MAINTAINING HIGH LEVEL INFORMATION SECURITY IN ENTERPRISES USING EVENT CORRELATION

Marius VLĂDESCU[1], Valentin SGÂRCIU[2]

This paper presents measures for ensuring high level information security for enterprise systems. These mechanisms are based on the correlation of the events with risk factor, collected from the security systems deployed in the company's infrastructure. The role of event correlation systems is to detect real time security threats and to notify security personnel about those breaches, in order to take measures to reduce the impact of the threat. Our personal contributions in this field consist in creating correlation rules meant to ensure enterprise sensitive data confidentiality inside the company, mostly compromised by employees, and to secure industrial processes targeted by worms. We are also extending the functionality of the event correlation systems from alerting capabilities to real time response capabilities. Also, we conceived additional measures to secure the correlator, which involve approval workflows and encryption techniques.

Keywords: information security, event correlation, cryptography

1. Introduction

Information is one of the most valuable assets of a company. Regardless of the industry in which it activates, a company has to manipulate information in order to manage big volumes of actions and transactions. Communication and document exchange are mostly made through technological communication channels. Enterprises store a big amount of data in different locations and they need that data to be available at every moment. More than that, they need their data to be safe, undamaged, unaltered and most of all, confidential. Most of the information belonging to a company is stored and manipulated using technology, which can be exploited by persons or systems, in order to profit from stolen, intercepted, altered or destroyed information.

Cybernetic crimes are considered to be actions against private individuals, companies and organizations, and cybernetic attacks are considered to be coordinated actions against state public institutions. The most common cyber crimes intended to enterprises are [2]:

[1] Eng., Dept. of Automatic Control and System Engineering, University POLITEHNICA of Bucharest, Romania, e-mail: marius.vladescu@yahoo.com

[2] Prof., Dept. of Automatic Control and System Engineering, University POLITEHNICA of Bucharest, Romania, e-mail: vsgarciu@aii.pub.ro

- Hacking of computer systems and networks
- Malware programs(Viruses, Worms, Trojans, Trackware, Joke programs, Exploits, Adware, Spyware, Rootkit)
- Sabotage
- Fraud
- SQL injection
- Web based attacks
- Man in the middle attack
- Access control attacks
- Denial-of-service attacks
- Social engineering (Pretending, Phishing, Trojan horse, Tailgating, IVR)
- Identity theft

Companies are subject to incidents generated by the personnel also. This occurs when too much access is given to one person or when an employee or another person with access to the company's resources compromises data or systems intentionally (those may include: contractors, consultants, outsourced teams, partners, time-limited employees). Inside the company, most common cyber crimes involve: economic espionage, consumer harassment and consumer protection, e-mail abuse, Spam e-mails, Cyber defamation, theft of source code, insider attacks on personal database, information espionage, Denial-of-service attacks, exchange of business' secrets and documents. The threats that they impose are: data alteration, data destruction, transmitting sensitive data to unauthorized persons, system malfunction and misuse of applications, intellectual property theft and others.

2. Event correlation

Enterprises usually have big infrastructures. There are many points in the infrastructure that can be exploited for vulnerabilities. Usually, hackers scan the entire network of a company and look for weak spots that they can exploit. Having a complex infrastructure is a disadvantage from information security point of view, because security administrators have to deal with a big volume of data and many systems to monitor. This involves that a threat can be easily overlooked and even if it is spotted, it requires a lot of time and man power to identify it. To overcome this problem, it is best that security teams install event correlating systems that can spot a threat in real time and report an incident. An event correlation system is a very powerful tool which helps on having a global vision of the security state of the infrastructure. The main functions of event correlation systems are to gather information from different sources, to aggregate them into a

centralized location and to be able to link different events in order to detect weather they form a threat or not..

The biggest disadvantage of common information security systems like IDSs, IPSs, routers and firewalls is that they are dominated by false positives and false negatives. False positive means that systems indicate a security breach, even though there is none, and false negative means that security systems indicate that there is no security breach, even though it is. A very important ability of event correlating systems is that they can reduce the cases of false positives and false negatives [3]. These capabilities are ensured by the fact that event correlation systems gather information about the same event from multiple sources, and it can rate the detection error based on the information correlated from those sources. Event correlation engines replicate in real-time the job that information security administrators and systems make post-incident. This is one of the main advantages of event correlation systems.

