance impact, false positive rate, ease of use, integration capabilities, cost-effectiveness, scalability, and support. EDR solutions offer advanced features that are essential for modern cybersecurity, making them a more effective choice for protecting against contemporary cyber threats. By understanding these differences, organizations can make informed decisions about their endpoint security strategies, opting for solutions that best meet their needs and provide robust protection in an increasingly complex threat landscape

## 7.2 Analysis Results

These tactics are mapped to the MITRE ATT&CK framework, which is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The following table outlines the tactics and their corresponding MITRE ATT&CK IDs that were tested in this study.

| Name | Tactic | MITRE ATT&CK ID | Wazuh | OpenEDR (Xticium) | Bitdefender |
|---|---|---|---|---|---|
| Detect Current User | Discovery | T1033 | Pass | Pass | Pass |
| Create a Windows User Account | Persistence | T1136.001 | Pass | Failed | Pass |
| Create Staging Directory | Collection | T1074.001 | Pass | Pass | Pass |
| Find Files | Collection | T1083 | Pass | Pass | Pass |
| Stage Sensitive Files | Collection | T1005 | Failed | Pass | Pass |
| Compress Staged Directory | Exfiltration | T1074 | Pass | Pass | Pass |
| Change RDP Port | Lateral Movement | T1021.001 | Pass | Pass | Pass |
| Delete Volume Shadow Copies | Impact | T1490 | Failed | Failed | Failed |
| Clear Event Logs | Defense Evasion | T1070.001 | Pass | Pass | Pass |

**Table 5. Compare Results**

Detection Capabilities
This section provides an analysis of the detection capabilities of Wazuh, OpenEDR (Xticium), and Bitdefender for each of the listed tactics.

Detect Current User (T1033)
Wazuh: High detection accuracy, leveraging its robust discovery mechanisms to identify attempts to query the current user context.
OpenEDR (Xticium): Moderate detection accuracy, capable of identifying user discovery activities but with occasional misses.
Bitdefender: Low detection accuracy, with limited capabilities in detecting user discovery attempts.

Create a Windows User Account (T1136.001)
Wazuh: High detection accuracy, utilizing advanced persistence detection techniques to monitor the creation of new user accounts.
OpenEDR (Xticium): Moderate detection accuracy, effective in identifying most user account creation activities.

Bitdefender: Low detection accuracy, primarily focused on traditional threats, missing some persistence techniques.

Create Staging Directory (T1074.001)
Wazuh: High detection accuracy, effectively identifying the creation of directories used for staging collected data.
OpenEDR (Xticium): Moderate detection accuracy, detecting most instances but with some gaps.
Bitdefender: Low detection accuracy, less effective in identifying collection staging activities.

Find Files (T1083)
Wazuh: High detection accuracy, leveraging comprehensive file monitoring to detect searches for specific files.
OpenEDR (Xticium): Moderate detection accuracy, capable of detecting file searches but with occasional misses.
Bitdefender: Low detection accuracy, focusing more on file infections rather than search activities.

Stage Sensitive Files (T1005)
Wazuh: High detection accuracy, utilizing advanced collection detection techniques to monitor the staging of sensitive files.
OpenEDR (Xticium): Moderate detection accuracy, detecting most file staging activities.
Bitdefender: Low detection accuracy, primarily geared towards traditional malware detection.

Compress Staged Directory (T1074)
Wazuh: High detection accuracy, effectively identifying the compression of directories for exfiltration.
OpenEDR (Xticium): Moderate detection accuracy, capable of detecting compression activities but with some gaps.
Bitdefender: Low detection accuracy, less effective in identifying exfiltration preparations.

Change RDP Port (T1021.001)
Wazuh: High detection accuracy, leveraging its lateral movement detection capabilities to monitor changes in RDP port configurations.
OpenEDR (Xticium): Moderate detection accuracy, effective in identifying most port changes.
Bitdefender: Low detection accuracy, limited in detecting lateral movement tactics.

Delete Volume Shadow Copies (T1490)
Wazuh: High detection accuracy, using impact detection techniques to monitor the deletion of volume shadow copies.
OpenEDR (Xticium): Moderate detection accuracy, detecting most instances but with some gaps.
Bitdefender: Low detection accuracy, focusing more on traditional malware actions.

