



ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

UNIVERSITY OF PIRAEUS

**Department of Digital Systems**

Master

**“Security of Digital Systems”**

Thesis:

**Security Logs Analysis (Big Data) Using Arcsight SIEM Tool**

***Author:***

George Kontogiannis - MTE1317

[kontogiannhs.g@gmail.com](mailto:kontogiannhs.g@gmail.com)

***Supervisor:***

Prof. Kostas Lambrinoudakis

[clam@unipi.gr](mailto:clam@unipi.gr)

Piraeus 2016

## Contents

<b>Table of Figures.....</b>	<b>4</b>
<b>List of Acronyms and Abbreviations.....</b>	<b>5</b>
<b>Abstract .....</b>	<b>6</b>
<b>1. Introduction .....</b>	<b>7</b>
<b>2. EVENTS CENTRALIZATION AND CORRELATION .....</b>	<b>8</b>
2.1 Introduction of Events Centralization and Correlation Systems.....	8
2.2 Importance of Events Centralization and Correlation Systems .....	8
<b>3. Arcsight SIEM Architecture .....</b>	<b>10</b>
3.1 Logs and Events .....	10
3.2 Types of logs.....	10
3.3 Collection of logs .....	12
3.4 Logs forwarding to Arcsight.....	14
3.5 Capabilities of Arcsight Logger .....	19
3.5.1 Logger charts .....	21
3.5.2 Logger Reporting .....	22
3.6 Capabilities of Arcsight Express/ESM.....	24
3.6.1 Event Correlation .....	24
3.6.2 Filters.....	25
3.6.3 Rules.....	25
3.6.4 Dashboards .....	26
3.6.5 Active Lists .....	26
<b>4. Arcsight Express / ESM usage in a big company .....</b>	<b>27</b>
4.1 OS Failed Login Attempts.....	28
4.2 OS Brute Force Login Attempts .....	31
4.3 DB Failed Login Attempts .....	33
4.4 DB Brute Force Failed Login Attempts .....	37
4.5 VPN Brute Force Login Attempts.....	40
4.6 VPN External authorized logins.....	42
4.7 Antivirus log – Malware monitoring.....	45

4.8 Suspicious Communication with malicious IP's – Domains .....	51
4.9 General Observation – incident example.....	54
<b>5. Conclusion and future work .....</b>	<b>55</b>
5.1 Conclusion .....	55
5.2 Future work .....	56
<b>References .....</b>	<b>57</b>

## Table of Figures

<a href="#">Figure 1. Annual increase of data</a>	7
<a href="#">Figure 2. Syslog (authpriv.log) example</a>	10
<a href="#">Figure 3. Syslog Application log example</a>	11
<a href="#">Figure 4: Architecture of Log collection to the Arcsight</a>	12
<a href="#">Figure 5: 3-days logs (syslog) for 1 system with ip 172.25.23.85</a>	13
<a href="#">Figure 6: sftp directories for logs transferred via sftp</a>	14
<a href="#">Figure 7: List of syslog directories</a>	14
<a href="#">Figure 8: Syslog Application log example</a>	15
<a href="#">Figure 9: Regex example</a>	16
<a href="#">Figure 10: Regex example</a>	17
<a href="#">Figure 11: Processed logs example</a>	18
<a href="#">Figure 12: Arcsight Logger application log example</a>	19
<b><a href="#">Figure 13: Arcsight Logger application log example</a></b>	19
<a href="#">Figure 14: Arcsight Logger overview</a>	20
<a href="#">Figure 15: Domain Controllers chart</a>	21
<a href="#">Figure 16: Scheduled Report Query</a>	22
<a href="#">Figure 17: Arcsight report export</a>	23
<a href="#">Figure 18: Staging server to Logger or ESM</a>	24
<a href="#">Figure 19: Arcsight Express / ESM overview</a>	27
<a href="#">Figure 20: OS Failed Login Attempts – Active Channel</a>	28
<a href="#">Figure 21: OS Failed Login Attempts – Filter</a>	29
<a href="#">Figure 22: OS Failed Login Attempts – Dashboard</a>	30
<a href="#">Figure 23: OS Brute Force Login Attempts – Active Channel</a>	31
<a href="#">Figure 24: OS Brute Force Login Attempts – Active Channel Filter</a>	32
<a href="#">Figure 25: OS Brute Force Login Attempts –event id 4625 filter</a>	32
<a href="#">Figure 26: DB Failed Login Attempts – Active Channel</a>	33
<a href="#">Figure 27: DB Failed Login Attempts – Filter</a>	34
<a href="#">Figure 28: DB Failed Login Attempts – Event Inspector</a>	35
<a href="#">Figure 29: DB Failed Login Attempts – Dashboard</a>	36
<a href="#">Figure 30: DB Brute force Login Attempts – Active Channel</a>	37
<a href="#">Figure 31: DB Brute force Login Attempts – Correlated Event</a>	38
<a href="#">Figure 32: DB Brute force Login Attempts – Inspect view</a>	38
<a href="#">Figure 33: DB Brute force Login Attempts – Filter</a>	39
<a href="#">Figure 34: VPN Brute Force Login Attempts – Active Channel</a>	40
<a href="#">Figure 35: VPN Brute Force Login Attempts – Filter</a>	41
<a href="#">Figure 36: VPN Brute Force Login Attempts – Rule</a>	42
<a href="#">Figure 37: VPN External Connections – Active List</a>	43
<a href="#">Figure 38: VPN External Connections – Active Channel</a>	43
<a href="#">Figure 39: VPN External Connections – Filter</a>	44

<a href="#">Figure 40: VPN External Connections – Dashboard</a> .....	45
<a href="#">Figure 41: Antivirus logs – Active Channel</a> .....	46
<a href="#">Figure 42: Antivirus logs – Event inspection</a> .....	47
<a href="#">Figure 43: Antivirus logs – Dashboard</a> .....	48
<a href="#">Figure 44: Antivirus logs – Active channel, multiple virus event inspector</a> .....	49
<a href="#">Figure 45: Antivirus logs – Filter for specific ransomware virus</a> .....	50
<a href="#">Figure 46: Antivirus logs – Dashboard overview</a> .....	50
<a href="#">Figure 47: Active Channel – Communication with suspicious domain</a> .....	52
<a href="#">Figure 48: Active Channel – Communication with suspicious IP</a> .....	52
<a href="#">Figure 49: Filter – Communication with suspicious IP</a> .....	53
<a href="#">Figure 50: Active List with malicious IP</a> .....	54

## List of Acronyms and Abbreviations

<b>ADAE</b>	Assurance of Privacy of Communications
<b>DB</b>	Database
<b>DDOS</b>	Distributed Denial of Service
<b>ESM</b>	Enterprise security management software
<b>IMEI</b>	International Mobile Equipment Identity
<b>IMSI</b>	International Mobile Subscriber Identity
<b>MSISDN</b>	Mobile Station International Subscriber Directory Number
<b>OS</b>	Operating System
<b>SIEM</b>	Security Information and Event Management
<b>VPN</b>	Virtual Private Network

## Abstract

This is the Master Thesis of George Kontogiannis. The main purpose of this project is to present a method for making Big Data analysis for Security Logs. This method should take as an input a great amount and variety of Data and analyze them in order to make useful conclusions about who made a malicious action, an information leakage, etc. The best method to achieve that in a big company where there are tons of logs is by using a SIEM.

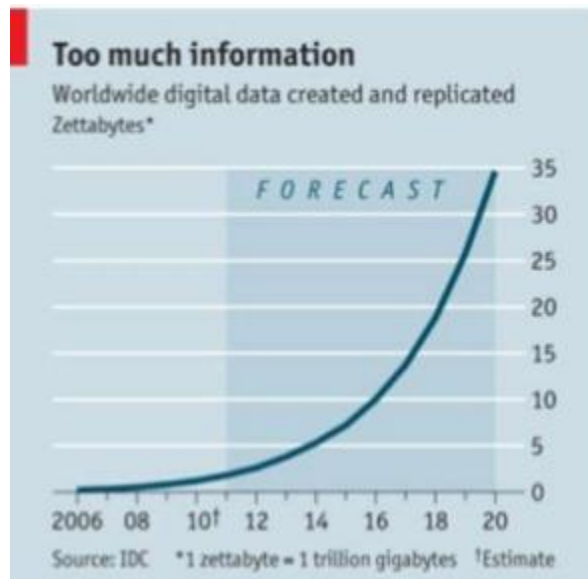
SIEM tool provide the ability to normalize and correlate log data from multiple sources on networks. The usage of a SIEM can also provide auditing controls checks, either the compliance of policies or of legal requirements and reduces the costs of them through the centralization of all events that occur in a big company. Moreover it can assist in early identification of the insider threat by correlating personal background investigations and normal user action information with the individual's online activities.

This Thesis presents the HP Arcsight Technology and Architecture SIEM solution. It's a SIEM solution that provides a variety of actions in order to perfectly understand and analyze all the logs that come out from enterprise systems, such as OS logs, DB logs, etc. An analytic presentation it's going to be done from the collection of logs until the final output of Arcsight(correlated events, Dashboards, Active Channels, etc).

## 1. Introduction

Nowadays, the continuous development of technology has led to big changes in the big companies. A telecommunications provider for example should constantly be equipped with the latest technology (new hardware, development of telecommunications applications, etc) in order to be competitive and gain the largest proportion of customers. Moreover, here in Greece, the telecommunications providers are subject to review from ADAE. This review could be made in different fields of the company, for example if some customer make a complaint in ADAE that his phone is monitored, the provider should present the appropriate evidence that during this period (of the complaint) the number was not monitored.

Also, over the years, it has sharply increased the amount of data. Data grow at a rate of almost 40% every year, according to the McKinsey Global Institute.



**Figure 1. Annual increase of data**

This means that with the passage of time digital data would be larger and larger and big companies would have to process and store more and more data each year which is very difficult and not affordable. Additionally ADAE requires every provider to store the logs from the corporate systems for several period of time, (about 2 years) as a result there is an important need for a centralized system/architecture that will store and analyze logs.

Furthermore, from the security perspective, companies care more to protect themselves from all kind of possible threats. The majority of companies have now created information security sections in order to successfully face external threats, (like

hackers/DDoS attacks, etc.) or to ensure that every procedure in company performed transparently. All of the above lead to the conclusion that a SIEM tool is necessary for each organization which respects their labors and the cost of enterprise operation.

## **2. EVENTS CENTRALIZATION AND CORRELATION**

### **2.1 Introduction of Events Centralization and Correlation Systems**

All the data generated by the system events is of great importance as a source of information for any organization, small, medium or large. As large organization you are, the more value they have your data, even more your sensitive data (Telecommunication providers for example have very sensitive data, as their log contain MSISDN, IMSI and other critical information). The proper control of this data ensures that the legal & compliance obligations will be accomplished and to address IT security risk. The need to include the real time monitoring of the network arises by the growing threats and logs to the business continuity. Companies need to be able to make a thorough analysis and detailed report-data to meet demanding legal and compliance obligations.

### **2.2 Importance of Events Centralization and Correlation Systems**

Events Centralization allows an organization to access and utilize devices that would not be available or have direct contact otherwise. The security department of each company is responsible for the global visibility of the centralized event system (SIEM). This system also controls the cost of demonstrating compliance and reduces the complexity of managing a heterogeneous IT infrastructure. SIEM tool facilitate compliance efforts with centralized log management, dashboard and reporting capabilities. Also there is an indirect benefit: the management tool recollects logs in real time, this fact ensures the non-manipulation of these logs. Another benefit is that it manages security operations effectively and efficiently with centralized security event correlation, prioritization, investigation and response.

Another problem that a SIEM try to solve is to reduce the number of internal attacks. Each year, a significant percentage of gross annual revenue (around 5%) is been lost due to internal attacks. The 5% corresponds to many thousands of Euros (€) for a big



company, so this fact motive the regulators and auditors to make security information an urgent matter for the company.

Businesses try to improve processes to implement controls to support policies in order to comply with industry and regulatory standards. For example, it's necessary to monitor who accessed the files with critical information for the customers of the company. Also it is very important to log the time and date of the incident in order to find accurately who made the violation. The continuous development is just as important to a compliance audit as approving that controls are in place.

Concerning the operations section, it is easy enough to extract important information when looking in an error log in order to find what's going wrong and fix the error occurred. Parsing a log into a normalized format benefits the search method, all the logs are saved with the same format (after processing of the Arcsight). The central event management system manage events (normalized logs) and match the incoming log with a defined event modeling to facilitate the management operations and integrate these logs with the business continuity functions.

Finally, a SIEM implementation could preserve in one log file clues from an attack. In case of internal investigations, these logs may be from users attempting to authenticate into various enterprise systems and applications. Database logs, application- specific logs or VPN and operating systems logs are used in forensic analysis to discover the real cause of this incident.

## 3. Arcsight SIEM Architecture

### 3.1 Logs and Events

The logs are the one and only input for Arcsight, without them no operation can proceed. A log is an official record of operations during a particular period of time. For information security professionals, a log is used to record data or to obtain information on who, what, when, where and why an activity occurs for a particular device or application. Then they have the ability to analyze the device or application activities in deep and to understand exactly what happened there.

### 3.2 Types of logs

There are several log categories, which depend on the system current system by which are gathered. The most common is the **syslog log**. Syslog is a way for network devices to send event messages to a logging server. The syslog protocol is supported by a wide range of devices and can be used to log different types of events. For example, a router might send messages about users logging on to console sessions, while a web-server might log access-denied events. The following image shows an example from a syslog log and more specific from an authpriv log. **Authpriv log** record the logins and logouts to a system. As it seems here user **root** has logged on in the system **rensdclb** (172.25.23.85) at **2 February 00:00:01**.

```
[arcsight@cosmolog02 172.26.231.7]$ head /data/rlogs/2016/ntnetwork/172.25.23.85/172.25.23.85-authpriv-20160202.log
Feb  2 00:00:01 Feb  2 00:00:01 172.25.23.85 rensdc1b 172.25.23.85 authpriv.info 6 su su: pam_unix(su-l:session): session opened for user root by (uid=0)
Feb  2 00:00:02 Feb  2 00:00:02 172.25.23.85 rensdc1b 172.25.23.85 authpriv.info 6 su su: pam_unix(su-l:session): session closed for user root
Feb  2 00:01:00 Feb  2 00:01:00 172.25.23.85 rensdc1b 172.25.23.85 authpriv.info 6 su su: pam_unix(su-l:session): session opened for user dataprtct by (uid=0)
Feb  2 00:01:20 Feb  2 00:01:20 172.25.23.85 rensdc1b 172.25.23.85 authpriv.info 6 su su: pam_unix(su-l:session): session closed for user dataprtct
```

**Figure 2. Syslog (authpriv.log) example**

Another important log category is the **application log**. An application log is a file of events that are logged by a software application. It contains errors, informational events and warnings. The format and content of an application log are determined by the developer of the software program, rather than the OS. The following image shows an

example of an application log. It's a log from a telecommunications system that indicates the **MSISDN** and the **IMEI** that have recently activated. The activation was made through a web application the numbers was recorded in the following log.

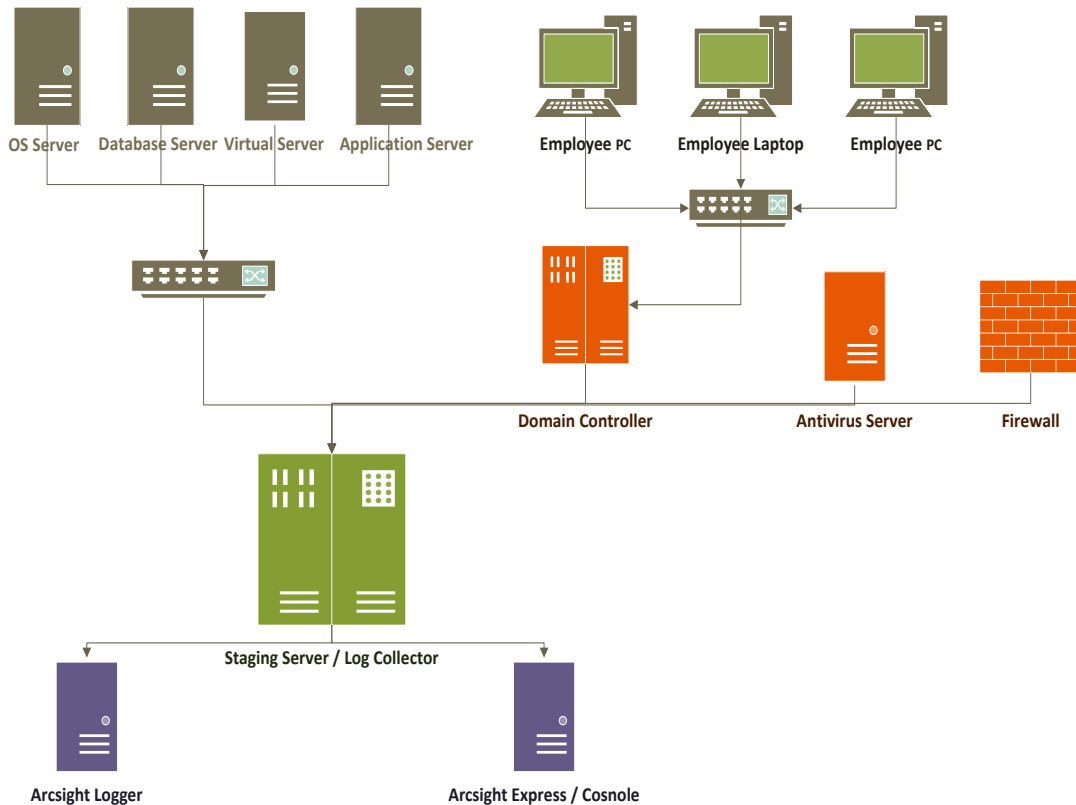
```
"Voice A Direction Number","Voice A Imei","Date Name","Event amount","A Side Successful Events","Voice A Cell",
"30690604","35768303028","2015/06/10 00:00:00","16","0","0","616","2","0","0","9","0","0","7"CRUE
"30690605","86004102121","2015/06/10 00:00:00","17","1","0","1406","1","1","0","5","0","1","12"CRUE
"30690615","35369006700","2015/06/10 00:00:00","22","0","0","524","3","0","0","8","0","1","14"CRUE
"30690621","35778606312","2015/06/10 00:00:00","18","0","1","1449","3","0","1","7","1","0","11"CRUE
"30690626","35928606281","2015/06/10 00:00:00","17","0","1","1978","9","0","1","6","1","0","10"CRUE
```

**Figure 3.** Syslog Application log example

There are more kinds of logs, some of them will be discussed in the following sections.

### 3.3 Collection of logs

The main **Arcsight SIEM** Architecture in one big company is the following:



**Figure 4:** Architecture of Log collection to the Arcsight

In each company, there are plenty of machines that produce useful logs for the security analysts. More specific:

- To begin with, a variety of **Operating Systems** (like Linux, Centos, AIX, etc.) produce logs about their function, the connections which made to them and more.
- Database servers go next. **Oracle** and **Solaris** is the most common used. Here the logs record the **queries** that have been made to a database, the **user** who made them, the source pc from which the connection was made, etc.
- **Application servers** run all the important applications of the company and many times the applications contain critical information (like customer numbers,

addresses, etc.), so it's a major priority to collect logs from this kind of applications.

- Employee's **pc** and **laptop** is the major working tool in the company. Each **pc** connects to a **Domain Controller** in order to authenticate to the intranet. Logs produced for every login or logout to the intranet. Also, the pc name is unique in order to be a match between the workstation and his holder. At each location where the employee will be connected, it will appear from where did the connection.
- **Antivirus solution** protects the workstations from virus, malwares and all kind of this malicious stuff. Moreover it produces **antivirus log** if a workstation infect with a malicious entry, indicating if the malicious entry deleted, or cleaned, or left alone, etc.
- **Firewall** is the one which says who will pass and which will be blocked. Logs about the incoming and out coming traffic produced giving the ability to know which machine connected with what, from the internal to the external network and the opposite.

