TIBCO LogLogic®

Security Event Manager (SEM)

Concepts Guide

Software Release: 3.6.0

March 2013

Two-Second Advantage®

Important Information

SOME TIBCO SOFTWARE EMBEDS OR BUNDLES OTHER TIBCO SOFTWARE. USE OF SUCH EMBEDDED OR BUNDLED TIBCO SOFTWARE IS SOLELY TO ENABLE THE FUNCTIONALITY (OR PROVIDE LIMITED ADD-ON FUNCTIONALITY) OF THE LICENSED TIBCO SOFTWARE. THE EMBEDDED OR BUNDLED SOFTWARE IS NOT LICENSED TO BE USED OR ACCESSED BY ANY OTHER TIBCO SOFTWARE OR FOR ANY OTHER PURPOSE.

USE OF TIBCO SOFTWARE AND THIS DOCUMENT IS SUBJECT TO THE TERMS AND CONDITIONS OF A LICENSE AGREEMENT FOUND IN EITHER A SEPARATELY EXECUTED SOFTWARE LICENSE AGREEMENT, OR, IF THERE IS NO SUCH SEPARATE AGREEMENT, THE CLICKWRAP END USER LICENSE AGREEMENT WHICH IS DISPLAYED DURING DOWNLOAD OR INSTALLATION OF THE SOFTWARE (AND WHICH IS DUPLICATED IN THE LICENSE FILE) OR IF THERE IS NO SUCH SOFTWARE LICENSE AGREEMENT OR CLICKWRAP END USER LICENSE AGREEMENT, THE LICENSE(S) LOCATED IN THE “LICENSE” FILE(S) OF THE SOFTWARE. USE OF THIS DOCUMENT IS SUBJECT TO THOSE TERMS AND CONDITIONS, AND YOUR USE HEREOF SHALL CONSTITUTE ACCEPTANCE OF AND AN AGREEMENT TO BE BOUND BY THE SAME.

THIS SOFTWARE MAY BE AVAILABLE ON MULTIPLE OPERATING SYSTEMS. HOWEVER, NOT ALL OPERATING SYSTEM PLATFORMS FOR A SPECIFIC SOFTWARE VERSION ARE RELEASED AT THE SAME TIME. PLEASE SEE THE README.TXT FILE FOR THE AVAILABILITY OF THIS SOFTWARE VERSION ON A SPECIFIC OPERATING SYSTEM PLATFORM.

THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. THIS DOCUMENT COULD INCLUDE TECHNICAL INACCURACIES OR TYPOGRAPHICAL ERRORS. CHANGES ARE PERIODICALLY ADDED TO THE INFORMATION HEREIN; THESE CHANGES WILL BE INCORPORATED IN NEW EDITIONS OF THIS DOCUMENT. TIBCO SOFTWARE INC. MAY MAKE IMPROVEMENTS AND/OR CHANGES IN THE PRODUCT(S) AND/OR THE PROGRAM(S) DESCRIBED IN THIS DOCUMENT AT ANY TIME.

THE CONTENTS OF THIS DOCUMENT MAY BE MODIFIED AND/OR QUALIFIED, DIRECTLY OR INDIRECTLY, BY OTHER DOCUMENTATION WHICH ACCOMPANIES THIS SOFTWARE, INCLUDING BUT NOT LIMITED TO ANY RELEASE NOTES AND "READ ME" FILES.

Contents

List of Figures

List of Tables

Preface

About This Guide

This guide introduces the main concepts to manage efficiently Security Event Manager.

In this document you will get information about:

- File conversion.
- TIBCO LogLogic® Taxonomy
- Alerts' correlation.
- Effective Security Compliance.
- Log signature and encryption .

Audience

This guide is intended for:

- Security Network Administrators who are responsible for installing and maintaining network security applications and who have a super user status.
- CISO who wants to understand how Security Event Manager responds to regulatory compliance issue.

Related Documentation

Table 1 Related Documentation

Documentation	Content
Administration Guide	This guide explains how to configure the various functions of the Security Event Manager Solution in an advanced manner.
Log Collector Installation Guide	This guide explains how to install and configure the Log Collector on both Windows and Linux/ Unix O.S.
Reference Guide	This guide gives a description of the various modules provided in the Web Console application.
SMP Installation Guide	This guide explains how to install and configure the Security Management Platform.
User Guide	This guide explains how to use and configure the various functions and modules provided in the Web Console application.

Technical Support Information

TIBCO LogLogic® is committed to the success of our customers and to ensuring our products improve customers' ability to maintain secure, reliable networks. Although TIBCO LogLogic® products are easy to use and maintain, occasional assistance might be necessary.

TIBCO LogLogic® provides timely and comprehensive customer support and technical assistance from highly knowledgeable, experienced engineers who can help you maximize the performance of your TIBCO LogLogic® Compliance Suites.

To reach TIBCO LogLogic® Customer Support:

Telephone: Toll Free—1-800-957-LOGS

Local—1-408-834-7480

EMEA— +44 1480 479391

Email: ll-support@tibco.com

You can also visit the **TIBCO LogLogic®** Support website at:
https://support.tibco.com/esupport/loglogic.htm

When contacting the support, be prepared to provide the following information:

- Your name, email address, phone number, and fax number
- Your company name and company address
- Your machine type and release version
- A description of the problem and the content of pertinent error messages (if any)

Documentation Support Information

The TIBCO LogLogic® documentation includes Portable Document Format (PDF) files. To read the PDF documentation, you need a PDF file viewer such as Adobe Acrobat Reader. You can download the Adobe Acrobat Reader at http://www.adobe.com.

Contact Information

Your feedback on the TIBCO LogLogic® documentation is important to us. If you have questions or comments, send email to DocComments@loglogic.com. In your email message, please indicate the software name and version you are using, as well as the title and document release date of your documentation. Your comments will be reviewed and addressed by the TIBCO LogLogic® Technical Publications team.

Conventions

The TIBCO LogLogic® documentation uses the following conventions to distinguish text and information that might require special attention.

Caution: Highlights important situations that could potentially damage data or cause system failure.

IMPORTANT! Highlights key considerations to keep in mind.

Note: Provides additional information that is useful but not always essential or highlights guidelines and helpful hints.

This guide also uses the following typographic conventions to highlight code and command line elements:

- `Monospace` is used for programming elements (such as code fragments, objects, methods, parameters, and HTML tags) and system elements (such as file names, directories, paths, and URLs).
- **`Monospace bold`** is used to distinguish system prompts or screen output from user responses, as in this example:

```
username: system
```

```
home directory: home\app
```

- *`Monospace italic`* is used for placeholders, which are general names that you replace with names specific to your site, as in this example:

```
LogLogic_home_directory\upgrade\
```

- Straight brackets signal options in command line syntax.

```
ls [-AabCcdFfgiLlmnopqRrstux1] [-X attr] [path ...]
```

Chapter 1 - Conversion

This chapter presents information regarding how the Security Event Manager processes log files and how the main converters are implemented.

Implementation of Log Converter

A log converter is used when the source of events to be monitored is a text file or received by Syslog.

Four files are used to format raw logs into an IDMEF format to subsequently transmit them to the Security Management Platform. The four files are:

- The Log file containing the event description.
- a converter file called `exa_productname.conf.xml` which describes an event characteristics.
- a ruleset file called like `ruleset_name.rules`.
- a log map file called like `log_converter_map_file.map` which describes the value of an event characteristics.

Figure 1 Four Main Files

Description of the Files

The Log File

The table below presents an excerpt of a typical `cisco.vpn` log.

Table 2 Excerpt of a Log File

```
11/08/2008 10:30       Local7.Notice   10.10.9.2       5396305:
2008 Aug 11 09:34:01.400 GMT +0:00 %AUTH-6-23: RPT=6818:
192.123.102.85: User [192.123.102.85] Group [192.123.102.85]
disconnected: duration: 0:20:30
```

The Converter File

In the converter file, you will find information about the various files used to make the conversion.

Below is the excerpt of a file `exa_productname.conf.xml`:

Figure 2 exa_productname.conf.xml File

```
<!-- DO NOT EDIT THIS FILE - IT IS AUTOMATICALLY GENERATED BY SMP -->
- <ExaAgentConf>
    <standard>true</standard>
    <type>logger</type>
  - <conf class="ExaConfLog">
    - <userDefPart>
      - <fileName>
          <name>/var/log/cisco_vpn.log</name>
          <useDateRolling>false</useDateRolling>
          <rotationPeriod>0</rotationPeriod>
          <useIdRolling>false</useIdRolling>
          <nbDigit>0</nbDigit>
          <startId>0</startId>
        </fileName>
        <timeZone>local</timeZone>
        <dateFormat>MMM dd HH:mm:ss</dateFormat>
        <langageCode>en</langageCode>
        <countryCode>US</countryCode>
      </userDefPart>
    - <rulesetName>
        <string>exa_cisco-VPN_IOScompat.rules</string>
      </rulesetName>
    - <mapFiles>
        <string>exa_cisco-VPN_IOScompat.map</string>
      </mapFiles>
    </conf>
    <name>exa_Cisco_VPN_IOS_compat</name>
    <description>Cisco VPN Concentrator 3000 series</description>
    <author>admin</author>
    <lastModifiedBy>admin</lastModifiedBy>
    <creationDate>2007-08-06 15:00:00.0 PM</creationDate>
    <lastModifiedDate>2007-08-06 16:53:02.550 PM</lastModifiedDate>
  </ExaAgentConf>
```

Let us review some of the information provided in the converter file.

Converter Type

At the beginning, we have general information such as the converter type. In this case, it is the **logger** converter type:

Figure 3 Converter type

```
- <ExaAgentConf>
    <standard>true</standard>
    <type>logger</type>
  - <conf class="ExaConfLog">
    - <userDefPart>
      - <fileName>
          <name>/var/log/cisco_vpn.log</name>
```

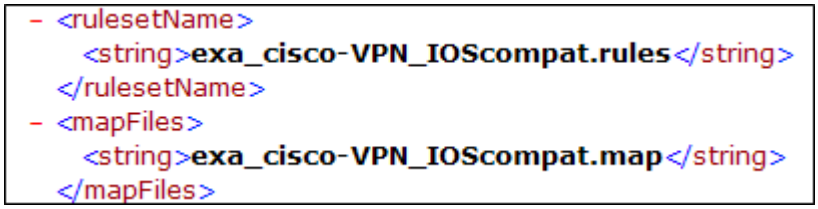
The file path is enclosed by the **`<name>`** tags and is:

```
/var/log/log_file_name.log
```

Map File and Ruleset Name

The map file and ruleset names are given next:

Figure 4 Map File and Ruleset Names



The Ruleset File

A `ruleset` file describes how to create SEM elementary events from raw log entries. This file is composed of a set of rules which, in turn, have numerous fields. The general syntax for a rule can be a list of regex or a tree structure.

Note: There are two versions of ruleset files. The behaviour of v1 and v2 slightly differs as explained in section "How to Read and Understand a Logger File".

Regex List:

```
regex=([^\t]+)\t+Local7.Notice\t+([\d.]+)\t+(\d+):\s+(.*)%AUTH-(
\w)-23: RPT=\d+:\s+([\d.]+):\s+User \[([\d.]+)\]\s+Group
\[([\d.]+)\] disconnected: duration: (\S+);
regexId=9;
categoryId=1.3.5_28.26_126.60;
skip=false;
classification.text=VPN user disconnected : $7;
assessment.impact.completion=succeeded;
analyzer.analyzerId=$2;
additionalData.meaningAndData=SEQ_ID=$3;
detectTime.time=$4;
assessment.impact.severity=$map(severity$5,1)$;
target.node.nameOrIp=$6;
target.user.userId.nameOrNumber=$7;
last;
```

This example above is taken from the `cisco_vpn.rules` file, a ruleset delivered by default with the SEM.

Regex Tree:

```
regex=B ([\w.-@]+);
regexId=1;
set=_var1=$1;
assessment.impact.severity=low;
last;

regex=B ([\w.-@]+) to ([\w.-@]+) at .*;
regexId=2;
parent=1;
categoryId=1.3.8_56.30_33.45;
classification.text=BC;
source.user.userId.nameOrNumber=$_var1$;
target.user.userId.nameOrNumber=$1;
patternAlreadyMatched=B ([\w.-@]+);
last;
```

Field Description

A description for each field is found below:

Table 3 Field Descriptions

Field Name	Card.	Description	Value Type	Possible Values
regex	1	Regular expression that should match the text in the log.	regex	
regexId	1	Identifier for the regex	text	
skip	0-1	Indicates if this ruleset is activated or not	boolean	true, false
[Deprecated] logRawData	0-1	Indicates if there is a need for storing the raw log entry in the SMP server database	boolean	true, false
dateToFormat	0-1	Formats the detection date according to the format described in the “converter”		
IDMEF fields	1+	One or more fields listed in the Table 22 "Definition of Fields"		

Table 3 Field Descriptions

Field Name	Card.	Description	Value Type	Possible Values
last	1	Indicates the end of the rule. This field does not accept any values.	none	none
[regex tree only] parent	1	Indicates the parent of the current regex.	list of existing regexId separated by commas	
[regex tree only] patternAlreadyMatched	1	Indicates the part of the pattern that can be deleted as it has already matched the previous regex tree level.	regex (beginning of the expression from the regex field)	
[regex tree only] set	0+	Sets a value to a variable. variable's name starts by _ (underscore). variable's content can be either a fixed string or $n, or a mix of both.	text	

Variables

The following table presents the special TIBCO LogLogic® variables which can be used in the definition for a field value.

Table 4 Special TIBCO LogLogic® Variables

Variable Name	Description
$n	The value found in the N position in case the expression is enclosed in parenthesis.
$analyzerId$	Identifier for the equipment unit.
$date$	Date when the message was detected. If there is no date, then the current date is retrieved.
$host$	The Syslog log source which managed the log (welf, multiline...) Only used in ruleset v2.
$hostIp$	IP address of the machine hosting the Log Collector.
$hostName$	The name of the machine hosting the Log Collector.

Example: `source.node.address.address = $hostIp$;`

The Split function

This function allows you to split a field into several values. The syntax is:

```
target.node.emailAddress=$split($3,',')$;
```

For example, you can use it if you want to display all the target e-mail addresses coming from a raw log such as the following one usually concatenated by the ruleset:

```
#Mar  5 09:11:30 bt1wd11b sendmail[13179]: JAA0000013186:
to=twittend@bcompany.fr,jmalplat@company.fr,frolland@company.fr,
delay=00:00:00, xdelay=00:
00:00, mailer=smtpr, relay=bt1sss00.bpa.company.fr.
[172.16.113.67], stat=Sent (JAA00948 Message accepted for
delivery)
```

In the GUI, you should obtain something like:

E-mail (3)

- twittend@bcompany.fr
- jmalplat@company.fr
- frolland@company.fr

The `Split` function applies to the following fields:

- `source.node.emailAddress`
- `source.node.ipv4Address`
- `source.process.arg`
- `source.process.env`
- `source.service.webService.arg`
- `target.node.emailAddress`
- `target.node.ipv4Address`
- `target.process.arg`
- `target.process.env`
- `target.service.webService.arg`

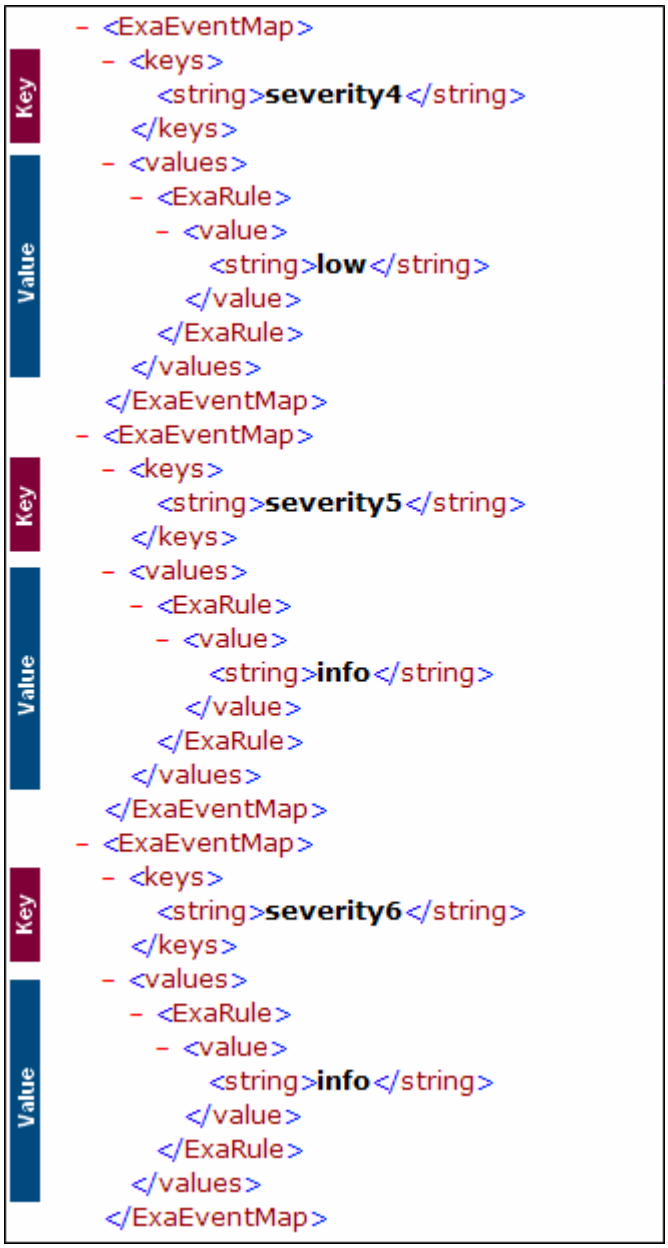
The Map File

The general structure of the `map` file is a sequence of keys, each containing one or more values, as follows:

Key Values
Key 1
Value a
Value b
Value c
Key 2
Value a
Value b
Value c
Etc.

For example, below is an excerpt of a real `map` file `log_converter_map_file.map`

Figure 5 Example of a Map File



The values refer to the severity. They will be used to map the information contained in the log file along with the ruleset to make the raw log understandable by the SMP.

How to Read and Understand a Logger File

Let us take an example to explain it.

To read and understand the log, we will compare and apply information from the converter file to the map file. The example will refer to the **severity** of the event.

- Open the `Log` file, the `Ruleset` file and the `Map` file.

Step 1: Reading the Ruleset File

In the `Ruleset` file, look at the line:

`assessment.impact.severity=$map(severity$5,1)$;`

```
regex=([^\t]+)\t+Local7.Notice\t+([\d.]+)\t+(\d+):\s+(.*)%AUTH-(
\w)-23: RPT=\d+:\s+([\d.]+):\s+User \[([\d.]+)\]\s+Group
\[([\d.]+)\] disconnected: duration: (\S+);
regexId=9;
categoryId=1.3.5_28.26_126.60;
skip=false;
classification.text=VPN user disconnected : $7;
assessment.impact.completion=succeeded;
analyzer.analyzerId=$2;
additionalData.meaningAndData=SEQ_ID=$3;
detectTime.time=$4;
assessment.impact.severity=$map(severity$5,1)$;
target.node.nameOrIp=$6;
target.user.userId.nameOrNumber=$7;
last;
```

Description

Table 5 Explanation

Term	Description
assessment.impact.severity	IDMEF field corresponding to the severity.
(severity$5,1)	$5 is the value that must be replaced by the **fifth** value contained into brackets on the line starting with **`regex=.`** E.g. in the above example, the fifth value is **(\W)**. 1 means the first value of the key**(\W)** in the Map file.

Ruleset Versions

There are two versions of ruleset files.

- v1 is the version used by default.
- v2 is used each time the key word **`version=2`** is displayed at the very beginning of the file *.rules. The behaviour differs from v1 in the two following cases:
  - hot is only used in v2. The name after the date is automatically retrieved.
  - The date is automatically retrieved in bsd or kiwi formats (see converter) and the parsing applies to the rest of the line.

Step 2: Comparing the Ruleset File with the Log File

Example with Version 1

The next step is to compare the values from the ruleset file with the ones in the raw log.

A value in a ruleset corresponds to a value into brackets. You can then easily replace the correct values from the Log file.

In the example below, the corresponding values are in the same color.

E.g. `11/08/2008 10:30` and `([^\t]+`

Log File

```
11/08/2008 10:30        Local7.Notice    10.10.9.2        5396305:
2008 Aug 11 09:34:01.400 GMT +0:00 %AUTH-6-23: RPT=6818:
192.123.102.85: User [192.123.102.85] Group [192.123.102.85]
disconnected: duration: 0:20:30
```

Excerpt of a Ruleset File

```
regex=([^\t]+)\t+Local7.Notice\t+([\d.]+)\t+(\d+):\s+(.*)%AUTH-(
\w)-23: RPT=\d+:\s+([\d.]+):\s+User \[([\d.]+)\]\s+Group
\[([\d.]+)\] disconnected: duration: (\S+);
regexId=9;
```

As a consequence, in our example, the value `(\w)` corresponds to the value `6`.

Example with Version 2

Log File

```
Mon 26 11 10:05:33 hostname %AUTH-6-23: RPT=6818: 192.123.102.85:
User [192.123.102.85] Group [192.123.102.85] disconnected:
duration: 0:20:30
```

Excerpt of a Ruleset File

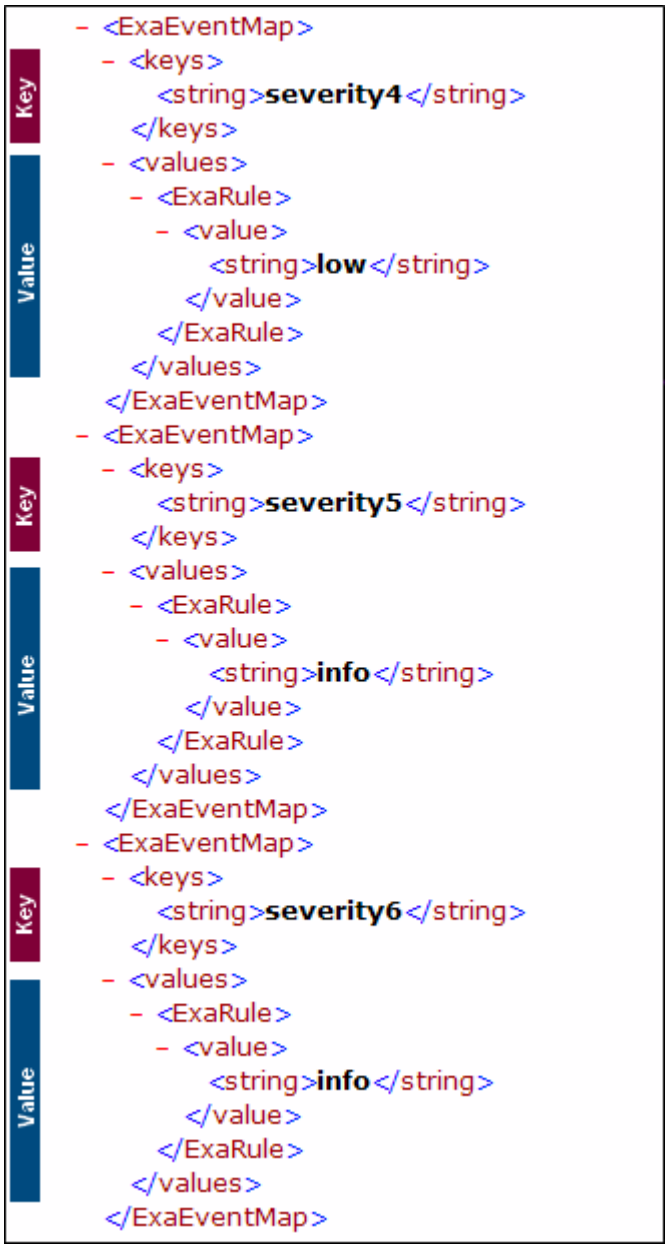
```
regex=%AUTH-(\w)-23: RPT=\d+:\s+([\d.]+):\s+User
\[([\d.]+)\]\s+Group \[([\d.]+)\] disconnected: duration: (\S+);
regexId=9;
```

Step 3: Comparing the Log File with the Map File

To know exactly the severity of the event, you must now look at the **Map** file and seek the **sixth** severity (remember that `(\w)` corresponds to the value `6`).

In our example, the **sixth** string is **`severity6`**.

Figure 6 Excerpt of a Map File



Step 4: Comparing the Ruleset File with the Map File

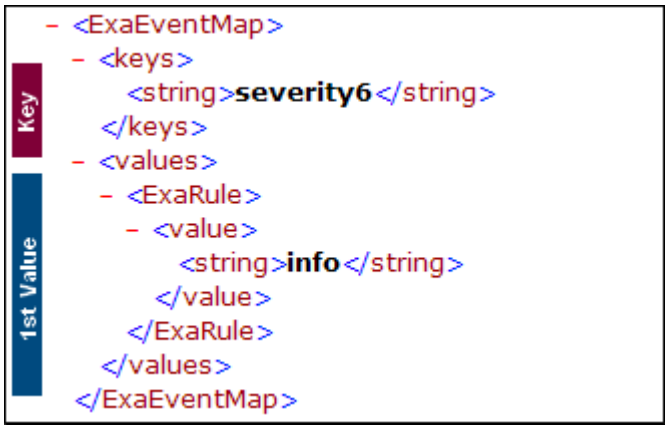
In the `Ruleset` file, look again at the line:

```
assessment.impact.severity=$map(severity$5,1)$;
```

The value `1` contained in `$map(severity$5,1)$;` indicates the position of the key value in the `Map` file. Here, it is the first position.

In our example, the first key value encountered for `severity6 is <string>info</string>.`

Figure 7 Excerpt of a Map File



Therefore, the conclusion is that the severity for the generated event is `info`.

In other words, you can say that:

```
assessment.impact.severity=info
```

In this manner, by examining each value and field definition in the converter file, you can determine the matching keys and their corresponding values in the map file for the entire log file.

Caution: If you decide to modify the XML converter manually, you must refresh the GUI just after, otherwise - at the next update of the GUI - your modification will be overwritten.

To refresh the GUI, go to **Log Management > Advanced > Convertors** and click on **Refresh the list**.

Implementation of WELF Converter

WELF (WebTrends Enhanced Logfile Format) converters are used when the source of events to be monitored is a text file in the WELF format or received by Syslog.

A Log Collector will use two files to format WELF raw logs emitted by a Cyberguard firewall into an IDMEF format to subsequently transmit them to the SMP. The two files are:

- `Cyberguard.map - XML` file containing keys and values used to format the raw log.
- `Cyberguard.conf.xml` - XML converter file.

> **Caution:** Those two files are provided along with the SMP. They are not editable except by the integrator in case he needs to modify it or if there is an unusual behaviour of the SMP.

The three main files must be compared alongside.

- The `Log` file contains the event description.
- The `Converter` file describes an event characteristics.
- The `Map` file describes the value of an event characteristics.

Figure 8 Three Main Files

Description of the Files

The Cyberguard WELF Log File

The table below presents an excerpt of a **`Cyberguard WELF`** log file.

Each date indicates the beginning of a new event, in this case `"Sep 6 …"`. The first event that we will take into account has been highlighted:

```
Sep  6 18:35:50 10.202.253.8 auditLogger:
time="2010-09-06T18:35:02.348" event="sessionCreated"
sensor="PF" sessionId="431825e7:76ec100"
sessionGroupId="431825e7:76ec100" filterAction="pasvProxy"
proxy="httpProxy" ruleType="staticRule" ruleId="7"
clientInAddr="10.202.252.10" serverInAddr="10.202.253.8"
protocol="TCP" clientInPort="42688" serverInPort="8181"

Sep  6 18:35:50 10.202.253.8 auditLogger:
time="2010-09-06T18:35:02.348" event="sessionClosed" sensor="http-
Proxy" sessionGroupId="431825e7:76ec100" reason="normal"

Sep  6 18:35:50 10.202.253.8 auditLogger:
time="2010-09-06T18:35:02.348" event="sessionDestroyed" sen-
sor="PF" sessionId="431825e7:76ec100" session-
GroupId="431825e7:76ec100" filterAction="pasvProxy"
proxy="httpProxy" ruleType="staticRule" ruleId="7" clientInAd-
dr="10.202.252.10" serverInAddr="10.202.253.8" protocol="TCP" cli-
entInPort="42688" serverInPort="8181" clientIfName="es0p1"
serverIfName="lo" clientTcpState="FIN" serverTcpState="FIN" forw-
Packets="3" forwBytes="164" backPackets="2" backBytes="112" start-
Time="2010-09-06T18:35:02.000"
```

The Converter File

In the converter file you will find the corresponding definitions for the values given in the map file. Below is the excerpt of the file `Cyberguard.conf.xml`:

Figure 9 Cyberguard.conf.xml File

```
<!-- DO NOT EDIT THIS FILE - IT IS AUTOMATICALLY GENERATED BY SMP -->
- <ExaAgentConf>
    <standard>true</standard>
    <type>welf</type>
  - <conf class="ExaConfWelf">
    - <userDefPart>
      - <fileName>
          <name>/var/log/message</name>
          <useDateRolling>false</useDateRolling>
          <dateFormat />
          <rotationPeriod>0</rotationPeriod>
          <useIdRolling>false</useIdRolling>
          <nbDigit>0</nbDigit>
          <startId>0</startId>
        </fileName>
        <timeZone>local</timeZone>
        <dateFormat>MMM d HH:mm:ss</dateFormat>
        <langageCode>en</langageCode>
        <countryCode>US</countryCode>
        <emptyFieldValue> </emptyFieldValue>
        <regex>([\d\.]+) auditLogger:</regex>
        <delimValue>=</delimValue>
        <delimField > </delimField >
      </userDefPart>
    - <mapFiles>
        <string>cyberguard.map</string>
      </mapFiles>
    - <rules>
      - <ExaRule>
          <field>skip</field>
        - <value>
          - <ExaRuleMap>
            - <key>
              - <ExaRuleReplaceField>
                  <field>event</field>
                </ExaRuleReplaceField>
              - <ExaRuleReplaceField>
                  <field>filterAction</field>
                </ExaRuleReplaceField>
              </key>
              <fieldId>1</fieldId>
            </ExaRuleMap>
          </value>
        </ExaRule>
      - <ExaRule>
          <field>classification.text</field>
        - <value>
          - <ExaRuleMap>
            - <key>
              - <ExaRuleReplaceField>
                  <field>event</field>
                </ExaRuleReplaceField>
              - <ExaRuleReplaceField>
                  <field>filterAction</field>
                </ExaRuleReplaceField>
              </key>
              <fieldId>4</fieldId>
            </ExaRuleMap>
          </value>
        </ExaRule>
```

Let us review some of the information provided in the converter file.

Converter Type

At the beginning, we have general information such as the converter type. In this case, it is the **welf** converter type:

Figure 10 Converter type

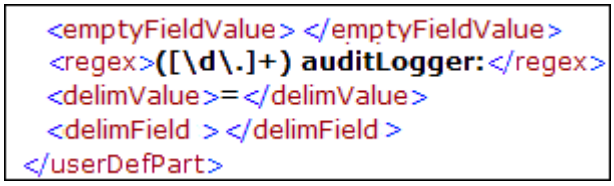
The file path is enclosed by the `<name>` tags and is:

```
/var/log/message
```

Equation Character

The tags `<delimValue>` and `<delimField>` inform which character is used to respectively serve as an equation character and as a delimiter in the map file. In this example, the equation character is "=" and the delimiter is " " (blank space).

Figure 11 Equation Character



For instance, it can refer to an IP address.

Map File Name

The map file name is given next:

Figure 12 Map File Name

IDMEF and Other Fields

The `<field>` tag indicates the IDMEF or other fields to be compared with the map file. Please refer to the list of IDMEF fields in the section Appendix A - "List of Alerts Fields" of this documentation.

Key Definition

Following the name of the field, we have the definitions for its keys:

- `"event"`
- `"filterAction"`

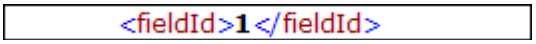
The definitions for the keys are enclosed by the `<key>` tags.

It means that if the event description contain the terms `event` and `filterAction` in the log, then the corresponding field will be replaced.

Map File Position

Next, we have the map file position for the corresponding information for this field. In this case, it is "1", or the first position.

Figure 13 Map File Position



In our example, it refers to the `false` value in the `cyberguard.map` file.

The Map File

The general structure of the `map` file is a sequence of keys, each containing one or more values, as follows:

Key Values
Key 1
Value a
Value b
Value c
Key 2
Value a
Value b
Value c
Etc.

For example, below is an excerpt of a real **`map`** file (`cyberguard.map`). Notice that the first two defined **keys** are `sessionCreated` and `pass`.

Figure 14 Example of a Real Map File

```
<!--  DO NOT EDIT THIS FILE - IT IS
  AUTOMATICALLY GENERATED BY SMP   -->

- <ExaEventMapList>
   <standard>true</standard>
  - <list>
   - <ExaEventMap>
     - <keys>
         <string>sessionCreated</string>
         <string>pass</string>
       </keys>
     - <values>
       - <ExaRule>
         - <value>
             <string>false</string>
           </value>
         </ExaRule>
       - <ExaRule>
         - <value>
             <string>low</string>
           </value>
         </ExaRule>
       - <ExaRule>
         - <value>
             <string>other</string>
           </value>
         </ExaRule>
       - <ExaRule>
         - <value>
             <string>Packet accepted</string>
           </value>
         </ExaRule>
```

Key

Value

Value

Value

Value

The 4 indicated values above will correspond to the **`<fieldID>`** tag in the `Cyberguard.conf.xml` converter file or "Map File Position".

How to Read and Understand a Welf Log File

Let us apply the above information from the converter file to the map file.

- Display the three relevant files.

Step 1: Reading the Converter File

In the Converter file:

1. Look at the `<regex>` tag. It indicates where you must start reading in the Log file.

For example, if you have in the Converter file
`<regex>([\d\.]+) auditLogger:</regex>`
then in the Log file, you will start reading the event from
`time="2010-09-06T18:35:02.348".`

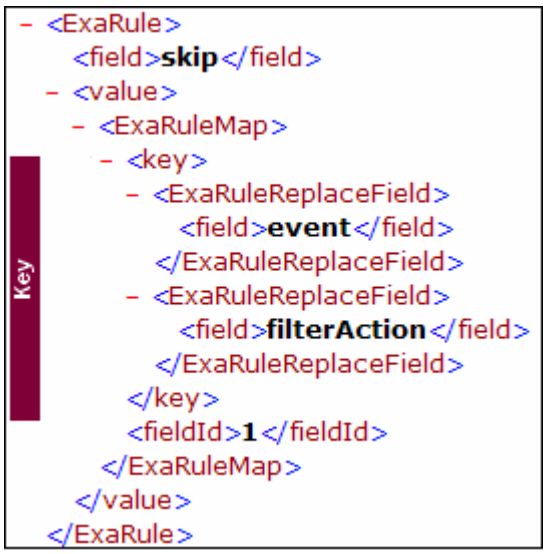
2. Look at the `<field>` tag. It indicates the action to perform or characteristic of the event.

In our example, the problem will be to know whether the event/alert will be skipped or not as we have `<field>skip</field>`.

3. Look at the `<key>` tag. The values in these tags indicate the fields to take into account in the `Log` file.

In our example, the`<key>` tags are:

Figure 15 Key Tags



Step 2: Comparing the Converter File with the Log File

Compare the value of the `<field>` tags
(**`<field>event</field>`** and **`<field>filterAction</field>`**) with the relevant fields in the Log file (example is in bold below):

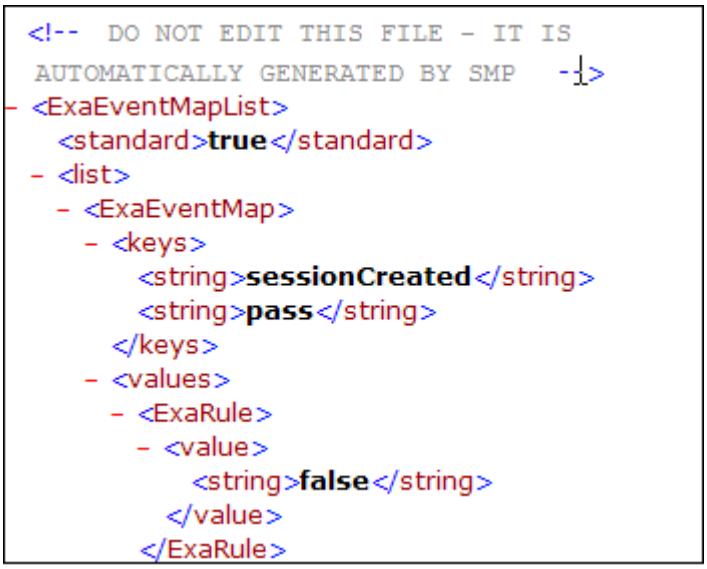
```
Sep  6 18:35:50 10.202.253.8 auditLogger:
time="2010-09-06T18:35:02.348" event="sessionCreated" sensor="PF"
sessionId="431825e7:76ec100" sessionGroupId="431825e7:76ec100"
filterAction="pass" proxy="httpProxy" ruleType="staticRule"
ruleId="7" clientInAddr="10.202.252.10" serverInAd-
dr="10.202.253.8" protocol="TCP" clientInPort="42688" serverIn-
Port="8181"
```

You can see that in the `Map` file, **`event`** will be replaced by **`sessionCreated`** and **`filterAction`** by **`pass`**.

Step 3: Comparing the Converter File with the Map File

1. In the Map File, compare the fields that have been replaced. Only **session Created** and **pass** are available in the file.

Figure 16 Map File

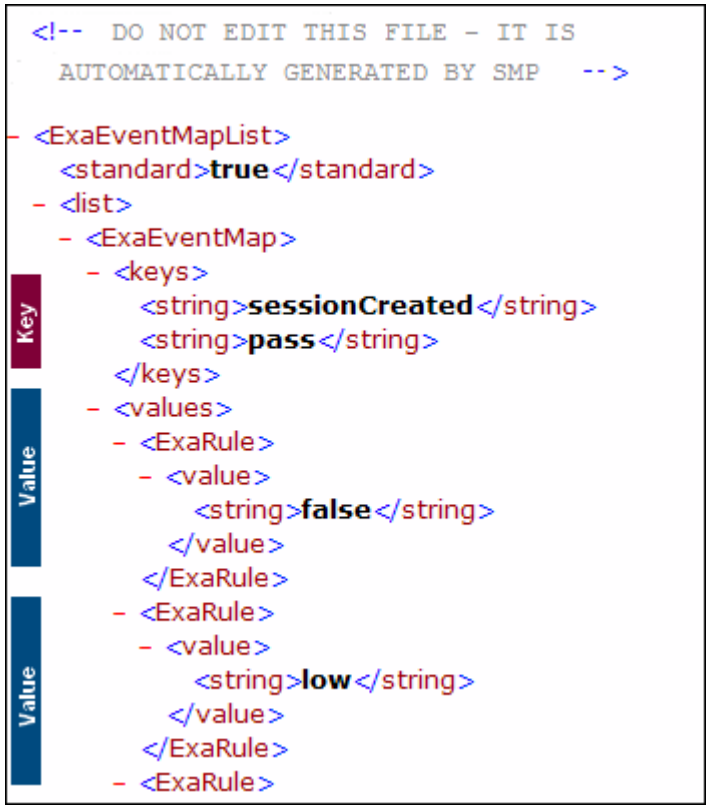


2. You must now check the tag **<fieldID>1<fieldID>** in the Converter File.
It indicates that the first field encountered in the **Map** file will be taken into account.

3. Then check the first field encountered in the Map File.

In our example, it is **<string>false</string>**. It means that the **skip** field will be set to **false**. In other words, it means that the event will not be skipped but displayed in the Web Console.

Figure 17 The First Value Encoutered is “false”



In this manner, by examining each value and field definition in the converter file, you can determine the matching keys and their corresponding values in the map file for the entire log file.

Caution: If you decide to modify the XML converter manually, you must refresh the GUI just after, otherwise - at the next update of the GUI - your modification will be overwritten.

To refresh the GUI, go to **Log Management > Advanced > Convertors** and click on **Refresh the list**.

Implementation of Database-Type Converter

Database-type converters are used when the source of events to be monitored is a database.

A Log Collector will put forth a data request to a database to obtain the information to be sent to the SMP. Before sending this information, the Log Collector will standardize it in an IDMEF format. The two files used to configure this process are:

- `*.map` - XML file containing keys and values used to format the raw log.
- `*.conf.xml` - XML converter file

TIBCO LogLogic® furnishes these two XML files by default. If necessary, you can modify these files according to your needs.

The two main files must be compared alongside.

- The `Converter` file describes an event characteristics.
- The `Map` file describes the value of an event characteristics.