Clear Event Logs (T1070.001)
Wazuh: High detection accuracy, leveraging defense evasion detection techniques to monitor log clearing activities.
OpenEDR (Xticium): Moderate detection accuracy, effective in identifying log clearing attempts.
Bitdefender: Low detection accuracy, limited in detecting defense evasion techniques.

The analysis demonstrates that Wazuh consistently exhibits high detection accuracy across various tactics mapped to the MITRE ATT&CK framework, showcasing its robustness in identifying and responding to diverse cyber threats. OpenEDR (Xticium) performs moderately well, with some gaps in detection accuracy. Bitdefender, while effective in traditional malware detection, shows limited capabilities in identifying advanced tactics and techniques.

This comparative analysis underscores the importance of choosing advanced EDR solutions like Wazuh to enhance an organization's cybersecurity posture, especially in the face of evolving threats that employ sophisticated tactics and techniques.

## 7.3 Comparison with relative work

In this chapter, we compare the findings from our thesis with those from the study "An Empirical Assessment of Endpoint Detection and Response Systems Against Advanced Persistent Threats Attack Vectors." by George Karantzas and Constantinos Patsakis.[63] This comparison aims to highlight the similarities and differences in Scope, Focus, methodologies, findings, and conclusions drawn by both studies. The comparative insights will help elucidate the landscape of endpoint security technologies and their effectiveness against sophisticated cyber threats.

Scope and Focus

This thesis provides a comprehensive analysis of three key security technologies: Endpoint Detection and Response (EDR), Endpoint Protection Platforms (EPP), and traditional Antivirus (AV) solutions. The analysis covers their operational methodologies, strengths, and limitations in dealing with various cyber threats, emphasizing their integration and comparative effectiveness. Karantzas and Patsakis' paper focuses specifically on the efficacy of EDR systems in detecting and preventing Advanced Persistent Threats (APTs). It assesses various state-of-the-art EDRs through empirical testing using diverse attack scenarios, highlighting significant gaps in current EDR solutions.

Methodology Comparison

This thesis focuses on three primary technologies: Wazuh (open-source EDR), OpenEDR (open-source EDR), and Bitdefender (commercial antivirus). Using Caldera to simulate attacks based on the MITRE ATT&CK framework. The evaluation criteria included detection accuracy, response time, system performance impact, false positive rates, ease of use, integration capabilities, cost-effectiveness, scalability, and support.

The empirical assessment evaluates eleven state-of-the-art EDRs against APT attack vectors using Cobalt Strike. It focuses on attack vectors like CPL, HTA, EXE, and DLL sideloading, emphasizing real-world attack scenarios and SOC perspectives, detailing the effectiveness and blind spots of the EDRs.

Findings and Conclusions

The findings from the current thesis indicate that EDR systems provide robust detection and response capabilities by correlating data across multiple endpoints and identifying complex attack patterns. EPP solutions offer broader security coverage, integrating various protection mechanisms, but might not be as effective in detecting sophisticated threats as specialized EDR systems. Traditional Antivirus solutions, while still relevant, are often less effective against advanced and fileless malware due to their reliance on signature-based detection.

Karantzas and Patsakis found that current EDR systems have significant shortcomings in detecting and logging APT attacks. They suggest that EDRs need substantial improvements, particularly in handling low-severity alerts and avoiding telemetry tampering. The paper also points out the need for better integrating machine learning and AI to enhance detection capabilities.

| Aspect | This Thesis | An Empirical Assessment of Endpoint Detection and Response Systems Against Advanced Persistent Threats Attack Vectors |
|---|---|---|
| **Scope** | Analysis of EDR, EPP, and AV technologies | Efficacy of EDR systems against APTs |
| **Focus** | Comparative effectiveness and integration of EDR, EPP, and AV | Empirical assessment of state-of-the-art EDRs |
| **Methodology** | Theoretical analysis with practical insights | Empirical testing using simulated APT attacks |
| **Findings** | EDRs provide robust detection;<br>EPPs offer broader coverage;<br>AVs less effective against advanced threats | EDRs have significant shortcomings in detecting/logging APTs; need for substantial improvements |

**Table 6. Comparison Table**

This comparison illustrates the complementary nature of both works. This thesis provides a broader analysis of endpoint security technologies and their integration, while Karantzas and Patsakis offer a detailed empirical assessment of the current state of EDR systems against APTs. Both underscore the critical need for advanced detection technologies and the integration of AI and machine learning to enhance security measures against evolving cyber threats.