Event correlation systems have 3 notification methods:

- To generate an alert in the monitoring dashboard
- To send an email regarding the incident to authorized personnel or information security teams
- To send a SMS regarding the incident to authorized personnel or information security teams

3. Types of event correlation systems

There is a large variety of event correlation systems, but most common ones are:

- event correlation systems based on predefined rules
- event correlation systems based on statistics

For understanding how different types of correlation systems work, we will use a common enterprise infrastructure, depicted in fig. 1.

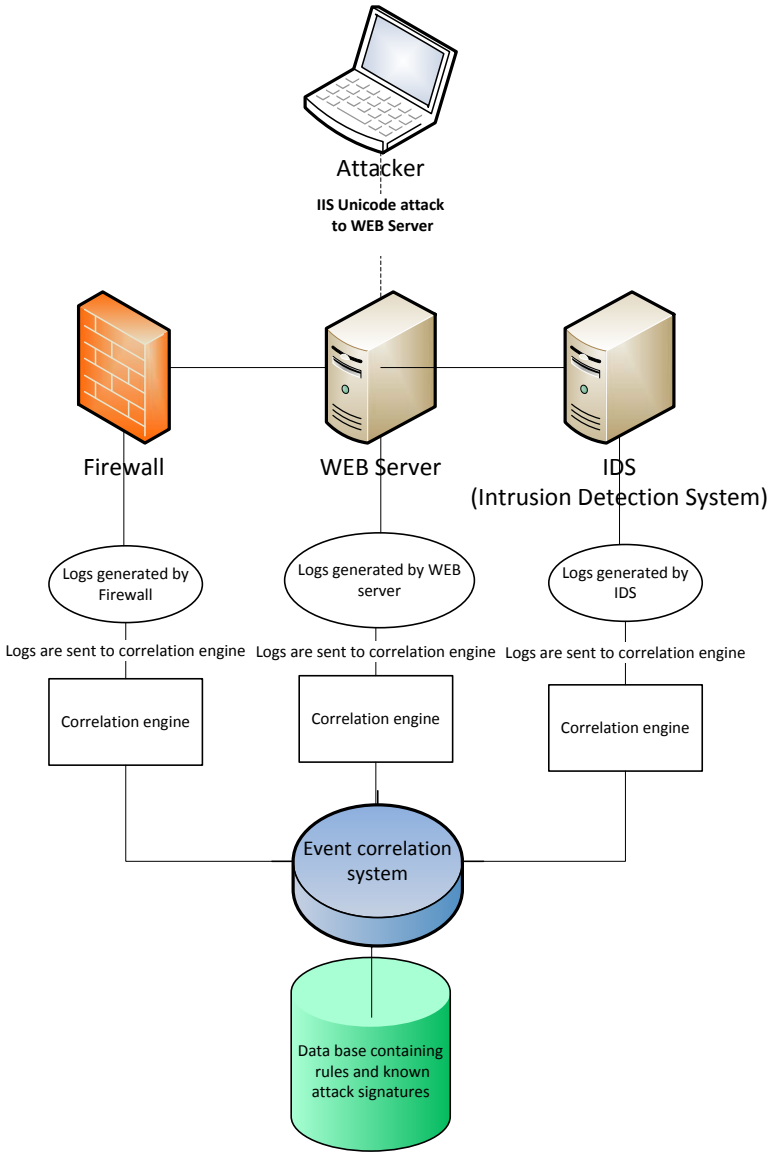

Fig. 1. IIS Unicode attack

Event correlating systems based on predefined rules recognize attack methods and weak spots in systems. The correlation rule applied for the IIS Unicode attack for example is build from 2 conditions:

- condition A: the logs provided by the intrusion detection system claim that there have been malicious demands that contain "cmd.exe" command

- condition B: the logs provided by IIS claim that there have been malicious demands that contain "cmd.exe" command

The 2 conditions fire rule nr #01IISUNI that states "known pattern attack IIS Unicode".

Event correlation systems based on statistics don't have any information about known attack rules, but they rely on monitoring the network and systems behavior inside the company. Ongoing events are analyzed by an algorithm and they are compared with stored activity patterns, in order to identify abnormal activity. This technique is based on analysis of time and value indicators. Companies must set systems value that they posses (servers and network devices) and the loss potential that those systems pose. Most correlation systems that use this technique use the following formula to determine the risk generated by an attack:

$$R = V * S * C, \tag{2}$$

Where:
V = value
S = severity
C = criticality

The severity is determined based on the type of the vulnerability exposed, and the criticality is determined based on the threat and the impact that the incident has on the data, on the systems involved and on other systems inter-correlated with the affected ones. If the criticality, severity or value set for the server involved in the incident is high, the risk will be set as high.

