UNIVERSITY OF PIRAEUS

DEPARTMENT OF DIGITAL SYSTEMS

Postgraduate Program

«Digital Systems Security»

Master's Thesis

Threat Intelligence Platforms Evaluation

Filippos Papaioannou

MTE1824, Filippos.papaioannou@ssl-unipi.gr

Under the supervision of:

Dr. Christoforos Dadoyan, dadoyan@unipi.gr

Piraeus, February 2021

ABSTRACT

This thesis focuses in the evaluation of Threat Intelligence Platforms (TIPs). TIPs are security tools that use global security data to help proactively identify, mitigate and remediate security threats. New and continually evolving sophisticated threats are surfacing every day making the processes of detection and mitigation far more complicated than some years ago. So it's obvious that the need for more and more intelligent security tools has become imperative. Thus, organizations were encouraged to change their traditional defence models and to use and to develop new systems with a proactive approach. Such changes are necessary because the old approaches are not effective anymore to detect advanced attacks. Also, the organizations are encouraged to develop the ability to respond to incidents in real-time using complex threat intelligence platforms.

This thesis is separated in three big sections. In the beginning we are going to discuss what threat intelligence is and how it is used by researchers and organisations. Subsequently a concise analysis and description of four open source and widespread TIPs will be presented. The platforms I chose are: MISP (**Malware Information Sharing Platform**), OpenCTI (**Open Cyber Threat Intelligence Platform),** CIF (**Collective Intelligence Framework)** and CRITs (**Collaborative Reasearch Into Threats)**. Finally, at the last section I will present the evaluation of these platforms according to specific criteria along with some key findings and limitations that extracted from the analysis.

ΠΕΡΙΕΧΟΜΕΝΑ

1 Εισαγωγή

1.1 Cyber Threat Intelligence

Τα τελευταία χρόνια, ο τομέας του Cyber Threat Intelligence θεωρείται πολύ σημαντικός για την αντιμετώπιση των κινδύνων ασφαλείας των οργανισμών. Το Cyber Threat Intelligence έχει τις ρίζες του στη διαχείριση συμβάντων και στη συμβατική νοημοσύνη. Το παρακάτω είναι μια ενδεικτική περιγραφή για τον ορισμό του CIT που μπορούμε να βρούμε στο Διαδίκτυο:

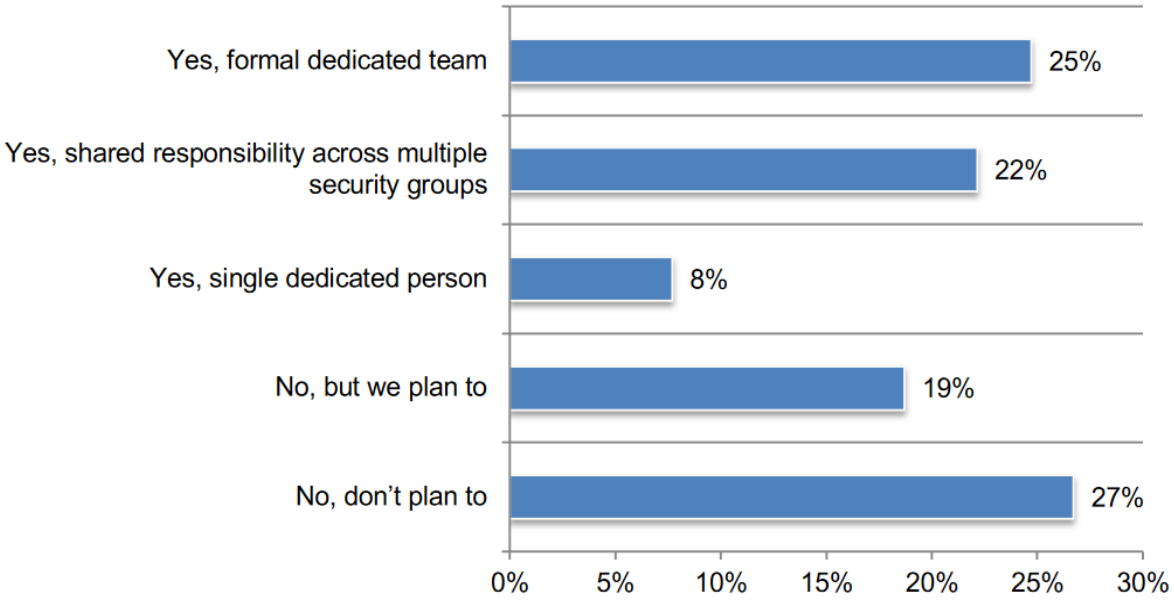
«Cyber threat intelligence is information about threats and threat actors that helps mitigate harmful events in cyberspace. Cyber threat intelligence sources include open source intelligence, social media intelligence, human Intelligence, technical intelligence or intelligence from the deep and dark web».

Είναι δηλαδή όλες εκείνες οι πληροφορίες σχετικά με τις διάφορες απειλές και τους παράγοντες που απειλούν να βλάψουν μια οντότητα, οι οποίες βοηθάνε στην άμβλυνση επιβλαβών γεγονότων στον κυβερνοχώρο

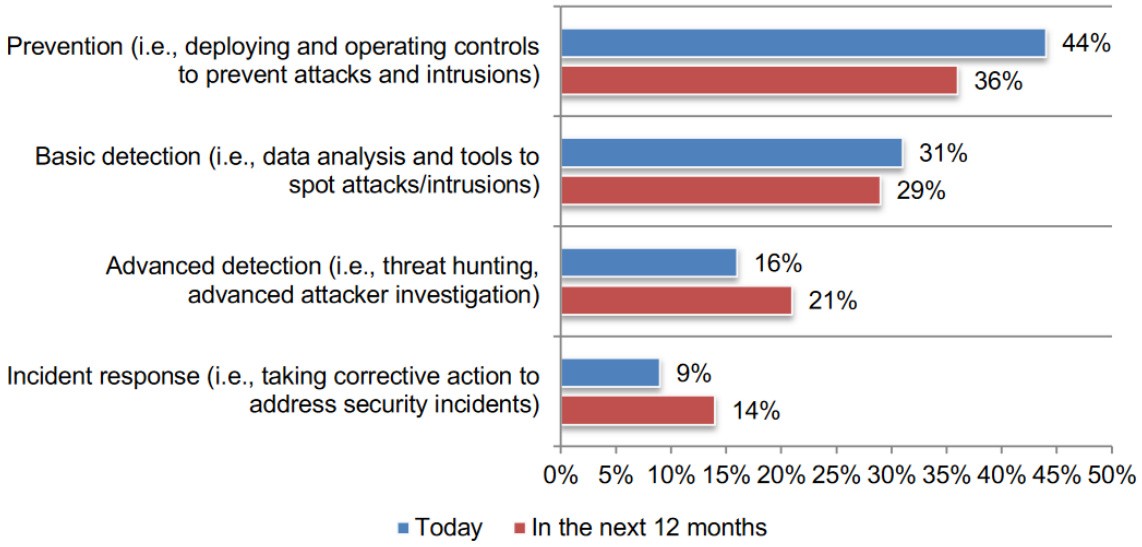
Σύμφωνα με μια έκθεση έρευνας του Ινστιτούτου Ponemon το 2019, οι περισσότεροι οργανισμοί ισχυρίζονται ότι διαθέτουν πόρους αφιερωμένους στην ανίχνευση απειλών. Σύμφωνα με το Σχήμα 1, το 25 τοις εκατό των ερωτηθέντων δηλώνουν ότι έχουν μια επίσημη ειδική ομάδα, το 22 τοις εκατό ότι έχουν επωμιστεί την ευθύνη πολλές ομάδες ασφαλείας του οργανισμού και τέλος 8 τοις εκατό ότι έχουν ένα μόνο άτομο που είναι αφιερωμένο στην ανίχνευση απειλών.

Ωστόσο, το 27% των ερωτηθέντων δηλώνουν ότι οι οργανισμοί τους δεν σχεδιάζουν να διαθέσουν τους πόρους τους στον εντοπισμό απειλών. Σύμφωνα με το Σχήμα 2 μπορούμε να δούμε πώς οι οργανισμοί κατανέμουν τον προϋπολογισμό τους σήμερα και πώς σκοπεύουν να τον διαθέσουν στο άμεσο διάσημα σχετικά με την ασφάλεια στον κυβερνοχώρο.

Σχήμα 1. Διαθέτει ο οργανισμός σας πόρους ειδικά για την ανίχνευση απειλών;



Σχήμα 2. Πως διανέμετε το budget του οργανισμού σας τώρα και πως στο άμεσο μέλλον;



Ο όρος νοημοσύνη έχει πολλούς διαφορετικούς ορισμούς. Αυτό μπορεί να εξηγηθεί από το γεγονότος ότι η νοημοσύνη είναι μια έννοια που εξαρτάται σε μεγάλο βαθμό από το πλαίσιο στο οποίο εισάγεται. Ένας γενικευμένος ορισμός περιγράφει τη νοημοσύνη ως τη διαδικασία μετατροπής θεμάτων από ένα εντελώς άγνωστο στάδιο μέχρι να φτάσει σε μια κατάσταση πλήρους κατανόησης. Προκειμένου να επιτευχθεί αυτός ο στόχος, τα τυχαία και γενικά δεδομένα πρέπει να φιλτραριστούν ώστε να καταλήξουν σ'ένα πιο σχετικό σύνολο δεδομένων με βάση ένα σχεδιαζόμενο πλαίσιο, τα οποία δεδομένα στη συνέχεια υποβάλλονται σε επεξεργασία και μετατρέπονται σε πληροφορίες.

Υπό αυτήν την έννοια, οι πληροφορίες, όταν αναλύονται και προσαρμόζονται σ' ένα context, γίνονται νοημοσύνη. Λαμβάνοντας υπόψη αυτές τις υποθέσεις, μια γενική διαδικασία παραγωγής πληροφοριών αποτελείται συνήθως από τρία κύρια στάδια:

- Συλλογή δεδομένων,
- Επεξεργασία των δεδομένων για μετατροπή σε πληροφορίες και
- Ανάλυση των πληροφοριών για την παραγωγή πληροφοριών.

Ακολουθώντας αυτό το μονοπάτι, η νοημοσύνη για τις απειλές(threat intelligence) θα πρέπει να ικανοποιεί αυτά τα χαρακτηριστικά για να παρέχει βοήθεια στην ανάπτυξη αποτελεσματικών μηχανισμών για την αντιμετώπιση απειλών, που συνήθως ορίζονται ως ένας τύπος ευέλικτης ευφυΐας. Επομένως, εκτός από τη ροή παραγωγής γενικής νοημοσύνης που προαναφέρθηκε, τα στάδια ανάπτυξης και διάδοσης της νοημοσύνης θεωρούνται επίσης απαραίτητα για τη διαδικασία δημιουργίας πληροφοριών απειλής. Έτσι, στο πλαίσιο αυτό η ροή του Cyber Threat Intelligence αποτελείται από πέντε κύρια στάδια, όπως παρουσιάζεται στο παρακάτω σχήμα(Threat Intelligence Production Process Flow):

1. Συλλογή: Το στάδιο αυτό αναφέρεται στη συλλογή δεδομένων
2. Επεξεργασία: Ο συνδυασμός των δεδομένων με σκοπό την απάντηση συγκεκριμένων ερωτήσεων και την παροχή πληροφοριών.
3. Ανάλυση: Η αξιολόγηση των δεδομένων και των πληροφοριών καθώς και η αποκάλυψη προτύπων και η παραγωγή ενεργητικής νοημοσύνης. Με την παραγόμενη νοημοσύνη, είναι δυνατόν να:
    - Να χρησιμοποιηθεί ώστε να ληφθούν οι σωστές αποφάσεις
    - Να διαδοθεί στα ενδιαφερόμενα μέρη

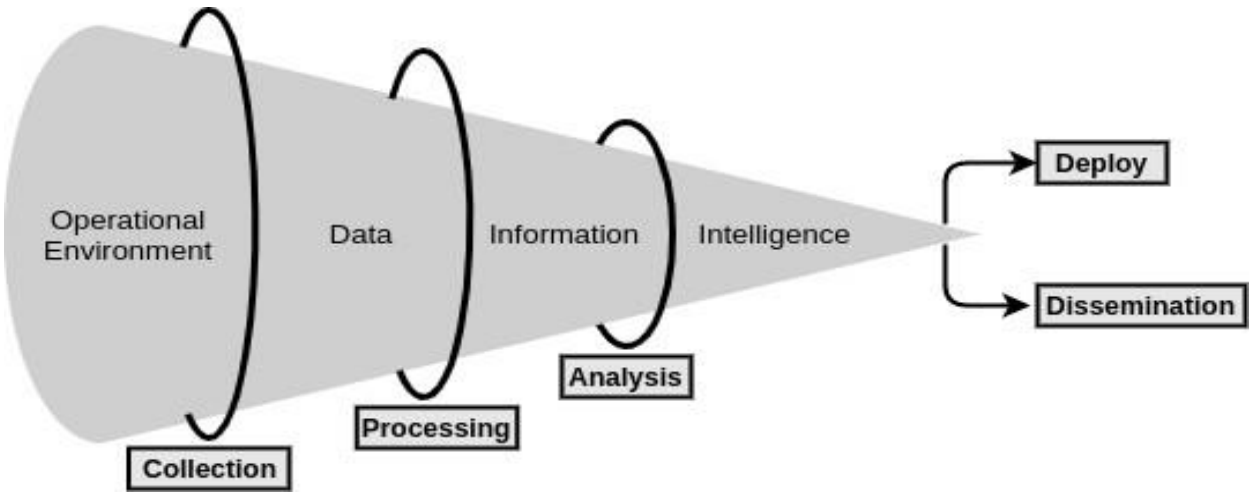


Figure 1: Threat Intelligence Production Process Flow.

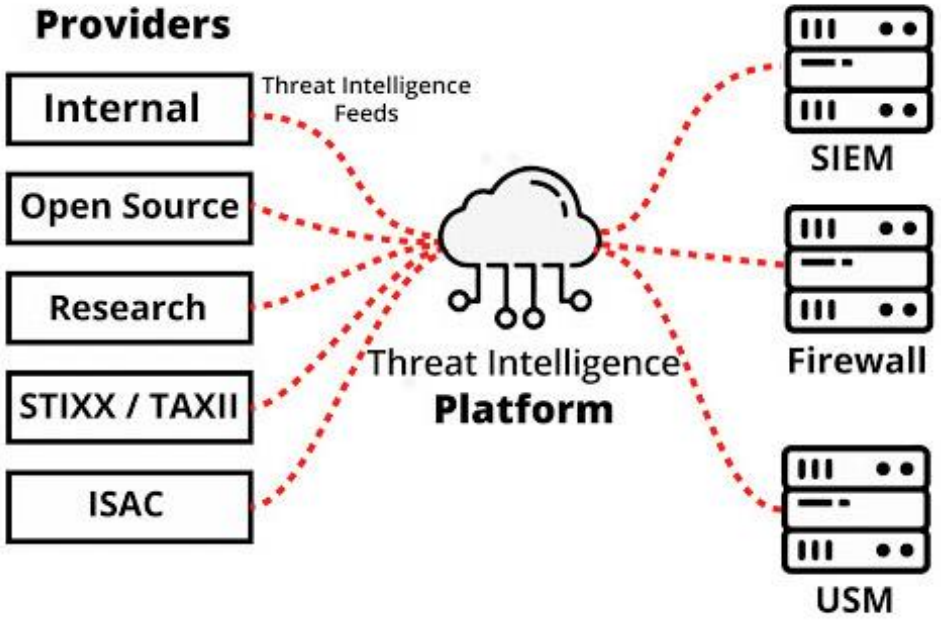


Figure 2: Intelligence cycle

1.2 Σκοπός της εργασίας

Ο σκοπός αυτής της εργασίας είναι να παρέχει μια διεξοδική επισκόπηση και σύγκριση των TIPs. Με βάση τα αποτελέσματα, θα συζητήσουμε τις συνέπειες και τη σημασία τους για την επιστημονική έρευνα αλλά και τους οργανισμούς. Πραγματοποίησα μια ανάλυση τεσσάρων TIPs, αποτελούμενα από προϊόντα ανοιχτού κώδικα, για την επίτευξη αυτού του στόχου. Η σύγκριση και η αξιολόγηση αυτών των λύσεων έγινε σύμφωνα με διάφορα κριτήρια, όπως περιπτώσεις χρήσης, λειτουργίες ανταλλαγής πληροφοριών και κατά πόσο αυτές οι πλατφόρμες προσφέρουν δυνατότητες συνεργασίας. Με βάση αυτά τα αποτελέσματα, θα παρουσιαστούν ορισμένα κύρια ευρήματα αλλά και κάποιοι περιορισμοί.

Αυτή η έρευνα έδειξε ότι, ενώ το ενδιαφέρον σε αυτόν τον τομέα έχει αυξηθεί δραματικά τα τελευταία χρόνια, εξακολουθεί να λείπει ένα κοινό concept σ' αυτές τις πλατφόρμες, μια κοινή ιδέα. Αν και το STIX είναι το ολοκληρωμένο de-facto πρότυπο για την περιγραφή δεδομένων απειλής, οι περιγραφικές του δυνατότητες δεν χρησιμοποιούνται πλήρως από τις περισσότερες πλατφόρμες. Αυτό αποδεικνύεται από το γεγονός ότι οι περισσότερες πλατφόρμες επικεντρώνονται κυρίως στην ανταλλαγή των indicators of compromise ή αλλιώς δεικτών συμβιβασμού δηλαδή των κινήσεων που παρατηρούνται σ' ένα δίκτυο οι οποίες με μεγάλη εμπιστοσύνη υποδηλώνουν εισβολή.

Πολλές εταιρείες άρχισαν να βασίζονται στις πλατφόρμες Threat Intelligence για να ξεπεράσουν τα κενά και τους περιορισμούς των πραγματικών συστημάτων ανίχνευσης και παρακολούθησης (π.χ. SIEMs). Αυτά τα συστήματα είναι υπεύθυνα για την επεξεργασία δεδομένων από διάφορες εξωτερικές πηγές και εκτελούν πολύπλοκες λειτουργίες όπως φιλτράρισμα, συγκέντρωση, τυποποίηση, αναγνώριση, ερμηνεία και εμπλουτισμό. Ωστόσο, η

εφαρμογή και η χρήση τους εξακολουθούν να είναι πολύπλοκη και υπάρχουν ακόμα πολλά μειονεκτήματα που πρέπει να αντιμετωπιστούν. Οι TIPs είναι ιδανικά εργαλεία για τη συλλογή δεδομένων, την αποθήκευση, την κοινή χρήση και την ενοποίηση με εξωτερικές οντότητες, που θα μπορούσαν να είναι συνδεδεμένες με άλλες πλατφόρμες ασφαλείας και εργαλεία, καθώς και εξαιρετικά χρήσιμες για συγκεκριμένες ομάδες για τον χειρισμό απόκρισης συμβάντων και διαχείρισης απειλών (π.χ. SOC, CSIRTs). Υπάρχουν αρκετές TIPs που διατίθενται στην αγορά (τα περισσότερα από αυτά με εμπορική άδεια). Όσον αφορά τις λύσεις ανοιχτού κώδικα, έχω εντοπίσει και ασχοληθεί παραπάνω σ' αυτή την εργασία με τα ακόλουθα:

- The Malware Information Sharing Platform(MISP),
- The Collective Intelligence Framework (CIF),
- The Collaborative Research Into Threats (CRITs), and
- Open Cyber Threat Intelligence platform (openCTI)

Στον παρακάτω πίνακα φαίνονται οι χρήστες που χρησιμοποιούν τις TIPs, ποιες είναι οι ανάγκες τους αλλα και ποιες είναι οι προκλήσεις που πρέπει να αντιμετωπίσουν.

