OSSIM
a Careful, Free and Always Available Guardian for Your Network

Monitor your network's security 24/7 with a free and open-source solution that collects, analyzes and reports logs of the events on your network.

MARCO ALAMANNI

Networks and information systems are increasingly exposed to attacks that are becoming more sophisticated and sustained over time, such as the so-called APT (Advanced Persistent Threats).

Information security experts agree on the fact that no organization, even the best equipped to protect itself from these attacks, can be considered immune, and that the issue is not whether its systems will be compromised, but rather when and how it will happen.

It is essential to be able to detect attacks in a timely manner and implement the relative countermeasures, following appropriate procedures to respond to incidents, thus minimizing the effects and the damages they can cause. In order to detect intrusions and attacks, system administrators and information security analysts make use of tools, such as IDS/IPS (Intrusion Detection/Prevention System) and analysis of logs (event records) of servers and network devices, looking for any significant events from a security point of view.

A network of an organization of average size produces, as a whole, such a quantity of logs that it is very difficult (and still very expensive) to check them all, one by one, to obtain meaningful information.

A further difficulty is that there is no single standard used to record the logs and often, depending on the type and size, they are not immediate or easy to understand.

It is even more difficult to relate other logs produced by many different systems to each other manually, to highlight anomalies in the network that would not be detectable by analyzing the logs of each machine separately.

SIEM (Security Information and Event Management) software, therefore, is not limited to being a centralized solution for log management, but also (and especially) it has the ability to standardize logs in a single format, analyze the recorded events, highlight the most important information and relate the logs to each other (correlation), allowing analysts to detect anomalies and attacks more easily.

For example, for log management software, three failed attempts to log in to the same user account from three different clients will be only three lines in your log file and not obviously related to each other. For an analyst, instead, it may be a sequence of events worthy of further analysis, and its correlation (looking for patterns in the log files) can generate alerts when these types of events occur.

Overview of a SIEM Open-Source Solution: OSSIM

OSSIM is a SIEM software platform, free and open-source, developed by AlienVault and based on a Debian 64-bit Linux distribution. OSSIM has four major components:

1. Sensor.

2. Server.

3. Framework.

4. Database.

You can install these components on a single physical machine (the default installation), on a single virtual machine, on different virtual machines and/or physical machines, depending on the size and configuration of the network to monitor.

For a relatively small network, installation on a single machine, which is the simplest configuration, may be the right solution. For larger networks, it is advisable to install the Sensor and the Database separately. Figure 1 shows the OSSIM architecture.

Sensor: The Sensor has two main components:

1. The rsyslog service, which listens

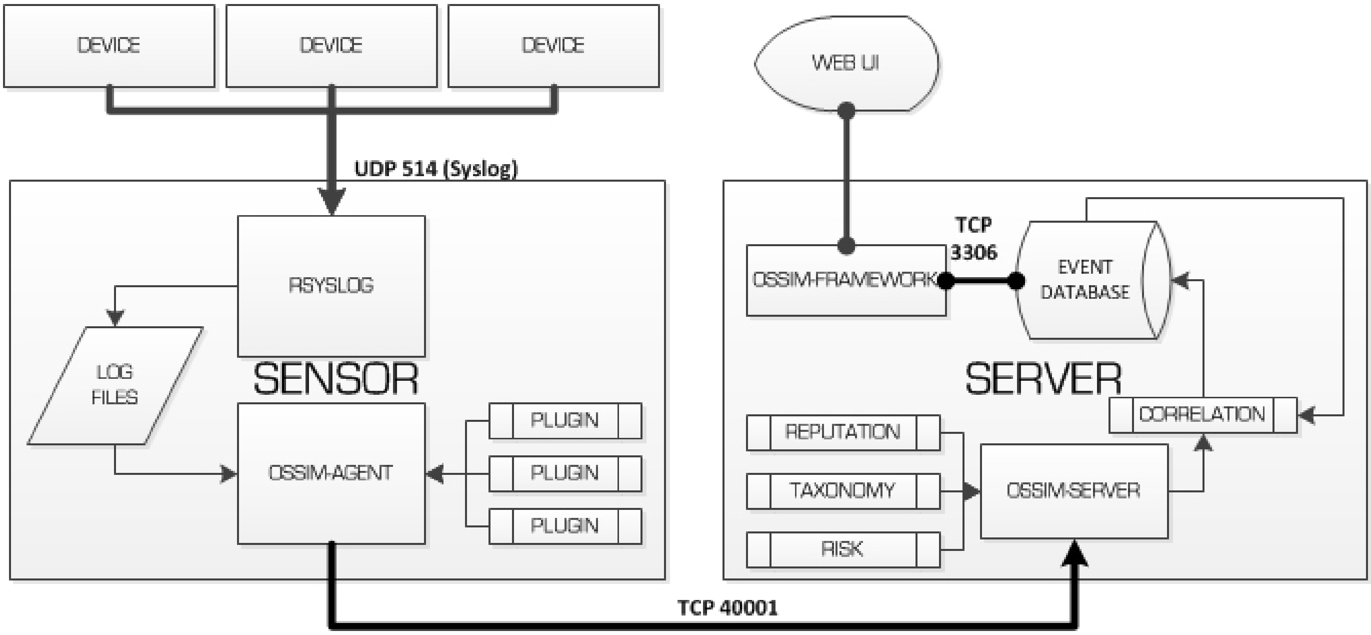


Figure 1. OSSIM Architecture

on TCP/UDP port 514, receives the logs from network devices and stores them locally, according to the configuration.

2. The Ossim-agent, using a series of modules called plugins, one for each type of log, performs log analysis and normalization, and sends that to the Server component.

Plugins are of two types: detectors, which detect anomalies and possible attacks (such as Snort, P0f, Arpwatch), and monitors to monitor the network status (like Ntop and Nagios).

Server: The Server performs the essential SIEM functions: aggregation, risk assessment and correlation of events that are received from the sensor through TCP port 40001. The server also sends the information concerning the events to the Database for storage.

Framework: The Framework connects and manages the OSSIM components and security tools included, and it provides the system administration Web interface. It is the component that needs the least hardware resources and is usually installed together with the Server component.

Database: The Database is a MySQL server instance that stores events and system configuration data.

Functionalities

Following is a brief description of OSSIM's main features and functionalities concerning the collection, analysis and correlation of logs and the primary tools included in the system for network security monitoring.