4. Steps necessary before the correlation

Before correlation rules can analyze the logs, preparatory steps are needed.

a. Log aggregation.

The first step in event correlation is to aggregate logs into a centralized unified system. This process poses the following risks [3]:

- logs can be intercepted
- logs can be altered
- logs can be transmitted with delays
- logs can be lost in the transmission process
- logs are not transmitted

In order to protect logs from being intercepted or altered, the transmission channels must be secured. We propose for this step an encryption technique that assures confidentiality, integrity and non-repudiation for transmitted data.

This crypto security system ensures (Fig. 2):

- Data integrity – using hash function

- Authentication and authenticity – using digital signature (DSA – asymmetric cryptography)
- Data confidentiality – using AES (Advanced Encryption Standard – symmetric cryptography algorithm)

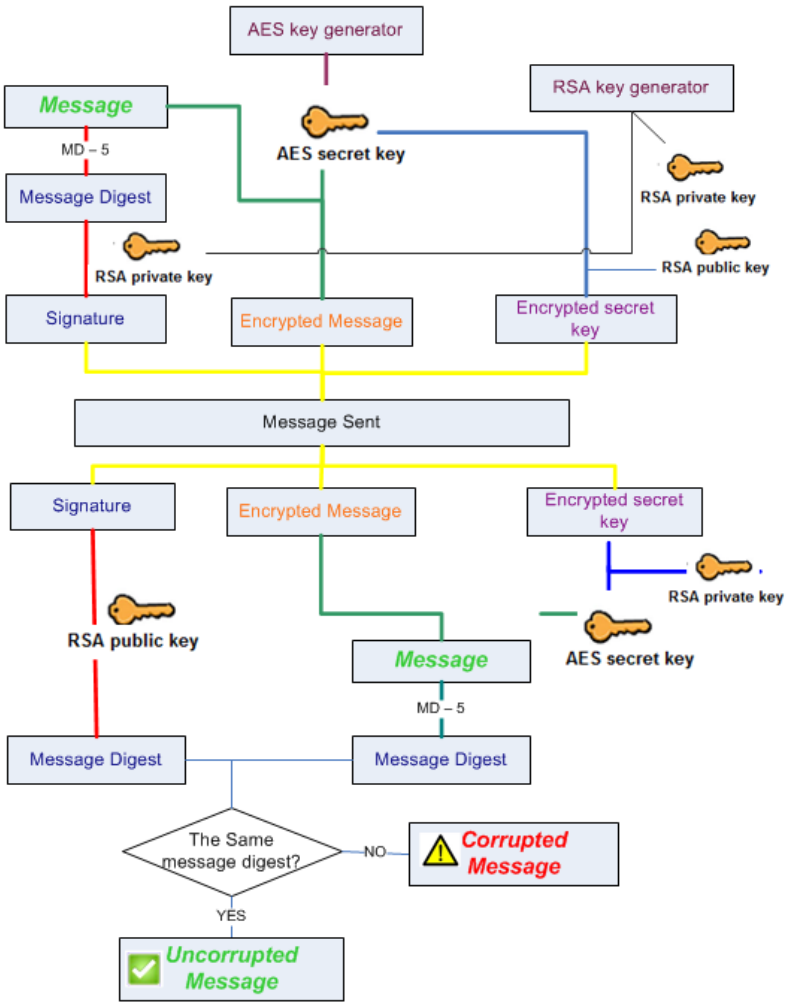

Fig. 2. Encryption schema

By combining different cryptography techniques, this approach offers a solution for various weaknesses that must be faced in a security crypto system including:

- Key encryption management: key generator, key storage, key transmission
- Reasonable computing time

