Concordia University College of Alberta

Master of Information Systems Security Management (MISSM) Program

7128 Ada Boulevard, Edmonton, AB

Canada T5B 4E4

Study of the Enterprise Security Manager / Security Incident Manager (ESM / SIM) Commercial and Open Source Solutions

by

CHOL, Emmanuel

A research paper submitted in partial fulfillment of the requirements for the degree of

Master of Information Systems Security Management

Date: April 2007

Research advisors:

Pavol Zavarsky, Director of Research and Associate Professor, MISSM

Study of the Enterprise Security Manager / Security Incident Manager (ESM / SIM) Commercial and Open Source Solutions

by

CHOL, Emmanuel

Research advisors:

Pavol Zavarsky, Director of Research and Associate Professor, MISSM

Andy Igonor, Associate Professor, MISSM

Reviews Committee:

Ron Ruhl, Assistant Professor, MISSM
Pavol Zavarsky, Associate Professor, MISSM

Date: April 2007

The author acknowledges the significant contributions to the work by Academic Advisors and Review Committee Members and gives the right to Concordia Univeristy College to reproduce the work for the Concordia Library, Concordia Websites and Concordia MISSM classes.

Emmanuel CHOL **27th April 2007**

ISSM Research Paper

Study of the Enterprise Security Manager / Security Incident Manager (ESM / SIM) commercial and open source solutions

Acknowledgements

I express my gratitude to all Canadian and French people who gave me the opportunity to complete this thesis trough their knowledge, ideas, references or contacts.

I would like particularly to thank Dr. Pavol Zavarsky - Director of Research and Associate Professor - who guided and followed me during this thesis, and also the Concordia teacher staff for their knowledge shared all along the Information System Security and Management Master Degree courses.

Furthermore, I would like to thank my French engineering school “Ecole Centrale d’Electronique” to offer this exchange program opportunity.

Table of contents

Table of figures

Introduction

The Enterprise Security Manager / Security Incident Manager (ESM / SIM) solutions were developed to enhance security. They are also called Security Information and Event Management (SIEM) from the merge of Security Event Manager (SEM) and SIM products. Such products were developed in order to solve difficulties. These ones resided in the fact of handling logs data from heterogeneous and independent sources spread across the company.

The idea was to collect and centralize data to process it using correlation methods, processes that could increase the detection of anomaly up to 35% [1]. These operations save time and increase the accuracy of security alerts. The cost of data analysis was reduced by more than 50% by the ESM / SIM users. Also a Managed Security Services Provider company claimed that, its incident count decreased by 70%, its incident management labour decreased by 80% and the reporting time requirement decreased by 83% [3].

Moreover, recent security laws, like the Sarbanes Oxley Act, led company to follow security compliances in order to provide evidence to business partners and stakeholders. The review of Security Information Management Tools article [8] stated that through the three past years the SIM products gain ease of installation and use. Some products are bounded on systems or appliances which could encourage companies to try and install them. North American companies showed a strong interest on ESM / SIM solutions, 30% planned to implement such a solution in 2006 [9].

The following study will rely on brochures, demonstrations, datasheets and manuals describing the ESM / SIM solutions. Each section of the outline will describe a panel of available methods. The Open Source Security Information Management (OSSIM) solution will be used to see an ESM / SIM in action [6]. Some correlation rules and console outputs will be showed. It will provide an insight on the logs and alerts management and also on data correlation.

I/ Logs files and flow transport to the SIM

Agent / Agentless / Flow (protocols and bandwidth use) / Security processes

Logs data need to be transported to the ESM/SIM solution to be processed. Nowadays, agent and agentless solutions combined with multiple options are available.

On one hand, I will describe the agent way of data collection through its tasks and roles.

Agents could be installed on a host to push information to the ESM/SIM server. Agents provide bandwidth management: by scheduling the data transmission they could optimise the network traffic during employees working time. The settings level of data compression could also save bandwidth, nevertheless it adds processing. Data transmission can be fired after a time window or when an amount of data is reached.

Agents can filter information in order to transmit only relevant ones. In that case the remaining information will not be stored, except if raw data are also transmitted.

Agents can adapt the level of risk. For example, two similar devices used as production and test will not require the same attention. A unique agent ID will be used to identify the agent into the SIM database.

Events aggregation could also be used. It aggregates N events based on similar field information. The agent sends to the SIM the number “N” to keep track of the real number of events and the X events corresponding to X/N events.

Agents also add information to identify the source and check the host time to insure time consistency.

Agents could normalize data to store them into a common format.

Depending on the source, the data processing priority can be set up. In case of high priority, the data are sent to the data repository and also directly to the processing stage in order to save time before processing them. Indeed, it is time consuming to write into the data repository, and then to search for new entries, read and process them. This is not the case for every solution and usually the data are only read from the database.

Agents CPU use can be limited in order to keep running services smoothly.

Agents’ transmission relies on the TCP protocol which provides security features. Indeed, the agent could be set up to open a secure tunnel to perform authentication and encryption. In case of data repository server failure, the agent will hold the data. The transmitted log file integrity could be checked by calculating a message digest based on MD5 or SHA-1 algorithms. The program compares if the agent and server message digests match to check the integrity.

On the other hand, the agentless way of data collection is used for devices on which program installation is impossible. Router sending events using syslog format for example. The syslog flow is based on the UDP protocol which is light, unsecured and does not require a

lot of processing. The agentless method also applies when hosts can send or share information without the installation of an agent. In such case there is no agent to maintain or update. For example, a samba server checking the ESM / SIM server authentication and granting access to log files. In this case the filtering, aggregation and normalization is performed on the server side. Some options like the compression may not be available.

Depending on the network architecture, the flow might be transferred on a separate network in order to avoid bandwidth problems and provide more security. It could be useful in case of syslog implementation; as it does not provide access control; which can lead to false inputs into the system to flood and misinform it.

Independently of the chosen mode of transmission data are stored into a database.

II/ Logs storage

Commercial database / Proprietary database / Performance / Normalization

The log storage is performed using commercial database like Oracle and MySql or proprietary database. Performances obviously depend on the hardware, but also on the database architecture.

Some companies developed architecture as the Internet Protocol Database (IPDB) [7] that was designed to capture all the data and analyze both real-time and historical data. It was also designed to:

- Store and work efficiently with unstructured data natively, without any filtering or data normalization
- Maintain a digital chain of custody for all data which assures that once data is committed to the database, it can never be altered — unlike most data schemas used in RDBMS based solutions.

This protocol also requires none agents and is based on a distributed peer-to-peer architecture that enables high scalability and performance.