Collection and Normalization of Logs: You can collect logs from the devices on your network in two ways:

1. Install a software agent (like Snare or SysLogAgent) in the source machine and configure it to read certain types of logs and send them to the Sensor component.

2. Configure the source machine to send the logs upon request of the appropriate Sensor plugins (for example, via WMI for Windows machines). Once the Sensor records the logs, the OSSIM Agent performs the analysis and converts them to a single format (normalization). Each log represents an event that will be sent to the server for analysis (Figure 2).

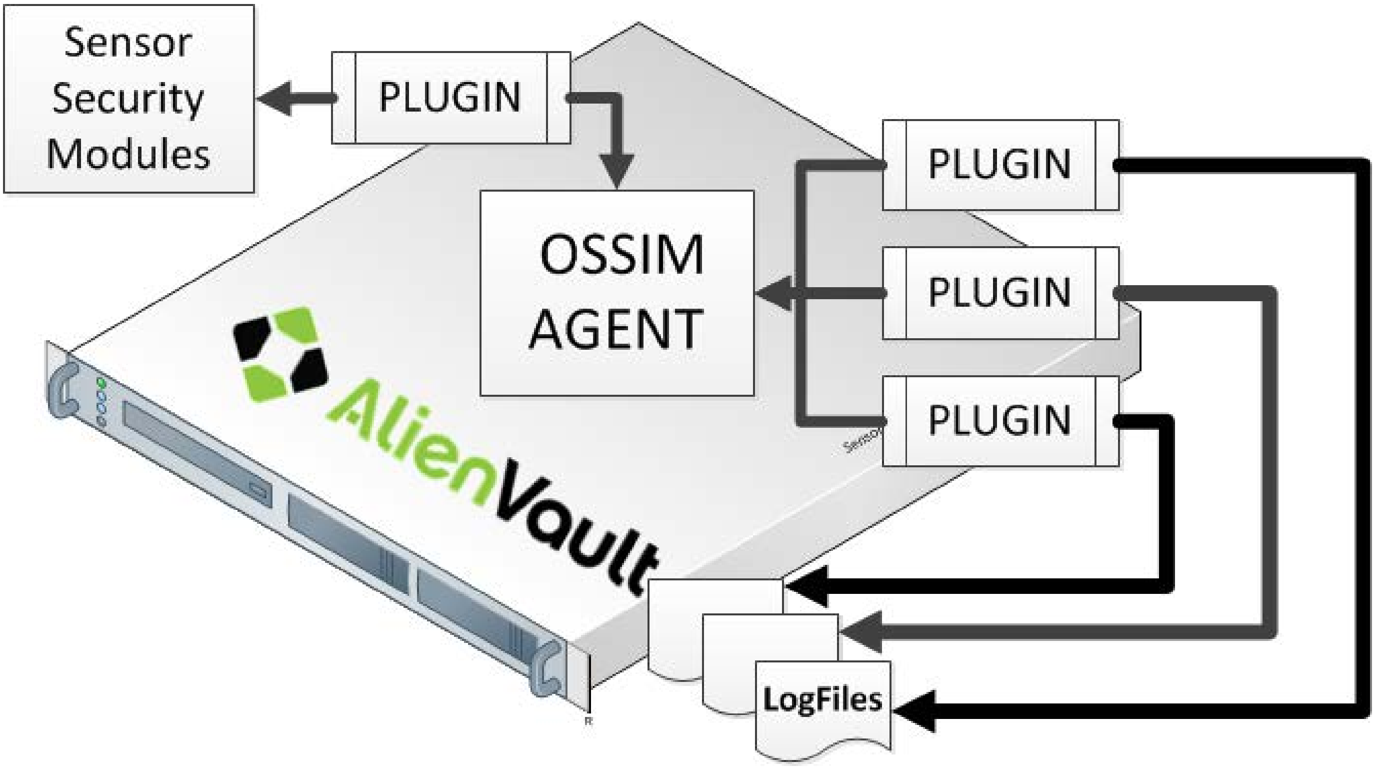


Figure 2. Log Collection and Normalization

Prioritization of Events and Risk Assessment: The prioritization process involves assigning priority values to the recorded events, which is done by the Server component. It depends on the structure of the network and it needs, as prerequisites, the definition of security policies and the inventory of information assets on the network, which can be managed in the Web administration panel. It sets the priority of an event based on the machine that generated it and the type of event to which it belongs.

The risk assessment of events is calculated in real time and is based on three main factors:

1. The value or level of importance of the machine that generated the event.

2. The type of threat posed by the event.

3. The probability that this event occurs.

The formula used for calculating risk is the following (Figure 3): Risk = value * (reliability * Priority / 25).

Analysis and Correlation of Events: The correlation of events essentially relates events to each other