- Ensure all the security goals: integrity, availability, authentication and confidentiality

b. Log normalization

Once the logs are transmitted securely and aggregated into a centralised system, they must be reformatted. In order for the correlation engine to apply patterns on the logs, logs must have a format that is recognizable for it [4]. Event correlation systems use parsers to identify key indicators in logs, and insert those indicators into a specified language. Most event correlation systems use XML as universal language for aggregated logs. Key indicators are based on meta-data identified in logs as: Session ID, Timestamp, Type of event, Impact of event, Priority of event, Log accuracy, Application, transport and network protocols, Source and destination IP, Source and destination UDP and TCP ports, Transmitted number of bytes, Decoded data, Session related information, Other fields from packet headers.

c. Log reduction and log size reduction

After they are normalised, the logs are inserted into the correlation engine database. In order to be easily interpreted by the correlation engine, the size of the logs must be reduced. This goal is achieved by correlating similar logs into one. For example, if there are 100 logs in an interval of one hour which state that "*port x scanned by aaa.bbb.ccc.ddd external IP*", they can be compressed into one log stating "*100 ports scanned by aaa.bbb.ccc.ddd external IP in the last hour*". Log reduction cannot be used for all types of logs and this is a choice that the system administrator must take. Log reduction can also lose important data in some cases. This is very useful for detecting threats in real time. If a post incident analysis is made, security administrators use the entire set of logs to make a root-cause analysis.

d. Log prioritization

Log prioritization is made by correlating events that contain meta-data regarding services, vulnerabilities, source and destination systems. The critical attributes for log prioritization are: Threat code, Threat description, Version and type of the OS from the machine on which the incident occurred, Ports, services and applications from the machine on which the incident occurred, References.

Based on the risk of the threat, every event gets a score. The events with high score are pushed forward. For each alert, the event correlation system looks for dependencies between events with risk and events without risk but related, based on key indicators like the IP of the attacker.

5. Event correlation for internal security

Internal threats are seen as security violations from persons inside the company. Those threats are more encountered than external threats, because

vulnerabilities are often overlooked and employees have easy access to sensible information and critical systems or programs. Also, employees have a better knowledge of internal software and hardware infrastructures. The most dangerous threats are represented by administrators, consultants, company partners, integration teams and outsourced teams that mainly have extended access to resources.

Intellectual property theft is very common in enterprises, mainly because it is hard to be identified. This usually occurs when an employee is about to leave the company and it is in short notice period. Most of the times, before they leave the company, employees transfers sensitive information on external devices such as USB drives or external hard disk drives. To prevent this from happening, we propose an integration of event correlation systems with:

- Data Loss Prevention System (DLP)
- Domain controller Active Directory (AD)
- VPN devices
- Operating systems used by employees

First of all, companies must identify and classify their sensitive information using DLP systems. Once this is done, DLPs can identify and stop any attempts of misuse of previously set sensitive information. The capabilities of DLP systems are [5]:

- Discovery and classification of data, even in heterogeneous environments: this function is assured by searching, inventorying and classification of stored information
- Information monitoring and information protection: based on configuration module, the system tracks and blocks misuse of data manipulation. In this cases the user responsible for the incident may or may not be warned about which information security policy he has broken
- Administration and reporting module: the system alerts authorized persons about data misuse inside the company. DLP must indicate the type of information involved in the incident, the name of the user that manipulates the data, location of the data and the station from where the incident occurred.

Internal procedures regarding employees' management should define special security rules and policies for groups of users with special status like employees that are in the short notice period. We propose to do that by setting special attributes like "employee_in_notice_period" and "remaining_time_in_company" in Active Directory Users and Computers in the Domain Controller. Active Directory logs must have those attributes predefined as meta-data, in order for the correlation engine to be able to prioritize them as important.

The event correlation system gathers information from both DLP and Active Directory systems, regarding the actions made by an employee. We created a correlation rule for one of the most common cases of internal information security breach: the theft of valuable confidential data like lists of account, clients, blueprints or designs. If, for example, the employee tries to transfer a large quantity of internal information (a transfer limit is set in the correlation rule) or he tries to copy sensitive data (identified by DLP) on an external storage unit, a correlation rule fires and the employee's User Account from Active Directory is disabled. Fig. 3. depicts the process in which a correlation rule is fired when an employee which is in notice period (and has a flag set in Active Directory) tries to send sensitive data through the internet or tries to copy data on external drive.