Figure 18 The database and the two main files

Description of the File

The Converter File

In the converter file you will find the corresponding definitions for the values given in the map file. Below is the excerpt of the file `exa_Arkoon_DB_IDPS.conf.xml`:

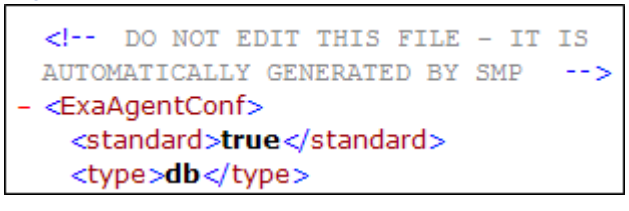
Figure 19 exa_Arkoon_DB_IDPS.conf.xml

Let us review some of the information provided in the converter file.

Converter Type

At the beginning, we have the converter type, in this case, `db` (database):

Figure 20 Converter File



Database Queries

In the `converter` file, you will see the various database request statements, for example:

Figure 21 Database Request Statements

```
- <request>
    <string>SELECT id_match, case id_idsalert when 0 then
      'detected' else case action when 1 then 'detected'
      else 'blocked' end end, ids_alert_matches.time_sec,
      sig_id, logs_idlog FROM ids_alert_matches, logs
      WHERE logs.id_log=ids_alert_matches.logs_idlog
      and id_match > %ID</string>
    <string>SELECT sig_desc from ids_sig_descriptions
      WHERE sig_sid=$1.4$</string>
    <string>SELECT ip_src, ip_dest, port_src, port_dest,
      protocol, intf, action, reason, time_sec, rulename,
      intf_out, username from logs WHERE id_log=$1.5
      $</string>
    <string>SELECT substring_index(rule_ref, '_',1),
      substring_index(rule_ref, '_',-1) FROM
      ids_sig_references WHERE rule_sid=$1.4$ and
      rule_ref not like("url_%") and rule_ref not like
      ("arachnids_%")</string>
  </request>
```

This file indicates the fields that have been exported from the database.

Map File Name

The `map` file name is given next:

Figure 22 Map File Name

```
- <mapFiles>
    <string>exa_arkoon_idps_db.map</string>
  </mapFiles>
```

The Map File

The general structure of the `map` file is a sequence of keys, each containing one or more values, as follows:

Key 1

Value a

Value b

Value c

Key 2

Value a

Value b

Value c

Etc.

For example, below is an excerpt of a real `map` file (`exa_arkoon_idps_db.map`).

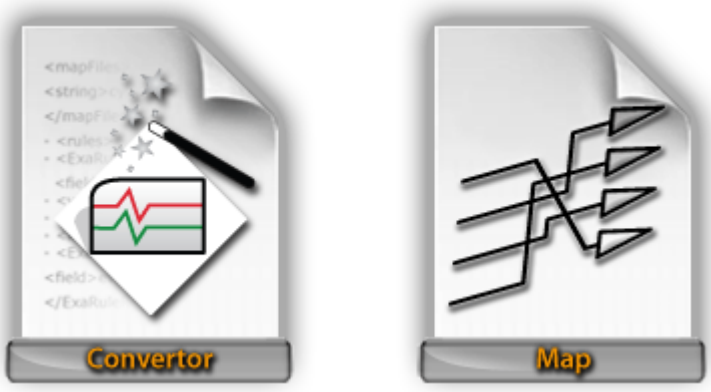
Figure 23 Example of a Real Map File

The indicated values above will correspond to the **`<fieldID>`** tag in the `exa_Arkoon_DB_IDPS.conf.xml` converter file or Map file position.

How to Read and Understand a Database Converter File

Let us apply the above information from the converter file to the map file.

- Display the two relevant files.



Step 1: Reading the Converter File

In the `Converter` file:

Look at the following paragraph in the `Converter` file.

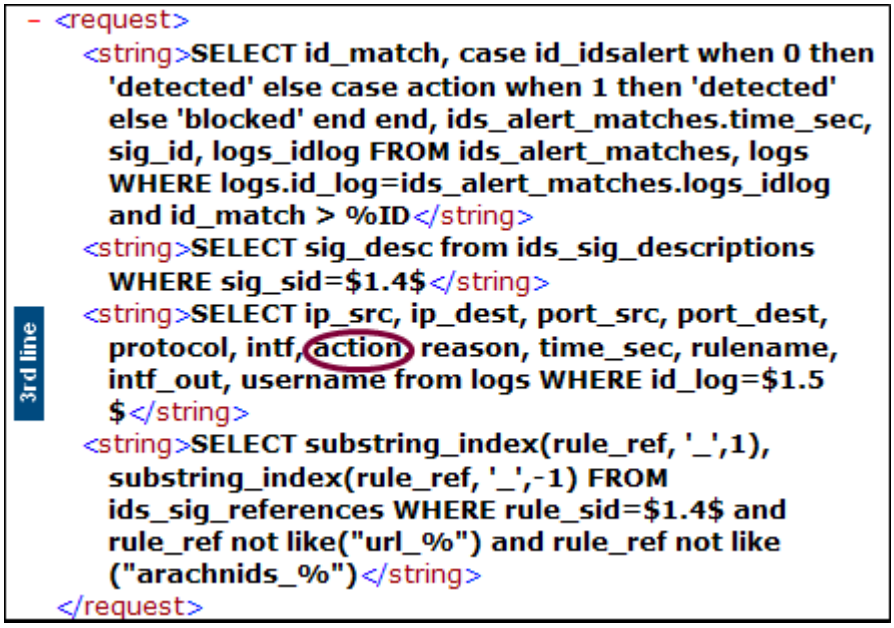
Figure 24 Database Reques - severity

```
- <ExaRule>
    <field>assessment.impact.severity</field>
  - <value>
    - <ExaRuleMap>
      - <key>
          <string>action_</string>
        - <ExaRuleReplaceField>
            <field>3.7</field>
          </ExaRuleReplaceField>
        </key>
        <fieldId>1</fieldId>
      </ExaRuleMap>
    </value>
  </ExaRule>
```

- It means that you must make the IDMEF field **`assessment.impact.severity`** match with the **seventh** item of the **third** query (**`<field>3.7</field>`**).
- **`<fieldId>1</fieldId>`** means that you will have to look at the number associated with the term `action_` in the `Map` file as explained in **Step 2: Reading the Map File**.

Look at the following paragraph in the `Converter` file.

Figure 25 Database Request



A line starts by `SELECT` and each item is separated by a comma.

As a consequence, our example shows that:

```
action = assessment.impact.severity
```

Step 2: Reading the Map File

From the Converter file, you know that the severity corresponds to the term `action_`.

You also have this information: **`<fieldId>1</fieldId>`** which means that you must add **`1`** to the term **`action_.`**

Then, in the `map` file, look at the relevant key.

Figure 26 Map file - severity


```
<!--  DO NOT EDIT THIS FILE - IT IS
AUTOMATICALLY GENERATED BY SMP   -->
- <ExaEventMapList>
    <standard>true</standard>
  - <list>
    - <ExaEventMap>
      - <keys>
          <string>action_0</string>
        </keys>
      - <values>
          <string>high</string>
        </values>
      </ExaEventMap>
    - <ExaEventMap>
      - <keys>
          <string>action_1</string>
        </keys>
      - <values>
          <string>medium</string>
        </values>
      </ExaEventMap>
    - <ExaEventMap>
      - <keys>
          <string>action_2</string>
        </keys>
      - <values>
          <string>high</string>
        </values>
```

`action_1` corresponds to `medium`.

As a conclusion, you know that the severity of the event is `medium`.

Caution: If you decide to modify the XML converter manually, you must refresh the GUI just after, otherwise - at the next update of the GUI - your modification will be overwritten.

To refresh the GUI, go to **Log Management > Advanced > Convertors** and click on **Refresh the list**.

Definition of Alert Fields

Definition of the Alerts Fields

Table 22, “Definition of Fields,” on page 153 presents:

- the fields supported in Security Event Manager;
- their respective correspondences with IDMEF fields (the IDMEF naming convention has been kept);
- the cardinality (as meant by IDMEF standards). There are four possible cardinalities:
  - 0+ for zero or greater than zero
  - 0-1 for zero or one
  - 1+ for at least one
  - 1 for one and one only
- a succinct description and the usage;
- the type of value that is expected (T. of V.);
- the permitted values (which can be case sensitive);
- an indication in case the element is “non-terminal” (N.T.) that is, it concerns an IDMEF class or attribute.

Note: The type written in bold in the “Permitted Values” column is the default value.

The multiple values 0+ or 1+ are defined using the '[n]' syntax where ***n*** corresponds to the index.

Example:

```
regex=…
…
classification.text=test;
classification.reference[0].name=first URL for the test;
classification.reference[0].url=www.google.fr;
classification.reference[1].name=second URL for the test;
classification.reference[1].url=www.yahoo.fr;
…
last;
```

Regular Expression Constructs

The following table lists a summary of regular-expression constructs. The original Sun document is found at the following URL:

http://java.sun.com/j2se/1.4.2/docs/api/java/util/regex/Pattern.html

Table 6 Regular-Expression Constructs

Construct	Matches
Characters	
x	The character *x*
\\	The backslash character
\0*n*	The character with octal value 0*n* (0 <= *n* <= 7)
\0*nn*	The character with octal value 0*nn* (0 <= *n* <= 7)
\0*mnn*	The character with octal value 0*mnn* (0 <= *m* <= 3, 0 <= *n* <= 7)
\x*hh*	The character with hexadecimal value 0x*hh*
\u*hhhh*	The character with hexadecimal value 0x*hhhh*
\t	The tab character ('\u0009')
\n	The newline (line feed) character ('\u000A')
\r	The carriage-return character ('\u000D')
\f	The form-feed character ('\u000C')
\a	The alert (bell) character ('\u0007')
\e	The escape character ('\u001B')
\c*x*	The control character corresponding to *x*
Character classes	
[abc]	a, b, or c (simple class)
[^abc]	Any character except a, b, or c (negation)
[a-zA-Z]	a through z or A through Z, inclusive (range)
[a-d[m-p]]	a through d, or m through p: [a-dm-p] (union)
[a-z&&[def]]	d, e, or f (intersection)
[a-z&&[^bc]]	a through z, except for b and c: [ad-z] (subtraction)
[a-z&&[^m-p]]	a through z, and not m through p: [a-lq-z] (subtraction)
Predefined character classes	
.	Any character (may or may not match line terminators)
\d	A digit: [0-9]
\D	A non-digit: [^0-9]
\s	A whitespace character: [\t\n\x0B\f\r]
\S	A non-whitespace character: [^\s]
\w	A word character: [a-zA-Z_0-9]
\W	A non-word character: [^\w]

Table 6 Regular-Expression Constructs

Construct	Matches
POSIX character classes (US-ASCII only)	
\p{Lower}	A lower-case alphabetic character: `[a-z]`
\p{Upper}	An upper-case alphabetic character: `[A-Z]`
\p{ASCII}	All ASCII: `[\x00-\x7F]`
\p{Alpha}	An alphabetic character: `[\p{Lower}\p{Upper}]`
\p{Digit}	A decimal digit: `[0-9]`
\p{Alnum}	An alphanumeric character: `[\p{Alpha}\p{Digit}]`
\p{Punct}	Punctuation: One of `!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~`
\p{Graph}	A visible character: `[\p{Alnum}\p{Punct}]`
\p{Print}	A printable character: `[\p{Graph}]`
\p{Blank}	A space or a tab: `[ \t]`
\p{Cntrl}	A control character: `[\x00-\x1F\x7F]`
\p{XDigit}	A hexadecimal digit: `[0-9a-fA-F]`
\p{Space}	A whitespace character: `[ \t\n\x0B\f\r]`
Classes for Unicode blocks and categories	
\p{InGreek}	A character in the Greek block (simple block)
\p{Lu}	An uppercase letter (simple category)
\p{Sc}	A currency symbol
\P{InGreek}	Any character except one in the Greek block (negation)
[\p{L}&&[^\p{Lu}]]	Any letter except an uppercase letter (subtraction)
Boundary matchers	
^	The beginning of a line
$	The end of a line
\b	A word boundary
\B	A non-word boundary
\A	The beginning of the input
\G	The end of the previous match
\Z	The end of the input but for the final terminator, if any
\z	The end of the input
Greedy quantifiers	
X?	*X*, once or not at all
*X**	*X*, zero or more times
X+	*X*, one or more times
X{*n*}	*X*, exactly *n* times
X{*n*,}	*X*, at least *n* times
X{*n*,*m*}	*X*, at least *n* but not more than *m* times

Table 6 Regular-Expression Constructs

Construct	Matches
Reluctant quantifiers	
X??	*X*, once or not at all
*X**?	*X*, zero or more times
X+?	*X*, one or more times
X{*n*}?	*X*, exactly *n* times
X{*n*,}?	*X*, at least *n* times
X{*n*,*m*}?	*X*, at least *n* but not more than *m* times
Possessive quantifiers	
X?+	*X*, once or not at all
*X**+	*X*, zero or more times
X++	*X*, one or more times
X{*n*}+	*X*, exactly *n* times
X{*n*,}+	*X*, at least *n* times
X{*n*,*m*}+	*X*, at least *n* but not more than *m* times
Logical operators	
XY	*X* followed by *Y*
X|*Y*	Either *X* or *Y*
(*X*)	X, as a capturing group
Back references	
n	Whatever the n^{th} capturing group matched
Quotation	
\	Nothing, but quotes the following character
\Q	Nothing, but quotes all characters until \E
\E	Nothing, but ends quoting started by \Q
Special constructs (non-capturing)	
(?:*X*)	*X*, as a non-capturing group
(?idmsux-idmsux)	Nothing, but turns match flags on - off
(?idmsux-idmsux:*X*)	*X*, as a non-capturing group with the given flags on - off
(?=*X*)	*X*, via zero-width positive lookahead
(?!*X*)	*X*, via zero-width negative lookahead
(?<=*X*)	*X*, via zero-width positive lookbehind
(?<!*X*)	*X*, via zero-width negative lookbehind
(?>*X*)	*X*, as an independent, non-capturing group

Chapter 2 - Correlation

What is Correlation?

Introduction

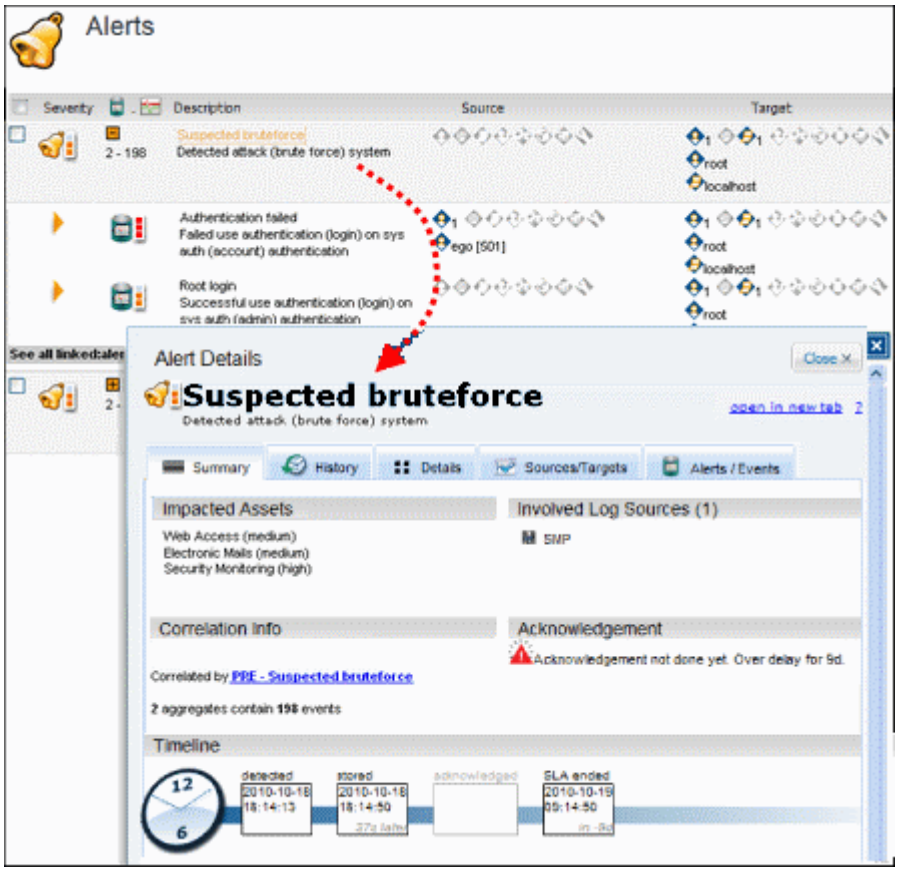
Correlation is the process of grouping different events coming from various security devices to create a unique alert.

Security Event Manager offers a correlation funtionality by using user-defined or default ***correlation rules***.

For example, several “Authentication failed logins” followed by a “successful login” event is correlated into a “Suspected bruteforce” alert.

Once the rule is triggered, the newly generated alert is available in the **Alerts** screen as in the example below.

Figure 27 Alerts screen



What are Rules Used for?

A correlation rule is a description that defines how to gather events into alerts according to alerts' value fields, also called conditions and exceptions. A counter and a time period are applied to a rule to trigger an action at a precise moment.

Rules control how events are correlated, and they allow you to build up consistent policies to provide a high level information system security overview.

You can define or find the default correlation rules from the general interface via the menu **Event Management > Correlation Policy**.

Figure 28 Correlation policy

#	Name	Starting thresholds	Sto
1	ADB - Misuse - Windows Domain Controller Output	1/60 events/seconds	500 216
2	ADB - Misuse - Windows Domain Controller Input	1/60 events/seconds	500 216
3	ADB - Misuse - Mail Server Output	1/60 events/seconds	500 216
4	ADB - Misuse - Mail Server Input	1/60 events/seconds	500 216
5	ADB - Misuse - Web Proxy Output	1/60 events/seconds	500 216
6	ADB - Misuse - Web Proxy Input	1/60 events/seconds	500 216

Why Using Correlation?

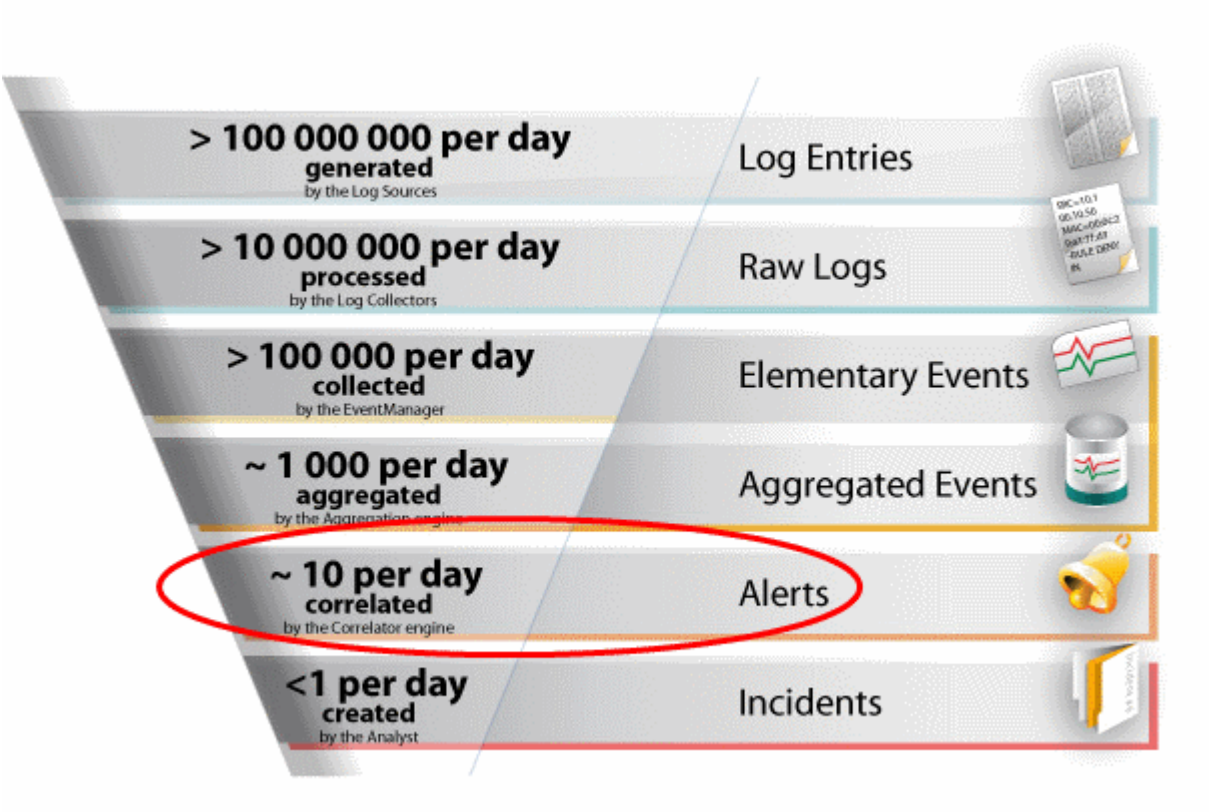
Correlation allows you to:

- reduce the mass of information to monitor.
- compensate for the lack of consistency among security device generated messages.
- automate the response after receiving a message.
- enhance the quality of the diagnosis.

To Reduce the Amount of Information to Monitor

Security administrators and analysts are facing a mass of information coming from numerous and heterogeneous security devices. This quantity of information cannot be monitored easily, therefore a grouping method must be applied to the various messages. This will be done via the correlation rules.

Figure 29 Reduction of the mass of information



To Automate the Response after Receiving a Message

Once correlation has been performed and according to your configuration of the correlation rule, an immediate action can take place such as the:

- automatic creation of an alert.
- modification of the event's severity.
- sending of an alert or event from one SMP to another one in a multi-instance environment.
- mailing of the event to contacts.
- automatic creation of an incident from the alert.
- creation of a scenario based on rules.

To Enhance the Quality of the Diagnosis

By using the Asset Database, the correlation process can meet your demand in terms of business security.

Once your business environment has been correctly configured in LM/EM (vulnerabilities, list of computers, etc) and with the help of the events generated by vulnerability scanners, you obtain an alert with information about your installed base.

Therefore, an alert linked with a critical server from the asset database will be considered as more important than an alert about a less sensitive server. Its severity will be modified and the alert will be processed in priority.

The information contained in the asset database will also be taken into account to fill the alerts' messages such as the IP address of a workstation.

To Compensate for the Lack of Consistency among Security Device Generated Messages

Messages generated by equipment are very different. Through correlation and standardization, messages will be classified so that events with the same information will always have the same description.

For example, if a detected port scan occurs:

- a Checkpoint firewall will generate a **Port Scanning** message.
- a NetASQ fireawll will generate a **Possible port scan** message.
- a Snort detection probe will generate a **Portscan detected** message.

Therefore, all these events can be correlated into one alert simply entitled **Port Scan**.

How Does Correlation Work?

Introduction

The SMP comprises three core engines to process the incoming events data: the aggregation, the totaling, and the correlation engines.

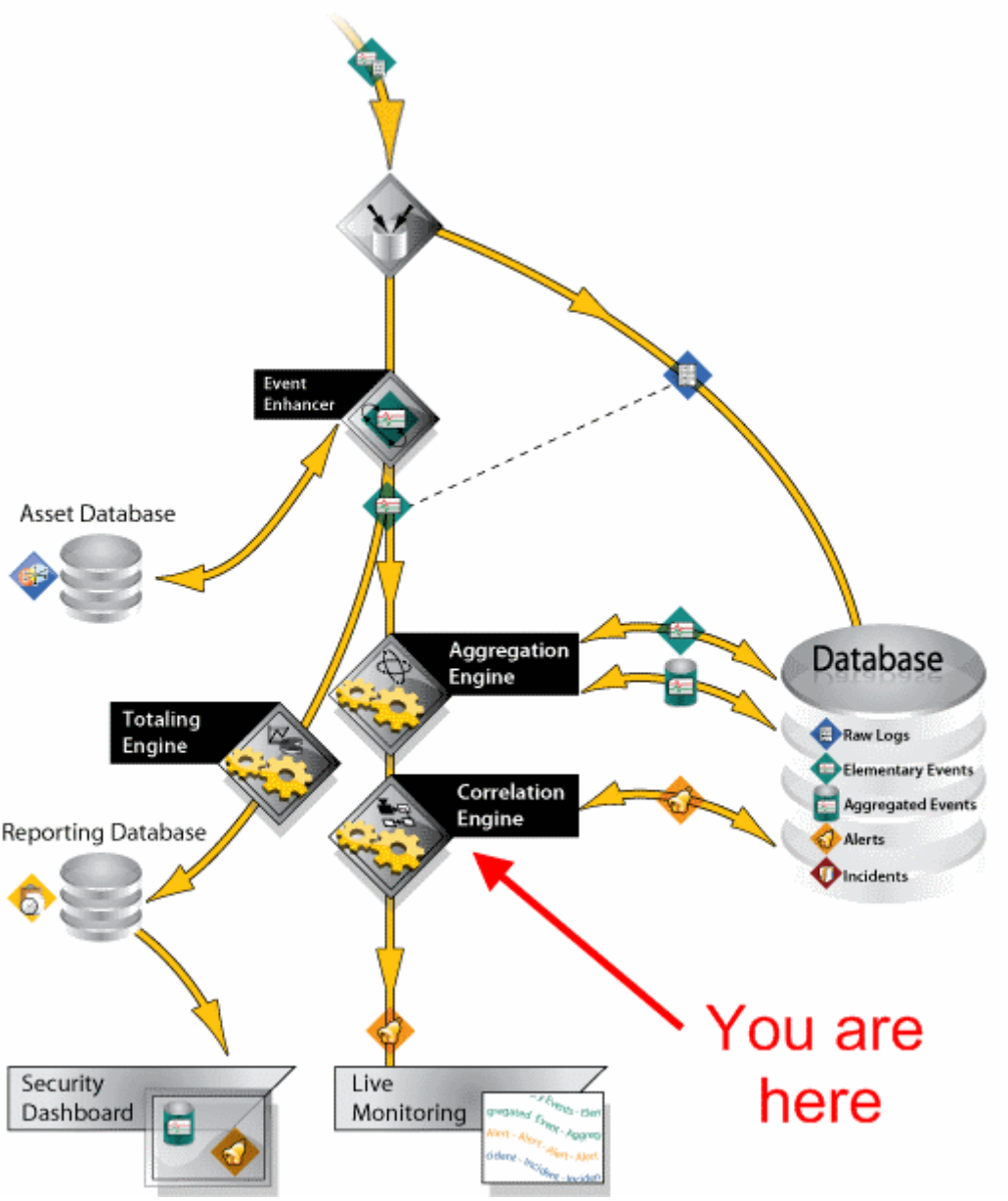
When the SMP receives an event (which has already been formatted in the IDMEF format by the Log Collector), it can extract information for statistics and reporting with the totaling engine and it can further process this information through the aggregation engine, synthetizing necessary information and discarding the remainder.

The aggregation engine analyzes incoming data and combines together similar elementary events into one aggregated event. Then, it will send the aggregated events to the correlation engine which will possibly correlate these events with other stored events to produce an alert or it may display this event as a sole component in an alert.

The correlation engine's procedure will depend on the rules and scenarios that have been previously configured by default or by the user.

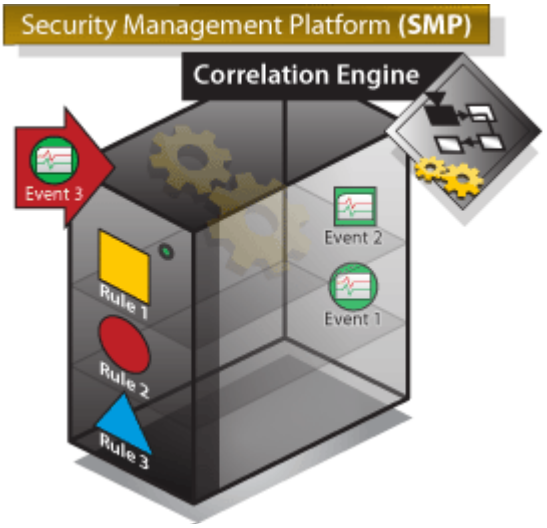
Graphical representation of the Three Engines

Figure 30 Three-engine Architecture

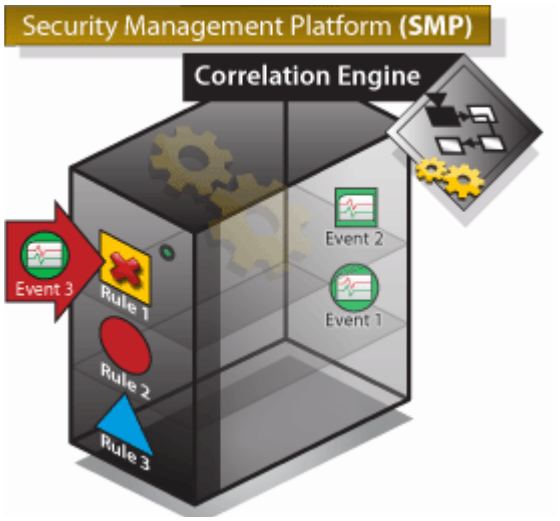


Schema of the Correlation Process

Inside the SMP correlation engine we find the SMP rules database. In our example, two events have already arrived at the engine and are pending.

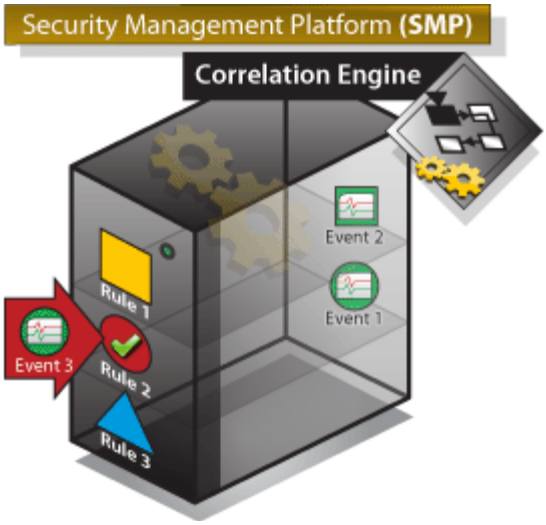


A new event arrives.



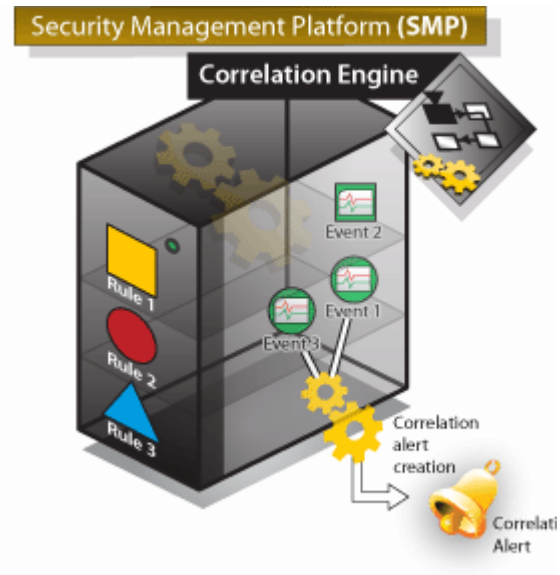
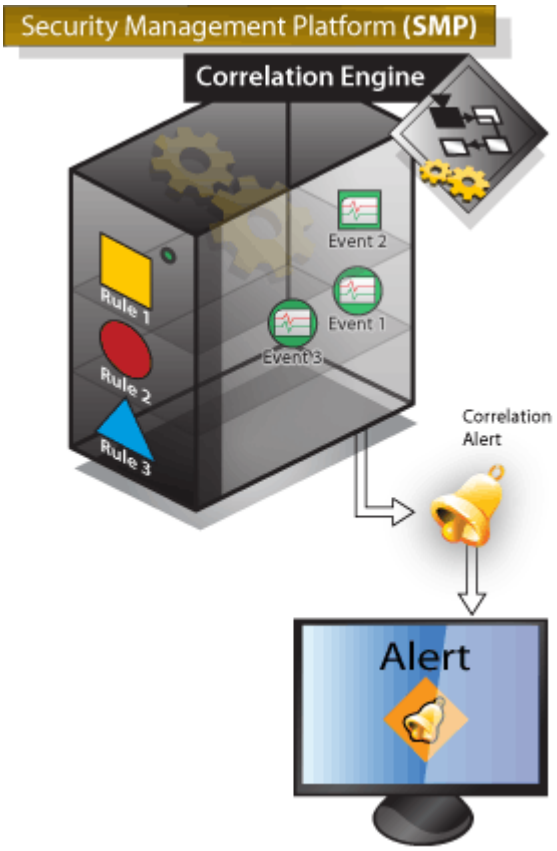
The SMP correlation engine compares information with the conditions in Rule 1, looking for a match.

No match is found with Rule 1.



The SMP correlation engine proceeds to compare information with the conditions in Rule 2.

A match is found with Rule 2.

<table>
<tr>
<td> 
</td>
<td> 
</td>
</tr>
<tr>
<td>For the purpose of this example, Rule 2 tells the SMP to create a correlation alert and stop the comparisons if a match is found. As a consequence, a correlation alert is created.</td>
<td>The corresponding alert is displayed in the GUI.</td>
</tr>
</table>

How to Correlate Events?

Deactivate the non Relevant Correlation Rules

When using the Security Event Manager application for the first time, all default correlation rules are activated. However, depending on the Information System, all the default correlation rules may not be needed (e.g. if you did not define any Domain Controller, the misuse and bypass are not relevant).

You must then deactivate some of them. To do so:

1. Go to **Event Management > Correlation Policy**.

2. Select the relevant checkboxes to deactivate the rules that are not needed (e.g. ADB - Misuse - Windows Domain Controller Output and ADB - Misuse - Windows Domain Controller Input) and click **Disable**.

3. Click **OK** to save the changes.

4. A message saying that the engine is not synchronized with the current policy is displayed. Click on the **synchronize** link.

Create a Correlation Rule

You can create your own correlation rule.

To create a new correlation rule, follow the procedure step-by-step.

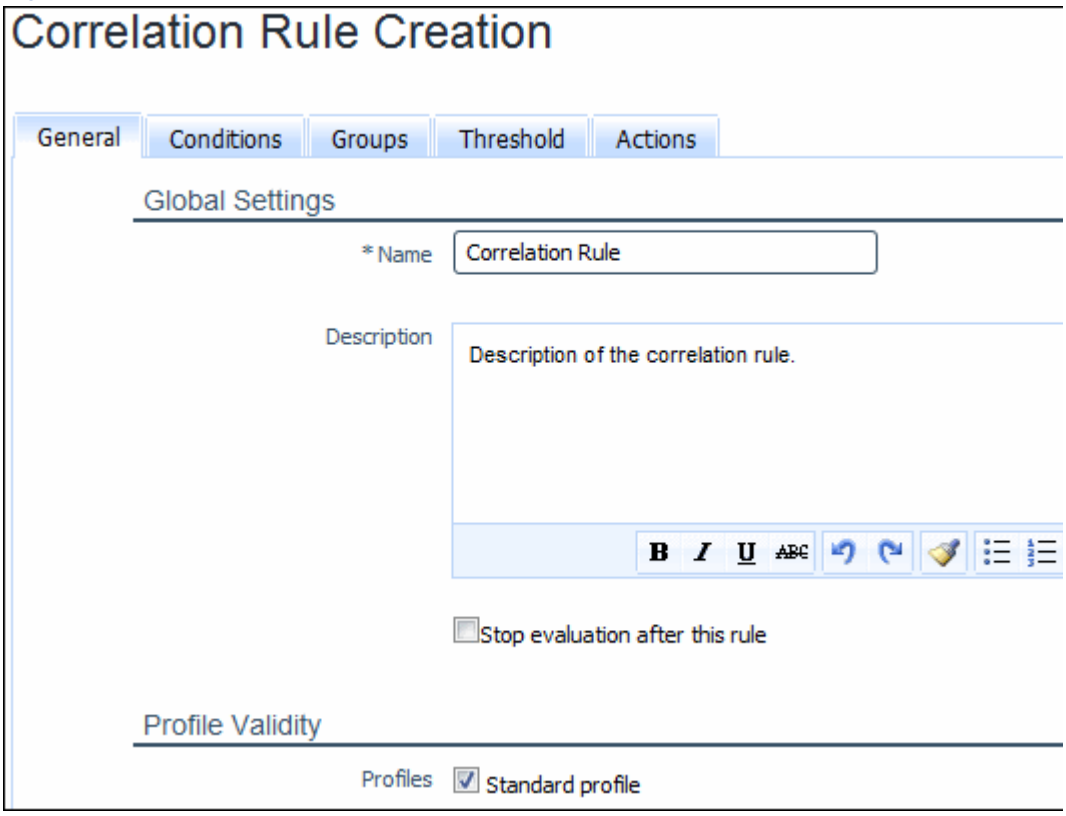
1. Select **Event Management** > **Correlation Policy**.
2. Click on the relevant button to create a new rule:
   - Either click on **Add** to create a completely new rule.

or

   - Select a checkbox in front of the rule you want to copy the information from and click on **Copy**. This action creates a copy of the rule entitled NameofRule _copy_1 which is added at the the very end of the table (click on the last arrow)
     

     .
1. Click the **Add** button. A screen like the following is displayed.

Figure 31 Correlation Rule General tab



Enter General Information

The **General** tab displays several fields described in the table below.

Table 7 Correlation rule - General Tab

Field	Description
Id	Every rule is given a unique id by the Security Management Platform.
Name	Every rule requires a unique name, specified by the administrator who creates it.
Description	User-entered description of the rule.

Table 7 Correlation rule - General Tab

Field	Description
Stop evaluation after this rule	If ticked, and if the rule is activated by an event, the event is not processed by subsequent rules. This is referred to as "cut" in the rule list.
Creation	The date and time that the rule was created and which user created it.
Last Update	The date and time the rule was last updated and which user updated it.
Profiles	Select in which security profiles this rule is active.

Define the Conditions and Exceptions of the Rule

Multiple conditions can be required to trigger the rule, add as many as required.

Exceptions are used to avoid triggering the rule when specified conditions occur. Specify exceptions in the same way as conditions.

Table 8 Correlation rule - Logical Expression

Field	Description
Logical Expression	Choose whether all conditions listed below are required to be matched or whether just one of them is enough. Select the logical expressions to make the conditions match. ▪ all conditions: means all conditions must be taken into account. ▪ any condition: means at least one condition must be taken into account. ▪ and ▪ no exception: means there is no exception to make the condition match. ▪ all exceptions: means all exceptions must be taken into account. ▪ any exception: means at least one exception must be taken into account.

1. Add the relevant conditions and/or exceptions by clicking **Add**. The **Add a new Condition/Exception** screen is displayed.

2. Select the type of condition/exception you want to use: either **Field Matching** or TIBCO LogLogic® Taxonomy.

- **Field Matching**: Specify the field contents in the event, e.g., Target hostname is "server1". Then several fields are displayed as described in the table below.
- TIBCO LogLogic® Taxonomy: Specify how the alert has been categorized, e.g., the action is ***malware*** and the target is a ***database***.

Table 9 Correlation rule - Add New Condition Fields

Field	Description
Multiple selector	There are two options: “any value of this field” and “all values of this field.” Select “any value of this field” when it suffices for only one element in the field to match the Matching Value. Select “all values of this field” when all elements in the field must match the Matching Value.
Matching field	Select which field in the event is to be checked in the **Matching field** drop-down list. If you select a TIBCO LogLogic® Taxonomy matching field, ONLY a **number (or ID)** found in the relevant ruleset file and corresponding to the Taxonomy field can be entered in the **Matching Value** field below. A text string will not be taken into account.
Negate	If set, the logic is reversed - e.g., to look for events which is not authentication
Matching type	Specify which type of test is to be performed

Matching Value	Specify the value to be tested.
	The value MUST be a number if you previously selected a TIBCO LogLogic® Taxonomy **matching field.**
	▪ Additional data: you must specify the value with the following format:
	`“my addData meaning=my addData value”.`
	For a test of authentication:
	`“rulesetName=esmp_auth.rules”`
	▪ DetectTime: the format is Tue May 13 11:50:06 CEST 2008.
	To search correlated alerts on a specific date: ".* May 13 .* 2008".
	Note: The field is not case sensitive.