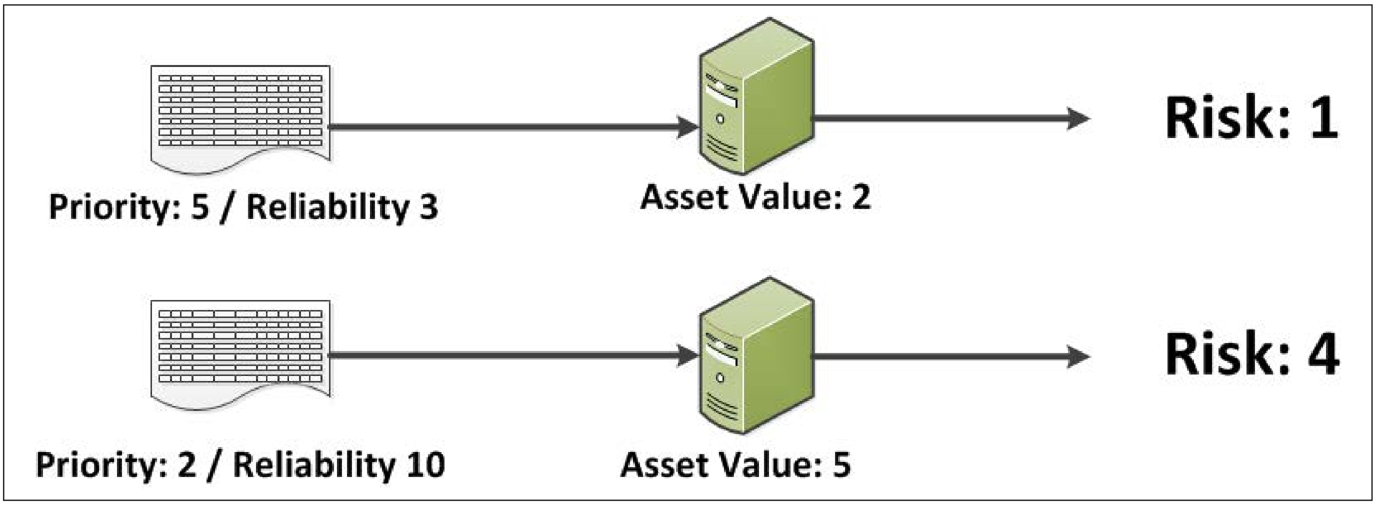


Figure 3. How to Calculate the Risk Associated with an Event

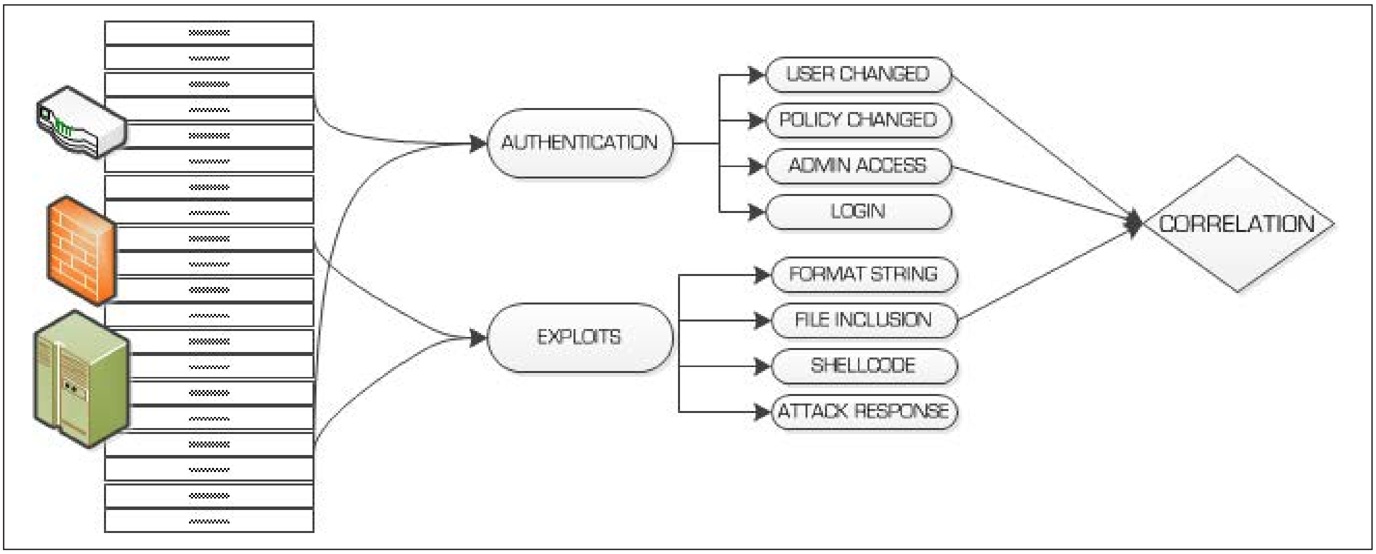


Figure 4. Example of Analysis and Correlation of Events

to achieve a comprehensive view of network security and to detect possible attacks or anomalies.

The correlation process is performed via two methods:

1. Correlation using sequence of events, using directives, consisting of rules that relate events to patterns of known attacks. This method is similar to using Snort for intrusion detection (signature-based detection).

2. Correlation using heuristic

algorithms can be detected by these abnormal situations that do not detect the preceding rules and may or may not be attacks (abnormality detection).

Directives are located in the /etc/ossim/server/directives.xml file. Directives are specified in XML using tags like Id, Name, Priority, Type, Reliability, Occurrence, Timeout, Source, Destination, Source port, destination port, protocol, PluginSid and Sensor.

Reliability is a measure of the probability that the considered event truly represents the attack referred to by the directive and is generally based on the number of occurrences of the event.

For example, consider the following directive to detect brute-force SSH attacks:

```
<directive id="20" name="Possible SSH brute force login
 ➥attempt against DST_IP" priority="5">
<rule type="detector" name="SSH Authentication failure"
 ➥reliability="3" occurrence="1" from="ANY" to="ANY"
 ➥port_from="ANY" port_to="ANY" time_out="10"
 ➥plugin_id="4003" plugin_sid="1,2,3,4,5,6">
<rules>
<rule type="detector" name="SSH Authentication failure (3 times)"
 ➥reliability="+1" occurrence="3" from="1:SRC_IP" to="ANY"
 ➥port_from="ANY" time_out="15" port_to="ANY"
 ➥plugin_id="4003" plugin_sid="1,2,3,4,5,6" sticky="true">
<rules>
<rule type="detector" name="SSH Authentication failure (5 times)"
 ➥reliability="+2" occurrence="5" from="1:SRC_IP" to="ANY"
 ➥port_from="ANY" time_out="20" port_to="ANY"
 ➥plugin_id="4003" plugin_sid="1,2,3,4,5,6" sticky="true">
<rules>
<rule type="detector" name="SSH Authentication failure (10 times)"
 ➥reliability="+2" occurrence="10" from="1:SRC_IP" to="ANY"
 ➥port_from="ANY" time_out="30" port_to="ANY"
 ➥plugin_id="4003" plugin_sid="1,2,3,4,5,6" sticky="true">
</rule>
</rules>
</rule>
</rules>
</rule>
</rules>
</rule>
</directive>
```

The directive assigns a value of reliability equal to 3 (30% probability) when the number of occurrences of the event detected by the sensor (SSH authentication error) is equal to 1, then increments it by 1 at the third occurrence of the event, by 2 at the fifth occurrence and by an additional 2 at the tenth, thereby achieving a reliability of 8 (80% of probability) when the incorrect authentication attempts are 10.

OSSIM also has the ability to correlate different types of logs, generated by various plugins (cross-correlation). The cross-correlation allows you to change the event reliability and risk assessment. For example, suppose that Nessus or OpenVAS has identified a vulnerability in a server. If Snort detects an event that indicates a possible attack on that server, the correlation engine increases the level of risk associated with the event.

Generation of Alarms and Response Actions: The directives can create alarms, which either are generated by a single event or by a specific sequence of events under certain conditions. The alarms can be displayed in the Web administration panel, under the menu item Incidents→Alarms.