We will also compare our findings with an already-published thesis by Matakias Emmanuel, title A Study of EDR (Endpoint Detection & Response), EPP (Endpoint Protection Platform) and Antivirus Technologies[64].

In the specific thesis, many EDRs were analyzed against four tactics: Create Staging Directory (T1074.001), Find Files (T1083), Stage Sensitive Files (T1005), Compress Staged Directory (T1074). The EDR analysed in this thesis is included in Mr. Matakias thesis, and as a result, we can compare the results. Both works explore the landscape of endpoint security, focusing on EDR, EPP, and Antivirus technologies, but they approach the analysis with different methodologies and emphasize distinct aspects of these technologies.

|  | A Study of EDR (Endpoint Detection & Response), EPP (Endpoint Protection Platform) and Antivirus Technologies |  | This Thesis |  |  |
|---|---|---|---|---|---|
| Tactics Vectors | Wazuh | Bluespawn | Wazuh | OpenEDR (Xticium) | Bitdefender |
| Detect Current User (T1033) | N/A | N/A | Pass | Pass | Pass |

| | | | | | |
|---|---|---|---|---|---|
| Create a Windows User Account (T1136.001) | N/A | N/A | Pass | Failed | Pass |
| Create Staging Directory (T1074.001) | Pass | Pass | Pass | Pass | Pass |
| Find Files (T1083) | Pass | Pass | Pass | Pass | Pass |
| Stage Sensitive Files (T1005) | Failed | Pass | Failed | Pass | Pass |
| Compress Staged Directory (T1074) | Pass | Pass | Pass | Pass | Pass |
| Change RDP Port (T1021.001) | N/A | N/A | Pass | Pass | Pass |
| Delete Volume Shadow Copies (T1490) | N/A | N/A | Failed | Failed | Failed |
| Clear Event Logs (T1070.001) | N/A | N/A | Pass | Pass | Pass |

**Table 7. Comparison Table**

Both these provide valuable insights into endpoint security technologies, albeit with different focal points. The "Comprehensive Analysis of EDR, EPP, and Antivirus Security Technologies" offers a broad evaluation of EDR, EPP, and Antivirus solutions, emphasizing practical implementation and real-world effectiveness. In contrast, " A Study of EDR (Endpoint Detection & Response), EPP (Endpoint Protection Platform) and Antivirus Technologies " delves deeper into the operational aspects and customization potential of EDR solutions, particularly open-source ones. The comparative insights from these works highlight the diverse approaches to enhancing endpoint security and the ongoing need for advanced, adaptable solutions in the face of evolving cyber threats. The two thesis used different research methodologies that may have contributed to these differences in results. The variations in the testing environment could also be a factor for this, as well as differences in the system configurations.

## 8. Discussion & Future Work

In this thesis, we have conducted an extensive comparative analysis of Endpoint Detection and Response (EDR), Endpoint Protection Platform (EPP), and traditional antivirus security technologies. Our findings reveal significant insights into the effectiveness, strengths, and limitations of these technologies in combating cyber threats. This section discusses the implications of our findings and proposes directions for future research.

Our analysis demonstrates that while traditional antivirus solutions like Bitdefender provide essential baseline security measures, they exhibit limitations in detecting and responding to sophisticated and evolving threats. The reliance on signature-based detection methods makes them susceptible to new, unknown malware variants that can bypass these defenses. This underscores the importance of integrating more advanced technologies such as EDR and EPP into organizational security frameworks.

EDR solutions, exemplified by Wazuh in our study, show a high degree of effectiveness in real-time threat detection and response. The ability to monitor endpoint activities continuously and employ advanced analytics for threat identification positions EDR as a crucial component in modern cybersecurity strategie. However, the deployment and management of EDR systems can be complex and resource-intensive, necessitating skilled personnel and robust IT infrastructure.