Table 1: Users of TIPs

Role	Major Contributions	Major Needs	Major Challenges
SOC analysts	1. SOC analysts provide feedback on indicators observed during triage phase. 2. They can also annotate indicators based on observations, alerts and actions taken.	1. Enhanced context and low false positive rates for basic indicators. 2. Vetted intelligence provided to SOC. 3. Automated data enrichment to reduce repetitive work. 4. Good integration with SIEM tools. 5. Playbooks and clear workflows. 6. Red flags related to key threats.	1.Too many alerts associated with threats, thus needing more context on which ones are the important ones and prioritize. 2. Lack of automation resulting in lots of manual tasks.
Incident responders (and digital forensics)	1. Incident responders can contribute new indicators and malware samples coming from investigations. 2. They can provide in depth analysis results from investigations and malware/log/forensics analysis. 3. Share tools and practices that helped them solve other problems.	1. Incident responders need tailored and ad-hoc intelligence related to tools, modus operandi, associated campaigns, actor intents and attributions, and forensic data for their investigations. 2. They also need detailed context and enrichment over the indicators provided. 3. Need to quickly identify if the investigated incident is part of a targeted attack and any other information that would help direct the response.	1. Lack of visibility into events across different systems or domains within the organisation. Thus, it is difficult to build the complete chain of the attack. 2. Manual tasks for collecting investigation logs/samples, for correlating collected data as well as for containing the incidents.
CTI analysts	1. CTI analysts are responsible for anything that goes in and out of the TIP (plus evaluate sources, intelligence and revise requirements). 2. They are responsible for enriching and analysing the data within TIP as well as linking intelligence. 3. Responsible for sharing intelligence with stakeholders (internal and external).	1. Need for a centralised platform for managing threat intelligence. 2. Unified relationship management with key internal and external stakeholders. 3. Trusted (personal and community) relationships for sensitive data sharing and trust in the access controls of the TIP. 4. Access and analysis from tactical to strategic threat intelligence.	1. Too much threat intelligence information floods CTI analysts who struggle to identify the most important and prioritise. 2. Too many manual tasks required for CTI analysts' workflows. 3. Lack of threat intelligence best practices and analysis capabilities toolsets.

Threat researchers and intelligence producers	1. High quality original research conducted (potentially large amounts). 2. They have access to a number of sources and tools for their threat research and fusion. 3. They can conduct threat research, enrichment and analysis based on request and existing cases (RFI process).	1. Power users need APIs so that they can work on importing and exporting data from/to their toolset. 2. Ability to customize certain parts of TIP so that their workflows are supported (e.g. UI, more detailed indicators, etc.).	1. API support that is critical for the integration of power users' toolset. 2. Limited customization capabilities for TIP hinders the streamlining of their workflows.
Cyber fraud analysts	1. New indicators and samples related to cyber fraud. 2. Information on fraud related campaigns targeting the organisation.	1. Need to quickly identify if the investigated fraud is part of a complex attack and any other information that would help direct the response. 2. Expand their fraud investigation to identify other elements of the fraud. 3. Fraud attribution information.	1. Limited technology enablement to connect cyber and fraud datasets for investigation providing the relevant analysis tools.
Vulnerability analysts	1. Provide insight on the vulnerability exposure of the organisation.	1. Intelligence on high impact vulnerabilities of the organisations assets that can be exploitable. 2. Intelligence that would help them prioritise on patching and focusing on critical assets.	1. Prioritisation of the vulnerabilities to be patched.
Decision makers, IT Managers and Executives	1. They are the decision makers for sharing highly sensitive information. 2. They are responsible for the overall sharing policy and sharing culture for the organisation. 3. Decision makers for the security investment, staffing and budget related issues.	1. Decision makers need high level reports on exposures and the top threat that are relevant to the organisation in order to minimize risks. 2. Need to evaluate the ROI for intelligence investment via relevant investigation metrics. 3. Need to evaluate the ROI for external intelligence sharing via relevant metrics and evidence. 4. Assurance required that external intelligence sharing does not create risks for the organisation.	1. Decision makers have limited understanding of the organisation's exposures before a security incident takes place. 2. They are challenged to prove the value for intelligence investment.

2 ΠΕΡΙΓΡΑΦΗ ΤΩΝ TIPs

2.1. MISP

2.1.1. OVERVIEW OF MISP

Η πλατφόρμα MISP (Malware Information Sharing Platform) είναι μια πλατφόρμα λογισμικού ανοιχτού κώδικα (ελεύθερη λήψη και χωρίς δικαιώματα εκμετάλλευσης) που μπορεί να εγκατασταθεί από οποιονδήποτε οργανισμό προκειμένου να συλλέξει και να διανείμει πληροφορίες κακόβουλου λογισμικού. Πρόκειται για μια πλατφόρμα προσανατολισμένη στη συνεργασία - μια κοινοτική πλατφόρμα, που στοχεύει σε εμπειρογνώμονες στον κυβερνοχώρο που μοιράζονται τις ανακαλύψεις και τις πληροφορίες τους.

Στην πράξη, χρησιμοποιείται από ορισμένους οργανισμούς (Ομάδες Απαντήσεων Έκτακτης Ανάγκης Υπολογιστών-CERTs ή Cyber Security Incident Response Teams-CSIRTs) που βοηθούν τα αντίστοιχα μέλη τους σε περίπτωση συμβάντων ασφαλείας στους υπολογιστές τους. Τα περιστατικά μπορεί να είναι παραβιάσεις δεδομένων (κλοπή ή απώλεια δεδομένων), αλλά και εισβολές από τρίτους (εγκληματίες στον κυβερνοχώρο), είσοδος σε εταιρικά δίκτυα, μέσω κακόβουλου λογισμικού (ιούς, ransomware, ...), botnets, επιθέσεις ddos, spam, phishing και άλλες κυβερνο-εγκληματικές δραστηριότητες.

Η MISP είναι μια πλατφόρμα για κοινή χρήση, αποθήκευση και συσχέτιση δεικτών συμβιβασμών στοχευμένων επιθέσεων. Η πλατφόρμα χρησιμοποιείται σήμερα σε πολλούς οργανισμούς όχι μόνο για την αποθήκευση, την κοινή χρήση δεδομένων απειλής αλλά και για τη χρήση των IoCs (Indicators of Compromise-Δείκτες συμβιβασμού) για την υποστήριξη της ανίχνευσης και πρόληψης συμβάντων και επιθέσεων. Ο κύριος σκοπός της πλατφόρμας είναι να βοηθήσει τις ομάδες διαχείρισης περιστατικών και συμβάντων να τα διερευνήσουν, να τα αναφέρουν στη πλατφόρμα ώστε με αυτό τον τρόπο να ειδοποιηθούν άλλοι συνδρομητές MISP ώστε να γνωρίζουν το συμβάν και

να ξέρουν ότι παρόμοια συμβάντα ενδέχεται να συμβούν στους ίδιους - ή σε ενδιαφερόμενα προς αυτούς μέρη. Αυτές οι ομάδες διαχείρισης συμβάντων μπορεί να είναι υπεύθυνες για έναν οργανισμό (μεγάλες εταιρείες ή εταιρείες υπηρεσιών ασφαλείας) ή για πολλούς οργανισμούς (όπως οι εθνικές CERT), που συνήθως φροντίζουν για τα περιστατικά των εθνικών κυβερνήσεων, των φορέων διοίκησης και της δημόσιας αρχής.

Το MISP όπως αναφέρθηκε σε προηγούμενη παράγραφο είναι ένα λογισμικό ανοιχτού κώδικα και υπάρχει μια μεγάλη κοινότητα χρηστών MISP που δημιουργούν, συντηρούν και που μοιράζονται πληροφορίες σχετικά με απειλές ή δείκτες ασφάλειας στον κυβερνοχώρο παγκοσμίως. Το project MISP δεν διατηρεί πλήρη κατάλογο όλων των κοινοτήτων που βασίζονται σ' αυτό, ειδικά όταν ορισμένες κοινότητες χρησιμοποιούν το MISP εσωτερικά ή ιδιωτικά.

Το MISP βρίσκει τις ρίζες του ήδη στις αρχές της δεκαετίας του 1990. Η πρώτη τεχνική πλατφόρμα δημιουργήθηκε το 2011 σαν απόρροια της απογοήτευσης που επικρατούσε όταν ο διαμοιρασμός των IoCs γινόταν μέσω email ή σε μορφή pdf και δεν ήταν αναγνώσιμα από αυτόματα μηχανήματα. Η πρώτη προσπάθεια ονομάστηκε CyDefSIG: Cyber Defense Signatures.Github (open source - open development platform), το οποίο αναπτύχθηκε περαιτέρω από τις ομάδες CERT του NATO και τις βελγικές στρατιωτικές ομάδες CERT. Ο κύριος προγραμματιστής συνεργάζεται με την ομάδα CERT του Λουξεμβούργου (CIRCL). Σήμερα, υπάρχει μια κοινότητα προγραμματιστών, συνεργατών και χρηστών, που εργάζονται για τη πλατφόρμα. Υπάρχει μια βασική ομάδα ατόμων με κίνητρα που πιστεύουν ότι η ανταλλαγή πληροφοριών μπορεί να βελτιωθεί και να υποστηριχθεί δημιουργώντας εργαλεία ανοιχτού κώδικα, ανοιχτή μορφή και πρακτικές.

Η κοινότητα πληροφορικής έρχεται αντιμέτωπη με περιστατικά κάθε είδους και φύσης και νέες απειλές εμφανίζονται καθημερινά. Είναι σχεδόν αδύνατη η καταπολέμηση αυτών των περιστατικών ασφαλείας μεμονωμένα. Η ανταλλαγή πληροφοριών σχετικά με τις απειλές μεταξύ της κοινότητας έχει γίνει βασικό στοιχείο στην αντιμετώπιση αυτών των περιστατικών. Οι αξιόπιστοι πόροι πληροφόρησης, που παρέχουν αξιόπιστες πληροφορίες, είναι επομένως απαραίτητοι για την κοινότητα πληροφορικής, ή ακόμη και σε ευρύτερη κλίμακα, για κοινότητες πληροφοριών ή ομάδες εντοπισμού απάτης. Οι επόμενες παράγραφοι παρουσιάζουν το project "Malware Information Sharing Plaform» -MISP στόχος του οποίου είναι να βοηθήσει στη δημιουργία προληπτικών ενεργειών και αντιμέτρων που χρησιμοποιούνται κατά των στοχευμένων αυτών επιθέσεων.

2.1.2. Μοντέλο δεδομένων

Ένας βασικός στόχος κατά την ανάπτυξη της πλατφόρμας ήταν τα δεδομένα που υπάρχουν και διαχειρίζονται οι χρήστες της να έχουν μια απλή και κατανοητή μορφή, καλύπτοντας ταυτόχρονα και πιο απαιτητικές ανάγκες. Ένα πλεονέκτημα αυτής της προσέγγισης είναι ότι ο χρήστης μπορεί να αποφασίσει τον όγκο των πληροφοριών που θέλει να μοιραστεί. Για παράδειγμα, όταν ο χρήστης θέλει να παρέχει όσο το δυνατόν περισσότερες πληροφορίες μπορεί, τότε μπορεί να ορίσει ένα συμβάν με πολλά χαρακτηριστικά(attributes) ή αντίθετα μπορεί να παρέχει μόνο ελάχιστες πληροφορίες για ένα συμβάν ορίζοντας και ελάχιστα χαρακτηριστικά. Ένας άλλος λόγος που επιλέχθηκε αυτό το μοντέλο ήταν η ύπαρξη ενός επίπεδου μοντέλου για τη διευκόλυνση της ανάλυσης της εργασίας και την αποφυγή ασάφειας (π.χ. STIX). Στο MISP, μια νέα καταχώρηση ονομάζεται αντικείμενο συμβάντος (event objects). Για ένα IoC, ένα συμβάν μπορεί να περιγραφεί ως μια συλλογή χαρακτηριστικών και όλων των ειδών περιγραφών, συμπεριλαμβανομένων συνημμένων κ.λπ. Τέτοιες λειτουργίες ονομάζονται χαρακτηριστικά(features). Για παράδειγμα, χαρακτηριστικά συμβάντων είναι η ημερομηνία ενός IoC, threat levels, comments, organisation κ.λπ.

Τα χαρακτηριστικά μπορούν να χωριστούν σε δύο διαφορετικές κατηγορίες, κατηγορία και τύπο. Η κύρια διαφορά είναι ότι ένα χαρακτηριστικό κατηγορίας περιέχει πιο γενικές πληροφορίες, όπως δεδομένα στόχευσης,

δραστηριότητα δικτύου, τύπο απάτης κ.λπ., ενώ ένα χαρακτηριστικό τύπου περιλαμβάνει πληροφορίες όπως τα αθροίσματα ελέγχου (md5, sha1), όνομα αρχείου, hostname, διεύθυνση IP, πηγή email και προορισμός, κ.λπ. Επιπλέον, ένα συμβάν μπορεί επίσης να έχει ετικέτες. Μια απλοποιημένη αναπαράσταση αυτού του μοντέλου δεδομένων δίνεται στο Σχήμα 1.

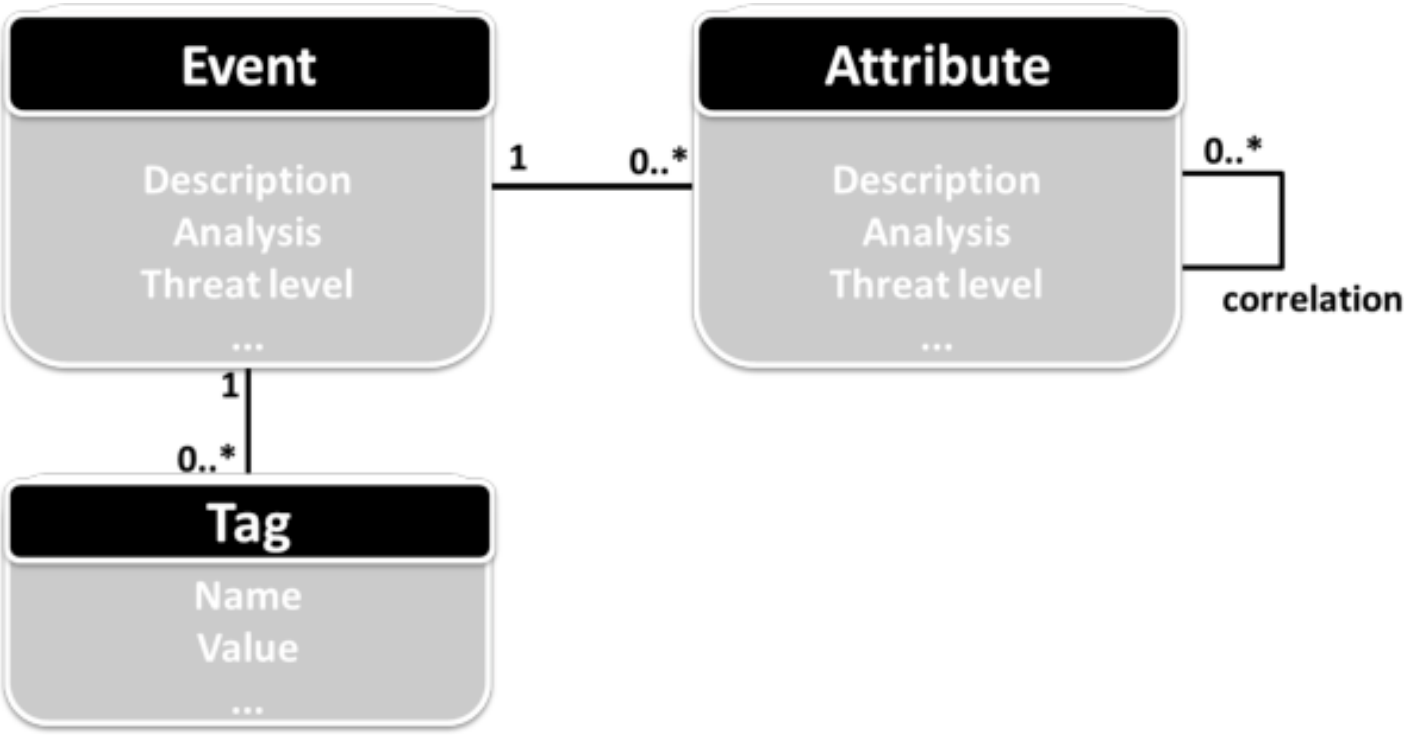
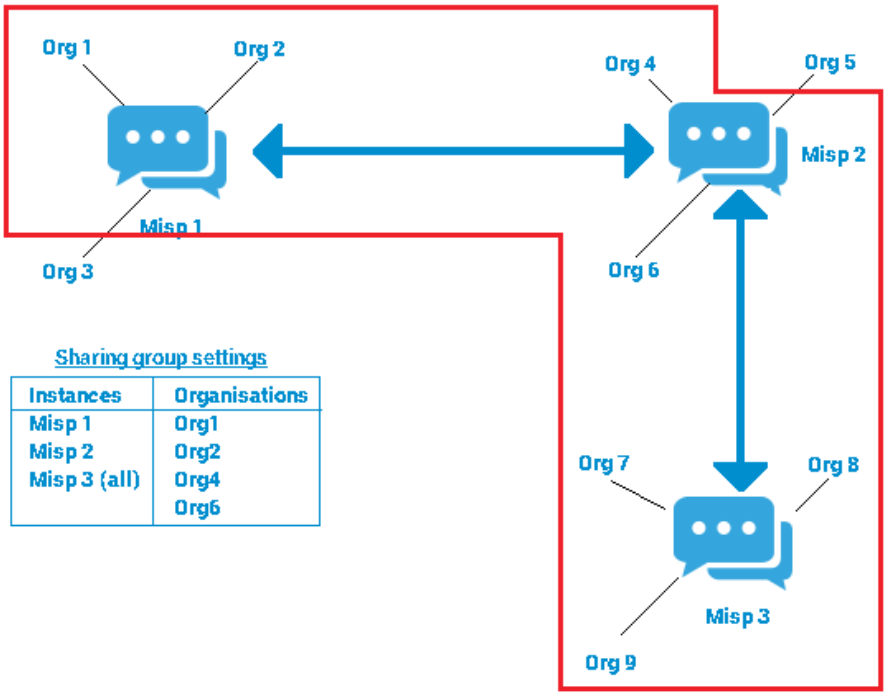


Figure 1: Misp data model

2.1.3. Μοντέλα διαμοιρασμού

Το κίνητρο για την ανταλλαγή πληροφοριών μπορεί να είναι πολλαπλό, καθώς οι άνθρωποι έχουν αντιφατικές ανάγκες με την έννοια του «security versus relatedness». Από τη μία πλευρά, οι άνθρωποι που μοιράζονται πληροφορίες σχετικά με απειλές και συμβάντα που σημειώθηκαν σε μια κοινότητα θα προτιμούσαν να τις διατηρήσουν μυστικές. Από την άλλη πλευρά όμως όταν οι άνθρωποι αποφασίζουν να μοιραστούν πληροφορίες τότε μπορούν να εξαχθούν απ' αυτή την κοινότητα νέες πληροφορίες ή παρόμοιες πληροφορίες, καθώς και οι πιθανές ενέργειες απόκρισης.