The commercial databases come with unuseful features that using processing resources like reindexing. They were also developed for multi reads and writes operations as it turns that only a single write and multiple reads operations is required.
According to the section of the article called « Is RDBMS Bad in the SIM World? »[8]; the proprietary databases are beneficial in case of multiple Terabyte data.

The way of storing the data is also a key point; the normalization into a common schema provides data consistency. Normalization requires logs parsing to extract information. The database contains all captured events but also the ESM/SIM configuration including rules, areas, reports and credentials. Raw events are often stored because it could be a requirement in case of lawsuit. The database confidentiality, integrity and availability are

critical as it will hold the system data. The system must be scaled to hold, protect and save this information.

In addition to the database storage, the storage of raw data can be performed and some message digest calculated and stored on another support as proof of integrity.

The knowledge contained into the database will be processed in order to detect alerts.

III/ Alerts classification

By level of risk / By device / By network

The aim of ESM / SIM solutions is to provide a clear understanding of what is happening on the companies' assets.

Searches are simplified by setting up some groups. It could be related to risks, devices, networks, users, types of attacks, etc. It will provide information to reduce the process to display relevant information on the control console. We will develop some of the classification groups.

- By level of risk

Each event is different and can be considered more or less risky depending on the situation. The level will be higher in a production environment than in a testing one. An event might occur on a running service or be non relevant in case of no such running services. The access to a device can be allow to anyone and does not need any supervision or might be confidential and supervised. These studied parameters led to set a risk level to an event and allow classifying it. It will be use to prioritize actions in case of multiple alerts.

- By device

In order to track efficiently which device is under attack, we need to organize and identify each device taking part of the IT security plans. The value of the asset can also be set up according to the specificities and functions mentioned previously.

- By networks

The companies are usually divided in several networks. One for each floor of the building or one by service and so on… Being able to identify which are concerned by an event and dig into the event will save time.

Alerts are part of information accessible from the SIM interface.

IV/ Interface and analyse functions

Java console / HTML console / Graphical summaries with clickable elements / Searching tools to dig into logs and/or databases / Searching tool through a knowledge database

The graphic user interface is the control and information center of the solution. It allows saving time to respond to an event. ESM / SIM products provide consoles developed in JAVA or HTML in order to be used on different platforms: UNIX, Windows, MAC and SUN. Consoles might need up to 2 GB of RAM to run smoothly [8].

Console provides critical information and allows digging into events. Alerts are displayed in real time. Some clickable graphics give an overview of what happened on which devises.

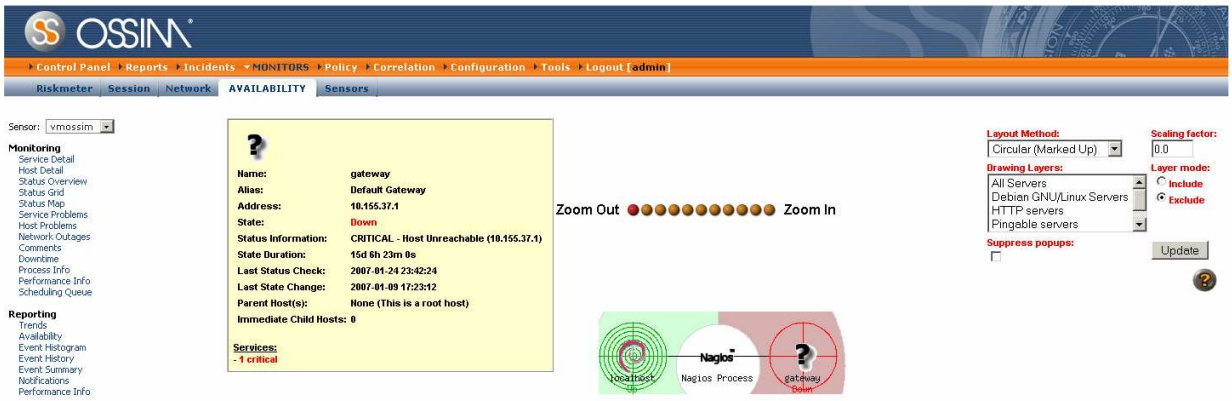


Figure 1: OSSIM availability console

Details on the concerned devices and the sequences of events allow tracking events through the network and the attack steps. The traffic payload that generates an alert can also be analyzed.

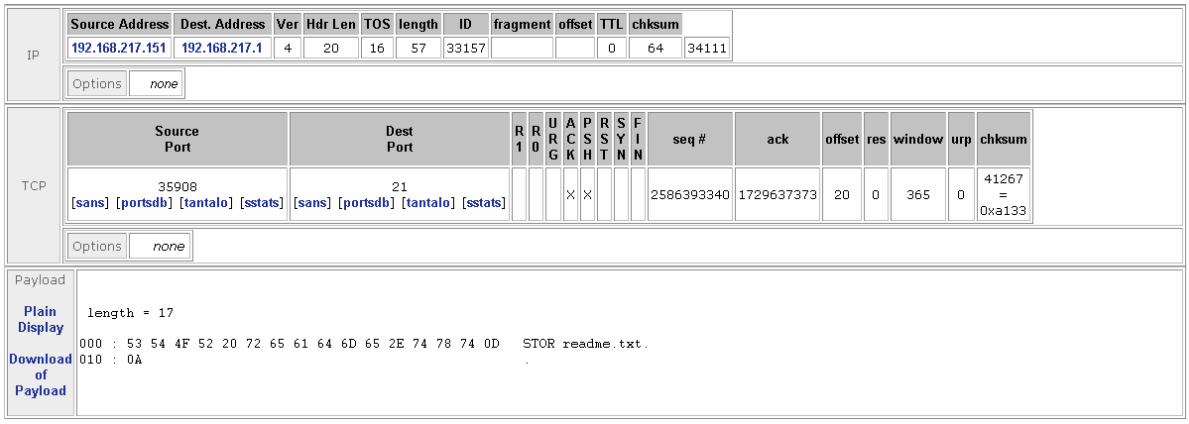


Figure 2: OSSIM Forensics BASE/ACID tool

The display mode can be set up to provide relevant information to a high level manager or a security specialist for example, in order to fit their job requirements. A specific area might always be on top of the windows due to its high security and short response requirements. The different information can also be displayed as a slide show to keep an eye on different windows. Some snapshots of events can be extracted from real time information.