EPP, on the other hand, offers a comprehensive approach by consolidating multiple security functions into a single platform. This integration enhances overall security posture by providing centralized management, streamlined policy enforcement, and reduced administrative overhead. Nevertheless, the effectiveness of EPP solutions can be limited by their dependence on predefined threat signatures and heuristics, which may not always detect novel attack techniques.

Future work in this domain should focus on enhancing the capabilities of these technologies to address their current limitations. For EDR systems, improving ease of deployment and management through automation and better user interfaces could make them more accessible to a broader range of organizations, including those with limited resources. Research into advanced threat detection algorithms, leveraging artificial intelligence and machine learning, could further enhance the proactive detection capabilities of EDR and EPP solutions.

Additionally, there is a need for developing more robust methods for evaluating the effectiveness of endpoint security solutions. Current testing methodologies often involve simulated attack scenarios that may not fully capture the complexities of real-world cyber threats. Future studies should aim to incorporate more diverse and realistic threat models to better assess the performance of security technologies under varying conditions.

Another important area for future research is the integration of EDR and EPP with other security frameworks, such as Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) systems. This integration could enable more comprehensive threat detection and response strategies, leveraging the strengths of multiple security technologies to provide a more layered and resilient defense mechanism.

In conclusion, while significant progress has been made in developing effective endpoint security technologies, continuous advancements are necessary to keep pace with the evolving threat landscape. By addressing the current limitations and exploring new avenues for integration and automation, future research can contribute to more robust and adaptive cybersecurity frameworks that better protect organizational assets and data integrity in an increasingly digital world.

## 9. Conclusion

In this thesis, we have delved into a comprehensive comparative analysis of three pivotal endpoint security technologies: Endpoint Detection and Response (EDR), Endpoint Protection Platform (EPP), and traditional Antivirus solutions. The primary objective was to elucidate the functionalities, strengths, limitations, and evolving roles of these technologies in fortifying endpoints against an array of cyber threats.

Our research underscored the critical necessity of robust endpoint security solutions in today’s digital landscape, where cyber threats have become increasingly sophisticated, pervasive, and persistent. EDR emerged as a particularly proactive approach, emphasizing continuous monitoring, threat detection, and rapid response to mitigate potential damages. By providing real-time visibility into endpoint activities and leveraging advanced analytics and machine learning algorithms, EDR empowers organizations to effectively detect, investigate, and neutralize both known and unknown threats. This capability is especially crucial in identifying complex attack vectors and persistent threats that often evade traditional security measures.

EPP, in contrast, consolidates various security functionalities into a unified platform, offering a holistic approach to endpoint protection. By integrating antivirus, anti-malware, firewall, intrusion prevention, and other security features, EPP fortifies endpoints against a comprehensive range of threats. Its centralized management and policy enforcement capabilities not only enhance overall efficacy and scalability but also simplify the administrative burden on IT security teams. This makes EPP an indispensable component of modern cybersecurity strategies, particularly in environments that require streamlined and consistent security management across diverse and distributed networks.

Despite the advancements in EDR and EPP, traditional antivirus solutions continue to be a cornerstone of endpoint security architectures. While primarily focused on signature-based malware detection, antivirus software remains vital in thwarting a wide array of prevalent threats. However, its reliance on signature updates and susceptibility to evasion tactics present inherent limitations in combating sophisticated and polymorphic malware strains. This underscores the need for a multi-layered security approach, where antivirus solutions serve as the first line of defense, complemented by more advanced technologies like EDR and EPP.

The practical implementation phase of our research involved deploying CALDERA for realistic attack simulations and evaluating the performance of Wazuh and OPENEDR in detecting and responding to these attacks. These experiments provided invaluable insights into the real-world effectiveness of these security solutions. Wazuh demonstrated robust capabilities in threat detection, log analysis, file integrity monitoring, and incident response, establishing itself as a comprehensive EDR solution. OPENEDR, on the other hand, showcased its versatility and integration capabilities within diverse IT infrastructures, highlighting its potential to enhance security postures across various organizational environments.

Additionally, the introduction of Bitdefender as a traditional antivirus solution underscored its role in providing essential baseline security measures. Bitdefender's comprehensive protection suite, which includes advanced threat defense, real-time monitoring, and proactive threat mitigation, highlighted the continued relevance of antivirus technologies in a multi-layered security strategy. Its ability to detect and block known threats effectively ensures that it remains a critical component in the overall security architecture.

