nPulse Technologies - CPX Pivot2Pcap splunk app – www.npulsetech.com

Description
Drill down to connections, packets and full session analysis using the Pivot2Pcap API found on all CPX.

CPX is an ultrafast, multi-petabyte traffic recording and analysis platform for security operations centers. With lossless packet capture, CPX provides easily searched, indexed storage of network packets, connections, and session data.

CPX captures 100% of the traffic, time stamping every packet with nanosecond resolution. CPX streams traffic to disk and generates a multi-key index for rapid search and retrieval of the traffic you need to see. A browser-based, drill-down interface analyzes user-selected packets without the need to export entire PCAP files.

This application 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_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 nPulse Technologies CPX Pivot2Pcap Splunk app to your splunk home.
By default, the app maps the ‘host’ field to a lookup to find which CPX will have recorded 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:
<splunk app root>/cpx_pivot2pcap/lookups/cpxLookup.csv

host,cpx
throneroom,www.npulsetech.com
yourhost,yourhammerhead.internalnetwork.org

Change the second two lines to map your source host to the CPX.
Restart splunk.
Find an event that has a combination of the listed fields above, and pull down the workflow action drop down, and link into the CPX with either a prepopulated search (Advanced Search) or an immediate packet download (streaming search).

Version and Release Note
Version 1.0 of this app is compatible with CPX version 4.0

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