The systems above producing interesting security logs, of course there are many more but they will not be analyzed in the current thesis.

All the above system, produce their logs locally and then forward them to a centralized log collector, the staging server (fig 4. Staging server/Log collector). Here it should be noted that logs are not saved locally but sent directly to the collector in order to comply with data retention rule (minimize the possibility someone touch the logs and change or leak some critical information). This server is something like a big bucket, all kind of logs land here and stored for a sufficiently long period (it depends on the individual company policy). It is therefore clear that staging server needs a great mount of hard drive storage to afford all Gigabytes of data coming in. The following images show some stored directories in the staging server:

```
[arcsight@cosmolog02 172.26.231.7]$ ls /data/rlogs/2016/ntnetwork/172.25.23.85
172.25.23.85-authpriv-20160202.log 172.25.23.85-cron-20160204.log 172.25.23.85-kern-20160203.log
172.25.23.85-authpriv-20160203.log 172.25.23.85-daemon-20160202.log 172.25.23.85-kern-20160204.log
172.25.23.85-authpriv-20160204.log 172.25.23.85-daemon-20160203.log 172.25.23.85-local5-20160202.log
172.25.23.85-cron-20160202.log 172.25.23.85-daemon-20160204.log 172.25.23.85-local5-20160203.log
172.25.23.85-cron-20160203.log 172.25.23.85-kern-20160202.log 172.25.23.85-local6-20160202.log
```

**Figure 5: 3-days logs (syslog) for 1 system with ip 172.25.23.85**

```

[arcsight@cosmolog02 172.26.231.7]$ ls /data/rlogs/sftp/
airlsftp/   cmsftp/    ebillotesftp/ fmssftp/    ilinksftp/  ouranosftp/ rombscssftp/ SAM/        sdp1bsftp/  sensagesftp/ sysinpp/
air2sftp/   cntdbsftp/ evesftp/     huaweims/   netactsftp/ polystarsftp/ romfmsftp/  sapsftp/    sdp2asftp/  syscps/     sysoasis/
ccuresftp/  cosfmsdlsftp/ fmslog/     ignitesftp/ nginsftp/   rasftp/      romrasftp/  sdp1asftp/  sdp2bsftp/  sysdp/      sysoss/

```

**Figure 6: sftp directories for logs transferred via sftp**

```

[arcsight@cosmolog02 172.26.231.7]$ ls /data/rlogs/2016/ntsyslog/
10.20.250.138 10.20.250.148 10.203.11.76 172.19.100.12 172.19.87.229 172.25.116.41 172.25.13.233 172.25.156.59 172.25.157.55 172.25.159.158
10.20.250.139 10.20.250.149 10.203.11.77 172.19.100.13 172.19.87.230 172.25.116.42 172.25.156.16 172.25.157.16 172.25.158.16 172.25.159.153
10.20.250.140 10.20.250.150 10.203.11.78 172.19.100.14 172.21.4.27 172.25.116.43 172.25.156.19 172.25.157.19 172.25.158.19 172.25.21.131
10.20.250.141 10.20.250.23 10.203.21.136 172.19.100.15 172.21.4.28 172.25.116.44 172.25.156.22 172.25.157.22 172.25.158.25 172.25.21.132
10.20.250.142 10.20.250.55 10.203.21.137 172.19.100.54 172.25.116.24 172.25.116.45 172.25.156.25 172.25.157.25 172.25.158.37 172.25.21.166
10.20.250.143 10.203.11.11 10.203.21.8 172.19.100.61 172.25.116.25 172.25.116.46 172.25.156.34 172.25.157.34 172.25.158.46 172.25.21.167
10.20.250.144 10.203.11.12 10.203.22.8 172.19.100.62 172.25.116.28 172.25.118.67 172.25.156.37 172.25.157.37 172.25.158.52 172.25.21.168
10.20.250.145 10.203.11.13 10.203.22.9 172.19.100.63 172.25.116.29 172.25.118.68 172.25.156.48 172.25.157.46 172.25.158.55 172.25.21.169
10.20.250.146 10.203.11.14 172.19.100.10 172.19.87.227 172.25.116.31 172.25.119.187 172.25.156.51 172.25.157.49 172.25.159.144 172.25.21.188
10.20.250.147 10.203.11.75 172.19.100.11 172.19.87.228 172.25.116.32 172.25.13.231 172.25.156.56 172.25.157.52 172.25.159.147 172.25.21.189

```

**Figure 7: List of syslog directories**

### 3.4 Logs forwarding to Arcsight

Logs stored in staging server in a raw form. Raw form is sometimes difficult to be read, so it needs Arcsight in order to separate log to specified fields and make log easily readable. Logs should therefore transfer to the Arcsight Logger. This procedure achieved with the usage of **flex connectors**. ArcSight connectors are the ideal interface to insulate the management, compliance and security from the technologies choices for the devices/application. These connectors can translate the collected raw logs into a data normalized structure with the same format. ArcSight Connectors produce a single structure for searching, correlating, and reporting on event information. With this feature the management tool is robust against changes and new network technologies.

There are 2 different ways of transfer depending on the kind of log:

- **Syslog** follows and automated procedure and forwarded through Arcsight Logger.
- **Application log** follows a more complicated way in order to pass through Logger.

To begin with, as said earlier application log usually has a strange structure so it's impossible to be forwarded to the Logger as it is. But what it means logs have to be parsed?

Logs are parsing in order to convert in a form that Arcsight can process and separate them into several fields. This can be done with the usage of **regular expressions**. Regular expression is a special text string for describing a search pattern. It can be more understandable with an example below:

The following log is an application log that needs to be parsed. In order to be forwarded to Logger it has to be separated into fields.

```
"Voice A Direction Number","Voice A Imei","Date Name","Event amount","A Side Successful Events","Voice A Cell",
"30690604","35768303028","2015/06/10 00:00:00","16","0","0","616","2","0","0","9","0","0","7"CRLF
"30690605","86004102121","2015/06/10 00:00:00","17","1","0","1406","1","1","0","5","0","1","12"CRLF
"30690615","35369006700","2015/06/10 00:00:00","22","0","0","524","3","0","0","8","0","1","14"CRLF
"30690621","35778606312","2015/06/10 00:00:00","18","0","1","1449","3","0","1","7","1","0","11"CRLF
"30690626","35928606281","2015/06/10 00:00:00","17","0","1","1978","9","0","1","6","1","0","10"CRLF
```

**Figure 8: Syslog Application log example**

Arcsight has a tool for implementing regular expressions, **Regex**. With regex it is feasible to parse almost any kind of application log. In this example the regular expression that will be used to parse the log above is the following:

Regex="\"([d]\*)\"\\\", \"([d]\*)\"\\\", \"([d\\s:]\*)\*\"\\\", (.\*)

**Red color** matches the first number, **green color** matches the second number, **blue color** matches the date/time and **purple color** matches the rest of the log.

The following image illustrates in detail all the hole procedure and the field mapping. The following file is named **example.sdkrfilereader.properties** and is the input of the connector in order to parse the log.

```

1 # FlexAgent Regex Configuration File
2 line.ignore.regex=(\\"Voice.\")
3 do.unparsed.events=true
4
5 regex=\\\" ([\\d]*)\\\"\\\",\\\" ([\\d]*)\\\"\\\",\\\" ([\\d\\\\\\\\\\\\s\\\\\\\\:]*)\\\"\\\", (.*)
6
7 token.count=4
8
9 token[0].name=deviceCustomString1
10 token[0].type=String
11
12 token[1].name=deviceCustomString2
13 token[1].type=String
14
15 token[2].name=endTime
16 token[2].type=TimeStamp
17 token[2].format=yyyy/MM/dd hh:mm:ss
18
19 token[3].name=message
20 token[3].type=String
21
22 #submessage.messageid.token=
23 #submessage.token=
24
25
26 event.deviceCustomString1=deviceCustomString1
27 event.deviceCustomString2=deviceCustomString2
28 event.endTime=endTime
29 event.message=message
30 event.deviceVendor=__stringConstant("COS ")
31 event.deviceProduct=__stringConstant("SAI_APP_CEM")
32 event.name=__stringConstant("cemapp1")
33
34
35
36 #l10n.filename.prefix=
37
38
39

```

### Figure 9: Regex example

**Line.igone.regex=(\\Voice.\*):** ignores all the lines starting with **Voice**. Only the pure log is usable for parsing so the rest information has to be excluded.

**Regex** : the regular expression to read the log.

**Tokens** are used to send each part of the log that has been read to a several field. For example:

**Token[0].name=deviceCustomString1** : means that the first number (30690604XXXX) of the first line of the log will be illustrated in the Logger field **deviceCustomString1**.

If the **example.sdksrfilereader.properties** filled correctly the Regex will look like the following image:



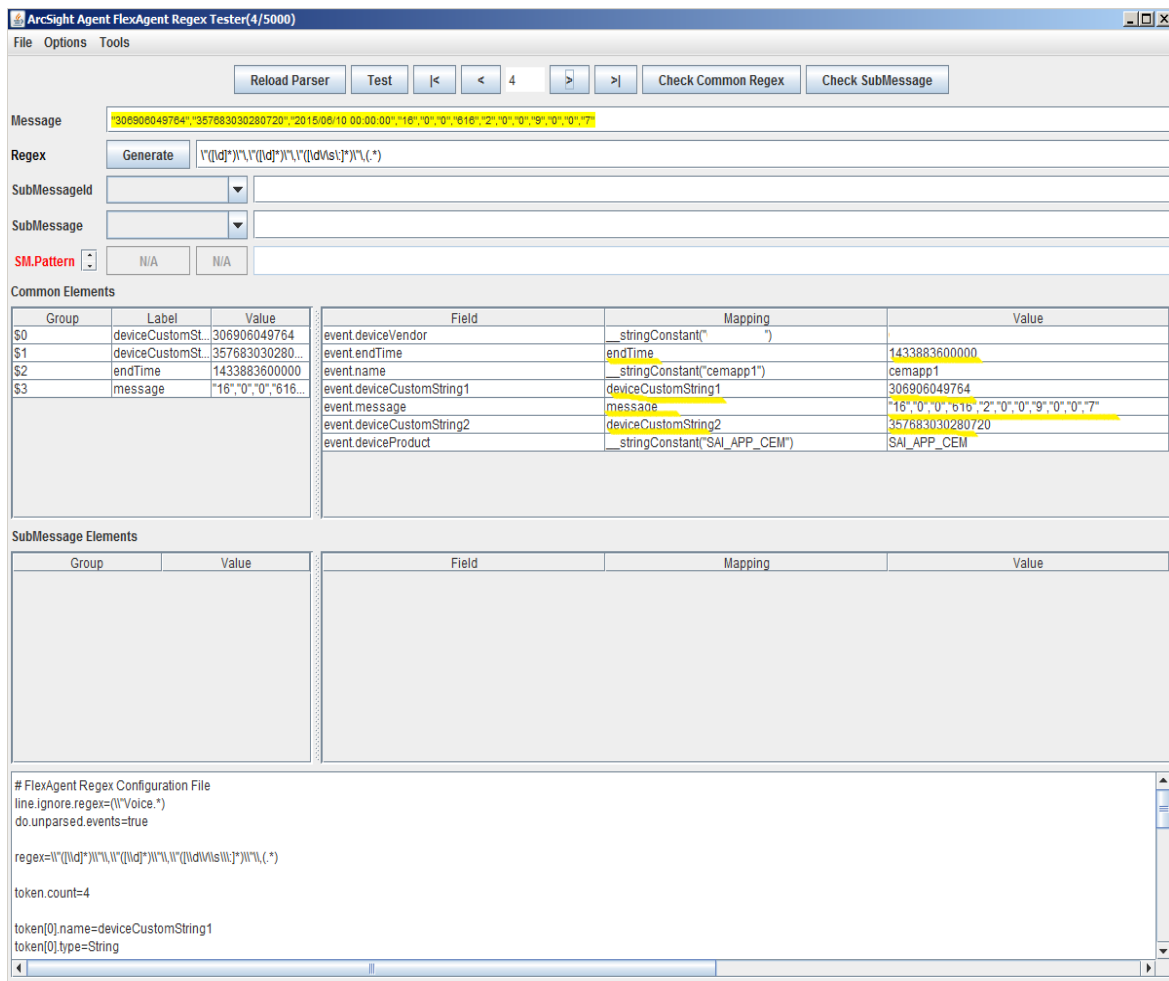


Figure 10: Regex example

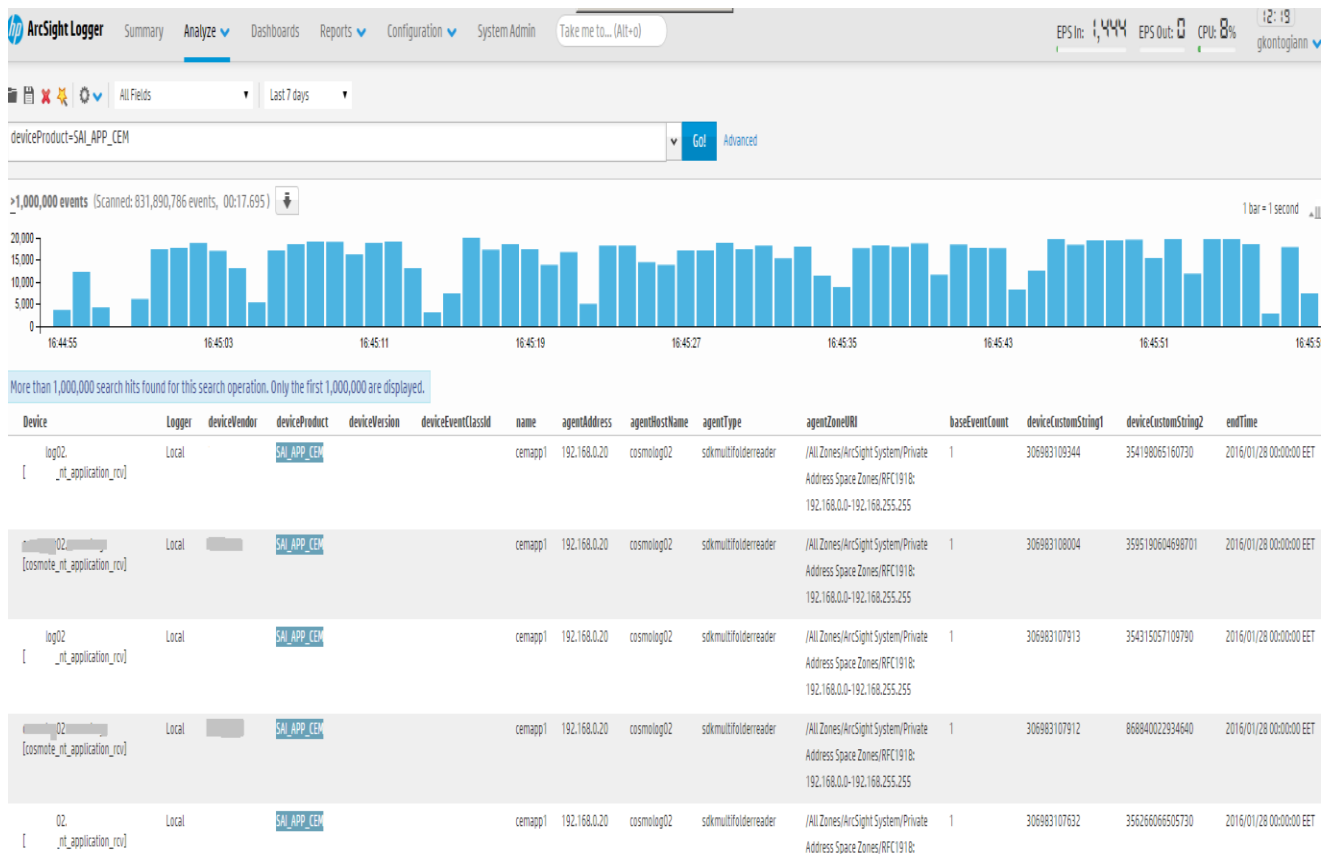
It seems that the mapping has done correctly and the fields have taken their values. For example, **endtime** field=1433883600000 which is the time in epoch (unix timestamp). In the Arcsight logger it will be displayed in regular form.

The next step is to configure the **agent.properties** file. This file says to Arcsight connector where each log file is located in the **staging server** and also which **example.sdkrfileloader.properties** file to be used for parsing. After correct configuration of all files the connector should be restarted and if everything is correct the logs on staging server should be renamed to **log.processed**, and start forwarding to the arcsight Logger. In the following image it seems the processed logs:

```
[arcsight@cosmolog02 data]$ ls -latr .././sysai/data/
total 632852
-rw-r--r-- 1 arcsight admins 1594727 Sep  4 2014 2014-09-03_Actions On Saved Non Saved Reports.csv.processed
-rw-r--r-- 1 arcsight admins 1599902 Sep  4 2014 2014-09-02_Actions On Saved Non Saved Reports.csv.processed
drwxr-xr-x 3 arcsight admins 4096 Feb  6 2015 ..
-rw-r--r-- 1 arcsight admins 2036053 Jan 30 08:20 2016-01-29_cemdb01.zip
-rw-r--r-- 1 arcsight admins 5087725 Jan 30 08:25 2016-01-29_cemdb02.zip
-rw-r--r-- 1 arcsight admins 108693904 Jan 30 08:28 2016-01-29_cemapp1.zip
-rw-r--r-- 1 arcsight admins 4665688 Jan 30 08:33 2016-01-29_cemapp2.zip
-rw-r--r-- 1 arcsight admins 411249 Jan 30 08:45 2016-01-27_cemapp1_actions_on_saved_nonsaved_reports.CSV.sanitized.2.processed
-rw-r--r-- 1 arcsight admins 55534718 Jan 31 03:03 2016-01-31_cemapp1_CEM.CSV.processed
-rw-r--r-- 1 arcsight admins 27097145 Jan 31 08:20 2016-01-30_cemdb01.zip
-rw-r--r-- 1 arcsight admins 4948591 Jan 31 08:25 2016-01-30_cemdb02.zip
-rw-r--r-- 1 arcsight admins 86250907 Jan 31 08:28 2016-01-30_cemapp1.zip
-rw-r--r-- 1 arcsight admins 4611171 Jan 31 08:33 2016-01-30_cemapp2.zip
-rw-r--r-- 1 arcsight admins 397109 Jan 31 08:45 2016-01-30_cemapp1_actions_on_saved_nonsaved_reports.CSV.sanitized.processed
-rw-r--r-- 1 arcsight admins 25401772 Feb  1 08:20 2016-01-31_cemdb01.zip
-rw-r--r-- 1 arcsight admins 4926351 Feb  1 08:25 2016-01-31_cemdb02.zip
-rw-r--r-- 1 arcsight admins 81110055 Feb  1 08:28 2016-01-31_cemapp1.zip
-rw-r--r-- 1 arcsight admins 4642094 Feb  1 08:33 2016-01-31_cemapp2.zip
-rw-r--r-- 1 arcsight admins 397109 Feb  1 08:45 2016-01-30_cemapp1_actions_on_saved_nonsaved_reports.CSV.sanitized.1.processed
-rw-r--r-- 1 arcsight admins 416120 Feb  2 03:37 2016-02-02_cemapp1_actions_on_saved_nonsaved_reports.CSV
-rw-r--r-- 1 arcsight admins 11176284 Feb  2 08:20 2016-02-01_cemdb01.zip
-rw-r--r-- 1 arcsight admins 5217662 Feb  2 08:25 2016-02-01_cemdb02.zip
-rw-r--r-- 1 arcsight admins 85532591 Feb  2 08:28 2016-02-01_cemapp1.zip
-rw-r--r-- 1 arcsight admins 4678897 Feb  2 08:33 2016-02-01_cemapp2.zip
-rw-r--r-- 1 arcsight admins 397109 Feb  2 08:45 2016-01-30_cemapp1_actions_on_saved_nonsaved_reports.CSV.sanitized.2.processed
-rw-r--r-- 1 arcsight admins 15131780 Feb  3 08:20 2016-02-02_cemdb01.zip
-rw-r--r-- 1 arcsight admins 5090037 Feb  3 08:25 2016-02-02_cemdb02.zip
-rw-r--r-- 1 arcsight admins 95710837 Feb  3 08:28 2016-02-02_cemapp1.zip
-rw-r--r-- 1 arcsight admins 4707033 Feb  3 08:33 2016-02-02_cemapp2.zip
drwxr-xr-x 2 arcsight admins 73728 Feb  3 08:36
-rw-r--r-- 1 arcsight admins 418290 Feb  3 08:45 2016-02-02_cemapp1_actions_on_saved_nonsaved_reports.CSV.sanitized.processed
[arcsight@cosmolog02 data]$
```