Furthermore, alarms can activate response actions, such as sending an alert by e-mail to the system administrator and/or the execution of appropriate scripts.

Vulnerability Analysis, Intrusion Detection and Network Monitoring: OSSIM includes many valuable tools, which also are open-source, that are among the most known and used for intrusion detection, vulnerability analysis and network management and monitoring:

- Arpwatch: used for monitoring ARP traffic on the LAN and for related attack detection.

- P0f: used for operating system identification and analysis.

- Pads: used for detecting anomalies of the services running on a host.

- Nessus and OpenVAS: the most widely used and popular vulnerability scanners.

- Nmap: the most famous and powerful network scanner.

- Snort: the most popular intrusion detection system (IDS).

- Tcptrack: used for TCP connection monitoring.

- Nagios and Ntop: used to monitor the status of the network, the hosts and the availability of services.

- Osiris and OSSEC: intrusion detection software for individual hosts (HIDS—Host-Based IDS).

- Snare: a software agent for collecting logs on Windows systems.

Installation and Hardware Requirements

You can download the ISO file for the installation from the

AlienVault Web site download page at **http://www.alienvault.com/free-downloads-services**.

The most recent version (February 2014) is 4.3.4, only for 64-bit architectures. You can choose the Automatic or Custom installation. The automatic installation is fairly simple, in graphical mode by default, and it installs all components of OSSIM on the same machine. The custom installation allows you to select the mode (graphical or textual) and which components to install. The custom installation is a little more complex because it has more configuration options. For instructions on how to install OSSIM, refer to the Installation Guide: **https://alienvault.bloomfire.com/posts/525575-installation-guide/public**.

The minimum hardware requirements are:

- 64-bit processor or virtualization software with support for 64-bit operating systems (at least a quad-core processor is recommended).
- 4GB of RAM.
- 500GB of free disk space.
- Network adapter with support for the Intel e1000 Ethernet driver.

Of course, the hardware requirements will be directly proportional to the size of the network (number of hosts and network devices connected) and consequently to the amount of logs produced and recorded.

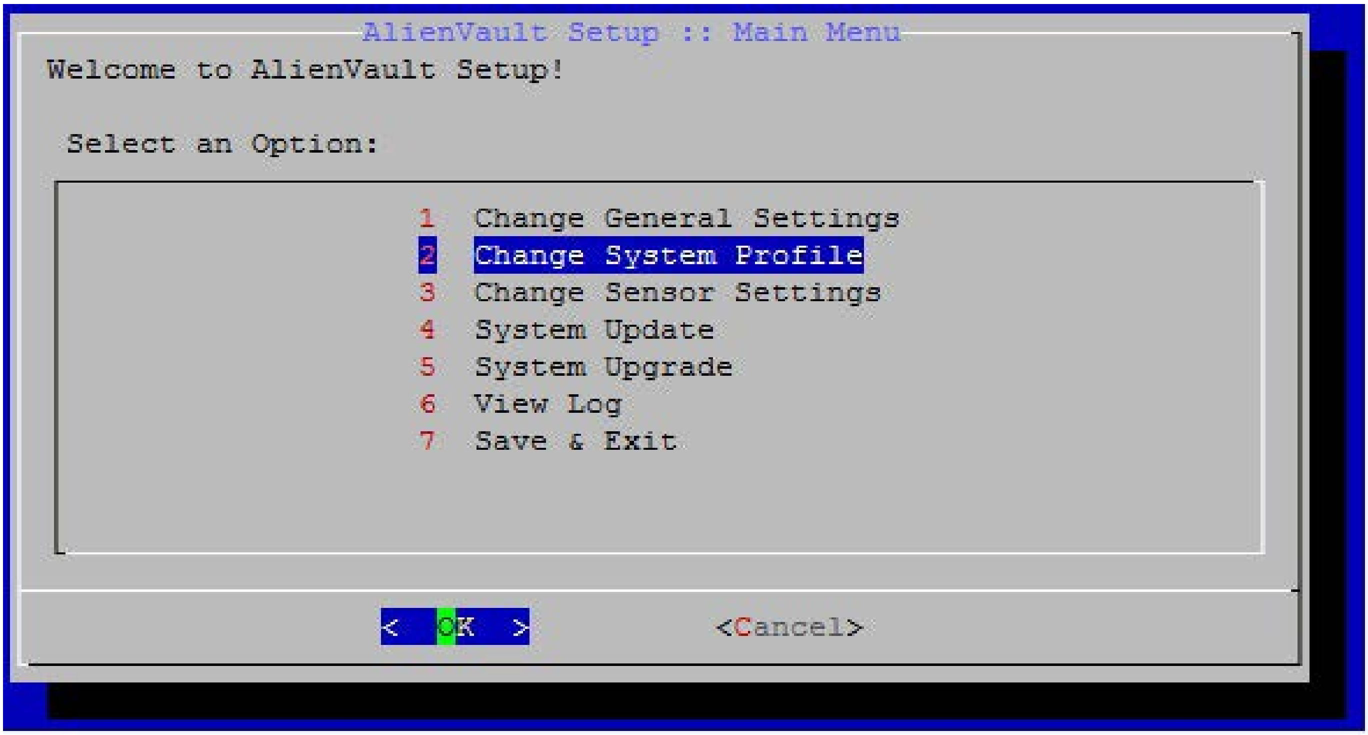
Configuration and Management

You can perform the system configuration and administration through the console, a Linux shell or through a more convenient and intuitive Web interface.

Configuration through the Console: To configure the system through the console, you need to log in as root with the password you set during the installation process. The directory that contains the system's configuration files is /etc/ossim.

The main configuration file is /etc/ossim/ossim_setup.conf, which contains the system's main settings, such as IP addresses and ports of the hosts on which components are installed, the active plugins and the password used by the root user of MySQL, randomly generated by the system during the installation procedure.