Performing queries might be complex, some solutions require several steps. The console gets a large dataset based on a single criterion and then the user performs a search on this dataset. This can be slow as the application needs to get a large amount of data to perform more precise research on. Others solutions allow to query directly the database and load only relevant information. The queries could be based on criteria such as time period, network address, type of devices, etc. Depending on the solution, it might be more or less complex to generate those queries. Some queries can be saved and use as filters for further investigation. Although searching through raw traffic stored about a critical asset could allow understanding which information has been or could have been stolen.

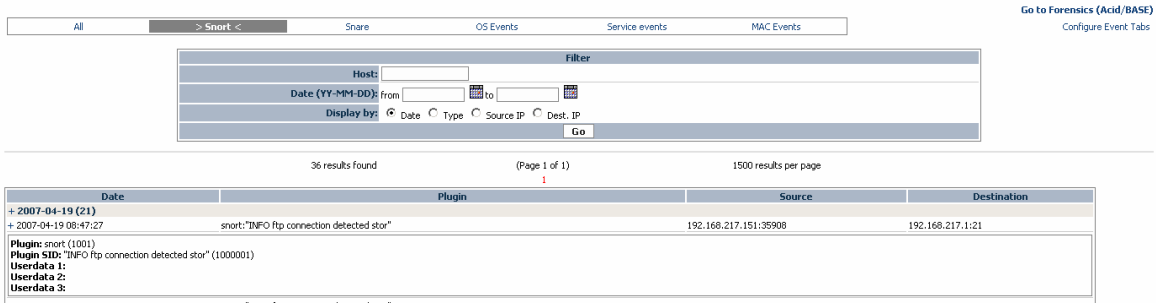


Figure 3: OSSIM Queries on events

Reports could be generated by querying for specific information and built using preconfigured templates. Historic of events which happened on different networks or devices for example can be generated. Actions done from an IP or to a destination can easily be tracked and displayed on a spreadsheet. Even if a lot of templates are available, solutions allow users to customize their reports to fit a special need. It allows creating a static report on a studied area. The reports can be generated for auditing purposes to show compliance with security or privacy regulations. Reports can be generated automatically; based on a time

period using different files' format like PDF, HTML, excel, CSV, etc. A report can also be produced from several reports by showing the differences or evolutions.

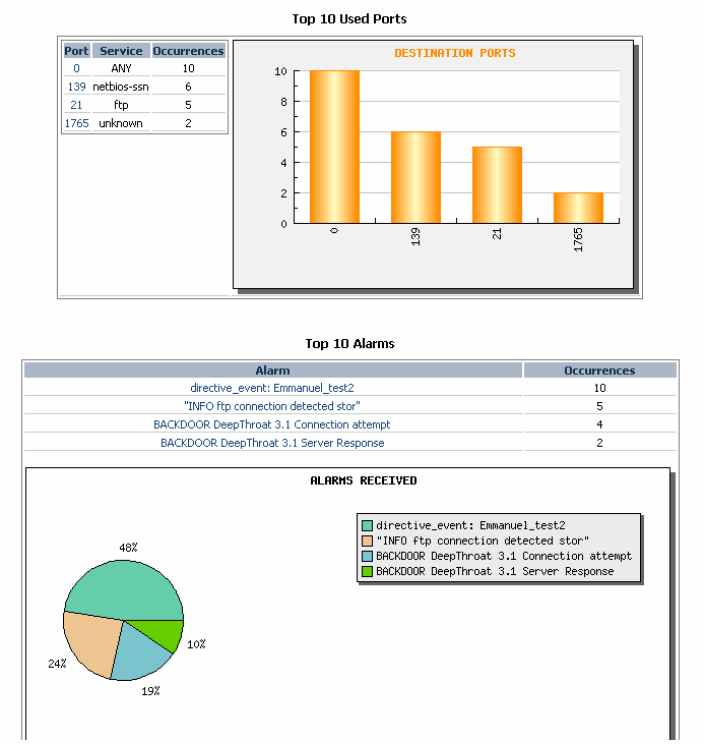


Figure 4: OSSIM Reports

Other features like the possibility to display devices' localization using GPS coordinates on Google Earth are available. This could be linked with events and quickly show which sections of the network are touched.

The log management can also be done by removing entries that are no longer relevant for security investigation.

The users and groups accounts to access the agents and shared information repository as well as the ESM / SIM credentials are set up through the interface. Credential might be delivered through Lightweight Directory Access Protocol or Active Directory accounts.

The actions of console users can be tracked and displayed to inform who has changed a correlation rule for example.

Depending on the software companies a lot of different functions are available. Like a notepad that allow leaving some comments on previous actions. It is always useful to follow up an investigation started by another person.

Rules can be set up using a pseudo programming language or via a rules editor. It allows through graphical options; containing conditional tabs and architecture information; to elaborate rules. Rules can be grouped by goals, studied areas and so on… to organise the events analysis. It is also possible to test the rules, and some ESM / SIM solutions auto disable a rule which is badly written and might trigger a large amount of alerts. When a rule is

triggered information about its frequency of occurrence, the level of security assigned to it and other user defined information; as the impact on the organization or on others dependant applications; is displayed. A unique ID is also generated in order to track and easily identify the event into the reports.

The architecture can be displayed based on assets, devices and network areas. It allows navigating through a graphic to get corresponding information like IP address, location, description of utilisation, historic of events and patches.

Some tools can auto perform ping test to check devices availability. Tracer, ping and such functions can be performed through the graphical console.

Scan, like Nessus one, can be scheduled and reports showed into the consoles.

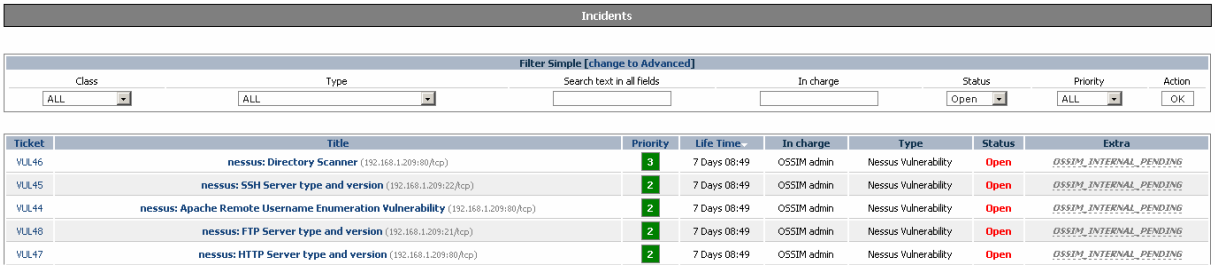


Figure 5: OSSIM Nessus incidents list

The policy can be set up to hosts, networks, agents and so on. We can describe devices and also set up the asset value.