Το εγγενές κίνητρο, όπως περιγράφεται στη θεωρία αυτοδιάθεσης, εξηγεί ότι οι άνθρωποι μπορούν να εκτελέσουν ή να ξεκινήσουν ενέργειες χωρίς την ανάγκη εξωτερικών ανταμοιβών . Σε αυτήν την περίπτωση, αυτό σημαίνει ότι οι άνθρωποι μοιράζονται ρητά πληροφορίες σχετικά με απειλές ή συμβάντα εντός μιας κοινότητας (reletedness) για να αποκτήσουν πληροφορίες σχετικά με νέες απειλές που δημοσιεύονται από άλλους (ασφάλεια).



2.1.3.1 Sharing levels

Το MISP βασίζεται στην εθελοντική δράση της κοινότητάς του για την ανταλλαγή πληροφοριών και δεικτών. Επιπλέον, το επίπεδο προσέγγισης του περιεχομένου αφήνεται στον χρήστη που μοιράζεται τα δεδομένα και ο οποίος μπορεί να επιλέξει διάφορα σενάρια κοινής χρήσης, όπως περιγράφονται παρακάτω:

- **Your organization only:** Αυτή η ρύθμιση θα επιτρέπει μόνο στα μέλη του οργανισμού σας να βλέπουν τις πληροφορίες.

- **This Community-only:** Μόνο οι χρήστες που ανήκουν στην κοινότητά σας θα μπορούν να δουν το συμβάν. Αυτό περιλαμβάνει τον δικό σας οργανισμό, οργανισμούς σε αυτόν τον διακομιστή MISP και οργανισμούς που έχουν διακομιστές MISP συγχρονισμένους με αυτόν τον διακομιστή. Τυχόν άλλοι οργανισμοί που είναι συνδεδεμένοι σε αυτούς τους συνδεδεμένους διακομιστές δεν θα βλέπουν το event.

- **Connected Communities:** Οι χρήστες που ανήκουν στην κοινότητα MISP θα μπορούν να δουν το συμβάν. Αυτό περιλαμβάνει όλους τους οργανισμούς σε αυτόν τον διακομιστή MISP, όλους τους οργανισμούς σε διακομιστές MISP που συγχρονίζονται με αυτόν τον διακομιστή και τους οργανισμούς φιλοξενίας διακομιστών που συνδέονται με αυτούς τους προαναφερθέντες διακομιστές (οπότε ουσιαστικά οποιοσδήποτε διακομιστής απέχει 2 λυκίσκους από αυτόν). Τυχόν άλλοι οργανισμοί που είναι συνδεδεμένοι σε συνδεδεμένους διακομιστές που απέχουν 2 λυκίσκους από αυτόν, δεν θα μπορούν να δουν το συμβάν.

- **All communities**: Αυτό θα μοιραστεί το συμβάν με όλες τις κοινότητες MISP, επιτρέποντας το συγκεκριμένο event να διαδίδεται ελεύθερα από τον ένα διακομιστή στον άλλο.

- **Sharing Group**: Αυτό θα κοινοποιήσει το συμβάν στην καθορισμένη ομάδα κοινής χρήσης. Αυτό περιλαμβάνει μόνο τους οργανισμούς που ορίζονται στην ομάδα κοινής χρήσης. Η διανομή μπορεί να είναι τοπική και cross-instance ανάλογα με τον ορισμό της κοινής χρήσης ομάδας.

Προκειμένου να διασφαλιστεί η αξιοπιστία των δεδομένων που διαβιβάζονται από το MISP, επιτρέπεται μόνο στα μέλη της οντότητας που σχηματίζουν τα γεγονότα(events) να τα αλλάξουν. Ωστόσο, μία από τις βασικές πτυχές της επιτυχούς ανταλλαγής πληροφοριών είναι η εστίαση στη συνεργασία και στην παροχή στη βάση χρηστών ενός βρόχου ανατροφοδότησης. Οι **προτάσεις(proposals)** που εισάγονται σαν έννοια στη πλατφόρμα επιτρέπουν στους χρήστες, που δημιουργούνται από άλλη οντότητα, να υποβάλλουν προτάσεις για βελτιώσεις. Οι προτάσεις αποτελούν αναπόσπαστο μέρος της γνώσης που μεταδίδεται μεταξύ των MISP instances. Ένας χρήστης μπορεί να υποβάλει μια πρόταση για ένα συμβάν σε ένα απομακρυσμένο instance που δημιουργήθηκε από διαφορετικό οργανισμό. Αυτή η πρόταση αναφέρεται στον αρχικό δημιουργό του event, ο οποίος μπορεί να την αποδεχτεί ή να την απορρίψει. Σε κάθε περίπτωση, το αποτέλεσμα αυτής της απόφασης θα μεταδοθεί σε όλες τα διασυνδεδεμένα instances.

Για παράδειγμα, ειδοποιώντας έναν δημιουργό ενός event για false positives, ζητώντας διόρθωση του σφάλματος ή απλά την συμπλήρωση ενός υπάρχοντος συμβάντος με πρόσθετα ευρήματα είναι κάποιες απ’ τις κοινές χρήσεις αυτής της δυνατότητας.

2.1.4 Taxonomies

Η εμπειρία από τους χρήστες που συλλέχθηκε από παλαιότερες εκδόσεις MISP έχει δείξει ότι οι άνθρωποι δεν θέλουν να ξοδέψουν πολύ χρόνο για να συμπληρώσουν πεδία σε φόρμες ιστού ή να αντιγράψουν και να επικολλήσουν πληροφορίες. Ένα περίπλοκο περιβάλλον εργασίας χρήστη λειτουργεί σαν ένας ανασταλτικός παράγοντας της ανταλλαγής πληροφοριών. Ως εκ τούτου, εισήχθη η δυνατότητα εισαγωγής ελεύθερου κειμένου. Ένας χρήστης μπορεί να αντιγράψει και να επικολλήσει ακατέργαστα δεδομένα σε ένα μόνο πεδίο που στη συνέχεια τροφοδοτείται μέσω ενός αλγορίθμου που βασίζεται σε ευρετικά στοιχεία(heuristics) για να ταιριάζει με τα χαρακτηριστικά(attributes). Με τη σειρά τους τα χαρακτηριστικά αυτά παρουσιάζονται στον χρήστη που πρέπει να επικυρώσει τις αντιστοιχίσεις.

Οι αλληλεπιδράσεις με το MISP μπορούν να γίνουν με μια διεπαφή REST (REp-resentational State Transfer). Εργαλεία όπως το Cuckoo sandbox2 και Viper analysis3 υποστηρίζουν τη πλατφόρμα MISP για να επιτρέπεται μια αμφίδρομη ροή πληροφοριών. Αυτές οι δυνατότητες, σε συνδυασμό με τον σταθερά αυξανόμενο αριθμό χρηστών, οδήγησε στην απαίτηση δυνατότητας επεξεργασίας ήδη δημιουργημένων συμβάντων. Αυτή η δυνατότητα είναι επίσης χρήσιμη ως προς τον χειρισμό της ταξινόμησης των πληροφοριών. Η ταξινόμηση συνδέεται συχνά με εσωτερικά, κοινοτικά ή εθνικά συστήματα ταξινόμησης.

Ένα άλλο κοινό πρόβλημα είναι η περιγραφή των events και η χαρτογράφηση τους σε κατηγορίες. Αυτό είναι ένα πολύπλοκο task, καθώς δυστυχώς ο αριθμός των κατηγοριών δεν είναι γνωστός εκ των προτέρων. Ένα τυπικό παράδειγμα εδώ είναι: οι τύποι της επίθεσης καθώς αυτοί εξελίσσονται και αλλάζουν γρήγορα. Η εμπειρία έχει δείξει ότι αυτές οι προκλήσεις σχετίζονται συχνά με το περιεχόμενο και, συνεπώς, με τους χρήστες του λογισμικού MISP. Ένα συγκεντρωτικό προκαθορισμένο σύνολο κατηγοριών που ικανοποιεί όλους τους πιθανούς χρήστες σίγουρα ακούγεται δύσκολο και έτσι, εισήχθη μια κατανεμημένη προσέγγιση που βασίζεται σε ετικέτες μηχανών(machine tags). Οι ετικέτες μπορούν να καθοριστούν ανά MISP instance και μπορούν να εξαχθούν. Αυτό

επιτρέπει την επαναχρησιμοποίηση ετικετών από άλλα MISP instances. Η ελευθερία ορισμού ετικετών οδηγεί γρήγορα σε μια κατάσταση όπου οι ετικέτες επαναπροσδιορίστηκαν καθιστώντας το φιλτράρισμα περίπλοκο.

Για να ξεπεραστεί αυτό το πρόβλημα, εισήχθη μια νέα έννοια της προσθήκης ετικετών(tags), οι ταξινομίες(taxonomies). Η ταξινομία βασίζεται στη λύση τριπλής ετικέτας(triple tag solution) που εισήχθη από τον Flickr.

Ένα σαφές πλεονέκτημα αυτής της έννοιας είναι η αναγνώσιμη από τον άνθρωπο μορφή των ετικετών του μηχανήματος. Το αποθετήριο ταξινομιών για την κοινότητα ανοιχτού κώδικα περιλαμβάνει ταξινόμηση μοντελοποίησης εθνικών, πληροφοριών, επιβολής του νόμου, ταξινομήσεων csirt και πολλών άλλων τομέων. Σε περίπτωση που καμία από τις προκαθορισμένες ταξινομήσεις δεν ταιριάζει με την περιγραφή ενός συμβάντος, ο χρήστης μπορεί να διατυπώσει τη δική του ταξινόμηση. Τα παρακάτω είναι μερικά παραδείγματα ταξινομιών που μπορούν να χρησιμοποιηθούν στο MISP (ως τοπικές ή κατανεμημένες ετικέτες) ή σε άλλα εργαλεία που επιθυμούν να μοιραστούν κοινές ταξινομίες μεταξύ εργαλείων ανταλλαγής πληροφοριών ασφαλείας:

Admiralty Scale: Η Admiralty Scale (also called the NATO System) χρησιμοποιείται για την κατάταξη της αξιοπιστίας μιας πηγής και της αξιοπιστίας μιας πληροφορίας. **Adversary**: An overview and description of the adversary infrastructure.

CIRCL Taxonomy - Schemes of Classification in Incident Response and Detection: CIRCL Taxonomy είναι ένα απλό σχήμα για την ταξινόμηση συμβάντων

Cyber Kill Chain DE German (DE) Government classification markings (VS)

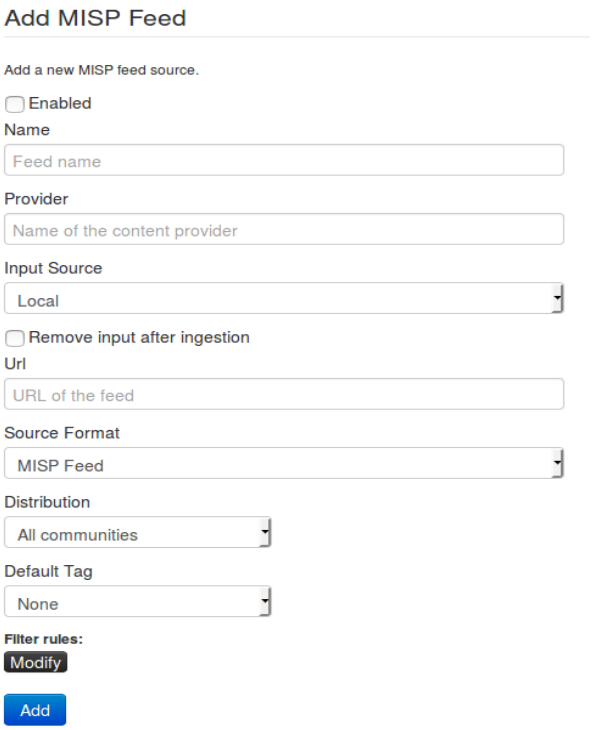
Europol Incident

Europol Events

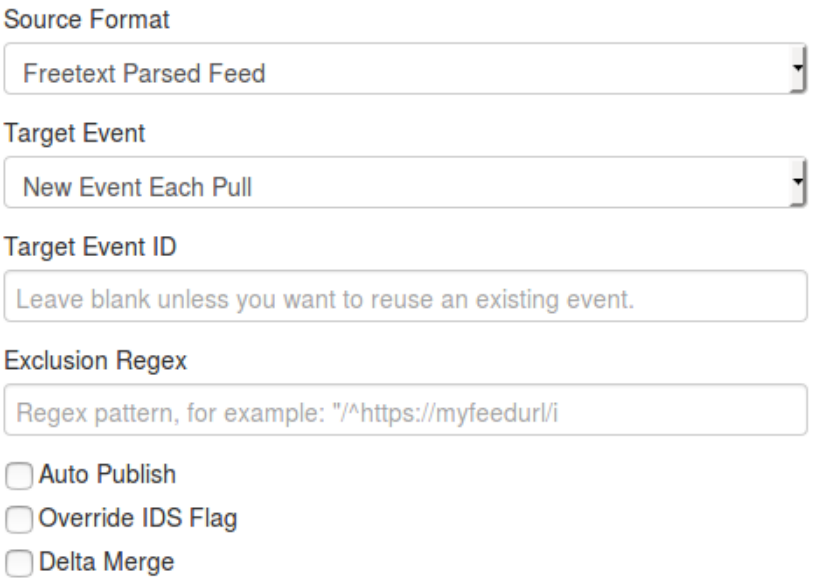
2.1.6 Ροές Συστήματος

Οι ροές είναι απομακρυσμένα ή τοπικά εργαλεία που περιέχουν δείκτες που μπορούν να εισαχθούν σε τακτά χρονικά διαστήματα αυτόματα στο MISP. Οι ροές μπορούν να οργανωθούν σε μορφές αρχείων MISP, CSV ή ακόμη και ελεύθερου κειμένου. Είναι ένας απλός τρόπος συγκέντρωσης πολλών εξωτερικών πηγών δεδομένων στο MISP χωρίς καμία ικανότητα προγραμματισμού. Ο ορισμός των ροών μπορεί επίσης να μοιραστεί εύκολα ανάμεσα σε διάφορες παρουσίες MISP, καθώς μπορεί να εξαχθεί μια περιγραφή ροής ως JSON και να εισαχθεί ξανά σε ένα άλλο instance του MISP.

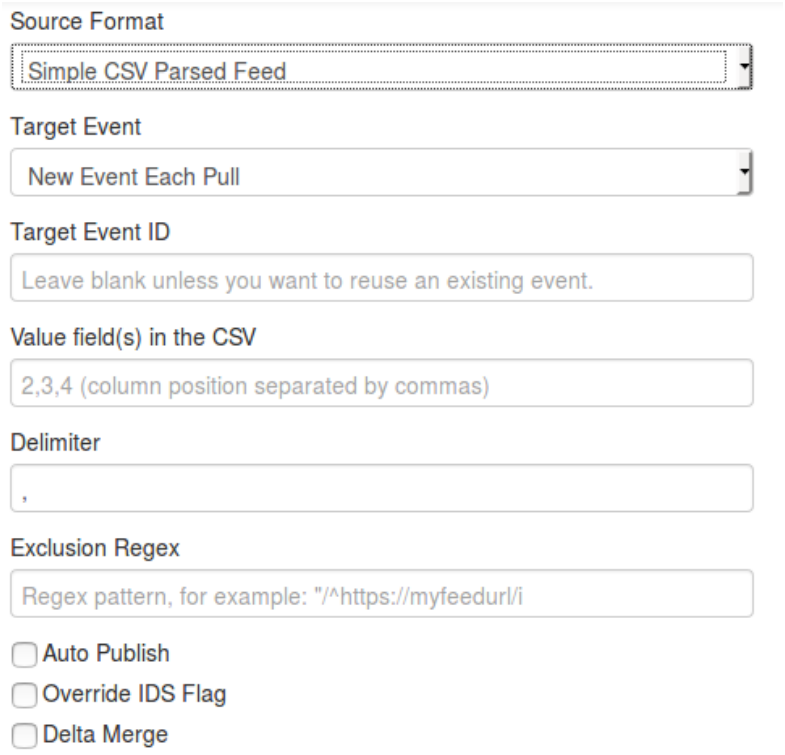
Παράδειγμα εισαγωγής ροής MISP:



Παράδειγμα εισαγωγής ροής ελευθέρου κειμένου:



Εισαγωγή ροής CSV:



2.2 OpenCTI

2.2.1 OpenCTI overview

Το OpenCTI (Open Cyber Threat Intelligence) είναι μια πλατφόρμα που αναπτύχθηκε με σκοπό την ενημέρωση, την ανταλλαγή πληροφοριών και τέλος την προστασία από την απειλή στον κυβερνοχώρο. Ιδρύθηκε, τον Σεπτέμβριο του 2018, από τη γαλλική εθνική υπηρεσία ασφάλειας στον κυβερνοχώρο (ANSSI) μαζί με το CERT-EU (Ομάδα έκτακτης ανάγκης για υπολογιστές της Ευρωπαϊκής Ένωσης). Αρχικά σχεδιάστηκε για να αναπτύξει και να διευκολύνει τις αλληλεπιδράσεις της ANSSI με τους συνεργάτες της. Αναπτύχθηκε με σκοπό να καλύψει την κοινή ανάγκη για μια κατάλληλη επιλογή για τη δομή, την αποθήκευση, την οργάνωση, την οπτικοποίηση και την κοινή χρήση πληροφοριών για απειλές στον κυβερνοχώρο σε διάφορα επίπεδα. Σήμερα, η πλατφόρμα είναι διαθέσιμη προς όλους, όντας ένα λογισμικό ανοιχτού κώδικα και διατίθεται ελεύθερα στην κοινότητα πληροφοριών.

Στοχεύοντας στην βελτιστοποίηση της αποστολής της η ANSSI επεκτείνει και μοιράζεται καθημερινά τις γνώσεις, τις καινοτομίες και τις αναλύσεις της σχετικά με στρατηγικές, επιχειρησιακές και τεχνικές πτυχές των απειλών στον κυβερνοχώρο. Αυτή η τεχνογνωσία είναι κομβική για να βοηθήσει το ANSSI να προβλέψει απειλές και κινδύνους και να ανταποκριθεί καλύτερα σε αυτά. Διαπιστώνουμε πως, για να υπάρξουν ακόμα μεγαλύτερα αποτελέσματα και προστασία των πληροφοριών, αυτή η τεχνογνωσία πρέπει να δομηθεί ενδελεχώς και να υποβληθεί σε κατάλληλη επεξεργασία.

Η ANSSI όχι μόνο αξιοποιεί αυτή τη γνώση για να εκπληρώσει σωστά τις αποστολές της στον κυβερνοάμυνα, αλλά και τη μοιράζεται με τους συνεργάτες της (όπως CSIRT και άλλες υπηρεσίες ασφάλειας στον κυβερνοχώρο) τόσο σε εθνικό όσο και σε διεθνές επίπεδο.

Μακροπρόθεσμα, η ευρεία χρήση της πλατφόρμας OpenCTI από την ANSSI και τους συνεργάτες της θα βοηθήσει στην ανάπτυξη και τη διευκόλυνση της ανταλλαγής δομημένων γνώσεων σχετικά με τις απειλές στον κυβερνοχώρο, προκειμένου να οικοδομηθεί ένα συλλογικό και όλο και πιο ακριβές όραμα αυτών των απειλών.

2.2.2 Μοντέλο Δεδομένων

Τα δεδομένα είναι δομημένα χρησιμοποιώντας ένα μοτίβο που βασίζεται στα πρότυπα STIX2. Έχει σχεδιαστεί ως μια σύγχρονη εφαρμογή ιστού που περιλαμβάνει ένα GraphQL API και ένα UX .

Επίσης, το OpenCTI μπορεί να ενσωματωθεί σε άλλα εργαλεία και εφαρμογές όπως MISP, TheHive, MITRE ATTACK κ.λπ.