**Figure 11: Processed logs example**

The final result in the Arcsight Logger should be the following:

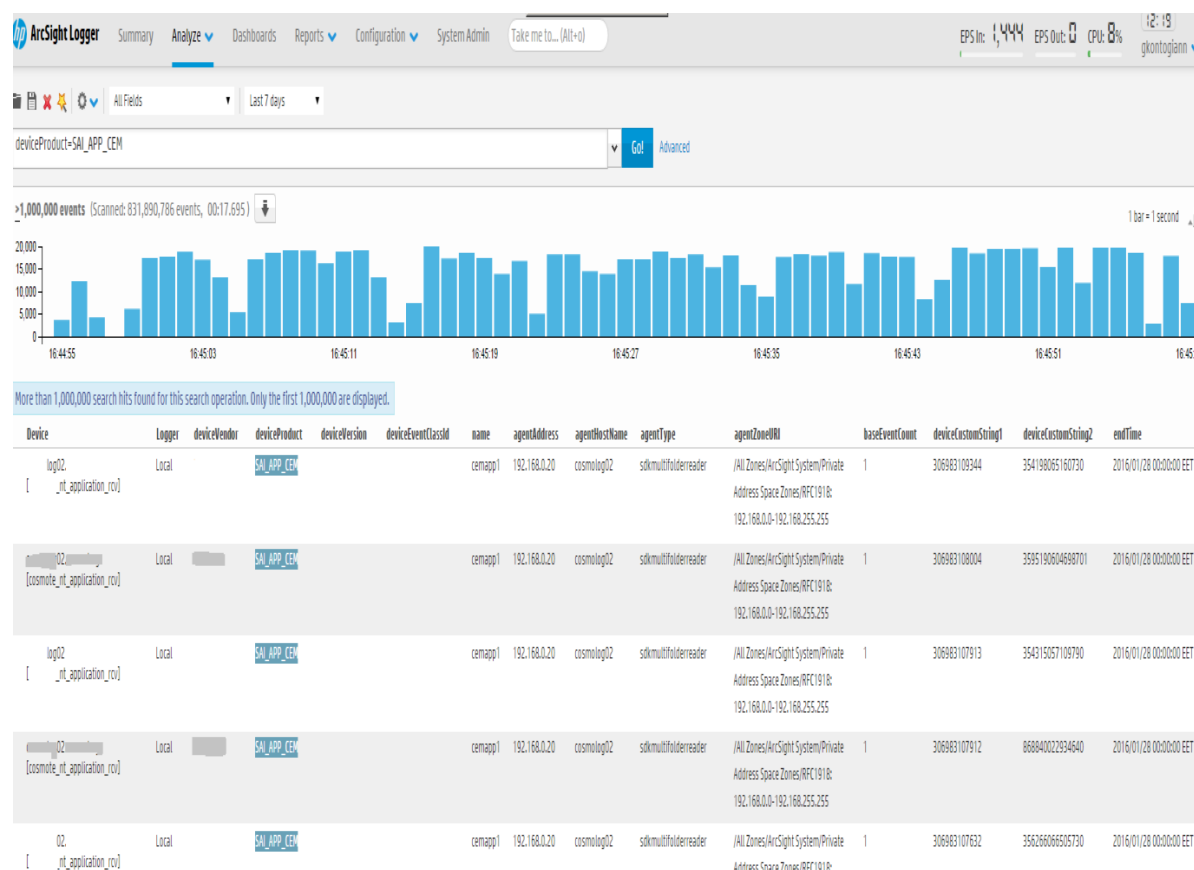


**Figure 12: Arcsight Logger application log example**

Log is now separated into fields and it's easier for the security analyst to read it and to deduce useful information.

### 3.5 Capabilities of Arcsight Logger

After forwarding the logs to the Arcsight logger, time has come for the real development of the Arcsight.



**Figure 13: Arcsight Logger application log example**

The raw log is now separated into several fields like:

- **deviceProduct:** SAI\_APP\_CEM → it's the mapped name of the log. Analyst uses this name in order to search for all the logs of this system.
- **agentHostName :** cosmology → it's the staging server where the logs are stored.

- **agentType** : sdkmultifolder → it's the kind of the used connector.
- **deviceCustomString1**: 3069831XXXXX → it's the content of the log
- **deviceCustomString2**: 35419XXXXXXXXXX → it's the content of the log
- **endTime**: 2016/01/28 → it's the time of the log creation

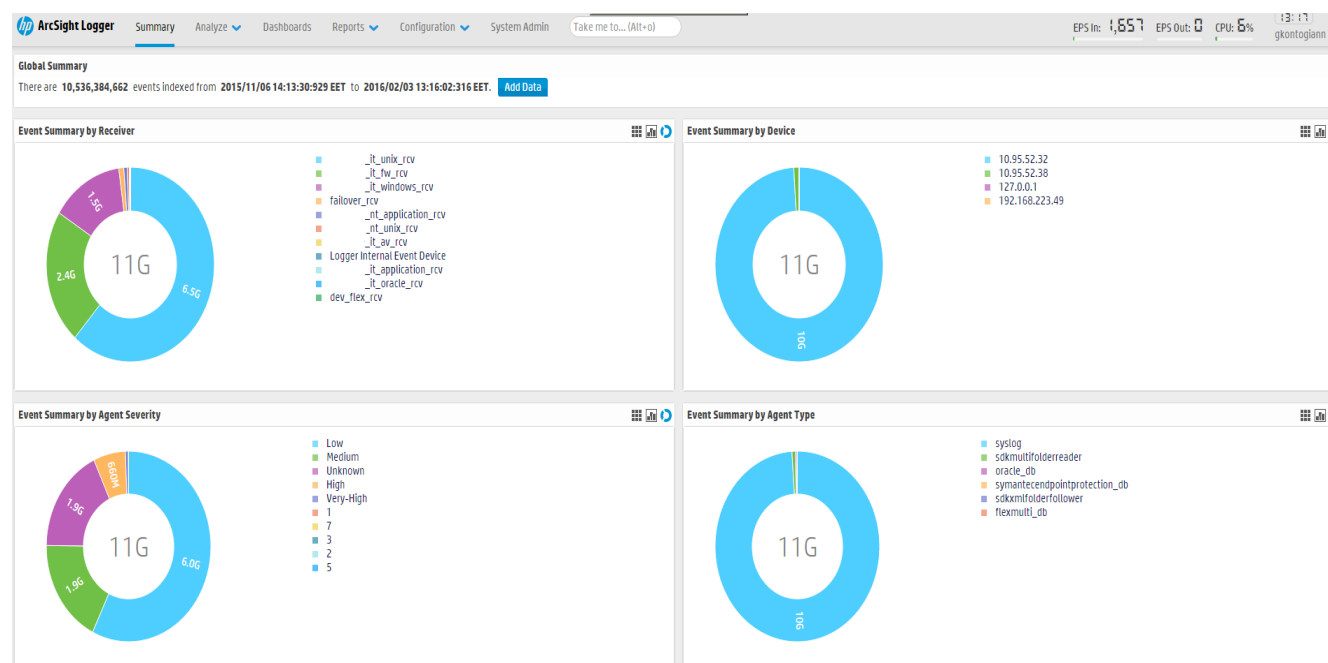
Arcsight support many fields to map big raw logs. At any case that the fields are not enough to cover the log, after a given point information can be added to a single field.

One use of the Arcsight Logger is for searching events from security incidents. It can present logs a depth of two months time in order to give a detailed view of what happened. It's highly efficient and performs the log research in a very short time. It gives the opportunity to deepen research by presenting specific log fields. This can be achieved using a Query and by using indicators like “CONTAINS”, “NOT CONTAINS”, “!=”, AND, OR, etc. For example in the image above a Query could be:

**“deviceProduct=SAI\_CEM\_APP and deviceCustomString1!=3069831XXXXX”**

This query will display all the logs except logs with deviceCustomString1=3069831XXXXX.

The image above presents the overview of the Arcsight Logger:



**Figure 14: Arcsight Logger overview**

In this view appears all the receivers (unix, firewall, windows, oracle, etc) which collects the logs to Logger. Also this view appears a generic viewpoint of the Logger like how much data size is stored, which is the severity of each event, etc.

3.5.1 Logger charts

Another useful usage of the Arcsight Logger is the charts. It can group the logs (with the proper query) and display them in charts, like the chart below:

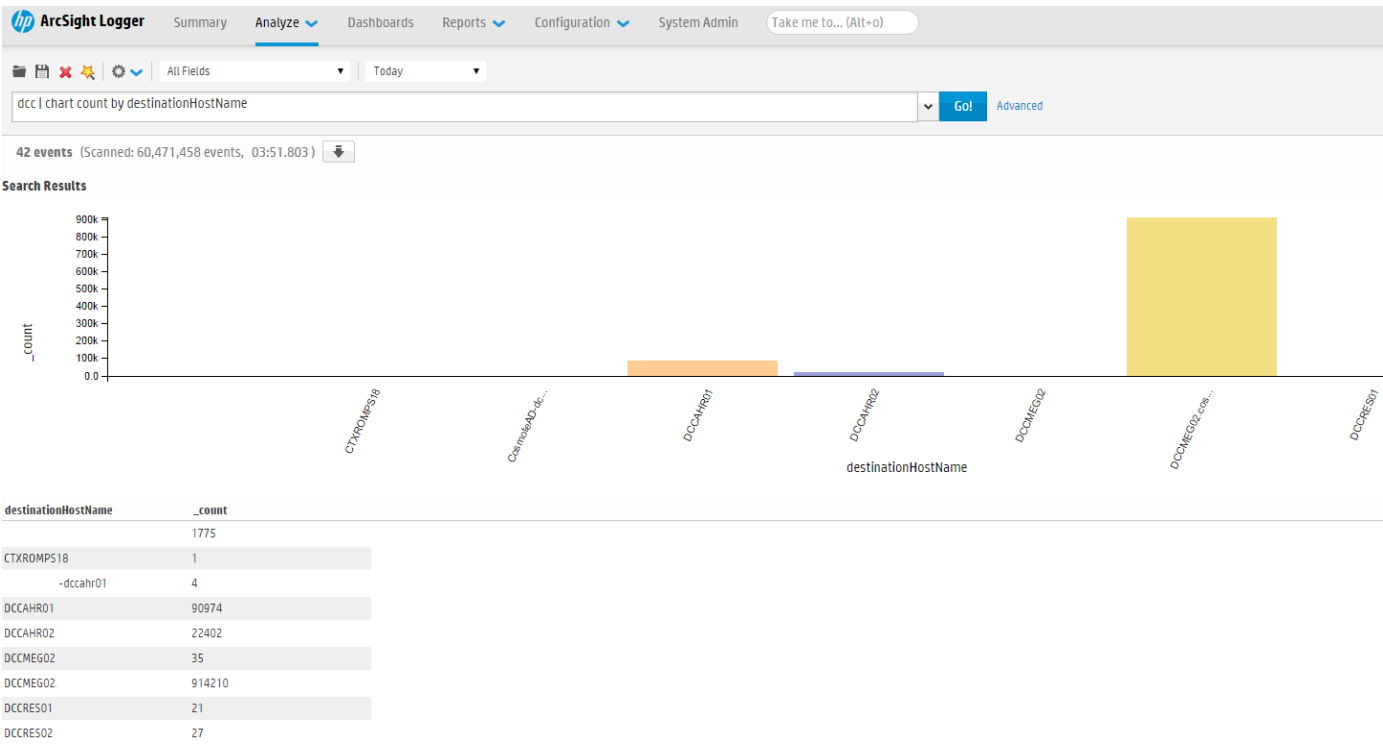


Figure 15: Domain Controllers chart

Here is presented a chart showing the logs from the domain controllers grouped by the name of each one. This can be performed by using the Query: “**dcc | chart count by destinationHostName**”. DestinationHostName contains the name of each domain controller.

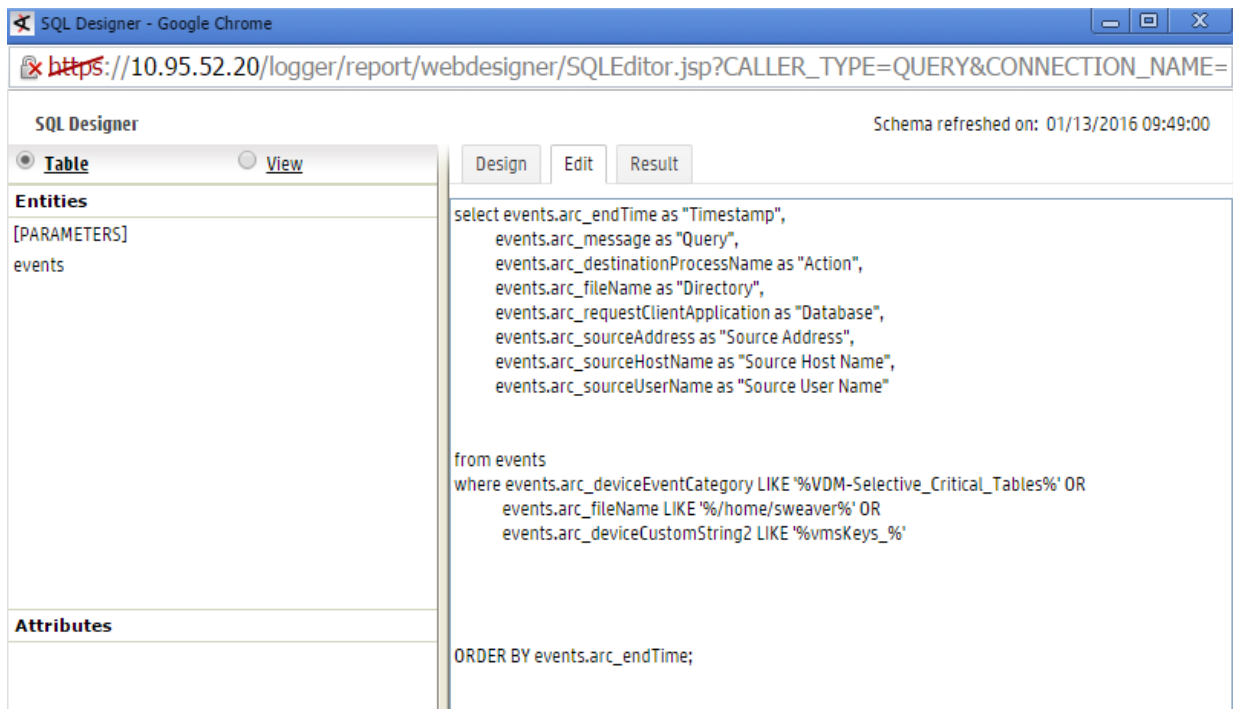
This chart presents an overview about pc’s logins and logouts and gives the opportunity to analyst to know if one day there are an increased number of incidents.

### 3.5.2 Logger Reporting

Moreover, the Arcsight Logger provides the capability of reporting. Daily log reporting is a very important stage of a big company's **Information Security Section**, because it offers an automated daily running procedure which produces an analytic report for every corporate system in the company. In this way the company's staff checked if there is an insider security incident. Furthermore security reports are also useful for the compliance audits from ADAE, as they present an analytical representation of what happened in a specific time period.

Reports can be easily created by using queries. After creating the appropriate query, it is stored in a report and the report scheduled to run daily at a specific time. The security analyst can export the query from logger and evaluate the results.

The image above shows the query used for one scheduled report:



**Figure 16: Scheduled Report Query**

The **SELECT** clause is used for choosing so the appropriate Arcsight fields that will be displayed in the report as the name of fields that will displayed in the report. Also the **WHERE** clause is used to extract only those records that fulfill a specified criterion. Finally the events will be order by **endTime** using the **ORDER BY** clause.

The result of the report shown above:

VDM - VMS								
Start Time: 10/31/15 11:56 AM Scan Limit: 100000			End Time: 11/04/15 11:56					
Timestamp	Action	Directory	Query	Database	Source Address	Source Host Name	Source User Name	
1/11/15 12:20 mp		/usr/bin/gzip /home/sweaver/log*log.Z*					sweaver	
1/11/15 3:35 mp	/bin/tar						root	
1/11/15 3:35 mp		/usr/bin/python /home/sweaver/scripts/backup/backup_vms.py > /home/sweaver/backup.log						
1/11/15 3:35 mp	/bin/tar	/home/sweaver/vmKeys/key/StoreKey.reg						
1/11/15 3:35 mp	/bin/tar							
1/11/15 3:35 mp		/home/sweaver/vmKeys/key/Store.reg						
2/11/15 12:20 mp		/usr/bin/gzip /home/sweaver/log*log.Z*					sweaver	
2/11/15 12:40 mp		/usr/bin/find /home/sweaver/log/ -name "*.gz" -daystart -mtime +20 -exec bash -c 'rm "311" - {} \;					sweaver	
2/11/15 3:35 mp		/usr/bin/python /home/sweaver/scripts/backup/backup_vms.py > /home/sweaver/backup.log					root	
2/11/15 3:35 mp	/bin/tar							
2/11/15 3:35 mp	/bin/tar							
2/11/15 3:35 mp		/home/sweaver/vmKeys/key/Store.reg						
2/11/15 3:35 mp	/bin/tar	/home/sweaver/vmKeys/key/StoreKey.reg						
2/11/15 10:19 mp								
2/11/15 10:33 mp								
2/11/15 10:35 mp								

select * from	sqlplus.exe	10.95.152.189	wks01753	dmar
VMS.VMS_VOUCHER				
select * from	sqlplus.exe	10.95.152.189	wks01753	dmar
VMS.VMS_VOUCHER				
WHERE				
STATE='ACTIVATED'				
select * from	sqlplus.exe	10.95.152.189	wks01753	dmar
VMS.VMS_VOUCHER				
WHERE				
SECRETNUMBER=ebdaa3				
00637c946861086dc1770d				
e1a'				

**Figure 17: Arcsight report export**

This report shows some actions that have been made in specific folders of an enterprise system. In the yellow circle, it displayed some sql queries.

More specific, in the field:

- **Query:** select \* from.... ➔ the sql query executed.
- **Database:** sqlplus.exe ➔ type of database running.
- **Source Address:** 10.95.152.189 ➔ the ip address from where the sql query was executed.
- **Source Host Name:** wks01753 ➔ the workstation from where the sql query was executed.
- **Source User Name:** dmar ➔ the user run the query

These are only some of the main functions of the Arcsight logger. Depending on the needs of each company it can be configured properly in order to provide the desired information.

### 3.6 Capabilities of Arcsight Express/ESM



**Figure 18: Staging server to Logger or ESM**

As it mentioned above, Log collector forwards the event logs both to Arcsight Logger and Arcsight Express / ESM. The Arcsight Logger receives all kind of logs stored in the staging server, but Arcsight Express receives only the most “important” logs for editing. It is used for 24/7 real time monitoring because all its filters, rules, etc. process logs non-stop.