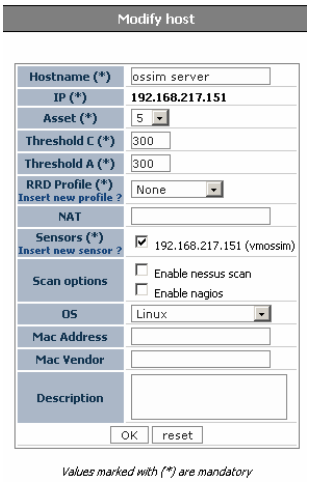


Figure 6: OSSIM host policy

In addition to the console, the solutions ease of use is also based on the installation and initialization which mainly depends on their compatibility.

V/ Compatibility

Log formats / Number of devices / Devices' flows (switch, firewall etc.) / Auto detection and calibration

The ESM /SIM out of the box compatibilities save a lot of implementation time. Most of solutions support information from Simple Network Management Protocol, HTTP, XML, Syslog, Syslog-ng, databases, formatted log file (ex: separated with comma), events Windows log API, and other proprietary protocols (ex: OPSEC originally created by Check Point Software). Log's formats are generated by applications, Operating Systems and devices.

For example, even a reader of badge data could be used to check if someone who is doing actions locally is physically present into the office-building. The SIM can extract information, knowing the data format, and gets values from a specific data area to normalize and store them.

The ESM / SIM can automatically detect devices, Operating Systems and application types. It categorizes information corresponding to a source flow. The data processing is calibrated to handle correctly these information sources.

Now that we have described how to collect and store data, we will see how we analyze them.

VI/ Correlation

Real time / Delayed / Both real time and delayed / Process from memory / Process from a database / Write correlation rules / Update of the common correlation rules / Multiple-event correlation / Linear / non linear correlation / heuristic algorithm

The heart of the ESM / SIM solution is the correlation process.

Correlation is the process of combining information from different sources in order to avoid false positive. For example, is an alert relevant for a specific asset? An Intrusion Detection System detects an attempt to exploit a web server breach but the device is not running any web server services. Or a firewall detects suspicious traffic to a web server but

the IDS did not reveal any attack on the web server. The correlation will avoid those false positive.

The correlation can be done in real time as soon as an event is received; it is test against a set of rules to check if it can drive to trigger an alert. An event might occur many times in a time period before it triggers an alert. Thus, correlation rules should be as specific as possible in order to provide more accurate information.

The pattern analysis also helps to elaborate correlation rules. The pattern analysis allows by the time to increase the strength of the system as it will hold larger information. Thus, pattern discovery will be easier. Normal patterns or potential threat pattern can be studied. This will give precious information in order to avoid false positive and to detect more accurately out of the line events or actions. The logs are checked against succession of correlation rules that are testing patterns.

Referring to part I/ Logs files and flow transport to the SIM, the event can be sent to the SIM database and also to the SIM correlation engine at the same time. Depending on the solution, the correlation process is done from memory or from the database. It is naturally better from memory as it reduces access time.

A delayed correlation might be run in order to study less important assets or to run a new investigation on previous events.

Programs may come with preinstalled correlation rules or example rules that help to get into the rules set up process. Rules are based on field information that are compared using “AND, OR, NOT, JOIN” conditions. The time frame and number of time an event occur, or how long after a first event a second occur is also taken into consideration. When a match is detected it triggers an alert and might also fire a response.

In order to demonstrate some correlation I built an OSSIM directive based on a scenario found in a commercial SIM brochure that I simplified for a better understanding. The step by step process is available in appendix A, page 19.

```
<?xml version='1.0' encoding='UTF-8' ?>
<directive id="2000" name="Emmanuel_test2" priority="5">
  <rule type="detector" name="SSH attempt intrusion" reliability="3"
  occurrence="1" from="ANY" to="ANY" port_from="ANY" port_to="ANY"
  plugin_id="4003" plugin_sid="7">
    <rules>
      <rule type="detector" name="use ftp to send information cf acid forensic to
      know more" reliability="4" from="1:DST_IP" to="ANY" port_from="ANY"
       port_to="ANY" plugin_id="1001" plugin_sid="1000001">
      </rule>
    </rules>
  </rule>
</directive>
```

A rule starts with a directive which is composed of a unique ID, a name that is displayed into the console when the directive is matched, and a priority level. The rule is then defined; it can be a detector type for rules received from the agent or a monitor type for rules

that must be queried by the ntop server. Rule is defined with a name and a reliability value, which is useful to follow an attack. The reliability will be low and increased further you detect events that correlate with an attack. The occurrence parameter is the number of times a rule must be matched before jumping to the next one. The from and to parameters are used to define an IP address, a group of IP coma separated or a variable corresponding to the network policy parameter might also be used. The port_from and port_to parameters are used to define the source port and the destination port or several ports separated by comas. This network parameters might be unuseful in this rule but using the ANY key-word it will allow to keep track of the connection in the following rules - using 1:DST_IP referring to the first rule or 2:DST_IP referring to the second one- . The plugin_id parameter is used to refer to the plugin we wish to use. Here, 4003 corresponds to the SSH, and the plugin_sid is the id of a plugin event, here it is SSH: Login successful (Accepted password).

The rules tag could be translated by an AND. The rules defined into these tags will be the next events that the directive must match. If several rules are defined into a rules tag an OR will apply between them. In our case, we detect if a snort alert (plugin_id 1001) is catching the ftp STOR event (plugin_sid 1000001). This event is initiated by the destination host of the first rule. This event pattern was added to the snort rules and has been register into OSSIM. It allows updating and adding rules built to fit security needs.

In addition to those parameters we can use:

- The time_out or interval parameter in case of monitor rules; it corresponds to the time windows - in second - during which a rule must be matched before it expires.
- The optional conditions: equal (eq), not equal (ne), lesser than (le), greater than (gt), lesser or equal (le) and greater or equal (ge); that need to be matched with the parameters value.
- The protocol can also be defined (TCP, UDP and ICMP). The negation is symbolised by “!”.

When a rule is matched, it is displayed into the event console. Its risk is calculated on OSSIM using this formula: "risk = (priority * reliability * asset) / 25". The asset value is set up into the policy section of the console.

We will have an overview of different methods used to do correlation.

The multiple event correlation is basically what we saw with the example rule where we tried to catch a sequence of events corresponding to attacks steps. The risk becomes higher when we detect more events that match the attack sequence.

The linear correlation method is used to correlate events succeeding in time.