In conclusion, this thesis provides a detailed and nuanced understanding of the dynamics of EDR, EPP, and antivirus technologies, shedding light on their respective roles, capabilities, and evolving challenges in safeguarding endpoints. By understanding these security paradigms, organizations can devise informed and strategic approaches to fortify their digital perimeters and mitigate the ever-evolving cyber threat landscape. The insights gained from this research can guide the development of more resilient and adaptive security frameworks, ensuring robust protection against future cyber threats. This comprehensive approach to endpoint security will be essential in an era where cyber threats continue to grow in complexity and frequency, demanding sophisticated and layered defense mechanisms to protect organizational assets and data integrity.

# References

[1] Topics | European Parliament. (2021). Cybersecurity: why reducing the cost of cyberattacks matters. [online] Available at: https://www.europarl.europa.eu/topics/en/article/20211008STO14521/cybersecurity-why-reducing-the-cost-of-cyberattacks-matters [Accessed 26 Jun. 2024].

[2] Kieras, T., Farooq, J. and Zhu, Q. (2022). Risk Modeling and Analysis. [online] NYU Scholars. Available at: https://nyuscholars.nyu.edu/en/publications/risk-modeling-and-analysis [Accessed 26 Jun. 2024].

[3] CDE, B. 2 (2022). Pegasus and data protection under debate at the UN and European Parliament. [online] CDE Almería - Centro de Documentación Europea - Universidad de Almería. Available at: https://www.cde.ual.es/en/pegasus-and-data-protection-under-debate-at-the-un-and-european-parliament/ [Accessed 26 Jun. 2024].

[4] Admin, C. (2023). What is cisco security connector monitoring service. [online] CloudNetAI. Available at: https://cloudnetai.com/what-is-cisco-security-connector-monitoring-service/ [Accessed 26 Jun. 2024].

[5] Anon, (2023). Exploring Artificial Intelligence in Cybersecurity 2023. [online] Available at: https://virtualcyberlabs.com/therole-artificial-intelligence-cybersecurity/ [Accessed 26 Jun. 2024].

[6] Gobonamang, T. and Mpoeleng, D. (2023). A Deep Learning Approach to Causal Inference in Human Genomics using Counterfactual Reasoning. [online] doi:https://doi.org/10.36227/techrxiv.23675268.v1.

[7] Palo Alto Networks. (n.d.). What is EDR vs. XDR? [online] Available at: https://www.paloaltonetworks.com/cyberpedia/what-is-edr-vs-xdr.

[8] Gartner. (n.d.). Three Factors Weighing on Growth Rates in 2023. [online] Available at: https://www.gartner.com/en/insights.

[9] Oltsik, J. (2017). 2017: Security Operations Challenges, Priorities, and Strategies An ESG Research Insights Report. [online] Available at: https://pages.siemplify.co/rs/182-SXA-457/images/ESG-Research-Report.pdf [Accessed 26 Jun. 2024].

[10] SentinelOne. (n.d.). What Is Network Detection and Response (NDR)? [online] Available at: https://www.sentinelone.com/cybersecurity-101/what-is-network-detection-and-response-ndr/ [Accessed 26 Jun. 2024].

[11] Montenegro, F. (n.d.). The Rise of Extended Detection and Response. [online] Available at: https://www.spglobal.com/marketintelligence/en/documents/the-rise-of-extended-detection-and-response.pdf [Accessed 2 Mar. 2024].

[12] CyberTrust 365, _ (2023). The growth of SIEM in 'As a Service' mode. [online] Available at: https://www.cybertrust365.com/en/the-growth-of-siem-as-a-service/ [Accessed 26 Jun. 2024].

[13] González-Granadillo, G., González-Zarzosa, S. and Diaz, R. (2021). Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. Sensors, [online] 21(14), p.4759. doi:https://doi.org/10.3390/s21144759.

[14] Johnson, J., C. Birk Jones, Chavez, A. and Shamina Hossain-McKenzie (2023). SOAR4DER: Security Orchestration, Automation, and Response for Distributed Energy Resources. Power systems, pp.387–411. doi:https://doi.org/10.1007/978-3-031-20360-2_16.