For top, capabilities of Arcsight Express /ESM will be presented:

#### 3.6.1 Event Correlation

After normalizing the log events for central collection and analysis, there must also be a way to correlate the events with each other. This correlation can be between events from the same source or from different sources. Manually correlating numerous logs can be a difficult process as the amount of data events produced from even a single node can yield vast amounts of information. Arcsight Express provides a means to apply pre-defined rules automatically to the collected, aggregated and normalized events. This removes the requirement for personnel to manually analyze events. Also a rule can be defined to indicate a correlation if certain log event parameters is met. These rules can be designed to highlight a correlation between events that may indicate malicious insider activity.

For example, a log event may be generated showing an employee accessing a station or office outside of normal work hours for that specific employee. In addition, log events may be generated showing a high level of printer activity from that employee’s workstation. Any or all employee actions that elicited these events may be benign, or they



may be indicative of malicious activity. By correlating the events, a deeper picture of that employee's overall network activities can be derived, and potential issues may be identified for further investigation.

### 3.6.2 Filters

With numerous nodes providing log events, it becomes necessary to filter out some log event inputs and concentrate on the important events. Important, in this context, means those events that are deemed most likely to provide meaningful security cueing information. Filters are used to reduce the overall amount of events processed by the SIEM. Filters can be designed to be broad or narrow in the scope of events they filter. For example, an administrator may wish to only include log events from certain workstations or IP addresses, or during a specific time period, or even certain applications involved. Filters can be specified to focus on these events for evaluation and they can also be used as components of a SIEM rule. Within the ArcSight SIEM product, filters are a basic component used in rule development. They are a “set of conditions that focus on particular event attributes”. The filters select only the events that match those conditions for further processing by the SIEM. A filter is defined using ArcSight's Common Conditions Editor, and once defined it can be saved as a named conditions filter that allows it to be used by other resources of the SIEM. Rules can then easily implement those named condition filters as components of the overall rule without having to define the same filter over and over.

### 3.6.3 Rules

Rules are used within a SIEM to evaluate events received from normalized log data that will produce a certain result. Rules within ArcSight are typically created using a combination of previously defined filters “joined together” using Boolean logic (e.g., AND, OR, NOT). The intent is to design rules to perform some useful security action when the semantics of some select subset of events collectively indicate the existence, or possibility of existence, of a security policy violation. Aggregation within rules allows for 12 for responses to be triggered after a specified number of occurrences within a specified time frame. This can be useful in recognizing patterns of activities and can also reduce false positives based on single occurrence events. Rules within ArcSight can be configured to take one or more actions based on one event, multiple events, event

thresholds, or some minimum number of events occurring within some specified time interval(s).

When the previously defined conditions of a rule are met within ArcSight, a correlation event occurs and is added to the database, highlighting the important event for SIEM operators. In addition to generating correlation events, matched rules can also perform previously defined actions. Two example actions are: 1) sending notifications to designated personnel, and 2) executing a mitigating response action such as shutting down an infected node.

### 3.6.4 Dashboards

The use of dashboards within SIEMs allows for a convenient central location for monitoring an organization's network activity. The various logs from nodes connected to the SIEM can be used as data sources for display on the dashboard. The dashboard may be configured to display a variety of information related to the dashboard monitor's advertised usage and functionality, or some other tailor-made information that supports the unique needs of an organization. If an item of interest or an alert shows up on a SIEM dashboard, the SIEM operator interface allows the operator to drill-down on the information regarding the event in order to more closely inspect and analyze the activity.

### 3.6.5 Active Lists

Active lists are comparable to a type of watch list as described in previous chapters. Active lists are typically used within ArcSight Express in "conjunction with rules specifically tailored to interact with and populate the lists dynamically". Rules are written to populate the list with certain data items of interest. Basically, the active list is a "shell to store/display the data" populated by any particular rule. In addition to being populated *dynamically* with rules driven data, active lists can also be populated *manually* with static entries. Active lists can also be used as input conditions for use in other rules.

## 4. Arcsight Express / ESM usage in a big company

In this section will be presented some Arcsight Express / ESM use case scenarios in a big company/organization. The screenshots have been taken from a real organization so some data is altered, in order to maintain company's anonymity. These scenarios will help to understand better the whole operation of Arcsight and the capabilities offered. Moreover it will be presented who the log events can be correlated and combined in order to perform an investigation about a security event that occurred.

The following image presents an overview about logs import in the Arcsight Express / ESM. Moreover, it can be used for performance control and possible error detection:

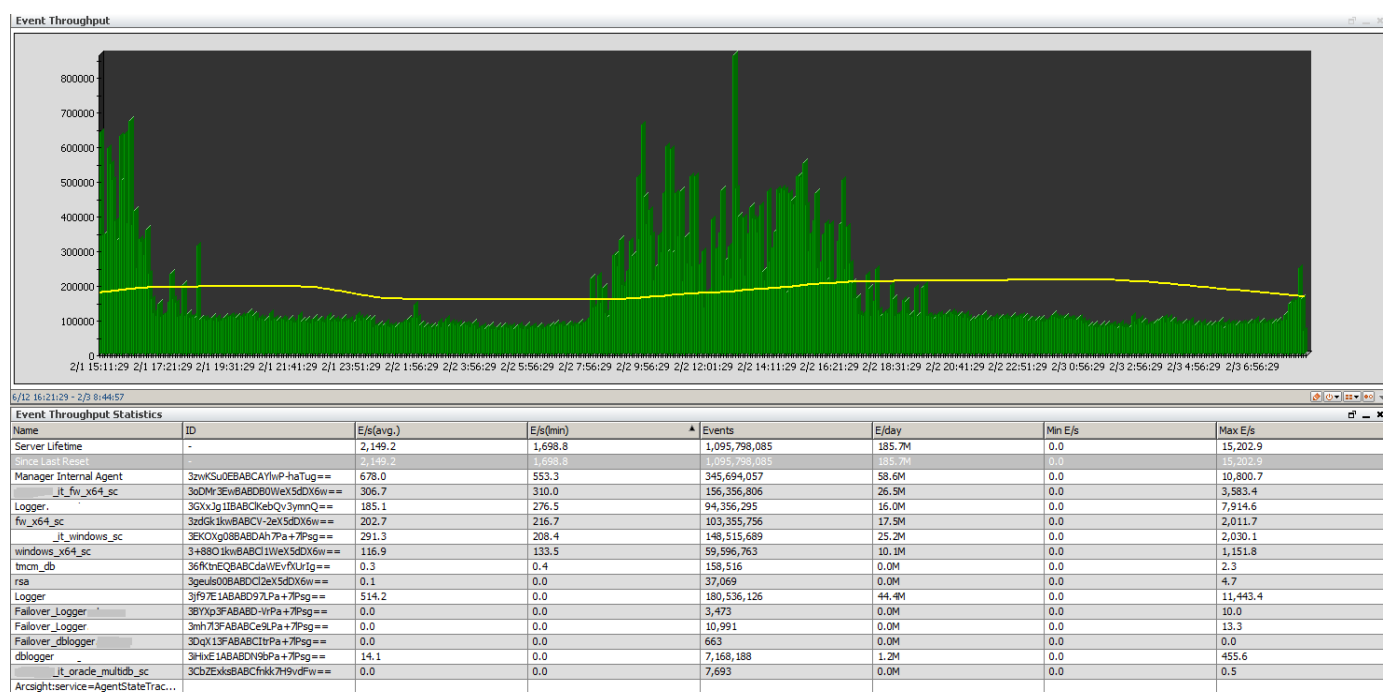


Figure 19: Arcsight Express / ESM overview

It shows the graphic representation of the number of logs that coming in, in real time and also it gives a statistical analysis about the number of events/sec that each connector forwards to Arcsight / ESM.

## 4.1 OS Failed Login Attempts

In this scenario, the Operating System's logs about login and logout will be analyzed. Each operation system produces a log event when logs in the company network. The Active Channel above monitors all the failed login attempts that are made by the users in the company network:

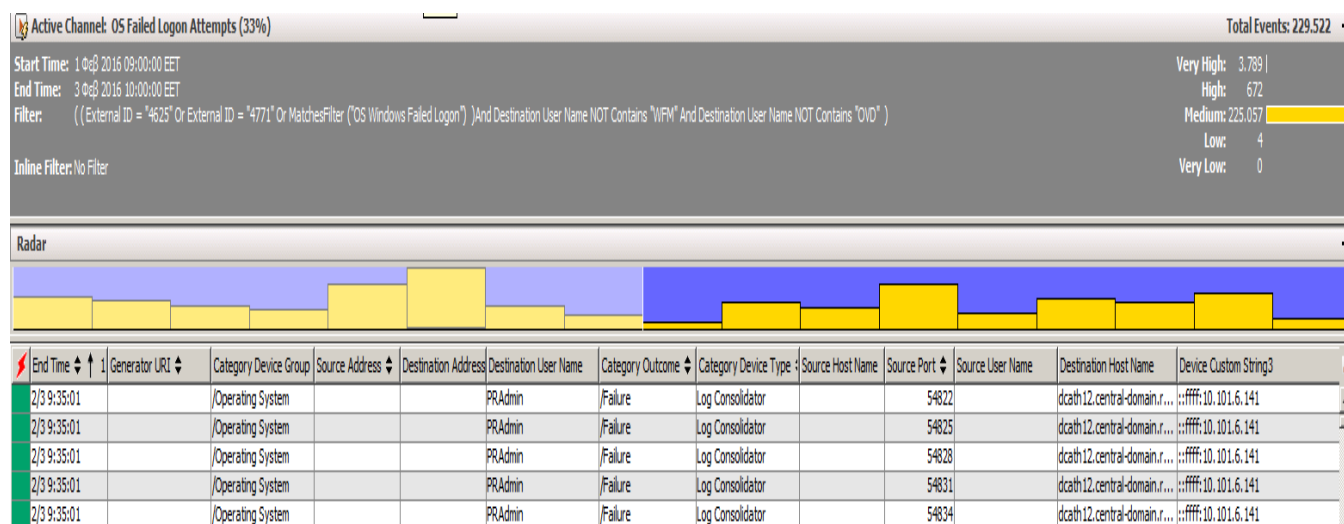


Figure 20: OS Failed Login Attempts – Active Channel

### Active Channel: OS Failed Logon Attempts

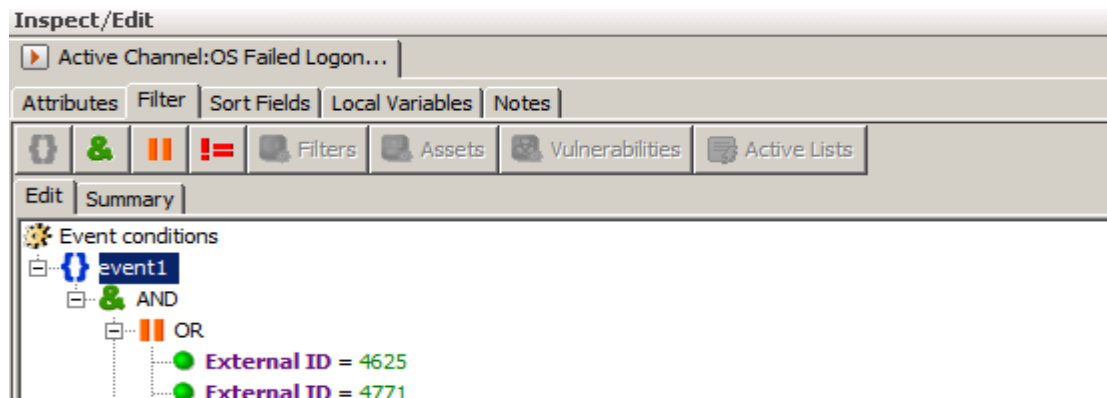
- **End Time:** 2/3 9:35:01 → indicates the time that the event occurred.
- **Category Device Group:** /Operating System → indicates the type of the system.
- **Destination User Name:** PRAAdmin → indicates the username that made the failed attempt.
- **Category Outcome:** /Failure → indicates the result of the attempt (failed)
- **Destination Host Name:** dcath12.centra-domain..... → Indicates the domain controller which recorded the failed login attempt.
- **Device Custom String 3:** 10.101.6.141 → indicates the ip address of the user pc that made the login attempt.

In order to create the Active channel above, the **Windows event ids** used. Event id is a 4 digit number that each one indicates specific event. In this case, the event ids 4625 and 4771 are used.

Event id **4625**: An account failed to log on → this is a useful event because it documents each and every failed attempt to logon to the local computer regardless of logon type, location of the user or type of account.

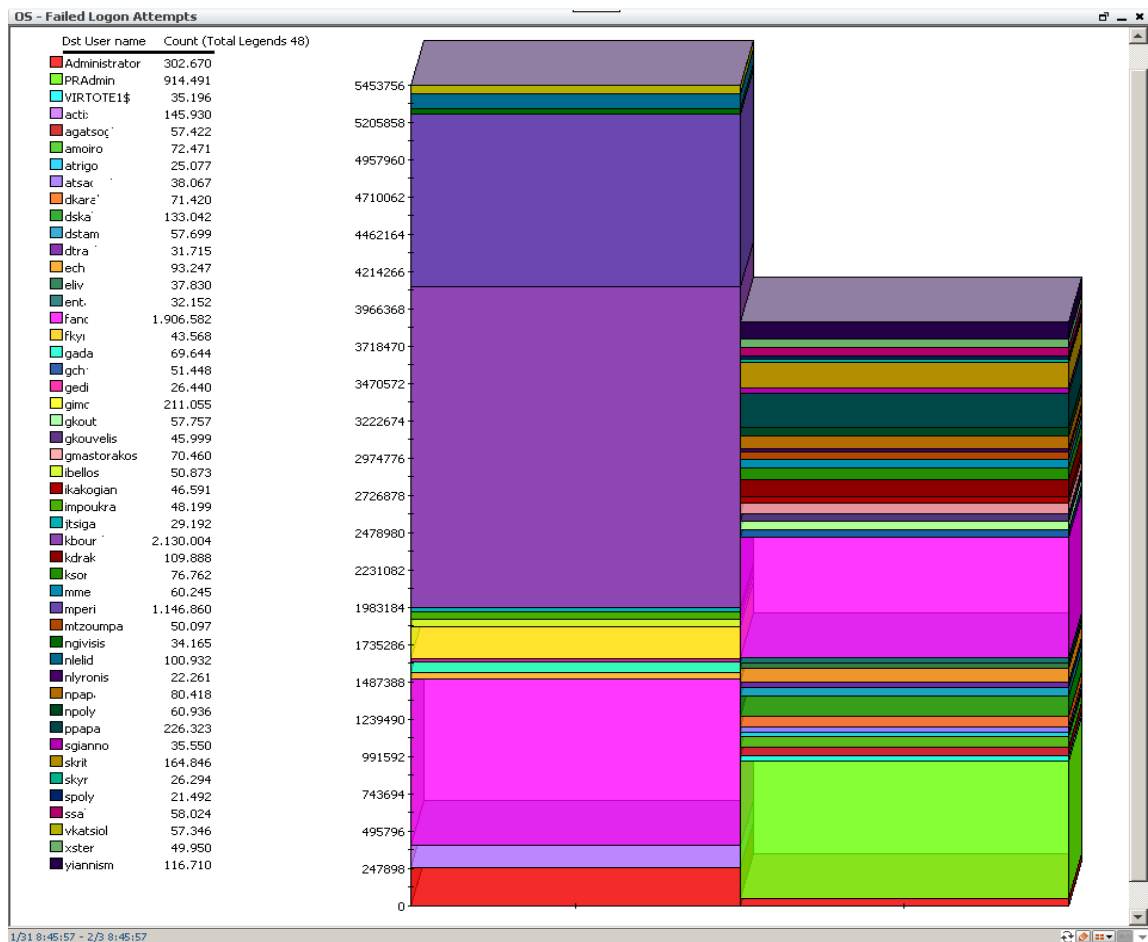
Event id **4771**: Kerberos pre-authentication failed ➔ this event is logged on domain controllers only and only failure instances of this event are logged.

So the filter that used for the Active Channel above is the following:



**Figure 21: OS Failed Login Attempts – Filter**

Finally in order to have a better view about the number of events in a specific period (like a week, or a month), a dashboard is used. The following image displays the results of a dashboard for the period of 2 weeks:



**Figure 22: OS Failed Logon Attempts – Dashboard**

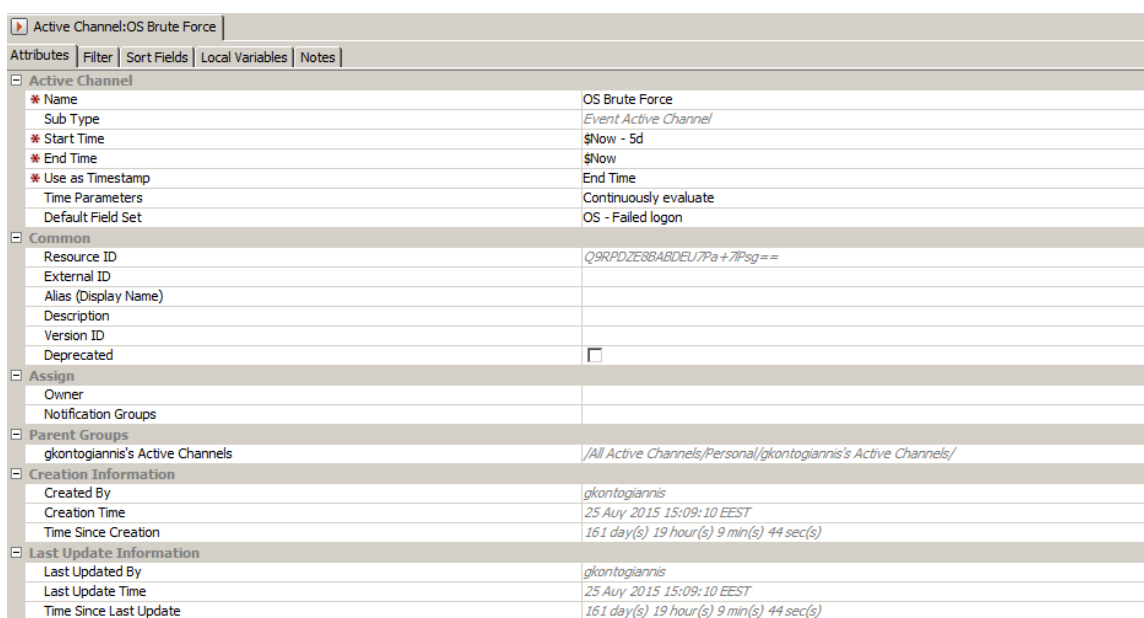
It displays all the failed login attempts made in 2 weeks, and counts the number of failed login attempts that each user made.

By this view, the security analyst can comprehend if something going wrong (some user doing failed login attempts all the time) and investigate the incident.

## 4.2 OS Brute Force Login Attempts

In the previous sector was presented the monitoring of Windows failed logon attempts. In order to have a better view about the failed attempts the simple monitoring of events isn't enough. It should be used event correlation in order to have clear view for a brute force attack for example. The following figures show the active channels, the filters and the rules for monitoring brute force login attempts in Operating Systems.

