splunk> POWERED

Pivot2Pcap

HAMMERHEAD

FLOW & PACKET CAPTURE

HammerHead pivot2pcap splunk app – www.npulsetech.com

Description

Drill down to raw packets using the Pivot2Pcap API found on all HammerHead Packet Capture appliances.

HammerHead Flow & Packet Capture is a High-speed, multi-terabyte traffic recording and analysis platform for Network Operations Center (NOC) and Security Operations Center (SOC) environments. The high-speed, continuous recording solution provides deep, high-fidelity indexed storage of network traffic for direct analysis or use with other security or monitoring applications. HammerHead delivers an easily-searched, multi-level, deep-time view of network packets, trends and events.

This app allows analysts access to details behind a Splunk event. Leveraging fields defined in the Splunk Common Information Model (CIM), this application adds value to any compliant splunk data set.

http://docs.splunk.com/Documentation/Splunk/latest/Knowledge/UnderstandandusetheCommonInformationModel

The following fields are leveraged from the CIM:

- src, dest
- src_ip, dest_ip
- src_port, dest_port

Different workflow actions are built, based on which CIM fields are available. If those fields are not available in your data source, follow the Splunk instructions on field mappings.

Install

Install the HammerHead pivot2pcap Splunk app to your splunk home.
By default, the app maps the ‘host’ field to a lookup to find which HammerHead device will have the packets associated with that event. To modify the lookup field, change props.conf’s lookup from ‘host’ to another field.
The lookup mappings are done in the <splunk app root>/Hammerhead/lookups/hammerheads.csv

```
host,hammerheadDevice
throneroom,www.npulsetech.com
yourhost,yourhammerhead.internalnetwork.org
```

Change the second two lines to map your source host to the HammerHead device.
Restart splunk.
Find an event that has a combination of the listed fields above, and pull down the workflow action drop down, and find some packets!

Version and Release Note

Version 1.0 of this app is compatible with HammerHead version 3.2

Support

visit www.npulsetech.com or email support [@] npulsetech.com