The non linear correlation method is useful when we have a timestamp or a synchronisation problem. Events might not appear in the sequence that we try to catch them; by implementing such method we will be able to catch patterns and behaviours of events in disorder.

The correlation using heuristic algorithms, it tends to detect events without patterns or behaviours matching them. It helps to detect unknown attacks.

The correlation led to events detections that may trigger alerts. We will see how alerts and following actions are submitted to the decision makers.

VII/ Available information and actions following an alert

Alerts send to a console, by email, by SMS, etc. / Automatic action to stop the abnormal event / Suggest some actions to stop the abnormal event

Alerts are sent to decision makers through a couple of ways. Messages appearing on a console, emails and SMS can also be sent.

Figure 7: OSSIM alerts list

The alarms information lists events that have triggered an alarm. The correlation level attained and the risk corresponding is displayed. Using the forensic tools we can dig into events to know more about the devices and users involved. The payload of network traffic can be displayed. These actions describe a top down approach. Another approach: the bottom up one consists of analysing network traffic, detect attacks and then display it. It is the agent process that sends data to the SIM and then the SIM correlate and display alerts [4].

In addition, the system can be set up to automatically block actions. For example, a breach is used by an attacker and detected by the system that could block the attacker source IP address as well as his MAC address to access to this asset. Also the console can display some possible responses taken in the past and wait for their validations [2]. It is important to keep track of previous actions in order to make grow up the database knowledge. This will improve the response time in recurrent or similar attacks. Alerts also have a status in order to show if someone is analyzing the problem, if it is resolved, and also to track performed

actions. Depending on the kind of alerts, it can be sent to different groups of employees whom have knowledge or use of the attacked asset.

Solutions can also compare attack information with a knowledge database; common to all companies that use the same product; and allow sharing knowledge.

All these features should provide enough information to deal with an alarm.

Conclusion

The ESM / SIM solutions as described through their specifications provide an efficient way to deal with enormous data logs to detect, respond and generate reports on the IT security health. The security teams only need to concentrate on the ESM / SIM and free up time to investigate and improve event detection accuracy.

The Gartner study: “2006 Magic Quadrant for Security Information and Event Management, 1H06” provides results of use cases especially designed according to SIM software specificities [5]. This analyse revealed that some products are not designed to keep all logs and are not scaled for the same market target depending on feature that they offered. Some solutions come without predefined functions and are difficult to get hands on. The customization, the compatibility with log formats and the database tuning are also some issues. The real time, processing and security event oriented needs, could not be fit by all the solutions. The compliance and reporting needs are also not well handled by every solution.

There is still some work to do on the pattern discovery process, the compatibility, the user interfaces and the way to resolve automatically abnormal events. Nevertheless, the progress made through the past years and the dynamism of the market; showed through lots of company acquisitions; testify of a real interest on such solution. Some companies also offer possibilities to interface their SIM with their other products, like their identity manager software. I got some echo that it is a bit painful to configure those several in one solutions. The price, about one million Canadian dollars for an implementation and half of it for a small implementation, can also be a problem for small and medium companies to adopt such solutions.

Due to comprehensive confidentiality, security and business issues I did not succeed to get much information neither from SIM commercial companies nor from IT security managers. I struggle to find materials to study and share this knowledge through this paper. Further work could be done trying to reproduce some commercial software features using the OSSIM project. Also some functions studies and tests could be performed on commercial products. Finally, incrementing and updating this document could also be an interesting plan.

Appendix

Appendix A

The OSSIM practical application

I built an OSSIM rule based on a scenario found in a commercial SIM brochure that I simplified for a better understanding.

a) Preparation

You need to download the VMOSSIM 0704 version from http://www.ossim.net/vmware.php. It runs using the vmware player free version from http://www.vmware.com/products/player/.

Then, you install vmware player and uncompressed the VMOSSIM0704 image. You launch the VMOSSIM.vmx file. You log in as root user with vmossim as password.

To configure your keyboard you use the "dpkg-reconfigure console-data" command.

You need to remove the "/etc/udev/rules.d/z25_persistent-net.rules" file in order to detect the eth0 network interface. Then you reboot the vmware image using the "ctrl+alt+inser" combination or the reboot command.

Then, you need to install the ftp package; log as root user and run "aptitude install ftp".
To get connected to the internet you need to switch the vmware network device to NAT mode. You have to click on the Ethernet button to switch down and then up the network interface to make the image aware of changes. You launch a "dhclient eth0" command to get a dhcp bail.

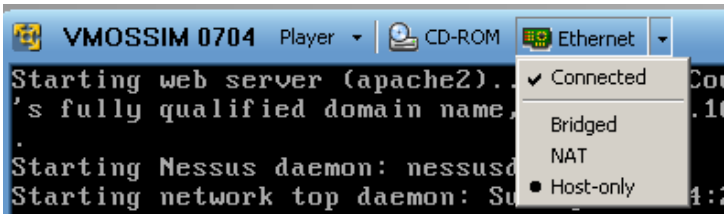


Figure 1: vmware player network configuration

After the installation, you switch to host only mode and configure your network interface by editing "/etc/network/interfaces". The defined IP configuration is written at the end of the file, please browse down. I set my VMOSSIM IP address to 192.168.217.151.Then restart it using "/etc/init.d/networking restart" and finally use the "/root/vmossim/tools/wizard.pl 192.168.217.151" to reconfigure the OSSIM server/sensor. You reboot the image.

b) Rule installation and OSSIM registration

You will add a new rule to snort: you could add a new file and register it into the snort.conf or add the rule directly into an existing rule like the /etc/snort/rules/info.rules file.

You add a rule tracking the ftp STOR command.

```
alert tcp 192.168.217.151 any -> any 21 (msg:"INFO ftp connection detected stor"; content:
"STOR"; nocase; pcre:"/^STOR\s[^\n]/smi"; reference:manu,2447; classtype:attempted-user;
sid:1000001; rev:1;)
```

Then you restart snort using “/etc/init.d/snort stop” and then “/etc/init.d/snort start”.