For example, if you want to



```
AlienVault Setup :: Main Menu
Welcome to AlienVault Setup!

 Select an Option:

              1  Change General Settings
              2  Change System Profile
              3  Change Sensor Settings
              4  System Update
              5  System Upgrade
              6  View Log
              7  Save & Exit

         <  OK  >          <Cancel>
```

Figure 5. Configuration with the ossim_setup Tool

change your password or other data, you need to edit the file with the command:

```
# vi /etc/ossim/ossim_setup.conf
```

Then run the following command:

```
# ossim-reconfig
```

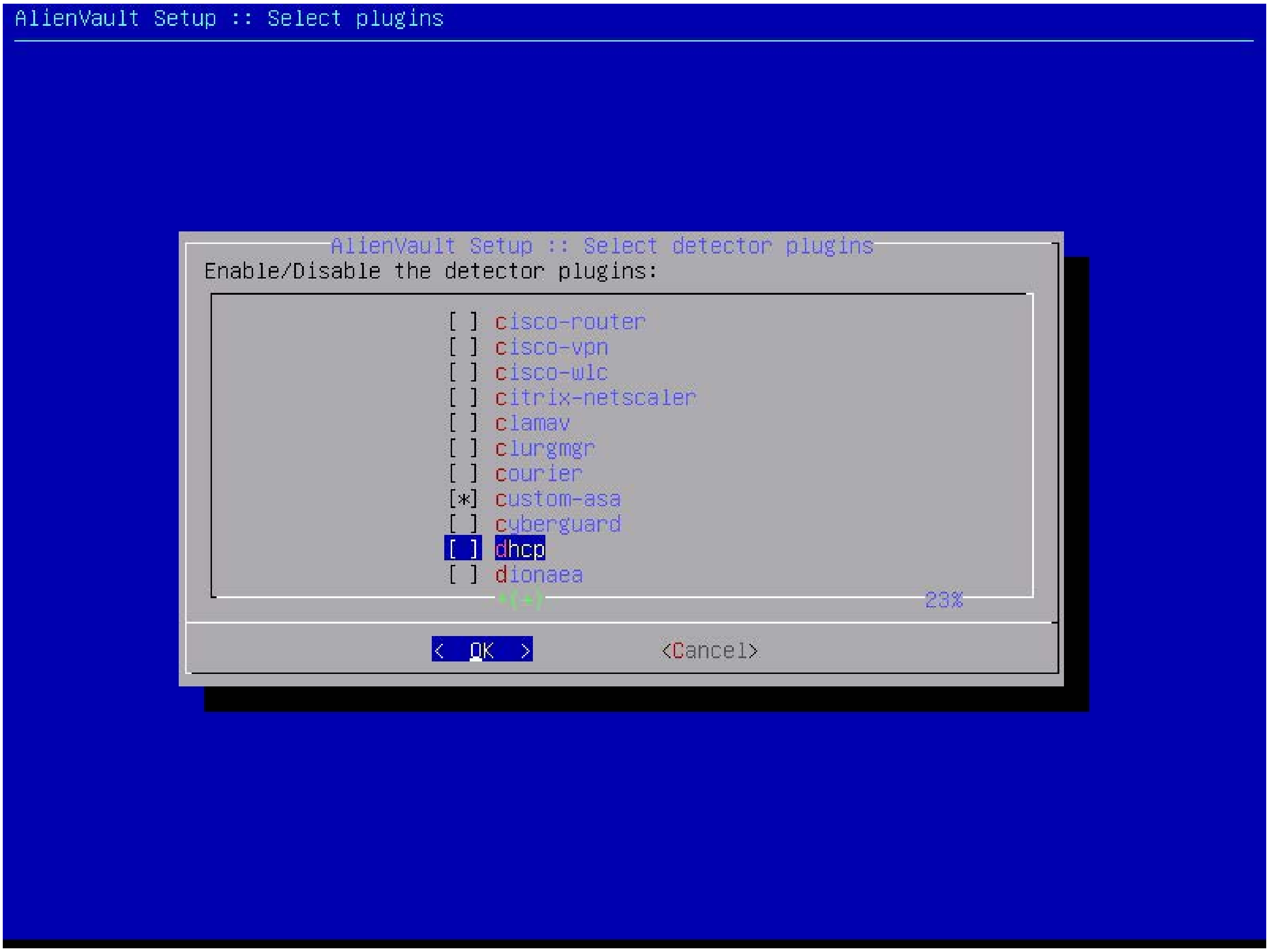
To change the main configuration file more easily, there is also a command called `ossim_setup`, which presents a graphical interface, shown in Figure 5.

Configuring the Sensor and Plugins: With the `ossim_setup` command, you can set the parameters of the previously shown configuration file, such as enabling or disabling plugins. To get a list of plugins that can be turned on or off, select the option Change sensor settings→Select detector plugins (Figure 6).

The OSSIM agent runs as a background service (dæmon), and you can start it with this command:

```
#  /etc/init.d/ossim-agent start
```

Its configuration file is /etc/ossim/agent/config.cfg. The plugins' configuration files also are text files with the .cfg extension and are in the /etc/ossim/agent/plugins/ directory.



```
AlienVault Setup :: Select plugins

          AlienVault Setup :: Select detector plugins
  Enable/Disable the detector plugins:

                    [ ] cisco-router
                    [ ] cisco-vpn
                    [ ] cisco-wlc
                    [ ] citrix-netscaler
                    [ ] clamav
                    [ ] clurgmgr
                    [ ] courier
                    [*] custom-asa
                    [ ] cyberguard
                    [ ] dhcp
                    [ ] dionaea
                        ↓(+)                      23%

                  <  OK  >          <Cancel>
```

Figure 6. List of Plugins in ossim_setup

When you activate new plugins, you must restart the server:

```
#  /etc/init.d/ossim-server restart
```

More than 2,000 plugins are available (**http://www.alienvault.com/docs/AlienVault%20Plugin%20List%20-%20Jun-20-2010.pdf**), which you can download and install via the Plugin Wizard. For example, run the following commands:

```
# cd /usr/share/ossim/scripts ;
# plugin_wizard.pl -s "oracle"
```