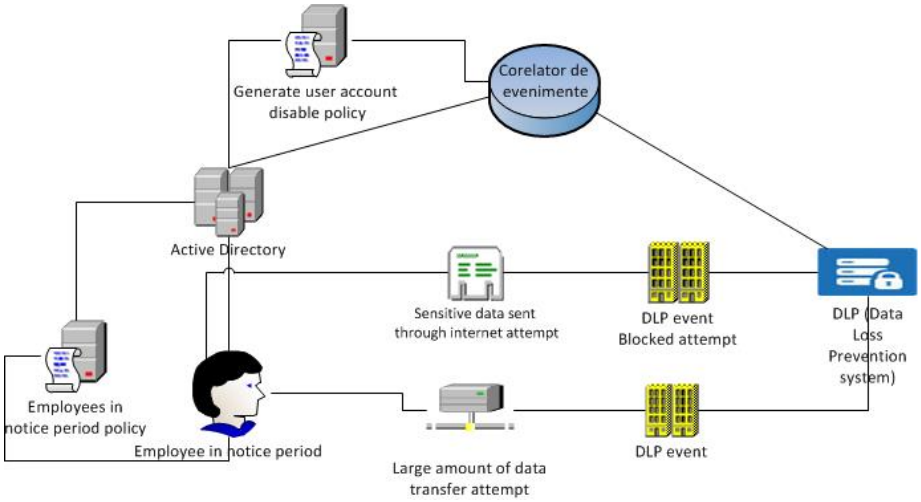

Fig. 3. Event correlation for internal security regarding theft of intellectual property

Based on the predefined rule, event correlation system must take an action. Most of them generate an alarm and notify security personnel about the incident. We have altered the action of alarm into a batch file that commands remotely the disabling of the user account that generated the incident through Active Directory controller. By that, we have extended the basic functionality of event correlation engines. The process is depicted in Fig. 4.

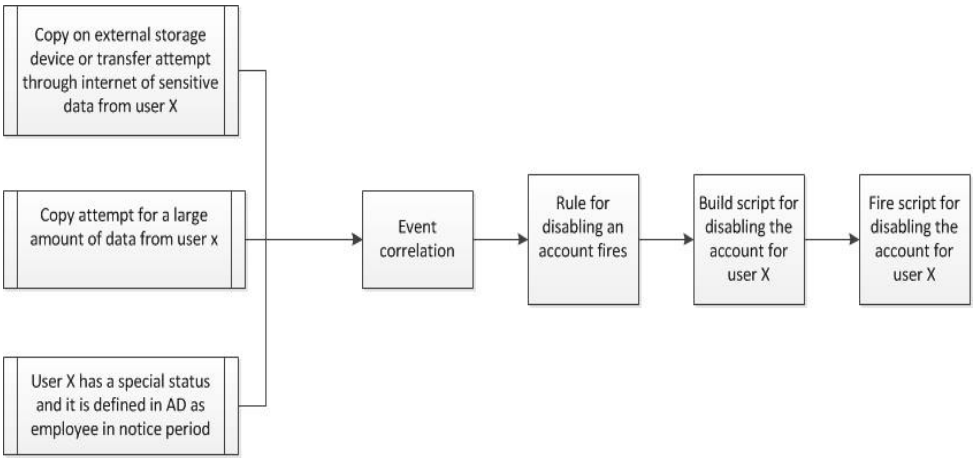

Fig. 4. Response of event correlation system for theft of intellectual property

The script for user account disabling process is built using the following command syntax and parameters:

dsmod user <UserDN> -disabled {yes|no}

Table 1

Parameter description for dsmod command

Parameter	Description
<UserDN>	Specifies the name of the object
-disabled	Sets the value UF_ACCTDISABLED in userAccountControl
{yes|no}	Specifies whether that account should be disabled (yes) or not (no)

The name of the object is defined by 3 attributes:

1. CN – Common Name: the name of the user stored in Active Directory
2. OU – Organizational Unit: structure that groups domain objects
3. DC – Domain Controller: authentication and authorization system for all users and all the computers from Windows domain in a network. This allows building and imposing security policies for all computers and users and can deploy, install or run programs

All the attributes must be correctly set in the script. Before building the script, event correlating systems take the meta-data about the user, provided through Active Directory logs.

