aria CYBERSECURITY SOLUTIONS

TECHNOLOGY BRIEF

Improve the Threat Detection Performance of Splunk Enterprise Security Solution

Many organizations rely on the Splunk Enterprise Security (ES) solution to quickly detect and respond to internal and external attacks. Splunk assists security teams in achieving enterprise-wide visibility and gathering security intelligence needed for continuous monitoring, incident response, and SOC activities.

However, Splunk's overall success in accurately identifying possible intrusions comes down to the quality and quantity of data it has to work with. Send it too much/irrelevant data and costs and false positives may skyrocket. On the other hand, if you feed it too little information, such as just north-south traffic, you'll suffer from a large gap in your view of your network traffic.

Using ARIA Cybersecurity Solutions' ARIA™ Packet Intelligence application, you can improve Splunk's performance in detecting threats, while also allowing the immediate containment of threats as they are detected.

splunk>

When deployed as an in-line probe, the ARIA Packet Intelligence application can deliver the following benefits.

1. Act as a network-independent NetFlow or IPFIX data generator

- Splunk ES can take in packet data ingested from your network to find network-borne threats. However, this approach may be too cost-prohibitive.
- Yet by providing the right amount of NetFlow data, you can derive 90% of the value of full packets with a 100X + cost reduction.
- This approach only collects and ingests selected packets of suspicious data conversations.
- To get the full benefit, you must generate complete metadata for all network traffic—not just a sample.
- Sampling can miss flows—and therefore, potential threats. For example, switches commonly sample just 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-borne threats. Splunk can immediately detect such threats and do so thousands of times faster than using other means.
- Network-borne threats can be found earlier in the kill-chain as they are attempting to land and spread – earlier in their lifecycle, before significant damage is done.
- More data options. You have the flexibility to send data 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 Packet Intelligence 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 its scope of impact and the stage it is in.
- Provide additional details to help SOC teams determine appropriate next steps, such as to further investigate or contain the threat.
- Speed up the threat detection process. ARIA Packet Intelligence provides 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 Packet Intelligence can classify, filter, and send specific data conversations – between specific source/destination pairs to any specified tool.
- It 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 Packet Intelligence'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 ongoing data passing from the suspected source/destination pairs to IR and DLP tools.
- Gives the option to shunt specified conversations to limit data ingesting after a payload bytes threshold is hit, which helps keep Splunk cost-effective.
- Provides the ability to send any conversation to Splunk and to other devices, such as our nVoy Packet Recorder, for later retrieval in the event that additional analysis is required or to satisfy compliance audits.
- Using the nVoy Packet Recorder, 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 nVoy Packet Recorder, which searches each alert. If a critical asset has been breached, it generates its own alert with an extract file that contains the exact exposed records or files.

3. Proactively take steps to immediately and automatically contain threats and limit their 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 Packet Intelligence'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.
- A deployed ARIA Cybersecurity Solution 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.

Contact Us Today: sales@ariacybersecurity.com or (978) 954-5038

ABOUT ARIA CYBERSECURITY SOLUTIONS

ARIA Cybersecurity Solutions recognizes that better, stronger, more effective cybersecurity starts with a smarter approach. Our solutions provide new ways to monitor all internal network traffic, while capturing and feeding the right data to existing security tools to improve threat detection and surgically disrupt intrusions. Customers in a range of industries rely on our solutions each and every day to accelerate incident response, automate breach detection, and protect their most critical assets and applications. With a proven track record supporting the Department of Defense and many intelligence agencies in their war on terror, and an award-winning portfolio of security solutions, ARIA Cybersecurity Solutions is committed to leading the way in cybersecurity success

ARIA Cybersecurity Solutions • 175 Cabot St, Suite 210 • Lowell, MA O1854

Connect with Us: ariacybersecurity.com / Linkedin / Twitter / Blog

aria CYBERSECURITY SOLUTIONS ariaSDS nVoy SECURITY APPLIANCES Myricom NETWORK ADAPTERS