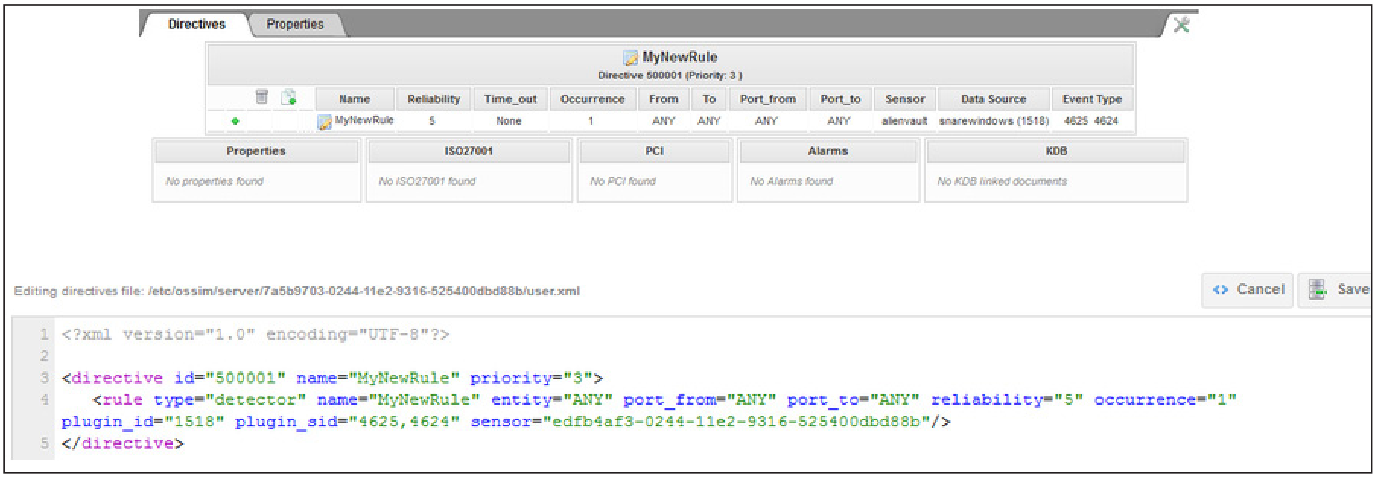
and you will get the plugins that contain the word "Oracle" in the name.

With the command:

```
#  ./plugin_wizard.pl -g -s "oracle"
```

these plugins will be extracted to a directory called win_plugins.

Next, you have to move them



MyNewRule
Directive 500001 (Priority: 3)

Name	Reliability	Time_out	Occurrence	From	To	Port_from	Port_to	Sensor	Data Source	Event Type
MyNewRule	5	None	1	ANY	ANY	ANY	ANY	alienvault	snarewindows (1518)	4625 4624

Properties	ISO27001	PCI	Alarms	KDB
No properties found	No ISO27001 found	No PCI found	No Alarms found	No KDB linked documents

Editing directives file: /etc/ossim/server/7a5b9703-0244-11e2-9316-525400dbd88b/user.xml

```
<?xml version="1.0" encoding="UTF-8"?>

<directive id="500001" name="MyNewRule" priority="3">
   <rule type="detector" name="MyNewRule" entity="ANY" port_from="ANY" port_to="ANY" reliability="5" occurrence="1"
plugin_id="1518" plugin_sid="4625,4624" sensor="edfb4af3-0244-11e2-9316-525400dbd88b"/>
</directive>
```

Figure 7. New Directives Specified in the user.xml File

to the default directory /etc/ossim/agent/plugins/:

```
#  mv win_plugins/*.cfg  /etc/ossim/agent/plugins/
```

Files with the .sql extension must be added to the MySQL database with the following command:

```
# ossim-db < ./win_plugins/*.sql
```

If the database server is not installed on the same machine, you need to copy the files on the server:

```
# scp win_plugins/*.sql root@<IP Database>:/root/
```

and run the `ossim-db` command from the database server.

Server Configuration: The configuration directory for the Server component is /etc/ossim/server. The main file is directives.xml, which specifies the configuration file directives, grouped by type of attack, such as malware, brute force and so on.

When you create new guidelines, they should be specified in user.xml rather than in the file containing the default directives (Figure 7).

rsyslog's Dæmon Configuration and Log Rotation: The /var/log/ossim directory contains the log files of OSSIM's components. The dæmon that keeps track of the logs is, as already mentioned, rsyslog, whose configuration file is /etc/rsyslog.conf.

During the installation process, you configure rsyslog to accept logs from remote machines and store them in different log files, depending on the type and the host that created them.

To achieve this, rsyslog uses filters

based on expressions, which are .conf files usually placed in the /etc/rsyslog.d/ directory. For example, to save the logs from a Fortinet firewall in the file /var/log/ossim/fortinet.log, the expression would be:

```
if ($source == '192.168.1.100' and $msg contains 'fortinet ')
➥and $severity <= '6' then /var/log/ossim/fortinet.log
```

Adding new hosts that send the logs to rsyslog, you quickly can run out of disk space. Therefore, it is important to define a policy for log rotation in /etc/logrotate.conf. This involves the regular archiving, at predefined intervals, of the existing log files. After a predefined period, the archived log files are deleted or stored on external devices for backup.

Administration through the Web Interface: OSSIM also can be configured and managed through a nice Web interface, connecting with the browser to the IP address of the machine on which you installed the Server/Framework component (Figure 8).

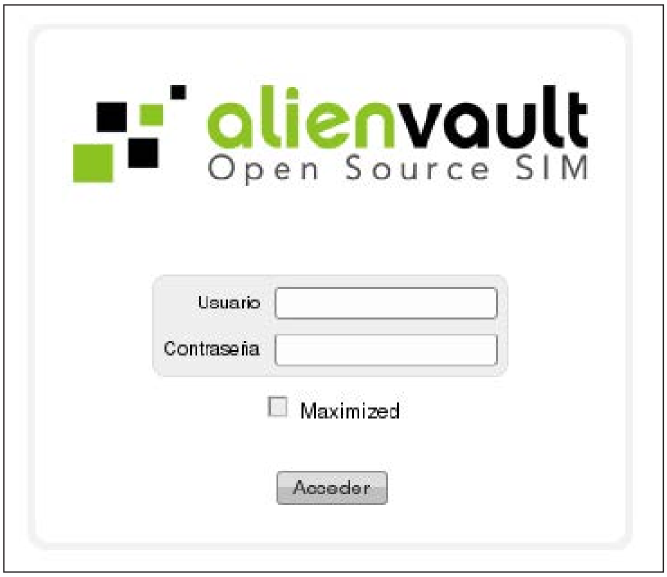


Figure 8. Web Administration Interface Login Screen

The default user and password are admin/admin. When you log in for the first time, you are prompted to change your password.

Through the Web interface, you can perform the following tasks:

- System configuration (users, update, backups and so on).
- Creation and configuration of directives, policies and actions.
- Real-time monitoring of network security.
- Report generation.
- Ticketing system.
- Vulnerability management and incident response.
- Management and optimization of network traffic.

The Web interface includes

several sections:

- Dashboard: provides an overview of detected security events. Displays the visual counters and statistics of the most important security events (Figure 9).

- Incidents: shows the list of security events and generated alarms with specific information, such as date, priority, risk, status and a brief history of the actions taken by system administrators.

