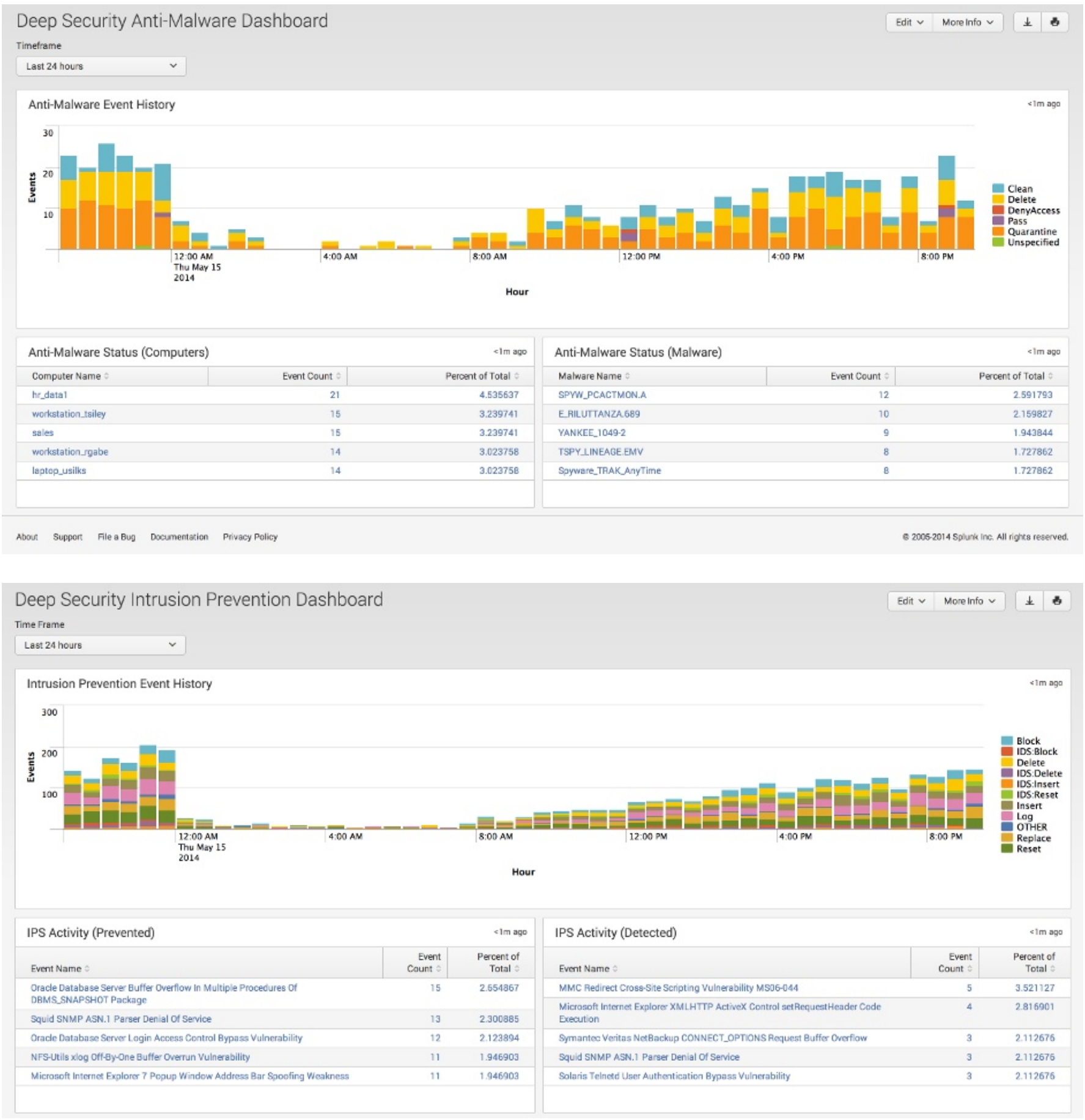
Trend Micro Deep Security

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.



Installation

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

Configure Deep Security to send events to your Splunk via syslog. After installing the Trend Micro Deep Security App in Splunk, 6 new UDP syslog listeners will be created. Individual UDP ports are used to facilitate the separation of the various event types within Deep Security.

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

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