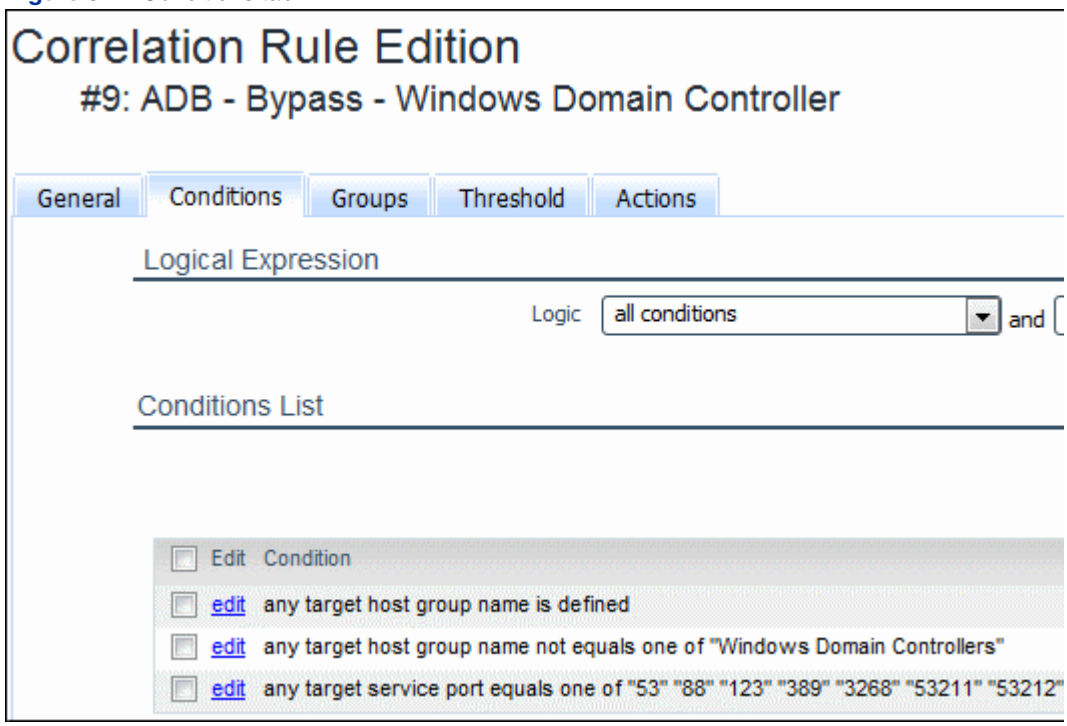
3. Click **OK**.

Example with a Default Correlation Rule

Let us take the example of the default correlation rule entitled **ADB-Bypass-Windows Domain Controller**.

If you click on its name to edit it, you will obtain the following screen.

Figure 32 Conditions tab



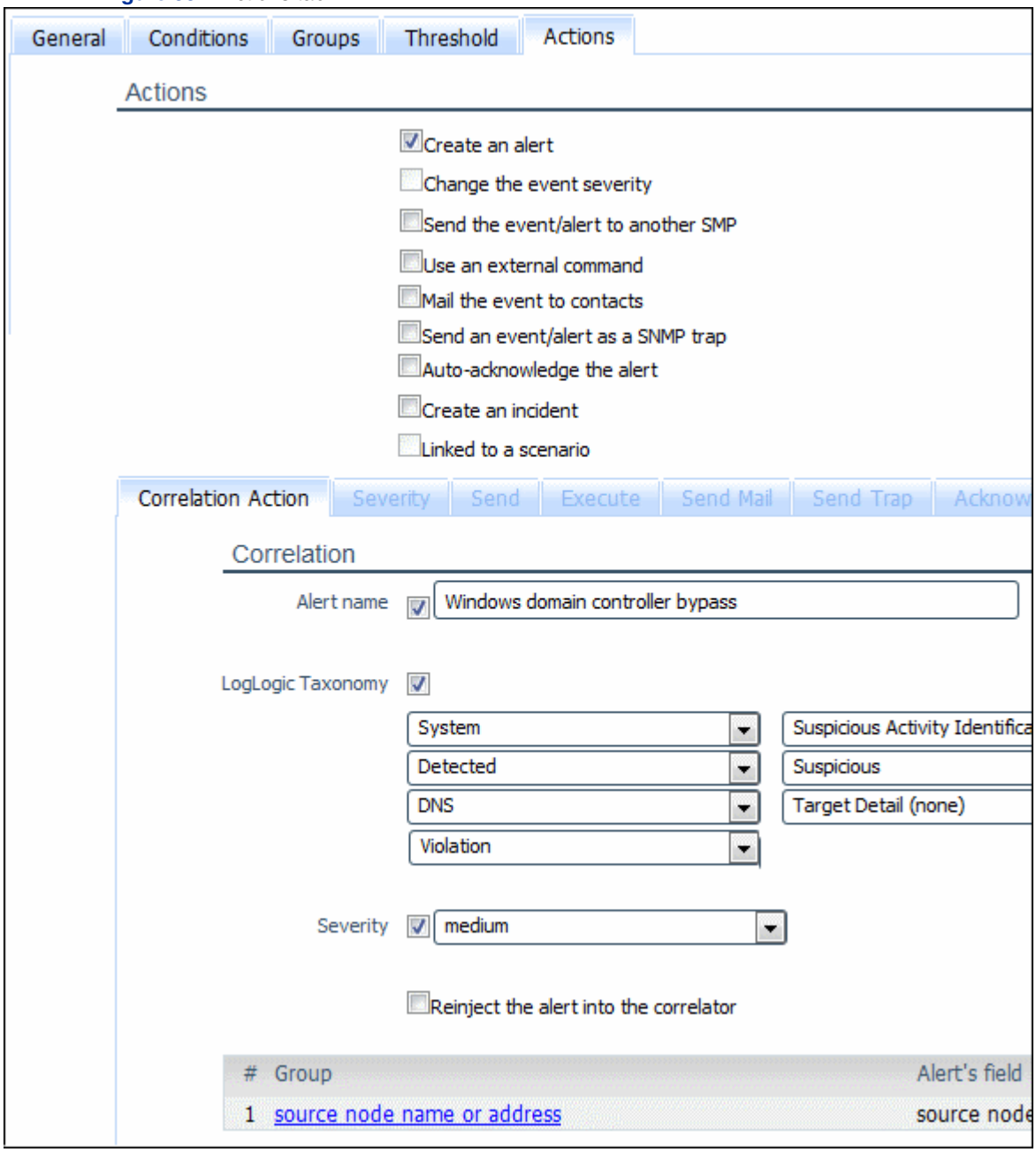
The rule detects all the events whose target is a host.

The host is in a host group that does not contain the name Mail (e.g. Mail server) in its name. The event refers to a connection to a known mail port.

This rule prevents from the risk of a fraudulent mail server in the customer's Information System (not monitored by the site network administrator and by SEM) which sends/receives mails in the client network.

Then when you click on the **Actions** tab, you will see details of the rule.

Figure 33 Actions tab



The risk is described as a detected suspicious violation of a mail, which is described in the Taxonomy.

As this is a known risk, the engine creates an alert called "Mail server bypass" with a medium priority to make the analyst investigate the problem.

Limitations

A mismatch may occur when defining correlations policies' conditions and exceptions as in the following example:

Let us suppose:

- Two Elementary Events (EE)
  - EE1 containing fields hostname = Administrator and user = User A.
  - EE2 containing fields hostname = Administrator and user = User B.
- An Aggregation rule (AR)
  - With a condition saying that EE1 and EE2 are grouped when the field hostname = Administrator.
- A correlation rule
  - With a condition saying that an Aggregated Event (AE) creates an alert except if one of the user is User B.

Description

EE1 is matching **AR** for 100 seconds during which an Aggregated Event (**AE**) containing values **Administrator** and **User A** is created. Then a Correlation Alert (**CA**) is created.

At the same time, **EE2** also matches **AR** because of the value **Administrator** . **EE2** enters into **AE**.

EE2 then should not be taken into account in **CA** because of the exception ignoring value **User B**. However, in this case, **CA** will contain values **Administrator**, **User A** but also an aggregated event containing the value **User B** forbidden by the rule.

> **Note:** Should **EE2** be processed before **EE1**, the behavior would be the expected one.

Define the Grouping Process

This type of rules enables the system to detect the common values of the fields contained in several Elementary Events.

For example, ***Corr. - Login Success*** detects that a user logged successfully on the server.

Associated with the rule called ***Corr. - Login Failed,*** the scenario ***Suspected bruteforce*** can be triggered.

To define how data will be grouped.

1. Click on the **(none)** entry. The **Group Field** pane is displayed.

2. Select the name of the field on which the grouping is performed. Refer to the ***Default Content*** section in the ***Reference Guide*** to get the full list of grouping fields.

3. Select the **Field's value Required** checkbox if only events with a defined field's value must be grouped.

4. Select a value in the **Grouping method** drop-down list. This information allows the creation of **one group** containing different elements from several incoming events. You can choose among the options described below:

- **same field values:** grouping is performed if at least one event field's value is the same as another one from a different event.
- **same split field values**: the principle of this grouping method is the same as that of the **same field values** option except that only the common value between several event's fields is kept as reference for the creation of a group.
- **distinct field values**: grouping is performed by adding all the different field's values from several events into only one group.

5. If you selected **distinct field values**, the **Minimum number of distinct values** field is displayed. Enter the minimum number of fields to add in the group to allow the creation of an alert.

6. Click **OK**.

7. In the **Groups** tab, indicate the processing order of rules by checking the relevant rule and clicking on **Move Up** or **Move Down**.

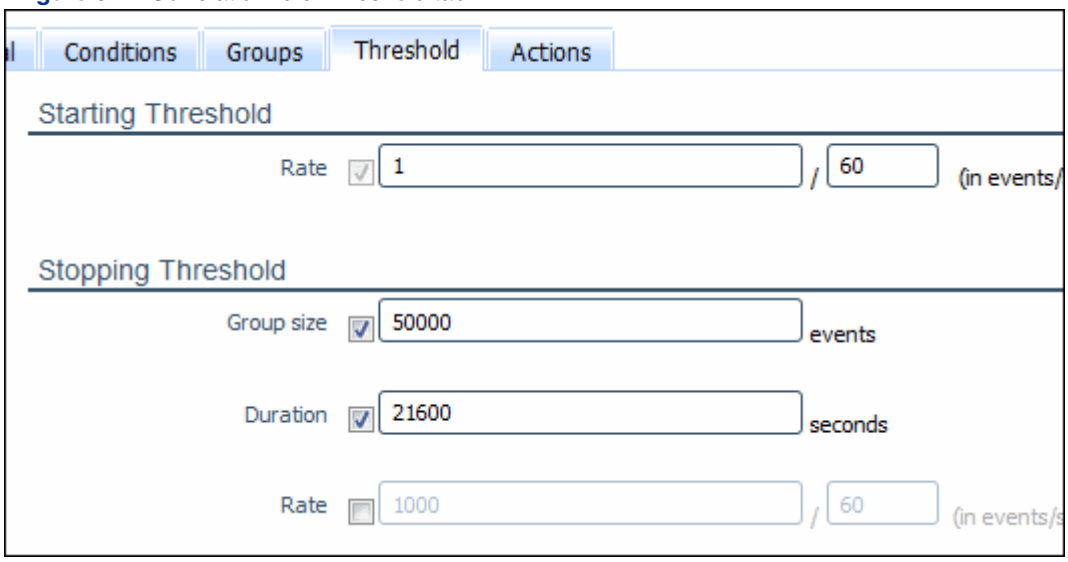
Define the Threshold for the Correlation Process

The threshold tab allows you to specify under which conditions a rule would be triggered, that is, to combine events into a single alert.

For example, the number of events that have to occur within a specified time period could be set as a threshold. If this condition was met, the events would be combined into a single alert.

For example, the threshold properties are the following:

Figure 34 Correlation rule Threshold tab



Note that when you select several checkboxes, it means that you define several possibilities to stop the aggregation process. They are not combined and the first to be met stops the process.

Table 10 Correlation - Threshold Tab

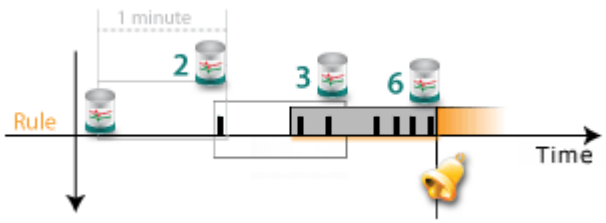
Property	To specify...
Starting Threshold	
Rate	the minimum number of events per defined interval (per second) needed to trigger a correlation process. Example with a rate set at 6/3600: 
Stopping Threshold	

Table 10 Correlation - Threshold Tab

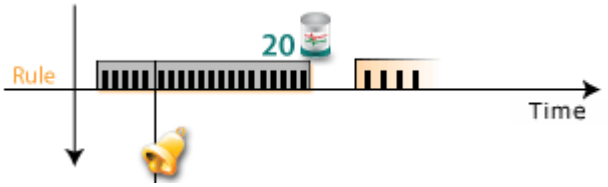
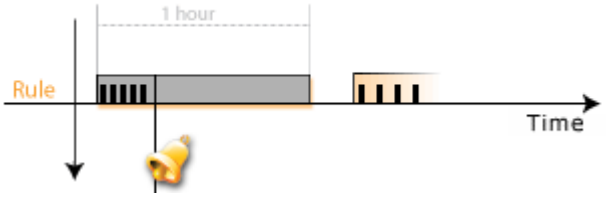
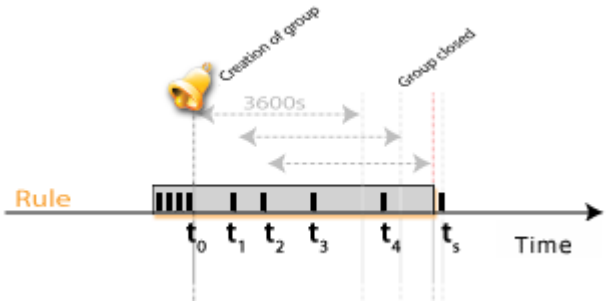
Property	To specify...
Group size	the maximum number of events to group into a single event/alert. If matching events are received after the maximum threshold has been reached, then a new event is created. By default, the maximum number of events is set at 50000. Example with a group size set at 20: 

Table 10 Correlation - Threshold Tab

Property	To specify...
Duration	the time frame (in seconds) for considering an event or alert for aggregation or correlation in a specific event/alert. For example, you could specify that an event or alert would not accept any further events/alerts 10 seconds after its creation. By default, the duration is set at 3600. Example with a duration set at 3600: 
Rate	the minimum number of events per defined interval (per second) under which to stop an aggregation or correlation process. Example with a rate set at 4/3600: ▪ t0 = time of creation of a group. ▪ t0 + 3600 = time before which at least 4 elementary events must have entered the group. ▪ t1, t2, t3, t4, t5 = elementary events entering the group. This group will be closed if it has not reached the minimum number of elements (4) in the time limit (3600s) to "stay alive".  Note: Usually, if the **Rate** checkbox is selected, the **Group size** and **Duration** checkboxes are not used.

Define the Correlation Action

Figure 35 Correlation Action tab

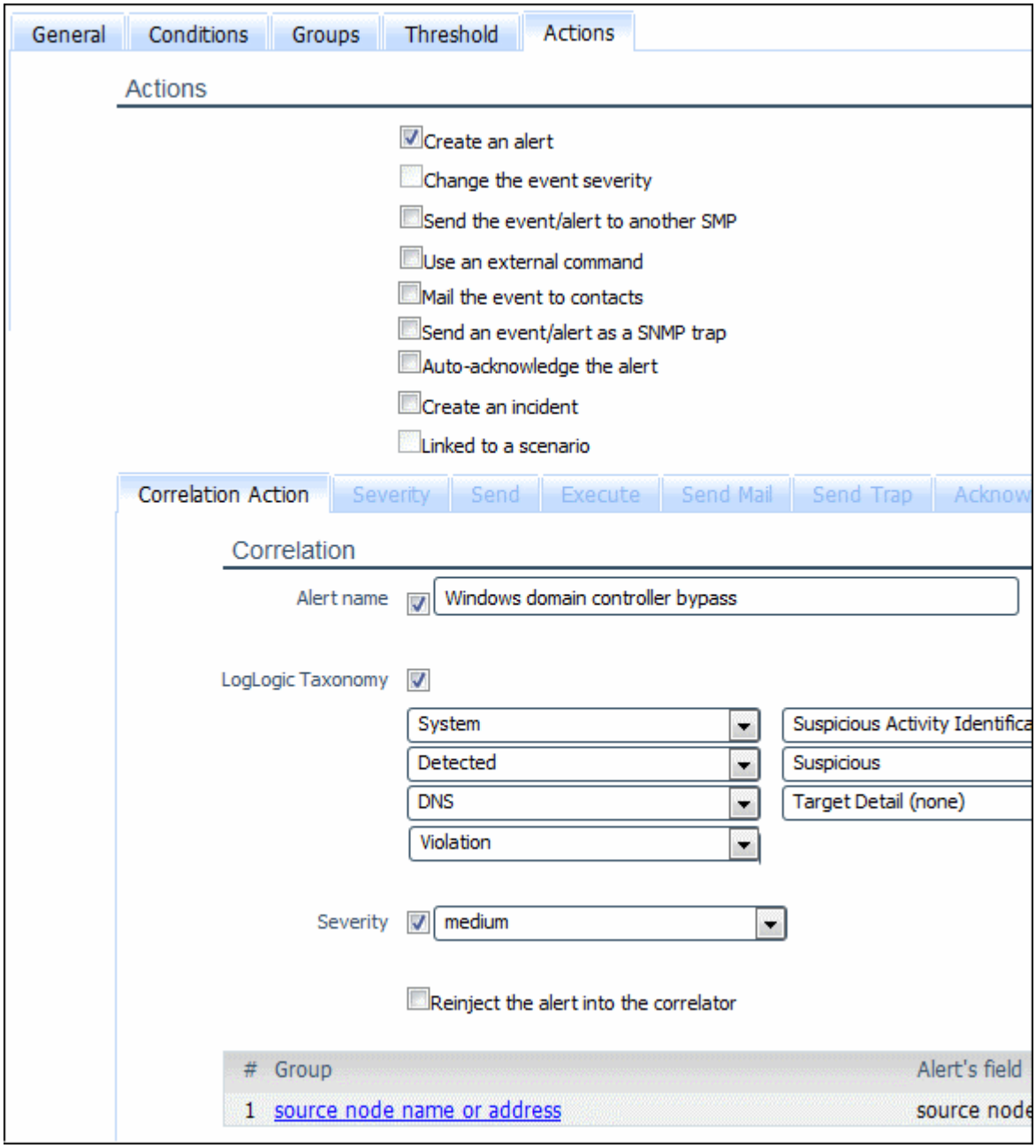


Table 11 Actions pane

Checkbox	Description
Create an alert	Creates an alert when the rule is triggered.
Change the event severity	Changes the event severity when the rule is triggered. Only available if the **Create an alert** checkbox is NOT selected.
Send the event/alert to another SMP	Sends an alert or event from one SMP to another one if you installed multiple SMPs.

Table 11 Actions pane

Checkbox	Description
Use an external command	Specifies the command to execute. The command will run in the context of the "TIBCO LogLogic®" account on the Security Management Platform.
Mail the event to contacts	Defines the group of contacts to whom you will automatically send an E-mail regarding the events.
Send an event/alert as SNMP trap	Generates an SNMP (Simple Network Management Protocol) trap and sends it to a specified IP address or host name.
Auto-acknowledge the alert	Acknowledges an alert that will not be listed on the "current alerts" display. Auto-acknowledged alerts are typically archived for future forensic work. Only available if the **Create an alert** checkbox is selected.
Create an incident	Creates automatically an incident from the alert.
Linked to a scenario	If a rule is already allocated to a scenario, the **Linked to a scenario** checkbox is automatically selected and a pane with the name of the scenario is displayed. You cannot configure this option.

General Behaviors:

If you select the **Create an alert** checkbox along with another possible action, the action will be performed on the alert only once.

E.g. Let us suppose the expected action is **Use an external command**. If a correlation alert is created, the script will be executed once (and only once) when the alert is created.

If you do NOT select the **Create an alert** checkbox but a possible action, then the action will apply on all the aggregated events each time conditions are matched.

E.g. Let us suppose the expected action is **Use an external command**. When the rule is triggered, the script will be executed as many times as the number of aggregated events contained in the aggregate (e.g. threshold set to 10 events: when the rule is triggered, the script is executed 10 times).

Create an alert

To create an alert:

1. Enter the alert's name. The text string will be displayed on the alerts screen.

2. Select the TIBCO LogLogic® Taxonomy or categories that can be used to match this new alert, with other rules that match by categories.

> **Note:** If you selected TIBCO LogLogic® Taxonomy **- (all fields)** in the **Groups** tab, the TIBCO LogLogic® Taxonomy checkbox is automatically selected.

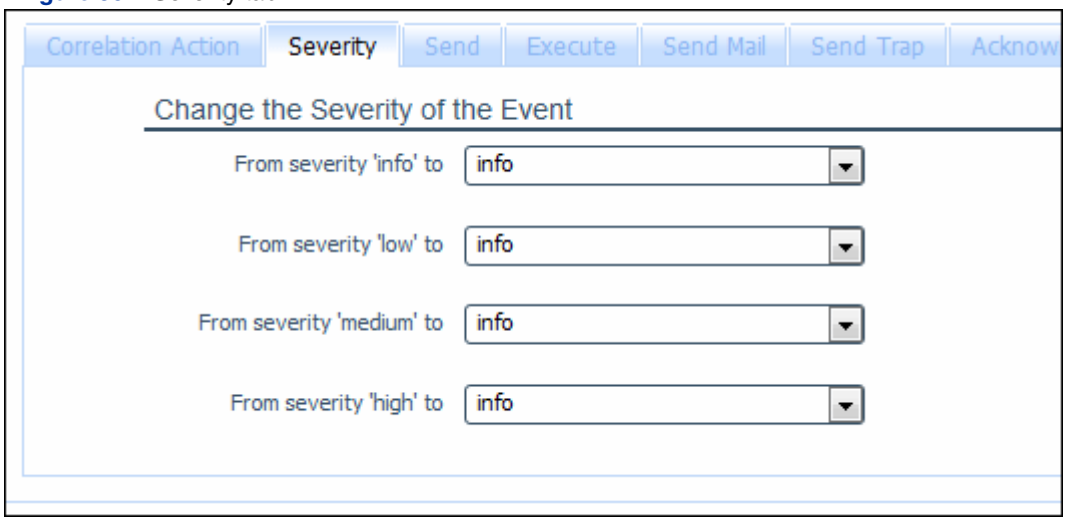
3. Select the severity of the new alert.

4. Indicate if the alert must be processed again by the correlation by selecting the **Reinject the alert into the correlator** checkbox. Then, a new aggregated event will be created.

5. Specify the fields that will be available for correlation.

Change the event severity

Figure 36 Severity tab



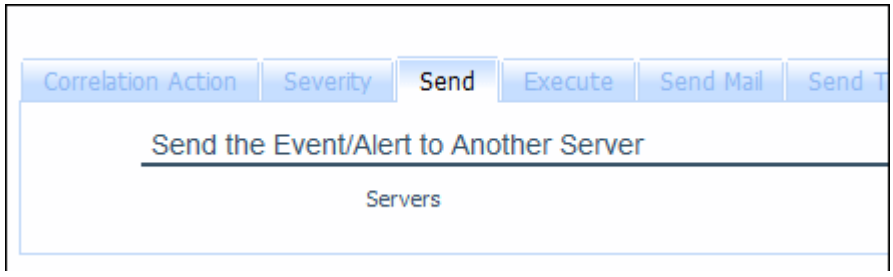
To change the new event severity:

- select the relevant severity in the drop-down lists.

Send the event/alert to another SMP

In the event of a multiphe instances configuration when several SMPs are connected, you can automatically send an event/alert to another SMP. Please refer to the ***Administration Guide*** for more information about the communication between several SMP servers.

Figure 37 Send tab

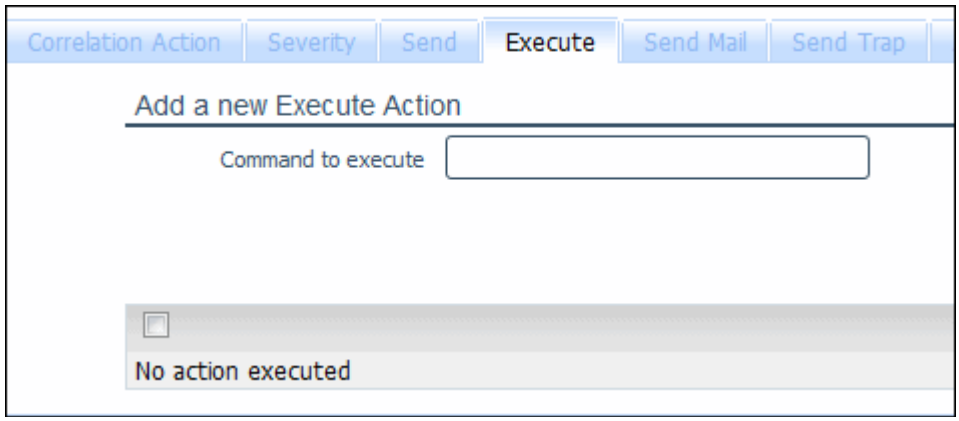


To send the event/alert to another SMP:

- select the target server.

Use an external command

Figure 38 Execute tab



To make this action efficient, please read carefully the following instructions:

In a shell:

- You must configure the user's permission to start the script.
Example: `[root@hostname script]# chmod +x ./command.pl`
- It is advised to specify the group and owner of the script as **exaprotect:exaprotect**.
Example: `[root@hostname script]# chown exaprotect:exaprotect ./command.pl`

In the interface:

- The command to execute (or script) must be located under home/exaprotect/scripts/.
- You must enter the file name in the **Command to execute** field (for example `command.pl`).

> **Note:** The SMP is executing external scripts with TIBCO LogLogic® user rights.

Mail the event to contacts

Figure 39 Send Mail tab

To configure the E-mail:

1. Configure default `exa_mail.properties` files that contain all the mail sending process configuration data.

> **Caution:** Please refer to the **Administration Guide** to learn how to precisely configure the sending of the mail (see *Sending Mails as Soon as an Event Occurs* section).

2. Enter the e-mail subject and add a comment.

3. Select the type of contacts to whom you want to automatically send the E-mail: either contacts assigned to the source, to the target, to the log source or to other contacts. You can configure these contact groups under the **Asset Database > Contact Groups** screen.

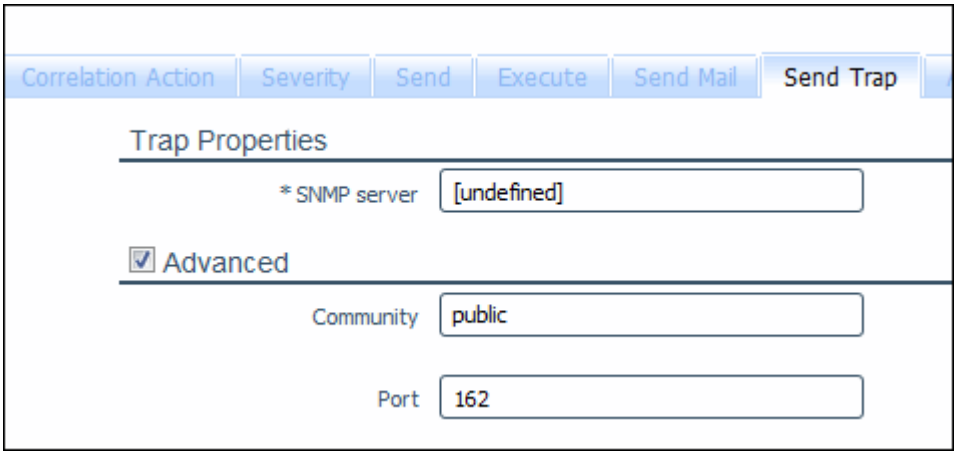
The sent mail generally looks like the following example:

```
SSH Remote root login
************************
Dates
 * Creation: 2007-05-07 16:26:30
 * Detection: 2007-05-07 16:26:29
 * Analyzer: 2007-05-07 16:26:30
************************
Alert Info
 * Alert Ident: 410
 * Action Category: Authentication Activity
 * SubAction Category: Session
 * Target Object Category: SSH
 * Target Attribute Category: Admin
 * State Category: Success
 * Kind: normal
 * Computed Severity: medium
************************
Analyzer #1
 * Analyzer ID: ESMP
 * Name: ESMP
 * Model: ExaLogConverter
 * Version: 1.0
 * Class: relay
 * Os Type: Linux
 * Os Version: 1.0
************************
Assessment
 * Impact
  - Severity: medium
  - Type: admin
  - Completion: succeeded
  - Description: see below
---%<---%<---%<---%<---%<---%<---%<---%<---%<---%<---%<---%<---%<---%<---%<---%<
Root logged in from 192.168.10.21:1523 using the password method ---%<---%<---%<---%<---%<---
%<---%<---%<---%<---%<---%<---%<---%<---%<---%<---%<
************************
Source #1
 * Node
  - Category: dns
  - Name: username
  - Address #1
   + Category: ipv4-addr
   + Address: <span style="white-space: nowrap;">192.168.10.21</span><br/><I style="white-
space: nowrap ;">( username.ept.<a HREF='Whois.jsp?TARGET=exaprotect.net'
TARGET=_blank>exaprotect.net</a>)</i>
 * Service
  - Port: 1523
  - Protocol: tcp
************************
Target #1
 * Node
  - Category: dns
  - Name: localhost
 * User
  - UserId #1
   + Name: root
 * Service
  - Port: 22
  - Protocol: tcp
************************
Additional Data
 * Log received from: /var/log/messages
 * rulesetName: ssh.rules
 * regexId: 1
            ************************
```

Figure 40 Example of a Sent Mail

Send an event/alert as SNMP trap

Figure 41 Send Trap tab



To generate an SNMP (Simple Network Management Protocol) trap and send it to a specified IP address or host name:

1. Enter either the IP address in dotted decimal format or the host name of the system to which you want to send an SNMP trap when an associated event occurs.
2. Enter the community name used by the destination host in the **Community** field. By default, the value is set to "public". It corresponds to the default installed account.
3. In the **Port** field, enter the port to which the **SNMP** server listens to.

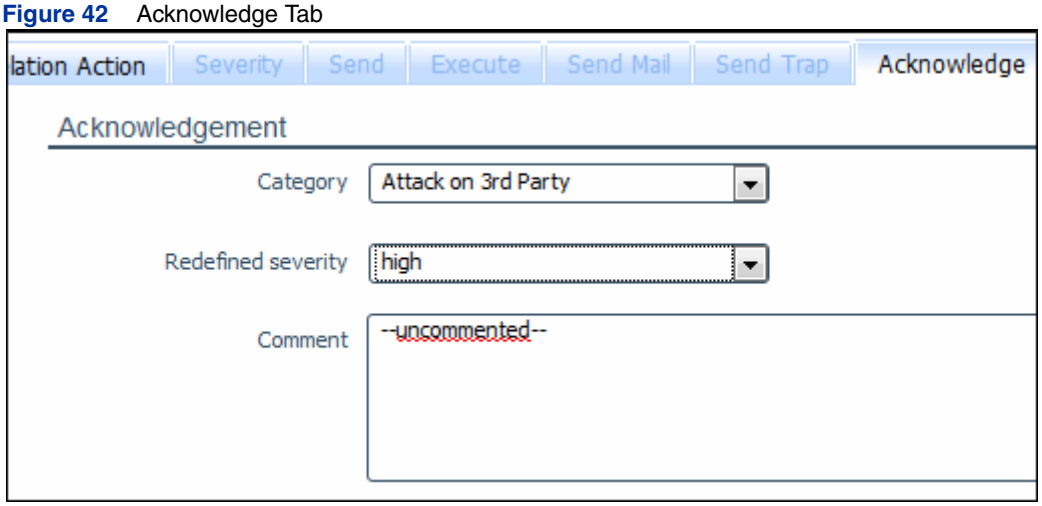
Here is an example of the syntax for a sent SNMP trap.

```
Dec  8 15:51:26 localhost snmptrapd[3684]: 192.168.10.221: Enterprise
Specific Trap (534) Uptime: 4:45:13.92, SNMPv2-MIB::sysDescr.0 =
STRING: id=594;alert=Root login;severity=medium;target0_name=local-
host;analyzer0_address0=192.168.11.110;analyzer0_name=esmp
```

It is not possible to configure content and syntax. However, this message allows you to know the alert's name, its severity, the alert's target, etc.

Auto-acknowledge the alert

Figure 42 Acknowledge Tab



To acknowledge an alert automatically:

1. Select the type of alert in the **Category** drop-down list. This field is used by the reporting module to show what type of alerts are being generated.

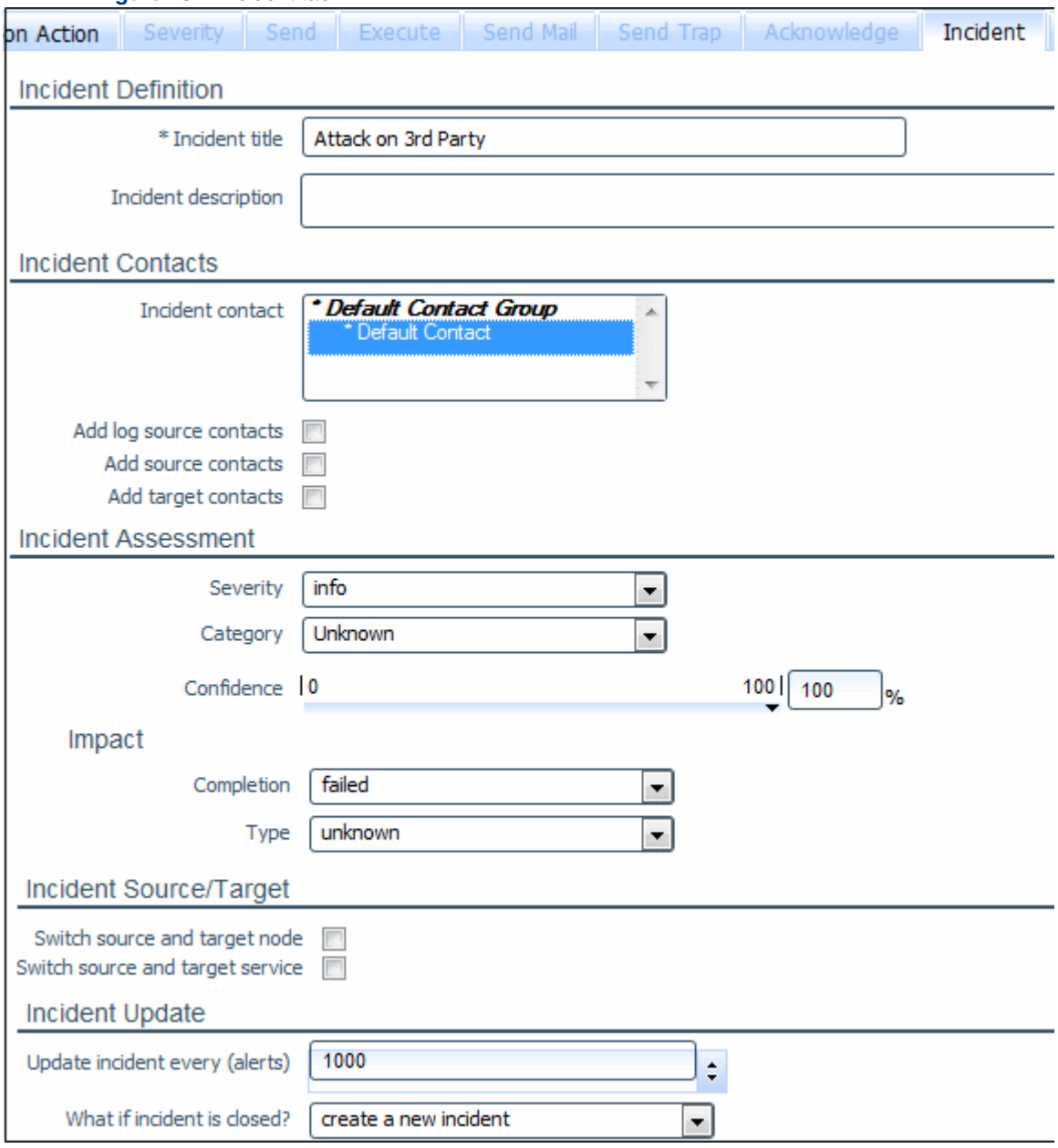
2. Select the severity for the alert in the **Redefined Severity** drop-down list. This will lower the confidence rating in the analyzer.

3. Enter a comment regarding the alert and the auto-acknowledgement.

Create an incident

Caution: Make sure you only have a limited number of incidents. Otherwise, the correlator may be slow in processing the alerts.

Figure 43 Incident tab



The new alert can automatically create an incident with the following properties:

Table 12 Incident Tab

Field	Description
Incident title	The title is displayed in the list of incidents and is used to reference the incident.
Incident category	Select the incident's category.
Incident description	Space for a description of the alert and why an incident was automatically created.
Incident contact	Select the previously defined contact to be marked as responsible for handling the incident.

Table 12 Incident Tab

Field	Description
Update incident every (alerts)	To send an update to the Incident Management System every X alerts (i.e., to avoid sending a modification each time the incident is updated). The default value is 1000. **Caution:** If the value is set to 1, the correlator may be slow in processing the alerts: they will be processed one by one.
Add log source contacts	If selected, the contacts responsible for the log source device will also be marked as responsible for the incident.
Add source contacts	If selected, the contacts responsible for the source host of the alert will also be marked as responsible for the incident.
Add target contacts	If selected, the contacts responsible for the target host will also be marked as responsible for the incident.
Severity	Select the severity level of the incident; leave blank to use the severity level of the alert.
Switch source and target node	Tick this box if the event's source should be recorded as the incident's target and vice versa.
Switch source and target service	Tick this box if the event's source should be recorded as the incident's target and vice versa.
Assign fields	Select which fields are passed as details.
What if incident is closed?	Select the type of scenario that should be applied if the incident is closed when new alerts are received: ▪ create a new incident in which the alerts will be stored ▪ add new alerts to the same incident even if it is closed ▪ add new alerts in the re-opened incidents ▪ keep as it is and lose the alerts.

Linked to a scenario

If a rule is already allocated to a scenario, the **Linked to a scenario** checkbox is automatically selected and a pane with the name of the scenario is displayed.

Create a Correlation Scenario

Scenarios are used to describe more complex situations requiring multiple actions that simple rules alone cannot manage to describe. A scenario is triggered when its rules are triggered. Scenario rules may be "required," "optional," or "exclusion." The scenario is triggered if the required rules are triggered, and the exclusion rules prevent the scenario from being triggered. Optional rules are useful for including extra evidence in the scenario.

Example of a Bruteforce Attack

We will consider a bruteforce attack when:

- More than two logins are "failed" on the same user name and on the same host.
- A login is "succeeded" on the user name on the previous host.

Define each correlation rules that must be triggered

1. Decompose the scenario into steps that the user must perform.

2. Create the rules. To ease the tracking in the event monitoring tab, generate an alert for each step.

3. Save your correlation rules by clicking **OK**.

4. Go to **Configuration > SMP Monitoring > Engine Management** tab and click on **Restart all Engines** to synchronize the correlation engine.

Create the Scenario

1. Click on the Scenario tab under the Correlation policy tab.

2. Enter a name and description.

3. Select in which security profiles this rule is active.

4. Click on the Selected Rules tab.

5. Select the matching rules that must be triggered in order for the scenario to be triggered in the **Required Rules** section. Click Change to select or deselect rules that must match.

6. Select the optional rules which are not required to trigger the scenario, but which can provide more information in the scenario alert in the **Optional Rules** section.

7. Select if at least one of the exception rules is triggered within the scenario threshold, the scenario is prevented from triggering for at least the threshold number of seconds in the **Exception Rules** section.

8. Select the matrix that shows which information items relate to which rule(s) in the **Fields Matching Matrix** section.

9. Enter a value in the **Duration** field. The duration is the time frame (in seconds) for considering an event or alert for aggregation or correlation. For example, you could specify that a rule would be triggered ten seconds after its creation.
By default, the duration is set at **3600**.

10. Enter the actions to be performed once the scenario is triggered. The procedure is the same than the procedures in correlation rules.

Test your correlation scenario

1. Fail multiple logins from your host on the root account of the web server.

2. Check that your alert is generated.

3. Succeed a login on the root account of the web server.

4. Check that both “your” second alert and the BruteForce scenario alert are generated.

List of Default Correlation Rules

The set of correlation rules per group is listed below.

