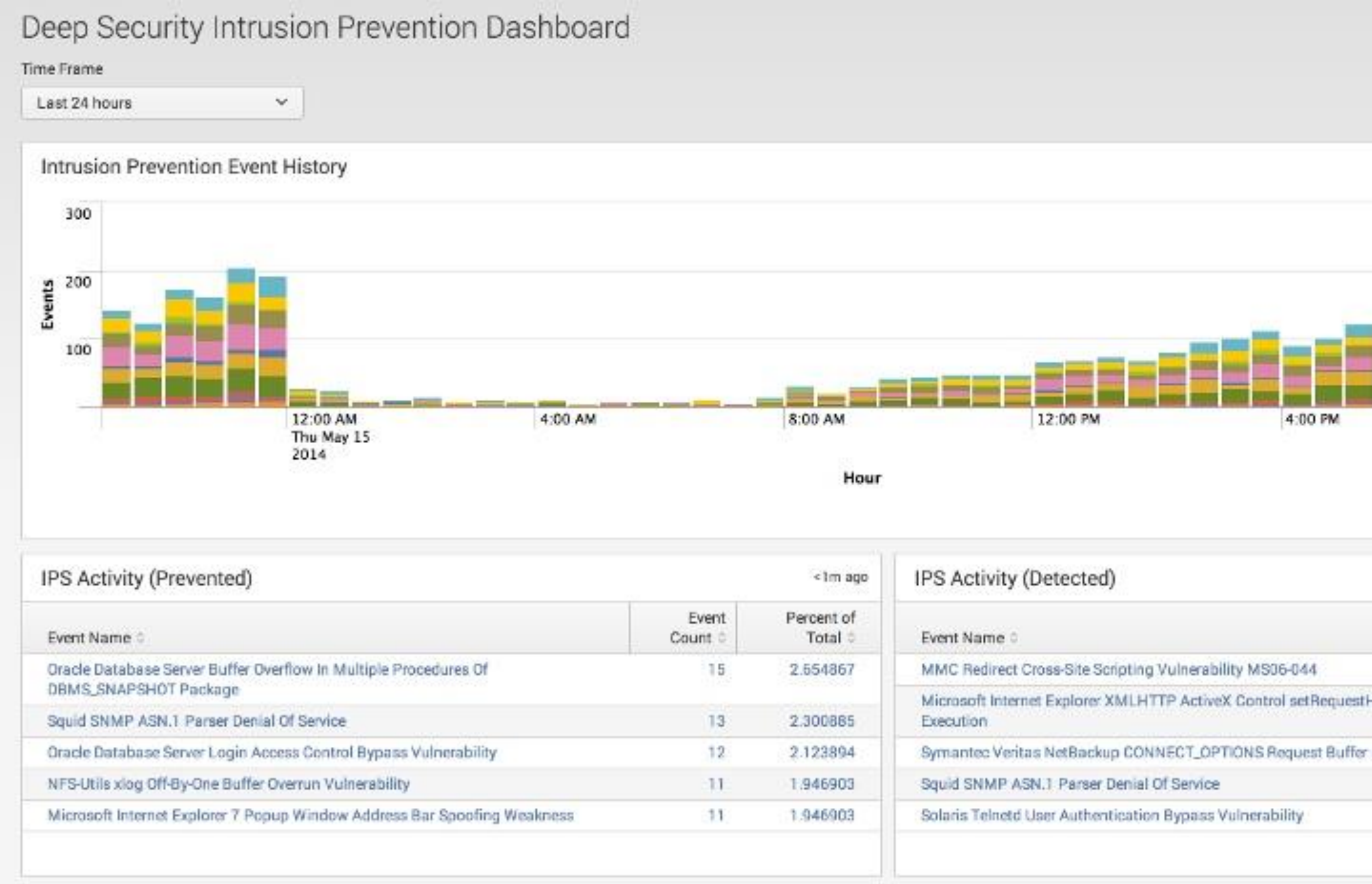
Trend Micro Deep Security for Splunk v1.5

Overview

This package contains parsing logic, saved searches, and dashboards for monitoring Trend Micro Deep Security via Splunk.