You can test the rule connecting to an ftp server. I installed and configured filezilla server on my windows box to do my tests.

```
VMOSSIM:~# ftp -n 192.168.217.1
220-FileZilla Server version 0.9.23 beta
220-written by Tim Kosse (Tim.Kosse@gmx.de)
220 Please visit http://sourceforge.net/projects/filezilla/
Name (192.168.217.1:root): anonymous
331 Password required for anonymous
Password:
230 Logged on
Remote system type is UNIX.
ftp> put readme.txt
local: readme.txt remote: readme.txt
200 Port command successful
150 Opening data channel for file transfer.
226 Transfer OK
6663 bytes sent in 0.03 secs (202.0 kB/s)
ftp> exit
221 Goodbye
```

Then you can check that it worked into the file:
VMOSSIM:~# vi /var/log/snort/alert

```
04/19-08:47:27.466385  [**] [1:1000001:1] <eth0> INFO ftp connection detected stor [**]
{TCP} 192.168.217.151:35908 -> 192.168.217.1:21 [14:1808]
```

You can also get more information into the corresponding tcpdump file; you can see “STOR readme.txt” at the end of the line.

Now you need to register the new plugin_sid into OSSIM by running
“/usr/share/ossim/scripts/create_sidmap.pl -e /etc/snort/rules/”

There is now a database entry for this rule.

c) Correlation rule

Now, our correlation rule is added to the OSSIM.

You create a myrules.xml file:

```
<?xml version='1.0' encoding='UTF-8' ?>
<directive id="2000" name="Emmanuel_test2" priority="5">
   <rule type="detector" name="SSH attempt intrusion" reliability="3"
   occurrence="1" from="ANY" to="ANY" port_from="ANY" port_to="ANY"
   plugin_id="4003" plugin_sid="7">
      <rules>
         <rule type="detector" name="use ftp to send information cf acid forensic to
         know more" reliability="4" from="1:DST_IP" to="ANY" port_from="ANY"
          port_to="ANY"   plugin_id="1001"   plugin_sid="1000001">
         </rule>
      </rules>
   </rule>
</directive>
```

You edit "/etc/ossim/server/directives.xml" and add:

```
<!DOCTYPE directives
 SYSTEM '/etc/ossim/server/directives.dtd'
 [
 <!ENTITY generic SYSTEM '/etc/ossim/server/generic.xml'>
 <!ENTITY trojans SYSTEM '/etc/ossim/server/trojans.xml'>
 <!ENTITY myrules SYSTEM '/etc/ossim/server/myrules.xml'>
 ]>

<directives>

 &generic;
 &trojans;
 &myrules;

 <groups>
  <group name="GroupTest1">
   <append-directive directive_id="1"/>
  </group>
 </groups>

</directives>
```

You copy "myrules.xml" to "/etc/ossim/server/"

You connect to http://IP_address/ossim and set up into the policy section both the OSSIM server and the attacker machine to an asset level of 5.

Now, you restart the vmware image and test the rule by connecting via SSH using putty for example to the OSSIM and then connect to the ftp server to send a file.

You connect again to http://IP_address/ossim and into the control panel/alarms section you should get a new entry and into the control panel/events you should see new events. You can go to forensics BASE/ACID page to check the event's payload.

Figure 2: OSSIM console control panel/alarm

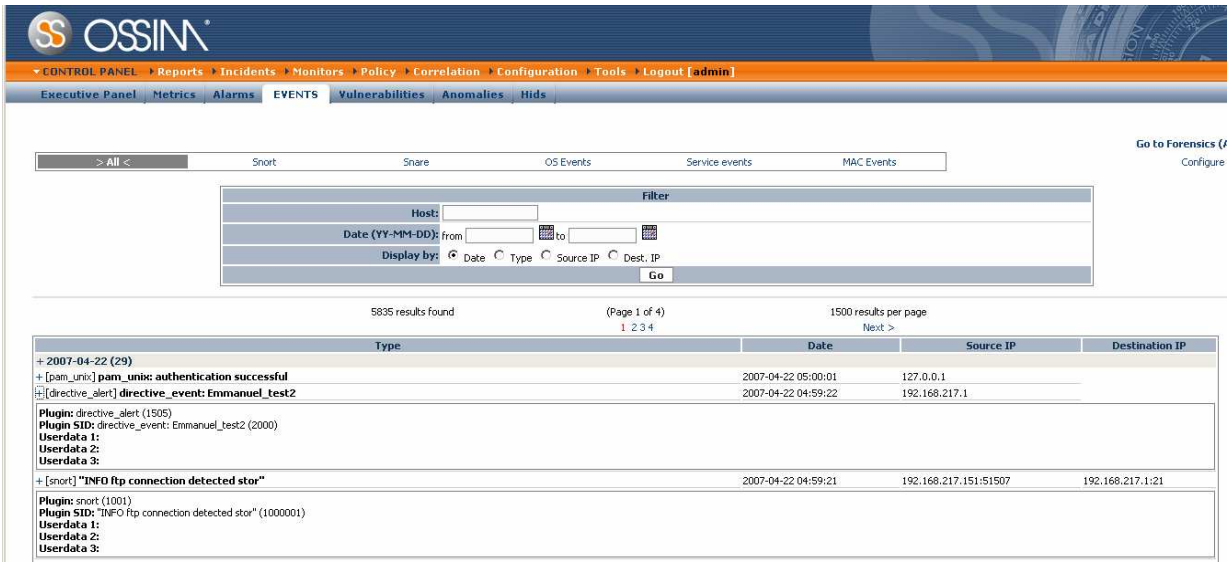


Figure 3: OSSIM console control panel/events

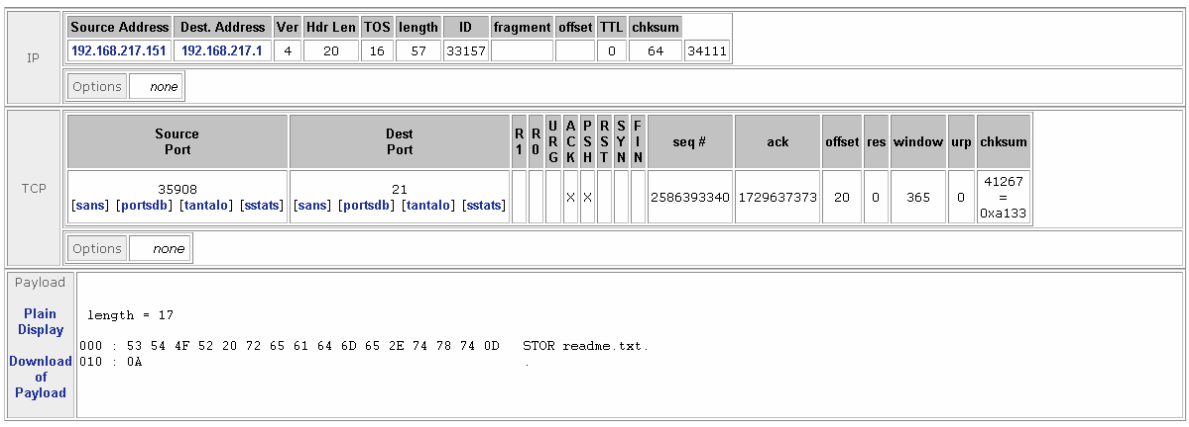


Figure 4: OSSIM Forensics BASE/ACID tool

I had set up into the policy section both the OSSIM server and the attacker machine to an asset level of 5. The priority and reliability are at a level of 5.
You obtain a risk of 4 which is equal to this formula: "risk = (priority * reliability * asset) / 25". I got risk=5 * 4* 5/25 =4.