Table 13 Asset Database Rules

Name	Description	Alert's Name	Alert's Severity
1 - ADB - Misuse - Windows Domain Controller Output	The rule controls that hosts from the "Windows Domain Controllers" host group use only authorized services. Only the following services are allowed from a "Windows Domain Controllers" host: ▪ DNS (53 tcp/udp) ▪ Kerberos (88 tcp/udp) ▪ NTP (123 udp) ▪ LDAP (389 tcp/udp) ▪ Global Catalog LDAP (3268 tcp) ▪ AD Replication (53211 tcp) ▪ File Replication Service (53212 tcp) An alert is raised if any other service is used from a "Windows Domain Controllers" host.	Windows domain controller misused	
2 - ADB - Misuse - Windows Domain Controller Input	The rule controls that hosts from the "Windows Domain Controllers" host group are only used for what they are designed for. Only the following services are allowed on a "Windows Domain Controllers" host: ▪ DNS (53 tcp/udp) ▪ Kerberos (88 tcp/udp) ▪ NTP (123 udp) ▪ LDAP (389 tcp/udp) ▪ Global Catalog LDAP (3268 tcp) ▪ AD Replication (53211 tcp) ▪ File Replication Service (53212 tcp) An alert is raised if any other service is used on "Windows Domain Controllers" hosts.	Windows domain controller misused	
3 - ADB - Misuse - Mail Server Output	The rule controls that hosts from the "Mail Servers" host group use only authorized services. Only the following services are allowed from a "Mail Servers" host: ▪ SMTP (25 tcp) ▪ POP3 (110 tcp) ▪ IMAP (143 tcp) ▪ IMAPS (993 tcp) ▪ POP3S (995 tcp) An alert is raised if any other service is used from a "Mail Servers" hosts.	Mail Server Misused	

Table 13 Asset Database Rules

Name	Description	Alert's Name	Alert's Severity
4 - ADB - Misuse - Mail Server Input	The rule controls that hosts from the "Mail Servers" host group are only used for what they are designed for. Only the following services are allowed on a "Mail Servers" host: ▪ SMTP (25 tcp) ▪ POP3 (110 tcp) ▪ IMAP (143 tcp) ▪ IMAPS (993 tcp) ▪ POP3S (995 tcp) An alert is raised if any other service is used on "Mail Servers" hosts.	Mail Server Misused	
5 - ADB - Misuse - Web Proxy Output	The rule controls that hosts from the "Web Proxys" host group use only authorized services. Only the following services are allowed from a "Web Proxys" host: ▪ HTTP (80 tcp) ▪ HTTPS (443 tcp) An alert is raised if any other service is used from a "Web Proxys" hosts.	Web Proxy Misused	
6 - ADB - Misuse - Web Proxy Input	The rule controls that hosts from the "Web Proxys" host group are only used for what they are designed for. Only the following services are allowed on a "Web Proxys" host: ▪ HTTP (80 tcp) ▪ HTTPS (443 tcp) ▪ SQUID (3128 tcp/udp) An alert is raised if any other service is used on a "Web Proxys" hosts.	Web Proxy Misused	
7 - ADB - Misuse - Corporate Application Servers	The rule controls that hosts from the "Corporate Application Servers" host group are only used for what they are designed for. Only the following services are allowed on a "Corporate Application Servers" host: ▪ HTTP (80 tcp) ▪ HTTPS (443 tcp) An alert is raised: ▪ if any other service is used on a "Corporate Application Servers" hosts ▪ and if the host IP address corresponds to private address (RFC 1918)	Web Server Misused	

Table 13 Asset Database Rules

Name	Description	Alert's Name	Alert's Severity
8 - ADB - Misuse - Instant Messaging	The rule controls that hosts from the "Mail Servers" host group (or any defined corporate instant messaging server) are only used for what they are designed for. Only the following services are allowed on a "Mail Servers" host: ▪ IRC (113 udp, 194 udp, 6660 to 6669 tcp) An alert is raised if any other service is used on a "Mail Servers" hosts.	Instant Messaging Misused	
9 - ADB - Bypass - Windows Domain Controller	The rule controls that "Windows Domain Controllers" services are provided by well known servers, defined in the asset database. An alert is raised when a host not linked to the "Windows Domain Controllers" host group provides one of the following services: ▪ DNS (53 tcp/udp) ▪ Kerberos (88 tcp/udp) ▪ NTP (123 udp) ▪ LDAP (389 tcp/udp) ▪ Global Catalog LDAP (3268 tcp) ▪ AD Replication (53211 tcp) ▪ File Replication Service (53212 tcp)	DNS Assets Bypass	
10 - ADB - Bypass - Mail Server	The rule controls that "Mail Servers" services are provided by well known servers, defined in the asset database. An alert is raised when a host not linked to the "Mail Servers" host group provides one of the following services: ▪ SMTP (25 tcp) ▪ POP3 (110 tcp) ▪ IMAP (143 tcp) ▪ IMAPS (993 tcp) ▪ POP3S (995 tcp)	Mail Server Bypass	
11 - ADB - Bypass - Web Proxy	The rule controls that "Web Proxys" services are provided by well known servers, defined in the asset database. An alert is raised when a host not linked to the "Web Proxys" host group provides one of the following services: ▪ Web Proxy (8080 tcp) ▪ SQUID (3128 tcp/udp)	Web Proxy Bypass	

Table 13 Asset Database Rules

Name	Description	Alert's Name	Alert's Severity
12 - ADB - Bypass - Corporate Application Servers	The rule controls that "Corporate Application Servers" services are provided by well known servers, defined in the asset database. An alert is raised when... ▪ a host is not linked to the "Corporate Application Servers" host group ▪ and the host IP address corresponds to RFC 1918 .... provides one of the following services: ▪ HTTP (80 tcp) ▪ HTTPS (443 tcp)	Web Server Bypass	
13 - ADB - Bypass - Instant Messaging	The rule controls that "Instant Messaging" services are provided by well known servers, defined in the asset database. An alert is raised when a host not linked to the "Mail Servers" host group (or any define instant messaging host group) provides one of the following services: ▪ IRC (113 udp) ▪ IRC (194 udp) ▪ IRC (6660 to 6669 tcp)	Instant Messaging Bypass	
14 - ADB - Cleartext Authentication Protocol	The rule controls that no cleartext authentication protocol is used on internal hosts. An alert is raised when a user authenticates himself on a host (linked to a defined host group) with one of the following protocols: ▪ Telnet (23 tcp) ▪ HTTP (80 tcp)	Unauthorized cleartext authentication protocol	
15 - ADB - Unauthorized Administration Stations	The rule controls that every IT administration task is performed from authorized "Administration Station". An alert is raised if a user authenticates himself ▪ on a defined host ▪ from a host not included in "Administration Station" host group ▪ with a protocol different from SSH or MS TSC	Unauthorized administration stations detected	
16 - ADB - Threat on Vulnerable Target	Detected attacks on target known to be vulnerable. A previous vulnerability scanner found vulnerability for the target and set the "target assessment" field to "vulnerable".	Known vulnerability exploited	

Table 14 Threshold Rules

Name	Description	Alert's Name	Alert's Severity
17 - Threshold - Information Threshold	The rule raises an alert when the same event occurs too many times and is considered as suspicious. Taxonomy: Information Status: Threshold Threshold: 3 events per minute	Threshold reached too many times	
18 - Threshold - Information Control	The rule raises an alert when the same event occurs too many times and is considered as suspicious. Taxonomy: Information Status: Control Threshold: 10 events per minute	Multiple invalid information controls	
19 - Threshold - Backup Management	The rule raises an alert when the same event occurs too many times and is considered as suspicious. Taxonomy: Standard Activity : Failed Backup Management Threshold: 3 events per minute	Multiple failed backup management activities	
20 - Threshold - Communication Flows	The rule raises an alert when the same event occurs too many times and is considered as suspicious. Taxonomy: Standard Activity: Denied Communication Connect Threshold: 10 events per minute	Multiple connections denied	
21 - Threshold - Control Use	The rule raises an alert when the same event occurs too many times and is considered as suspicious. Taxonomy: Standard Activity: Invalid Control Threshold: 10 events per minute	Multiple errors in controls use	
22 - Threshold - Data Access	The rule raises an alert when the same event occurs too many times and is considered as suspicious. Taxonomy: Standard Activity: Failed Data Access Threshold: 10 events per minute	Multiple failed data access	

Table 14 Threshold Rules

Name	Description	Alert's Name	Alert's Severity
23 - Threshold - Data Exchange	The rule raises an alert when the same event occurs too many times and is considered as suspicious. Taxonomy: Standard Activity: Error Data Exchange Threshold: 10 events per minute	Multiple errors in data exchanges	
24 - Threshold - Gain Activities	The rule raises an alert when the same event occurs too many times and is considered as suspicious. Taxonomy: Standard Activity: Failed Gain Threshold: 5 events per minute	Multiple failed right gain attempts	
25 - Threshold - Processing Activities	The rule raise an alert when the same event occurs too many times and is considered as suspicious. Taxonomy: Standard Activity: Error Process Threshold: 50 events per minute	Multiple processing errors	
26 - Threshold - Service Availability	The rule raises an alert when the same event occurs too many times and is considered as suspicious. Taxonomy: Standard Activity: Service Availability Threshold: 1 event per minute	Service Availability Transition	
27 - Threshold - State Transition	The rule raises an alert when the same event occurs too many times and is considered as suspicious. Taxonomy: Standard Activity: State Transition Threshold: 1 event per minute	Process stopped	
28 - Threshold - User authentication	The rule raises an alert when the same event occurs too many times and is considered as suspicious. Taxonomy: Standard Activity: Failed Authentication Threshold: 5 events per minute	Multiple user authentication failures	

Table 14 Threshold Rules

Name	Description	Alert's Name	Alert's Severity
29 - Threshold - Account Locking	The rule raises an alert when the same event occurs too many times and is considered as suspicious. Taxonomy: Configuration: Successful Account Lock/ Unlock Threshold: 10 events per minute	Multiple accounts locked or unlocked	
30 - Threshold - Configuration Repair Failed	The rule raises an alert when the same event occurs too many times and is considered as suspicious. Taxonomy: Configuration: Failed Repair Threshold: 1 event per minute	Configuration Repair Failure	
31 - Threshold - Configuration Repair Success	The rule raises an alert when the same event occurs too many times and is considered as suspicious. Taxonomy: Configuration: Successful Repair Threshold: 10 events per minute	Multiple configuration repairs (possible virus outbreak)	
32 - Threshold - Configuration Update	The rule raises an alert when the same event occurs too many times and is considered as suspicious. Taxonomy: Configuration: Error Update Threshold: 1 event per minute	Configuration Update Error	
33 - Threshold - Configuration Management Failed	The rule raises an alert when the same event occurs too many times and is considered as suspicious. Taxonomy: Configuration: Failed Administration Add/ Delete/Modify Threshold: 3 events per minute	Multiple failed configuration management activities	
34 - Threshold - Configuration Management Success	The rule raises an alert when the same event occurs too many times and is considered as suspicious. Taxonomy: Configuration: Successful Administration Delete/Modify Threshold: 10 events per minute	Multiple successful configuration management activities	

Table 14 Threshold Rules

Name	Description	Alert's Name	Alert's Severity
35 - Threshold - Vulnerability	The rule raises an alert when some vulnerabilities are detected on the same target node defined in the asset database. Taxonomy: Vulnerability Status Threshold: 1 event per minute	Vulnerability detected	
36 - Threshold - Suspicious	The rule raises an alert when some suspicious activities are detected on the same target node defined in the asset database. Taxonomy: Suspicious Activity Threshold: 1 event per minute	Suspicious activity detected	
37 - Threshold - Malware	The rule raises an alert when some malwares are detected on the same target node defined in the asset database. Taxonomy: Malware Threshold: 1 event per minute	Malware detected	
38 - Threshold - Attack	The rule raises an alert when some attacks are detected on the same target node defined in the asset database.. Taxonomy: Attack Threshold: 1 event per minute	Attack detected	

Table 15 Correlation Rules for Scenario

Name	Description	Alert's Name	Alert's Severity
39 - Corr. - Attacks T(Node+Srv.)	The rule correlates all attacks detected on same target node or service. This rule is used in a default scenario named "Known Vulnerability Exploited on same Target Node or Service".	Known Vulnerabilities Exploited	
40 - Corr. - Vulnerabilities	The rule correlates all vulnerabilities detected on same target node or service. This rule is used in a default scenario named "Known Vulnerability Exploited on same Target Node or Service".	Known Vulnerabilities Exploited	

Table 15 Correlation Rules for Scenario

Name	Description	Alert's Name	Alert's Severity
41 - Corr. - Attacks ST(Node+Srv.)	The rule correlates all attacks detected on same: ▪ source node or service ▪ or target node or service This rule is used in a default scenario named "Malicious Service Node Activities".	Suspect service node activities	
42 - Corr. - Suspicious	The rule correlates all suspicious activities detected on same: ▪ source node or service ▪ or target node or service This rule is used in a default scenario named "Malicious Service Node Activities".	Suspect service node activities	
43 - Corr. - Attacks T(Node)	The rule correlates all attacks detected on same target node. This rule is used in a default scenario named "Successful Target Node Attacks".	Successful Node Attacks	
44 - Corr. - Configuration Activity	The rule correlates all configuration activities detected on same target node. This rule is used in a default scenario named "Successful Target Node Attacks".	Successful Node Attacks	
45 - Corr. - Brute Force Detected	The rule correlates all brute force attacks detected on same target node or target users account. This rule is used in a default scenario named "Successful Target Node Bruteforce".	Successful target node bruteforce	
46 - Corr. - Login Success	The rule correlates all successful login detected on same target node and target users account ("root", "administrator", "admin", "administrateur" by default). This rule is used in default scenario named "Successful Target Node Bruteforce".	Successful target node bruteforce	
47 - Corr. - Backdoor Detected	The rule correlates all detected backdoor (attacks or vulnerabilities) on a target node or service. This rule is used in default scenario named "Known Target Node Backdoor Acceded".	Known Target Node Backdoor Accessed	
48 - Corr. - Connection success	The rule correlates all successful connection on the same target node and service defined in the asset database. This rule is used in default scenario named "Known Target Node Backdoor Accessed".	Known target node backdoor acceded	

Table 15 Correlation Rules for Scenario

Name	Description	Alert's Name	Alert's Severity
49 - Corr. - DOS Activities	The rule correlates all detected denial of services on a same target node. This rule is used in default scenario named "Successful Node DOS".	Successful Node DOS	
50 - Corr. - Service Loss	The rule correlates all services unavailability on a same target node. This rule is used in default scenario named "Successful Node DOS".	Successful Node DOS	
51 - Corr. - Denied Activity	The rule correlates all kinds of denied activities on a same source or target node defined in the asset database. This rule is used in default scenario named "Malicious Node Activity".	Malicious Node Activity	
52 - Corr. - Attack or Suspicious	The rule correlates all kinds of attacks or suspicious activities performed on the same source or target node. This rule is used in default scenario named "Malicious Node Activity".	Malicious Node Activity	
53 - Corr. - Privilege Mgt. (T+S)	The rule correlates all kinds of configuration changes performed from an account on a target node. This rule is used in default scenario named "Segregation of duties violation".	Segregation of duties violation	
54 - Corr. - Privilege Mgt. (S+T)	The rule correlates all kinds of configuration changes performed on an account on a target node. This rule is used in default scenario named "Segregation of duties violation".	Segregation of duties violation	
55 - Corr. - Login Failed	The rule correlates all failed logins performed on an account on a target node. This rule is used in default scenario named "Suspected bruteforce".	Suspected bruteforce	
56 - Corr. - User Account Sharing	This rule raises an alert when the same login is used several times on a host defined in the asset database from different locations. Taxonomy: Standard Activity: Authentication Login Grouping method: ▪ Same login value ▪ Same target node ▪ 2 or more distinct source nodes	User Account sharing detected	

Table 15 Correlation Rules for Scenario

Name	Description	Alert's Name	Alert's Severity
57 - Corr. - User Account Usurpation	This rule raises an alert when differents logins are used on a host from the same location. Taxonomy: Standard Activity: Authentication Login ▪ Grouping method: ▪ Same source node ▪ Same target node 3 or more distinct logins	User Account usurpation detected	
58 - Corr. - Distributed DOS	This rule raises an alert when multiple DOS are detected from different sources. Taxonomy: Attack Identification: Detected Attack DoS Grouping method: ▪ Same target node ▪ 10 or more distinct source nodes	Distributed DOS detected	

Table 15 Correlation Rules for Scenario

Name	Description	Alert's Name	Alert's Severity
59 - Corr. - Port Scan	This rule raises an alert when someone tries to connect to a computer on different ports. Taxonomy: Standard Activity: Communication Grouping method: ▪ Same source node ▪ Same target node ▪ 50 or more distinct target services	Port Scan detected	
60 - Corr. - US - Access to a Country under Embargoes	The rule controls any illegal activity with countries that are under a specific US policies and embargoes: (http://www.pmddtc.state.gov/embargoed_countries/index.html) ▪ fghanistan ▪ China ▪ Congo, The Democratic Republic of the ▪ Cuba ▪ Cyprus ▪ Eritrea ▪ Haiti ▪ Iran, Islamic Republic of ▪ Iraq ▪ Korea, Democratic People's Republic of ▪ Lebanon ▪ Liberia ▪ Libyan Arab Jamahiriya ▪ Sierra Leone ▪ Sudan ▪ Syrian Arab Republic ▪ Venezuela ▪ Vietnam ▪ Yemen An alert is raised if there is any outbound connection to one of these countries.	Access detected to a country under embargo or restricted by US State Dept. trade policies	

Chapter 3 - Log Signature and Encryption

The main reason for the importance of the raw log is in view of required legal proof about an event generated by a supported ìproduct. A raw log entry is the most faithful format derived from the data produced by a log source. This is why the SEM can be configured to keep a record of the event generated by a supported product in the raw log format.

A raw log archive is always **signed** and can be **encrypted**.

Signing Raw Logs

By default, each raw log is signed by the TIBCO LogLogic® SMP, which allows a safe treatment of logs such as:

- non-repudiation: ensures that the archive was generated by the TIBCO LogLogic® SMP and no other one.
- log integrity: ensures that logs have not been modified since their creation.

To sign logs:

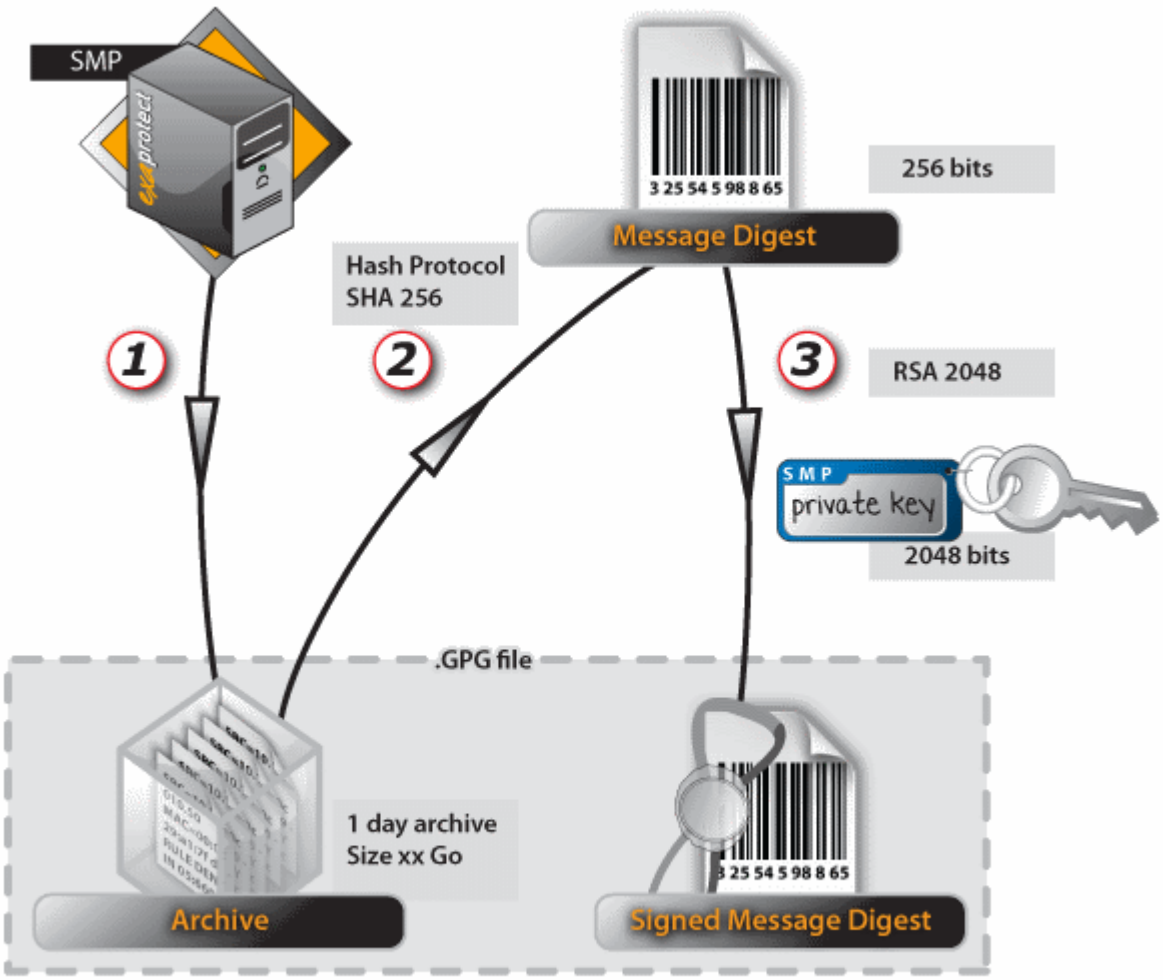
- The hash protocol used is SHA 256. It creates a message digest of 256 bits of the archive that will be ciphered by the RSA key.
- The signature is possible via the RSA key algorithm and a key of 2048 bits.

Here is a schema representing the mechanism of signing logs during the process of archiving and restoring raw logs.

Archiving Process

Schema

Figure 44 Signature - Archiving Process



Description

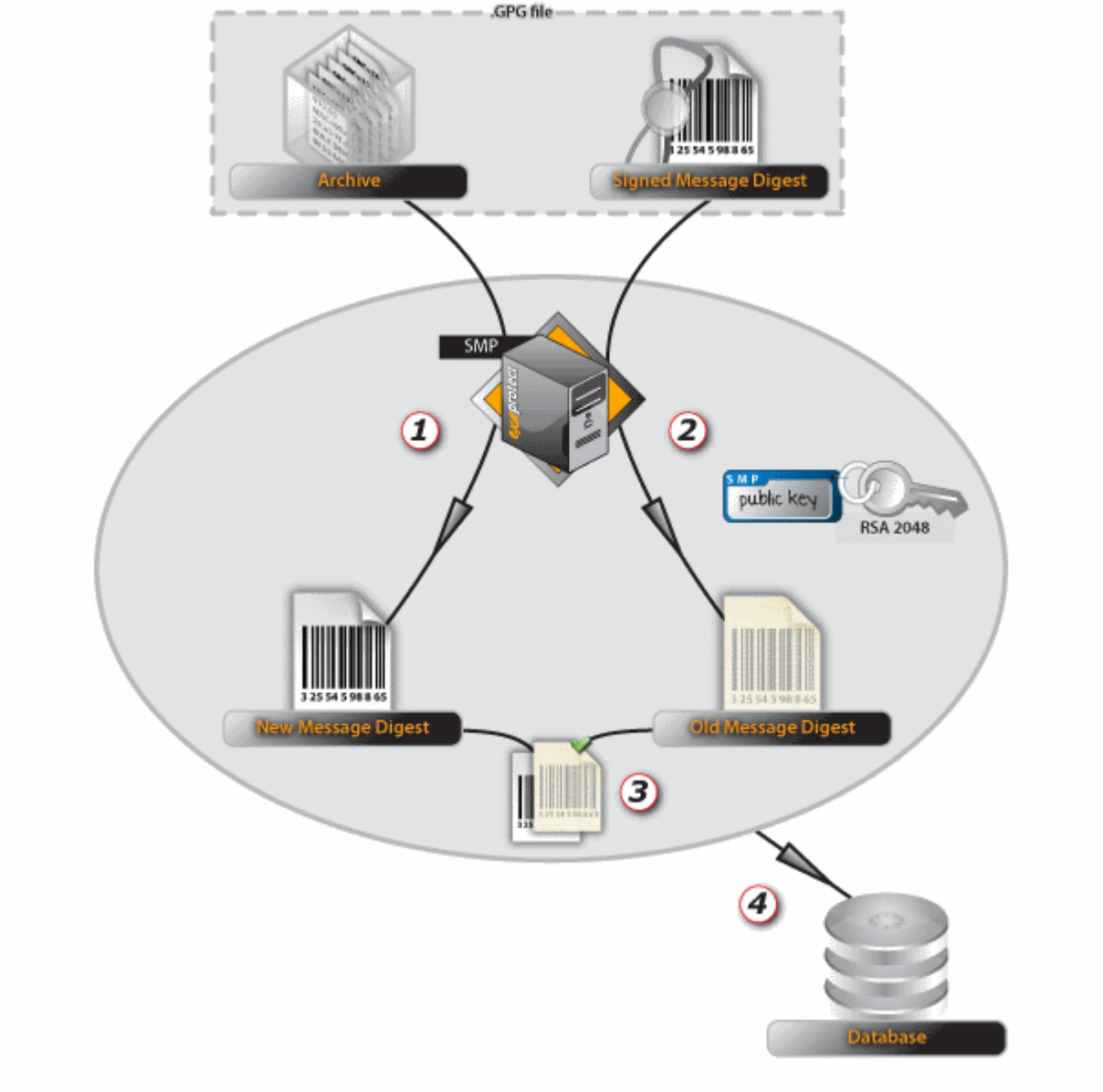
1	Every day, an archive (alerts/Elementary Events) is generated and exported to the SMP.
2	The archive goes through a hash function which calculates and generates a message digest to ensure integrity.

3	The SMP private key signs the message digest to ensure non-repudiation.

Restoration Process

Schema

Figure 45 Signature - Restoration Process



	Description
	With the archive file, the SMP computes a new digest message.
	The old signed digest message is deciphered via the RSA algorithm and the SMP public key.
	The two digest messages are compared. If they are identical, integrity is ensured.
	The archive is restored into the database.

Encrypting Raw Logs

Optionally, a user can decide to encrypt logs, which would allow a safe treatment of logs such as:

- confidentiality: ensures that information is accessible only to those authorized to have access.

To encrypt logs, the administrator must generate a key pair with the following conditions:

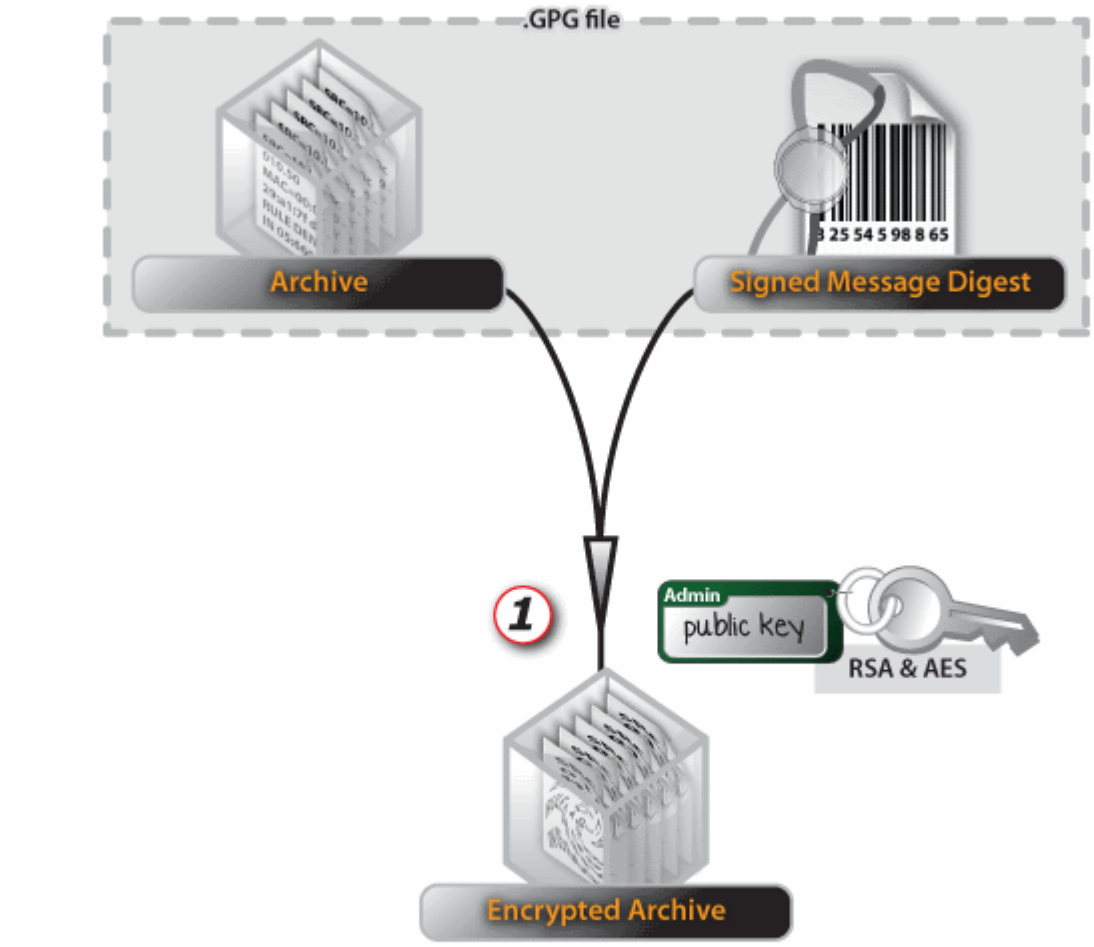
- key type, size and cipher protocol depends on the user choice during key generation.
- the key type must be:
  - DSA
  - DSA and El Gamal
  - **RSA** (recommended)
- the key size must be from 768 to **2048** (recommended).
- The cipher protocol used must be
  - 3DES
  - CAST5
  - BLOWFISH
  - **AES** (recommended), AES192, AES256
  - TWOFISH.
- The public key must be stored in TIBCO LogLogic® GUI.
- The private key is stored by the administrator.

Here is a schema representing the mechanism of encrypting logs during the process of archiving and restoring raw logs.

Archiving Process

Schema

Figure 46 Encryption - Archiving Process



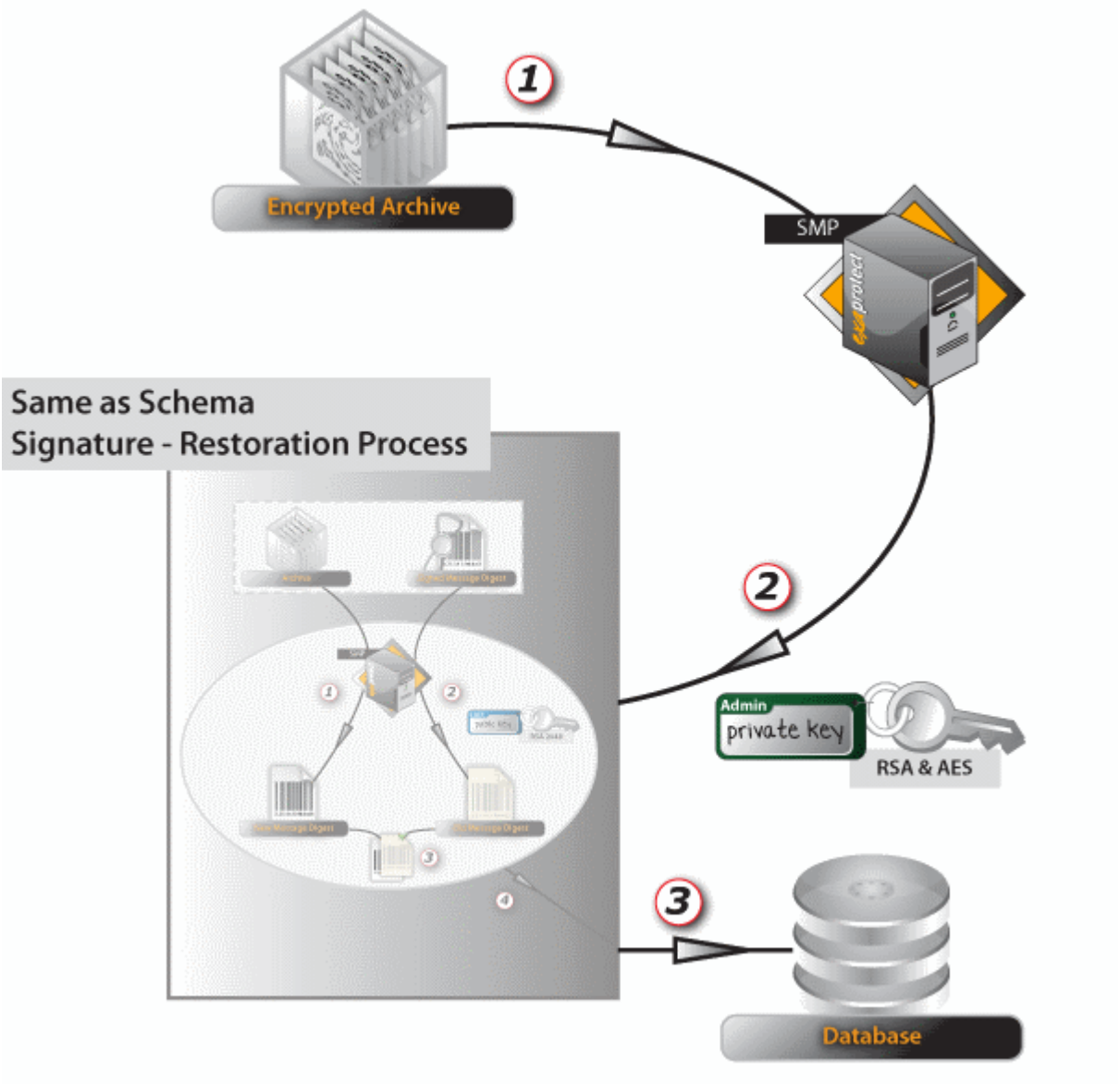
Description

1	The archive is encrypted with the help of the user public key and the cipher algorithms (AES + RSA). The message digest is signed.

Restoration Process

Schema

Figure 47 Encryption - Restoration Process



Description

1	The archive is sent to the SMP.

	The server deciphers the archive with the administrator private key asked during restoration and not stored on the server.
	The archive is in clear mode and ready to be restored in the database.

Chapter 4 - TIBCO LogLogic®'s Taxonomy

What is TIBCO LogLogic®'s Taxonomy?

A Problem's Answer

Information systems have numerous and varied procedures for monitoring security, such as intrusion detection sensors and auditing processes of operating systems (i.e., syslog subroutine). The function of these security procedures is to alert the security analyst to problems so that he can apply appropriate countermeasures whenever necessary. However, without normalizing the information contained in the large volume of events that are constantly produced, several problems ensue:

- Events are transmitted to the analyst in an unstructured format
- A confusing variety of terms are used to express the very same event action
- The event correlation process is not possible without structured data.
- Given the gigantic overall volume of information, it is also impossible for the analyst to know the totality of these events.

All of these problems require a normalization solution, a process transforming the original message into a structured standardized message which can be efficiently processed by the system.

A Simplified Language to Manage Security Events

The standardization of logs using the IDMEF format makes it possible to define a storage format for all types of logs destined for correlation but this is not sufficient, since the IDMEF format does not allow describing a log entry in a formal way.

To tackle the aforementioned problems, TIBCO LogLogic® devised its own normalization system (or TIBCO LogLogic® Taxonomy) based on the in-depth knowledge of its security experts as well as its own research work, and it established a formalism which makes it possible to characterize each log entry. This is called TIBCO LogLogic® Taxonomy. Furthermore, all log entries having the same characteristics are standardized in the same way. For example, independently from the technology used for a firewall, a blocked package will be always standardized with the following labels:

E.g. Denied use communication forward on system.

A Security Event's Classification Method

Through its security Taxonomy system, TIBCO LogLogic® established a classification of all activities which take place within the Information System (IS). A set of rules was also elaborated for the classification of original messages while simultaneously preserving their meaning. Each SEM event represents an activity and each activity constitutes a classification category in the system.

By modeling the key activities within the IS, TIBCO LogLogic® established approximately around 2000 categories representing more than 30.000 different events coming from approximately 200 different third-party products. The benefit produced by this standardization procedure is enormous since a security analyst will analyze and control a mass of information with a simple tool.

Why Using TIBCO LogLogic®'s Taxonomy?

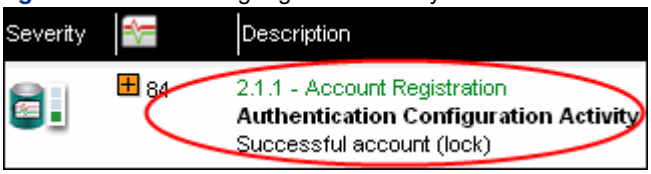
TIBCO LogLogic® Taxonomy allows you to:

- Understand logs.
- Control events.
- Manage security.

To Understand Logs

TIBCO LogLogic® Taxonomy is used in the Alert/Event list and details of the Web Console:

Figure 48 TIBCO LogLogic® Taxonomy in the event list



As you can see, the sentence is presented in the form of a phrase, that gives meaning to the IT event.

To Control Events

TIBCO LogLogic® Taxonomy is used in the Web Console collection, aggregation and correlation policies.

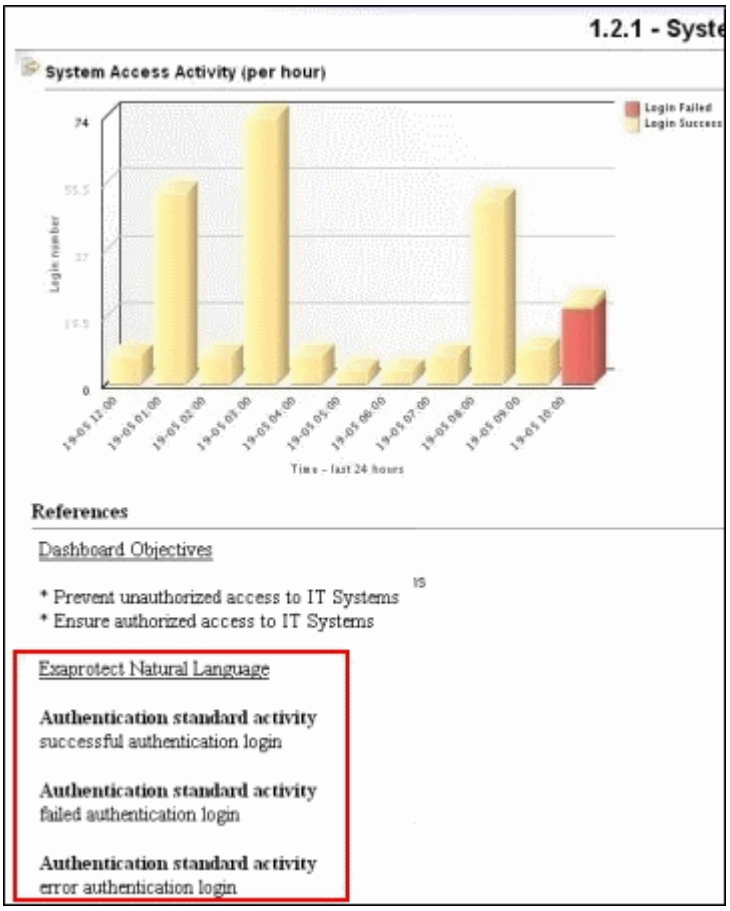
By selecting the various elements from the TIBCO LogLogic® Taxonomy, you will define vendor-independent rules for collecting logs.

In other terms, this method will allow you to create unified and normalized rules that will be based on the multitude of logs and messages that any product may generate. This will facilitate and improve your alert's detection process but also allow you to keep control on IT security.

To Manage Security

TIBCO LogLogic® Taxonomy is used in Web Console reporting policies and security dashboards:

Figure 49 TIBCO LogLogic® Taxonomy in a Security Dashboard



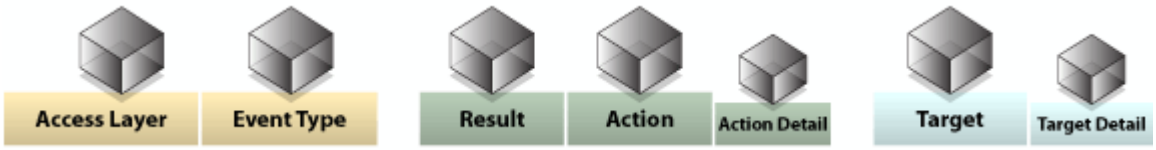
A normalized event, its impact and its regulatory compliance are graphically represented. This is an easy, clear and intelligent way of reading and monitoring any of your security events.

How Does TIBCO LogLogic®'s Taxonomy System Work?

Main Concepts

An event is the result of an action observed by a source. After TIBCO LogLogic®'s Taxonomy process, an action is generally expressed through seven main concepts:

Figure 50 The Seven Main Concepts in the TIBCO LogLogic® Taxonomy System



This means that an ***access layer*** is directed towards a ***target*** by means of an ***event type*** and its linked ***action*** which ultimately produces a ***result***.

> **Note:** The TIBCO LogLogic® Taxonomy graphically represented above refers to the logical structure used in data entry forms and in the sentence displayed in the details of an alert or event.

Let us describe these seven main concepts more precisely.

Access layer

The ***access layer*** field defines which part of the ***target*** (or IT resource) must be achieved.

To reach the ***access layer***, three main phases must be sequentially followed:

- ***Authentication***: the first step to reach the ***objective*** is the authentication service. Authentication is the verification of the user's identity.
- ***Rights***: the second step to reach the ***objective*** is to check user authorization or privileges.
- ***System***: the final step to reach the ***objective*** is to access system resources.

Event Type

The ***event type*** field indicates the kind of activity the event refers to.

There are seven types of events: Information status/ Vulnerability status/ Standard activity / Configuration activity / Suspicious activity identification / Malware identification / Attack identification.

- Information status: information concerning the state of a target, for example, an invalid service configuration.
- Vulnerability status: information related to a vulnerability, for example, a vulnerability scanner displays a vulnerability regarding a refusal of service.
- Standard activity: the event is to execute an action without making any unusual changes to the system, for example, opening a user session.
- Configuration activity: the event relates to a normal configuration procedure for a target (for example, a change of a system password).
- Suspicious activity identification: a suspect/suspicious activity.
- Malware identification: a malicious event consisting of the injection of a Malware infecting a target.
- Attack identification: a malicious event consisting of launching an attack on a target.