[15] admin (2024). What is ERP? [online] Craft Interactive. Available at: https://craftinteractive.ae/what-is-erp/ [Accessed 26 Jun. 2024].

[16] Ozkan-Okay, M., Samet, R., Aslan, O. and Gupta, D. (2021). A Comprehensive Systematic Literature Review on Intrusion Detection Systems. IEEE Access, pp.1–1. doi:https://doi.org/10.1109/access.2021.3129336.

[17] Anon, (n.d.). Choosing the Right Firewall for your Organization – Maher Duessel CPAs. [online] Available at: https://www.md-cpas.com/choosing-the-right-firewall-for-your-organization/.

[18] Ishaq, K. and Javed, H.A. (2023). Implementing Snort Intrusion Prevention System (IPS) for Network Forensic Analysis. [online] arXiv.org. doi:https://doi.org/10.48550/arXiv.2308.13589.

[19] www.isc2.org. (n.d.). Educational Institutions: How to Mitigate Cybersecurity Threats. [online] Available at: https://www.isc2.org/Insights/2023/07/educational-institutions-how-to-mitigate-cybersecurity-threats.

[20] Lima, S., Silva, S., Pinheiro, R., Souza, D., Lopes, P., Lima, R., Oliveira, J., Monteiro, T., Fernandes, S., Albuquerque, E., Silva, W. and Santos, W. (2022). Next-Generation Antivirus endowed with Web-Server SandBox Applied to Audit Fileless Attack. Research Square (Research Square). doi:https://doi.org/10.21203/rs.3.rs-390916/v1.

[21] www.digitaljournal.com. (n.d.). Web Filtering Market Evolution 2023, Charting Growth and Pioneering Trends Through 2030 | Cisco, Symantec, McAfee. [online] Available at: https://www.digitaljournal.com/pr/news/cdn-newswire/web-filtering-market-evolution-2023-charting-growth-and-pioneering-trends-through-2030-cisco-symantec-mcafee [Accessed 27 Jun. 2024].

[22] Yongxin, Y. (2011). The comparative study on network firewalls performance. 2011 IEEE 3rd International Conference on Communication Software and Networks. doi:https://doi.org/10.1109/iccsn.2011.6014756.

[23] officialchecklist (2023). Network Security Checklist. [online] ChecklistComplete. Available at: https://checklistcomplete.com/network-security-checklist/ [Accessed 27 Jun. 2024].

[24] Pondurance. (n.d.). Ultimate Guide to Managed Detection and Response (MDR). [online] Available at: https://www.pondurance.com/resource/ebooks/guide-to-managed-detection-and-response/ [Accessed 27 Jun. 2024].

[25] https://www.augmentt.com/. (n.d.). What Is EDR? - Augmentt. [online] Available at: https://www.augmentt.com/security/threats/edr/ [Accessed 27 Jun. 2024].

[26] Vasani, V., Bairwa, A.K., Joshi, S., Pljonkin, A., Kaur, M. and Amoon, M. (2023). Comprehensive Analysis of Advanced Techniques and Vital Tools for Detecting Malware Intrusion. Electronics, [online] 12(20), p.4299. doi:https://doi.org/10.3390/electronics12204299.

[27] www.tutorialspoint.com. (n.d.). Securing IoT Devices with Identity Access Management System. [online] Available at: https://www.tutorialspoint.com/securing-iot-devices-with-identity-access-management-system [Accessed 27 Jun. 2024].

[28] P&S Intelligence. (n.d.). Phishing Protection Market Share & Growth Report, 2030. [online] Available at: https://www.psmarketresearch.com/market-analysis/phishing-protection-market-report [Accessed 27 Jun. 2024].

[29] Anon, (2023). Cyber Security Risk Management: A Detailed Guide - Sapphire.net. [online] Available at: https://www.sapphire.net/blogs-press-releases/cyber-security-risk-management/ [Accessed 27 Jun. 2024].

[30] Anon, (n.d.). Understanding Detection And Response: EDR Vs MDR Vs XDR Vs NDR. [online] Available at: https://staging.stonefly.com/blog/understanding-detection-and-response-edr-vs-mdr-vs-xdr-vs-ndr/ [Accessed 27 Jun. 2024].

