Secureworks®

NOTICE

Announcement of End of Life / Feature Retirement for Palo Alto Network (PAN) Countermeasures

Publish Date: July 2021   Version: 1.0

This EOL Announcement arises from a decision by Secureworks to retire / End of Life the Countermeasures feature for Palo Alto Networks. This notice applies for both the Counter Threat (CTP) and Taegis XDR platforms.

The following milestones are included in this EOL along with their respective EOL effective date:

Service	Effective EOL Date
Last PAN based signature update	May 30, 2021
PAN Countermeasures Retired	July 31, 2021

Secureworks will continue to provide signatures in Suricata and open source SNORT formats. Palo Alto is a proprietary format which runs with limited computing power. For reference, customers may leverage a converter plug-in such as one listed here. Please note, this is not a Secureworks written or supported converter. Customers could utilize this at their own choice/risk: https://docs.paloaltonetworks.com/pan-os/10-0/pan-osnew-features/content-inspection-features/ips-signature-converter-plugin-forpanorama.html

For Taegis XDR customers, when you integrate your PAN firewalls into our application, your HTTP coverage will increase. We have over 1000 HTTP rules our customers will experience which is an increase in the limited set of detection rules that PAN firewalls have capacity to support. Taegis XDR is most effective when Firewall logs are configured to forward all URL categories. Additional information on how to ingest the firewall logs can be found on the help section of XDR under Integrations.

Please note that Attacker Database, consisting of IP and Domain watchlists, is not affected by this notice. Managed firewall customers can continue use the Attacker Database for Palo Alto.   Taegis XDR customers can now download IP and domain

watchlists from Taegis Threat Intelligence API, documented [here](#) under Threat Intelligence API.