Result

An event describes an action observed by a security device; the consequence of this action is expressed in the ***result*** field.

E.g. Successful/Failed, Valid/Expired...

Action

To achieve his/her goals, the author of the action will use specific means or methods which will be expressed in the ***action*** field.

E.g. Authentication, Data Access, Configuration Update...

Action Detail

The ***action detail*** field furnishes additional information concerning the above ***action***.

E.g. Login/Logout/Lock, Read/Write/Delete...

Target

The ***target*** field can represent any IT resources.

E.g. File, E-mail, Proxy, Antivirus...

Target detail

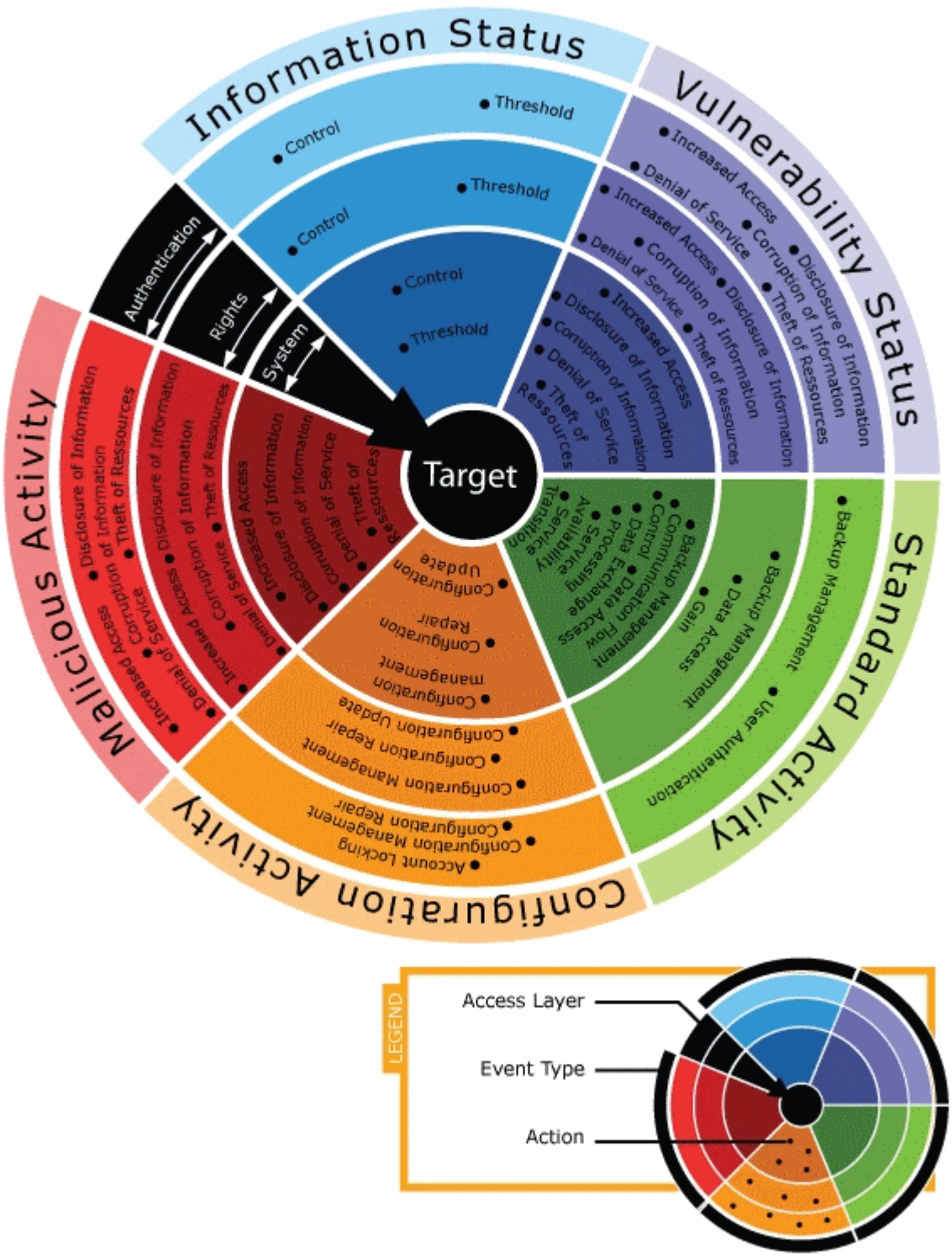
The ***target detail*** field furnishes additional information concerning the above ***target***.

E.g. Log file, Certificate, Message...

The TIBCO LogLogic® Taxonomy Target

To help you understand the TIBCO LogLogic® Taxonomy, Figure below gives a synthetic view based on three concepts which are **Access Layer**, **Event Type** and **Action**.

Figure 51 TIBCO LogLogic® Taxonomy Target



How to Interpret a Normalized Event?

One of the main aspects of the TIBCO LogLogic® Taxonomy is to give a name as simple and clear as possible to a complex and unstructured event. A brief look at the structure and syntax will allow you to quickly interpret and manage normalized events in an efficient way.

Method

The figure below shows an already normalized event as displayed in the Web Console event's view:

If we click on the classification information for an event displayed in the monitoring window, we will see the window "Event Details" showing numerous event details.

Notice that the normalized fields for the event appear under the event's description.

To make your sentence construction easier, you can use a table like the following one:

Figure 52 Table of Normalized events

Access Layer	Event Type		Result	Action	Action Detail		Target	Target Detail
System	Configuration Activity	:	Successful	Administration	Add	on	Web	Proxy
Authentification	Information Status	:	Exceeded	Threshold		on	Database	
Rights	Configuration Activity	:	Successful	Administration	Add	on	Firewall	

Examples

Here are few examples of normalized events and their descriptions.

Table 16 Interpreting Normalized Events

Normalized Event	Explanation
Authentication Standard Activity: Successful Authentication (Login) on SMP (Account)	The standard activity which consists in authenticating on an SMP with a login account is successful.
System Standard Activity: Error Communication (Connect) on Log Collector	During the system standard activity, an error of communication occurred because of a loss of connectivity with the Log Collector. No target detail needs to be specified.
System Configuration Activity: Successful Update on SMP	The system configuration activity which consists in updating the SMP server is successful.

Possible Values for Normalized Fields

The following tables present the possible values for the normalized fields.

Access Layer

Table 17 The three access layers

The three objectives		
Authentication	Rights	System

Event Types, Actions, Action Details and Results

The following table presents a reference for interpreting normalized events.

Table 18 Reference for Interpreting Events

Event Type	Action	Action Detail	Result
The three main Event Types			
Information Status	Control	Control	▪ Invalid ▪ Notify ▪ Valid
	Threshold	Threshold	▪ Exceeded ▪ Expired ▪ Low ▪ Normal

Table 18 Reference for Interpreting Events

Event Type	Action	Action Detail	Result
Standard activity	Backup Management	Backup	▪ Error
		Restore	▪ Failed
			▪ Successful
	Communication	Connect	▪ Denied
		Disconnect	▪ Error
		Forward	▪ Successful
	Control	Control	▪ Error
			▪ Successful
	Data Access	Read	▪ Error
		Write	▪ Failed
		Delete	▪ Successful
	Data Exchange	Send	▪ Error
		Receive	▪ Successful
	Gain	Gain	▪ Error
			▪ Failed
			▪ Successful
	Process	End	▪ Error
		Execute	▪ Successful
	Service Availability	Down	▪ Error
		Up	▪ Successful
	State Transition	Start	▪ Error
		Restart	▪ Successful
		Stop	
	Authentication	Login	▪ Error
		Logout	▪ Failed
		Lock	▪ Successful
Configuration activity	Administration	Add	▪ Error
		Delete	▪ Failed
		Modify	▪ Successful
	Update	Update	▪ Error
			▪ Successful
	Repair	Repair	▪ Error
			▪ Failed
			▪ Successful
	Account	Lock	▪ Error
		Unlock	▪ Failed
			▪ Successful

Table 18 Reference for Interpreting Events

Event Type	Action	Action Detail	Result
Other Event Types			
Vulnerability status	Vulnerability	Backdoor Bounce Brute Force Bypass Concealment DDoS Directory Traversal DoS Evasion Gain Hijacking Information Gathering Information Leak Injection Other Overflow P2P Phishing Physical Poisoning Protocol Spam Spoofing Spyware Steal Trojan Violation Virus Worm	▪ Detected

Table 18 Reference for Interpreting Events

Event Type	Action	Action Detail	Result
Suspicious activity identification	Suspicious	Bounce Brute Force Concealment DDoS DoS Evasion Gain Hijacking Information Gathering Information Leak Injection Other Overflow Spoofing Violation Virus	▪ Detected

Table 18 Reference for Interpreting Events

Event Type	Action	Action Detail	Result
Malware identification	Malware	Other P2P Spam Spyware Trojan Virus Worm	▪ Detected
Attack identification	Attack	Backdoor Bounce Brute Force Bypass Concealment DDoS Directory Traversal DoS Evasion Gain Hijacking Information Gathering Information Leak Injection Other Overflow Phishing Physical Poisoning Protocol Spoofing Steal Violation	▪ Detected

Target and Target Details

Other references can be used to normalize events such as **Target** and **Target details** as displayed in the tables below.

Target

Table 19 List of Targets

Targets
Account
Account Group
Account Host

Table 19 List of Targets

Targets
Account Service
Admin
Admin Group
Anonymous
Antivirus
Application
Application Payment
ARP
Attach
Audit
Battery
Cache
Certificate
Chat
Client
Cluster
Command
Component
Conf File
CPU
Credential
Data
Database
DHCP
Directory
Disk
DNS
Domain
Ethernet
File
Finger
Firewall
FTP
Guest
GUI
HA
Host
ICMP
IDS
Interface
IP
IPSec
LDAP

Table 19 List of Targets

Targets
License
Log Collector
Log File
Mail
Management
Memory
Message
Modem
Multimedia
NFS
OS
P2P
Packet
Parameter
Password
Patch
Pattern
PKI
Port
Printer Device
Printer Protocol
Process
Protocol
Proxy
PUP
Queue
Registry
Relay
Request
RIP
Router
RPC
Security Tools
Service
Service Group
SMP
SSH
SSL
Switch
Sys Auth
Sys Crypt
Sys Data
Sys Directory

Table 19 List of Targets

Targets
Sys File
TCP
Telnet
Time
Traffic
Tunnel
UDP
Update Service
UPS
URL
VLAN
VPN
Web
Wireless

Target Details

Table 20 List of Target Details

Account
Account Group
Account Host
Account Service
Address
Admin
Admin Group
Anonymous
Application
Attach
Battery
Cache
Certificate
Client
Cluster
Command
Component
Conf File
CPU
Credential
Data
Directory
Disk

Table 20 List of Target Details

File
Firewall
Format
Guest
GUI
Host
ICMP
IDS
Image
Integrity
Interface
License
Log File
Memory
Message
Method
Modem
Name
P2P
Packet
Parameter
Password
Patch
Path
Pattern
Policy
Port
Power
Printer Device
Process
Protocol
Proxy
Queue
Registry
Relay
Reply
Request
Router
Scan
Security Tools
Service Group
State
Switch

Table 20 List of Target Details

Sys Auth
Sys Data
Sys Directory
Sys File
Table
Temperature
Timeout
Traffic
Trap
Tunnel
Version
VLAN
VPN

Chapter 5 - Compliance

This chapter gives an overview of Regulatory Compliance through its three underlying domains: regulation, standards and technical reporting.

The aim is to:

- explain how to use the SEM environment to address these requirements.
- present a default IT reporting framework provided by SEM and an example of a security dashboard use.

TIBCO LogLogic® Security Dashboards: from Compliance to Technical Reporting

This section gives an overview of the three main themes that will help you understand how to work with TIBCO LogLogic® reporting tool in terms of compliance.

Themes are:

- Regulations.
- Standards.
- Technical Reporting.

Regulations

In order to gain a maximum level of security in their business IT infrastructure, each company is entitled to follow and apply security laws and regulations, e.g. as SOX regulation underlines, a secured IT is mandatory to secure financial assets.

Main laws and regulations are:

- Basel II Accord.
- Federal Information Security Management Act of 2002 (FISMA).
- Financial Services Authority (FSA).
- Gramm-Leach-Bliley Act (GLBA).
- Health Insurance Portability and Accountability Act (HIPAA).
- Loi sur la Sécurité Financière - Financial Security Law of France (LSF).
- Markets in Financial Instruments Directive (MiFID).
- Payment Card Industry Data Security Standard (PCI-DSS).
- Sarbanes-Oxley Act of 2002 (SOX).

As laws and regulations are - in their vast majority - subdued to each countries' jurisdiction, the choice made by TIBCO LogLogic® is to work with their related ***standards.*** Indeed, standards can be easily applied, no matter the country.

Standards

Law and Regulation standards are composed of a list of measures, processes and best practices intended to help security managers in their security development process and daily use.

These detailed procedures can be easily followed.

Main supported standards are:

- ISO 27002:2010:
- Control Objectives for Information and related Technology (COBIT), e.g. adopted by public companies that are subject to the U.S. Sarbanes-Oxley Act of 2002.
- Payment Card Industry Data Security Standard (PCI-DSS) v1.2.

Companies are usually audited on a regular basis. Auditing information security covers topics from auditing the physical security of data centers to the auditing logical security of databases and highlights key components to look for and different methods for auditing these areas.

This particular appointment needs an important preparation as well as a structured information gathering.

TIBCO LogLogic® offers a comprehensive solution through its reporting module. Indeed, dashboards and reports take ***standards*** controls (organizational, technical...) as reference to construct business and security-oriented dashboards.

Technical Reporting

To evaluate and monitor each standard control, reports based on technical data collected by Security Event Manager are provided.

These reports are based on technical activities contained in device logs such as:

- packet forwarding logs of router.
- user authentication logs of data servers.

The TIBCO LogLogic® Solution

TIBCO LogLogic® innovative reporting tool can help you prepare audits and offers a clear and useful representation of your IT security environment by:

- Managing Regulations.
- Managing Standards.
- Managing Technical Reporting.

Managing Regulations

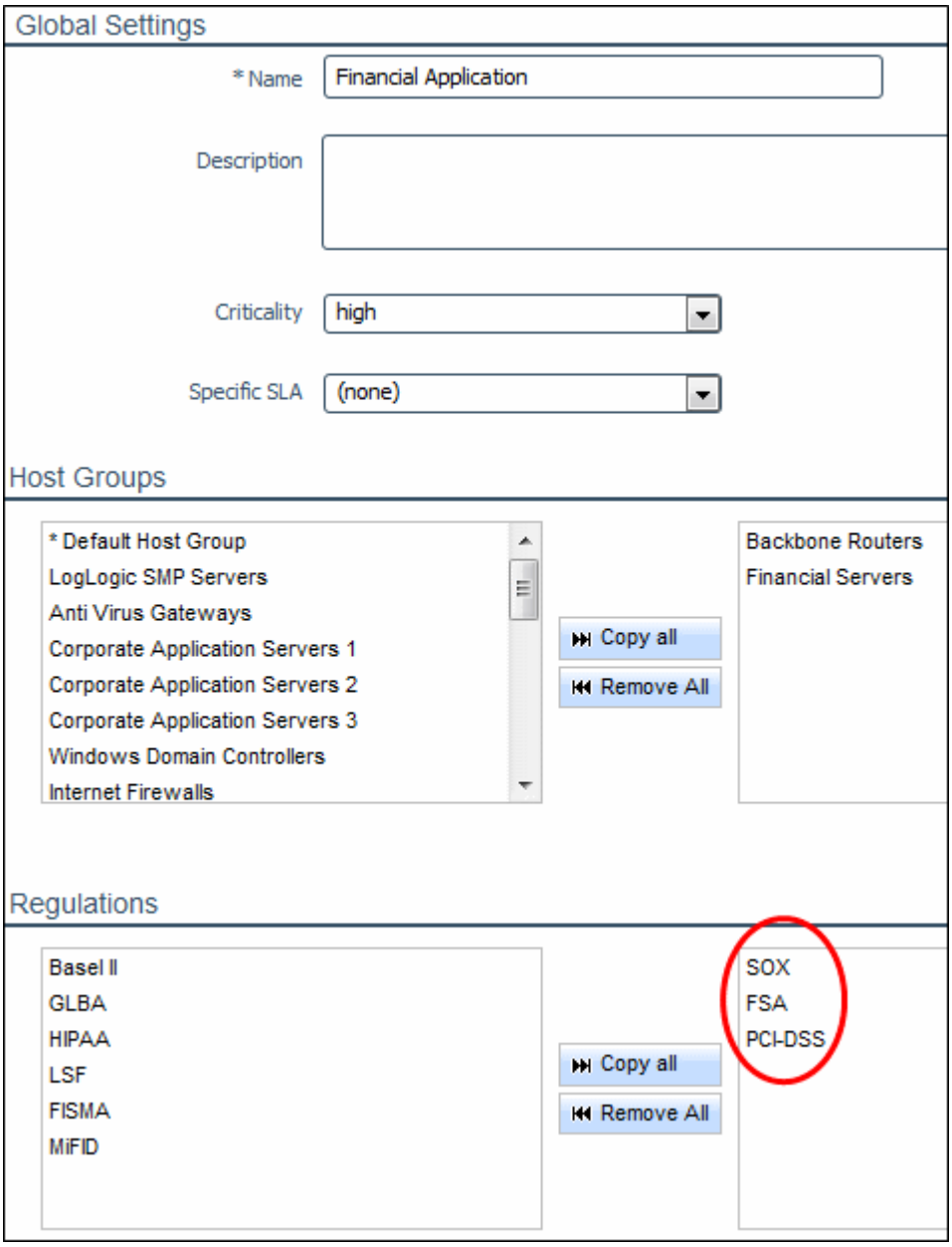
Create a Business Asset

To be able to manage regulations, you must identify your IT devices impacted by a regulation and make sure the TIBCO LogLogic® asset database is correctly filled. Indeed, the reporting tool will use the “regulation tag” from the asset database to create and filter the necessary data according to the regulations your company follows.

To do so:

1. Identify IT devices submitted to a regulation.

2. Tag related Business Assets with relevant regulation fields by defining them in **Configuration > Asset Database > Business Assets > click on a business asset**.



1. Then, in each dashboard, you can filter the data to be displayed for a specific regulation.

When using TIBCO LogLogic® reports and dashboards, you will see that they are automatically based upon ***Standards*** and not regulations.

However, if your business activity is submitted to one regulation and you want a dedicated reporting environment for this regulation, you just have to use the pre-defined compliance dashboards furnished by TIBCO LogLogic® as explained in the section Dashboards Based on Regulations.

Managing Standards

The reporting module is by default based upon well-known standards. This makes your dashboards' views easier to display and explain during an audit.

TIBCO LogLogic® Dashboards Framework

Seven groups of dashboards are available.

Standards are combined into three main groups, each group containing the report suitable for a given standard. These groups are the result of an important work carried out on data compilation and a synthesis of the main standards and regulations currently in use.

Two other groups have been created in order to meet regulation demands. In other words, some of the relevant standards from the first three groups have been extracted and inserted into regulation groups, i.e. Regulatory Compliance and SANS.

Eventually, two groups are available for you to manage printable versions of the dashboards you need (**Executive Report** and **PDF Report** groups).

A summary table of default TIBCO LogLogic® dashboards is available under the **Dashboards** tab by selecting **Regulatory Compliance > Standards Mapping > Standards Mapping and Coverage >** TIBCO LogLogic® **Sec. Dashboards** tab.

Group 1

1 - Access Control Security

1.1 - Account Management

1.2 - User Access

1.3 - Remote Access

Group 2

2 - Operation Security

2.1 - Malware Protection

2.2 - Data Exchange

2.3 - Operation Security Management

2.4 - Network Security

2.5 - Incident and Alert Management

2.6 - Log & Event Management

Group 3

3 - Asset Security

3.1 - Asset Identification

3.2 - Change Management

3.3 - Backup Management

3.4 - Capacity Management

3.5 - Vulnerability Management

3.6 - Asset Availability

Group 4

Monthly Executive Report

Group 5

5 - Regulatory Compliance

5.1 - Standards Mapping

5.2 - FSA

5.3 - PCI-DSS

5.4 - Sarbanes-Oxley

Group 6

6 - SANS Top 5

6.1 - Attempts to Gain Access Through Existing Accounts

6.2 - Failed File or Resource Access Attempts

6.3 - Unauthorized Changes to Users, Groups and Services

6.4 - Systems Most Vulnerable to Attack

6.5 - Suspicious or Unauthorized Network Traffic Patterns

Group 7

7 - PDF Reports

7.1 - Executive

7.2 - FSA

7.3 - PCI-DSS

7.4 - Sarbanes-Oxley

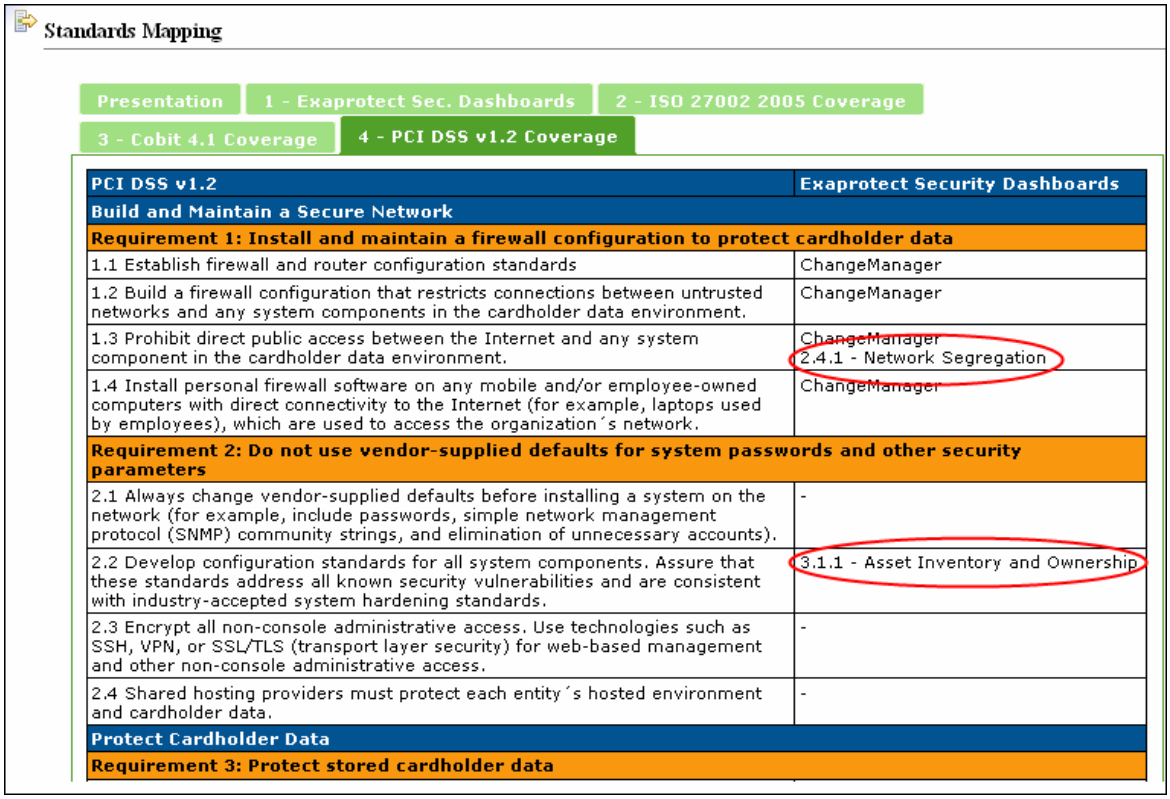
7.5 - Other Reports

Standards Mapping

In Security Event Manager, standards mapping has been performed to adapt a particular procedure taken from a standard to the relevant TIBCO LogLogic® security dashboards and reports.

A summary table of the main standards are available under the **Dashboards** tab by selecting **Regulatory Compliance > Standards Mapping > Standards Mapping and Coverage > "name of the relevant standards" Coverage** tab.

Figure 53 Standards mapping



In the above example, you can see that each point of the PCI DSS v1.2 has been listed. For each main points, the relevant dashboard is indicated.

> **Note:** When **ChangeManager** is indicated, it means that we suggest the use of the TIBCO LogLogic® **ChangeManager** solution to meet your demand in terms of compliance.

The process is the same for ISO 27002 2010 and Cobit 4.1 standards. In that way, you know exactly which dashboard you must use to be compliant with standards - and by extension regulations - followed by your company.

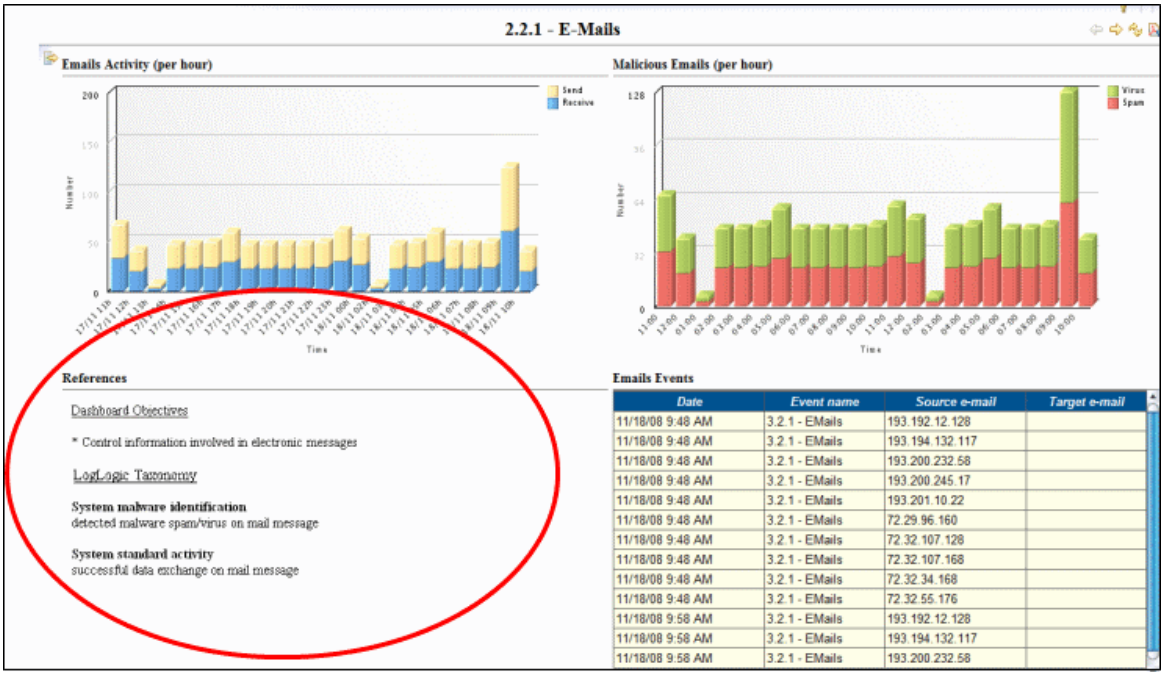
Standards Display in Dashboards

When creating a dashboard, you will see four main blocks.

The fourth block entitled **References** sums up important information such as the aim of the report, the TIBCO LogLogic® Taxonomy and the standards compliance applied.

Here is an example:

Figure 54 Block 4



Managing Technical Reporting

The reporting module offers the possibility to monitor data through detailed technical reporting.

This type of data can be sorted according either to time or frequency. If data is sorted according to frequency, we talk about **Top** list.

Technical data is always available in the third block of a security dashboard as shown in the two examples below.

Technical Data Sorted by Frequency (TOP)

Figure 55 Technical data - TOP list

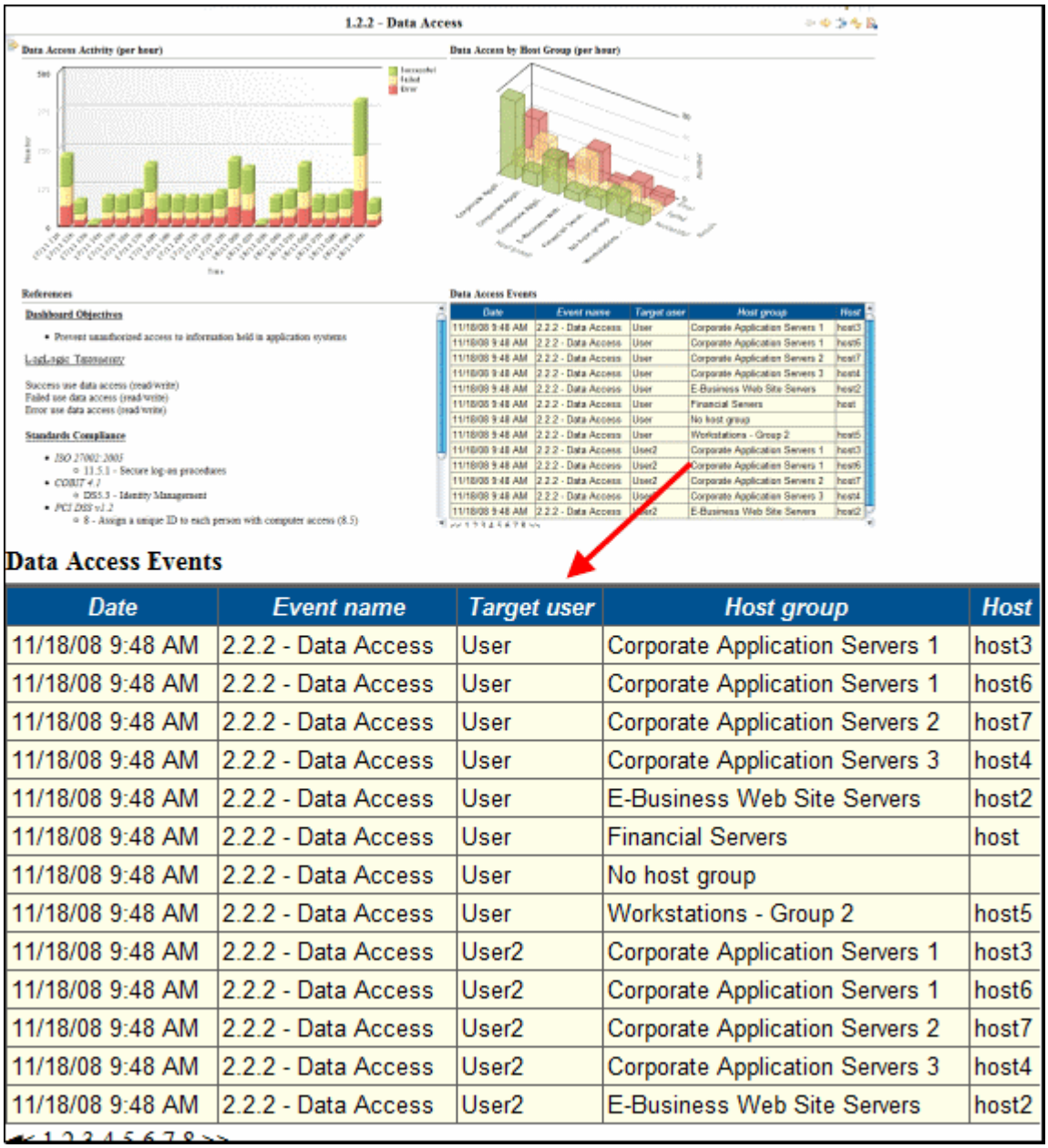
System Access TOP (per hour)

#	Target user	Result	Host group
62	User	Failed	Corporate Application Servers 1
53	User5	Successful	Corporate Application Servers 2
36	User	Successful	No host group
36	User2	Successful	No host group
35	User	Successful	Financial Servers
35	User4	Failed	No host group
33	User5	Successful	Corporate Application Servers 1
32	User	Failed	Corporate Application Servers 3
29	User2	Error	Workstations - Group 2
29	User3	Failed	Financial Servers
29	User4	Failed	Workstations - Group 2
28	User4	Error	Corporate Application Servers 1
11	User3	Failed	No host group

<< 1 2 3 4 5 6 7 8 >>

Technical Data Sorted by Time

Figure 56 Technical data - detailed list



Use of Security Dashboards

A dashboard is a set of reports. A report is a graphical representation of the number of alerts, incidents and/or vulnerabilities. You can display real-time reports, that is to say, reports based on raw logs.

Open Security Dashboards Screens

To access the **Reporting** module, you must go to **Reporting > Security Dashboards** in the menu bar.

A table giving an overview of the content of the dashboard module is displayed:

Figure 57 Default Dashboard Display

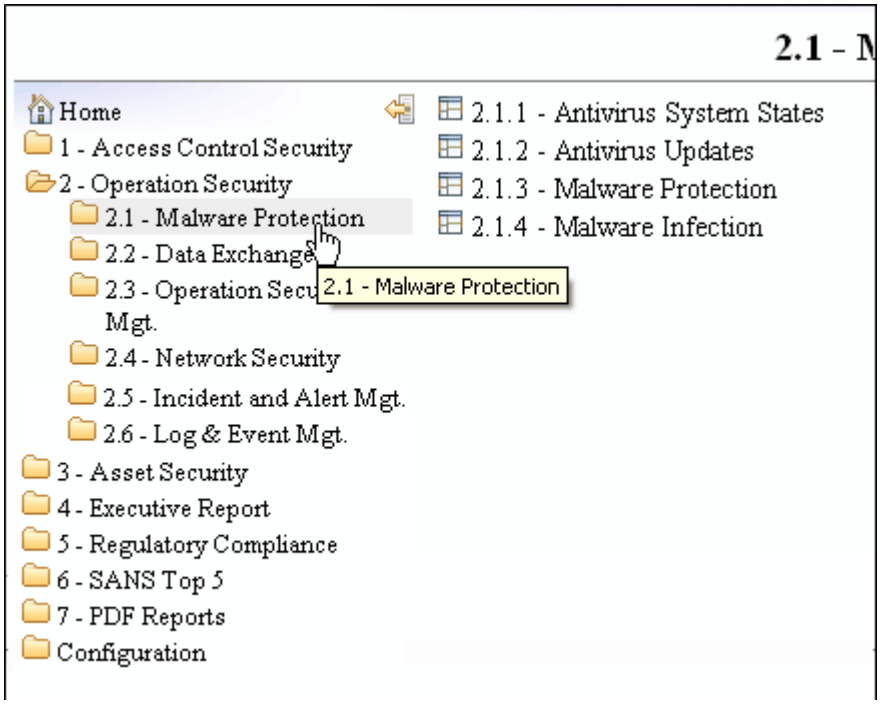
	Content	Type		Time Scale			
		Dynamic	Static	Hour	Day	Month	Year
Home	Dashboards welcome page. It summarises the reporting content, accessible from the top left menu.						
1 - Access Control Security	User access, account management and remote access to systems.			•	•	•	•
2 - Operation Security	Basic IT operations: malware, viruses, e-mails, network, alerts, configuration management...	•		•	•	•	•
3 - Asset Security	Dedicated to the security of assets identified in the Asset Database: changes and backup activities, capacity management, vulnerabilities status and availability for each asset.	•		•	•	•	•
4 - Executive Reports	Combines all previous security dashboards in a single monthly report.		•		•	•	
5 - Regulatory Compliance	Reports specific for each of the main regulations (FSA, PCI-DSS, SOX). References for mapping to main regulations and standards (ISO 27002, CobiT 4.1, ...)		•		•	•	
6 - SANS Top 5	EventManager dashboards recommended by the SANS (SysAdmin, Audit, Network, Security) Institute in its "Top 5 Essential Log" document.	•		•	•	•	•
7 - PDF Reports	Executive Reports (part 4) and Regulatory Compliance Reports (part 5) . These reports are automatically generated in PDF format at the end of each month.		•		•	•	
Configuration	Access to reporting environment configuration.						

Display and Explore a Security Dashboard

Displaying a Security Dashboard

1. Click on the icon and deploy the tree structure until you display the relevant dashboard.

Figure 58 Tree structure



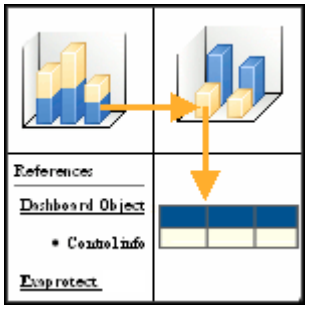
2. Click on the relevant dashboard's entry. The dashboard interface is divided into four main areas:

- The top-left area displays a graph, e.g. System Access Activity per hour.
- The top right area displays a more precise graph, e.g. System Access Activity per host group per hour.
- The bottom right area displays the events or logs that were used for the report generation.
- The bottom left area entitled **References** contains various information about the dashboard, such as a description, the related TIBCO LogLogic® Taxonomy used to generate the dashboard and the compliance with security standards.

Exploring a Security Dashboard

The Drill-down Approach

To explore dashboard data, the Drill Down approach is used. This approach can be represented as follows:

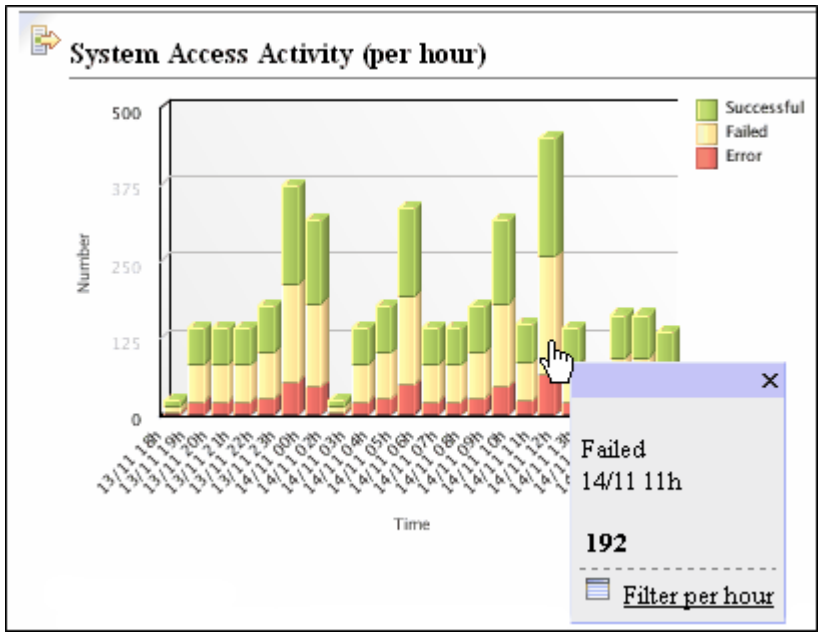


The orange arrows correspond to the dynamic links between the different reports.

Here is a real example.

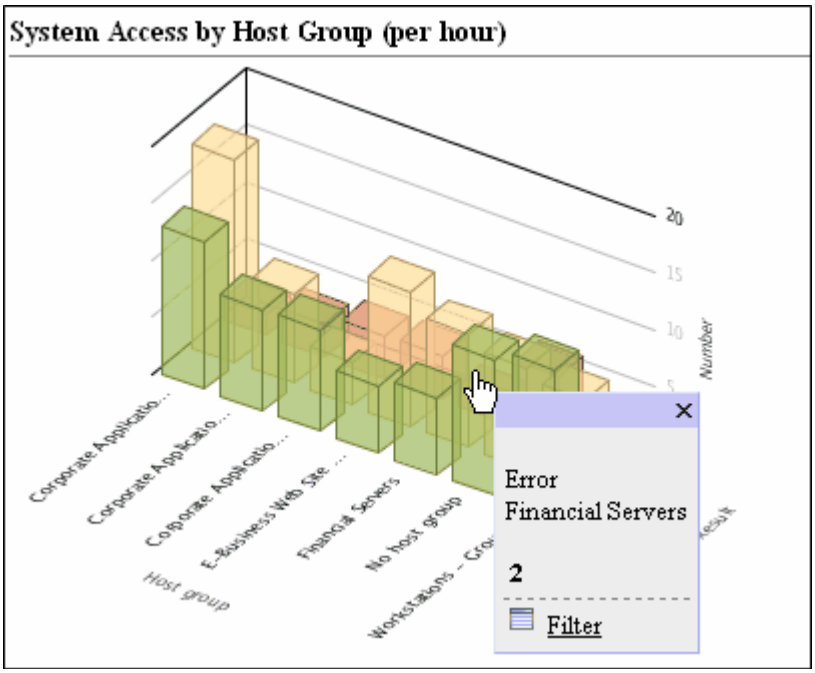
- If you click on the top-left graph, a pop-up screen is displayed asking you to filter data. This updates the graph on the right.

Figure 59 Filter on the top-left graph to update the top right graph



- If you click on the top right graph, you can **update** the table below by displaying updated events. Note that if this is an hour-type dashboard with a list of events, this action **displays the table for the first time**.

