Improve the Threat Detection Performance of Splunk Enterprise Security Solution

For many organizations, the Splunk Enterprise Security (ES) solution is the tool relied upon to quickly detect and respond to internal and external attacks. Splunk assists security teams in achieving enterprise-wide visibility and gathers security intelligence needed for continuous monitoring, incident response, and SOC operations.

However, Splunk's overall success in accurately alerting of intrusions comes down to the quality and quantity of data it has to work with. Send it too much data and/or irrelevant data, and it is not only expensive, but it can also create a lot of false positives. The flip side is if you feed it too little information, such as north-south traffic only, you'll suffer from a large gap in your network view.

Using CSPi's ARIATM Packet Intelligence application, organizations can improve Splunk's performance in detecting threats, while also allowing the immediate containment of such threats as they are detected.

The ARIA PI application deployed on an in-line probe can:

1. **Act as a network-independent Netflow or IPFIX data generator:**

   - Splunk ES can intake packet data ingest from your network to find network born threats but its too cost prohibitive.
   - Whereas by ingesting the right amount of NetFlow metadata you can derive 90% of the value of full packets with a 100x + cost reduction.
   - Only collect and ingest selective packet captures of suspicious data conversations as you need to
   - To get the benefit you must generate complete metadata for all network traffic– not just a sample.
   - Sampling can miss flows – and therefor threats. For example, switches commonly sample 1 in 10,000 packets to generate flow data.
   - Generating IPFIX provides the richest information for threat detection, better than NetFlow v9, “jflows” or “sflows.”

Benefits of network metadata generation:

- No more missing of network-born threats. Splunk can immediately detect such threats and do so thousands of times faster than using other means.
- Network born threats can be found earlier in the kill-chain as they are attempting to land and spread – earlier in their life cycle before significant damage is done
- More data options. You have the flexibility to ingest directly via the Splunk Stream™ add-on, or through third-party aggregators.
- Improve detection by achieving up to 80% greater network threat surface coverage – when deploying ARIA PI within your east west, (as well as north-south) network paths.

Splunk can correlate this information with other log-sourced events to:

- Properly prioritize critical events.
- Validate a threat and better understand it's scope of impact and the stage it is in.
- Provide additional details to help SOC teams determine appropriate next steps, to further investigate or contain the threat.
- Speed up the threat detection process. CSPi's solutions provide enough data in real time to help Splunk leverage its machine learning capabilities.
- Reduce false positives common with log-sourced events.

2. Send select packet-level conversations:

- ARIA PI can classify, filter and send specific data conversations – between specific source/destination pairs to any specified tool.
- Allows Splunk ES to apply full rule sets and algorithms to look into these specific data packets to verify or determine the issue in more detail.
- ARIA PI's actions can be directed by the SecOps team, or programmatically and automatically through the Phantom Workflow or other SOAR tool APIs.
- Allows threats detected by Splunk ES to be investigated further by sending copies of on-going data passing from the suspected source/destination pairs to IR and DLP tools
- Gives the option to shunt specified conversations to limit the ingest after a specified number of payload bytes as desired, which helps keep Splunk cost-effective.
- Provides the ability to send any conversation to Splunk and to other devices, such as CSPi's forensic Packet Recorder, for later retrieval in the event that additional analysis is required or to satisfy compliance audits.
- With our recorder in place you can also go back in time to ingest entire data conversations to/from newly identified threat sources
- Allows threats detected by Splunk ES to be sent to the CSPi packet recorder which searches each alert and generates its own alert if a critical asset being monitored has been breached with an extract file that contains the exact exposed records or files

3. **Proactively take steps to immediately and automatically contain threats and limit impact:**

- Take immediate action to block specific conversations once threats are found on the network. This is better than isolating the device which may be running critical processes
- ARIA PI's threat containment actions can be directed by the SecOps team, or programmatically through Splunk ES, the Phantom Workflow or other SOAR tool APIs
- This can be a part of the response workflows or directly and automatically within an MDR or IR process.
- The CSPi device can also redirect specific active traffic flows away from their destination to be sent for further investigation before being allowed to proceed.
- It can also isolate any device, or group of devices, so they can no longer communicate over the network. This is independent of the type of network equipment or wireless network infrastructure on which they are connected.

Secure your Enterprise today. Contact us: sales@cspi.com

About CSPi

CSPi (NASDAQ: CSPi) is a global technology innovator driven by a long history of business ingenuity and technical expertise. A market leader since 1968, we are committed to helping our customers meet the demanding performance, availability, and security requirements of their complex network, applications and services that drive success.

CSPi Corporate Headquarters
175 Cabot Street - Suite 210
Lowell, MA 01854
800.325.3110 (US & Canada)

CSPi High Performance Products
800.325.3110 (US & Canada)
us-hpp-sales@cspi.com

CSPi Technology Solutions
800.940.1111
us-ts-sales@cspi.com

www.linkedin.com/company/csp-inc
@ThisIsCSPi
us-hpp-sales@cspi.com
www.cspi.com