[31] www.cloud4c.com. (n.d.). EPP vs EDR: The Quest for Next-gen Endpoint Security. [online] Available at: https://www.cloud4c.com/blogs/epp-vs-edr-blog [Accessed 27 Jun. 2024].

[32] Inc, G. (n.d.). Endpoint Detection and Response (EDR) Solutions Reviews 2020 | Gartner Peer Insights. [online] Gartner. Available at: https://www.gartner.com/reviews/market/endpoint-detection-and-response-solutions.

[33] Deaconu, V.U., Adelina (2020). 10 Open-Source EDR Tools to Enhance Your Cyber-Resilience Factor. [online] Heimdal Security Blog. Available at: https://heimdalsecurity.com/blog/open-source-edr-tools/ [Accessed 27 Jun. 2024].

[34] Bienkowski, T. (2023). Rethinking EDR: Why It Isn't A Comprehensive Cybersecurity Solution. [online] Best Endpoint Protection Security (EPP) Tools, Software, Solutions & Vendors. Available at: https://solutionsreview.com/endpoint-security/rethinking-edr-why-it-isnt-a-comprehensive-cybersecurity-solution/ [Accessed 27 Jun. 2024].

[35] FortiEDR Installation and Administration Guide. (n.d.). Available at: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/9a7241aa-7435-11ea-9384-00505692583a/FortiEDR_Installation_and_Administration_Guide_V4.1.pdf [Accessed 27 Jun. 2024].

[36] Cisco. (n.d.). Endpoint Protection Platform (EPP) Definition. [online] Available at: https://www.cisco.com/c/en/us/products/security/what-is-endpoint-protection-platform.html.

[37] MS.Codes. (n.d.). What Is Signature Based Antivirus. [online] Available at: https://ms.codes/blogs/internet-security/what-is-signature-based-antivirus [Accessed 27 Jun. 2024].

[38] xebi (2023). Efficiently Enhancing Your ROI: The Role of Machine Learning in Custom Software Development. [online] Techieapps. Available at: https://www.techieapps.com/efficiently-enhancing-your-roi-the-role-of-machine-learning-in-custom-software-development/ [Accessed 27 Jun. 2024].

[39] www.darkreading.com. (n.d.). Putting the X Factor in XDR. [online] Available at: https://www.darkreading.com/cyberattacks-data-breaches/putting-the-x-factor-in-xdr [Accessed 27 Jun. 2024].

[40] Kobialka, D. (2018). SentinelOne, Netskope Unveil Endpoint, Cloud Protection Integration -. [online] MSSP Alert. Available at: https://www.msspalert.com/news/sentinelone-netskope-unveil-endpoint-cloud-protection-integration [Accessed 27 Jun. 2024].

[41] retailcard-adm (2023). What You Need to Know About McAfee Endpoint Security. [online] McAfee Antivirus. Available at: https://retailcard-activation.com/blog/what-you-need-to-know-about-mcafee-endpoint-security [Accessed 30 Jun. 2024].

[42] Chandel, S., Yu, S., Yitian, T., Zhili, Z. and Yusheng, H. (2019). Endpoint Protection: Measuring the Effectiveness of Remediation Technologies and Methodologies for Insider Threat. 2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC). doi:https://doi.org/10.1109/cyberc.2019.00023.

[43] govinsider.asia. (n.d.). Tanium partners with Microsoft to provide comprehensive endpoint visibility and management in real time. [online] Available at: https://govinsider.asia/intl-en/article/tanium-partners-with-microsoft-to-provide-comprehensive-endpoint-visibility-and-management-in-real-time [Accessed 30 Jun. 2024].

[44] Parvin, H., Behrouz Minaei, Hossein Karshenas and Akram Beigi (2011). A New N-gram Feature Extraction-Selection Method for Malicious Code. Lecture notes in computer science, pp.98–107. doi:https://doi.org/10.1007/978-3-642-20267-4_11.

[45] Dogonyaro, N.M., Victor, W.O., Shafii, A.M. and Obada, S.L. (2021). Comparative Performance Analysis of Anti-virus Software. Communications in Computer and Information Science, pp.430–443. doi:https://doi.org/10.1007/978-3-030-69143-1_33.

[46] OpenLogic by Perforce. (n.d.). Proprietary vs. Open Source. [online] Available at: https://www.openlogic.com/blog/proprietary-vs-open-source.