Figure 60 Filter on the top right graph to update the table below



- The table containing the events reference is updated:

Figure 61 The table is updated

System Access TOP (per hour)

#	Target user	Result	Host group
80	User5	Failed	Corporate Application Servers 1
53	User4	Successful	Financial Servers
28	User4	Failed	No host group
28	User4	Successful	Corporate Application Servers 1
27	User	Error	No host group
27	User3	Successful	No host group
27	User4	Successful	Corporate Application Servers 2
26	User	Failed	E-Business Web Site Servers
26	User2	Successful	Corporate Application Servers 2
26	User3	Error	Workstations - Group 2

Three Different Scales

You can display a single dashboard based on a different time unit (hour, day or month).

Figure 62 The three different scales: Hour, Day and Month

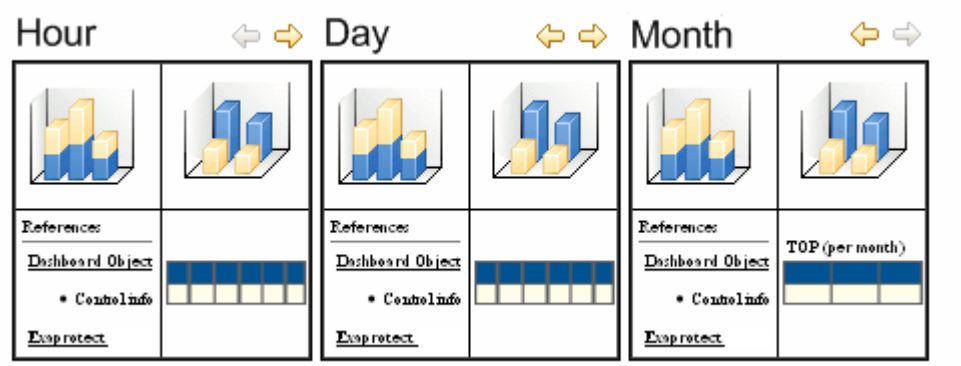
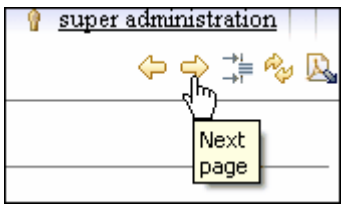


Table 21 The three different scales: Hour, Day and Month

Scale	Description
Hour	displays Elementary Events.
Day	displays Elementary Events and TOP 100 events.
Month	displays TOP 100 events.

To navigate between the different graphs, click on the top right arrows to navigate between the dashboards.

Figure 63 Navigating between hour, day and month dashboards



Executive Report

Content

The **Executive Security Report** combines all default security dashboards in a single static monthly report. It provides a monthly overview of the whole enterprise IT security status. Security controls covered by Security Event Manager are divided into three main parts:

1 - Access Control Security

This section provides information on user access, account management and remote access to systems.

2 - Operation Security

This section contains basic IT operation information: malware, viruses, emails, network, alerts, configuration management...

3 - Asset Security

This section is dedicated to the security of assets identified in the Asset Database: changes and backup activities, capacity management, vulnerabilities status and availability for each asset.

Location

To preview the dashboard, select **Home > Executive Report > Monthly Executive Report**.

The PDF file is located in:

```
/var/lib/exaprotect/archives/<INSTANCE>/report/pdf/executive
```

Note: The **Executive Security Report** is optimized for printing (A4 paper format).

Dashboards Based on Regulations

Each month, four dashboards based on specific regulations are automatically generated and exported in PDF. These dashboards are:

- FSA-ComplianceReport-Month<nb>.pdf
- PCI-ComplianceReport-Month<nb>.pdf
- SOX-ComplianceReport-Month<nb>.pdf

The pdf exported files are accessible via:

- **Home > PDF Reports > "name of reports"**

or

- **Home > Regulatory Compliance > "name of reports"**. In this screen, you will be able to get a preview of the selected reports.

A maximum of 12 pdf files are generated per year, one for each month. Previous year's dashboards are overriden by newly generated ones.

Only day and month scales are available (no hour scales).

Note: These dashboards are optimized for printing (A4 paper format).

FSA Compliance Dashboard

Content

The **FSA** dashboard includes existing reports with a filter on the **FSA** regulation. It is exported in format A4 Portrait and contains 56 pages:

- The first pages describe the FSA regulation.
- the rest of the document is composed of reports which:
  - describes the FSA section.
  - shows the evolution during the last month (in days)
  - shows a monthly activity in 3 dimensions (**X**: HostGroup or Asset, **Y**: TIBCO LogLogic® Taxonomy, **Z**: number)
  - shows 1 TOP for the month

Location

To preview the dashboard, select **Home > Regulatory Compliance > FSA > Monthly FSA Compliance Report**.

The PDF file is located in:

```
/var/lib/exaprotect/archives/<INSTANCE>/report/pdf/fsa
```

PCI Compliance Dashboard

Content

The **PCI-DSS** dashboard includes existing reports with a filter on the **PCI-DSS** regulation. It is exported in format A4 Portrait and contains 39 pages:

- The first pages describe the **PCI-DSS** regulation.
- The rest of the document is composed of reports which:
  - describes the **PCI-DSS** section.
  - shows the evolution during the last month (in days)
  - shows a monthly activity in 3 dimensions (**X**: HostGroup or Asset, **Y**: TIBCO LogLogic® Taxonomy, **Z**: number)
  - shows 1 TOP for the month

Location

To preview the dashboard, select **Home > Regulatory Compliance > PCI-DSS > Monthly PCI-DSS Compliance Report**.

The PDF file is located in:

```
/var/lib/exaprotect/archives/<INSTANCE>/report/pdf/pci-dss
```

SOX Compliance Dashboard

Content

The **Sarbanes-Oxley** dashboard includes existing reports with a filter on the **Sarbanes-Oxley** regulation. It is exported in format A4 Portrait and contains 62 pages:

- The first pages describe the **Sarbanes-Oxley** regulation.
- The rest of the document is composed of reports which:
  - describes the **Sarbanes-Oxley** section.
  - shows the evolution during the last month (in days)
  - shows a monthly activity in 3 dimensions (**X**: HostGroup or Asset, **Y**: TIBCO LogLogic® Taxonomy, **Z**: number)
  - shows 1 TOP for the month

Location

To preview the dashboard, select **Home > Regulatory Compliance > Sarbanes-Oxley > Monthly SOX Compliance Report**.

The PDF file is located in:

```
/var/lib/exaprotect/archives/<INSTANCE>/report/pdf/sox
```

Sample Dashboard 1 - Access Control Security

This section gives samples of Access Control Security dashboards through three main themes:

- Account Management
  - Account Registration
  - Privilege Management
  - Password Management
- User Access
  - System Access
  - Data Access
- Remote Access
  - Virtual Private Networks
  - Remote Administration Security

Account Management

Account Registration

Dashboard Objectives

- Remove or adjust access rights of all IT System users that leave or change function.

TIBCO LogLogic® Taxonomy

- Authentication configuration status
successful administration add/delete
- Authentication configuration status
successful account lock/unlock

Figure 64 Account Registration

Date	Event name	Host group	Host	Target user
11/18/08 9:48 AM	2.1.1 - Account Registration	Corporate Application Servers 1	host3	User
11/18/08 9:48 AM	2.1.1 - Account Registration	Corporate Application Servers 1	host3	User2
11/18/08 9:48 AM	2.1.1 - Account Registration	Corporate Application Servers 1	host3	User3
11/18/08 9:48 AM	2.1.1 - Account Registration	Corporate Application Servers 1	host3	User4
11/18/08 9:48 AM	2.1.1 - Account Registration	Corporate Application Servers 1	host3	User5
11/18/08 9:48 AM	2.1.1 - Account Registration	Corporate Application Servers 1	host6	User
11/18/08 9:48 AM	2.1.1 - Account Registration	Corporate Application Servers 1	host6	User2

Privilege Management

Dashboard Objectives

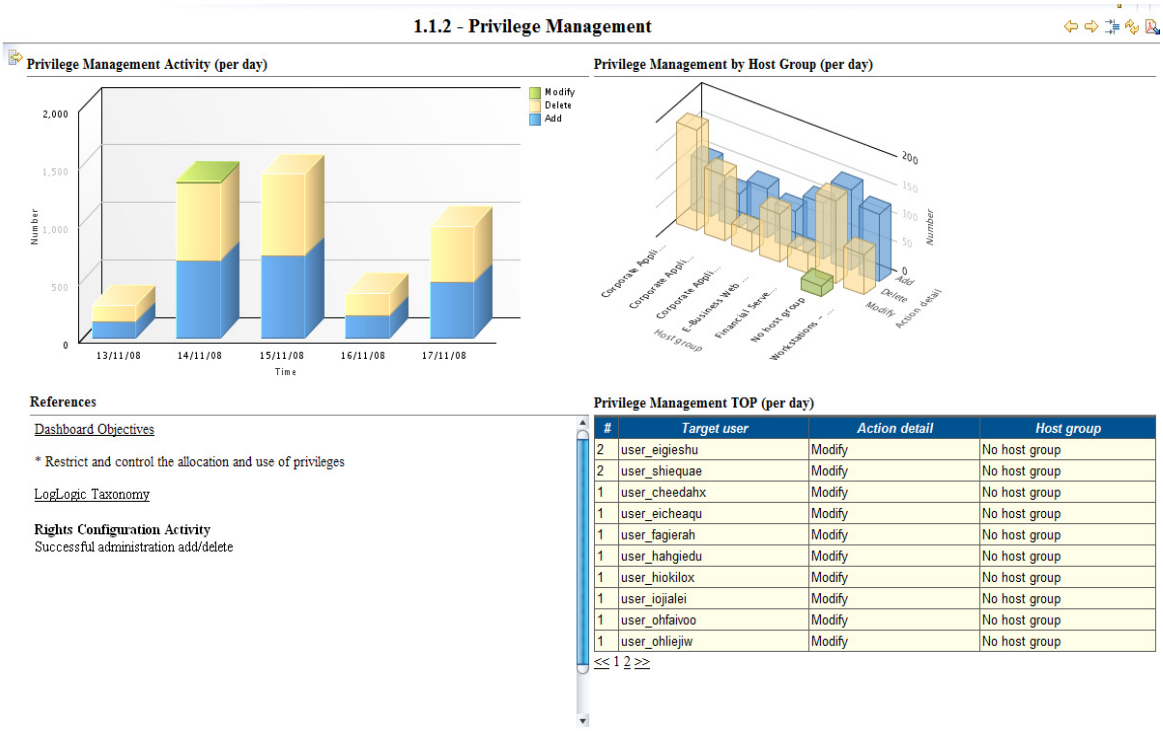
- Restrict and control the allocation and use of privileges.

TIBCO LogLogic® Taxonomy

- Rights configuration activity

successful administration add/delete

Figure 65 Privilege Management



Password Management

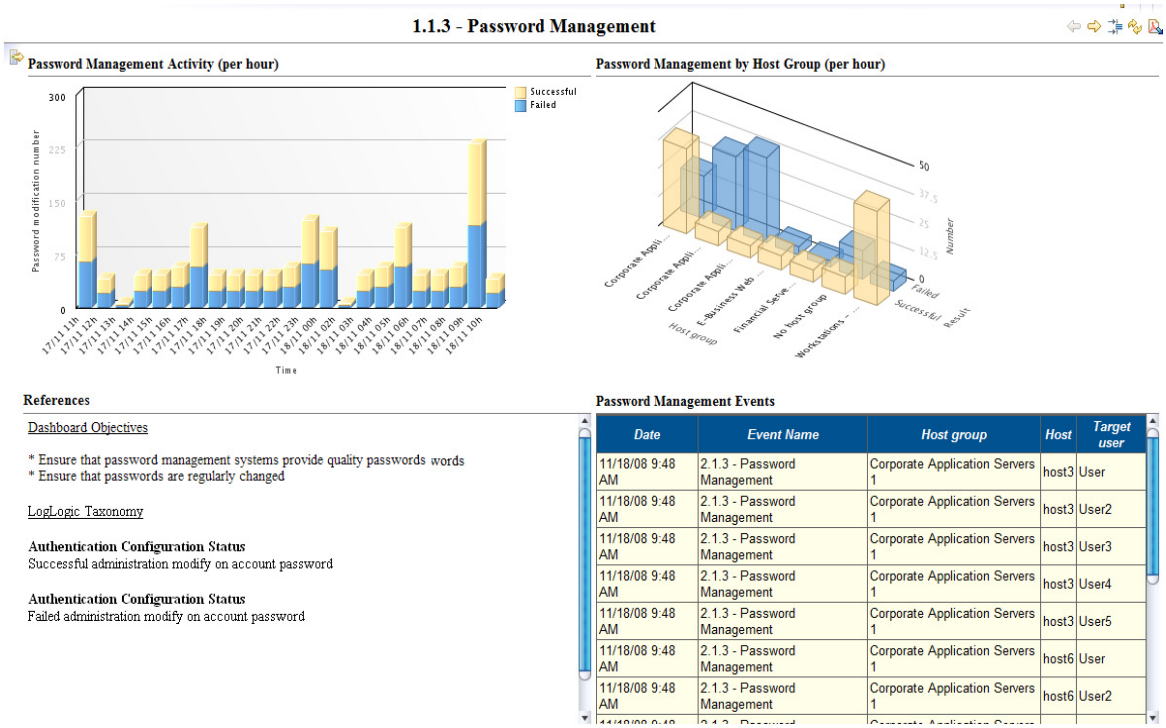
Dashboard Objectives

- Ensure that password management systems provide quality passwords.
- Ensure that passwords are regularly changed.

TIBCO LogLogic® Taxonomy

- Authentication configuration status
successful administration modify on account password
- Authentication configuration status
failed administration modify on account password

Figure 66 Password Management



User Access

System Access

Dashboard Objectives

- Prevent unauthorized access to IT Systems.
- Ensure authorized access to IT Systems.

TIBCO LogLogic® Taxonomy

- Authentication standard activity successful authentication login
- Authentication standard activity failed authentication login
- Authentication standard activity error authentication login

Figure 67 System Access

Data Access

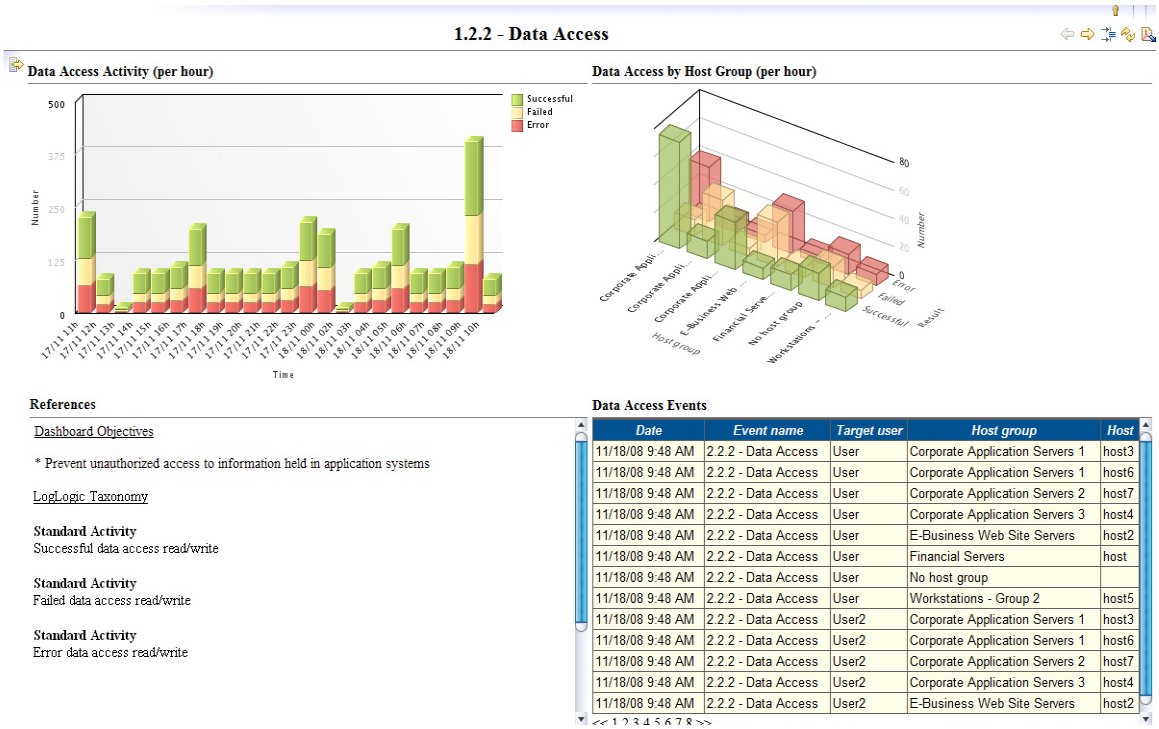
Dashboard Objectives

- Prevent unauthorized access to information held in application systems.

TIBCO LogLogic® Taxonomy

- Standard activity
successful data access read/write
- Standard activity
failed data access read/write
- Standard activity
error data access read/write

Figure 68 Data Access



Remote Access

Virtual Private Networks

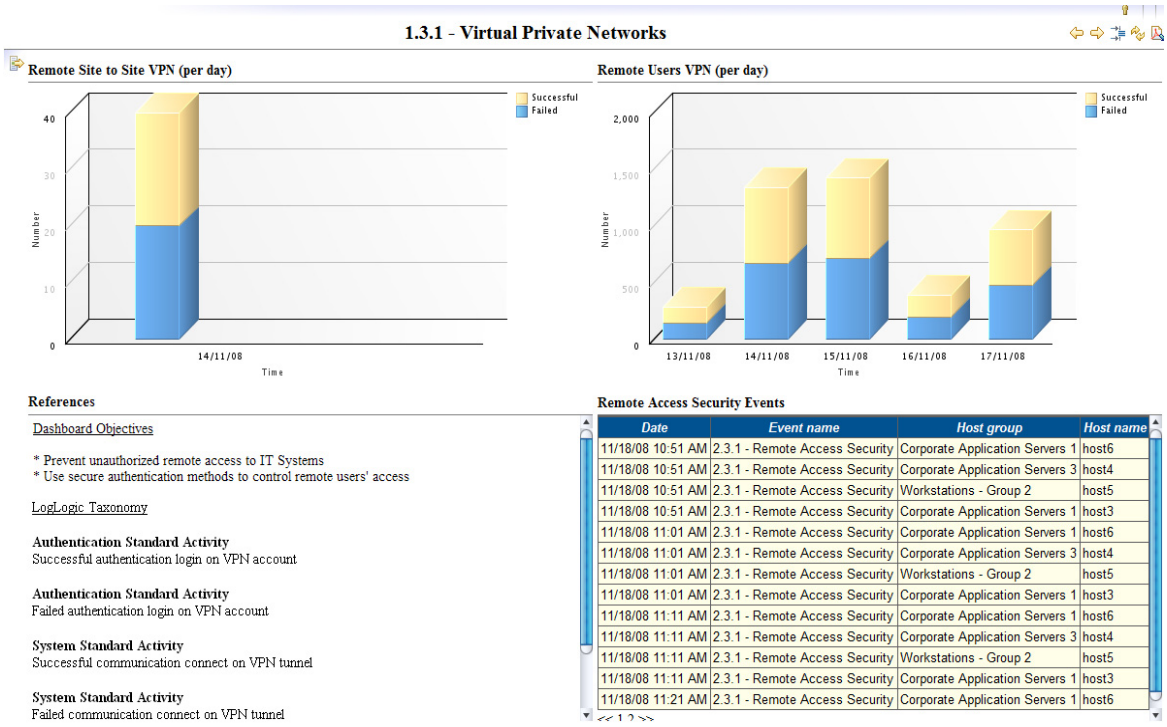
Dashboard Objectives

- Prevent unauthorized remote access to IT Systems.
- Use secure authentication methods to control remote users' access.

TIBCO LogLogic® Taxonomy

- Authentication standard activity
successful authentication login on VPN account
- Authentication standard activity
failed authentication login on VPN account
- System standard activity
successful communication connect on VPN tunnel
- System standard activity
failed communication connect on VPN tunnel

Figure 69 Virtual Private Networks



Remote Administration Security

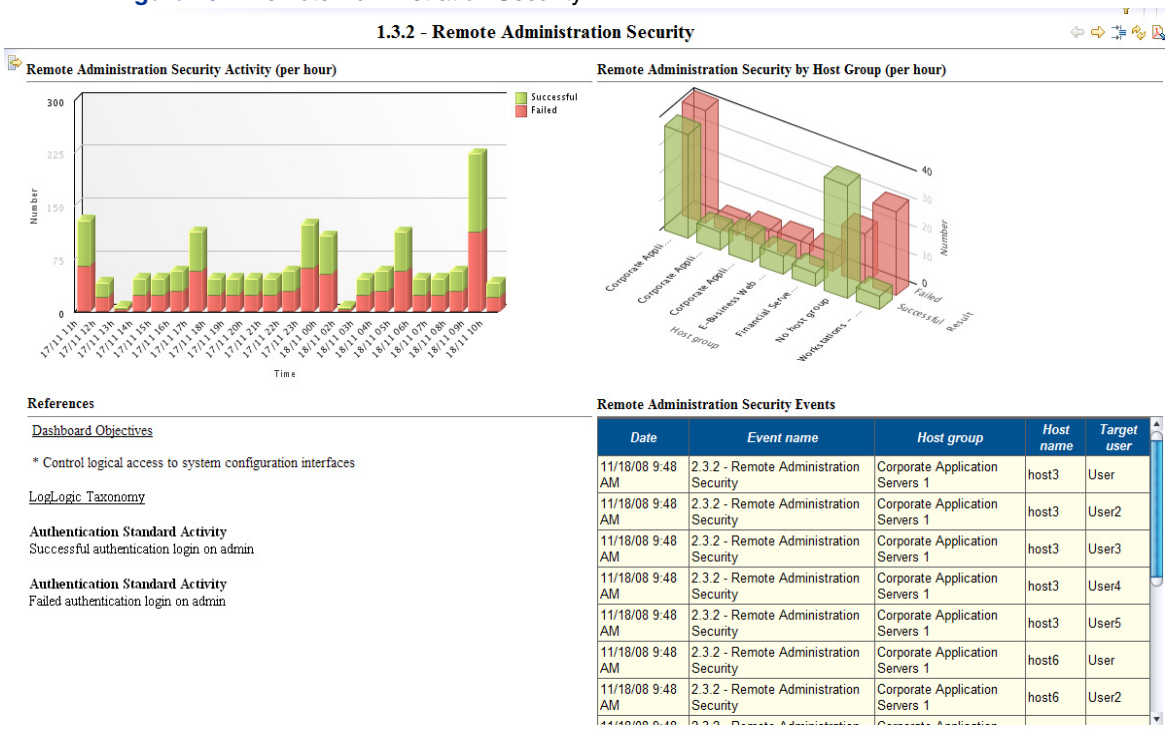
Dashboard Objectives

- Control logical access to system configuration interfaces.

TIBCO LogLogic® Taxonomy

- Authentication standard activity
successful authentication login on admin
- Authentication standard activity
failed authentication login on admin

Figure 70 Remote Administration Security



Date	Event name	Host group	Host name	Target user
11/18/08 9:48 AM	2.3.2 - Remote Administration Security	Corporate Application Servers 1	host3	User
11/18/08 9:48 AM	2.3.2 - Remote Administration Security	Corporate Application Servers 1	host3	User2
11/18/08 9:48 AM	2.3.2 - Remote Administration Security	Corporate Application Servers 1	host3	User3
11/18/08 9:48 AM	2.3.2 - Remote Administration Security	Corporate Application Servers 1	host3	User4
11/18/08 9:48 AM	2.3.2 - Remote Administration Security	Corporate Application Servers 1	host3	User5
11/18/08 9:48 AM	2.3.2 - Remote Administration Security	Corporate Application Servers 1	host6	User
11/18/08 9:48 AM	2.3.2 - Remote Administration Security	Corporate Application Servers 1	host6	User2

Sample Dashboard 2 - Operation Security

This section gives samples of Operation Security dashboards through five main themes:

- Malware Protection
  - Antivirus System States
  - Antivirus Updates
  - Malware Protection
  - Malware Infection
- Data Exchange
  - E-Mails
  - Instant Messaging
- Operation Security Management
  - Configuration Management
  - Clock Synchronization
- Network Security
  - Network Segregation
  - Network Servers
  - Network Clients
- Incident and Alert Management
  - Alerts & Victims
  - Alerts & Attackers
  - Alert Acknowledgment
- Log & Event Management
  - Collected Elementary Events
  - Events Rates (EPS)
  - Elementary Event Taxonomy
  - Log Protection

Malware Protection

Antivirus System States

Dashboard Objectives

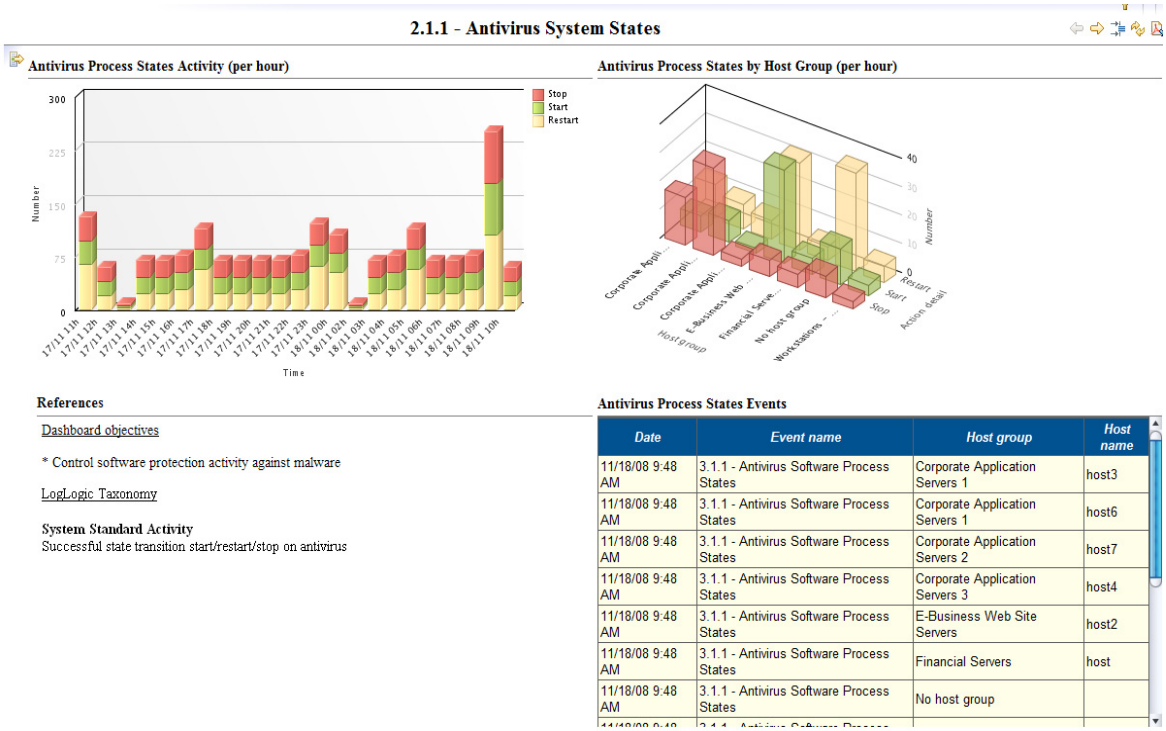
- Control software protection activity against malware.

TIBCO LogLogic® Taxonomy

- System standard activity

successful state transition start/restart/stop on antivirus

Figure 71 Antivirus System States



Date	Event name	Host group	Host name
11/18/08 9:48 AM	3.1.1 - Antivirus Software Process States	Corporate Application Servers 1	host3
11/18/08 9:48 AM	3.1.1 - Antivirus Software Process States	Corporate Application Servers 1	host6
11/18/08 9:48 AM	3.1.1 - Antivirus Software Process States	Corporate Application Servers 2	host7
11/18/08 9:48 AM	3.1.1 - Antivirus Software Process States	Corporate Application Servers 3	host4
11/18/08 9:48 AM	3.1.1 - Antivirus Software Process States	E-Business Web Site Servers	host2
11/18/08 9:48 AM	3.1.1 - Antivirus Software Process States	Financial Servers	host
11/18/08 9:48 AM	3.1.1 - Antivirus Software Process States	No host group	

Antivirus Updates

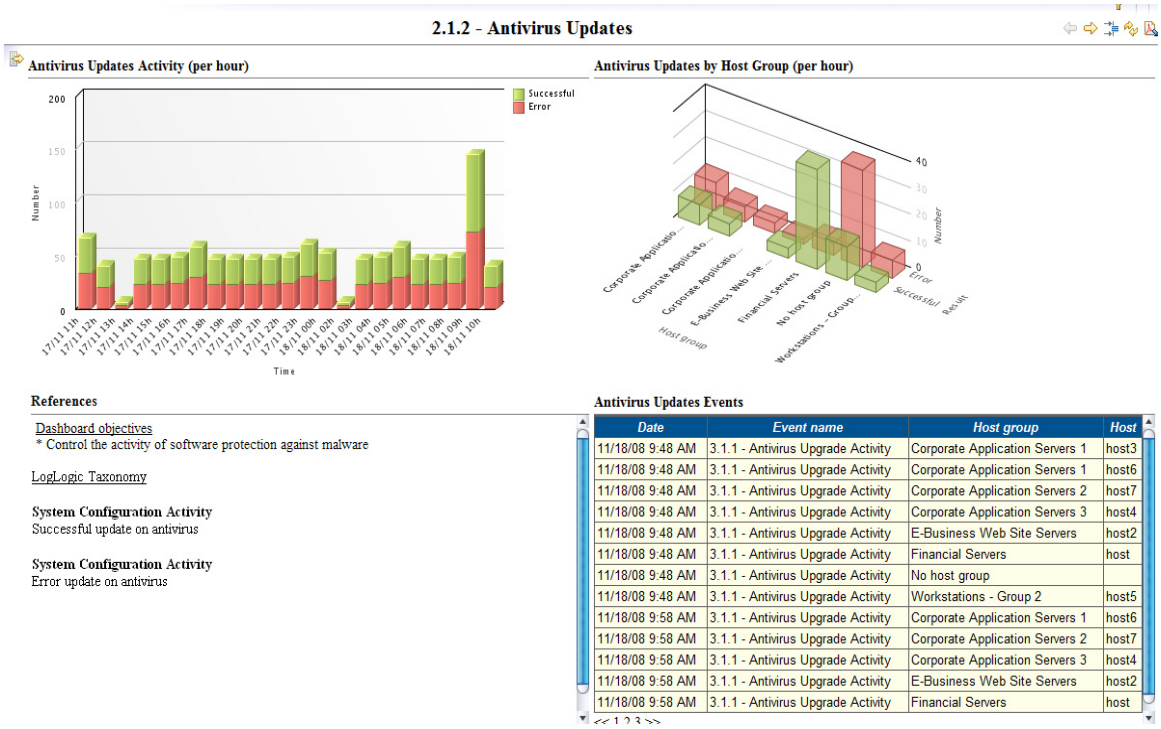
Dashboard Objectives

- Control the activity of software protection against malware.

TIBCO LogLogic® Taxonomy

- System configuration activity successful update on antivirus
- System configuration activity error update on antivirus

Figure 72 Antivirus Updates



Malware Protection

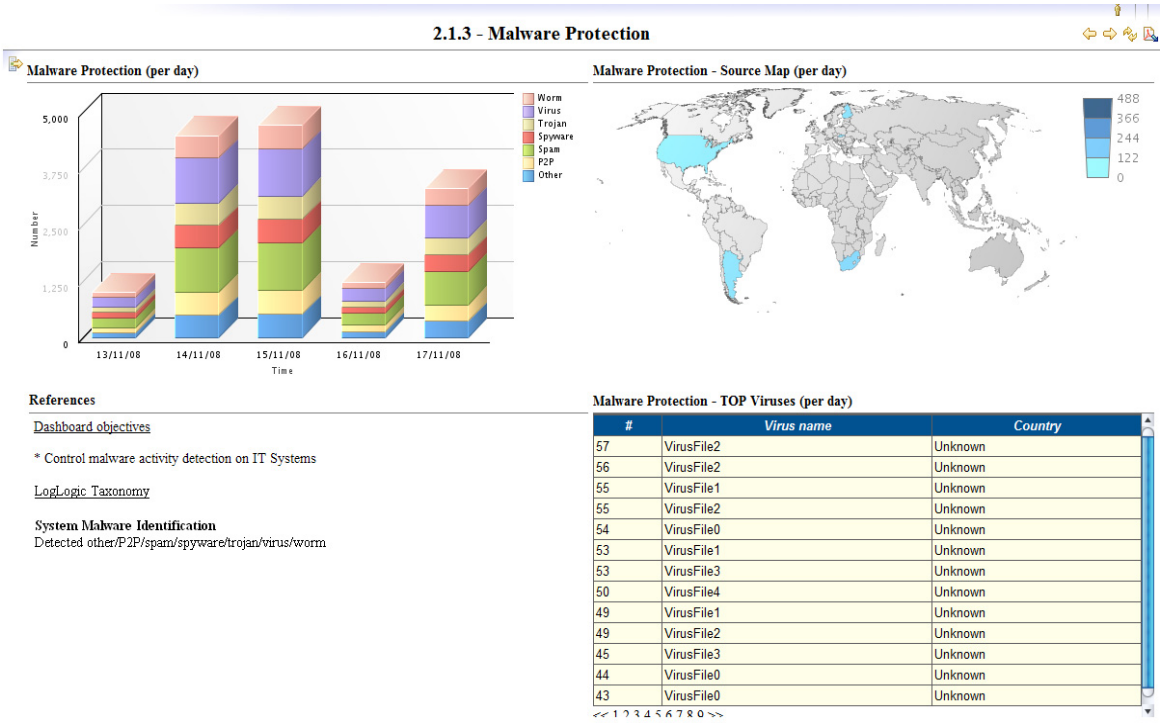
Dashboard Objectives

- Control malware activity detection on IT Systems.

TIBCO LogLogic® Taxonomy

- System malware identification
detected other/P2P/spam/spyware/trojan/virus/worm

Figure 73 Malware Protection



Malware Infection

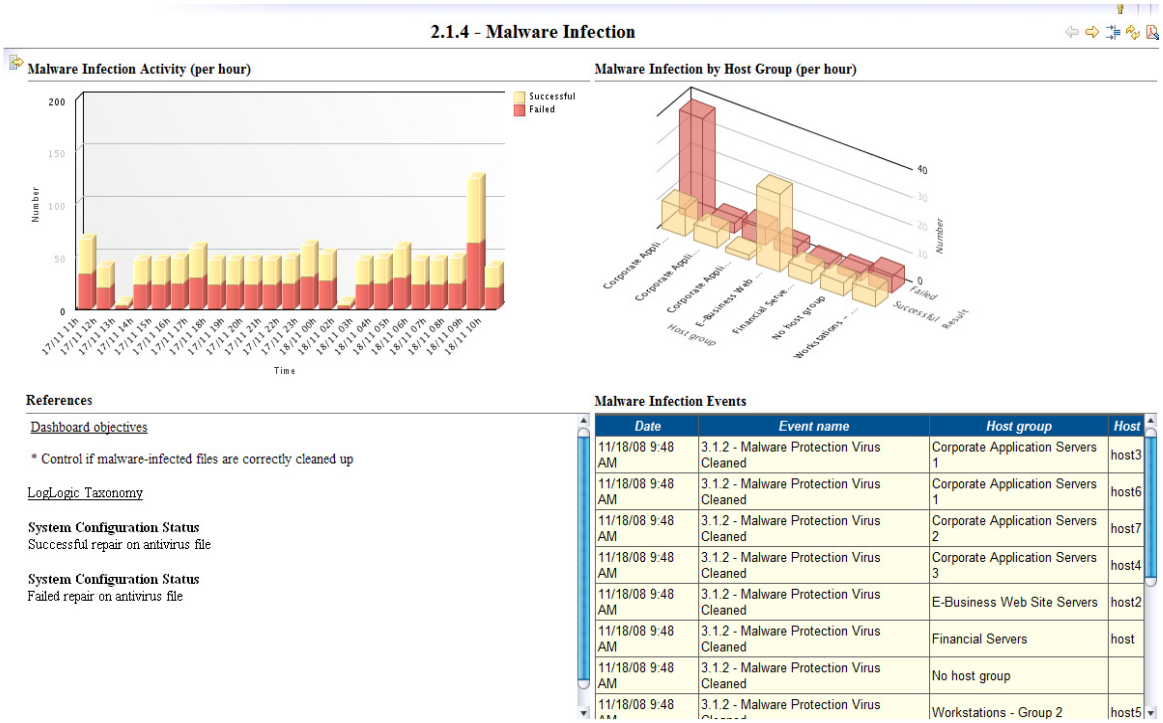
Dashboard Objectives

- Control if malware-infected files are correctly cleaned up.

TIBCO LogLogic® Taxonomy

- System configuration status successful repair on antivirus file
- System configuration status failed repair on antivirus file

Figure 74 Malware Infection



Date	Event name	Host group	Host
11/18/08 9:48 AM	3.1.2 - Malware Protection Virus Cleaned	Corporate Application Servers 1	host3
11/18/08 9:48 AM	3.1.2 - Malware Protection Virus Cleaned	Corporate Application Servers 1	host6
11/18/08 9:48 AM	3.1.2 - Malware Protection Virus Cleaned	Corporate Application Servers 2	host7
11/18/08 9:48 AM	3.1.2 - Malware Protection Virus Cleaned	Corporate Application Servers 3	host4
11/18/08 9:48 AM	3.1.2 - Malware Protection Virus Cleaned	E-Business Web Site Servers	host2
11/18/08 9:48 AM	3.1.2 - Malware Protection Virus Cleaned	Financial Servers	host
11/18/08 9:48 AM	3.1.2 - Malware Protection Virus Cleaned	No host group	
11/18/08 9:48 AM	3.1.2 - Malware Protection Virus Cleaned	Workstations - Group 2	host5

Data Exchange

E-Mails

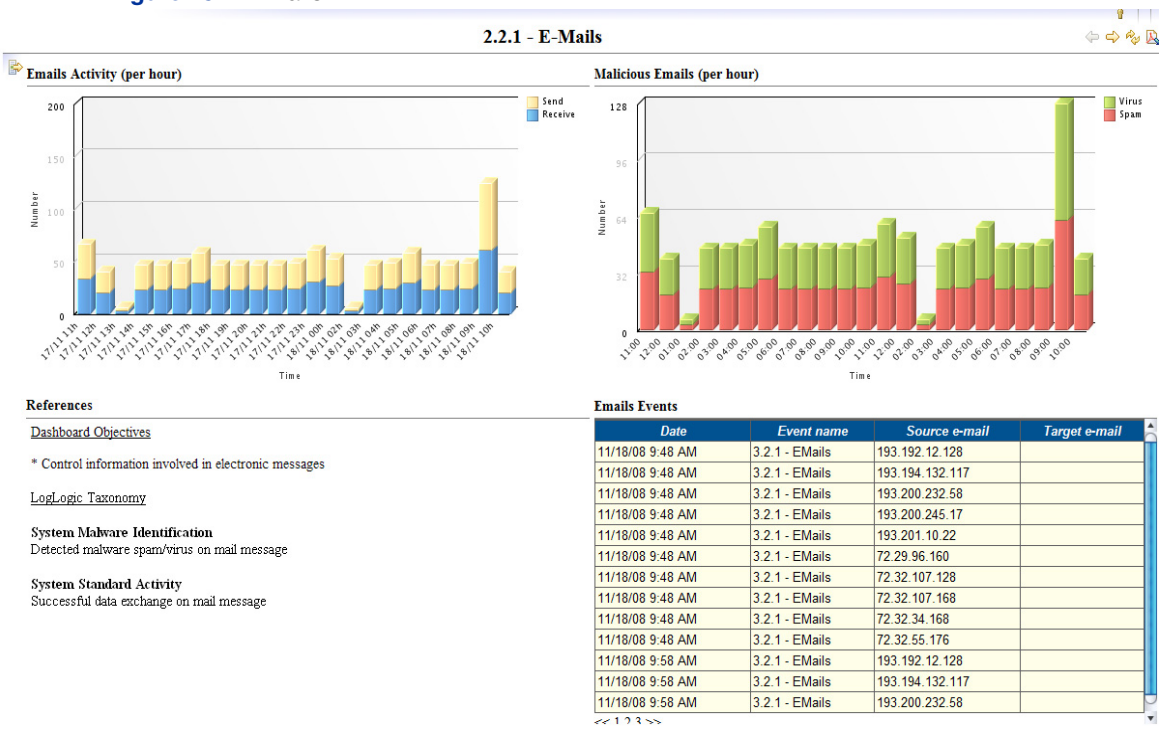
Dashboard Objectives

- Control information involved in electronic messages.