- Analysis: shows a table with the latest events detected, the type, date, origin, destination, the OSSIM node that detected it and the risk. From here, the user can search for patterns in the events according to different criteria (for example, the source IP address). This includes a real-time list of

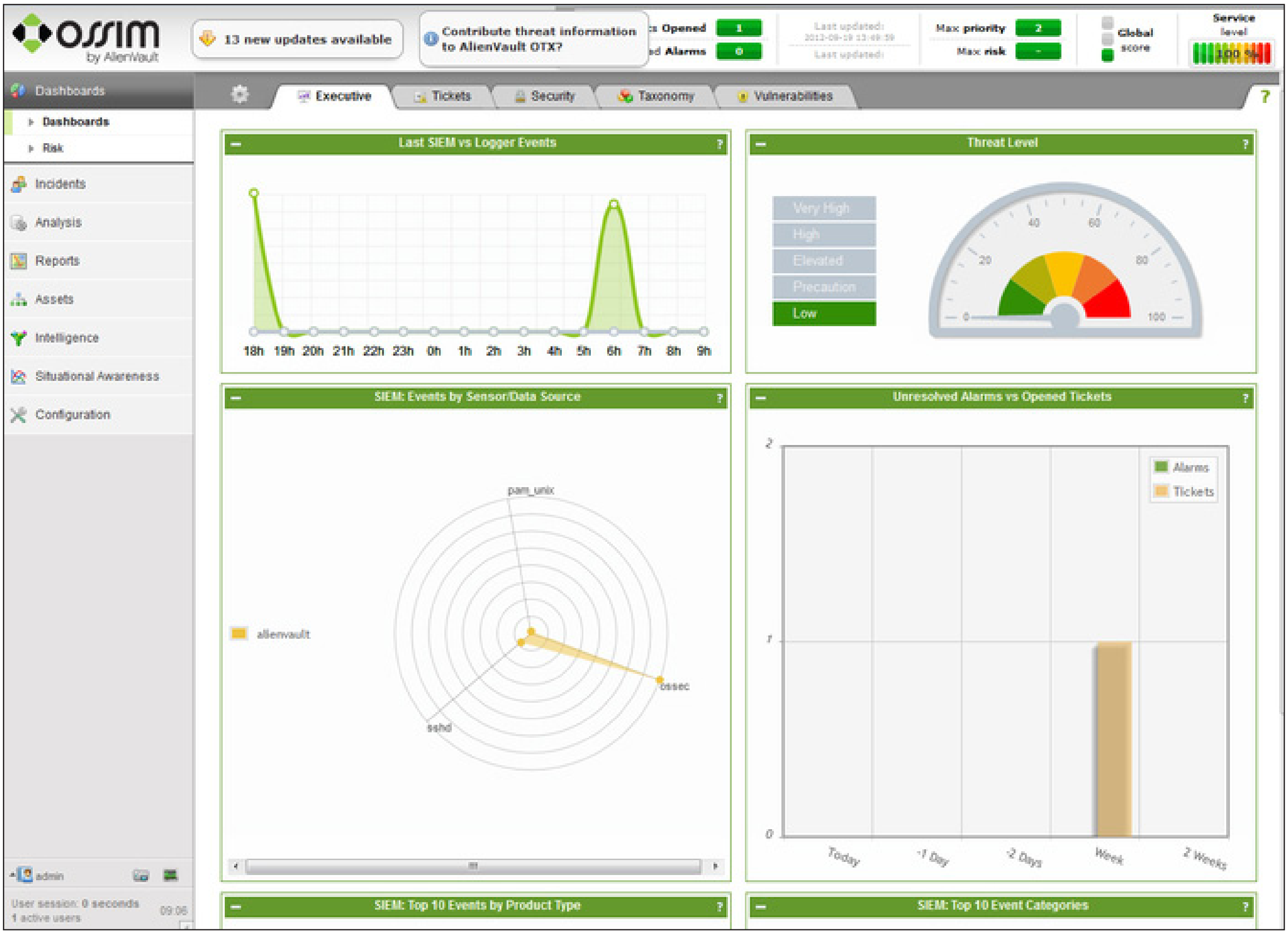
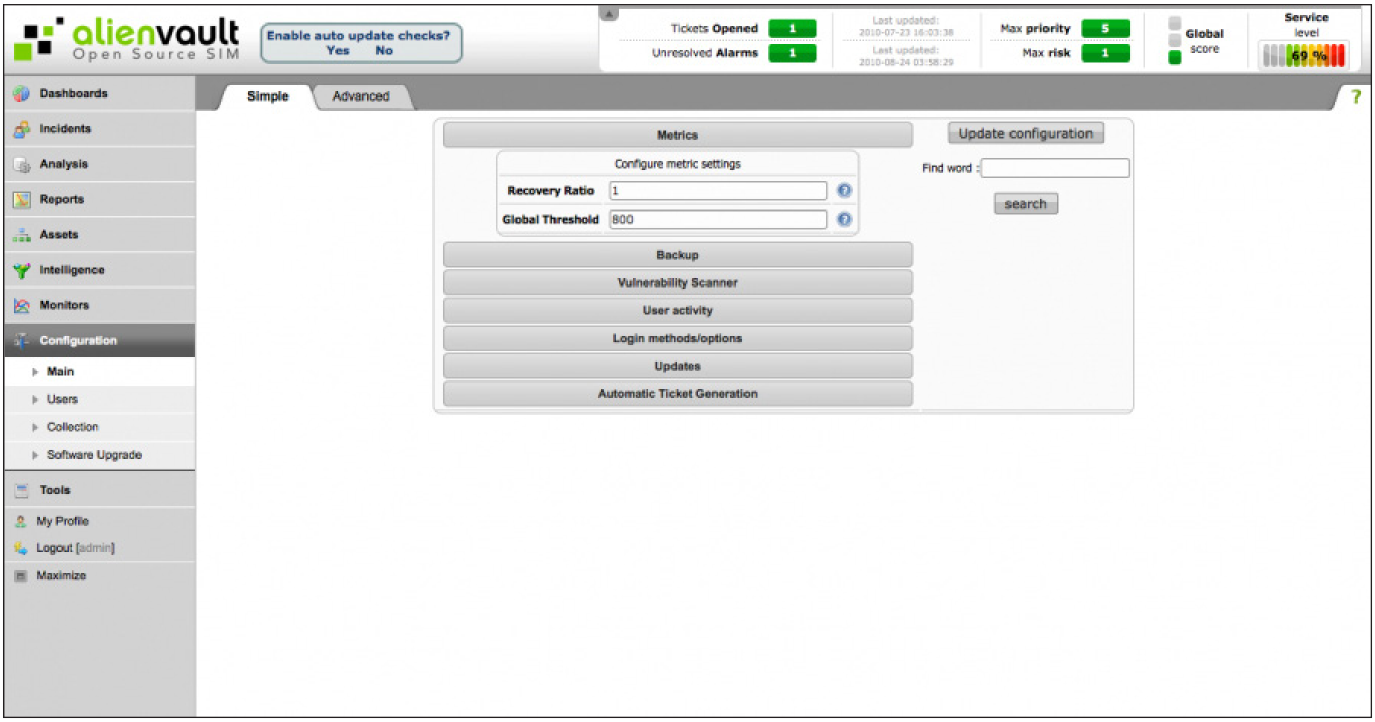