<table>
<tr><th colspan="5">STIX Objects</th><td rowspan="3">STIX Bundle Object</td></tr>
<tr><th colspan="3">STIX Core Objects</th><th colspan="2">STIX Meta Objects</th></tr>
<tr><td>STIX Domain Objects (SDO)</td><td>STIX Cyber-observable Objects (SCO)</td><td>STIX Relationship Objects (SRO)</td><td>Language Content Objects</td><td>Marking Definition Objects</td></tr>
</table>

Ο στόχος του OpenCTI είναι να αποτελεί ένα ολοκληρωμένο εργαλείο που επιτρέπει στους χρήστες να ενσωματώνουν τεχνικές πληροφορίες (όπως TTP) και μη τεχνικές πληροφορίες (όπως προτεινόμενη απόδοση, θυματολογία, τομέας δραστηριότητας και εντοπισμός), ενώ συνδέουν κάθε πληροφορία με την κύρια πηγή (μια αναφορά, ένα συμβάν MISP, κ.λπ.) και παρέχει δυνατότητες όπως συνδέσμους μεταξύ κάθε πληροφορίας, ημερομηνίες πρώτης και τελευταίας εμφάνισης, επίπεδα εμπιστοσύνης και πεδία περιγραφής. Το εργαλείο μπορεί να χρησιμοποιήσει το πλαίσιο MITRE ATTACK (μέσω ειδικής σύνδεσης) για να βοηθήσει στη δομή των δεδομένων. Ο χρήστης μπορεί επίσης να επιλέξει να χρησιμοποιήσει τα δικά του σύνολα δεδομένων.

Όταν τα δεδομένα ενσωματωθούν στο OpenCTI από τους αναλυτές, ενδέχεται να δημιουργηθούν νέες σχέσεις από τις υπάρχουσες για να διευκολυνθεί η κατανόηση και η αναπαράσταση αυτών των πληροφοριών. Αυτό επιτρέπει στον χρήστη να εξαγάγει και να αξιοποιήσει σημαντικές γνώσεις από τα μη επεξεργασμένα δεδομένα.

Το OpenCTI επιτρέπει όχι μόνο τις εισαγωγές αλλά και τις εξαγωγές δεδομένων σε διαφορετικές μορφές (δέσμες CSV, STIX2 κ.λπ.). Οι σύνδεσμοι βρίσκονται υπό ανάπτυξη για να επιταχύνουν τις αλληλεπιδράσεις μεταξύ του εργαλείου και άλλων πλατφορμών.

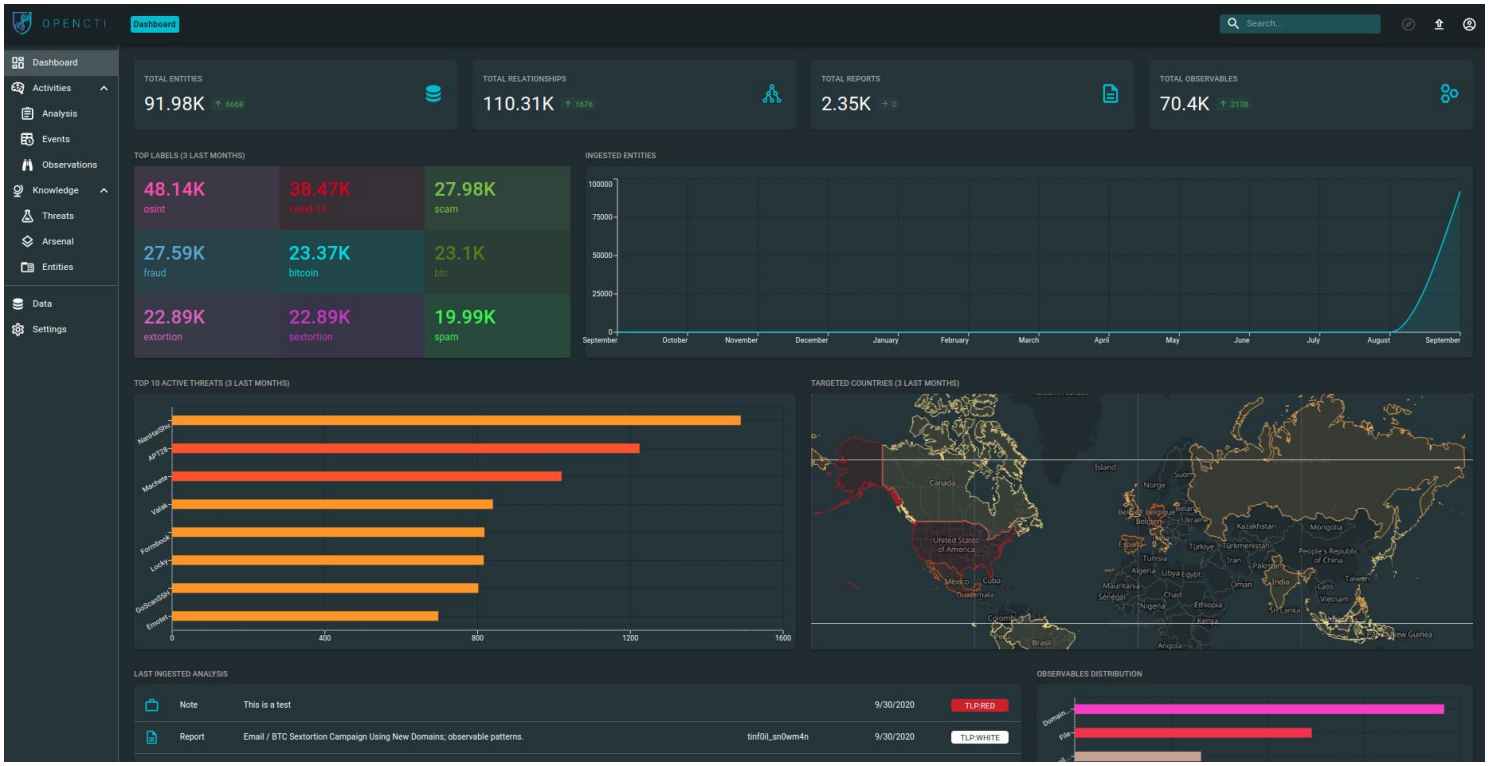
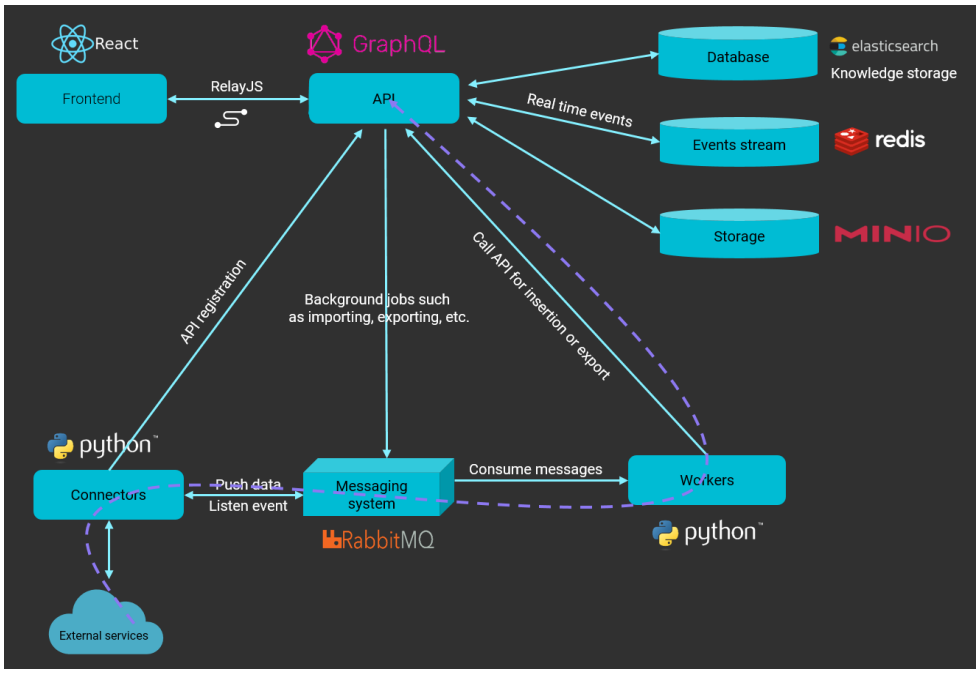


Figure 3: openCTI dashboard

2.2.4 Knowledge management

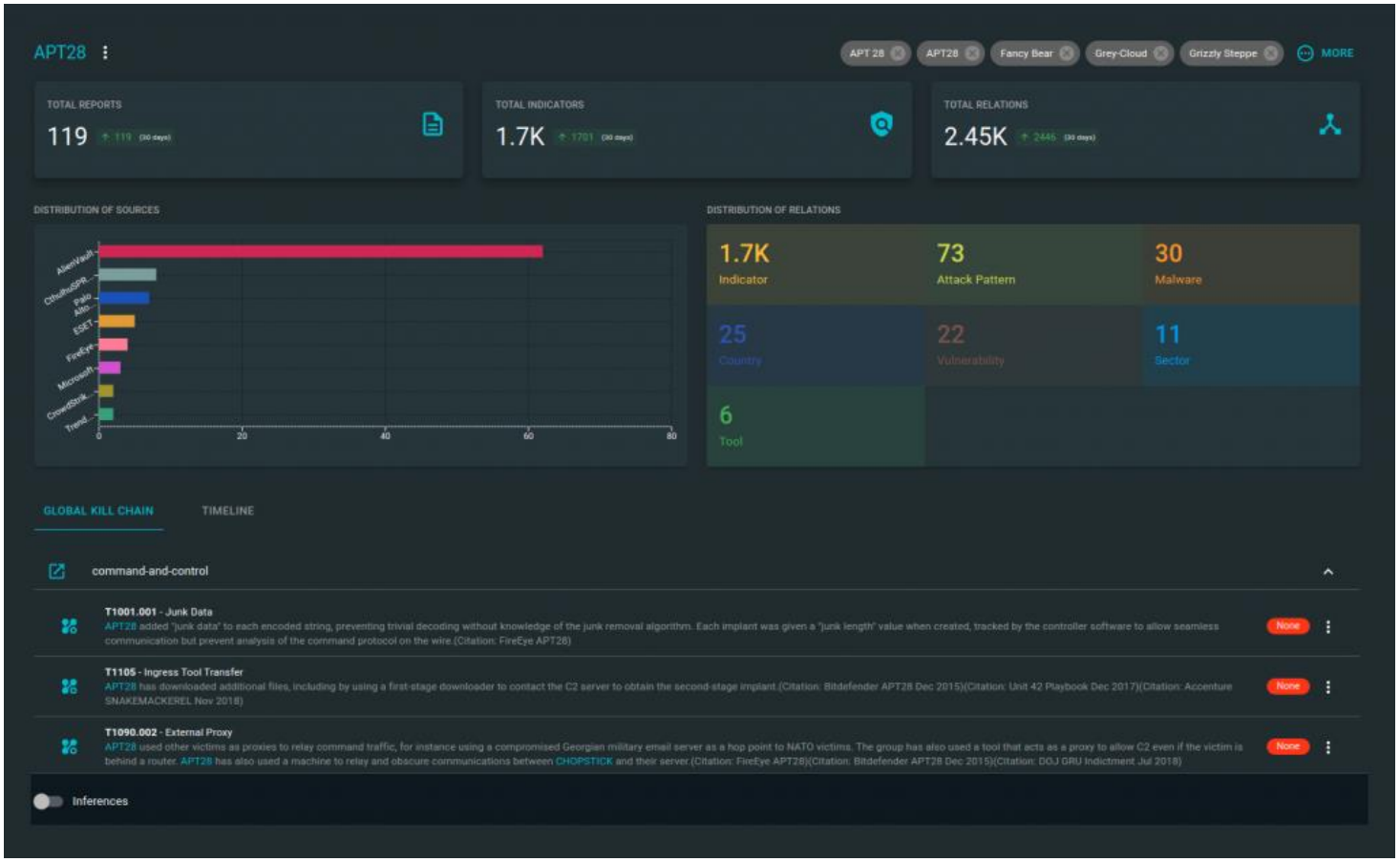
Ο κύριος στόχος της πλατφόρμας OpenCTI είναι η παροχή μιας ισχυρής βάσης δεδομένων διαχείρισης γνώσης με ένα ενισχυμένο σχήμα ειδικά προσαρμοσμένο για τη χρήση πληροφοριών για την απειλή στον κυβερνοχώρο. Με τα πολλαπλά εργαλεία και δυνατότητες προβολής που προσφέρει η πλατφόρμα, οι αναλυτές μπορούν να εξερευνήσουν ολόκληρο το σύνολο δεδομένων περιδιαβαίνοντας την πλατφόρμα μεταξύ οντοτήτων και σχέσεων.



2.2.5 Data visualization

Το OpenCTI επιτρέπει στους αναλυτές να απεικονίζουν οποιαδήποτε οντότητα και τις σχέσεις της. Διατίθενται πολλές προβολές, καθώς και ένα σύστημα ανάλυσης που βασίζεται σε δυναμικά widget. Για παράδειγμα, οι χρήστες μπορούν να συγκρίνουν τη θυματολογία (victimology) δύο διαφορετικών συνόλων εισβολής.

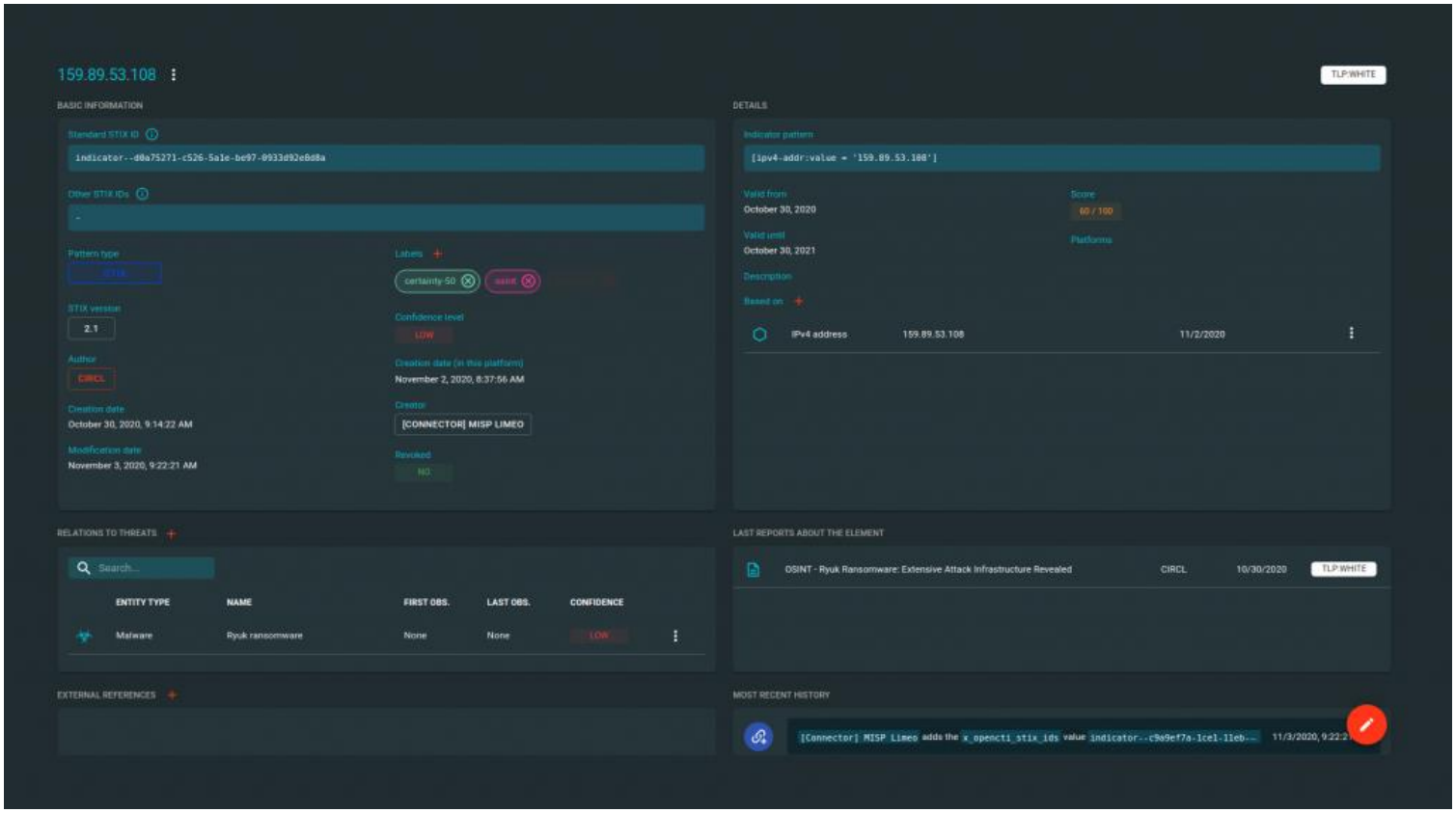
Στο μέλλον, σύμφωνα με τους προγραμματιστές, ο χάρτης πορείας OpenCTI θα περιλαμβάνει την ανάπτυξη μιας πλήρους ικανότητας έρευνας, επιτρέποντας στους αναλυτές να εξερευνήσουν ολόκληρο το γράφημα γνώσεων περιδιαβαίνοντας τις οντότητες σε έναν ενοποιημένο χώρο.



2.2.6 Observables and indicators context

Ο στόχος του OpenCTI είναι να αποτελεί ένα ολοκληρωμένο εργαλείο που επιτρέπει στους χρήστες να αξιοποιούν τεχνικές (όπως TTP) και μη τεχνικές πληροφορίες (όπως προτεινόμενη απόδοση, θύμα κλπ.) ενώ συνδέουν κάθε κομμάτι πληροφοριών με την κύρια πηγή τους (μια αναφορά , ένα συμβάν MISP, κ.λπ.).

Όλοι οι δείκτες συνδέονται με απειλές με όλες τις πληροφορίες που χρειάζονται οι αναλυτές για να κατανοήσουν πλήρως την κατάσταση, τον ρόλο που διαδραματίζουν τα παρατηρήσιμα σχετικά με την απειλή, την πηγή των πληροφοριών και τη βαθμολογία κακόβουλης συμπεριφοράς.



2.3 CIF

Το Collective Intelligence Framework (CIF) δημιουργήθηκε για την αποθήκευση πληροφοριών και πληροφοριών ασφαλείας σε ένα μοναδικό repository που δημιουργήθηκε από το Κέντρο Ανταλλαγής και Ανάλυσης Πληροφοριών Δικτύου Έρευνας και Εκπαίδευσης (REN-ISAC). Ο κύριος στόχος του έργου είναι η συλλογή δεδομένων που σχετίζονται με την ασφάλεια από πολλές πηγές και η παροχή μηχανισμών για την αποτελεσματική αναζήτηση, συσχέτιση και κοινή χρήση αυτών των δεδομένων. Το CIF εξελίχθηκε από το Σύστημα Εκδηλώσεων Ασφαλείας – ένα έργο με παρόμοιους στόχους, που αναπτύχθηκε επίσης από το REN-ISAC– και χρηματοδοτείται επί του παρόντος μέσω επιχορήγησης του Εθνικού Επιστημονικού Ιδρύματος (NSF).