TIBCO LogLogic® Taxonomy

- System malware identification
detected malware spam/virus on mail message
- System standard activity
successful data exchange on mail message

Figure 75 E-Mails



Instant Messaging

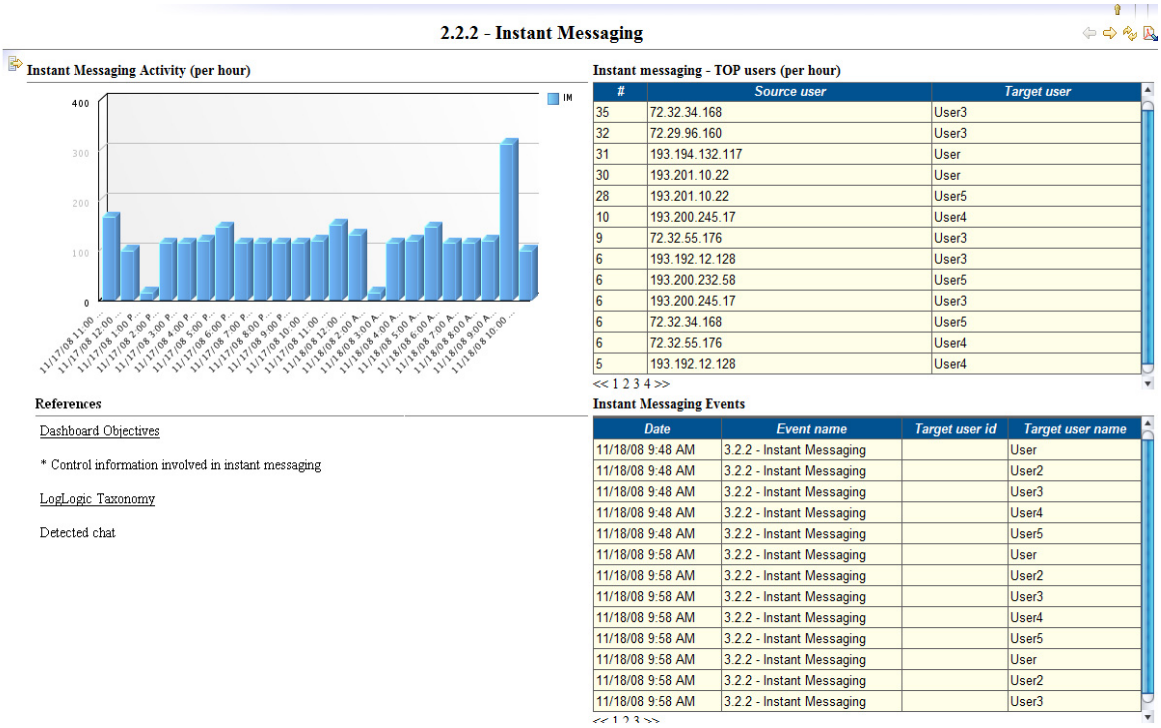
Dashboard Objectives

- Control information involved in instant messaging.

TIBCO LogLogic® Taxonomy

- Detected chat.

Figure 76 Instant Messaging



Operation Security Management

Configuration Management

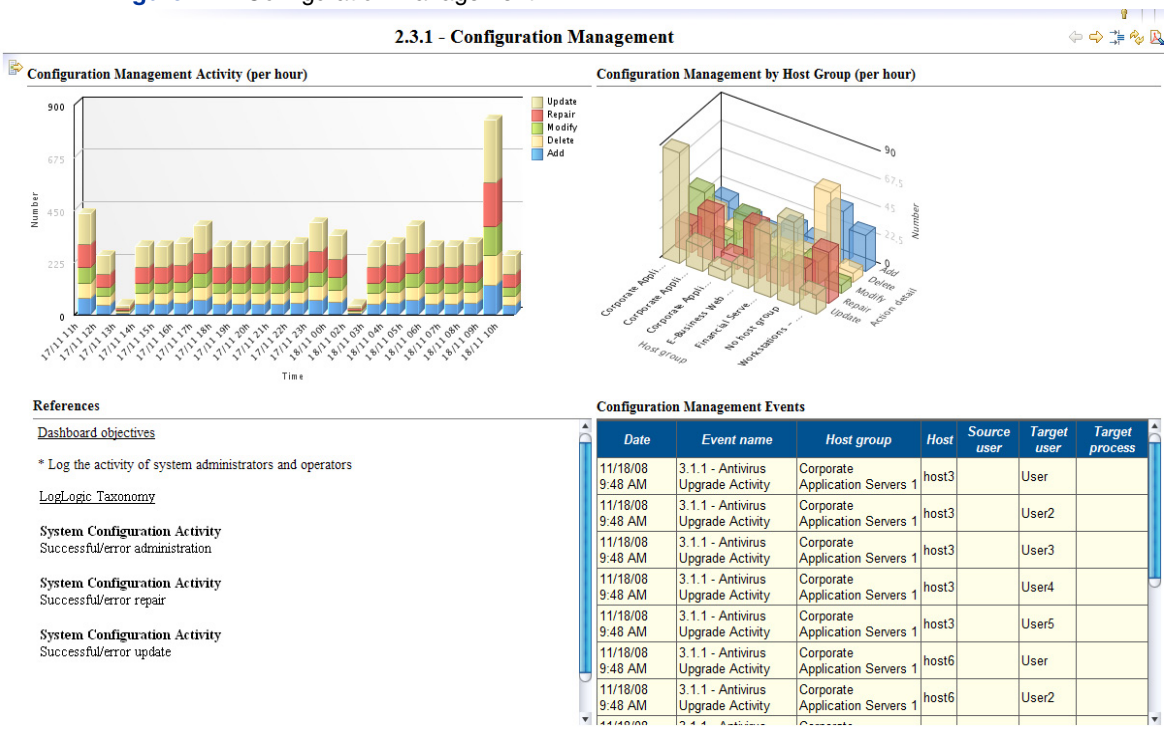
Dashboard Objectives

- Log the activity of system administrators and operators.

TIBCO LogLogic® Taxonomy

- System configuration activity successful/error administration
- System configuration activity successful/error repair
- System configuration activity successful/error update.

Figure 77 Configuration Management



Clock Synchronization

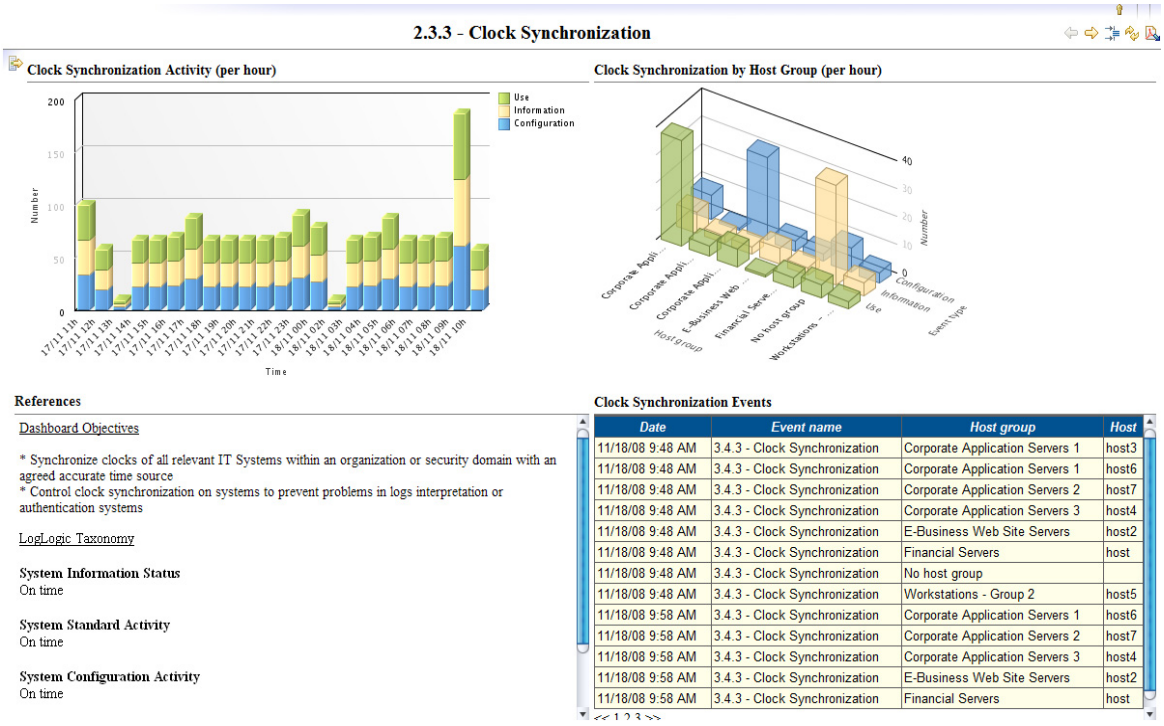
Dashboard Objectives

- Synchronize clocks of all relevant IT Systems within an organization or security domain with an agreed accurate time source.
- Control clock synchronization on systems to prevent problems in logs interpretation or authentication systems.

TIBCO LogLogic® Taxonomy

- System information status on time
- System standard activity on time
- System configuration activity on time

Figure 78 Clock Synchronization



Network Security

Network Segregation

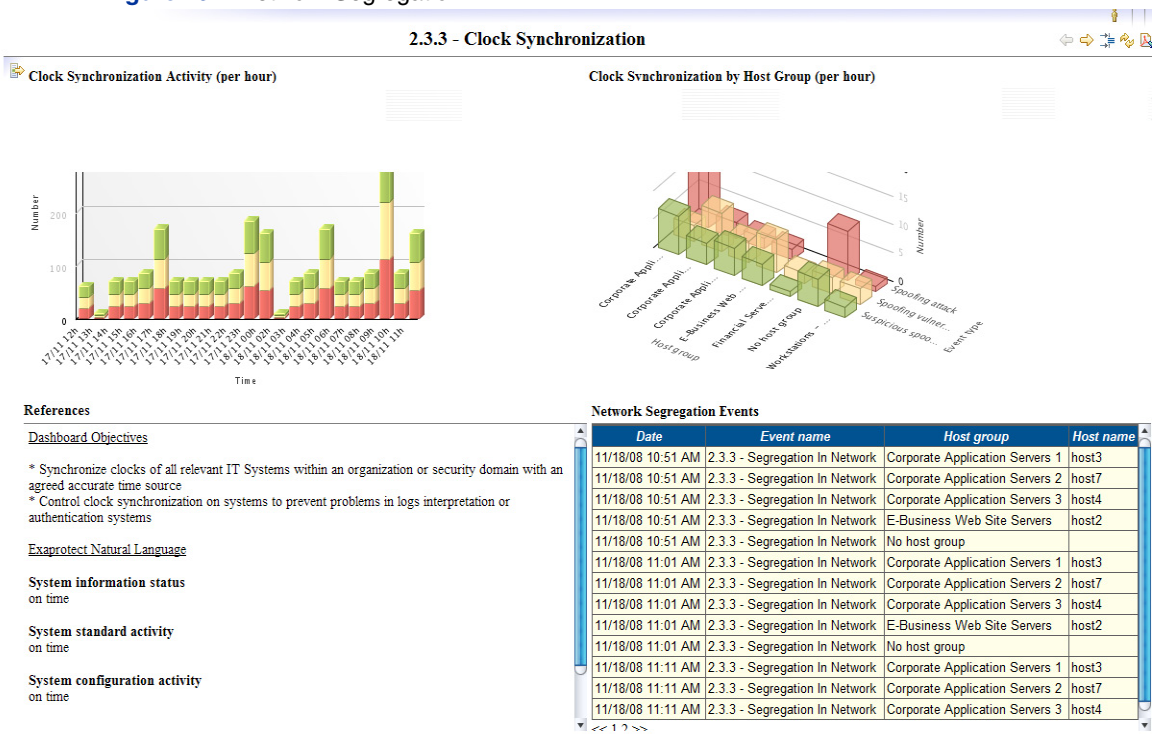
Dashboard Objectives

- Control that the segregation policy defined between different networks is efficient.
- Ensure that groups of information services, users, and information systems are segregated on networks.

TIBCO LogLogic® Taxonomy

- Suspicious activity identification
detected spoofing
- Vulnerability status
detected spoofing
- Attack identification
detected spoofing

Figure 79 Network Segregation



Network Servers

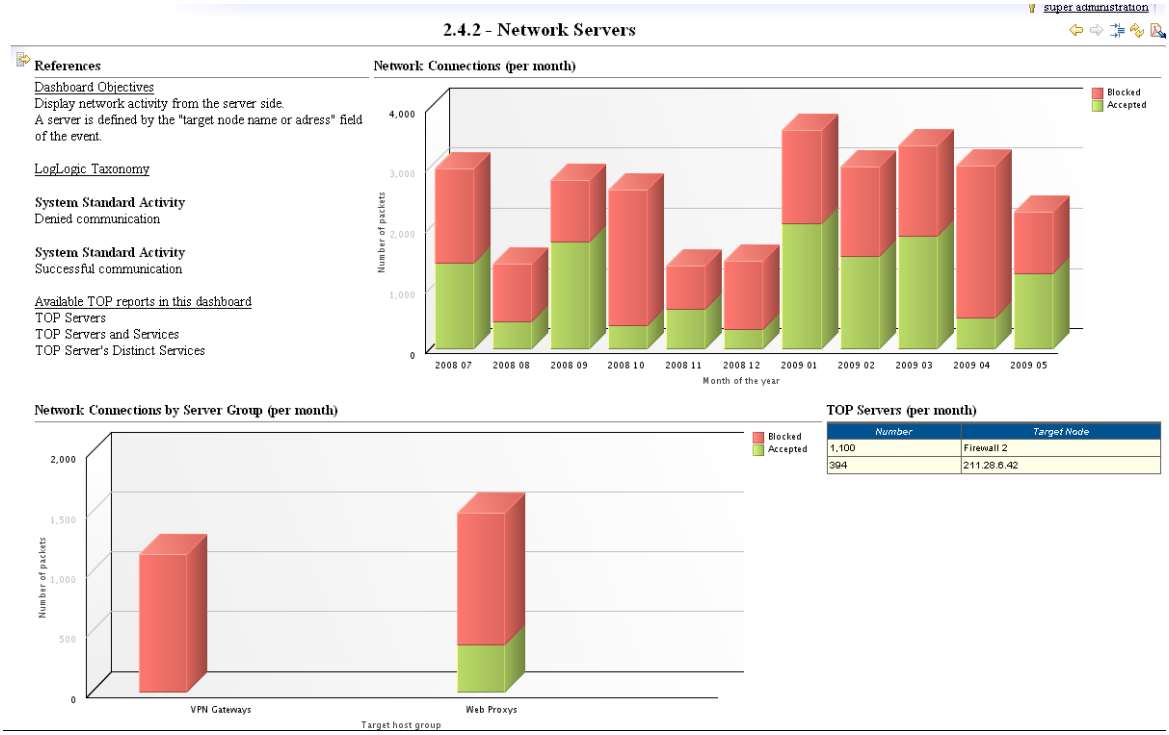
Dashboard Objectives

- Display network activity from the server side. A server is defined by the "target node name or address" field of the event.

TIBCO LogLogic® Taxonomy

- System standard activity
Denied communication
- System standard activity
Successful communication

Figure 80 Network Servers



Network Clients

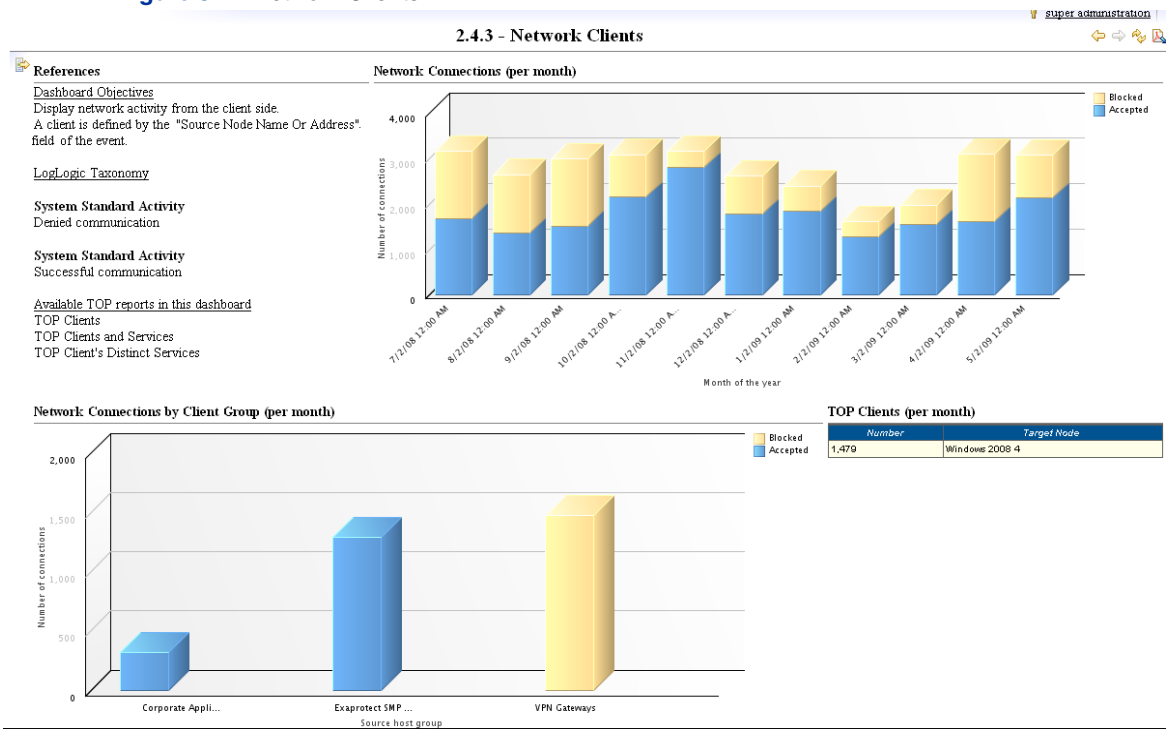
Dashboard Objectives

- Display network activity from the client side. A client is defined by the "Source node name or adress" field of the event.

TIBCO LogLogic® Taxonomy

- System Standard Activity
Denied communication
- System Standard Activity
Successful communication

Figure 81 Network Clients



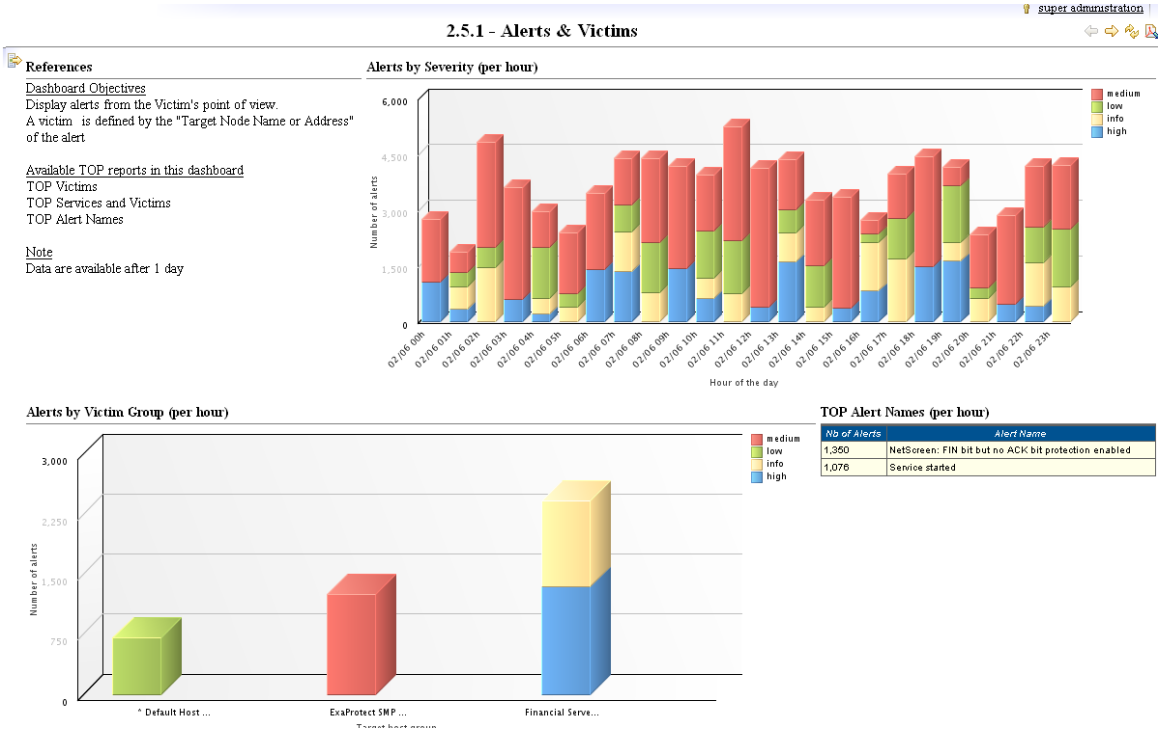
Incident and Alert Management

Alerts & Victims

Dashboard Objectives

- Display alerts from the Victim's point of view. A victim is defined by the "Target Node Name or Address" of the alert.

Figure 82 Alerts & Victims

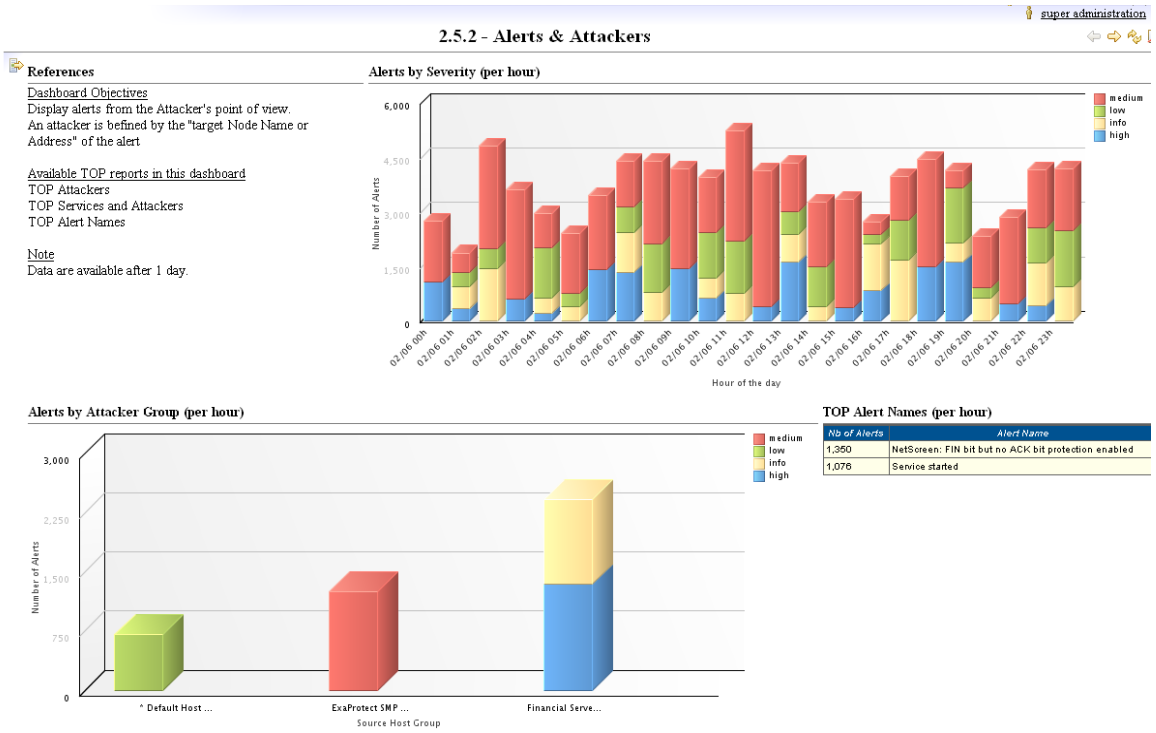


Alerts & Attackers

Dashboard Objectives

- Display alerts from the Attacker's point of view. An attacker is defined by the "Target Node Name or Address" of the alert.

Figure 83 Alerts & Attackers

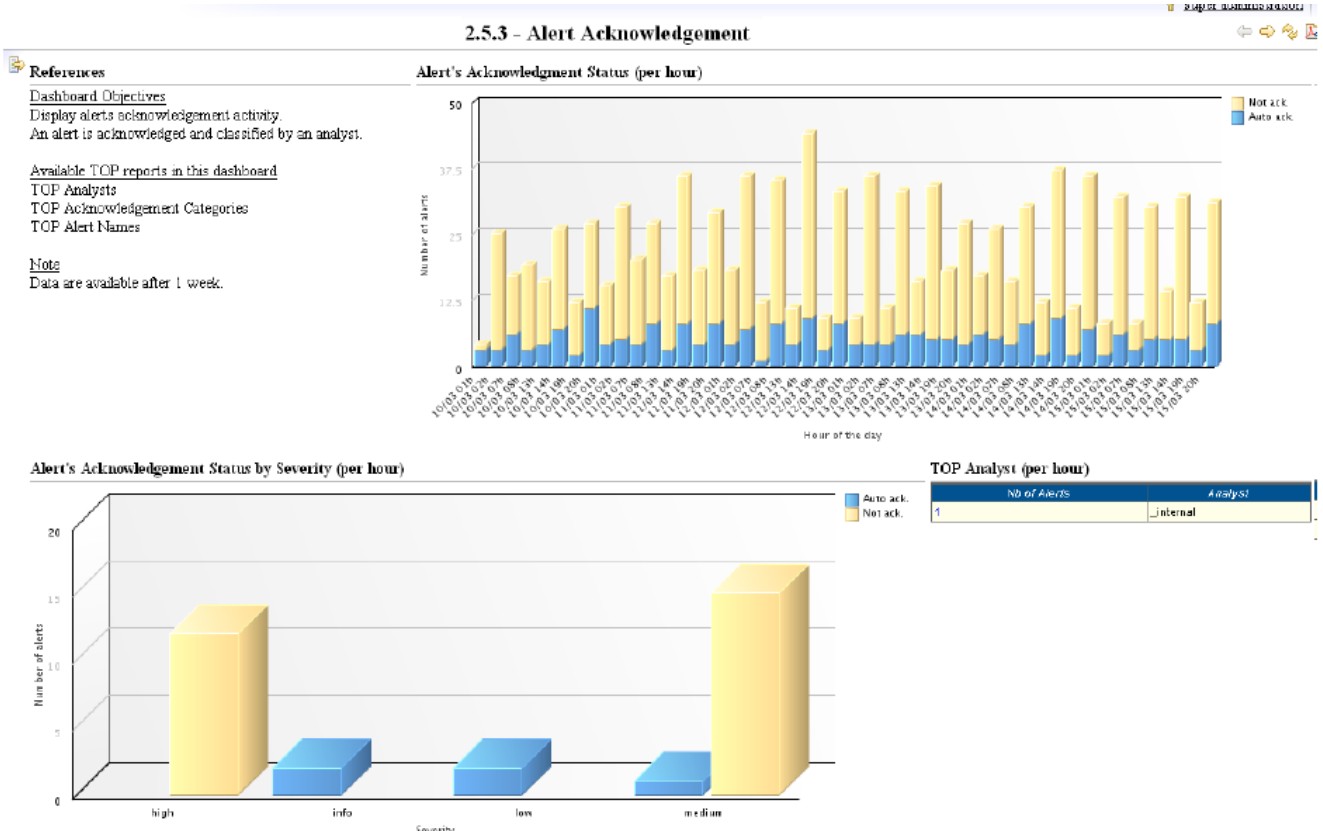


Alert Acknowledgment

Dashboard Objectives

- Display alerts acknowledgement activity.
- An alert is acknowledged and classified by an analyst.

Figure 84 Alerts Acknowledgement



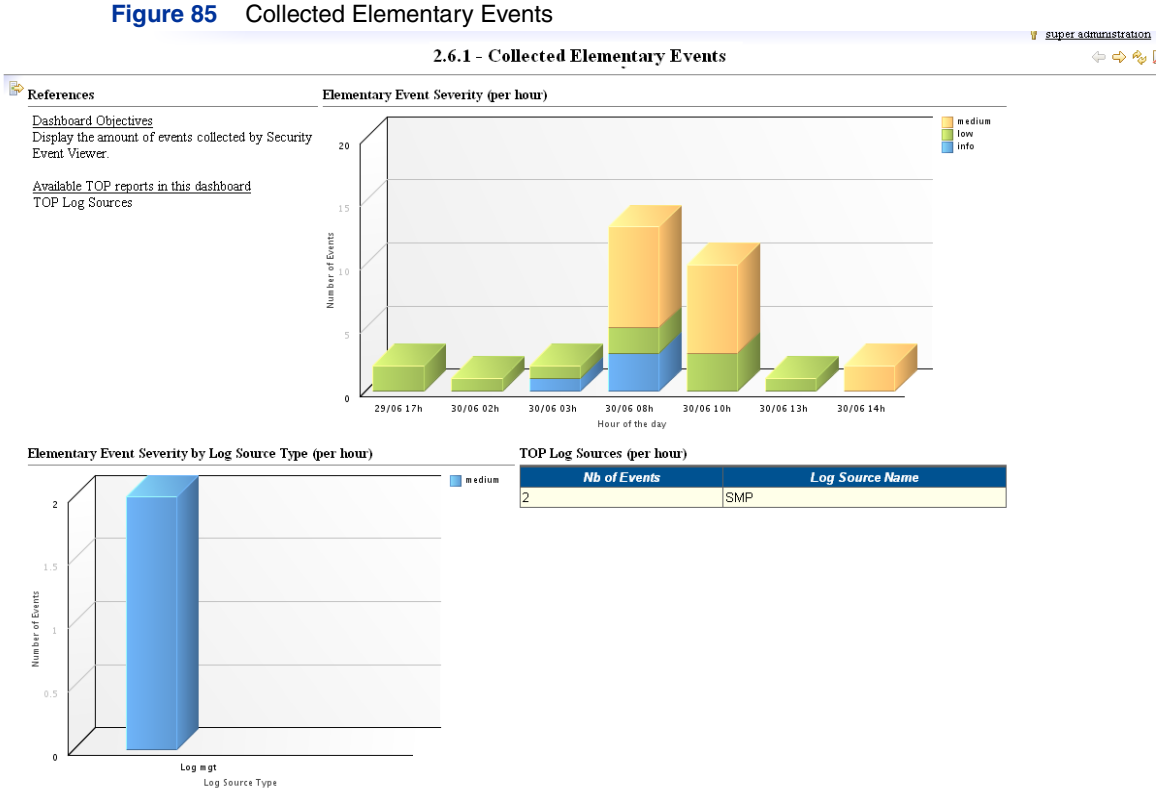
Log & Event Management

Collected Elementary Events

Dashboard Objectives

- Display the amount of events collected by Security Event Viewer.

Figure 85 Collected Elementary Events

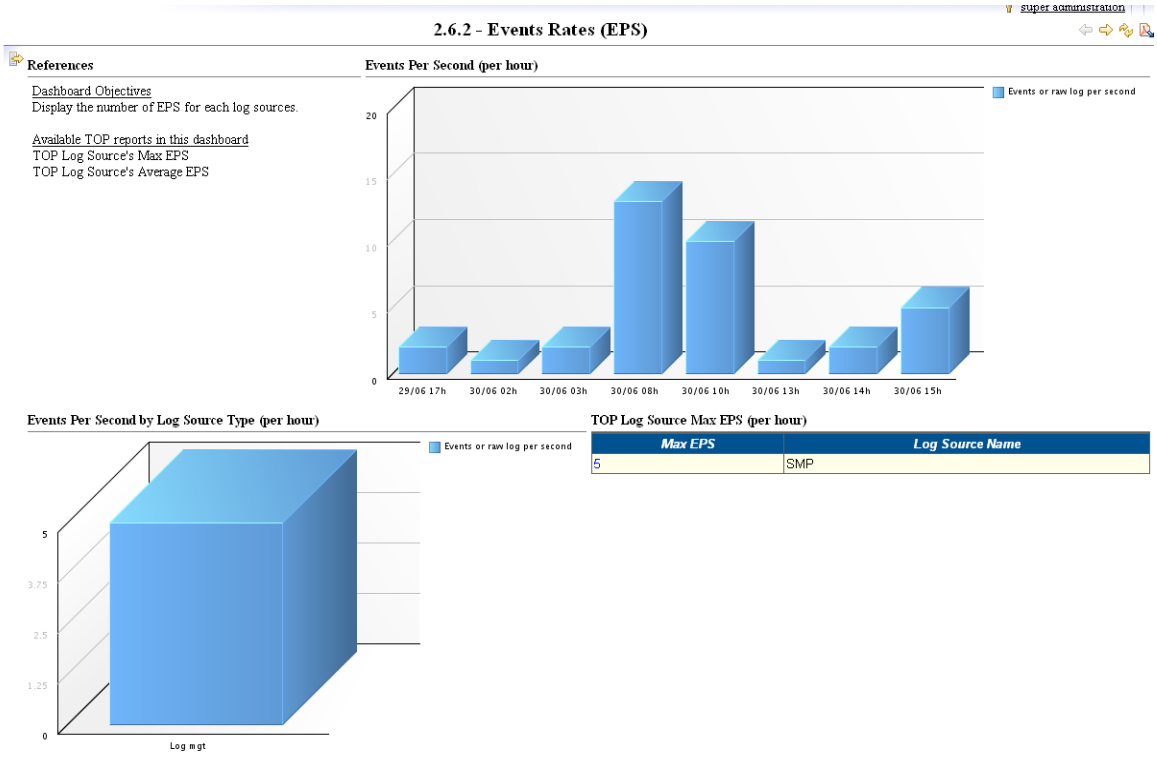


Events Rates (EPS)

Dashboard Objectives

- Display the number of EPS for each log source.

Figure 86 Events Rates (EPS)

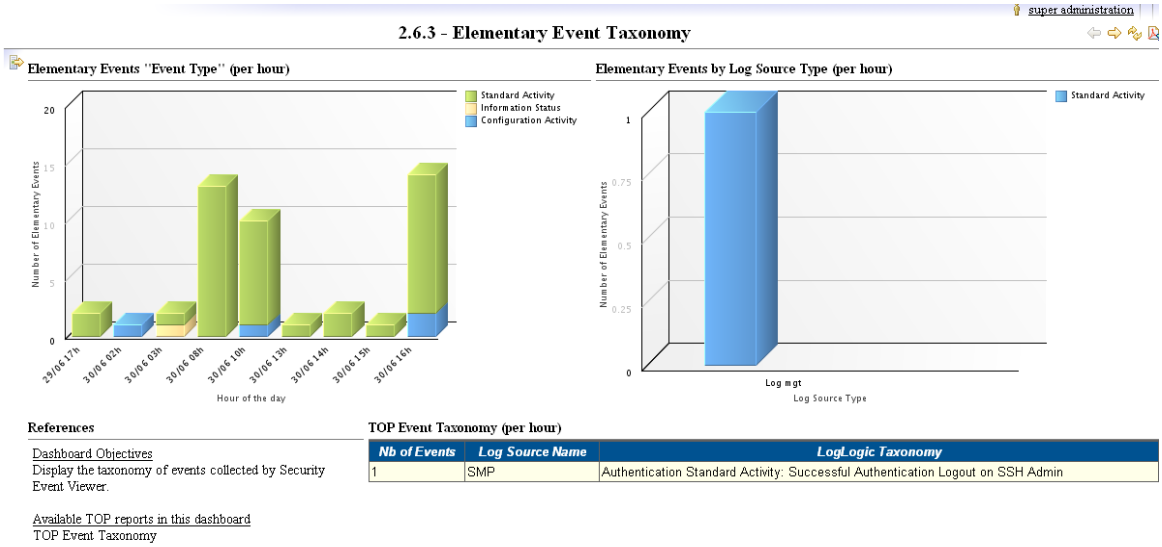


Elementary Event Taxonomy

Dashboard Objectives

- Display the Taxonomy of events collected by Security Event Viewer.

Figure 87 Elementary Event Taxonomy



Log Protection

Dashboard Objectives

- Protect logging devices and logs against tampering and unauthorized access.

TIBCO LogLogic® Taxonomy

- System suspicious activity

Detected on log file

- System malware/attack identification

Detected on log file

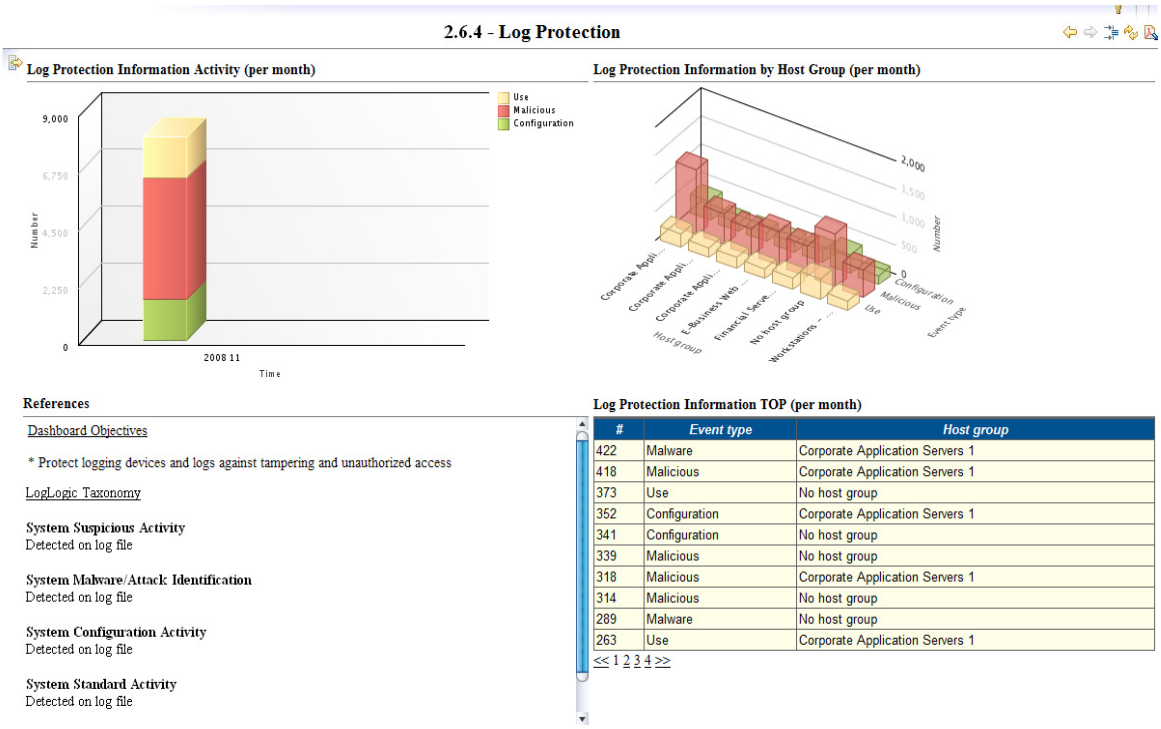
- System configuration activity

Detected on log file

- System standard activity

Detected on log file

Figure 88 Log Protection



Sample Dashboard 3 - Asset Security

This section gives samples of Asset Security dashboards through six main themes:

- Asset Identification
- Change Management
- Backup Management
- Capacity Management
- Vulnerability Management
- Asset Availability

Asset Identification

Asset Inventory and Ownership

Dashboard Objectives

- Achieve and maintain appropriate protection of organizational assets
- Identify all assets and maintain an inventory
- Identify for each asset the part of the organization that owns it.

Figure 89 Asset Inventory and Ownership

3.1.1 - Asset Inventory and Ownership

References

Dashboard Objectives

* Achieve and maintain appropriate protection of organizational assets
* Identify all assets and maintain an inventory
* Identify for each asset the part of the organization that owns it

Asset Inventory

Electronic Mails - Criticality : medium

Host Group Name	Site Name	Host Name
Windows Domain Controllers	* Default Site	mydc.exaprotect.fr
Windows Domain Controllers	* Default Site	mydc2.exaprotect.fr

Remote Access - Criticality : medium

Host Group Name	Site Name	Host Name
Windows Domain Controllers	* Default Site	mydc.exaprotect.fr
Windows Domain Controllers	* Default Site	mydc2.exaprotect.fr

Security Monitoring - Criticality : high

Host Group Name	Site Name	Host Name
Exaprotect SMP Servers	* Default Site	smp

Web Access - Criticality : medium

Host Group Name	Site Name	Host Name
Windows Domain Controllers	* Default Site	mydc.exaprotect.fr
Windows Domain Controllers	* Default Site	mydc2.exaprotect.fr

Change Management

Change Management

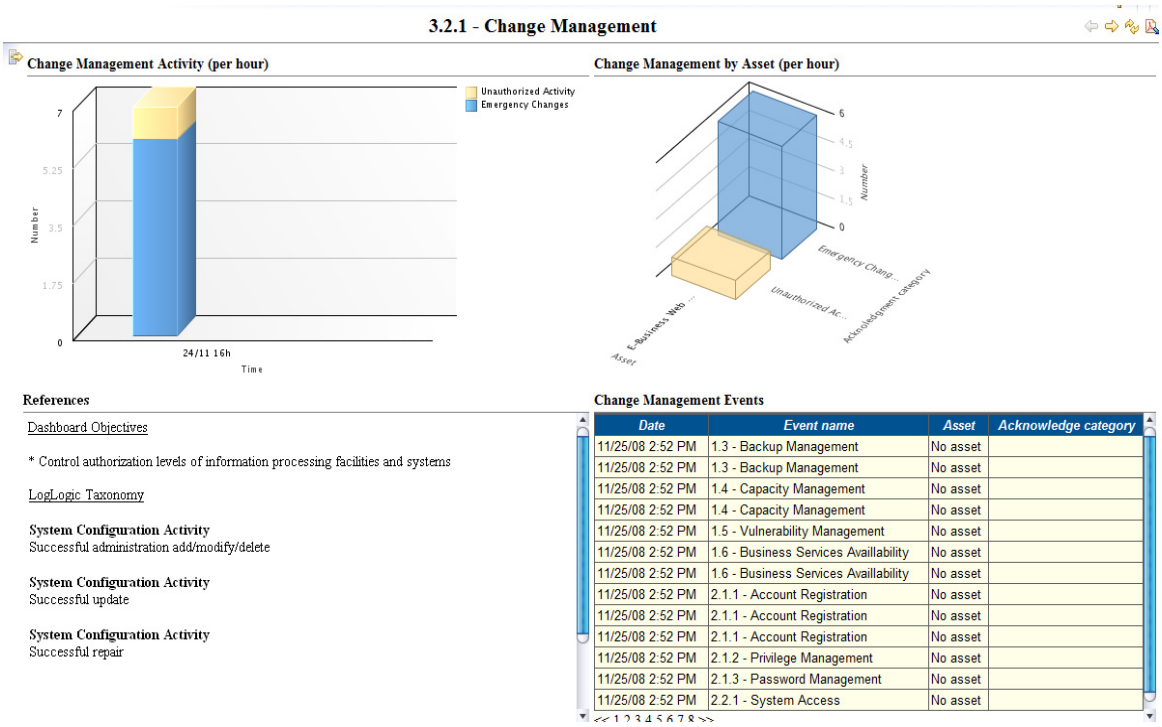
Dashboard Objectives

- Control authorization levels of information processing facilities and systems.