In this scenario a brute force login attempt considered the event occurring 5 “same” failed login attempts over a period of 2 minutes. The following images display the configuration of an active channel for monitoring Brute force login attempts for Operating Systems:



Active Channel: OS Brute Force	
Attributes   Filter   Sort Fields   Local Variables   Notes	
Active Channel	
Name	OS Brute Force
Sub Type	Event Active Channel
Start Time	\$Now - 5d
End Time	\$Now
Use as Timestamp	End Time
Time Parameters	Continuously evaluate
Default Field Set	OS - Failed logon
Common	
Resource ID	Q9RPDZE88ABDEU7Pa+7Ifsg==
External ID	
Alias (Display Name)	
Description	
Version ID	
Deprecated	<input type="checkbox"/>
Assign	
Owner	
Notification Groups	
Parent Groups	
gkontogiannis's Active Channels	/All Active Channels/Personal/gkontogiannis's Active Channels/
Creation Information	
Created By	gkontogiannis
Creation Time	25 Aug 2015 15:09:10 EEST
Time Since Creation	161 day(s) 19 hour(s) 9 min(s) 44 sec(s)
Last Update Information	
Last Updated By	gkontogiannis
Last Update Time	25 Aug 2015 15:09:10 EEST
Time Since Last Update	161 day(s) 19 hour(s) 9 min(s) 44 sec(s)

**Figure 23: OS Brute Force Login Attempts – Active Channel**

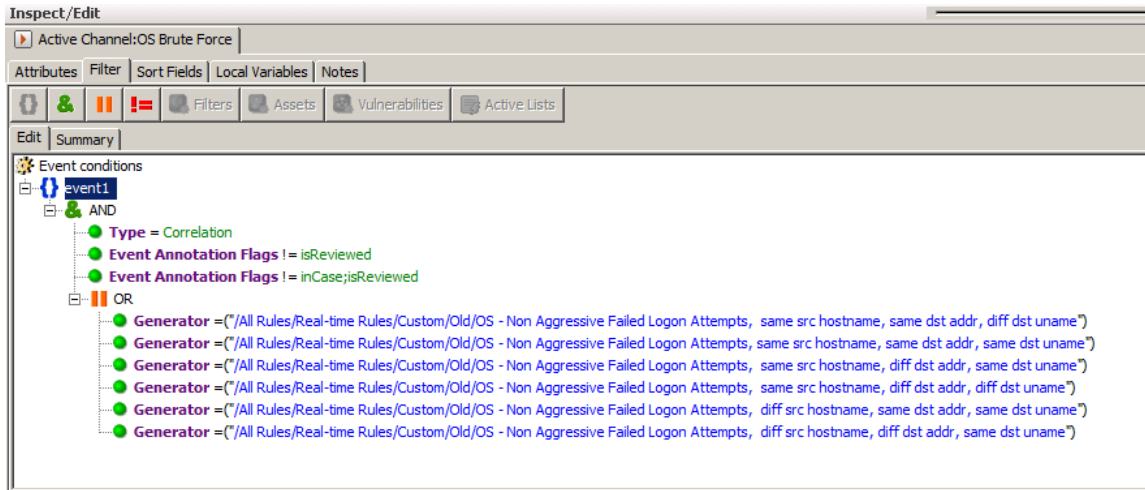
- **Start Time:** \$Now – 5d → indicates the time frame that the active channel will run
- **Time Parameters:** Continuously evaluate → indicates if the active channel will run once or continuously.

The next image shows all the rules that have been attached to active channel. Brute force login attack can be separated into the following categories:

Brute force attack from:

- **Same** source hostname & **same** destination address & **different** destination username
- **Same** source hostname & **same** destination address & **same** destination username

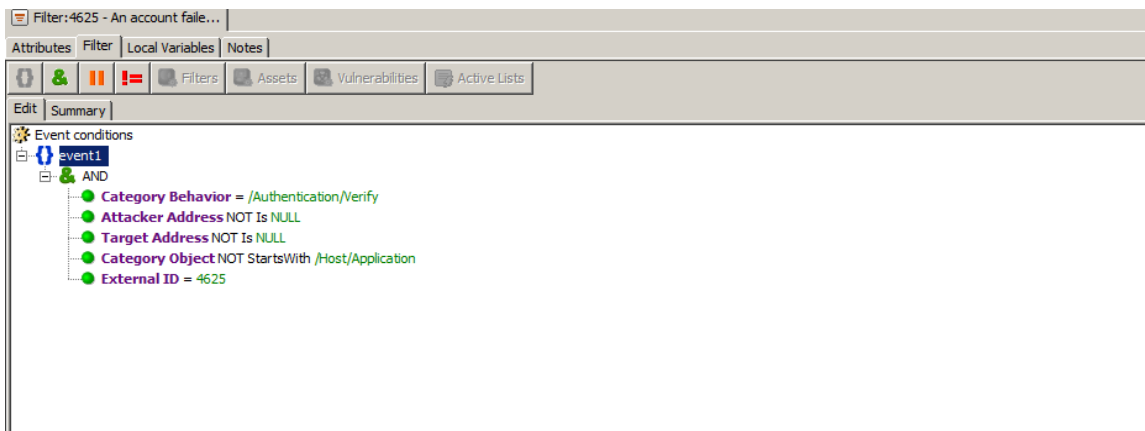
- **Same** source hostname & **different** destination address & **same** destination username
- **Same** source hostname & **different** destination address & **different** destination username
- **Different** source hostname & **same** destination address & **same** destination username
- **Different** source hostname & **different** destination address & **same** destination username



**Figure 24: OS Brute Force Login Attempts – Active Channel Filter**

Generator is the rule used and **Type=Correlation** → indicates that the results of active channel will be only correlated events.

The Active Channel uses the same filters as the sector **4.1** namely the windows event ids: **4625 & 4771**



**Figure 25: OS Brute Force Login Attempts –event id 4625 filter**

By this view, the security analyst can be alerted if a malicious entity performs a brute force attack in order to take access to a corporate system.



## 4.3 DB Failed Login Attempts

In this scenario, the Databases logs about login and logout will be analyzed. The Active Channel above monitors all the Database failed login attempts that are made by the users in the company network:

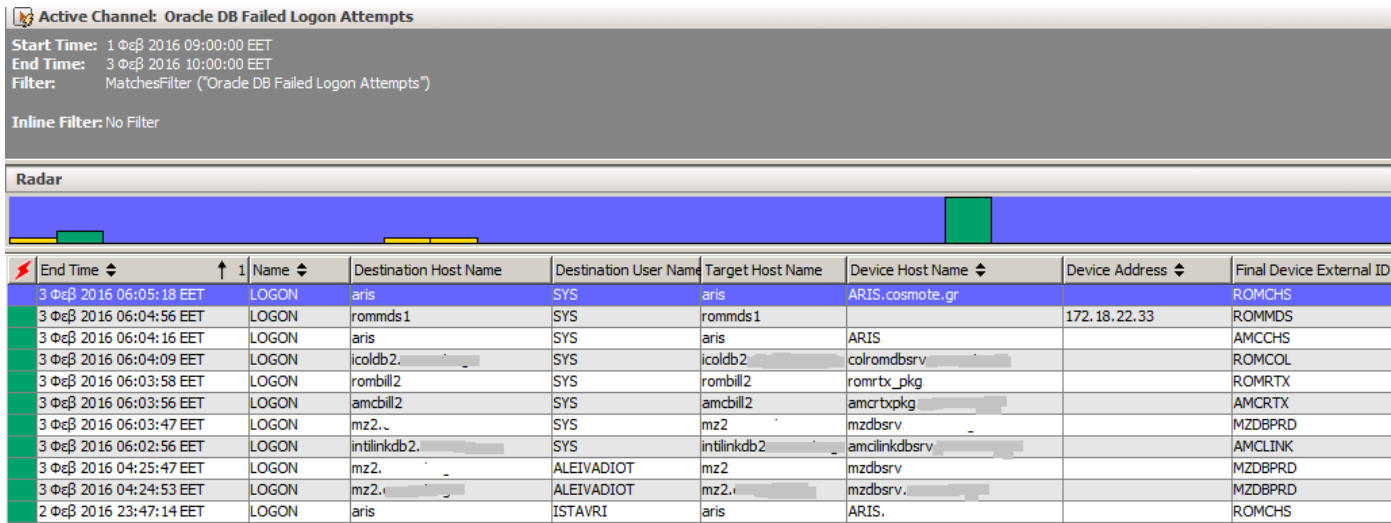
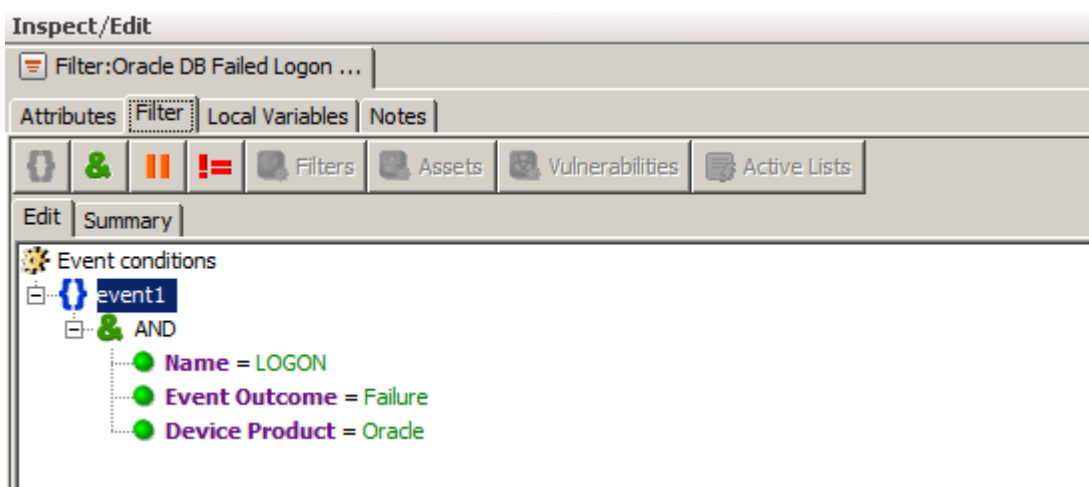


Figure 26: DB Failed Login Attempts – Active Channel

### Active Channel: DB Failed Logon Attempts

- **End Time:** 3 feb 2016 06:05:18 EET → indicates the time that the event occurred
- **Destination Host Name:** aris → indicates the name of the system where made the failed login attempt.
- **Destination User Name:** SYS → indicates the username which used to make the failed login attempt.
- **Device Address:** 172.18.22.33 → indicates the ip address of the Database

In order to create the Active Channel above was used the following filter:



**Figure 27: DB Failed Login Attempts – Filter**

- **Name:** LOGON → indicates the name of the events that will be filtered.
- **Event outcome:** Failure → indicates the result of the login attempt.
- **Device Product:** Oracle → indicates the kind of device that will be monitored (in this scenario its Oracle database)

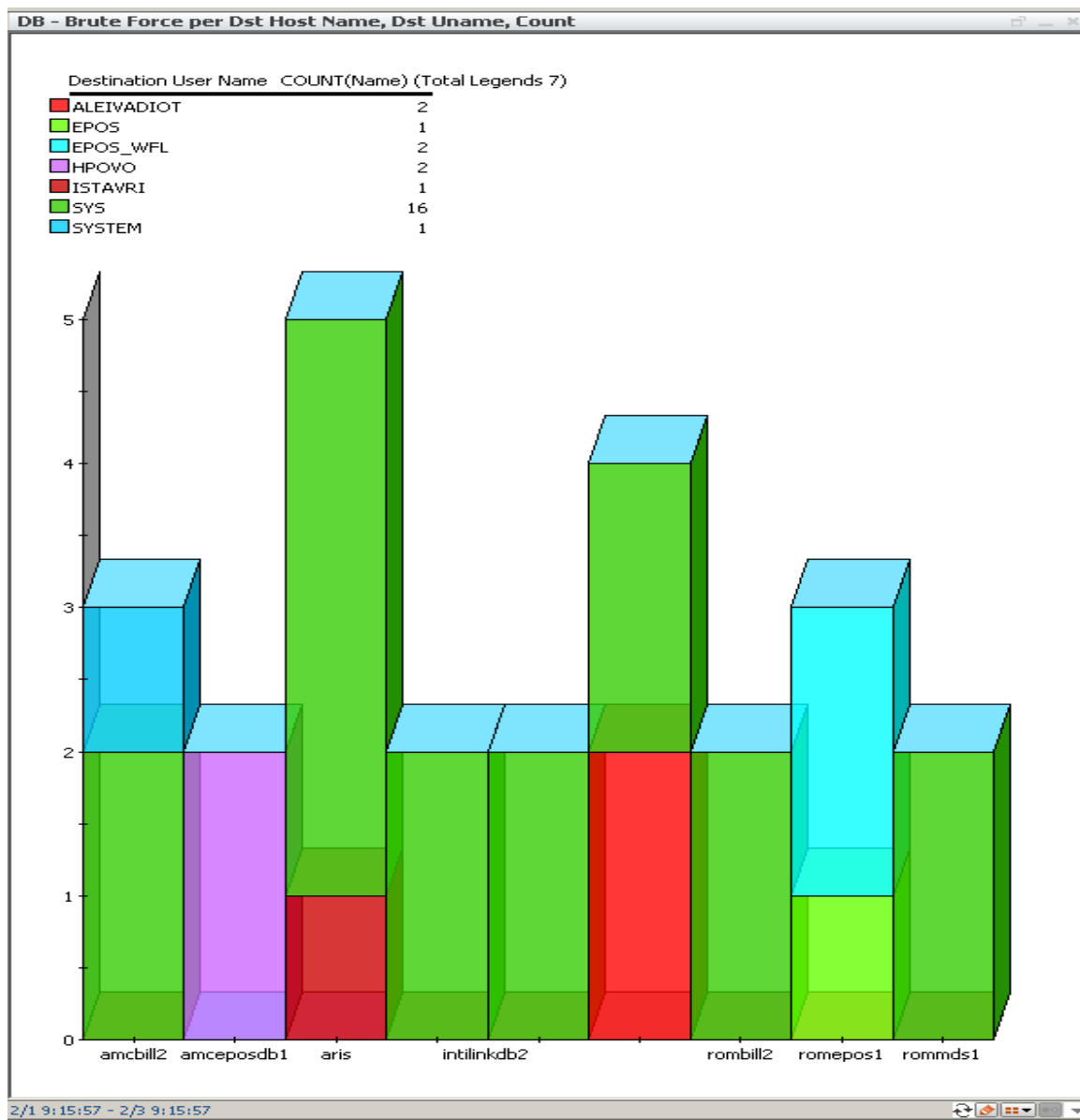
Also, it is possible to open a specific event of arcsight Express in order to make an investigation with all the fields provided. All the fields displayed in the following image:

Event Inspector	
Description	
Events	
LOGON	
Event Details Annotations Payload	
Name Value	
<b>Attacker</b>	
Attacker Host Name	TPAMCONSOLE
Attacker User Name	QuestService
Attacker User ID	QuestService
<b>Target</b>	
Target Host Name	aris
Target User Name	SYS
Target Process Name	LOGON
<b>Original Agent</b>	
Original Agent Host Name	dblog02
Original Agent Address	192.168.0.20
Original Agent Zone	<Resource URI="/All Zones/ArcSight System/Private Address Space Zones/RFC1918: 192.168.0.0-192.168.255.255"/>
Original Agent Zone ID	M-fU32AABABCDVFPYAT3UdQ==
Original Agent Zone URI	/All Zones/ArcSight System/Private Address Space Zones/RFC1918: 192.168.0.0-192.168.255.255
Original Agent Zone Resource	RFC1918: 192.168.0.0-192.168.255.255
Original Agent Zone Name	RFC1918: 192.168.0.0-192.168.255.255
Original Agent Version	7.1.7.7600.0
Original Agent Time Zone	Europe/Athens
Original Agent Time Zone Offset	7200000
Original Agent ID	3Smyr8IEBABCAA3zY+LP7uw==
Original Agent Type	oracle_db
<b>Final Device</b>	
Final Device Host Name	ARIS
Final Device Version	9.2.0.6.0
Final Device Time Zone	Europe/Athens
Final Device Time Zone Offset	7200000
Final Device External ID	ROMCHS
Final Device Vendor	ORACLE
Final Device Product	Oracle
<b>Event Annotation</b>	
Event Annotation Stage	<Resource URI="/All Stages/Queued" ID="R9MHInfoAABCAssxbPIxG0g=="/>
Event Annotation Stage ID	R9MHInfoAABCAssxbPIxG0g==
Event Annotation Stage URI	/All Stages/Queued
Event Annotation Stage Resource	Queued
Event Annotation Stage Name	Queued
Event Annotation Modification Time	3 Φεβ 2016 06:06:20 EET
Event Annotation Audit Trail	1 entry
Event Annotation Version	1

Figure 28: DB Failed Login Attempts – Event Inspector

There are many fields with information about the event, but it's up to the security analyst to choose which of them will display and monitor in the Active Channel.

Finally in order to have a better view about the number of events in a specific period (like a week, or a month), a dashboard is used. The following image displays the results of a dashboard for the period of 2 weeks:



**Figure 29: DB Failed Login Attempts – Dashboard**

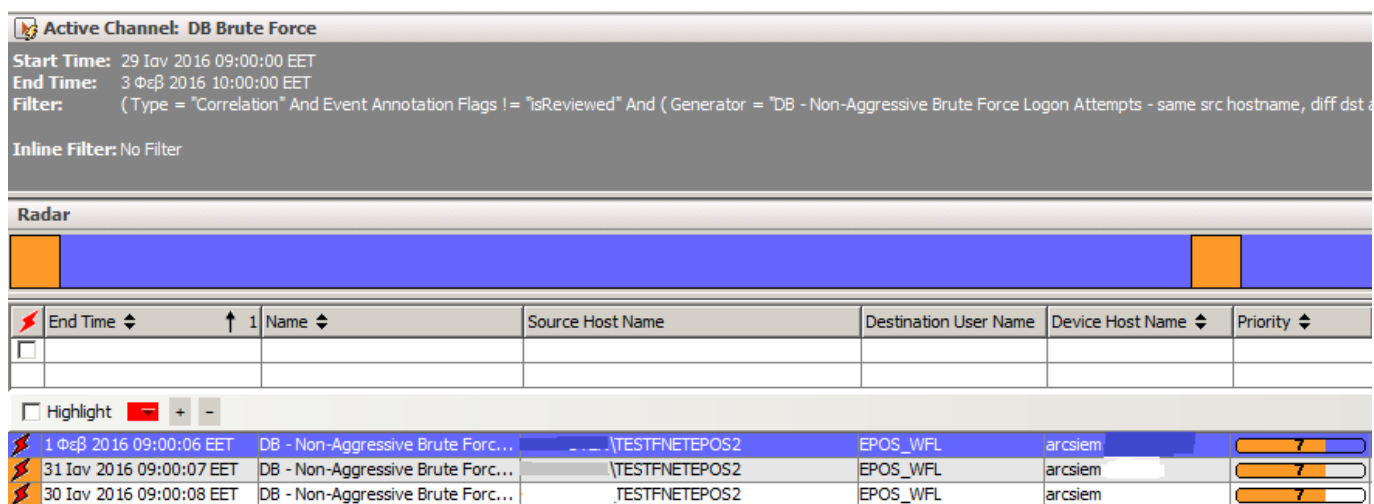
It displays all the Database failed login attempts made in last 2 weeks, and counts the number of DB failed login attempts that each user made.

By this view, the security analyst can comprehend if something going wrong (some user doing failed login attempts all the time) and investigate the incident.

## 4.4 DB Brute Force Failed Login Attempts

In the previous sector was presented the monitoring of DB failed logon attempts. As presented in the previous chapter with Windows logs, DB logs can also be correlated in order to have clear view for a brute force attack. The following figures show the active channels, the filters and the rules for monitoring brute force login attempts in Databases.