Το CIF εφαρμόζει εσωτερικά το IODEF. Η υιοθέτηση του IODEF σημαίνει ότι κάθε στοιχείο των πληροφοριών που αποτελεί μέρος μιας αναφοράς συμβάντων έχει σαφώς καθορισμένη σημασιολογία. Το σύστημα δημιουργεί περιοδικά ροές πρόσφατων αναφορών για κάθε τύπο απειλής με βάση τα μέσα που μπορούν να χρησιμοποιηθούν για τον προσδιορισμό της, όπως μια διεύθυνση IP, μια διεύθυνση URL ή ένα κρυπτογραφικό κατακερματισμό. Το CIF εκτελεί περιοδικά ένα σύνολο ρουτίνων εμπλουτισμού δεδομένων (analytics) σε πρόσφατα συλλεγόμενα συμβάντα. Το CIF ενσωματώνεται επίσης με την υπηρεσία Team Cymru Hash Registry για τον έλεγχο hashes κακόβουλου λογισμικού, αναζητά καταχωρήσεις στη βάση δεδομένων Spamhaus και χρησιμοποιεί κανονική υποδομή DNS για εξαγωγή διευθύνσεων και διακομιστών ονομάτων (A και NSrecords) για τομείς.

Πάνω από 1000 χρήστες βρίσκονται στη λίστα αλληλογραφίας CIF, συμπεριλαμβανομένων εθνικών και ιδιωτικών CERT, ιδιωτικών ερευνητών και εταιρικών ομάδων ασφαλείας από όλο τον κόσμο. Επίσης στις αναπτυσσόμενες χώρες τα CERT στρέφονται στην πλατφόρμα CIF για να λάβουν πληροφορίες. Σε αντίθεση με άλλες πλατφόρμες

ανταλλαγής πληροφοριών, οι οποίες βασίζονται σε διάφορες «γλώσσες απειλής», η CIF επικεντρώνεται στη λήψη των δεδομένων σε μορφή εξόδου που προτιμά ο χρήστης, είτε πρόκειται για ζεύγη STIX, JSON, CSV ή Snort.

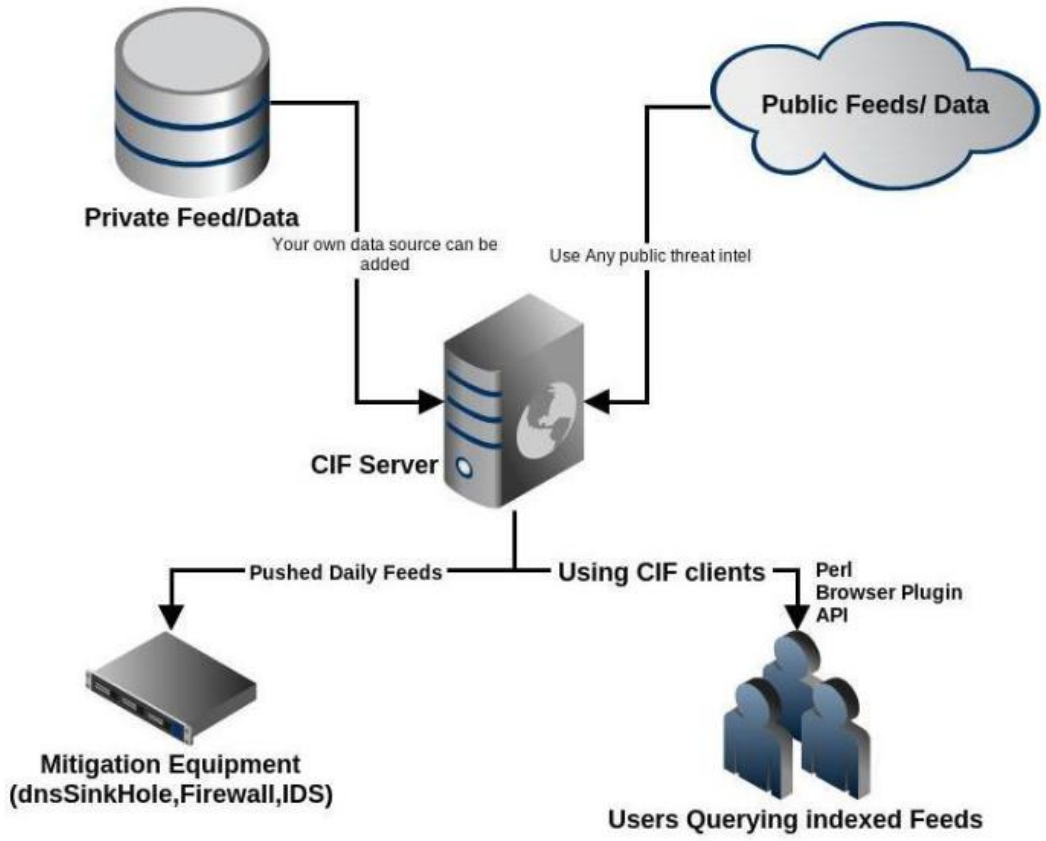


Figure 4: CIF architecture

2.4 CRITs

Τα CRITs είναι ένα διαδικτυακό εργαλείο που συνδυάζει μια μηχανή ανάλυσης με μια βάση δεδομένων απειλών στον κυβερνοχώρο που όχι μόνο χρησιμεύει ως σημείο αποθήκευσης δεδομένων που αφορούν επιθέσεις μέσω κακόβουλου λογισμικού, αλλά παρέχει επίσης στους αναλυτές μια ισχυρή πλατφόρμα για τη διεξαγωγή αναλύσεων, και τη συσχέτιση κακόβουλου λογισμικού. Αυτές οι αναλύσεις και συσχετισμοί μπορούν επίσης να αποθηκευτούν και να αξιοποιηθούν εντός CRITs. Η πλατφόρμα CRITs χρησιμοποιεί μια απλή αλλά πολύ χρήσιμη ιεραρχία για τη δομή πληροφοριών σχετικά με την απειλή στον κυβερνοχώρο. Αυτή η δομή δίνει στους αναλυτές τη δυνατότητα να «περιδιαβαίνουν» στα metadata για να ανακαλύψουν παλιότερο άγνωστο σχετικό περιεχόμενο. Η πλατφόρμα έχει σχεδιαστεί για να λειτουργούν σε αρχιτεκτονική 64-bit του Ubuntu ή του RHEL6 χρησιμοποιώντας το Python 2.7. Η εγκατάσταση έχει υποστήριξη beta για OSX χρησιμοποιώντας το Homebrew.

Υπάρχουν γενικά δύο τύποι υπηρεσιών που προσφέρει το CRIT:

- Analytic services
- Tabbed services.

Analytic services

Αυτές οι υπηρεσίες έχουν σχεδιαστεί ώστε:

a) Ο αναλυτής να μπορεί τρέξει ένα εργαλείο, να καταγράψει τα αποτελέσματα και να αποθηκεύσει τα αποτελέσματα.

β) Να υποβάλει τα δεδομένα σε μια υπηρεσία, να καταγράψει και να αποθηκεύσει τα αποτελεσμάτα στη πλατφόρμα.

γ) Να υποβάλει τα δεδομένα σε άλλο σύστημα που θα ενημερώσει το CRITs με τα αποτελέσματα όταν γίνουν διαθέσιμα.

Tabbed Services

Αυτές οι υπηρεσίες παρέχουν γενικά μια πιο διαδραστική εμπειρία για τον χρήστη. Τα χαρακτηριστικά που αντιμετωπίζουν τείνουν να μην αποθηκεύουν αποτελέσματα ανάλυσης, αλλά εξακολουθούν να παρέχουν στο χρήστη χρήσιμους τρόπους αλληλεπίδρασης με δεδομένα στο σύστημα.

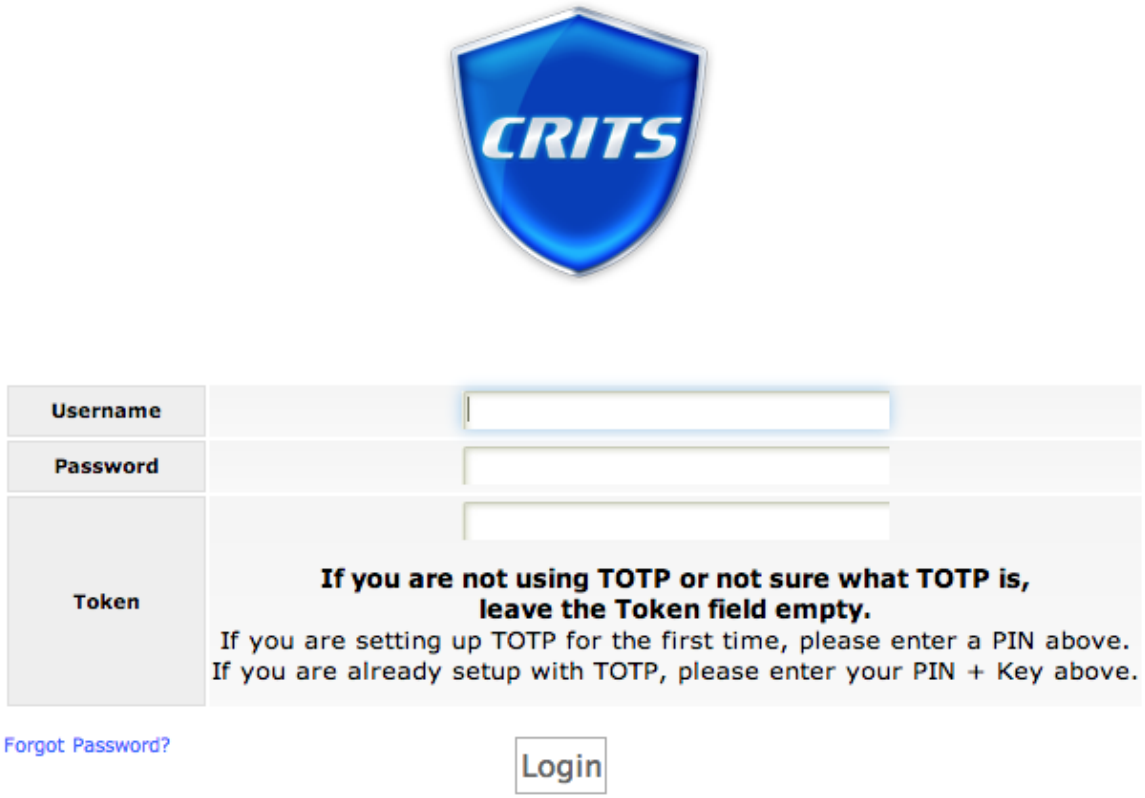


Figure 5: CRITs start page

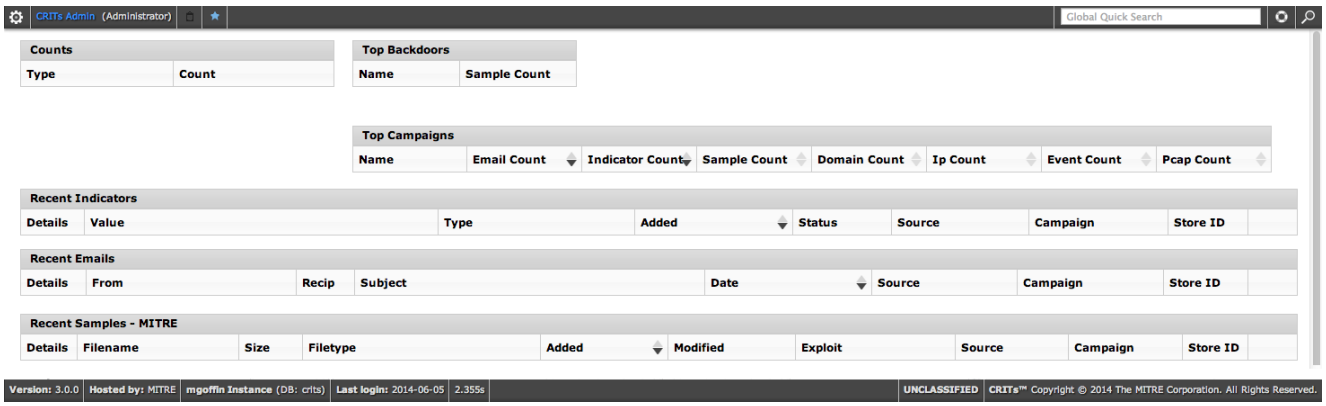


Figure 6: CRITs dashboard

Η ενότητα **Counts/Μετρήσεις** είναι μια γενική επισκόπηση της ποσότητας ορισμένων δεδομένων στο σύστημα. Αυτά τα δεδομένα καθορίζονται από mapReduce jobs που εκτελούνται σε ώρες που ορίζονται από τον διαχειριστή του συστήματος.

Η ενότητα **Top Backdoors** δείχνει τα πιο δημοφιλή backdoors που έχουν ανατεθεί σε δείγματα στη βάση δεδομένων.

Η ενότητα **Top Campaigns** δείχνει μερικές από τις πιο δημοφιλείς καμπάνιες που έχει προσθέσει ο χρήστης στο CRITs, καθώς και πόσα από τα αντικείμενα ανώτερου επιπέδου έχουν αποδοθεί σε αυτές τις campaigns.

Οι πρόσφατες ενότητες(recent sections) δείχνουν μερικά από τα νέα αντικείμενα ανώτερου επιπέδου που προστέθηκαν στο CRITs που μπορεί να σας ενδιαφέρουν

CRITs key objects

Actors

Ο Actor στο CRITs μπορεί να σημαίνει δύο πράγματα. Ένα άτομο ή μια οργανωμένη ομάδα ατόμων.

Τα CRITs επιτρέπουν να παρακολουθούμε Actors και να συσχετίζουμε σε αυτούς μεταδεδομένα χαρακτηριστικών. Μπορούμε να χαρτογραφήσουμε πολύπλοκους οργανισμούς, συσχετίζοντας τους Actors με σχέσεις. Για παράδειγμα:

Δημιουργούμε έναν Actor με το όνομα "Evil Organization".

Δημιουργούμε έναν Actor με το όνομα "Evil Actor"

Χρησιμοποιούμε τη λειτουργία "Σχέσεις" για να σημειώσουμε ότι το "Evil Actor" περιλαμβάνεται στο "Evil Organization".

Campaigns

Τα Campaigns ορίζεται ως μια ομάδα σχετικών γεγονότων / συμβάντων / δεικτών / κακόβουλου λογισμικού / κ.λπ. που παρατηρούνται με την πάροδο του χρόνου για τα οποία μπορεί να οριστεί ένα σαφές σύνολο TTP (Τακτική, Τεχνικές και Διαδικασίες).

Τα CRIT επιτρέπουν να παρακολουθούμε Campaign και να τις συσχετίζουμε / αποδίδουμε με οποιοδήποτε άλλο αντικείμενο ανώτερου επιπέδου στο σύστημα..

Υπάρχουν δύο τρόποι για να γίνει αυτό:

Χρησιμοποιούμε τη δυνατότητα Relationships και συσχετίζουμε ένα αντικείμενο ανώτατου επιπέδου με το Campaign.

Η πιο ενδεδειγμένη μέθοδος είναι να χρησιμοποιήσουμε την ενότητα Campaign του αντικειμένου ανώτερου επιπέδου και να αποδώσουμε εκεί την Καμπάνια.

PCAPs

Η συλλογή PCAPs επιτρέπει να ανεβάσουμε μια μικρή, εντοπισμένη κακόβουλη κίνηση δικτύου στο CRITs για περαιτέρω ανάλυση. Σε πολλές περιπτώσεις, είναι σημαντικό να αποθηκεύσουμε την κυκλοφορία δικτύου για μακροπρόθεσμη ανάλυση. Αυτή η δυνατότητα του CRITs θα επιτρέψει να αποθηκεύσουμε και να συσχετίσουμε αυτήν την κυκλοφορία δικτύου με άλλα αντικείμενα που έχουμε προσθέσει.

Υπάρχουν πολλές υπηρεσίες που έχουν αναπτυχθεί για την αξιοποίηση των PCAP.

Δύο σημαντικές τέτοιες υπηρεσίες είναι:

MetaCap

Το MetaCap παρέχει μια λειτουργία MetaCap Tcpdump που επιτρέπει να εκτελούμε το PCAP μέσω του tcpdump (με μερικές επιλογές διαμόρφωσης) και να βλέπουμε τα αποτελέσματα με UI. Υπάρχει επίσης το MetaCap Viewer που δημιουργεί ένα αρχείο PDML χρησιμοποιώντας το tshark (από το Wireshark). Χρησιμοποιεί αυτό το αρχείο PDML για τη δημιουργία HTML, δίνοντάς μια τύπου wireshark προβολή του PCAP απευθείας από το περιβάλλον εργασίας χρήστη.

Chopshop

Το Chopshop είναι ένα εργαλείο ανοιχτού κώδικα για την αποκρυπτογράφηση της κίνησης δικτύου. Η υπηρεσία Chopshop στο CRITs επιτρέπει να αξιοποιήσουμε τη δύναμη του Chopshop απευθείας από το περιβάλλον χρήστη. Έρχεται επίσης με μια λειτουργία Filecarver για PCAP. Αυτό επιτρέπει να επεξεργαστούμε αιτήματα HTTP, HTTP Responses, SMTP και Raw TCP και, στη συνέχεια, να προσθέσουμε το περιεχόμενο που έχει προκύψει πίσω σε CRITs και να συσχετιστεί αυτόματα με το PCAP.

3 Αξιολόγηση και Σύγκριση

Η αξιολόγηση και η σύγκριση συνοψίζονται στον Πίνακα 2 και 3 και πραγματοποιήθηκε λαμβάνοντας υπόψη τα ακόλουθα κριτήρια:

Μορφή αρχείων εισαγωγής/εξαγωγής: Τα MISP, CRITs και το OpenCTI μπορούν να λειτουργήσουν με μεγάλο αριθμό μορφών αρχείων (π.χ. PDF, doc, xls, txt, JSON, XML, STIX). Το MISP υποστηρίζει ένα ad-hoc πρότυπο για την εκπροσώπηση του Threat Intelligence (μια προσαρμοσμένη μορφή JSON12) και των βασικών ενσωματωμένων δυνατοτήτων για τη μετατροπή STIXv.2.013. Επιτρέπει επίσης την προσθήκη ενοτήτων για εισαγωγή / εξαγωγή ad-hoc χωρίς τροποποίηση των βασικών λειτουργιών. Το CIF δεν είναι τόσο ευέλικτο όσο οι προηγούμενες τρείς TIPs, ειδικά εάν ληφθούν υπόψη συγκεκριμένα πρότυπα (π.χ. STIX).

Ενσωμάτωση με / Εξαγωγή σε τυπικά εργαλεία ασφαλείας: Το MISP και το openCTI επιτρέπει την εύκολη αλληλεπίδραση με Συστήματα Ανίχνευσης Εισβολής (IDS) και SIEM, και περιέχει εύκαμπτα REST API για ενσωμάτωση εσωτερικών λύσεων στην πλατφόρμα. Το CIF είναι επίσης μια βιώσιμη πλατφόρμα για ενσωμάτωση με IDS και SIEM, αν και λιγότερο ευέλικτη από το MISP. Τα CRITs είναι ένα τεράστιο αποθετήριο TI, που δεν έχει σχεδιαστεί ειδικά για αλληλεπίδραση με συστήματα όπως SIEM και IDS, ωστόσο η ευελιξία του επιτρέπει την κατασκευή ad-hoc λύσεων για αυτούς τους σκοπούς.

Υποστήριξη συνεργασίας: Το MISP επιτρέπει την κεντρική υποστήριξη, κοινοποιώντας το ίδιο instance σε μια κοινότητα στην οποία υπάρχει εμπιστοσύνη και αποκεντρωμένη υποστήριξη, όταν πολλές περιπτώσεις αλληλεπιδρούν με τρόπο peer-to-peer.. Η CIF επιτρέπει τη χρήση ενός ιδιωτικού instance και την εφαρμογή ενός κοινού instance μέσω μιας κεντρικής υπηρεσίας. Τα CRITs και το OpenCTI επιτρέπουν τη χρήση ενός ιδιωτικού ή ενός κοινού instance στο πλαίσιο μιας αξιόπιστης κοινότητας. Ωστόσο, αυτό που συμπέρανα είναι ότι τα CRITs έχουν πολύ κακές ενσωματωμένες δυνατότητες κοινής χρήσης.