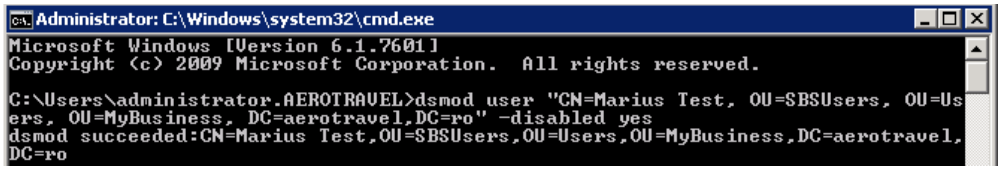

Fig. 5. Script for disabling a user account in Active Directory

If the user is disabled, he will not be able to logon next time he accesses the computer. But in order to withdraw all the rights instantly, a second script fires that logs off the user automatically. The script has the following syntax:

shutdown /l /f /m \\userx

Table 2

Prameters for remote logoff

Parameter	Description
/l	Logs off the computer
/f	Enforces running the application to close without forewarning users.
/m \\computer	Specifies the target computer

If the second script is run, the user is logged off automatically and he will not be able to login again, until an Active Directory administrator reinstates it. Companies that have many platforms and programs for one user, use identity management systems, which are integrated with the Active Directory. Once the Active Directory account is disabled, all the accounts from the other platforms are disabled as well.

6. Contribution of event correlation in industrial process control

Big scale industrial processes use industrial networks to handle communication between command control computers and process devices. If a control system network is compromised, this has a direct impact on the processes. Consequences of a disturbed process workflow can be devastating and can even result with human casualties. For example, tampering with the temperature of the cooling tower in a nuclear power plant can have as effect a nuclear explosion. Tempering with the turbine speed in a water power plant can cause enormous pressure or it can indicate that the speed is high even though the turbine is not working. This could cause massive blackouts [6].

The worm Stuxnet, for example, is part of the APTs (Advanced Persistent Threats) and it is considered the new weapon of cyber war. In 2010, the worm was used to destroy 1,000 centrifuges which were responsible for enriching weapons-grade uranium at the Natanz nuclear facility in Iran, by accelerating the electric motors to damaging speeds [7]. A worm like Student must be deployed into a system through a USB stick, but after it is deployed, it proceeds on infecting all interconnected machines that run Microsoft Windows, by replicating itself. It is able to convince the other computers that it comes from a reliable company by brandishing a digital certificate that can bypass automated detection systems. After the infection has taken place, the worm verifies if the machine is part of the targeted industrial control system made by Siemens. If it is, the worm accesses the internet and updates itself to the latest version. Otherwise, it does nothing. The next step is to compromise the target system's logic controllers, by exploiting "zero day" vulnerabilities software weaknesses that security experts

haven't identified. After the system is compromised, the worm studies the operations on the target system and uses that information to take control of the processes. While it has control on the processes, it provides false feedback to outside controllers or monitoring systems, in order to hide the malicious activity until it is too late to take action to minimize the damage.

Event correlation could identify the worm from the first step of its action cycle (the infection and replication). As the worm is instructed to replicate itself on the other interconnected machines, an event correlation rule can fire if it detects exchange of packages between then in a certain order, based on the infrastructure of the network. Let's take for example the bellow infrastructure depicted in Fig. 6.

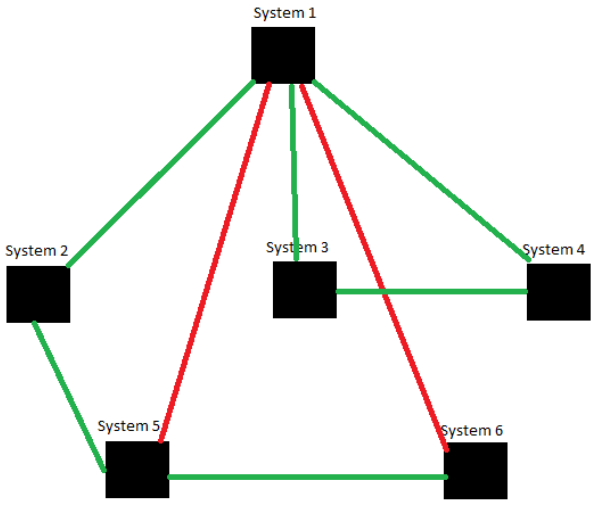

Fig. 6. System infrastructure

In our infrastructure, the green line represents direct communication between systems, and the red line represents indirect communication. The event correlation system should fire an alarm if one or more of the following sequence of events take place:

1. System 1 tries to access the internet (to update for the latest version)
2. System 1 transmits X Mb to System 2, System 3 and System 4
3. Systems 2,3,4 try to access the internet (to update for the latest version)
4. System 2 transmits X Mb to System 5
5. System 3 transmits X Mb to system 4
6. System 5 transmits X Mb to System 6
7. System 4 transmits X Mb to System 3

The communication between the controllers and the control system must be made using the encryption schema that we exposed at point 4, which insures

data integrity, authentication and authenticity and data confidentiality. If all communication links between the systems are secured with strong encryption, the risk of tempering the data and replication of the worm are diminished.