In this scenario a brute force login attempt considered the event occurring 5 “same” failed login attempts over a period of 2 minutes. The following images display the configuration of an active channel for monitoring Brute force login attempts for Databases:

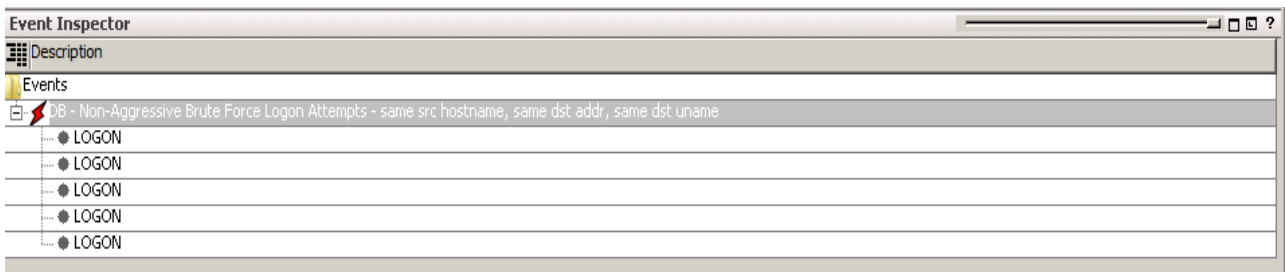


**Figure 30: DB Brute force Login Attempts – Active Channel**

This is an active channel showing the correlated events of Databases Brute force attacks. When a user make 5 consecutive failed login attempts in 2 minutes, a correlated event is generated as shown above.

- **End Time:** 1 Feb 2016 09:00:06 → indicates the time of the correlated event occurred
- **Name:** DB – Non-Aggressive Brute force login attempt → indicates the name of the event occurred
- **Source Host Name:** TESTFNETEPOS2 → indicates the name of the Database
- **Destination User Name:** EPOS\_WFL → indicates the username who used in the brute force login attempt.

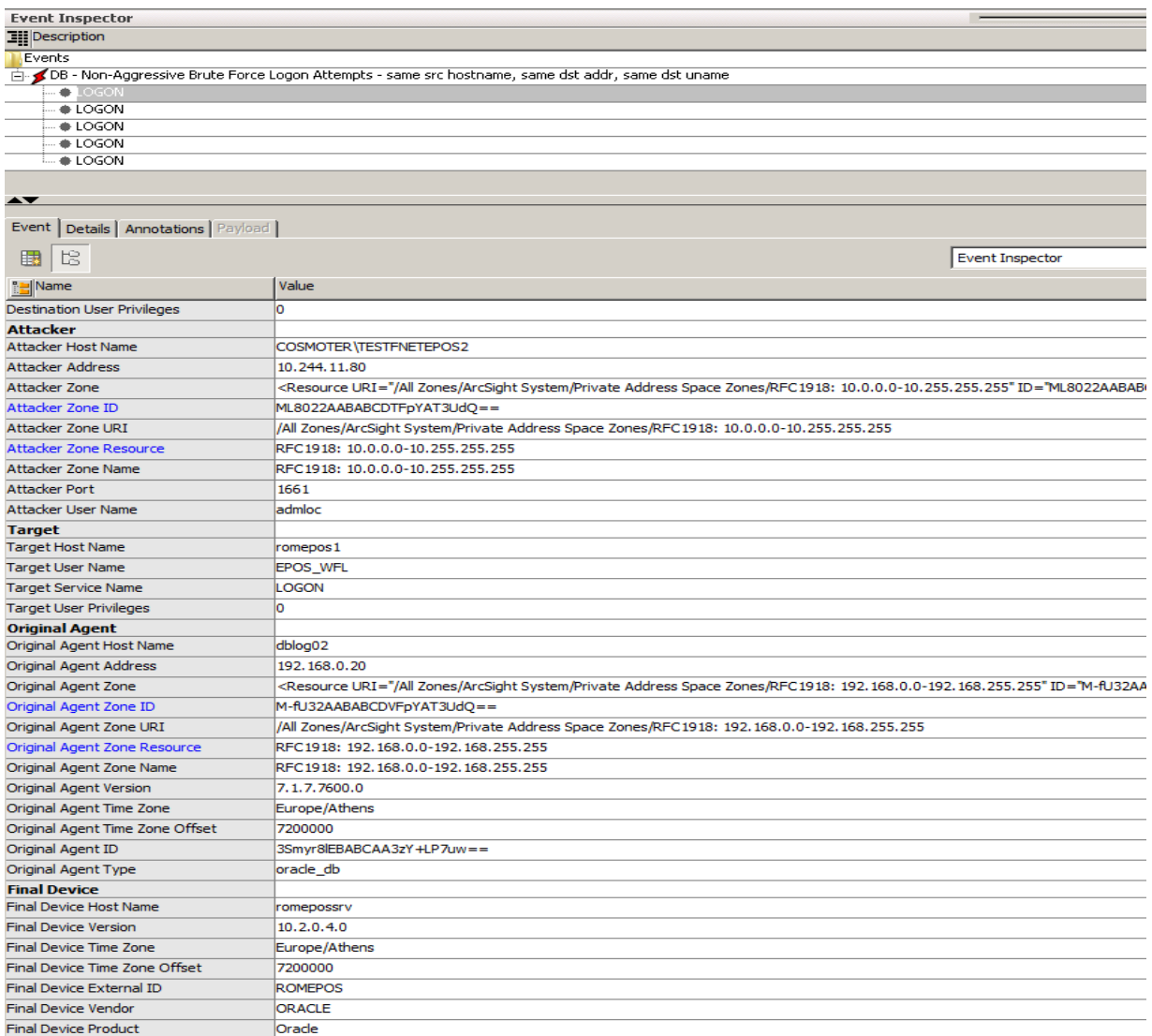
It is possible to add more fields if desired, in order to have a more detailed view about the incident. A view with more fields is the following:



**Figure 31: DB Brute force Login Attempts – Correlated Event**

The image from above presents a correlated event. As it said above in our scenario a Brute force correlated event consists of **5 failed login attempts in 2 minutes**. As shown in the image, there are 5 failed login events that create **1 Brute force login attempt event**.

The image below shows an analytic view of 1 failed login attempt with many filed displayed:

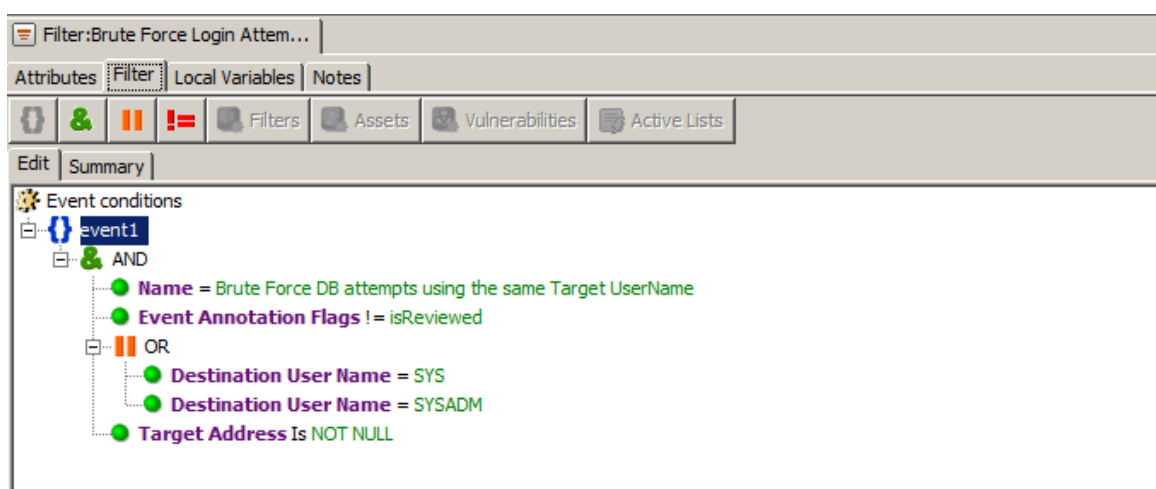


**Figure 32: DB Brute force Login Attempts – Inspect view**

This figure presents a more detailed view of a failed login attempt. Some of them are:

- **Attacker Address:** 10.244.11.80 → indicates the ip address of the system that attempted the login.
- **Attacker port:** 1661 → indicates the port used for the login.
- **Attacker User Name:** admloc → indicates the name of the “attacker”
- **Original Agent Host Name:** dblog02 → indicates that the current agent is used for DB logs.
- **Final Device Product:** Oracle → indicates the type of database.

The filter used for creating the current active channel is the following:



**Figure 33: DB Brute force Login Attempts – Filter**

- **Name:** DB Brute Force login attempts → indicates the name of the rule used (rule used in order to create the correlated event).
- **Event Annotation Flags!= isReviewed** → shows only incidents that have not been marked as reviewed by the security analyst.
- **Destination User Name:** SYS → defines the username be equal to SYS, that's because username SYS & SYSADM are used by the administrators.
- **Target Address** is NOT NULL → don't appears the event with null destination address.

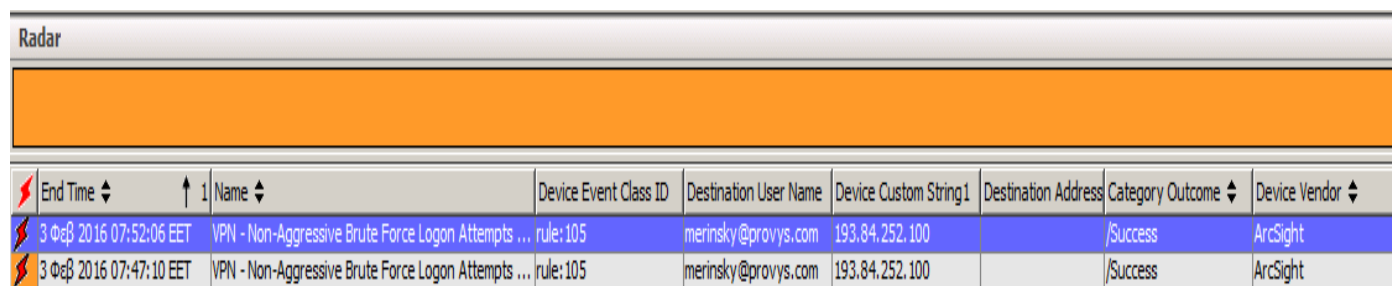
Implementing this scenario, a company could monitor their databases and protect them from malicious **brute force attempts**. Moreover, depending on the criticality of each database further measures can be added. For example, company's Information Security wants only designated users to have access to the “critical” Databases. This could be easily implemented by the usage of an **Active List** that will store all the privileged users and allow them access the Database.

## 4.5 VPN Brute Force Login Attempts

Another big issue for big companies is the VPN connection. A **virtual private network (VPN)** extends a private network across a public network, such as the Internet. It enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network, and thus are benefiting from the functionality, security and management policies of the private network. It is therefore easily understood that a big company has to thoroughly check and monitor the VPN logs.

In this sector, Active Channel that monitors the VPN Brute force login attempts and VPN attempts for external authorized logins will be presented. In this scenario a brute force login attempt considered the event occurring 5 “same” failed login attempts over a period of 2 minutes.

The following images display the configuration of an active channel for monitoring Brute force login attempts for VPN connections:



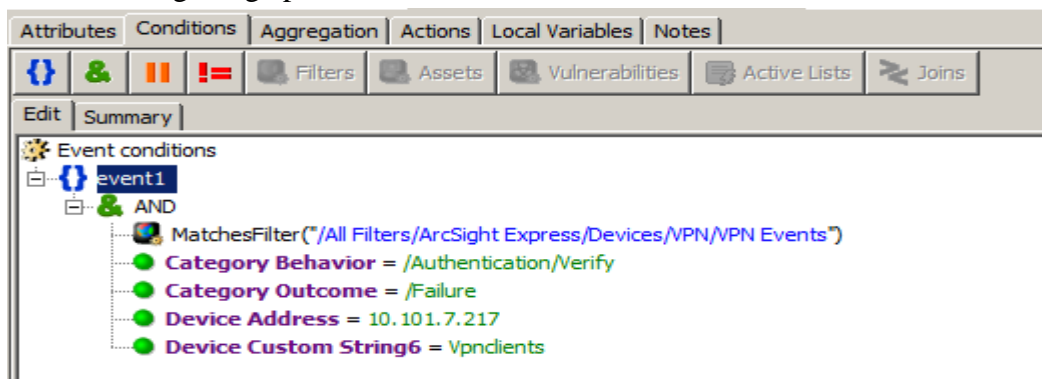
End Time	Name	Device Event Class ID	Destination User Name	Device Custom String1	Destination Address	Category Outcome	Device Vendor
3 0eβ 2016 07:52:06 EET	VPN - Non-Aggressive Brute Force Logon Attempts ...	rule:105	merinsky@provys.com	193.84.252.100		/Success	ArcSight
3 0eβ 2016 07:47:10 EET	VPN - Non-Aggressive Brute Force Logon Attempts ...	rule:105	merinsky@provys.com	193.84.252.100		/Success	ArcSight

**Figure 34: VPN Brute Force Login Attempts – Active Channel**

- **Destination User Name:** [merinsky@provys.com](mailto:merinsky@provys.com) → indicates the username of the user who attempted the VPN login attempt.
- **Device Custom String1:** 193.84.252.XXX → indicates the source ip address of the user who attempted the VPN login attempt.
- **Category Outcome:** success → indicates the result of the VPN connection (Success / Failed)



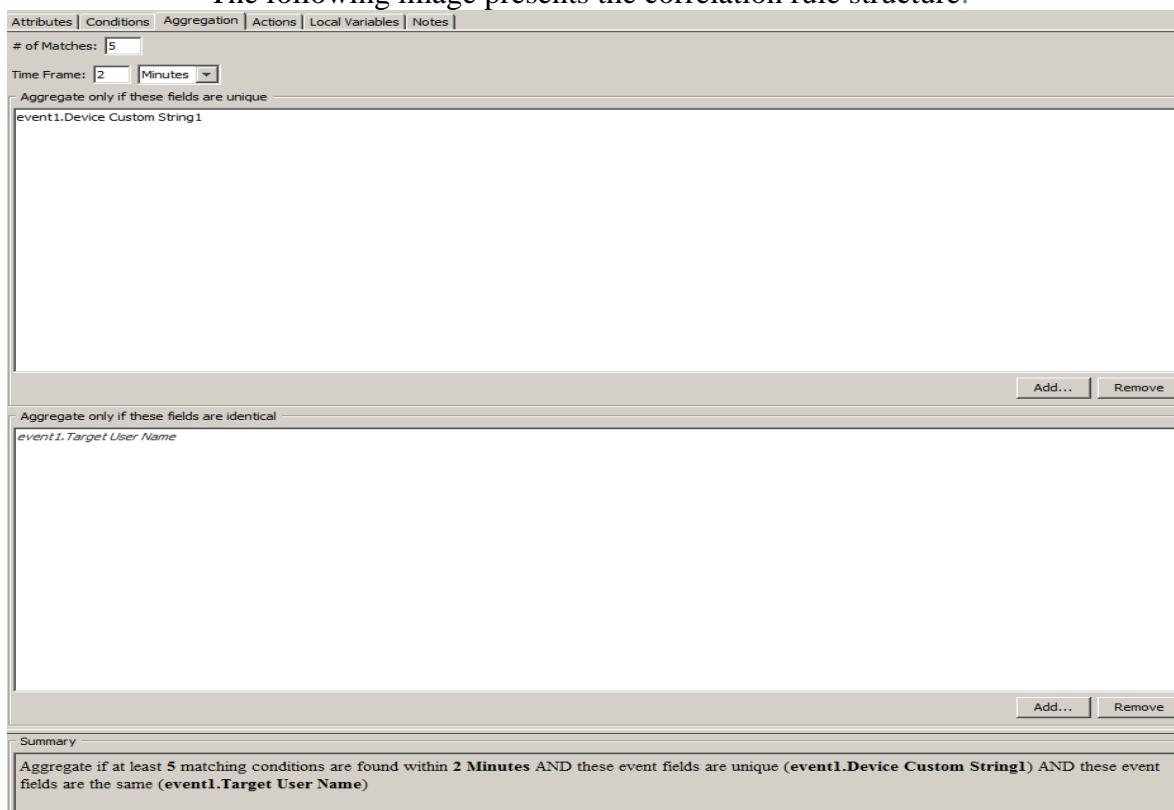
The following image presents the structure of the filter for the Active Channel:



**Figure 35: VPN Brute Force Login Attempts – Filter**

- **MatchesFilter(XXXXXXX)** → indicates one filter that is going to be used. In this example it is used a default filter of the Arcsight Express for the VPN Events.
- **Category Behavior:** Authentication/verify → indicates that this is a case of authentication.
- **Category Outcome:** Failure → indicates that the result of the authentication will be failed
- **Device Address:** 10.101.7.217 → that's the address used for VPN Events.

The following image presents the correlation rule structure:



### Figure 36: VPN Brute Force Login Attempts – Rule

In this Figure appears the configuration of the correlation rule in order to “match” 5 consecutives events in 2 minutes, as a correlated event.

- **# of Matches:** 5 ➔ indicates the number of matching events.
- **Time Frame:** 2 minutes ➔ indicates the minutes that the rule will wait in order to create the correlated event.
- **Aggregate only if these fields are unique:** Event1.Device Custom String1 ➔ indicates the fields that are going to be unique in the correlated event.
- **Aggregate only if these fields are identical:** event.1Target User Name ➔ indicates the fields that are going to be identical in the correlated event.

By implementing this filter, the security analysts have a detailed view about the VPN Brute Force Logins attempted from the external network to the company’s network. Furthermore it is a very important monitoring because if an attacker gains access to a company system using a VPN connection, it can easily leak critical information outside of the company.

## 4.6 VPN External authorized logins

Except for VPN brute force login attempts, there are VPN external logins by authorized users that can be monitored. This could become very important information about security sector of the company. It’s a kind of firewall, because it monitors specified users that exist in a specific active list.

The following image displays an active list filled with the usernames of legitimate users:

<b>Name:</b> VPN External Users Always On <b>Start Time :</b> 7 Nov 2015 11:49:56 EET <b>End Time :</b> 5 Feb 2016 11:49:56 EET <b>Last Update:</b> 5 Feb 2016 11:49:56 EET <b>Filter:</b> No Filter	
Destination User Name ↓	Creation Time
a.dimitro,	30 Iouv 2015 12:51:12 E...
a.hunashikatti	30 Iouv 2015 12:51:12 E...
a.ntoucharis@ ....	30 Iouv 2015 12:51:12 E...
a.srinivas.achar@ ..	30 Iouv 2015 12:51:12 E...
abir.bhattacharya@ ..	30 Iouv 2015 12:51:12 E...
afentakis.l	30 Iouv 2015 12:51:12 E...
AGEORGE!	30 Iouv 2015 12:51:12 E...
ajay.kuma@	30 Iouv 2015 12:51:12 E...
Akanksha.anilkumar _	30 Iouv 2015 12:51:12 E...
akhilesh.shrivastava@	30 Iouv 2015 12:51:12 E...