I would like to thanks from the OSSIM developers team Dominique for the “–e” switch into the registering plugin_sid command and Juan Manuel for his tips to debug and test the OSSIM server. Thanks to these tests the OSSIM wiki was updated (sim_organizer_reprioritize: Error Plugin 1001, PluginSid xxxxxx section) http://www.ossim.net/dokuwiki/doku.php?id=vmossim:known_issues.

References

[1] Cristina Abadyz, Jed Taylory, Cigdem Senguly, William Yurcikz, Yuanyuan Zhouy and Ken Rowex. Log Correlation for Intrusion Detection: A Proof of Concept. *Department of Computer Science, University of Illinois at Urbana-Champaign, National Center for Supercomputing Applications (NCSA) and Science Applications International Corporation (SAIC)*, 2003.

[2] Gianluca Capuzzi, Egidio Cardinale, Ivan Di Pietro and Luca Spalazzi. An Incident Response Support System. *Università Politecnica delle Marche ,IJCSNS International Journal of Computer Science and Network Security, VOL.6 No.10*, October 2006.

[3] Brian Contos. Enemy at the Water Cooler, *Syngress*, August 2006

[4] Dario Forte. The"ART"of log correlation: part 1 - Tools and techniques for correlating events and log files. *Computer Fraud & Security, Volume 2004, Issue 6, Pages 7-11*. 1 June 2004

[5] Mark Nicolett, Paul E. Proctor, Amrit T. Williams. 2006 Magic Quadrant for Security Information and Event Management, 1H06, *Gartner RASCore Research Note G00139431, RA3 1192006*. 12 May 2006

[6] Open Source Security Information Manager: *http://ossim.net/*

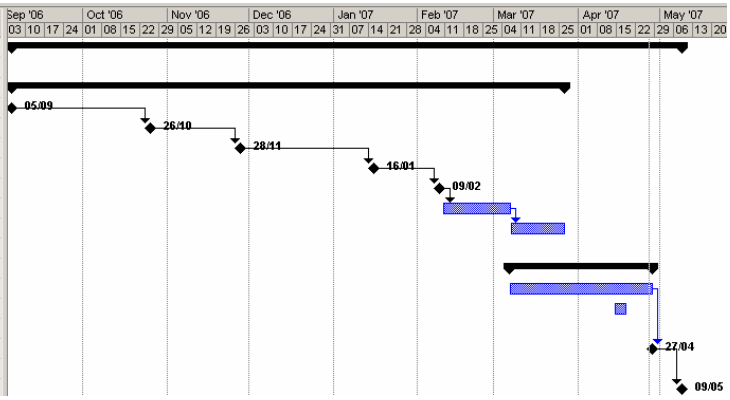
[7] RSA Envision : *http://www.rsa.com/node.aspx?id=3170*

[8] Greg Shipley. Review: Security Information Management Tools, *http://www.networkcomputing.com/showArticle.jhtml?articleID=187203569*, May 22, 2006

[9] Greg Shipley. Market Analysis: Security Information Management, *http://www.networkcomputing.com/channels/security/showArticle.jhtml?&articleID=187203568&pgno=5*, May 22, 2006

Final research schedule

Task Name	Duration	Start	Finish
Thesis schedule	**206,86 days**	**Tue 05/09/06**	**Wed 09/05/07**
Topic building	**168 days**	**Tue 05/09/06**	**Mon 26/03/07**
Starting thesis	0 days	Tue 05/09/06	Tue 05/09/06
Presentation 1	0 days	Thu 26/10/06	Thu 26/10/06
Presentation 2	0 days	Tue 28/11/06	Tue 28/11/06
Presentation 3	0 days	Tue 16/01/07	Tue 16/01/07
Presentation 4 and thesis outline approved	0 days	Fri 09/02/07	Fri 09/02/07
writing proposal	21,71 days	Sat 10/02/07	Tue 06/03/07
proposal review	16 days	Wed 07/03/07	Mon 26/03/07
Paper building	**46,86 days**	**Tue 06/03/07**	**Fri 27/04/07**
writing paper	46,86 days	Tue 06/03/07	Fri 27/04/07
testing and experimenting on OSSIM	5 days	Sat 14/04/07	Wed 18/04/07
submit paper	0 days	Fri 27/04/07	Fri 27/04/07
paper presentation	0 days	Wed 09/05/07	Wed 09/05/07



ISSM Research Proposal

Emmanuel Chol **6th March 2007**

2007 - Master of Information System Security Management, Concordia University College of Alberta (Canada) pending on Thesis completion.
2006 - Engineer Degree (equivalent to Master Degree) in Information Technology and Network, Ecole Centrale d'Electonique E.C.E Paris (France)
2001 - French Scientific Baccalaureate (math major) (equivalent to A Level)

ISSM Research Proposal

Study of the Enterprise Security Manager / Security Incident Manager (ESM / SIM) commercial and open source solutions

Research statement: a study of the specifications of ESM / SIM solutions that will lead to provide some improvement suggestions.

Proposed research advisors:

Primary: Dr. Pavol Zavarsky Director of Research & Associate Professor

Faculty of Professional Education
Gold Bar Campus

Office: GB.E
Phone: (780) 413-7810
Fax: (780) 466-9394
E-mail: pavol.zavarsky@concordia.ab.ca

Secondary: Dr. Andy Igonor Visiting Assistant Professor - Management Sciences

Faculty of Professional Education
Highlands Campus

Office: GB-9A
Phone: (780) 378-8465
Fax: (780) 466-9394
E-mail: andy.igonor@concordia.ab.ca

Abstract: This study will provide an accurate picture of the ESM / SIM current functions. It will describe inputs, processing and outputs of such solution. The study will cover features and models from about ten commercial and open source solutions. The aim is to provide to information systems security professionals, managers, developers of the ESM/SIM solutions, or even students in information systems security, information on available ESM/SIM solutions in order to choose, improve or discover such solutions.

Outline:

Introduction
Description of the ESM / SIM solutions, definition, history and uses.