7. Security measures for event correlation system

Giving event correlation systems extended functionality like taking and action is risky. In our case, if the event correlation system is compromised, it can disable all accounts, including the accounts of the administrators. Securing the event correlation system is a very important aspect. All aspects of security must be taken in consideration when such system is in action. It is important that even if an attacker gains access to it, he won't be able to disable the systems that communicate with it also. For securing the transmission channels between the event correlation system and the other security systems, we use the encryption technique used for log aggregation, presented at chapter 4. Most of the attackers try to get more rights when they breach a system. In order to exclude this vulnerability, we propose an approval workflow defined by the Identity Management system. This workflow has the following steps:

1. Every user must make a request for gaining rights to 2 administrators
2. Every administrator validates what rights he trusts to be safe to give
3. Only the rights that have been approved by both administrators are enabled
4. All the security administrators and HR department are notified via SMS and email
5. The timestamp for each enabled right is stored

The same workflow is followed also for deletion, creating and altering the rules. No single administrator can manipulate the rules. There must be at least 2 administrators to do so.

For communicating with the other security systems, we use uncommon ports.

8. Conclusions

In order to ensure an efficient alert system for information security threats, enterprises use event correlation systems. The only purpose of those systems is to alert security administrators. We have extended this functionality into taking real time action against the information security threats that occur. Our model is based on internal security measures, intended to block attempts of intellectual property theft, from employees who are about to leave the company. Our event correlation system works with Active Directory domain controller and Data Loss Prevention system and gathers information related to internal employees that are in notice period, in order to detect sensitive data transfer attempts. In case the events

collected from the sources indicate that there is an ongoing incident, a rule fires and deactivates the user account. In order to regain access to the company's resources, the employee must reclaim its rights. We used this scenario because this is the most common scenario for intellectual property theft in enterprises.

For securing industrial process systems, which are found mostly in militarized zones, but subject to worm attacks, we propose a correlation rule that identifies replication attempts of the worm. In this manner, we can alert the security personnel about the threat in the early stages of the attack.

To secure the event correlation system, we impose an approval workflow for gaining access rights and bring modifications to the correlation rules. Also, for securing the communication channels between the event correlation system and the security systems which communicate with it, we propose an encryption technique, that ensures confidentiality, integrity and non-repudiation for sent logs.

Event correlation systems that take real time actions are very efficient security tools, because the damage is reduced to the maximum due to real-time response and future attempts are stopped.

R E F E R E N C E S

[1] *Ponemon Institute,* 2013 cost of Data breach Study: Global Analysis, 2013 https://www4.symantec.com/mktginfo/whitepaper/053013_GL_NA_WP_Ponemon-2013-Cost-of-a-Data-Breach-Report_daiNA_cta72382.pdf

[2] *M.Harkins*, Managing Risk and Information Security, December 17, 2012, ISBN-10: 1430251131, ISBN-13: 978-1430251132, Edition 1

[3] *Anton A. Chuvakin, Kevin J. Schmidt, „Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management „ Decembrie 13, 2013, ISBN-10: 1597496359 | ISBN-13: 978-1597496353 | Ediţia: 1*

[4] *Debar, Hervé and Wespi, Andreas,* Aggregation and Correlation of Intrusion-Detection Alerts.. London : Springer-Verlag, 2001. RAID '00 Proceedings of the 4th International Symposium on Recent Advances in Intrusion Detection . pp. 85-103.

[5] *K. Roebuck,* Data Loss Prevention (DLP): High-impact Strategies – What You Need to Know: Definiions, Adoptions, Impact, Benefits, Maturity, Vendors, ISBN 1743045492, 9781743045497, Emereo Pty Limited, 2011

[6] *Eric D. Knapp*, industrial Network Security, 2011 Elsevier Inc.

[7] *David Kushner,* The Real Story of Stuxnet, 26 Feb 2013, IEEE Spectrum