**Figure 37:** VPN External Connections – Active List

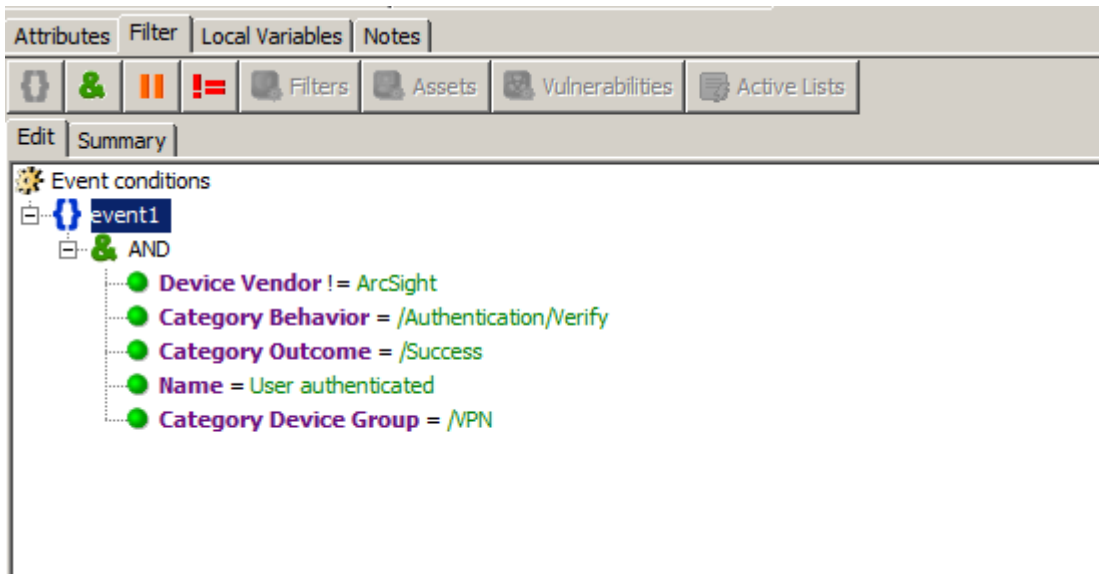
The Active Channel filter checks if the VPN login is made by a user in active list and if the user is in the active list (legitimate) user it produces one event. The following image displays the VPN external successful login active channel:

Radar					
Name ↕	End Time ↕	1	Destination Address	Destination Geo Country	Destination User Name
VPN - External Authorized Users Successfull Logon	5 Feb 2016 11:38:20 EET		144.36.214.		pallavi.s.deshpande_
VPN - External Authorized Users Successfull Logon	5 Feb 2016 11:03:06 EET		194.30.241.		hladas@x
VPN - External Authorized Users Successfull Logon	5 Feb 2016 10:55:56 EET		85.72.53.		gkar@x
VPN - External Authorized Users Successfull Logon	5 Feb 2016 10:29:31 EET		144.36.214.		bhushan.s.pawar@
VPN - External Authorized Users Successfull Logon	5 Feb 2016 09:58:58 EET		144.36.214		m.sudarshan.gundeli@x
VPN - External Authorized Users Successfull Logon	5 Feb 2016 09:58:53 EET		144.36.214		pallavi.s.deshpande@x
VPN - External Authorized Users Successfull Logon	5 Feb 2016 09:47:35 EET		193.84.252		merinsky@x

**Figure 38:** VPN External Connections – Active Channel

- **Name:** VPN – External Authorized Users Successful Logon → indicates the name of the rule used
- **Destination Address:** 144.36.214.XXX → indicates the ip address of the user who attempted the VPN connection
- **Destination Geo Country:** → indicates the flag of the country that launched the VPN connection.
- **Destination User Name:** [hladas@xxxx.com](#) → indicates the username used for the VPN connection.

In order to monitor only the successful login attempts, the following filter is necessary:

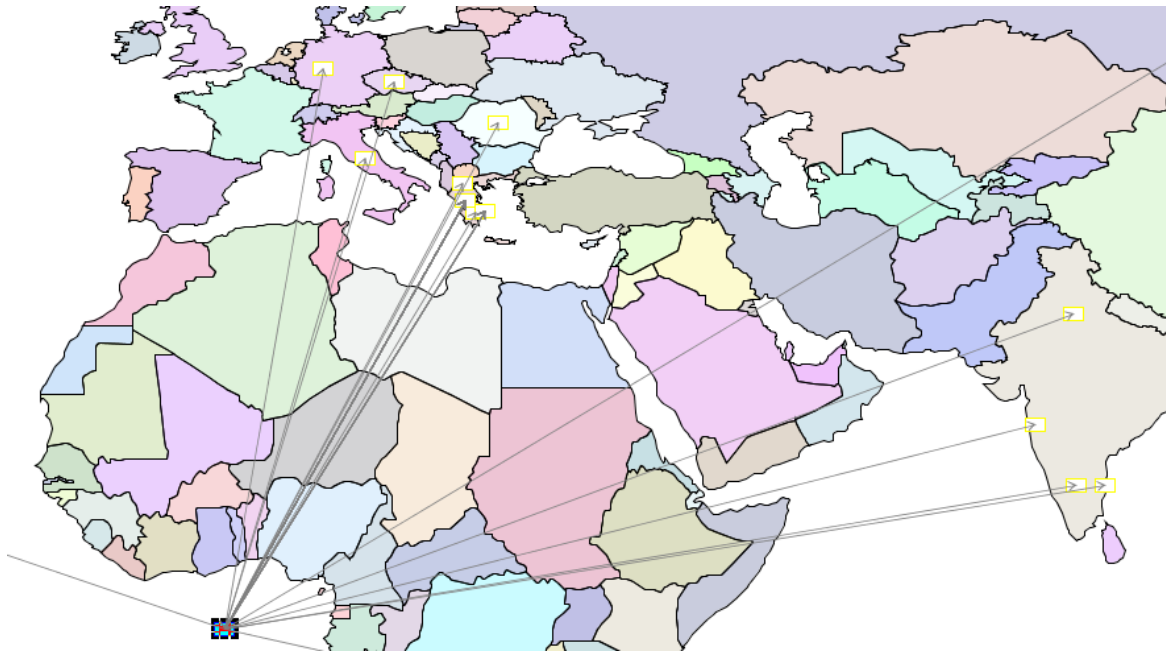


**Figure 39:** VPN External Connections – Filter

- **Device Vendor != Arcsight** → indicates that the events with name “Arcsight” will not appeared(they are internal events).
- **Category Behavior : /Authentication/Verify** → indicates the kind of authentication.
- **Category Outcome: /Success** → indicates the result of the connection.
- **Category Device Group : /VPN** → indicates the kind of the connection.

Except the active channel, security analyst could have a better view of the VPN connections performed. This could be performed by the use of a Dashboard which will presents the whole planet in a graphical display and the VPN connections performed by each country.

The following image presents this option:



**Figure 40:** VPN External Connections – Dashboard

As it said above, the dashboard shows the connections that have been successfully performed. For example, there are connections from Italy, Greece, East Asia, etc. The target of the VPN connections is not appeared. The Arcsight can be configured properly in order to display as the target the company's Country.

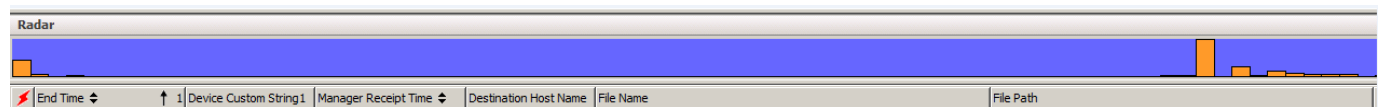
Finishing this sector, it is obvious that VPN connection of a company should be monitored because it's a major passageway of which can seep corporate data. Security Analysts should monitor in detail VPN connection attempts, and and perform the appropriate action if a VPN incident occurs.

#### 4.7 Antivirus log – Malware monitoring

Another big issue concerning the companies is the virus infection. A virus can be very destructive for a company, if for example infect a large number of computers and encrypt all the containing files. This scenario could make the company lose a great amount of money, that's why all the big companies have installed Antivirus programs. All of these programs are sending logs also, and the security analysts check them in order to confirm that no computer is infected.

In this scenario the Active channels, filters, dashboards of antivirus & malware monitoring will be presented.

The following image presents an active channel containing the infected workstations that have not been cleaned, and there is a need for further investigation.



End Time	Device Custom String1	Manager Receipt Time	Destination Host Name	File Name	File Path
1 Feb 2016 16:11:29 EET	Trojan.Gen	1 Feb 2016 16:14:08 EET	WKS01963	c:\users\skaramanos\appdata\local\temp\{abf9eb94-9e9e-4841-...	/All Rules/Real-time Rules/Custom/Old/AV - C...
1 Feb 2016 14:10:04 EET	Eicar_test_1	1 Feb 2016 14:10:09 EET	LAB-PC	a.txt	C:\Users\Administrator\Desktop\
1 Feb 2016 14:10:04 EET	Possible_SCRDL	1 Feb 2016 14:10:09 EET	LAB-PC	C233E60386B9543D80CBFDE5E0163689A1617E74	C:\Users\Administrator\AppData\Local\Mozila...
1 Feb 2016 14:10:04 EET	TROJ_GEN.R02C0ECR15	1 Feb 2016 14:10:09 EET	LAB-PC	6f12DXlp.rar.part	C:\Users\ADMINI~1\AppData\Local\Temp\
1 Feb 2016 14:10:04 EET	TROJ_GEN.R002C00J315	1 Feb 2016 14:10:09 EET	LAB-PC	RedKite.dll	C:\Users\Administrator\AppData\Local\MSBirds\
1 Feb 2016 14:10:04 EET	TROJ_GEN.R047C0RAK15	1 Feb 2016 14:10:09 EET	LAB-PC	Hard Disk Sentinel PRO 4.60 patch [www.procracks.com].rar.part	C:\Users\Administrator\Desktop\
1 Feb 2016 14:10:04 EET	Eicar_test_1	1 Feb 2016 14:12:25 EET	LAB-PC	a.txt	C:\Users\Administrator\Desktop\
1 Feb 2016 14:10:04 EET	Possible_SCRDL	1 Feb 2016 14:12:25 EET	LAB-PC	C233E60386B9543D80CBFDE5E0163689A1617E74	C:\Users\Administrator\AppData\Local\Mozila...
1 Feb 2016 14:10:04 EET	TROJ_GEN.R02C0ECR15	1 Feb 2016 14:12:25 EET	LAB-PC	6f12DXlp.rar.part	C:\Users\ADMINI~1\AppData\Local\Temp\
1 Feb 2016 14:10:04 EET	TROJ_GEN.R002C00J315	1 Feb 2016 14:12:25 EET	LAB-PC	RedKite.dll	C:\Users\Administrator\AppData\Local\MSBirds\
1 Feb 2016 14:10:04 EET	TROJ_GEN.R047C0RAK15	1 Feb 2016 14:12:25 EET	LAB-PC	Hard Disk Sentinel PRO 4.60 patch [www.procracks.com].rar.part	C:\Users\Administrator\Desktop\
1 Feb 2016 14:09:23 EET	TROJ_GEN.R02KCOOA215	1 Feb 2016 14:09:32 EET	LAP-9JH1KX1	SmdmFHpFF32.dll	C:\Users\Administrator\AppData\Roaming\Fir...
1 Feb 2016 14:09:23 EET	TROJ_GEN.R00UC00A416	1 Feb 2016 14:09:32 EET	LAP-9JH1KX1	animatedxmaswalls_12828_j1776447170_#14332.exe	C:\Users\Administrator\downloads\
1 Feb 2016 14:09:23 EET	TROJ_GEN.R02KCOOA215	1 Feb 2016 14:10:26 EET	LAP-9JH1KX1	SmdmFHpFF32.dll	C:\Users\Administrator\AppData\Roaming\Fir...
1 Feb 2016 14:09:23 EET	TROJ_GEN.R00UC00A416	1 Feb 2016 14:10:26 EET	LAP-9JH1KX1	animatedxmaswalls_12828_j1776447170_#14332.exe	C:\Users\Administrator\downloads\
1 Feb 2016 14:09:05 EET	TROJ_GEN.R0C1COPF815	1 Feb 2016 14:09:21 EET	LAB-PC	GarreDeskman.xyz.exe	C:\Users\Administrator\AppData\Local\Temp\...
1 Feb 2016 14:09:05 EET	TROJ_GEN.R0C1COPF815	1 Feb 2016 14:09:30 EET	LAB-PC	AV - Multiple Viruses - Same PC	/All Rules/Real-time Rules/Custom/Old/AV - M...
1 Feb 2016 14:09:05 EET	TROJ_GEN.R0C1COPF815	1 Feb 2016 14:10:26 EET	LAB-PC	GarreDeskman.xyz.exe	C:\Users\Administrator\AppData\Local\Temp\...
1 Feb 2016 14:07:48 EET	TROJ_GEN.R0C1C00A215	1 Feb 2016 14:08:02 EET	LAP-9JH1KX1	SmdmFHpFF29.dll	C:\Users\Administrator\AppData\Roaming\Fir...
1 Feb 2016 14:07:48 EET	TROJ_GEN.R0C1C0EAE15	1 Feb 2016 14:08:02 EET	LAP-9JH1KX1	SmdmFHpFF12.dll	C:\Users\Administrator\AppData\Roaming\Fir...
1 Feb 2016 14:07:48 EET	TROJ_GEN.R0C1C00A215	1 Feb 2016 14:08:02 EET	LAP-9JH1KX1	SmdmFHpFF30.dll	C:\Users\Administrator\AppData\Roaming\Fir...
1 Feb 2016 14:07:48 EET	TROJ_GEN.R0C1C00A215	1 Feb 2016 14:08:02 EET	LAP-9JH1KX1	SmdmFHpFF13.dll	C:\Users\Administrator\AppData\Roaming\Fir...
1 Feb 2016 14:07:48 EET	TROJ_GEN.R0C1C00A215	1 Feb 2016 14:08:02 EET	LAP-9JH1KX1	SmdmFHpFF21.dll	C:\Users\Administrator\AppData\Roaming\Fir...
1 Feb 2016 14:07:48 EET	TROJ_GEN.R02KCOOA215	1 Feb 2016 14:08:02 EET	LAP-9JH1KX1	SmdmFHpFF26.dll	C:\Users\Administrator\AppData\Roaming\Fir...
1 Feb 2016 14:07:48 EET	TROJ_GEN.R0C1C00A215	1 Feb 2016 14:08:02 EET	LAP-9JH1KX1	SmdmFHpFF14.dll	C:\Users\Administrator\AppData\Roaming\Fir...
1 Feb 2016 14:07:48 EET	TROJ_GEN.R0C1C00A215	1 Feb 2016 14:08:02 EET	LAP-9JH1KX1	SmdmFHpFF28.dll	C:\Users\Administrator\AppData\Roaming\Fir...
1 Feb 2016 14:07:48 EET	TROJ_GEN.R02KCOOA215	1 Feb 2016 14:08:02 EET	LAP-9JH1KX1	SmdmFHpFF4.dll	C:\Users\Administrator\AppData\Roaming\Fir...
1 Feb 2016 14:07:48 EET	TROJ_GEN.R021C00A215	1 Feb 2016 14:08:02 EET	LAP-9JH1KX1	SmdmFHpFF18.dll	C:\Users\Administrator\AppData\Roaming\Fir...

**Figure 41:** Antivirus logs – Active Channel

- **End Time:** 1 Feb 2016 16:11:00 ➔ indicates the date & time of the infection.
- **Device Custom String1 :** Trojan Gen ➔ indicates the type of the virus.
- **Device Host Name :** LAB-PC ➔ indicates the name of the workstation infected.
- **File Name:** a.txt ➔ indicates the “suspicious”file.
- **File Path:** C:\Users\Administator\Desktop ➔ indicates the path destination of the “suspicious”file.

Moreover, each virus log could be opened to analyzed most and retrieve more information about the incident.

The following 2 images present the event inspection of a virus log:

<b>Device Custom</b>	
Device Custom IPv6 Address4.Agent ...	fe80::c634:6bff:feb8:3b4a
Device Custom Date1.CLF_LogGenera...	23 Ιουλ 2015 13:14:15 EEST
Device Custom Number1.VLF_Pattern...	1230900
Device Custom Number2.VLF_Second...	4
Device Custom String1.Virus Name	Eicar_test_1
Device Custom String2.VLF_EngineVer...	9.850.1008
Device Custom String3.CLF_ProductV...	11.0
Device Custom String4.CLF_ReasonC...	virus log
Device Custom String5.VLF_FirstActio...	Clean unsuccessful
Device Custom String6.VLF_SecondAc...	Upload unsuccessful

Event Inspector	
Event	Details Annotations Payload
Name	Value
<b>Event</b>	
Event ID	89673634366
External ID	103391
Name	Eicar_test_1
Type	Base
Start Time	1 Φεβ 2016 14:10:04 EET
End Time	1 Φεβ 2016 14:10:04 EET
Manager Receipt Time	1 Φεβ 2016 14:12:20 EET
Concentrator Agents	[AgentDescriptor=[id=[3X1K1EMBABCAA4vDzh13zA==]name=[null]type=[trendmicrong_db]SensorRelatedDescriptor=[descriptorID=[
Originator	Source
Aggregated Event Count	1
Correlated Event Count	0
Locality	Local
<b>Category</b>	
Category Significance	/Informational/Warning
Category Behavior	/Modify/Content
Category Device Group	/IDS/Host/Antivirus
Category Device Type	Anti-Virus
Category Outcome	/Success
Category Object	/Host/Resource/File

**Figure 42:** Antivirus logs – Event inspection

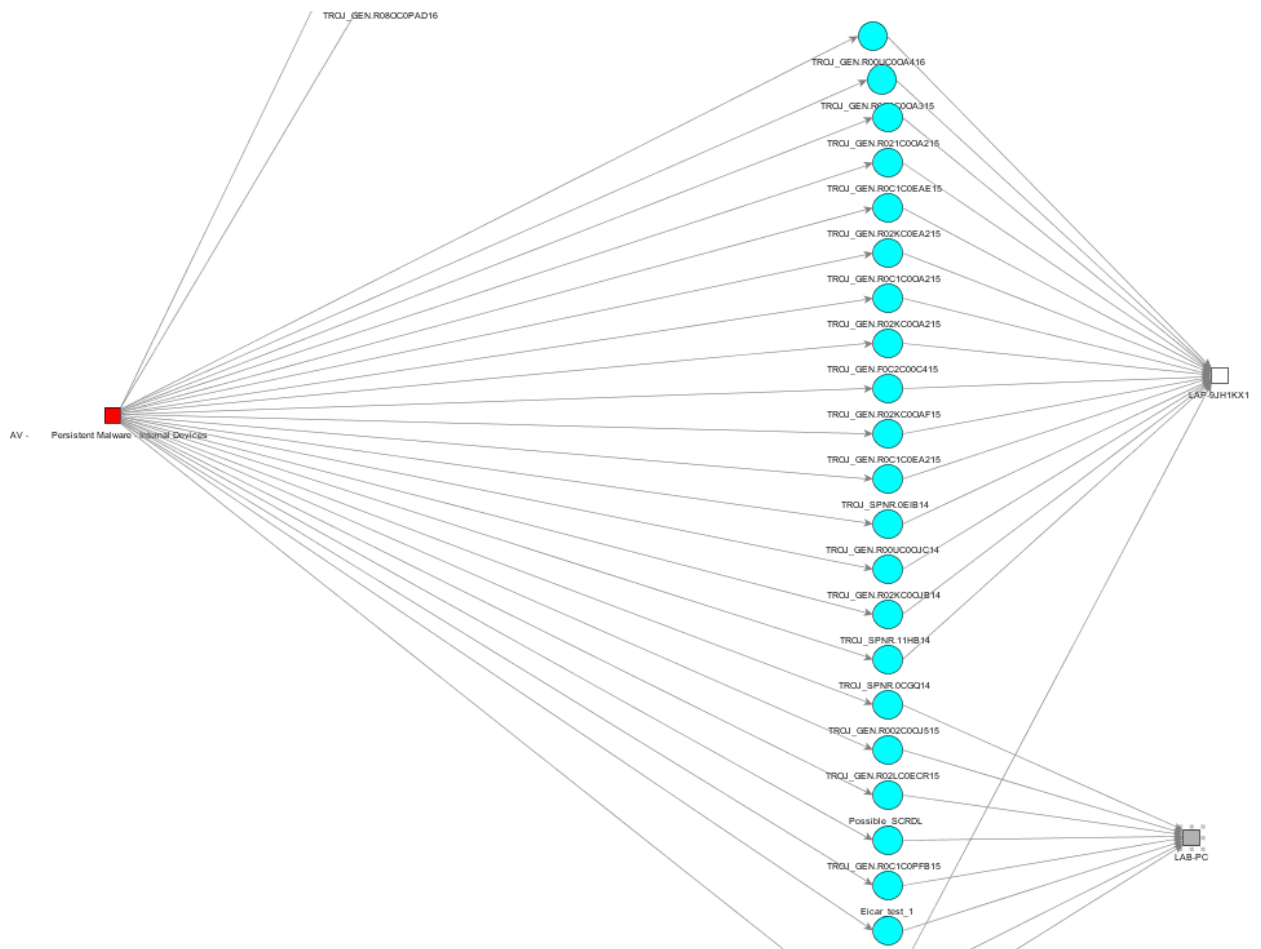
Some more fields are:

- **Device Custom String5:** Clean unsuccessful → indicates the result of the virus detection from the Antivirus. In this case the antivirus could not clean the virus.
- **Device Custom String6:** Upload unsuccessful → indicates the result of the virus update in the antivirus database. In this example the antivirus could not update the database with the virus signature.
- **Category Significance:** /Informational/Warning → indicates the Significance of the virus. In this case is just a warning.
- **Category Behavior:** /Modify/Content → indicates the “possible” action of the virus.