Πρότυπα ανταλλαγής δεδομένων: Τα MISP, openCTI και CRITs είναι σε θέση να υποστηρίξουν πολλά διαφορετικά πρότυπα, συμπεριλαμβανομένων των STIX και TAXII. Το CIF, έχει σχεδιαστεί για να λειτουργεί με άλλα CIF instances χρησιμοποιώντας ιδιωτικές λύσεις για την κάλυψη απαιτήσεων υψηλής απόδοσης με μερική ή καθόλου υποστήριξη σε πρότυπα όπως ως STIX και TAXII.

Δυνατότητες ανάλυσης: οι υψηλές δυνατότητες ανάλυσης θα μπορούσαμε να πούμε ότι είναι ένα τρωτό σημείο για όλες τις τρέχουσες πλατφόρμες. Μόνο η πλατφόρμα CRITs θα μπορούσαμε να πούμε ότι αποτελεί ένα κεντρικο repository για συνεργατική ανάλυση αλλά σίγουρα δε μπορούμε να ισχυριστούμε ότι είναι μια πλατφόρμα κοινής χρήσης. Έχει όμως καλύτερες ενσωματωμένες δυνατότητες ανάλυσης σε σύγκριση με τη MISP και τη CIF.

Δημιουργία γραφημάτων: οι δυνατότητες οπτικοποίησης σχετίζονται αυστηρά με την ανάλυση των προαναφερθεισών χαρακτηριστικών και μπορεί εύκολα κανείς να βγάλει το ίδιο συμπέρασμα. Ότι δηλαδή, αυτός είναι ένας ακόμα περιορισμός των τρεχόντων TIPs.

Άδεια: όλες οι TIPs που εξετάζονται σε αυτήν την εργασία κυκλοφορούν με άδειες ανοιχτού κώδικα.

Απαιτήσεις υλικού: Αυτό που συμπέρανα είναι ότι οι πλατφόρμες MISP, CRITs και OpenCTI έχουν πολύ παρόμοιες απαιτήσεις όσον αφορά τη μνήμη RAM και το μέγεθος του σκληρού δίσκου. Το CIF, σε αντίθεση, έχει υψηλότερες απαιτήσεις, ειδικά όσον αφορά τις δυνατότητες επεξεργασίας.

Table 2: Evaluation of TIPs

Evaluated criteria	MISP	CIF	CRITs	openCTI
Import/Export Format	Advanced	Average	Advanced	Advanced
Integration Capabilities	Advanced	Advanced	Average	Average
Support of Collaboration	Advanced	Advanced	Average	Advanced
Data Exchange Std.	Advanced	Average	Average	Advanced
Analysis Capabilities	Average	Average	Advanced	Average
Graph Generation	Average	Average	Advanced	Average
License	Advanced	Advanced	Advanced	Advanced
Hardware Requirements	Advanced	Advanced	Advanced	Advanced

Table 3: Evaluation of TIPs

	MISP	OpenCTI	CIF	CRITs
Import formats	OpenIOC, STIX, CybOX,JSON, CSV, XML	STIX, CybOX, JSON, CSV,XML	XML, JSON, Zip	CSV, STIX, CybOX
Export Formats	MISP, OpenIOC, CSV, XML,JSON	CSV, STIX	CSV, JSON, HTML, XLS	CSV, STIX, CybOX
Graphic visualization	General and intuitivedashboard and relationshipgraphics	Diverse dashboards andSTIXv2 based graphics	Command line interfacewith possible integrationwith visualization tool	Simple dashboard andan extension service forgenerating relationshipgraphics
Correlation	Automatic for every datain platform	Automatic for every datain platform	Not addressed	Necessary an extensionservic
Classification	Based on the type ofthe indicato	Based on STIXv2 objects	Based on the type ofthe indicato	Based on a proposed datamodel
Intergation	DS, SIEMs and other TIplatforms	Other TI platforms	DSs (Snort, Splunk, Bro,Bind)	Not addressed
Sharing method	Reliable group of instancesusing different model	Particular instance to sharebetween user	Reliable group of instancesusing a centralized se	eliable group of instance
Documentation	Extensive and wellelaborated	Extensive and wellelaborated	Limited detail with succinctdescriptions	Limited detail with succinctdescriptions
License model	Open Source (GNU GeneralPublic License	Open Source (GNU GeneralPublic License	Open Source (GNU GeneralPublic License	Open Source (GNU GeneralPublic License

Η ανάλυση των πλατφορμών που περιγράφηκαν προηγουμένως όπως και μια σύντομη ενασχόληση μερικών ακόμη TIPs που είναι διαδεδομένες οδήγησαν στα ακόλουθα βασικά ευρήματα:

Το STIX είναι το πιο διαδεδομένο πρότυπο:

Το πλαίσιο των προτύπων που είναι διαθέσιμο για την περιγραφή των πληροφοριών σχετικά με τις απειλές είναι αρκετά μικρό σε σύγκριση με τον αριθμό των διαθέσιμων πλατφορμών TI. Η ανάλυση έδειξε ότι οι περισσότερες πλατφόρμες threat intelligence βασίζονται σε πρότυπα όπως OpenIOC, STIX και IODEF. Πάνω από τα δύο τρίτα των πλατφορμών παρέχουν άμεσες δυνατότητες εισαγωγής και εξαγωγής που υποστηρίζουν τα προαναφερόμενα πρότυπα. Αναλυτικά, ορισμένες από τις πλατφόρμες βασίζονται στο STIX, λιγότερες στο OpenIOC, μερικές και στις δύο και μόνο μία πλατφόρμα στο IODEF. Για παράδειγμα, η πλατφόρμα Open Threat Exchange (OTX) παρέχει λειτουργίες STIX καθώς και OpenIOC εισαγωγής και εξαγωγής. Διαπιστώθηκε ότι το STIX είναι το πιο συχνά χρησιμοποιούμενο πρότυπο και μπορεί να θεωρηθεί ως το de-facto πρότυπο για τις TIPs. Βασίζεται στα πρότυπα CybOX, CAPEC, MAEC και CVRF και παρέχει μια αρχιτεκτονική που συνδυάζει ένα διαφορετικό σύνολο πληροφοριών σχετικά με τις απειλές στον κυβερνοχώρο.

Η αρχιτεκτονική STIX αποτελείται από οκτώ βασικές έννοιες απειλών στον κυβερνοχώρο ως ανεξάρτητες και επαναχρησιμοποιήσιμες constructs και λαμβάνει υπόψη τη σχέση τους. Οι οκτώ κατασκευές είναι οι εξής:

- Cyber Observables (π.χ. διευθύνσεις IP, ονόματα αρχείων, κατακερματισμούς),
- Δείκτες
- Συμβάντα,
- Τεχνικές και διαδικασίες αντίστροφης τακτικής (συμπεριλαμβανομένων μοτίβων επίθεσης, αλυσίδων δολοφονίας κ.λπ.),
- Εκμετάλλευση στόχων (π.χ. ευπάθειες, αδυναμίες),
- Μαθήματα δράσης (π.χ. απάντηση συμβάντων, στρατηγικές μετριασμού),
- Εκστρατείες Cyber Attack και
- Cyber Threat Actors.

Αυτά τα constructs μπορούν - τουλάχιστον εν μέρει - να βρεθούν σε όλες τις πλατφόρμες. Επιπλέον, αυτές οι κατασκευές μπορούν να χρησιμοποιηθούν για την παροχή σημαντικών εισροών σε διαδικασίες ασφάλειας πληροφοριών, όπως πρόληψη, ανίχνευση ή απόκριση.

Η πλειονότητα των πλατφορμών είναι περιορισμένης πρόσβασης (closed source):

Υπάρχουν έξι ελεύθερα διαθέσιμες στην αγορά TIPs, από τις οποίες τέσσερις είναι εργαλεία ανοιχτού κώδικα που διανέμονται βάσει της άδειας GNU General Public License, συμπεριλαμβανομένης της πλατφόρμας MISP, CIF, CRITs και openCTI. Υπάρχει επίσης η πλατφόρμα Open Threat Exchange (OTX) και SoltraEdge που είναι δωρεάν για χρήση, αλλά δεν κυκλοφόρησαν με άδεια ανοιχτού κώδικα. Οι υπόλοιπες πλατφόρμες είναι closed source.

Το ακαδημαϊκό και εμπορικό ενδιαφέρον για τις TIPs αυξάνεται:

Τον Νοέμβριο του 2011, το πρότυπο OpenIOC κυκλοφόρησε και έθεσε τα θεμέλια για την ανταλλαγή TI. Μεταξύ του 2010 και του 2012 δόθηκε ελάχιστη προσοχή στην απειλή της ανταλλαγής πληροφοριών στην έρευνα και την πρακτική. Το 2013 παρουσιάστηκε μια πρώτη ιδέα μιας πλατφόρμας διαχείρισης πληροφοριών απειλής. Μεταξύ 2013 και 2014 κυκλοφόρησαν τα ολοκληρωμένα πρότυπα STIX και TAXII. Από τότε, ο αριθμός των δημοσιεύσεων και των vendors που παρέχουν τέτοιες πλατφόρμες(TIPs) έχει αυξηθεί σημαντικά. Για παράδειγμα, ο συνολικός αριθμός των δημοσιεύσεων το 2015 ήταν πάνω από τριπλάσιο σε σύγκριση με το 2014 και το 2018 ήταν τριπλάσιος από το 2015. Καθώς η αγορά τέτοιων πλατφορμών είναι σχετικά νέα και εξακολουθεί να αναπτύσσεται, αναμένεται ότι ο αριθμός των πλατφορμών και των επιστημονικών δημοσιεύσεων θα συνεχίσει να αυξάνεται στο εγγύς μέλλον.

Στις TIPs υπάρχουν ακόμα πολλές μη αυτοματοποιημένες διεργασίες:

Οι TIPs παρέχουν περιορισμένες αυτοματοποιημένες δυνατότητες ενσωμάτωσης και επεξεργασίας δεδομένων. Επομένως, απαιτείται πολύ μη αυτόματη αλληλεπίδραση χρήστη για τον διαμερισμό και απόκτηση πολύτιμης νοημοσύνης. Δεδομένου ότι οι περισσότερες πλατφόρμες δεν διαθέτουν αυτοματοποιημένα μέσα συλλογής πληροφοριών και το πιο σημαντικό, νοημοσύνης, αυτές οι δραστηριότητες απαιτούν χειροκίνητη προσπάθεια. Εκτός από τις κλασικές λειτουργίες εισαγωγής αρχείων, τα περισσότερα TIPs στερούνται φιλικών προς τον χρήστη διεπαφών για γρήγορη προσθήκη νέων αρχείων δεδομένων και απαιτούν πολλές αλληλεπιδράσεις χρηστών για την επίτευξη του επιθυμητού στόχου.

4 Περιορισμοί

Σε αυτήν την ενότητα, θα παρουσιαστούν οι περιορισμοί που σχετίζονται με την τρέχουσα κατάσταση και τη χρήση των πλατφορμών Threat Intelligence.

Οι πληροφορίες που κοινοποιούνται μέσω των TIPs είναι πολύ ογκώδεις

Σύμφωνα με μια πρόσφατη έρευνα στην οποία έλαβαν μέρος εργαζόμενοι στο Cyber Security, μεγάλο ποσοστό των ερωτηθέντων απάντησε ότι οι πληροφορίες απειλής που κοινοποιούνται συχνά είναι πολύ ογκώδεις και πολύπλοκες ώστε να ληφθούν τα κατάλληλα μέτρα. Ένα από τα προβλήματα που απεικονίζει αυτό είναι η υπερφόρτωση πληροφοριών απειλών που κοινοποιούνται μέσω ανοιχτού κώδικα, εμπορικών πηγών καθώς και των ιδιωτικών κοινοτήτων και των ISACs(*Information Sharing and Analysis Centers*). Ο συνδυασμός πληροφοριών για απειλές από διάφορες πηγές και βιομηχανίες καθιστά δύσκολη την εύρεση της σχετικής ευφυΐας και καθιστά δύσκολη την εκμετάλλευση αυτών.

Περιορισμένη χρησιμοποίηση της τεχνολογίας

Η προαναφερθέν πολυπλοκότητα των διαμοιρασμένων πληροφοριών σχετικά με τις απειλές σε συνδυασμό με τα εργαλεία απειλών και προσδιορισμού συνάφειας περιορίζουν την προσβασιμότητα και κατανόηση των δεδομένων. Η περιορισμένη τεχνολογία αποτρέπει στους τελικούς χρήστες να διευκολυνθούν και να μπορούν εύκολα να κατανοούν ποιες απ’ τις πληροφορίες που λαμβάνουν είναι σημαντικές γ’ αυτούς και ποιες όχι. Επί του παρόντος, αυτή η διαδικασία γίνεται χειροκίνητα, με πολύ περίπλοκο τρόπο και εξαρτάται από τον αναλυτή. Δυνατότητες των

TIPs που θα μπορούσαν να βοηθήσουν τους αναλυτές είναι η προηγμένη αναζήτηση, το προσαρμοσμένο φιλτράρισμα, οι μηχανές προτάσεων, (ημι-) αυτοματοποιημένη δοκιμή απειλών και η ροή εργασιών δημιουργίας δοκιμών.

Παρ 'όλα αυτά, οι παραπάνω δυνατότητες δεν παρέχονται σε πολλές περιπτώσεις και οι τελικοί χρήστες αντιμετωπίζουν το πρόβλημα της διαχείρισης και ιεράρχησης των αμέτρητων πληροφοριών απειλής που λαμβάνονται. Κάποιος θα υποστήριζε ότι ενώ τα προηγούμενα χρόνια το κύριο μέλημα ήταν η παροχή κινήτρων, προτύπων και εργαλείων για την ανταλλαγή πληροφοριών, επί του παρόντος το πρόβλημα έχει μετακινηθεί σε αποτελεσματική διαχείριση πληροφοριών απειλών.

Δείκτες συμβιβασμού(IoCs)

Μέσω της έρευνας διαπιστώθηκε ότι η πλειονότητα των πλατφορμών επικεντρώνεται στους τακτικούς δείκτες συμβιβασμού. Υπάρχουν περιπτώσεις που λείπει το πλαίσιο γύρω από τους τακτικούς δείκτες και αυτό είναι κάτι που εμποδίζει το έργο που πρέπει να γίνει από αναλυτές CTI και τους παραλήπτες των πληροφοριών. Κατά την διαδικασία ανταλλαγής πληροφοριών, τα τυποποιημένα πρωτόκολλα επικοινωνίας δεν χρησιμοποιούνται συνήθως και ανταλλάσσονται ως επί το πλείστων μη δομημένα PDF ή CSV. Από την άλλη πλευρά, όποτε χρησιμοποιούνται πρότυπα για κοινή χρήση πληροφοριών απειλών, τότε τα STIX 1.x, OpenIOC και MISP JSON είναι τα πιο συνηθισμένα. Έχει παρατηρηθεί ότι αυτά των πρότυπα δεν αξιοποιούνται σωστά όσον αφορά την ανταλλαγή πληροφοριών. Για παράδειγμα, το STIX 1.x είναι ένα αρκετά εκφραστικό μοντέλο δεδομένων σχετικά με πληροφορίες για τις απειλές στον κυβερνοχώρο και έχει κάποιες βασικές κατασκευές(constructs) που περιλαμβάνουν τη γλώσσα STIX 1.x τα οποία θα συζητηθούν αργότερα. Ωστόσο, έχει παρατηρηθεί ότι τα περισσότερα από τα εργαλεία μοιράζονται δείκτες συμβιβασμού που μπορούν να περιγραφούν από δύο μόνο κατασκευές του προτύπου STIX 1.x, Indicators and Observables. Έτσι, ένας τρέχων περιορισμός είναι ότι οι τακτικοί δείκτες συμβιβασμού, μοιράζονται ως επί των πλείστων χωρίς ολοκληρωμένες πληροφορίες απειλών, ενώ συγχρόνως δε χρησιμοποιείται σωστά το μοντέλο δεδομένων STIX 1.x Ορισμένοι επαγγελματίες υποστηρίζουν επίσης ότι το STIX είναι αρκετά περίπλοκο, ότι δεν υπάρχει κοινό λεξιλόγιο για την περιγραφή TTPs και γι 'αυτό οι περισσότεροι παραγωγοί πληροφοριών επικεντρώνονται μόνο στις δύο προαναφερθείσες κατασκευές του STIX 1.x.

Αποθήκες δεδομένων

Ενώ η τεχνολογία επικεντρώνεται κυρίως στη φάση συλλογής της νοημοσύνης, οι δραστηριότητες που σχετίζονται με άλλες φάσεις του κύκλου νοημοσύνης έχουν ως επί των πλείστων παραμεληθεί. Μόνο ένα μικρό μέρος των δραστηριοτήτων που σχετίζονται με τις φάσεις Επεξεργασίας και Εκμετάλλευσης, Ανάλυσης και Παραγωγής καθώς και των φάσεων Διάδοσης θα μπορούσε να υποστηριχθεί επαρκώς από τις πλατφόρμες Threat Intelligence. Επί του παρόντος, οι πλατφόρμες Threat Intelligence παρέχουν βασικές δυνατότητες ανάλυσης, οι οποίες οδηγούν σε περιορισμό της ικανότητας των αναλυτών να διεξάγουν ολοκληρωμένη ανάλυση απειλών, να ακολουθούν τις ροές εργασιών τους και συνήθως τους αναγκάζουν να κάνουν πολλές χειροκίνητες εργασίες. Λαμβάνοντας υπόψη τον μεγάλο αριθμό πληροφοριών απειλής και τις περιορισμένες δυνατότητες ανάλυσης που παρέχονται από τις TIPs, οι περισσότερες από τις τρέχουσες πλατφόρμες καταλήγουν να είναι αποθήκες δεδομένων και όχι πλατφόρμες όπου μπορούν να κοινοποιηθούν και να αναλυθούν πληροφορίες σχετικά με τις απειλές**.**

Θέματα που σχετίζονται με την εμπιστοσύνη

Οι ερευνητές έχουν εντοπίσει προβλήματα εμπιστοσύνης που σχετίζονται με τους χρήστες και τους παρόχους πλατφόρμας. Οι οργανισμοί που συμμετέχουν σε μια πλατφόρμα Threat Intelligence (π.χ. η πλατφόρμα του ISAC), θα πρέπει να έχουν ορισμένα επίπεδα εμπιστοσύνης προς τον πάροχο της πλατφόρμας, καθώς και τους υπόλοιπους οργανισμούς και αντίστροφα. Έχουν εντοπιστεί οι παρακάτω σχέσεις εμπιστοσύνης:

- Ο οργανισμός εμπιστεύεται τον πάροχο της πλατφόρμας ότι ο χειρισμός των κοινόχρηστων πληροφοριών και των ελέγχων πρόσβασης δεν εκθέτει εμπιστευτικά δεδομένα σε μη εξουσιοδοτημένους παραλήπτες.
- Ο οργανισμός εμπιστεύεται τους υπόλοιπους συμμετέχοντες οργανισμούς ότι ο χειρισμός των κοινών πληροφοριών γίνεται σύμφωνα με ένα προκαθορισμένο πρωτόκολλο π.χ. Πρωτόκολλο σήμανσης TLP, κ.λπ.
- Ο πάροχος πλατφόρμας (προμηθευτές, ISAC κ.λπ.) και οι υπόλοιποι οργανισμοί εμπιστεύονται τον οργανισμό ότι οι πληροφορίες που κοινοποιούνται από τον οργανισμό είναι αξιόπιστες και αξιόπιστες**.**

Οι TIPs από την άλλη πλευρά, παρέχουν μηχανισμούς ελέγχους πρόσβασης κυρίως βάσει ομάδων. Οι τελικοί χρήστες TIP χρειάζονται περισσότερη ευελιξία, ώστε να μπορούν να διευκολύνουν την προσαρμόσιμη, ελεγχόμενη και πολυμερή κοινή χρήση μεταξύ αξιόπιστων μερών.

