&
RT Logic CyberC4:Alert v4.12

Lifecycle of a Log
### DOCUMENT HISTORY AND VERSION CONTROL

<table>
<thead>
<tr>
<th>Edition</th>
<th>Date of Issue</th>
<th>Description of Change(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>08/01/15</td>
<td>Initial Version</td>
</tr>
</tbody>
</table>
TABLE OF CONTENTS

1. **Introduction** ........................................................................................................................................ 4

2. **LOG COLLECTION** ............................................................................................................................. 4
   2.1. Logs Sent from Devices to the Sensor .............................................................................................. 4
   2.2. Logs parsed by the agent using plugins ............................................................................................ 5
   2.3. Security events extracted from the logs ............................................................................................ 5
   2.4. Normalization of SID’s ...................................................................................................................... 6
   2.5. Normalized SIDs transmitted to the alienvault server ........................................................................ 6

3. **HOW EVENTS ARE PROCESSED** ..................................................................................................... 7
   3.1. Events from the server to the database ............................................................................................. 7
   3.2. The server parses the event priority and reliability .......................................................................... 7
   3.3. The server checks assets to assign a risk score .................................................................................. 8
   3.4. Application of the event taxonomy .................................................................................................. 8
   3.5. The server crosschecks reputation data ........................................................................................... 9
   3.6. The event feeds into the correlation engine ....................................................................................... 10
   3.7. Events available for searching and browsing ................................................................................... 11
   3.8. Correlation directives create alarm events ....................................................................................... 11

4. **EVENTS VISUALIZATION** .................................................................................................................. 11
1. INTRODUCTION

The objective of this document is to show the life cycle of a log message through AlienVault USM™ for Government from the device to the user interface.

2. LOG COLLECTION

Log collection is the heart of a SIEM. AlienVault collects logs from devices, systems and software:

- Some logs are transmitted to AlienVault
- Others are retrieved by AlienVault

These logs are normalized, extracting common data fields from them: IP address, host names, user names, interface names, etc.

Key events are assigned a Security ID (SID). These are the events that are of interest to a Security Analyst.

SIDs are correlated into alarms. Log correlation can see patterns in activity that a single device or security control cannot.

2.1. Logs Sent from Devices to the Sensor

Devices that support the Syslog protocol are configured to transmit their log events to the AlienVault Sensor over UDP port 514 or TCP port 514.

Rsyslog on the AlienVault Sensor receives these events and buffers them locally into log files according to configuration.
2.2. Logs parsed by the agent using plugins

AlienVault-Agent. Running on the AlienVault-Sensor is configured with a series of log-parsing plugins, which read the incoming log files (and also control other event-gathering functions on the sensor, such as Intrusion Detection).

2.3. Security events extracted from the logs

Each plugin parses the log file text according to a series of Security Identities (SID). The SID is the “name” of the log message, its meaning. Some examples of SIDs are the following:

- “User Logged In”
- “New Connection From”
- “File matched Signature”
2.4. Normalization of SID’s

No matter the format of a log message, certain pieces of data are common throughout all of them:

- User names
- IP Addresses
- MAC addresses
- URI’s

Extracting these values out of the log message text and into a field is called Normalization.

Normalization is what allows us to perform queries such as: “Show all events where the source IP is 192.168.1.3”.

2.5. Normalized SIDs transmitted to the alienvault server

The logs are broken down into the type of message, and the information from them used to populate the fields:

- date
- sensor
- interface
- plugin_id
- plugin_sid
- priority
- protocol
- src_ip
- src_port
- dst_ip
- dst_port
- username
- password
- filename
- userdata1
- userdata2
- userdata3
- userdata4
- userdata5
- userdata6
- userdata7
- userdata8
- userdata9
3. HOW EVENTS ARE PROCESSED

3.1. Events from the server to the database

The event database is commonly on the same host as the AlienVault Server, but in large deployments, the database can be a separate host for increased performance capacity.

Although the events are now stored to disk, the server still has several more operations to perform on them before they’re ready to be searched.

The database is accessed via TCP port 3306. You may need to check your firewall settings if you are deploying an AlienVault Server in a different network that the AlienVault Database.

3.2. The server parses the event priority and reliability

Each event type that has a SID is assigned a priority and reliability score when the plugin is created.

- Priority. How urgently the event should be investigated.
• Reliability. The chance the event is a false positive.

A low-priority, the high reliability event could be: user joe@mydomain logged in from 10.53.80.3

This message is always accurate, but normal behavior.

A high-priority, low reliability event could be: “Authentication protocol anomaly from 10.53.80.3”.

This message is a best guess; detection, but highly unusual.

3.3. The server checks assets to assign a risk score

The server maintains an inventory of known devices on the network, with an associated asset value for each, defining their importance to the organization. This asset score is then weighted against the event’s priority and reliability score to produce a risk value.

\[
\text{Risk} = \text{Asset} \times (\text{Reliability} \times \text{Priority} / 25)
\]

Higher Risk Scores help the analyst know what to examine first!

3.4. Application of the event taxonomy

No matter the source of the event, or the format it originated in, there are types of system and network events common across many system types.

A security analyst wanting to see all user logins within a certain time period, should not have to know what the specific SID for each event type for each system type is, to retrieve that information.

AlienVault maintains a taxonomy of event types that SIDs can be matched to and retrieved via.
Correlation directives can also correlate events via their taxonomy allowing the creation of device-independent correlation rules.

The following image describes how taxonomy applies to a specific event:

3.5. **The server crosschecks reputation data**

If Open Threat Exchange (OTX) is enabled, the server checks the IP addresses in the events against the reputation database of Internet addresses.

IP addresses that match will be flagged for reference later.

Later on, events that indicate attacks from external addresses will be anonymized and submitted back to OTX to corroborate what other AlienVault users are seeing from those hosts.
3.6. The event feeds into the correlation engine

Event Correlation is one of the great powers of SIEM – being able to look for patterns and sequences of events across multiple devices and types.

Events may actually go through this stage several times – different correlation rules may take the same events as input.

The normalization on the events performed earlier is what allows correlation directives to work with events from different device types – critical fields such as usernames, IP address, etc., can be referenced without the directive being written for that particular event type.
3.7. **Events available for searching and browsing**

The events from AlienVault components and external log sources are now available in the SIEM UI and/or in the USM Logger.

Events are searched via the fields normalized out from the events, pulled into reports and used to trigger policy actions.

3.8. **Correlation directives create alarm events**

As events continue to feed into the correlation engine, conditions are met, that starts an alarm processing.

Alarms may trigger on a single event matching certain conditions, or may require a specific sequence of events to trigger.

Alarms may continue to process through the stages of priority over a matter of hours – alarms that appear in the system may indicate they are still processing additional incoming events to further corroborate detection.

Alarms are the events themselves and can feed into other correlation directives once their triggers, creating cascading levels of alarms.

4. **EVENTS VISUALIZATION**

Events can be visualized through these 2 options:

1. “Analysis > Security Events (SIEM)”.
The events can be grouped by clicking on the “Grouped” tab:

Events can be grouped by the following:
2. “Analysis > Raw Logs”. Events can be visualized by a time frame.