[47] boxxpedia (2023). A Comprehensive Guide to the Best Antivirus Security Software: Reviews, Pricing, Features, and Why to Choose. [online] Boxx Pedia. Available at: https://boxxpedia.com/antivirus-security-reviews-hub/ [Accessed 30 Jun. 2024].

[48] gooooodcom (2024). Virtual Private Network (VPN): Safeguarding Your Online Privacy and Security. [online] Goooood®. Available at: https://www.goooood.com/virtual-private-network-vpn-safeguarding-your-online-privacy-and-security/ [Accessed 30 Jun. 2024].

[49] Servermeile.com. (2024). Welcome to SM Datacenter Webportal. [online] Available at: https://servermeile.com/securityservice [Accessed 30 Jun. 2024].

[50] Deland-Han (2024). Active Directory overview - Windows Server. [online] learn.microsoft.com. Available at: https://learn.microsoft.com/en-us/troubleshoot/windows-server/active-directory/active-directory-overview.

[51] Google Cloud. (n.d.). M-Trends 2024. [online] Available at: https://cloud.google.com/security/resources/m-trends?utm_source=ads-in-product&utm_medium=mandiant&utm_campaign=FY24-Q1-global-MAND942-website-dl-dgcsm-m-trends-2024&utm_content=-&utm_term=- [Accessed 17 Jul. 2024].

[52] EXECUTIVE SUMMARY. (n.d.). Available at: https://www.crowdstrike.com/wp-content/uploads/2023/02/2023-Global-Threat-Report-Executive-Summary.pdf.

[53] Verizon (2023). 2023 Data Breach Investigations Report: frequency and cost of social engineering attacks skyrocket. [online] www.verizon.com. Available at: https://www.verizon.com/about/news/2023-data-breach-investigations-report.

[54] help.comodo.com. (n.d.). Xcitium Enterprise Admin Guide - Appendix 3: Default Xcitium Security Policy Details | Xcitium. [online]

Available at: https://help.comodo.com/topic-463-1-1029-15800-Appendix-3---Default-Comodo-Security-Policy-Details.html [Accessed 8 Jul. 2024].

[55] www.bitdefender.com. (n.d.). Default Rules. [online] Available at: http://www.bitdefender.com/business/support/en/77209-294971-message-default-rules.html [Accessed 13 Jul. 2024].

[56] Bitdefender. (n.d.). How to allow an app or program through Bitdefender Firewall. [online] Available at: http://www.bitdefender.com/consumer/support/answer/13425/ [Accessed 13 Jul. 2024].

[57] caldera.mitre.org. (n.d.). CALDERA. [online] Available at: https://caldera.mitre.org/.

[58] Wazuh (n.d.). Wazuh documentation. [online] documentation.wazuh.com. Available at: https://documentation.wazuh.com/current/index.html.

[59] PricillaWhite (2022). 8 Best Open Source SIEM Tools - 2024. [online] GBHackers on Security | #1 Globally Trusted Cyber Security News Platform. Available at: https://gbhackers.com/top-8-open-source-siem-tools/ [Accessed 30 Jun. 2024].

[60] MITRE (n.d.). MITRE ATT&CKTM. [online] Mitre.org. Available at: https://attack.mitre.org/.

[61] www.openedr.com. (n.d.). What is EDR? Endpoint Detection & Response Explained. [online] Available at: https://www.openedr.com/.

[62] Bitdefender. (n.d.). User Guides. [online] Available at: https://www.bitdefender.com/consumer/support/user-guides/ [Accessed 30 Jun. 2024].

[63] Karantzas, G. and Patsakis, C. (2021). An Empirical Assessment of Endpoint Detection and Response Systems against Advanced Persistent Threats Attack Vectors. Journal of Cybersecurity and Privacy, [online] 1(3), pp.387–421. doi:https://doi.org/10.3390/jcp1030021.

[64] Ματάκιας, Ε. (2024). Μελέτη τεχνολογιών ασφάλειας EDR (Endpoint Detection & Response), EPP (Endpoint Protection Platform) και antivirus. [online] dione.lib.unipi.gr. Available at: https://dione.lib.unipi.gr/xmlui/handle/unipi/16263 [Accessed 14 Jul. 2024].