Please read the Installation section below for details on how to configure Deep Security to use this App.



Deep Security Intrusion Prevention Dashboard

Time Frame: Last 24 hours

Intrusion Prevention Event History

IPS Activity (Prevented) <1m ago

Event Name	Event Count	Percent of Total
Oracle Database Server Buffer Overflow In Multiple Procedures Of DBMS_SNAPSHOT Package	15	2.654867
Squid SNMP ASN.1 Parser Denial Of Service	13	2.300885
Oracle Database Server Login Access Control Bypass Vulnerability	12	2.123894
NFS-Utils xlog Off-By-One Buffer Overrun Vulnerability	11	1.946903
Microsoft Internet Explorer 7 Popup Window Address Bar Spoofing Weakness	11	1.946903

IPS Activity (Detected)

Event Name
MMC Redirect Cross-Site Scripting Vulnerability MS06-044
Microsoft Internet Explorer XMLHTTP ActiveX Control setRequestH Execution
Symantec Veritas NetBackup CONNECT_OPTIONS Request Buffer
Squid SNMP ASN.1 Parser Denial Of Service
Solaris Telnetd User Authentication Bypass Vulnerability

Installation

Install this App through the “Manage Apps” functionality within Splunk. For additional information on installing Splunk Apps please refer to the Splunk documentation.

After installing the Trend Micro Deep Security App in Splunk, a new syslog listener will be created on UDP port 1514.

Next, you will configure Deep Security to send event data to the newly created syslog listener. For System Events, this is configured via Administration -> System Settings -> SIEM. For security module events, this is configured within your security policies in the Settings -> SIEM section. For additional information, refer to the Deep Security online help or product documentation.

Upgrade from Version 1.4

Version 1.4 of the Deep Security for Splunk app used an individual UDP port for each module within Deep Security. This is no longer required in version 1.5. As such, the following UDP listeners are still included for backwards compatibility however they are disabled by default. If you do not want to modify your Deep Security configured to use a single UDP port, you will want to enable the following syslog listeners.

10701 - Syslog UDP port for System Events
10702 - Syslog UDP port for Anti-Malware Events
10703 - Syslog UDP port for Web Reputation Events
10704 - Syslog UDP port for Firewall and IPS Events
10705 - Syslog UDP port for Integrity Monitoring Events
10706 - Syslog UDP port for Log Inspection Events

Note: These syslog listeners will be removed in version 1.6 of this applications so it is highly recommended you migrate to the single port configuration after upgrading to version 1.5 of this application.

Usage

Deep Security can be configured to send event data in Common Event Format (CEF). This add-on will parse the various syslog message and extract the appropriate fields including the custom key/value pairs.

Example:

```
CEF:0|Trend Micro|Deep Security Agent|8.0.0.995|1001111|Test Intrusion Prevention
Rule|3|cn1=1 cn1Label=Host ID dvchost=hostname dmac=00:50:56:F5:7F:47
smac=00:0C:29:EB:35:DE TrendMicroDsFrameType=IP src=192.168.126.150
dst=72.14.204.105 out=1093 cs3=DF 0 cs3Label=Fragmentation Bits proto=TCP spt=49786
dpt=80 cs2=0x00 ACK PSH cs2Label=TCP Flags cnt=1 act=IDS:Reset cn3=10
cn3Label=Intrusion Prevention Packet Position cs5=10 cs5Label=Intrusion Prevention Stream
Position cs6=8 cs6Label=Intrusion Prevention Flags
```

Using the message above as an example, the add-on will extract the following custom key/value pairs:

```
Host_ID=1
Fragmentation Bits=DF
```

```
Intrusion Prevention Packet Position=10
Intrusion Prevention Stream Position=10
Intrusion Prevention Flags=8
```