TIBCO LogLogic® Taxonomy

- System configuration activity
successful administration add/modify/delete
- System configuration activity
successful update
- System configuration activity
successful repair

Figure 90 Change Management



Backup Management

Backup Management

Dashboard Objectives

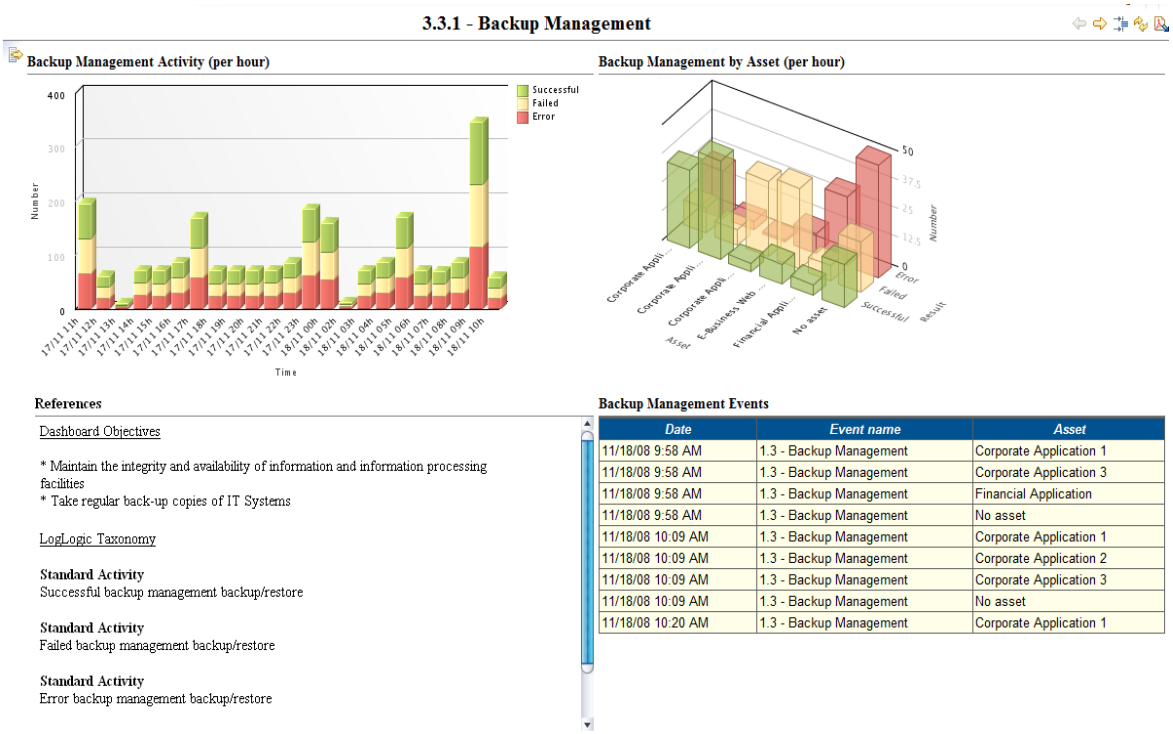
- Maintain the integrity and availability of information and information processing facilities.
- Take regular backup copies of IT Systems.

TIBCO LogLogic® Taxonomy

- Success use backup management backup/restore.

- Failed use backup management backup/restore.
- Error use backup management backup/restore.

Figure 91 Backup Management



Date	Event name	Asset
11/18/08 9:58 AM	1.3 - Backup Management	Corporate Application 1
11/18/08 9:58 AM	1.3 - Backup Management	Corporate Application 3
11/18/08 9:58 AM	1.3 - Backup Management	Financial Application
11/18/08 9:58 AM	1.3 - Backup Management	No asset
11/18/08 10:09 AM	1.3 - Backup Management	Corporate Application 1
11/18/08 10:09 AM	1.3 - Backup Management	Corporate Application 2
11/18/08 10:09 AM	1.3 - Backup Management	Corporate Application 3
11/18/08 10:09 AM	1.3 - Backup Management	No asset
11/18/08 10:20 AM	1.3 - Backup Management	Corporate Application 1

Capacity Management

Capacity Management

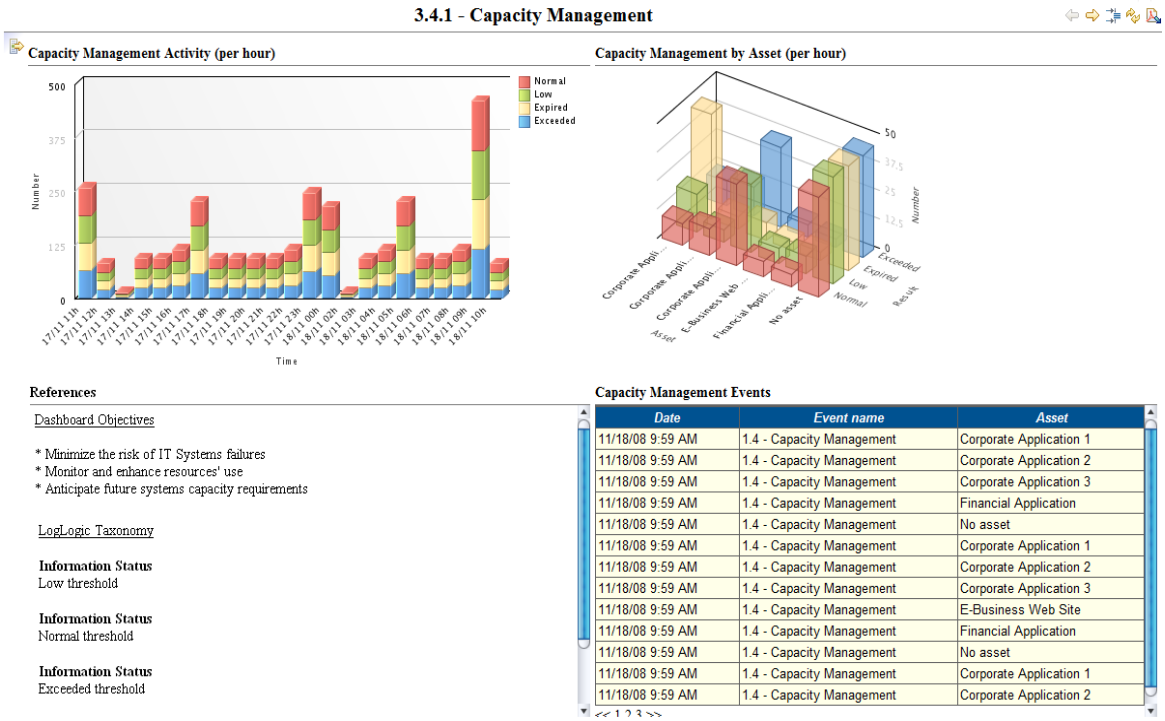
Dashboard Objectives

- Minimize the risk of IT Systems failures.
- Monitor and enhance resources' use.
- Anticipate future systems capacity requirements.

TIBCO LogLogic® Taxonomy

- Information status
low threshold
- Information status
normal threshold
- Information status
exceeded threshold
- Information status
expired threshold

Figure 92 Capacity Management



Vulnerability Management

Vulnerability Management

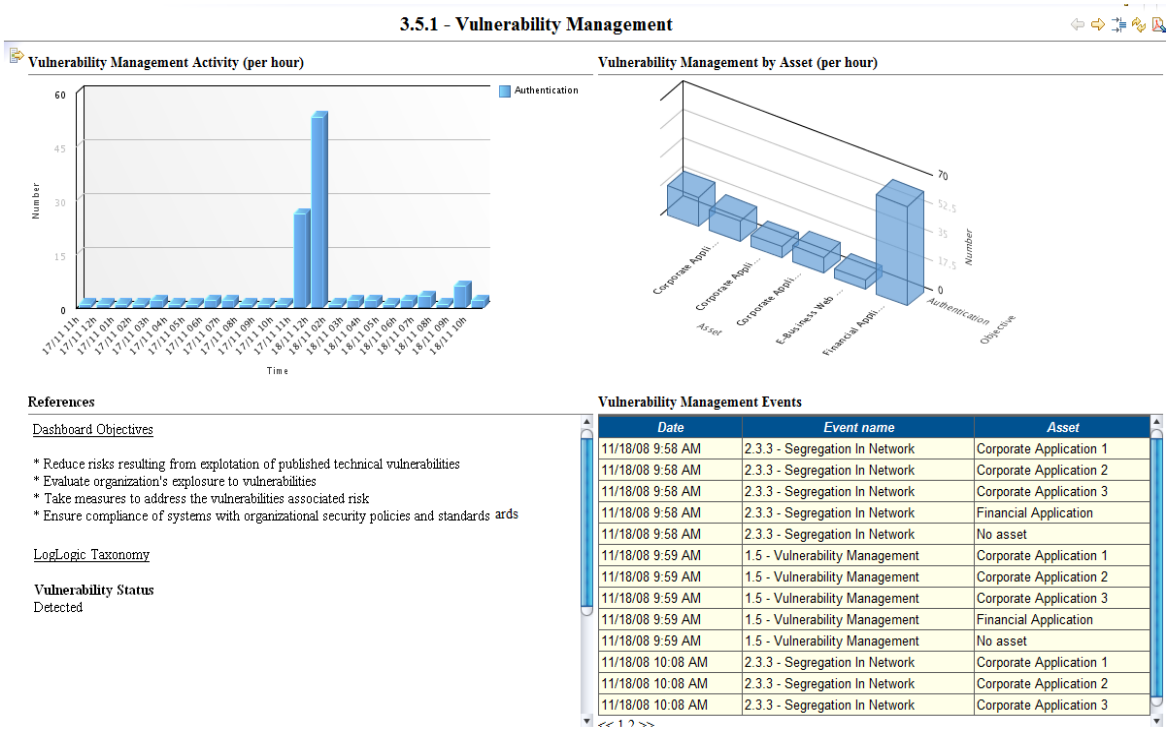
Dashboard Objectives

- Reduce risks resulting from exploitation of published technical vulnerabilities.
- Evaluate organization's explosure to vulnerabilities.
- Take measures to address the vulnerabilities associated risk.
- Ensure compliance of systems with organizational security policies and standards.

TIBCO LogLogic® Taxonomy

- Vulnerability status detected

Figure 93 Vulnerability Management



Asset Availability

Asset Availability

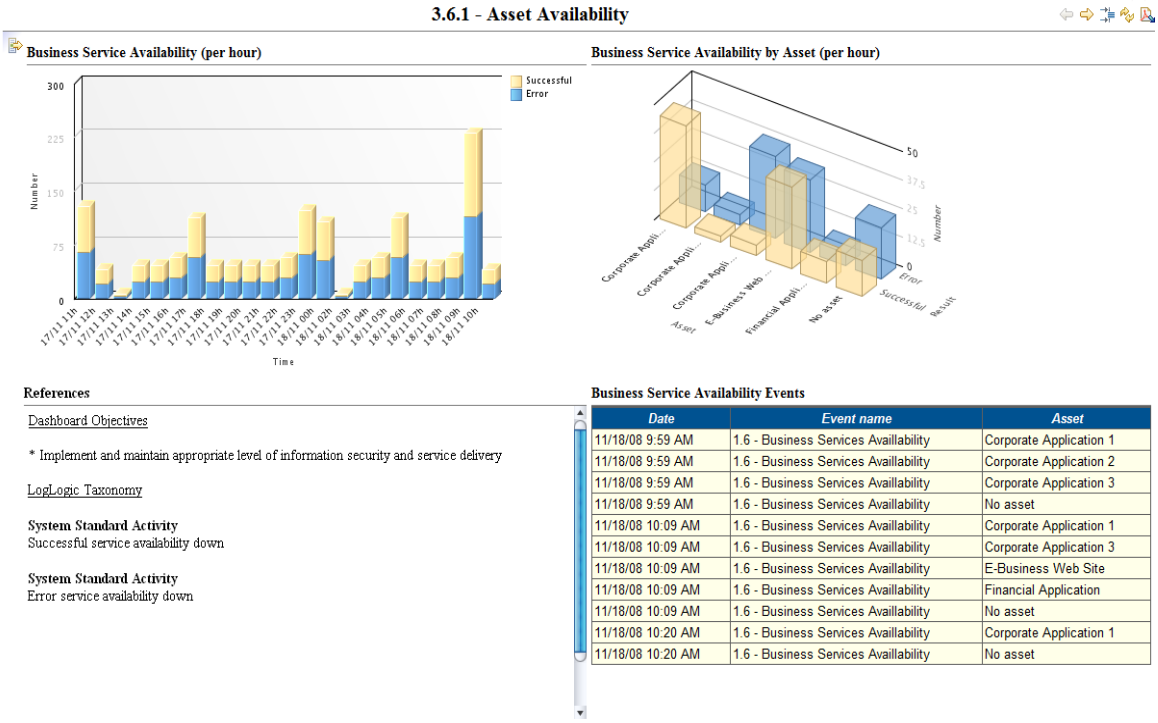
Dashboard Objectives

- Implement and maintain appropriate level of information security and service delivery.

TIBCO LogLogic® Taxonomy

- System standard activity
successful service availability down
- System standard activity
error service availability down

Figure 94 Asset Availability



Date	Event name	Asset
11/18/08 9:59 AM	1.6 - Business Services Availability	Corporate Application 1
11/18/08 9:59 AM	1.6 - Business Services Availability	Corporate Application 2
11/18/08 9:59 AM	1.6 - Business Services Availability	Corporate Application 3
11/18/08 9:59 AM	1.6 - Business Services Availability	No asset
11/18/08 10:09 AM	1.6 - Business Services Availability	Corporate Application 1
11/18/08 10:09 AM	1.6 - Business Services Availability	Corporate Application 3
11/18/08 10:09 AM	1.6 - Business Services Availability	E-Business Web Site
11/18/08 10:09 AM	1.6 - Business Services Availability	Financial Application
11/18/08 10:09 AM	1.6 - Business Services Availability	No asset
11/18/08 10:20 AM	1.6 - Business Services Availability	Corporate Application 1
11/18/08 10:20 AM	1.6 - Business Services Availability	No asset

Sample Dashboard - Executive Report, Regulatory Compliance, SANS Top 5 and PDF Reports

Dashboards based on compliance are the same as the ones explained earlier in this documentation.

Working with these types of dashboards allows you to filter your display according to your regulation needs.

Executive Report

The report entitled **Montly Executive Report** combines all default security dashboards in a single static monthly report:

- Access Control Security (refer to Sample Dashboard - Executive Report, Regulatory Compliance, SANS Top 5 and PDF Reports).
- Operation Security (refer to Sample Dashboard 2 - Operation Security).
- Asset Security (refer to Sample Dashboard 3 - Asset Security).

Regulatory Compliance

Standards Mapping

See Standards mapping.

FSA

The report entitled **Monthly FSA Compliance Report** is based upon the FSA Essential standards. To know more about PCI official standards, refer to http://www.fsa.gov.uk.

PCI-DSS

The report entitled **Monthly PCI-DSS Compliance Report** is based upon the PCI Essential standards. To know more about PCI official standards, refer to https://www.pcisecuritystandards.org/.

Sarbanes-Oxley

The report entitled **Monthly SOX Compliance Report** is based upon the CobiT Essential standards. To know more about CobiT official standards, refer to http://itgi.org/cobit.

SANS Top 5

These reports are based upon the TOP 5 established by the SANS Institute. To get the SANS official report about the TOP 5 essential log reports, refer to http://www.sans.org/resources/top5_logreports.pdf.

- Attempts to Gain Access Through Existing Accounts.
- Failed File or Resource Access Attempts.
- Unauthorized Changes to Users, Groups and Services.

- Systems Most Vulnerable to Attack.
- Suspicious or Unauthorized Network Traffic Patterns.

PDF Reports

Here is the list of the folders where PDF generated reports are stored:

- Executive
- FSA
- PCD-DSS
- Sarbanes-Oxley
- Other Reports

Appendix A - List of Alerts Fields

Table 22 Definition of Fields

TIBCO LogLogic® Syntax	IDMEF Field	C.	Description	T. of TV.	Permitted Values	N T
`additionalData`	`AdditionalData`	0+	Displays one or more additional pieces of data			X
`additionalData.data`	`AdditionalData`	0-1	Indicates the additional data	text		
`additionalData.meaning`	`AdditionalData.meaning`	0-1	Gives a description of the additional data	text		
`additionalData.meaningAndData`	`AdditionalData.meaning + AdditionalData`	0-1	Indicates and gives a description of the additional data	text		
`additionalData.type`	`AdditionalData.type`	0-1	Indicates the type of additional data	text	▪ boolean ▪ byte ▪ character ▪ date-time ▪ integer ▪ ntpstamp ▪ portlist ▪ real ▪ **string** ▪ byte-string ▪ xml	
`analyzer.analyzerId`	Analyzer.analyzerid	0-1	Indicates the equipment identifier **Usage**: This field is filled in when an Event Collector is added using the Log Collector configuration window.	text		
`assessment.action`	Assessment.Action	0-n	Describes the action			X
`assessment.action.category`	Assessment.Action.Category	0+	Indicates the type of action taken	list	▪ block-installed ▪ notification-sent ▪ taken-offline ▪ other	
`assessment.action.description`	`N/A`	0+	Describes the action	text		
`assessment.impact`	`Assessment.Impact`	0-1				X
`assessment.impact.completion`	`Assessment.Impact.completion`	0-1	Indicates whether the event was a success or failure	text	▪ failed ▪ succeeded	

Table 22 Definition of Fields

TIBCO LogLogic® Syntax	IDMEF Field	C.	Description	T. of TV.	Permitted Values	N T
assessment.impact.description	N/A	0-1	Describes the impact	text		
assessment.impact.severity	Assessment.Impact.Severity	0-1	Indicates the impact gravity	text	▪ info ▪ low ▪ medium ▪ high	
assessment.impact.type	Assessment.Impact.impacttype	0-1	Indicates the type of impact	text	▪ admin ▪ dos ▪ file ▪ recon. user ▪ **other**	
categoryId	N/A	1	Indicates the TIBCO LogLogic® Taxonomy fields taken into account to categorize the event. **E.g.** categoryId=1.3.8_56.67_57.60; 1 means Authentication 3 means Use 8 means User authentication 56 means Login 67 means SSH 57 means admin 60 means Success	text	Please refer to the TIBCO LogLogic® Taxonomy Guide.	
classification.reference	Classification.Reference	0+	Displays one or more references	text		X
classification.reference.name	Classification.Reference.name	0-1	Indicates the reference name	text		
classification.reference.origin	Classification.Reference.origin	0-1	Indicates the reference origin	text	▪ nessusid ▪ **unknown** ▪ vendor-specific ▪ user-specific ▪ bugtraqid ▪ cve ▪ osvdb	
classification.reference.url	Classification.Reference.url	0-1	Indicates the reference's URL	text		
classification.text	Classification.text	1	Indicates the name of the alert. **Usage**: Required	text		

Table 22 Definition of Fields

TIBCO LogLogic® Syntax	IDMEF Field	C.	Description	T. of TV.	Permitted Values	NT
detectTime.time	DetectTime	0-1	Indicates the time when the alert was detected by the equipment unit in timestamp. It is the number of seconds since 01/01/1970. **Usage**: Most of the time, this information is extracted automatically from the event data.	date and time		
dateToFormat	DetectTime		Indicates the date when the alert was detected by the equipment unit in timestamp. The date whose format has been entered in the converter.	date		
duration	N/A	0-1	Duration	integer		
eventWeight	N/A	0-1	Indicates the number of events contained in this event.	integer		
returnCode	N/A	0-1	Return code of the event. **E.g.** 400 for a HTTP query.	text		
size	N/A	0-1	Size	integer		
source	Source	0+	One or more sources			X
source.interface	Source.interface	0-1	Indicates the name of the source network interface	text		
source.node.address	Source.Node.Address	0+	One or more source node addresses			X
source.node.address.address	Source.Node.Address.address	0-1	Indicates the address of the source node	text		

Table 22 Definition of Fields

TIBCO LogLogic® Syntax	IDMEF Field	C.	Description	T. of TV.	Permitted Values	NT
source.node.address.category	Source.Node.Address.address.category	0-1	Indicates the category of the source node address	list	▪ **unknown** ▪ atm ▪ e-mail ▪ lotus-notes ▪ mac ▪ sna ▪ vm ▪ ipv4-addr ▪ ipv4-addr-hex ▪ ipv4-net ▪ ipv4-net-mask ▪ ipv6-addr ▪ ipv6-addr-hex ▪ ipv6-net ▪ ipv6-net-mask	
source.node.category	Source.Node.category	0-1	Indicates the type of domain where the source network node name originates	list	▪ unknown ▪ ads ▪ afs ▪ coda ▪ dfs ▪ dns ▪ hosts ▪ kerberos ▪ nds ▪ nis ▪ nisplus ▪ nt ▪ wfw	
source.node.emailAddress	Source.Node.Address	0+	One or more addresses of the source node (category = 2)	list		
source.node.ipLittleIndian	N/A	0-1	Retrieves a source ip address in the right order	integer		
source.node.ipv4Address	Source.Node.Address	0+	ipv4 host address in dotted-decimal notation (category = 7)	list		
source.node.location	Source.Node.location	0-1	Indicates the location of the source network node	text		
source.node.name	Source.Node.name	0-1	Indicates the name of the source network node	text		

Table 22 Definition of Fields

TIBCO LogLogic® Syntax	IDMEF Field	C.	Description	T. of TV.	Permitted Values	N T

`source.node.nameOrIp`
 	
or
 	
`source.node.nameElseAddress`
	If the character string is an email or IP address, the value is stored in `source.node.address.address`, otherwise in `source.node.name`	0-1	Indicates the name or network address of the source network node depending on the type of value.
			▪ if it corresponds to a valid IPv4 address, the field is automatically positioned at "ipv4-addr"
			▪ if it corresponds to a IPv4 address written with 4 bytes, the address is written as a pointer and the field `source.node.address.category` is automatically positioned at "ipv4-addr"
			▪ if it corresponds to a valid IPv6 address, the field source.node.address.category is automatically positioned at "ipv6-addr"
			▪ if it corresponds to an email address (a character string containing the @ character), the field source.node.address.category is automatically positioned at "e-mail"
			Note: To avoid recording the machine twice in an event (IP address and name) during a correlation process, use `source.node.nameElseAddress`
				text or integer		

`source.process`	`Source.Process`	0-1	A process at a source node			X
`source.process.arg`	`Source.Process.arg`	0+	Indicates the command line arguments for the process	text		
`source.process.env`	`Source.Process.Env`	0+	Indicates the environment variables associated to a process	text		

Table 22 Definition of Fields

TIBCO LogLogic® Syntax	IDMEF Field	C.	Description	T. of TV.	Permitted Values	N T
source.process.name	Source.Process.Name	1	Indicates the name of the source process If this field is empty whereas the fields: ▪ source.process.path ▪ source.process.pid ▪ source.process.arg ▪ source.process.env ▪ etc... are filled in, the value retrieved is automatically **unknown**.	text		
source.process.path	Source.Process.path	0-1	Indicates the path of the source process	text		
source.process.pid	Source.Process.pid	0-1	Indicates the pid of the source process	integer		
source.service	N/A	0-1	Gives information about the event's source			X
source.service.name	Source.Service.name	0-1	Indicates the name of the source request	text		
[recommended] source.service.nameOrPort or source.service.nameElsePort	If the value is an integer, it is stored in source.service.port, otherwise in source.service.name	0-1	Indicates the name or the port of the source request depending on the type of value	text or integer		
source.service.port	Source.Service.port	0-1	Indicates the source request port	integer		
source.service.protocol	Source.Service.protocol	0-1	Indicates the protocol name and/or number of the source request	text		
source.service.protocolNameOrNumber						
source.service.webService.arg	Source.Service.webService.arg	0+	Indicates the CGI script arguments of the source	text		
source.service.webService.cgi	Source.Service.webService.cgi	0-1	Indicates the CGI script used in the source request	text		
source.service.webService.httpMethod	Source.Service.webService.httpMethod	0-1	Indicates the HTTP method used in the source request	text		
source.service.webService.url	Source.Service.webService.url	0-1	Indicates the source request	text		
source.spoofed	Source.spoofed	0-1	Indicates if the source is spoofed	list	▪ **unknown** ▪ yes ▪ no	
source.tool.command	n/a	0-1	Indicates the command that was executed	text		

Table 22 Definition of Fields

TIBCO LogLogic® Syntax	IDMEF Field	C.	Description	T. of TV.	Permitted Values	N T
source.tool.name	n/a	0-1	Indicates the name of the tool or malware	text		
source.user	Source.User	0-1	Indicates the source user	text		X
source.user.category	Source.User.category	0-1	Indicates the type of source user	list	▪ **unknown** ▪ application ▪ os-device	
source.user.userId	Source.User.userId	1+	Indicates one or more source user identifiers			X
source.user.userId.name	Source.User.userId.name	0-1	Indicates the name of the source user. If this field is empty whereas the fields: ▪ source.user.userId.number ▪ source.user.userId.tty ▪ source.user.userId.type ▪ etc... are filled in, the value retrieved is automatically **unknown**.	text		
[recommended] source.user.userId.nameOrNumber or source.user.userId.nameElseNumber	if the value is an integer, it is stored in the attribute source.user.userId.number, otherwise in source.user.userId.name	0-1	Indicates the name or the identifier of the source user depending on the type of value	text or integer		
source.user.userId.number	Source.User.UserId.number	0-1	Indicates the identifier of the source user	integer		
source.user.userId.tty	Source.user.UserId.tty	0-1	Indicates the origin tty of the user	text		
source.user.userId.type	Source.User.UserId.type	0-1	Indicates the type of source user	list	▪ current-user ▪ **original-user** ▪ target-user ▪ user-privs ▪ current-group ▪ group-priv ▪ other-privs	
target	Target	0+	One or more targets			X
target.decoy	Target.decoy	0-1	Indicates if the target is a decoy	list	▪ **unknown** ▪ yes ▪ no	

Table 22 Definition of Fields

TIBCO LogLogic® Syntax	IDMEF Field	C.	Description	T. of TV.	Permitted Values	NT
target.file	Target.File	0+	One or more target file			X
target.file.name	Target.File.name	0-1	Indicates the name of the targeted file	text		
target.file.path	Target.File.path	0-1	Indicates the name of the targeted path	text		
target.file.pathAndName	Target.File.path + Target.File.name	0-1	Indicates the name of the targeted file and its path	text		
target.interface	Target.interface	0-1	Indicates the name of the targeted network interface	text		
target.node.address	Target.Node.Address	0+	One or more addresses of the targeted node	list		X
target.node.address.address	Target.Node.Address.address	0-1	Indicates the network address of the destination network node	text		
target.node.address.category	Target.Node.Address.category	0-1	Indicates the address category of the targeted node	list	▪ **unknown** ▪ atm ▪ e-mail ▪ lotus-notes ▪ mac ▪ sna ▪ vm ▪ ipv4-addr ▪ ipv4-addr-hex ▪ ipv4-net ▪ ipv4-net-mask ▪ ipv6-addr ▪ ipv6-addr-hex ▪ ipv6-net ▪ ipv6-net-mask	

Table 22 Definition of Fields

TIBCO LogLogic® Syntax	IDMEF Field	C.	Description	T. of TV.	Permitted Values	N T
target.node.category	Target.Node.category	0-1	Indicates the type of domain where the source network node name originates	list	▪ **unknown** ▪ ads ▪ afs ▪ coda ▪ dfs ▪ dns ▪ hosts ▪ kerberos ▪ nds ▪ nis ▪ nisplus ▪ nt ▪ wfw	
target.node.emailAddress	Target.Node.Address	0+	One or more addresses of the targeted node (category = 2)	list		
target.node.ipLittleIndian	N/A	0-1	Retrieves a target ip address in the right order	integer		
target.node.ipv4Address	Target.Node.Address	0+	ipv4 host address in dotted-decimal notation (category = 7)	list		
target.node.location	Target.Node.location	0-1	Indicates the location of the targeted network node	string		
target.node.name	Target.Node.name	0-1	Indicates the name of the targeted network node	string		

Table 22 Definition of Fields

TIBCO LogLogic® Syntax	IDMEF Field	C.	Description	T. of TV.	Permitted Values	N T

[recommended]
`target.node.nameOrIp`
 	
or
 	
`target.node.nameElseAddress`
	if the character string is an IP or mail address, the value is stored in target.node.address.address, otherwise in target.node.name.	0-1	Indicates the name or network address for the target network node depending on the type of value.
			▪ if it corresponds to a valid IPv4 address, the field is automatically positioned at "ipv4-addr"
			▪ if it corresponds to a IPv4 address written with 4 bytes, the address is written as a pointer and the field target.node.address.category is automatically positioned at "ipv4-addr"
			▪ if it corresponds to a valid IPv6 address, the field target.node.address.category is automatically positioned at "ipv6-addr"
			▪ if it corresponds to an email address (a character string containing the @ character), the field target.node.address.category is automatically positioned at "e-mail"			

`target.process`	`Target.Process`	0-1	Indicates the process of a targeted node			X
`target.process.arg`	`Target.Process.arg`	0+	Indicates the command line arguments of the targeted process			
`target.process.env`	`Target.Process.env`	0+	Indicates the environment variables associated to a targeted process			

Table 22 Definition of Fields

TIBCO LogLogic® Syntax	IDMEF Field	C.	Description	T. of TV.	Permitted Values	N T
target.process.name	Target.Process.name	1	Indicates the target process name If this field is empty whereas the fields ▪ target.process.path ▪ target.process.pid ▪ target.process.arg ▪ target.process.env ▪ etc... are filled in, the value retrieved is automatically **unknown**.			
target.process.path	Target.Process.path	0-1	Indicates the target process path			
target.process.pid	Target.Process.pid	0-1	Indicates the target process pid			
target.service.name	Target.Service.name	0-1	Indicates the target service name			
[recommended] target.service.nameOrPort or target.service.nameElsePort	if the value is an integer, it is stored in target.service.port, otherwise in target.service.name	0-1	Indicates the name or the port of the target service depending on the type of value			
target.service.port	Target.Service.port	0-1	Indicates the target service port			
target.service.protocol	Target.Service.protocol	0-1	Indicates the target service protocol name and/or Port			
target.service.protocolNameorNumber						
target.service.webService.arg	Target.Service.webService.arg	0+	Indicates the ARG script arguments for the target request			
target.service.webService.cgi	Target.Service.webService.cgi	0-1	Indicates the CGI script for the target request			
target.service.webService.httpMethod	Target.Service.webService.httpMethod	0-1	Indicates the HTTP method used in the target request			
target.service.webService.url	Target.Service.webService.url	0-1	Indicates the target request			
target.tool.command	n/a	0-1	Indicates the command that was executed			
target.tool.name	n/a	0-1	Indicates the name of the tool or malware			
target.user	Target.User	0-1	Indicates the target user	text		X
target.user.category	Target.User.category	0-1	Indicates the type of targeted user		▪ **unknown** ▪ application ▪ os-device	

Table 22 Definition of Fields

TIBCO LogLogic® Syntax	IDMEF Field	C.	Description	T. of TV.	Permitted Values	NT
`target.user.userId`	`target.user.userId`	1+	One or more identifiers for the targeted user			X
`target.user.userId.name`	`Target.User.UserId.name`	0-1	Indicates the name of the targeted user If this field is empty whereas the field `target.user.userId.number` is filled in, the value retrieved is automatically **unknown**. If this field is empty whereas the fields ▪ `target.user.userId.number` ▪ `target.user.userId.tty` ▪ `target.user.userId.type` ▪ etc... are filled in, the value retrieved is automatically **unknown**.			
[recommended] `target.user.userId.nameOrNumber` or `target.user.userId.nameElseNumber`	if the value is an integer, it is stored in the attribute target.user.userId.number, otherwise in target.user.userId.name	0-1	Indicates the name or identifier of the targeted user depending on the type of value			
`target.user.userId.number`	`Target.User.UserId.number`	0-1	Indicates the identifier for the targeted user			
`target.user.userId.tty`	`Target.User.tty`	0-1	Indicates the destination tty for the targeted user			
`target.user.userId.type`	`Target.User.userId.type`	0-1	Indicates the type of target user		▪ current-user ▪ **original-user** ▪ target-user ▪ user-privs ▪ current-group ▪ group-priv ▪ other-privs	

SEM Glossary

Table 23 Glossary

Term	Definition
Acknowledgement	The task of validating an alert displayed on the monitoring screen.
Administrator (User Rights)	See User Rights.
ADA	Archiving Disk Array.
Aggregation Engine	The process of using a pre-defined set of rules to group very similar events, reducing the total number that require further processing. For example: Several elementary events that have the same meaning (same TIBCO LogLogic® Taxonomy) and the same target address would be aggregated in one event.
Alert	An alert is composed of an event or a set of events that has/have an impact on confidentiality, integrity or availability of the information system. An alert is generated by the correlation engine according to predefined rules and scenarios.
Analyst (User Rights)	See User Rights.
Appliance	An equipment unit dedicated to be solely used as a software component of the SEM solution.
Backup	The TIBCO LogLogic® SMP Backup tool enables you to schedule automatic backups of the instance including database and configuration information held on the TIBCO LogLogic® SMP server. It is version-dependent. A backup file contains all of the backup configuration details - so that in the event of hardware or software application failure, this valuable information could be restored and would not need to be manually recreated.
Batch Reporting	Rules that allow the enrichment of the reporting database via alerts and aggregated events batch treatments.
Business Asset	Company items whose threats and vulnerabilities must be controlled, identified and calculated to evaluate risks.
Collection Policy	A collection policy allows you to determine which events will be selected to be forwarded to the TIBCO LogLogic® SMP. Filtering is carried out by the Log Collector, to avoid wasting bandwidth from the Log Collector to the TIBCO LogLogic® SMP.
Configuration Profile	See Security Profile.
Confset	Definition of a set of converters, filters and parameters to collect the log entries of an equipment.
Converter	Set of rules for converting a log entry into an event.
Conversion Ruleset	File containing conversion rules.

Table 23 Glossary

Term	Definition
Correlation Engine	The process of using a pre-defined set of rules and scenarios to combine one or more events into an alert.
Correlation Scenario	Scenarios are used to describe a situation matching the occurrence of a group of rules. Scenarios are used to describe complex situations requiring action which cannot be handled by the definition of a simple rule. For example, Rule A is used to detect when a process has stopped, Rule B is used to detect when a process has started. A scenario is created to detect that a process has been restarted (Rule A plus Rule B), that is, when both the stopped and the started rules match.
Criticality	Failure probabilities and severities referring to a certain asset, categorized as low, medium, or high.
Event	An event is a standardized data object (IDMEF and TIBCO LogLogic® Taxonomy) representation of a log entry that has been generated by a log source. The events collected by the SMP is also called 'elementary events'. On the SMP, these events are aggregated by the aggregation engine. Events generated by this engine is called 'aggregated event'.
Heartbeat	A message sent by the Log Collector to the SMP to indicate the Log Collector is active.
IDMEF	Intrusion Detection Message Exchange Format. The IDMEF is a special data format used for sharing information of interest to intrusion detection and response systems, and to the management systems which may need to interact with them. Standard RFC 4765.
IODEF	Incident Object Description and Exchange Format.
Incident	Container of alerts of IODEF format, allowing to ensure the management of these alerts. It specifies their cause and the actions that must be triggered.
Instance	An instance consists of: ▪ the configuration of logs and devices to be monitored ▪ the collected events ▪ the rules and scenarios to apply to the collected events ▪ a console server (the Web Console)
Live Explorer screen	The Live Explorer screen allows you to monitor everything that happens on the SMP server.
Live Reporting	Rules used by the Totaling Engine to enrich the reporting database in real time.
Log Collector	The software Log Collector installed on a machine to collect information, format it, and forward it to the SMP.

Table 23 Glossary

Term	Definition
Log Entry	A log entry is an individual message recording of an occurrence in an application, operating system or log source. For example, this could be a line in a text file describing a failed connection attempt, or a database record outlining a successful user log-in.
TIBCO LogLogic® Taxonomy	A TIBCO LogLogic® defined Taxonomy enabling to normalise events. A TIBCO LogLogic® Taxonomy is composed of seven fields that are themselves composed of three main groups: ▪ Result ▪ Objective, Event Type, Action, Action Detail ▪ Target, Target Detail
Log Source	Product that generates log entries collected by a Log Collector.
SEM	Security Event Manager. The SEM consists of a system where Log Collectors collect event data from application and device logs, then the data is treated and transmitted to the Security Management Platform (SMP). This allows the SMP to analyze and correlate a multitude of events, providing real-time monitoring. In addition, a comprehensive security record is created.
ODA	Online Disk Array.
Organization Unit (OU)	An Organization Unit (OU) is a collection of host groups. Typically this is based on overseeing responsibility, e.g., all host groups that the UK IT department are responsible for would be assigned to the "UK IT" OU. The OU is used in reports, such as a report listing the number of alerts (by priority) for each OU.
Raw Log	A record of individual activities of one or more equipment units, applications, operating systems or devices. The raw log provides an audit trail that can be used to diagnose problems or provide legal proof of said activity. It is a text-format representation of a log entry. A raw log is created by the Log Collector. A Raw Log Entry is an individual entry recorded in the raw log referring to a single device event.
Rules	Engines need various configuring rules to manage events and then build up complex scenarios to deal with events and alerts. There are different types of rules: ▪ Collection rule ▪ Aggregation rule ▪ Correlation rule ▪ Live or Batch Reporting rules
Security Dashboard	Screen displaying a set of reports.
Security Profile	A security configuration profile is a group of rules and scenarios along with a Service Level Agreement set.

Table 23 Glossary

Term	Definition
Site	Sites are used to group hosts in reports (e.g., Lyon, Paris, or London, Cambridge), and to specify who is to be contacted when alerts have notification actions, such as emails. Sites are therefore used to define the sphere of responsibility of one or more contacts. For example if London_Analysts are responsible for all the hosts in London, create a site called “London” and allocate the relevant hosts to the site "London".
Site Group	A Site Group contains several sites. (See Site).
SLA	Service Level Agreement. Indicator specifying the maximum delay (in minutes) for an alert to be acknowledged. It takes into account the severity of the alert, the criticality on the impacted machine, the current security level and the work hours of the security analyst.
SMP	Security Management Platform. The appliance which runs the SEM software. The SMP aggregates, enriches, and correlates received event data.
Super-Administrator (User Rights)	See User Rights.
Supported Product	A product supported by TIBCO LogLogic® SEM (Check Point Firewall-1, Windows 2003, ...).
Top Level Alert	Alert displayed on the main alert monitoring screen.
Totaling Engine	Engine which counts collected events according to Live reporting rules. It allows the enrichment of the Reporting Database used for security dashboards generation.
User Rights	There are four user rights available in the Security Event Manager: ▪ Viewer: Viewers have read-only access to the GUI and cannot acknowledge alerts. ▪ Analyst: Analysts have all the rights of viewers, plus they can acknowledge alerts and manage incidents. ▪ Administrator: Administrators have all the rights of analysts, plus they can make changes to the Security Event Manager Solutions configuration and configure the TIBCO LogLogic® policies (collection...). ▪ Super-Administrator: Super-Administrators have all the rights of administrators, plus they can manage all user accounts.
Viewer (User Rights)	See User Rights.
Web Console	The web-based graphical user interface (GUI) used for the administration of the SMP.

Index

T