AlienVault Unified Security Management™ Solution

Complete. Simple. Affordable

Device Integration: CyberGuard SG565

CONTENTS

1. INTRODUCTION

The objective of this document is to explain how to configure a CyberGuard device to send log daa to AlienVault USM.

This document is related to the AlienVault document "Data Source Plugin Management". The explanation about how to enable plugins can be found in that document.

2. CYBERGUARD SG565 INFORMATION

Device Name	CyberGuard SG565
Device Vendor	CyberGuard
Device Type	Firewall
Data Source Name	cyberguard
Connection Type	Select Connection Type
Data Source ID	1575

3. CONFIGURING CYBERGUARD SG565 TO SEND LOG DATA TO ALIENVAULT

CyberGuard SG565 must be configured to send log data to an AlienVault Sensor over the syslog protocol.

Pre-Requisites:

- IP Address of the AlienVault Sensor or All-in-One

1. Log into the CyberGuard GUI.
2. Create a new Endpoint (Customize > Environment > Endpoints).
   - Select **Insert New File**.
   - In the *Name_field* enter 'Alienvault' and set **Type** to **Host**.
   - Set *Address_field* to the IP Address of an Alienvault Sensor and **Save**.
3. Configure syslog:
   - Select *Customize* > *System* > *Syslog*.
   - Select **Insert New File**.

- Set Facility to ‘LocalO’ and Level to ‘Debug’, check ‘**include higher levels**’.
- Select *Action* > *send to host*.
- In the host drop-down menu, select the entry for ‘Alienvault’ and **Save**.

4. Create Alert Filters:
   - Select *Customize* > *Audit & Alerts* > *Audit Filters*.
   - Set the filter to accept everything.
   - Select **Insert New File**.
   - Set the Name field to ‘Alienvault-Logging’.
   - Set the **Attribute** drop-down, to time, and the **Relation** drop-down to **Exists**. And then **Save**.
5. Set up a syslog relay:
   - Select *Customize* > *Audit & Alerts* > *Syslog Relay*.
   - Select **Insert New File**.
   - Enter ‘Alienvault Sensor’ into the **Name** field.
   - Set **Facility** to ‘LocalO’.
   - Set **Level** to ‘Debug’.
   - Set **Format** to ‘Native’.
   - Set **Filter** to ‘Alienvault-Logging’.
6. Save.
   - *Control* > *Firewall* > *Apply Configuration*.

4. CONFIGURING ALIENVAULT TO RECEIVE LOGS FROM CYBERGUARD SG565

Devices that send log data via Syslog require configuration of the Syslog service to process those incoming logs into a unique file destination.

1. Open the AlienVault USM Console.
2. Select and accept the ‘Jailbreak this appliance’ option to gain command line access.
3. Create a new configuration file to save incoming CyberGuard logs:

```
nano -w /etc/rsyslog.d/cyberguard.conf
```

4. Add the following line to the file, one for each CyberGuard device you are sending logs from:

```
if ($fromhost-ip == ‘<IP_Address_CyberGuard>’) then -
/var/log/cyberguard.log
```

5. Press **Crtl+W** to save the file and **Ctrl+X** to exit the editor.

6. Restart the Syslog Collector:

```
/etc/init.d/rsyslog restart
```

5. CONFIGURING LOG FILE EXPIRATION

Incoming logs will be processed by the Sensor and passed on to the SIEM Service. Keeping the raw log files on the sensor for more than a few days is unnecessary and they should be purged to maintain adequate free filesystem capacity.

1. Create a new log rotation configuration file.

```
nano -w /etc/logrotate.d/cyberguard
```

2. Add the follows content to the file:

6. HOW TO ENABLE THIS PLUGIN

This plugin is already configured but it is necessary to enable it, through command line console or through web interface. The instructions about how to enable this plugin can be found in the AlienVault document “Data Source Plugin Management”.