aria CYBERSECURITY SOLUTIONS

TECHNOLOGY BRIEF

Four Techniques to Take Splunk Enterprise Security to New Levels of Effectiveness

Splunk Enterprise Security (ES) has proven to be a very valuable tool in today's modern enterprise. For many organizations, Splunk is a cornerstone technology for application management, security, compliance, and business/web analytics. However, it still has some areas where its performance and overall value could be improved.

Any system that depends on data ingestion is only as good as the information it is provided. Too much of the wrong data increases costs and leads to an increase in false positives. Not enough of the right data and the threats can be missed.

Now, ARIA Cybersecurity Solutions has a better way to address all of these challenges while delivering many powerful benefits at the same time.

Four ways ARIA Cybersecurity Solutions improves Splunk ES

1. Generates unsampled NetFlow data (not full packets) to Splunk ES to save up to 1000x on data ingest

Using the ARIA SDS Packet Intelligence (PI) application removes the need to ingest full network packets directly into Splunk as it proves to be too much information, at too high of a cost. Instead, our application generates and sends lightweight NetFlow/IPFIX metadata for every packet crossing the network to Splunk Stream.

Although lightweight, the NetFlow data generated by ARIA PI provides the details modern SIEMs like Splunk require to detect network-borne threats accurately. Unlike network switch-generated NetFlow that is sampled at up to one flow record for every 10,000 packets, we provide metadata for every single packet. This ensures you won't miss a thing and can find potential threats sooner.

Benefits:

- Drastically reduce network data-ingestion costs
- Capture more network-borne threats and reduce the number of false positives
- Find threats faster and earlier in the kill chain
- Enrich Splunk ES alerts by correlating generated metadata and selective packet capture with existing log data and threat intelligence

2. Sends only select data conversations as requested to find specific threats

The ARIA Packet Intelligence application classifies all traffic as it crosses the network. It can then create copies or redirect live, select traffic data conversations based on filters like SRC/DST to Splunk Stream and other tools as requested. This can be part of the incident response process after an issue has been identified by Splunk ES, where an incident response workflow requires that the actual data be reviewed for further investigation.

Benefits:

- Provide packet-level detail on malware or threat payloads - without the need to ingest high volumes of packets
- Help eliminate the need for incident response as well as the costs associated with other IR tools to find this information

3. Stops east-west network-borne threats immediately

Firewalls only see and stop threats coming in from the Internet. They don't see traffic moving laterally, or east-west, within a site's network and don't look inside trusted VPN tunnels running between sites or to the public cloud. Endpoint security tools can only stop certain threats once they land on a device and miss many others, including insider threats, compromised credentials, data exfiltration, and data leaks, and more.

The same probes and intelligent NICs that generated the metadata are already sitting in-line. They can be directed to intercept and stop threat conversations on the network as they are identified by Splunk ES – as performed by SOC teams manually or automatically with SOAR APIs (such as Phantom). Stopping a threat conversation between two devices is a much better approach than taking critical devices or VMs off the network.

Benefits:

- Gain a surgical means to stop threat conversations deeper in the network—covering east-west as well as north-south conversations
- Keep critical processes safely running—blocking the threat while providing time for remediation action plans to be implemented
- Use automation to eliminate the need for manual intervention by SOC teams, improving effectiveness and reducing missed threats
- Offload significant CPU cycles from firewalls and EP clients, allowing them to return to core functions
- Provide coverage for devices that can't use endpoint detection and remediation applications, such as medical devices, VMs, IoT devices, and industrial controls
- Stop threats faster without having to make changes to NetOps-owned devices

4. Reviews previously recorded network activities to locate impacted devices and identify exposed records

By integrating our nVoy Series Packet Recorder with Splunk ES – as new threats are identified, any recorded metadata can be revisited to immediately find all of the impacted devices. Alternatively, select captured data feeds can be replayed (such as those that may be recoded against critical assets housing files or PI/PHI).

Benefits:

- Identify the exact records exposed automatically
- Provide historical information on all impacted devices to determine root cause and patient zero

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