Οι προαναφερθείσες σχέσεις εμπιστοσύνης και οι περιορισμένες δυνατότητες των TIPs εισάγουν διάφορους περιορισμούς στον τρόπο με τον οποίο οι οργανισμοί αλληλεπιδρούν και συμβάλλουν σε συγκεκριμένες κοινότητες. Δηλαδή οι οργανισμοί μπορούν να επιλέξουν να μοιράζονται μόνο συγκεκριμένους τύπους δεδομένων απειλών με συγκεκριμένες κοινότητες και οργανισμούς και πλησιάζοντας πιο κοντά σε αξιόπιστες και κλειστές κοινότητες (ή ακόμη και συνδέσεις από ομοτίμους) να μοιράζονται πιο ευαίσθητα δεδομένα. Επιπλέον, οι προγραμματιστές και οι χρήστες TIP πρέπει να εξετάσουν κατά πόσον τηρούνται νέες προϋποθέσεις νομοθεσίας κατά την επεξεργασία και τη χρήση τόσο μεγάλων συνόλων δεδομένων (για παράδειγμα, υπάρχουν ανησυχίες σε σχέση με τον GDPR).

Ποιότητα κοινών δεδομένων απειλής και περιορισμοί των TIP

Η εμπιστοσύνη είναι μια ιδιότητα που σχετίζεται με την ποιότητα των κοινών πληροφοριών, κάτι που δεν παρέχεται από τις περισσότερες από τις ροές. Επιπλέον, σχετικές έρευνες επισήμαναν ότι οι περισσότερες από τις κοινόχρηστες αναφορές STIX 1.x και APT παρέχουν ελλιπείς πληροφορίες. Το περιεχόμενο, τα ποιοτικά δεδομένα και η εμπιστοσύνη στα κοινόχρηστα δεδομένα μπορούν να βοηθήσουν τους τελικούς χρήστες να αποφύγουν τα ανεπιθύμητα αποτελέσματα και να μην καταβάλουν επιπλέον προσπάθεια για την αξιολόγηση και την επαλήθευση των ληφθέντων δεδομένων. Η προέλευση των πληροφοριών έχει να κάνει με τη διασφάλιση της ποιότητας των κοινόχρηστων δεδομένων παρακολουθώντας την εξέλιξή τους και είναι ένα από τα δυσκολότερα προβλήματα στην ασφάλεια των πληροφοριών. Προηγούμενη έρευνα έχει εντοπίσει την ανάγκη τελικών χρηστών του TIP να καθοριστεί η προέλευση (και η ιχνηλασιμότητα). Επομένως, υπάρχει ανάγκη παροχής, παρακολούθησης και διαχείρισης πληροφοριών εμπιστοσύνης και προέλευσης (ως metadata των κοινών δεδομένων) από διαφορετικές οπτικές γωνίες (καταναλωτής, παραγωγός και κοινότητα). Τα υπάρχοντα προβλήματα επικύρωσης ποιότητας δεδομένων οφείλονται επίσης στην αδυναμία σύγκρισης των διαφορετικών προοπτικών σχετικά με την ποιότητα και την εμπιστοσύνη στις πληροφορίες που μοιράζονται.

Περιορισμένες δυνατότητες ανάλυσης

Οι επαγγελματίες χρησιμοποιούν περισσότερο email και υπολογιστικά φύλλα σε σύγκριση με TIP για να συγκεντρώσουν, να αναλύσουν και να παρουσιάσουν πληροφορίες CTI . Αυτό είναι ενδεικτικό της τρέχουσας περιορισμένης ανάλυσης πληροφοριών και των ικανοτήτων διαχείρισης που παρέχονται από TIPs, κάτι που έχει επίσης εντοπιστεί από παλιότερες έρευνες. Πιο συγκεκριμένα, δυνατότητες όπως περιήγηση, φιλτράρισμα βάσει χαρακτηριστικών, προηγμένες πληροφορίες αναζήτησης, pivoting, εξερεύνηση και οπτικοποίηση είναι μερικές από τις σημαντικότερες δυνατότητες για τις οποίες έχουν παρατηρηθεί περιορισμοί. Έτσι, η αξία του TIP εξαρτάται από την τεχνική του αναλυτή και την ικανότητα να ερμηνεύει, να αναλύει και να αντιδρά στις απειλές που λαμβάνονται. Τέλος, μόνο ένα μικρό υποσύνολο των πλατφορμών παρέχει ενοποίηση με εργαλεία τρίτων που θα μπορούσαν να βοηθήσουν στην αντιμετώπιση δραστηριοτήτων κατά τη φάση ανάλυσης του κύκλου πληροφοριών. Τα πιο συνηθισμένα εργαλεία τρίτων που παρέχουν τις δυνατότητες περιστροφής και ανάλυσης είναι το Paterva's Maltego, το IBM's i2 Analyst's Notebook, Palantir, Tableau, Microsoft Excel κ.λπ.

Χρησιμοποιούνται διαφορετικά μοντέλα δεδομένων και formats

Ένας άλλος περιορισμός που εντοπίζονται στις TIPs είναι η ποικιλία προτύπων και μορφών δεδομένων που χρησιμοποιούνται για την ανταλλαγή πληροφοριών σχετικά με τις απειλές. Ενώ υπάρχουν κοινοτικές προσπάθειες για την παροχή συνδέσμων μεταξύ διαφορετικών προτύπων και formats, εξακολουθούν να υπάρχουν περιορισμοί για τις πλατφόρμες TI που πρέπει να συλλέγουν, να εκμεταλλεύονται και να ανταλλάσσουν πληροφορίες μεταξύ μη συμβατών προτύπων και μορφών. Επιπλέον, η μετατροπή πληροφοριών χωρίς απώλεια στοιχείων ή πλαισίων από την αρχική μορφή / πηγή (lossless conversion) είναι επίσης μια πρόκληση στην ευφυΐα απειλών (ακόμη και σε μια μετατροπή μεταξύ STIX 1.x και STIX 2.0 ενδέχεται να χαθούν πληροφορίες). Είναι κοινή πρακτική ότι οι ιδιοκτήτες TIP βασίζονται και υποστηρίζουν ένα συγκεκριμένο πλαίσιο και τείνουν να παραμείνουν με αυτό το πλαίσιο. Αυτό είναι κάτι που περιορίζει την ευελιξία των χρηστών TIP όσον αφορά το πλαίσιο στο οποίο εργάζονται και συχνά οδηγεί σε ένα μοντέλο κλειδώματος δεδομένων. Τέλος, πρέπει να αναφερθεί ότι η χρήση διαφορετικών format μερικές φορές έχει νόημα επειδή ταιριάζει σε μια συγκεκριμένη ανάγκη ή σκοπό, π.χ. Yara, Sigma, Suricata κ.λπ.

Περιορισμένες προηγμένες δυνατότητες ανάλυσης και αυτοματοποίησης εργασιών

Οι TIPs έχουν περιορίσει τις προηγμένες δυνατότητες ανάλυσης, κάτι που σύμφωνα με έρευνες επαληθεύεται και από τους επαγγελματίες. Αυτές οι δυνατότητες σχετίζονται με τη φάση επεξεργασίας και εκμετάλλευσης του κύκλου πληροφοριών όταν απορροφώνται νέα δεδομένα και πρέπει να αναλυθούν, να εμπλουτιστούν και να συνδεθούν με τα υπάρχοντα. Οι προηγμένες αναλύσεις είναι ζωτικής σημασίας για την επακόλουθη ανάλυση των δεδομένων, τον προσδιορισμό της απειλής και τον προσδιορισμό της συνάφειας. Μια TIP που έχει προηγμένες δυνατότητες ανάλυσης μπορεί να δημιουργήσει πολύπλοκες σχέσεις μεταξύ δεδομένων, όπως η συγκέντρωση, η σύνθεση, η γενίκευση, καθώς και η δυνατότητα αυτόματης επισήμανσης και ταξινόμησης δεδομένων.

Δεδομένου ότι τα περισσότερα από τα κοινόχρηστα δεδομένα απειλής είναι τακτικά, οι εργασίες ρουτίνας μπορούν να προέρχονται από προηγμένες αναλύσεις και να αυτοματοποιούνται. Ορισμένες TIPs έχουν εισαγάγει δυνατότητες playbook / ενορχηστρώσεων που μπορούν να εκμεταλλευτούν περαιτέρω τα προηγμένα analytics και να βοηθήσουν τους αναλυτές CTI στις καθημερινές τους δραστηριότητες.

Μεγάλη ποικιλία API

Οι TIPs ως το κεντρικό μέρος όπου πραγματοποιούνται οι περισσότερες δραστηριότητες του κύκλου πληροφοριών, θα πρέπει να παρέχουν διεπαφές στα σχετικά εργαλεία και υπηρεσιών τρίτων, που χρησιμοποιούνται από τους τελικούς χρήστες του οργανισμού. Αυτές οι διεπαφές ενσωμάτωσης μπορούν να συμπεριληφθούν σε δραστηριότητες που σχετίζονται με τις περισσότερες φάσεις του κύκλου πληροφοριών (από τη συλλογή έως τη διάδοση). Σχετικά με την εταιρική ενοποίηση και τη χρήση API, ορισμένα TIP είναι πιο ώριμα από άλλα. Ωστόσο, η ανάγκη για ενσωμάτωση έχει επιπλέον προκλήσεις για τις TIPs που πρέπει να ενσωματωθούν σε ένα συνεχώς αυξανόμενο σύνολο υπηρεσιών και εργαλείων (έλεγχοι ασφαλείας και συστήματα ροής εργασίας) με διαφορετικά API και απαιτήσεις. Ως αποτέλεσμα, τα TIP ενσωματώνονται σε ένα (περισσότερο ή λιγότερο) τυπικό σύνολο υπηρεσιών και εργαλείων, ενώ τα αιτήματα για πρόσθετες ενοποιήσεις έχουν προτεραιότητα από τους προμηθευτές TIP καθώς και από προγραμματιστές ανοιχτού κώδικα.

Περιορισμένο workflow

Επί του παρόντος, οι TIPs παρέχουν περιορισμένες δυνατότητες που θα κάνουν τη διαδικασία διαχείρισης απειλών πιο αποτελεσματική. Ορισμένα συγκεκριμένα παραδείγματα περιλαμβάνουν την ικανότητα των ενδιαφερομένων να στέλνουν RFIs (αιτήματα για πληροφορίες) στους αναλυτές μέσω του TIP, εργαλεία συνεργασίας κατά τη διάρκεια της ανάλυσης και της φάσης παραγωγής με ένα ευρύτερο σύνολο SMEs και δυνατότητα εισαγωγής επαναληπτικών βρόχων ανατροφοδότησης στο προϊόν πληροφοριών με τον ενδιαφερόμενο. Αυτό που είναι ενθαρρυντικό είναι ότι

ορισμένοι προμηθευτές TIP προσθέτουν λειτουργίες συνεργασίας ("Tasking" για ευρύτερες ομάδες) με περιορισμένη προειδοποίηση σχετικά με τις προθεσμίες των task καθώς και δυνατότητα chatting.

Περιορισμός των γνώσεων πάνω στο Threat Management

Οι TIPs χρησιμοποιούνται επίσης ως λύση διαχείρισης γνώσης απειλών. Η διαχείριση πληροφοριών σχετικά με TTP, παράγοντες απειλής και καμπάνιες διαχειρίζεται και οι αναλυτές χρησιμοποιούν αυτήν τη βάση γνώσεων για να παρακολουθούν τη δραστηριότητα των σχετικών απειλών, φορέων και εργαλείων. Ωστόσο, έχουν προσδιοριστεί περιορισμοί στον τρόπο με τον οποίο αυτές οι πληροφορίες καταγράφονται σε αυτές τις πλατφόρμες. Δεν χρησιμοποιείται κοινό λεξιλόγιο για την περιγραφή φορέων απειλής, TTP καθώς και εργαλείων. Παρέχεται πολύ ελεύθερο κείμενο ακόμη και σε έγγραφα STIX 1.x κάτι που κάνει μια δομημένη ανάλυση να μην είναι σχετική. Επιπλέον, τα TIP παρέχουν περιορισμένη ευελιξία στη χρήση του λεξιλογίου άλλων πλαισίων όταν χρειάζεται π.χ. Πλαίσιο MITRE ATTACK.

5 Αποτελέσματα

Αυτή η μελέτη έδειξε ότι υπάρχει αυξανόμενο ενδιαφέρον για την ανταλλαγή πληροφοριών σχετικά με απειλές στην έρευνα άλλα και τους οργανισμούς. Είναι ξεκάθαρο πλέον ότι ο αριθμός των σχετικών δημοσιεύσεων και ο αριθμός των TIPs αυξήθηκε τα τελευταία χρόνια. Επιπλέον, φαίνεται ότι υπάρχει διαφορετικές οπτικές πάνω στον τομέα αυτόν, καθώς αρκετές δημοσιεύσεις συζητούν ποιες πρέπει να είναι τις αρχές της ανταλλαγής πληροφοριών σχετικά με την απειλή, παρόλο που υπάρχουν ήδη διάφορες λύσεις στην αγορά. Αυτό μπορεί να οφείλεται στην απουσία κοινής κατανόησης σχετικά με το τι ορίζεται ως ανταλλαγή πληροφοριών και threat intelligence, λόγω της ποικιλομορφίας των TIPs. Ως εκ τούτου, ένα από τα μεγαλύτερα κενά είναι η έλλειψη κοινού ορισμού και προσδιορισμού των πλατφορμών ανταλλαγής πληροφοριών απειλής. Δεδομένου ότι τα βασικά ευρήματα έδειξαν ότι οι πωλητές λογισμικού αντιλαμβάνονται διαφορετικά την ανταλλαγή πληροφοριών απειλής, είναι απαραίτητο να αναπτυχθεί έναν τυποποιημένο ορισμό και προσδιορισμό των TIPs. Σε αυτό το πλαίσιο μπορεί να είναι ωφέλιμο να υιοθετηθεί το ευρέως διαδεδομένο μοντέλο κύκλου ζωής νοημοσύνης, συμπεριλαμβανομένου του σχεδιασμού, της συλλογής, της ανάλυσης και των δραστηριοτήτων διάδοσης, στον τομέα ανταλλαγής πληροφοριών για την απειλή προκειμένου να δημιουργηθεί νοημοσύνη.

Επιπλέον, αυτές οι προσπάθειες τυποποίησης ενδέχεται να ανοίξουν το δρόμο για τον σχεδιασμό TIPs, οι οποίες να παρέχουν «πραγματική» νοημοσύνη αντί για αποθήκευση δεδομένων και περιορισμένες δυνατότητες ανάλυσης δεδομένων. Επιπλέον, οι οργανισμοί μπορεί να επωφεληθούν από έναν κοινό ορισμό, καθώς μπορεί να απλοποιήσει την επιλογή μιας κατάλληλης πλατφόρμας πληροφοριών για τις απειλές.

Μέσα απ’ αυτήν την έρευνα καταλάβαμε επίσης ότι χρησιμοποιούνται τρία πρότυπα για τη διευκόλυνση του προσδιορισμού των πληροφοριών απειλής, από τις οποίες το STIX είναι αυτό που χρησιμοποιείται περισσότερο. Είναι με σιγουριά το de-facto πρότυπο στον τομέα. Το STIX είναι ένα λεπτομερές και εκτεταμένο πρότυπο που επιτρέπει την περιγραφή ενός ευρέος φάσματος πληροφοριών που σχετίζονται με την ασφάλεια και τις σχέσεις τους. Ενώ ο αριθμός των προτύπων είναι προς το παρόν περιορισμένος, μπορεί να παρατηρηθεί μια τάση προς τη χρήση μορφών περιγραφής συγκεκριμένων περιπτώσεων (π.χ. εσωτερική κοινή χρήση έναντι κοινής χρήσης πέρα από τα οργανικά όρια).

Είναι γεγονός ότι η πλειονότητα των πλατφορμών επικεντρώνεται στους τακτικούς δείκτες συμβιβασμού που μπορούν να περιγραφούν από δύο «κατασκευές»(constructs) του προτύπου STIX. Με βάση αυτήν την παρατήρηση μπορούν να προκύψουν τα ακόλουθα δύο συμπεράσματα:

- Τα πρότυπα για την περιγραφή της νοημοσύνης απειλής είναι πολύ γενικά
- Τα μόνοι που μοιράζονται με ευκολία μέχρις στιγμής είναι τα indicators of compromise.

Για να αποκτήσουμε περισσότερες και βαθύτερες γνώσεις σχετικά με αυτό το ζήτημα, απαιτείται εμπειρική έρευνα σχετικά με τις αναμενόμενες, απαραίτητες και διαμοιραζόμενες πληροφορίες σε μια TIP. Η πλειονότητα των εργαλείων που υπάρχουν αυτή τη στιγμή είναι μάλλον πιο πολύ αποθήκες δεδομένων παρά threat intelligence πλατφόρμες. Κατά συνέπεια, οι οργανισμοί πρέπει συχνά να αξιολογούν τις ληφθείσες πληροφορίες πράγμα που ενδέχεται να έχει ως αποτέλεσμα αρκετή επιπλέον εργασία. Προκειμένου να αντιμετωπιστεί αυτό το ζήτημα, η έρευνα σε αυτόν τον τομέα πρέπει να επικεντρωθεί στην απομάκρυνση από την απλή ανταλλαγή δεδομένων ασφαλείας και να κατευθυνθεί προς τη γνώση και τελικά την ανταλλαγή νοημοσύνης. Καθώς τα βασικά ευρήματα έδειξαν ότι οι TIPs υποφέρουν από την έλλειψη προηγμένων εργαλείων ανάλυσης και οπτικοποίησης και η υποβολή νέας νοημοσύνης παρεμποδίζεται από περιορισμένες επιλογές εισαγωγής, οι υπάρχουσες πλατφόρμες και οι διεπαφές χρήστη τους πρέπει να αξιολογηθούν επιστημονικά ώστε να εντοπιστούν οι πιθανές αδυναμίες. Με αυτόν τον τρόπο, θα πρέπει να διεξαχθούν εμπειρικές μελέτες σχετικά με τις απαιτούμενες λειτουργίες και τις επιλογές οπτικοποίησης αυτών των πλατφορμών.

Ένα άλλο πράγμα που μάθαμε είναι ότι η εμπιστοσύνη παίζει πρωταρχικό ρόλο στο πλαίσιο των TIPs. Σε κάποιο βαθμό, οι πλατφόρμες πληροφοριών απειλής παρέχουν ήδη κάποιες λειτουργίες για τη δημιουργία εμπιστοσύνης μεταξύ των συνεργατών. Προκειμένου να υποστηριχθεί η τρέχουσα έρευνα και να παρασχεθεί ένα γενικά αποδεκτό μοντέλο που να εγγυάται την εμπιστοσύνη, απαιτείται εμπειρική έρευνα σχετικά με το πως αντιλαμβάνονται οι χρήστες τον διαμοιρασμό νοημοσύνης και τις προσδοκίες τους σχετικά με το απόρρητο και την ασφάλεια των δεδομένων. Μάθαμε επίσης ότι υπάρχει ένα αυξανόμενο ενδιαφέρον της ανταλλαγής πληροφοριών για απειλές στην έρευνα αλλά και στους οργανισμούς.