1) Logs files and flow transport to the SIM
    a) Agent
    b) Agentless
    c) Flow (protocols and bandwidth use)
    d) Security processes

2) Logs storage
    a) Commercial database
    b) Proprietary database
    c) Performance
    d) Normalization

3) Alerts classification
    a) By level of risk
    b) By device
    c) By network

4) Interface and analyse functions
    a) Java console
    b) HTML console
    c) Graphical summaries with clickable elements
    d) Searching tools to dig into logs and/or databases
    e) Searching tool through a knowledge database about attacks and their historic

5) Compatibility
    a) Log formats
    b) Number of devices
    c) Devices' flows (switch, firewall etc.)

6) Auto detection and analysis of the log sources sent to the SIM
    a) Operating Systems
    b) Software
    c) Devices

7) Correlation
    a) Real time
    b) Delayed
    c) Both real time and delayed
    d) Process from memory
    e) Process from a database
    f) Write correlation rules
    g) Update of the common correlation rules
    h) Multiple-event correlation
    i) Linear / non linear correlation

8) Available information and actions following an alert
    a) Alerts send to a console, by email, by SMS, etc.
    b) Automatic action to stop the abnormal event
    c) Suggest some actions to stop the abnormal event

Conclusion

Improvement suggestions

Ex: self learning, new events detection, compatibility, user interface, auto resolution of events, etc.

Disciplinary context: Companies need to comply with regulations like the Sarbanes Oxley Act due to law or business requirements. The SIM / ESM solutions provide critical information on security health of an information system.

Methodology: The study will be based on brochures, demos, datasheets and manuals describing the ESM / SIM solutions. Each section of the outline will describe a panel of methods available. The Open Source Security Information Management (OSSIM) solution will be used to see an ESM / SIM in action. Some correlation rules and console outputs will be shown as appendixes. It will provide an insight on the logs management, the data correlation and alerts management.

Review of the existing research: According to the Forester SIM survey [12] there is a strong companies' interest on ESM / ISM solutions, 30% planned to implement such a solution in 2006. The top reason for implementing SIM solutions was to quickly detect and be alerted to attacks on their infrastructure. In addition the ESM / SIM solutions are based on log correlation that produce far better results compare to a separate analysis on logs. The "Log correlation for intrusion detection : A Proof of Concept paper" [16] showed that correlation could increase abnormally detection up to 35%. The paper "An Incident Response Support System" [15] develops the idea of providing a one click solution to solve a detected alert which could be a new function that SIM could provide. The market, technologies and functionalities evolution led me to explore the ESM / SIM area.

Contribution to knowledge: This paper will provide a big picture of the ESM / SIM development status. Each features description will provide information that will help to choose which solution to implement for regulation enforcement and security needs. Some improvement suggestions will provide a starting point to increase the ESM / SIM capabilities.

Preliminary bibliography:

The ESM / SIM products' websites:

[1] ArcSight ESM: http://www.arcsight.com/index.htm
[2] RSA Envision : http://www.rsa.com/node.aspx?id=3170
[3] High Tower Software Security Event Manager: http://www.high-tower.com/
[4] Q1 Labs QRadar: http://www.q1labs.com/
[5] Symantec Security Information Manager 9500: http://www.symantec.com/enterprise/products/overview.jsp?pcid=1004&pvid=929_1
[6] LogLogic ST 3000 and LX 2000: http://www.loglogic.com/products/st/specifications/
[7] OpenService Security Threat Manager 3.5: http://www.openservice.com/products/smc.php

[8] Trigeo SIM: http://www.trigeo.com/products/
[9] eIQnetworks Enterprise Security Analyzer: http://www.eiqnetworks.com/products/EnterpriseSecurityAnalyzer.shtml
[10] Open Source Security Information Manager: http://ossim.net/

Articles about ESM / SIM:

[11] Review: Security Information Management Tools June 2, 2006: http://www.darkreading.com/document.asp?doc_id=96188&page_number=1
[12] Market Analysis: Security Information Management May 22, 2006 - By Greg Shipley: http://www.networkcomputing.com/channels/security/showArticle.jhtml?queryText=&articleID=187203568&pgno=5
[13] Symantec ESM comprises all required enterprise compliance components By Mandy Andress, Network World, August 8, 2006: http://www.networkworld.com/reviews/2006/061206-compliance-test-symantec.html?prl
[14] Security information management products help you make sense of all your threat data by David Essex, April 17, 2006, http://www.gcn.com/print/25_8/40391-1.html

Research papers:

[16] An Incident Response Support System: Gianluca Capuzzi, Egidio Cardinale, Ivan Di Pietro and Luca Spalazzi Università Politecnica delle Marche, Via Brecce Bianche, 1, Ancona, 60131, Italy; IJCSNS International Journal of Computer Science and Network Security, VOL.6 No.10, October 2006

[17] Log Correlation for Intrusion Detection: A Proof of Concept: Cristina Abadyz, Jed Taylory, Cigdem Senguly, William Yurcikz, Yuanyuan Zhouy and Ken Rowex; Department of Computer Science, University of Illinois at Urbana-Champaign, National Center for Supercomputing Applications (NCSA) and Science Applications International Corporation (SAIC), 2003

[18] The "ART" of log correlation: Dario Forte, CISM, CFE, instructor in Informatics Incidents Handling at the University of Milan.

Research Schedule:

Task Name	Duration	Start	Finish
Thesis schedule	**186,29 days?**	**Tue 05/09/06**	**Mon 16/04/07**
Topic building	**150,86 days?**	**Tue 05/09/06**	**Mon 05/03/07**
Starting thesis	0 days	Tue 05/09/06	Tue 05/09/06
Presentation 1	0 days	Thu 26/10/06	Thu 26/10/06
Presentation 2	0 days	Tue 28/11/06	Tue 28/11/06
Presentation 3	0 days	Tue 16/01/07	Tue 16/01/07
Presentation 4 and thesis outline approved	0 days	Fri 09/02/07	Fri 09/02/07
writing proposal	13,71 days?	Sat 10/02/07	Sat 24/02/07
proposal review	6,86 days?	Mon 26/02/07	Mon 05/03/07
Paper building	**21,71 days?**	**Wed 07/03/07**	**Sun 01/04/07**
writing paper	21,71 days?	Wed 07/03/07	Sun 01/04/07
testing and experimenting on OSSIM	5 days?	Thu 08/03/07	Wed 14/03/07
submit paper	0 days?	Mon 02/04/07	Mon 02/04/07
paper presentation	0 days?	Mon 16/04/07	Mon 16/04/07