Another critical incident that can occur is the **multiple workstations virus infection**. This incident is very serious because it can make useless all the workstations of a company sector for example.

A dashboard could be applied for this situation in order to appear graphically if a workstation has been infected with multiple viruses or multiple workstations have been infected by a virus.

The following image presents a workstation that has been infected by multiple viruses:



**Figure 43:** Antivirus logs – Dashboard

As shown in the dashboard, different kind of virus has infected the workstation “**LAB-9JH1KX1**”. Some of these viruses’ names are **TROJ\_GEN\_RO2KCOBUC14**, **TROJ\_GEN\_RO2KCOBUC14**, **TROJ\_GEN\_SPNR.11BH14**, etc.

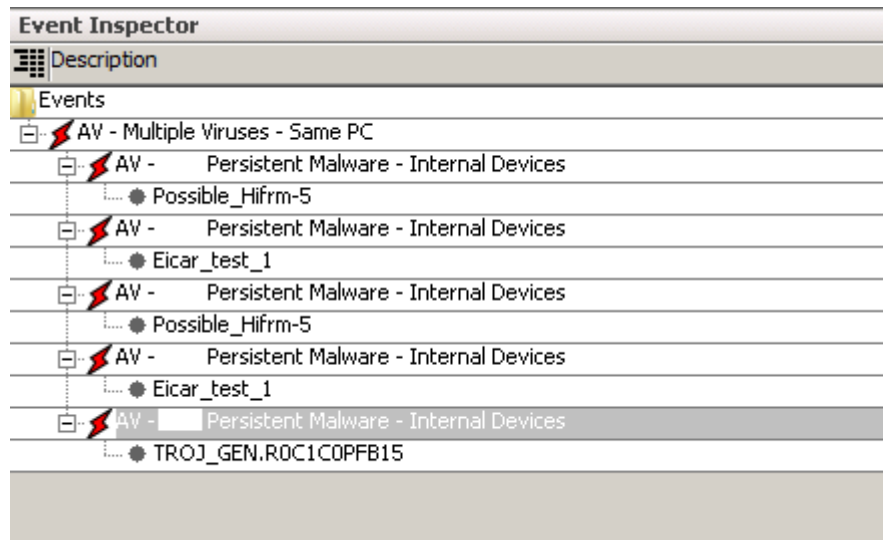
In the Active channel the above event will look like:



1 Φαβ 2016 14:09:05 EET		1 Φαβ 2016 14:09:30 EET	LAB-PC	AV - Multiple Viruses - Same PC
-------------------------	--	-------------------------	--------	---------------------------------

**Fig 42.** Antivirus logs – Active channel, multiple virus

and



**Figure 44:** Antivirus logs – Active channel, multiple virus event inspector

Another critical action that the security analysts have to perform after a critical virus infection is the «marking» of the virus.

For example if a **ransomware** Crypto Locker virus occurs (which is very important virus – can encrypt all the files of a system), the analysts can create a channel only for the **ransom** virus and monitor it so that when it appears again to make immediate actions to clean it.

The following image presents a filter that monitors one particular **ransomware virus**.



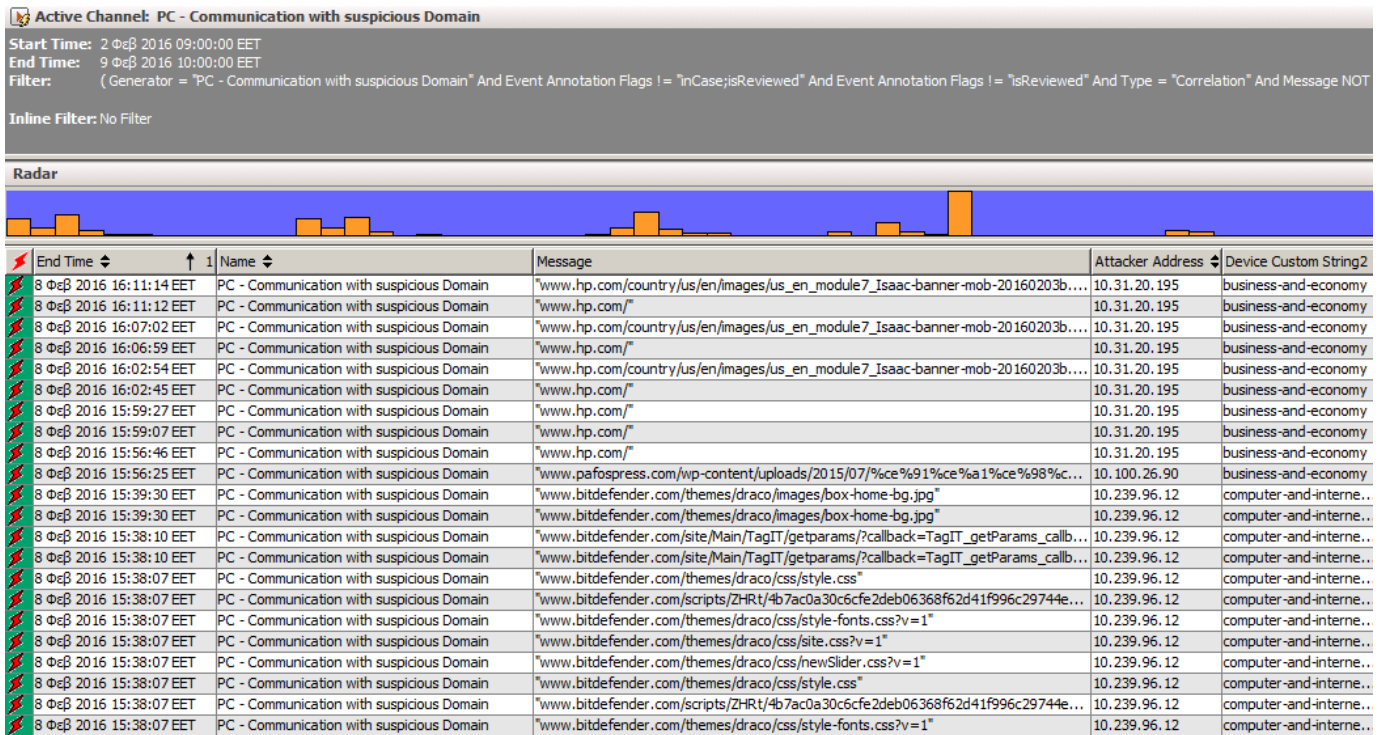
- **Malware Count per Workstation:** presents the count of the virus infections in each workstation
- **Virus Activity (Ransomware):** presents the dashboard for the specific monitoring of high importance virus.
- **Persistent Malware:** presents the workstations with the virus which has infected each one.

The conclusion of this scenario is that there are many ways to secure company's workstation, but the combination of all the measures with the antivirus logs monitoring could lead to a unique result and give the opportunity to the security analysts to be updated for every virus incident occurs in the company and its facilities.

#### 4.8 Suspicious Communication with malicious IP's – Domains

In the final scenario, the Firewall / Proxy logs will be analyzed in order to “capture” communications with suspicious **domains** or **ip**. This technique can help the security analysts to gather information about a workstations behavior. For example, if a workstation is infected with a malware, it will probably start trying to communicate with known C&C servers. If this server contained in the active list of suspicious domains / ip then an alert log will be produced.

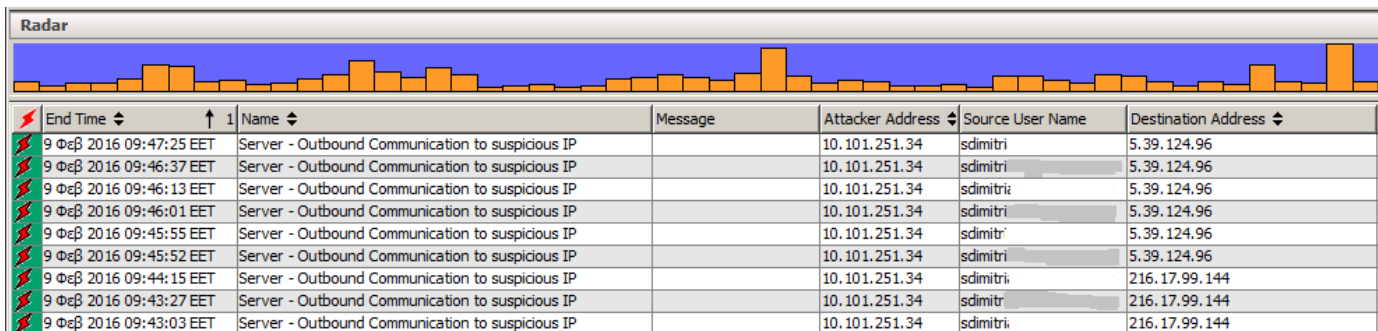
The following image presents the active channel “communication with suspicious domain”:



- **Message:** [www.bitdefender.com/themes/draco/images/box-home-bg.jpg](http://www.bitdefender.com/themes/draco/images/box-home-bg.jpg) → indicates the suspicious domain name.
- **Attacker Address:** 10.31.20.195 → indicates the ip address of the workstation performed the connection with the “suspicious” destination.
- **Device Custom String2:** business-and-economy → indicates the informational type of the “malicious” link.

Some of the “malicious” domains aren’t really malicious, but one link of the domain may be blacklisted and the domain enters the blacklist.

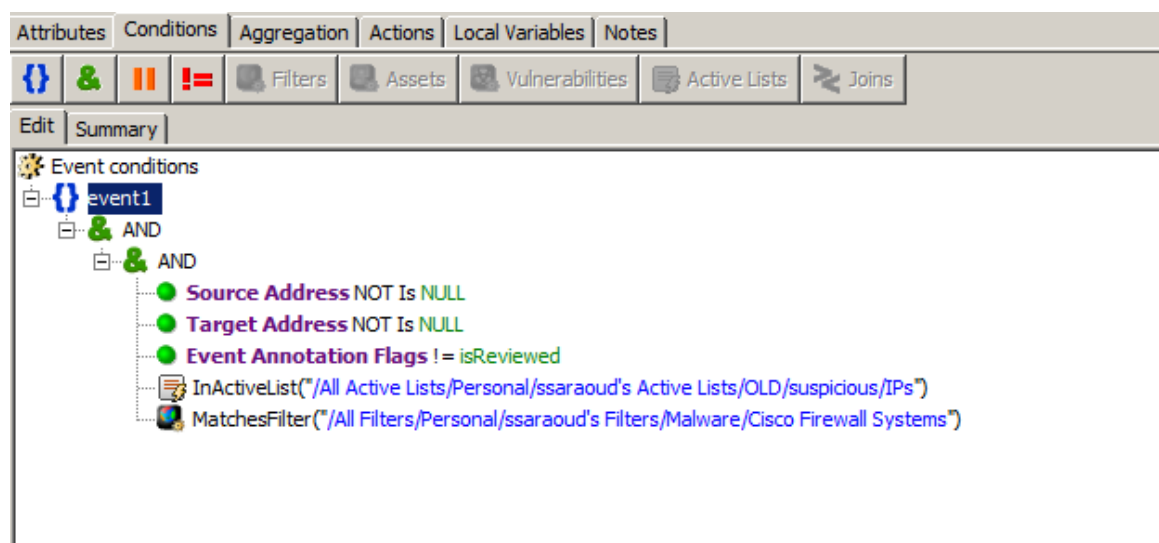
The following image presents the active channel “communication with suspicious IP”:



- **Attacker Address:** 10.31.20.195 → indicates the ip address of the workstation performed the connection with the “suspicious” destination.

- **Source User Name:** sdmitri → indicates the username of the user who made the connection.
- **Destination Address:** 5.39.124.96 → indicates the suspicious IP.

The filter used to make the above active channels is the following:



**Figure 49:** Filter – Communication with suspicious IP

As it seems the **Attacker** and **Target** address shouldn't be null, and the basic filter use another pre-installed Arcsight's filter for "Cisco Firewall Systems" in order to monitors the Firewall traffic. Moreover, an active list is used in order to indicate all the malicious IP/Domains that the filter compares.

The active list is update daily with the latest malicious IP/Domains from the internet.

The following image presents an Active list that contains suspicious IP:

<b>Name:</b> IPs <b>Start Time :</b> 11 Νοε 2015 09:59:10 EET <b>End Time :</b> 9 Φεβ 2016 09:59:10 EET <b>Last Update:</b> 9 Φεβ 2016 09:59:09 EET <b>Filter:</b> No Filter	
IPs	Creation Time
0.0.0.1	23 Ιουλ 2015 12:56:23 E...
0.0.0.2	23 Ιουλ 2015 12:56:23 E...
1.234.27.146	22 Ιαν 2016 16:53:42 EET
1.234.79.115	23 Ιουλ 2015 12:56:23 E...
2.6.177.172	25 Ιαν 2016 09:34:09 EET
2.9.230.142	25 Ιαν 2016 09:34:09 EET
2.25.33.250	22 Ιαν 2016 16:53:41 EET
2.28.172.202	25 Ιαν 2016 09:34:10 EET
2.83.221.52	22 Ιαν 2016 16:53:41 EET
2.86.73.253	22 Ιαν 2016 16:53:41 EET
2.87.175.233	22 Ιαν 2016 16:53:41 EET
2.92.173.175	22 Ιαν 2016 16:53:41 EET
2.93.99.41	22 Ιαν 2016 16:53:41 EET
2.93.244.58	22 Ιαν 2016 16:53:41 EET
2.103.218.9	22 Ιαν 2016 16:53:41 EET
2.110.60.68	22 Ιαν 2016 16:53:41 EET
2.110.146.134	22 Ιαν 2016 16:53:41 EET
2.110.219.47	22 Ιαν 2016 16:53:41 EET
2.111.70.28	22 Ιαν 2016 16:53:41 EET
2.123.185.238	22 Ιαν 2016 16:53:42 EET
2.133.128.98	23 Ιουλ 2015 12:56:23 E...
2.143.9.100	22 Ιαν 2016 16:53:42 EET
2.221.8.243	22 Ιαν 2016 16:53:41 EET
2.225.141.134	22 Ιαν 2016 16:53:41 EET

**Figure 50:** Active List with malicious IP

If a corporate system communicate or connect with one from the IP above then a security event will be produced. This is the most efficient way to monitor all the corporate systems massively and be informed if a suspicious communication occurs.

## 4.9 General Observation – incident example

After all these scenarios/examples, it is understood that Arcsight has unlimited capabilities and can help significantly in monitoring and also in investigating security incidents. A possible security event that could be investigated with all the above information is the following:

**Security Incident Example:** A virus has compromised a user's workstation.

- 1) First of all, the security analysts check the antivirus logs in order to identify what is the state of the virus (cleaned, deleted, and quarantined).

- 2) Moreover, they check the domain controller logs in order to match the infected workstation with its user. By domain controller logs can be seen the username that logged in the workstation, and find out who is its user.
- 3) After that, the web-proxy logs are checked in order to observe what kind of domains the user visited and stuck the virus.
- 4) Finally, if the workstation is infected the analysts check the firewall logs to identify if the infected workstation tries to communicate with malicious domains or IP (a C&C server probably).

There are many more similar examples that could be investigated with the same way. When all the company's logs are centralized storing and easily searchable then the investigation of a security event would have more successful results.

## **5. Conclusion and future work**

### **5.1 Conclusion**

The thesis has sought to reflect the importance of centralize, collect and correlate events of a big Telecommunications company. The Security Information and Event Management systems enhance the value of an existing security infrastructure by consolidating and archiving log and event data from across the organization. An efficient solution as a central event management tool helps to contain the growing-cost of the audits controls, reducing the investment on security and compliance technologies, improve the efficiency of the forensic investigations and minimize the incident response time.

The company needs to manage the large amount of events generated by the security-points technologies (Antivirus, Proxy, Firewall, etc), network devices, OS, Databases, physical access, etc. The manual monitoring of these events turn the environment intractable and difficult to prioritize. The SIEM tool (Arcsight) receives all the logs generated at the company, generates the programmed report and is used to reduce the audit cost and the IT team efforts and time helping them to track incidents through their lifecycle and effectively respond to them. It is in the choice and discretion of the company what kind of the Arcsight filters, rules, Dashboards, Active Channels, etc. will use in order to better organize and secure its systems.

## 5.2 Future work

There are some basic issues that will need to be researched and addressed prior to including a SIEM tool as a basic component of a command's insider threat program. The architecture described in Chapter 4 uses basic filters, active lists and rules as its components. These filters can be further defined to capture even more relevant data based on a variety of log sources, producing even more active lists and potentially more rules.

Purchase costs, administration, and training for the use and implementation of this tool also need to be considered. A cost-benefit analysis can assist in determining the feasibility of using this type of tool, quantifying the costs of the SIEM, maintenance, training, and administration against its ability to effectively combat insider threats. Additionally, the legalities of including an individual's PSI and administrative actions on a network access request form need to be addressed out of concern for privacy and possible Constitutional issues.

Furthermore, something little more technical and complicated would be the profiling of the users. Recording and archiving of users actions in the company's systems in order to make a profile about him for a several time period. If the "behavior" of some user suddenly changes, then there is likely an incident. There are different tools that make this job but only "archives" a users failed logon attempts for example. The Arcsight provides the power of make a profiling using all the most useful logs of the company, that's the big difference with other tools. It's a project which requires a lot of work but worth it.



## References

- [1] Dr. A. Chuvakin. Leveraging compliance for security with SIEM and log management. Available at <http://goo.gl/m3ILQ> , june 2011.
- [2] A. Chuvakin. The complete guide to log and event management. Available from <http://goo.gl/0lr7f> , 2010.
- [3] A. Chuvakin. Practical strategies to compliance and security with SIEM. Presented at the “Vendor T” webinar, available at <http://goo.gl/kifj2> , october 2012.
- [4] LBNL’s Network Research Group. arpswatch – Homepage of LBNL’s Network Research Group. Available at <http://ee.lbl.gov>, 2012.
- [5] Insider threat control: using a SIEM signature to detect potential precursors to IT sabotage. Pittsburgh, PA: Carnegie Mellon Software Engineering Institute. Retrieved from [http://www.cert.org/insider\\_threat/](http://www.cert.org/insider_threat/) , (2011, April).
- [6] Insider threat control: using centralized logging to detect data exfiltration near insider termination. Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University. Retrieved from <http://www.cert.org/archive/pdf/11tn024.pdf> , Hanley, M., & Montelibano, J. (2011, October).
- [7] Sensage. (n.d.) A practical guide to next-generation SIEM. Retrieved from [http://www.sensage.com/sites/default/files/sens\\_gd\\_next-gen\\_siem\\_03ol.pdf](http://www.sensage.com/sites/default/files/sens_gd_next-gen_siem_03ol.pdf) . Last checked 2013, September 16.
- [8] Mohamed Zohair, “Business Development Consultant”. <http://www.slideshare.net/zohair1980/hp-arcsight> , ( November 2013).
- [9] General consulting [www.en.wikipedia.org](http://www.en.wikipedia.org).
- [10] SANS Institute InfoSec Reading Room, <https://www.sans.org/reading-room/whitepapers/analyst/arcsight-logger-review-34750>, (January 2009).