Επιπλέον, όπως αναφέρθηκε σε προηγούμενο κεφάλαιο οι περισσότερες πλατφόρμες είναι closed source. Κατά συνέπεια, ενδέχεται να μην υπάρχουν αρκετές TIPs και ανοικτά σύνολα δεδομένων διαθέσιμα για επιστημονική έρευνα, π.χ. για τη διεξαγωγή εμπειρικών μελετών. Προκειμένου να αντιμετωπιστεί αυτό το κενό είναι απαραίτητο η έρευνα να συνεργαστεί με τον κόσμο της βιομηχανίας. Προκειμένου να αντιμετωπιστεί το γεγονός ότι η επιτυχία μιας TIPs εξαρτάται από την προθυμία των χρηστών να μοιράζονται πληροφορίες, είναι απαραίτητο να διεξαχθεί εμπειρική έρευνα για το πώς να παρακινήσετε τους χρήστες και τον οργανισμό να μοιράζονται πληροφορίες σε μια τέτοια πλατφόρμα. Για παράδειγμα, μπορεί να είναι απαραίτητο να αναπτυχθούν και να αξιολογηθούν μηχανισμοί τόνωσης για την προώθηση της συνεργασίας εντός αυτών των πλατφορμών.

Λαμβάνοντας υπόψη την προηγούμενη συζήτηση θα αναφέρω ορισμένα πράγματα που πρέπει να κάνουν οι TIPs:

1. Οι πλατφόρμες αυτές θα πρέπει να παρέχουν ένα φιλικό περιβάλλον προς τον χρήστη.
2. Μια TIP πρέπει να παρέχει τη δυνατότητα εξαγωγής δεδομένων με μη αυτόματο τρόπο σε διάφορες μορφές (STIX, STIX2, OpenIOC, IDS υπογραφές, κανόνας Yara, XML, CSV κ.λπ.) και με βάση διαφορετικά χαρακτηριστικά δεδομένων (τύπος δείκτη, ώρα, ετικέτα, λέξη-κλειδί, και τα λοιπά..).
3. Το TIP πρέπει να παρέχει διεπαφή μηχανής και λεπτομερές API. Το API θα πρέπει να μπορεί να προσθέτει και να επεξεργάζεται πληροφορίες απειλών καθώς και δείγματα κακόβουλου λογισμικού.
4. Το TIP θα πρέπει να παρέχει την ικανότητα και τα εργαλεία που να επιτρέπουν τη συνεργασία με εσωτερικούς και εξωτερικούς ενδιαφερόμενους φορείς σχετικά με την απειλή, την ανάλυση και την

ανταπόκριση. Οι επαναληπτικές διαδικασίες πρέπει επίσης να είναι σε θέση να καθιερωθούν έτσι ώστε κάθε άτομο να μπορεί να παρέχει την ανατροφοδότησή του.

5. Υποστήριξη γνωστών πλαισίων πληροφοριών και πληροφοριών στον κυβερνοχώρο π.χ. kill chain, diamond model, TLP, NATO Admiralty code, ATT & CK framework, κ.λπ.
6. Το TIP θα πρέπει να έχει δυνατότητα αναζήτησης που θα επιτρέπει στους αναλυτές να βρίσκουν και να φιλτράρουν τις σχετικές πληροφορίες με βάση το περιεχόμενο.
7. Το TIP θα πρέπει να έχει μια ισχυρή ικανότητα αναζήτησης που θα αναλύουν οι αναλυτές και θα φιλτράρουν τις σχετικές πληροφορίες βάσει σχέσεων, ομοιότητας και αλληλοπικάλυψης με άλλα στοιχεία πληροφοριών.
8. Το TIP θα πρέπει να χρησιμοποιεί στατιστικές μεθόδους και να τις παρουσιάζει στους αναλυτές, ώστε να μπορούν να εντοπιστούν τάσεις και να απλοποιηθεί η ανάλυση δεδομένων.
9. Το TIP πρέπει να ενσωματωθεί με το SIEM, διάφορες λύσεις EDR και μεγάλους όγκους δεδομένων ασφαλείας, έτσι ώστε η αναζήτηση για υψηλής εμπιστοσύνης IoC να μπορεί να αυτοματοποιηθεί κατά τη φάση της ανάλυσης.

6 Επίλογος

Καθώς το τοπίο στον χώρο της ασφάλειας στον κυβερνοχώρο αλλάζει ριζικά και αναδύεται κάθε στιγμή νέα σενάριο απειλών, η ανάπτυξη και διερεύνηση αποτελεσματικότερων αμυντικών μηχανισμών έχουν γίνει απαραίτητες. Σε αυτή την εργασία, δόθηκε μια επισκόπηση των Threat Intelligence Platforms που υπάρχουν αυτή τη στιγμή. Με βάση ακαδημαϊκή βιβλιογραφία, επίσημους ιστότοπους και documentations , καθορίστηκε και αναλύθηκε μια ομάδα σχετικών πλατφορμών. Έτσι προτάθηκε και εφαρμόστηκε μια στρατηγική επιλογής προκειμένου οι πλατφόρμες που αναλύθηκαν να είναι οι πιο δημοφιλείς και αποτελεσματικές και συγχρόνως δωρεάν ή ανοιχτού κώδικα.

Στη συνέχεια, οι επιλεγμένες πλατφόρμες αξιολογήθηκαν με βάση μια προκαθορισμένη μεθοδολογία. Όσον αφορά τα πρότυπα που συναντάμε στις TIPs, καταλήξαμε στο συμπέρασμα ότι το STIX είναι το πιο διαδεδομένο πρότυπο στην περιοχή, κυρίως λόγω της ολιστικής προσέγγισής του, η οποία το καθιστά εφαρμόσιμο σε ένα ευρύ φάσμα σεναρίων. Όσον αφορά τις πλατφόρμες TI, το MISP και το OpenCTI θεωρήθηκαν οι πιο πλήρεις και ευέλικτες πλατφόρμες. Αν και υπάρχουν διαθέσιμες εξελιγμένες λύσεις, δεν υπάρχει καμία που να καλύπτει ολόκληρη τη διαδικασία CTI(CTI Process lifecycle).

Συμπερασματικά, παρόλο που υπάρχουν μερικές εξαιρετικές λύσεις στην αγορά(open και closed source), εξακολουθεί να θεωρείται πρόκληση να βρεθεί μια ολοκληρωμένη και απόλυτη λύση, καθώς η κάθε πλατφόρμα εστιάζει σε διαφορετικό κομμάτι του CTI process και συνεπώς αντιστοιχεί σε λίγα μόνο στάδια αυτού του process. Οι νέες έρευνες σε αυτόν τον τομέα πρέπει να κατευθυνθούν και να επικεντρωθούν στην αξιολόγηση της πληρότητας της διαδικασίας CTI που μπορεί να παρέχεται από τις διαθέσιμες πλατφόρμες με πρακτικό τρόπο, χρησιμοποιώντας τα οφέλη της διαλειτουργικότητας (interoperability) μεταξύ των πλατφορμών. Στο ίδιο πνεύμα, στο μέλλον η έρευνα πρέπει να επικεντρωθεί στην ενοποίηση μεταξύ των συμπληρωματικών πλατφορμών και εργαλείων, προκειμένου να παρέχει μια πληρέστερη λύση για τη διαχείριση και τη χρήση πληροφοριών για τις απειλές. Τέλος, μπορούμε να συμπεράνουμε ότι κρίνεται απαραίτητη η εύρεση ενός απόλυτου ορισμού για την έννοια και τη διαδικασία CTI που θα μπορούσε να βοηθήσει στον σχεδιασμό νέων και βελτιστοποιημένων συστημάτων πληροφοριών απειλής ικανά να δημιουργήσουν ένα πιο αποτελεσματικό μοντέλο ασφάλειας.

Βιβλιογραφία

1. The Cost of Cybercrime—Ninth Annual Cost of Cybercrime Study. 2019. Available online:https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime- study-final.pdf.
2. Bissell, K. 2020 Cyber Security Report.
3. Tounsi. (2005) What is Cyber Threat Intelligence and How is it Evolving?
4. Alshamrani, Myneni A, Chowdhary S, Huang A. A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities. IEEE Commun. Surv. Tutorials 2019, 21, 1851–1877, doi:10.1109/COMST.2019.2891891.
5. Wu, J. (2020). New Approaches to Cyber Defense. In Cyberspace Mimic Defense; Springer: Berlin/Heidelberg, Germany, pp. 113–157.
6. Abu, M. Selamat, S & Ariffin, A., Yusof, R. Cyber Threat Intelligence—Issue and Challenges. Indones. J. Electr. Eng. Comput. Sci. 2018, 10, 371.
7. Chadwick, D.W. Fan, W. Costantino, G. de Lemos, R. Cerbo, F.D. Herwono, I. Manea, M. Mori, P. Sajjad, A. Wang, X.S. A cloud-edge based data security architecture for sharing and analysing cyber threat information. Future Gener. Comput. Syst. 2020, 102, 710–722,
8. Zhao, J. Yan, Q. Li, J. Shao, M. He, Z. Li, B. TIMiner: Automatically extracting and analyzing categorized cyber threat intelligence from social data. Comput. Secur. 2020, 95, 101867
9. Gao, Y. LI, X. PENG, H. Fang, B. Yu, P. HinCTI: A Cyber Threat Intelligence Modeling and Identification System Based on Heterogeneous Information Network. IEEE Trans. Knowl. Data Eng. 2020,
10. Riesco, R. Larriva-Novo, X. Villagra, V.A. Cybersecurity threat intelligence knowledge exchange based on blockchain. Telecommun. Syst. 2019, 73, 259–288,
11. Rantos, K. Spyros, A. Papanikolaou, A. Kritsas, A. Ilioudis, C. Katos, V. Interoperability Challenges in the Cybersecurity Information Sharing Ecosystem. Computers 2020.
12. Ramsdale, A. Shiaeles, S. Kolokotronis, N. A Comparative Analysis of Cyber-Threat Intelligence Sources, Formats and Languages. Electronics 2020,.

13. Bauer, S. Fischer, D. Sauerwein, C. Latzel, S. Stelzer, D. Breu, R. Towards an Evaluation Framework for Threat Intelligence Sharing Platforms. In Proceedings of the 53rd Hawaii International Conference on System Sciences, Maui, HI, USA, 7–10 January 2020.
14. Shin, B. Lowry, P.B. A review and theoretical explanation of the 'Cyberthreat-Intelligence (CTI) capability' that needs to be fostered in information security practitioners and how this can be accomplished. Comput. Secur. 2020.
15. Sauerwein, C. Sillaber, C. Mussmann, A. Breu, R. Threat intelligence sharing platforms: An exploratory study of software vendors and research perspectives. In Proceedings of the 13th International Conference on Wirtschaftsinformatik, St.Gallen, Switzerland, 12–15 February 2017.
16. Skopik, F. Settanni, G. Fiedler, R. (2016) A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. Comput. Secur. 60, 154–176.
17. ENISA. (2020) Exploring the Opportunities and Limitations of Current Threat Intelligence Platforms. 2018. Available online:https://www.enisa.europa.eu/publications/exploring-the-opportunities-and-limitations- of-current-threat-intelligence-platforms(accessed on 16 March).
18. Poputa-Clean, P. Stingley, M. (2015) Automated Defense-Using Threat Intelligence to Augment Security. . Available online:https://www.sans.org/reading-room/whitepapers/threats/paper/35692 (accessed on 23 March 2020)
19. Wagner, T.D. Mahbub, K. Palomar, E. Abdallah, (2019) A.E. Cyber threat intelligence sharing: Survey and research directions. Comput. Secur.
20. Sarker, I.H. Abushark, Y.B. Khan, A.I. ContextPCA: Predicting Context-Aware Smartphone Apps Usage Based On Machine Learning Techniques. Symmetry 2020, 12, 499.
21. Sarker, I.H. Kayes, A.S.M. Watters, P. Effectiveness analysis of machine learning classification models for predicting personalized context-aware smartphone usage. J. Big Data 2019.
22. Sarker, I.H. Abushark, Y.B. Alsolami, F. Khan, A.I. IntruDTree: A Machine Learning-Based Cyber Security Intrusion Detection Model. Symmetry 2020, 12, 754.
23. Truong, T.C. Zelinka, I. Plucar, J. Cˇ andík, M. Šulc, V. Artificial Intelligence and Cybersecurity: Past,
Presence, and Future. In Advances in Intelligent Systems and Computing; Springer: Singapore, 2020; pp. 351–363,
24. Noor, U. Anwar, Z. Amjad, T. Choo, K.K.R. A machine learning-based FinTech cyber threat attribution framework using high-level indicators of compromise. Future Gener. Comput. Syst. 2019, 96, 227–242.
25. Dalton, A Aghaei, E. Al-Shaer, E. Bhatia, A. Castillo, E.; Cheng, Z. Dhaduvai, S. Duan, Q. Islam, M.M. Karimi, Y. et al. The Panacea Threat Intelligence and Active Defense Platform.
26. Kazato, Y. Nakagawa, Y. Nakatani, Y. Improving Maliciousness Estimation of Indicator of Compromise Using Graph Convolutional Networks. In Proceedings of the 2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 10–13 January 2020.
27. Albakri, A. Boiten, E. Lemos, R.D. Sharing Cyber Threat Intelligence Under the General Data Protection Regulation. In Privacy Technologies and Policy; Springer: Cham, Switzerland, 2019; pp. 28–41.
28. Wu, Y. Qiao, Y. Ye, Y. Lee, B. Towards Improved Trust in Threat Intelligence Sharing using Blockchain and Trusted Computing. In Proceedings of the 2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS),

Granada, Spain, 22–25 October 2019.
29. Tlelo-Cuautle, E. Díaz-Muñoz, J.D. González-Zapata, A.M.; Li, R. León-Salas, W.D. Fernández, F.V. Guillén-Fernández, O. Cruz-Vega, I. Chaotic Image Encryption Using Hopfield and Hindmarsh–Rose Neurons Implemented on FPGA. Sensors 2020.
30. Khan, M. Masood, F. Alghafis, A. Secure image encryption scheme based on fractals key with Fibonacci series and discrete dynamical system. Neural Comput. Appl. 2019.
31. Burger, E.W. Goodman, M.D. Kampanakis, P. Zhu, K.A. Taxonomy Model for Cyber Threat Intelligence Information Exchange Technologies. In Proceedings of the 2014 ACM Workshop on Information Sharing & Collaborative Security—WISCS-14, Scottsdale, AZ, USA, 3–7 November 2014.

32. Mavroeidis, V.; Bromander, S. Cyber Threat Intelligence Model: An Evaluation of Taxonomies, Sharing Standards, and Ontologies within Cyber Threat Intelligence. In Proceedings of the 2017 European Intelligence and Security Informatics Conference (EISIC), Athens, Greece, 11–13 September 2017; doi:10.1109/eisic.2017.20.
33. Asgarli, E.; Burger, E. Semantic ontologies for cyber threat sharing standards. In Proceedings of the 2016 IEEE Symposium on Technologies for Homeland Security (HST), Waltham, MA, USA, 10–11 May 2016, doi:10.1109/ths.2016.7568896.
34. Steinberger, J.; Sperotto, A.; Golling, M.; Baier, H. How to exchange security events? Overview and evaluation of formats and protocols. In Proceedings of the 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM), Ottawa, ON, Canada, 11–15 May 2015, doi:10.1109/inm.2015.7140300.
35. Tounsi, W.; Rais, H. A survey on technical threat intelligence in the age of sophisticated cyber attacks.
Comput. Secur. 2018, 72, 212–233, doi:10.1016/j.cose.2017.09.001.
36. Menges, F.; Pernul, G. A comparative analysis of incident reporting formats. Comput. Secur. 2018, 73, 87–101, doi:10.1016/j.cose.2017.10.009.
37. Ferreira, H.G.C.; de Sousa Junior, R.T. Clust. Comput. Security analysis of a proposed internet of things middleware. Clust. Comput. 2017, 20, 651–660, doi:10.1007/s10586-017-0729-3.
38. de Melo Silva, C.C.; Ferreira, H.G.C.; de Sousa Júnior, R.T.; Buiati, F.; Villalba, L.J.G. Design and Evaluation of a Services Interface for the Internet of Things. Wirel. Pers. Commun. 2016, 91, 1711–1748, doi:10.1007/s11277-015-3168-6.
39. Sillaber, C.; Sauerwein, C.; Mussmann, A.; Breu, R. Data Quality Challenges and Future Research Directions in Threat Intelligence Sharing Practice. In Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security—WISCS16, Vienna, Austria, 24–28 October 2016; doi:10.1145/2994539.2994546.
40. Barnum, S. Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX). 2012. Available online:https://www.mitre.org/publications/technical-papers/ standardizing-cyber-threat-intelligence-information-with-the(accessed on 17 March 2020).
41. Chismon, D.; Ruks, M. Threat Intelligence: Collecting, Analysing, Evaluating; MWR InfoSecurity Ltd.: Basingstoke, UK, 2015.
42. Friedman, J.; Bouchard, M. Definitive Guide to Cyber Threat Intelligence: Using Knowledge about Adversaries to Win the War against Targeted Attacks; CyberEdge Group: Annapolis, MD, USA, 2015.
43. CERT-UK. An Introduction to Threat Intelligence. 2015. Available online:http://dl.icdst.org/pdfs/files/ 85d0b11467a3e30bf12a5bbc6c3e543c.pdf(accessed on 4 May 2020).
44. Shackleford, D. Cyber Threat Intelligence Uses, Successes and Failures: The Sans 2017 Cti Survey. 2017. Available online:https://www.sans.org/reading-room/whitepapers/threats/paper/37677(accessed on 12 May 2020)
45. OASIS. STIX Version 2.0. Part 1: STIX Core Concepts. 2017. Available online:http://docs.oasis-open.org/ cti/stix/v2.0/stix-v2.0-part1-stix-core.html(accessed on 18 May 2020).
46. OASIS. STIX Version 2.0. Part 2: STIX Objects. 2017. Available online:http://docs.oasis-open.org/cti/stix/ v2.0/stix-v2.0-part2-stix-objects.html(accessed on 18 May 2020).
47. Corporation, M. Cyber Observable eXpression (CybOX™) Archive Website. 2017.

Available online: https://cyboxproject.github.io/(accessed on 21 May 2020).
48. OASIS. STIX™ Version 2.0. Part 3: Cyber Observable Core Concepts. 2017. Available online:http: //docs.oasis-open.org/cti/stix/v2.0/stix-v2.0-part3-cyber-observable-core.pdf(accessed on 18 May 2020).
49. OASIS. TAXII Version 2.0. 2017. Available online:http://docs.oasis-open.org/cti/taxii/v2.0/taxii-v2.0.html (accessed on 21 May 2020).
50. Danyliw, R.; Meijer, J.; Demchenko, Y. The Incident Object Description Exchange Format. 2007. Available online:https://tools.ietf.org/html/rfc5070(accessed on 25 May 2020).
51. Danyliw, R. The Incident Object Description Exchange Format Version 2. 2016. Available online: https://tools.ietf.org/html/rfc7970(accessed on 25 May 2020).
52. Moriarty, K. Real-Time Inter-Network Defense (RID). 2012. Available online:https://tools.ietf.org/html/ rfc6545(accessed on 27 May 2020).
53. Inc., M. An Introduction to Open IOC. 2011. Available online:https://www.academia.edu/31820654/An_ Introduction_to_Open_IOC(accessed on 27 May 2020).