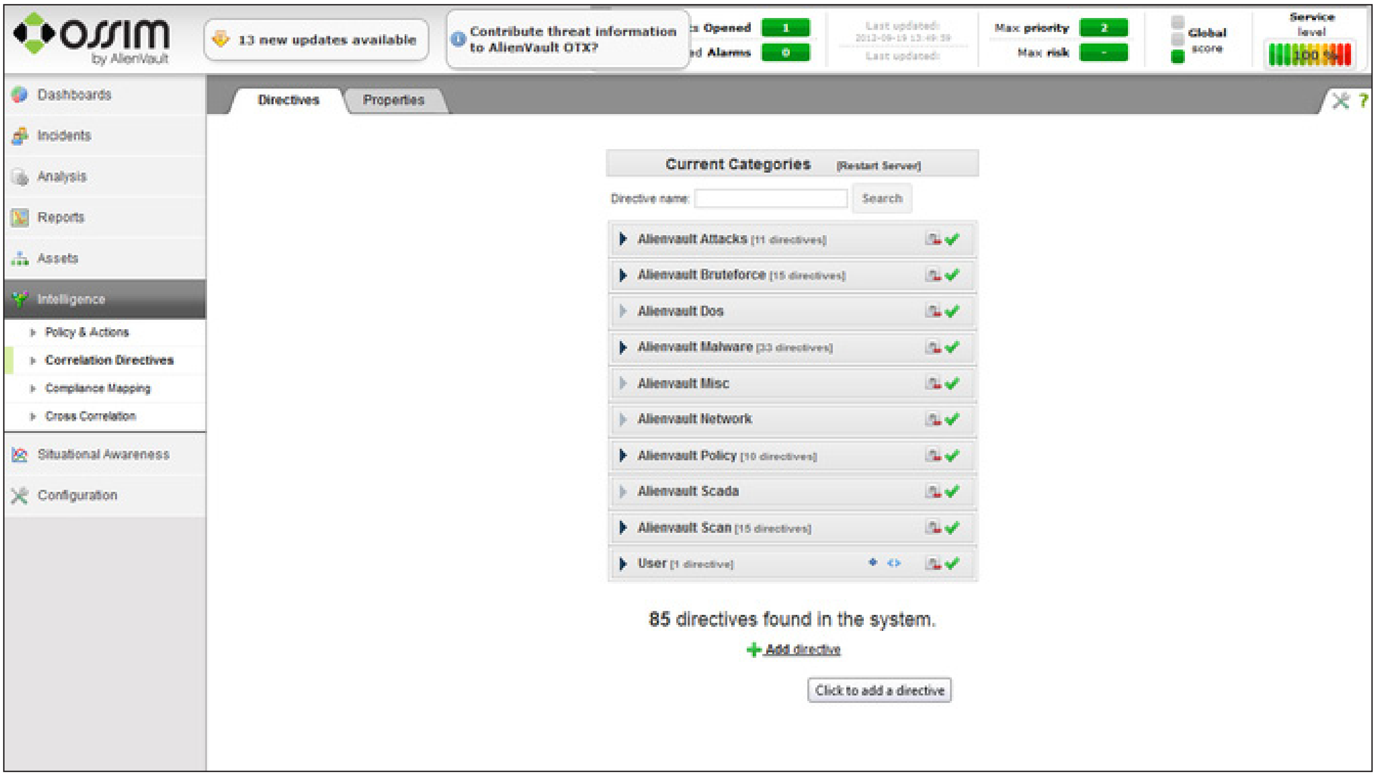
Figure 9. Dashboard with Statistics and Diagrams about Security Events



Recovery Ratio: 1

Global Threshold: 800

Figure 10. This section manages the system logic: definition and management of policies, directives and actions.



85 directives found in the system.

Figure 11. Configuration Panel

detected events that is updated every two seconds.

- Report: allows you to generate reports about security events and network status.

- Activities: this interface allows you to run and manage network inventory, identify and add new machines from which to record the logs.

- Intelligence: this section handles the system logic—definition and management of policies/actions, directives, event correlation and statistics of the network and of the OSSIM nodes.

- Configuration: this section allows you to manage all the system configurations (Figure 10).

Conclusion

OSSIM is a viable open-source SIEM solution and a free alternative to other commercial SIEM products (including AlienVault USM, the commercial version of OSSIM), which are much more expensive, and it is supported by a community of developers and users through forums and documentation available on the AlienVault's Web site.■

Marco Alamanni has professional experience working as a Linux system administrator and information security administrator in banks and financial institutions in Italy and Peru. He holds a BSc in Computer Science and an MSc in Information Security, and his interests in information technology include ethical hacking, digital forensics, malware analysis, Linux and programming. He also collaborates with IT magazines writing articles about Linux and IT security.

Send comments or feedback via http://www.linuxjournal.com/contact or to ljeditor@linuxjournal.com.

Resources

OSSIM Installation Guide: **https://alienvault.bloomfire.com/posts/525575-installation-guide/public**

AlienVault User Manual: **http://www.alienvault.com/wiki/doku.php?id=user_manual:introduction**

The Alienvault Repository of Knowledge: **https://alienvault.bloomfire.com**

AlienVault OSSIM Forum: **http://forums.alienvault.com**

Service Level SIEM—User and Programmer Guide: **http://forge.fi-ware.org/plugins/mediawiki/wiki/fiware/index.php/Security_Monitoring_/Service_Level_SIEM_-_User_and_Programmers_Guide**