aria CYBERSECURITY SOLUTIONS

TECHNOLOGY BRIEF

# Five Game-Changing Enhancements for Splunk ES

## *Significant Improvements for Threat Detection, Verification and Containment*

**Splunk ES has proven to be of tremendous value in today's modern enterprise. For many organizations, it's a cornerstone technology for application performance management, compliance, and business/web analytics.**

However, Splunk suffers from constraints when used for security due to the typical large number of sources that must be ingested to find and investigate threats. This can lead to ineffective threat hunting, slow search performance, and expensive, ever-climbing ingestion costs. Any system that is dependent on data ingestion is only as good as the information it is provided. Too much of the wrong type of data increases costs and false positives rise. Not enough of the right data and threats will be missed.

The ARIA™ Software-Defined Security (SDS) solution helps solve the ingestion issues, while significantly improving Splunk ES's effectiveness at detecting, verifying, and stopping attacks. Intelligently monitor all network traffic with ARIA SDS by feeding flow metadata to Splunk ES to give it the visibility it needs to detect network-borne threats. It also classifies all traffic conversations so action can be taken to verify, and then stop, attacks at the conversation level. Because flow metadata is generated for every packet, Splunk is assisted in detecting attacks as they spread earlier in the kill chain, minimizing the harm.

Essentially, security operations center (SOC) teams using Splunk are provided the visibility and confirming data needed to quickly, but properly, detect and stop internal network threats. All of this drastically improves Splunk's ability to search, detect, and investigate any threat, whether it appears on networks, in the customer premises, in the data center, in the cloud, or in between.

This document reviews five critical missing capabilities that provide significant new benefits to Splunk ES customers using ARIA SDS.  You can now find threats that were previously missed or contain attacks without shutting down affected devices – including internet of things (IoT) devices. We enable you to speed up searches by 10x and even reduce complexity around query-string creation. Most importantly, we save precious time and money by reducing ingestion, indexer, and compute costs associated with owning and managing Splunk.

## How is this done?

### 1. Create/feed unsampled NetFlow for improved detection and search functionality at lower ingestion cost

The ARIA SDS solution creates unsampled NetFlow (IPFIX) records for every network packet and feeds it into Splunk's free Stream collector. Unlike network switch-generated NetFlow that is sampled at one flow record created for every 10,000 packets, ARIA SDS generates NetFlow for every single packet, so that nothing is missed.

Up to 80% of attacks and exfiltrations can be detected within the network data; as such Gartner has deemed the ability to ingest network data in flow or packet form to be a critical requirement for any device to meet its classification of a modern SIEM. Unsampled NetFlow provides the crucial details modern SIEMs like Splunk require to detect network-borne threats – in a lightweight form factor that doesn't overburden ingestion. This allows security resources to find malware, ransomware, APTs, and other attacks live as they become active and not after the fact as detected by log sources – if at all.

This approach provides a decrease in ingestion costs by limiting the amount of log sources required to hunt through to find such attacks. Since NetFlow records are extremely lightweight, with a standard fixed format, ARIA SDS provides quick ingestion with fewer indexers, saving underlying compute requirements. This in turn allows for rapid search results to detect and investigate network-borne threats in seconds as compared to minutes or longer from typical multi-source, log-reliant threat searches.

The NetFlow generated by ARIA SDS is a more reliable source of information. This is because logs can be manipulated/shut off by a threat actor, or may not provide the level of information an analyst needs to make a proper determination if there is a threat and what it is impacting. A typical practice is to wait for further corroborating log inputs that can be found and correlated in Splunk after the threat has fully materialized and the damage has been done.

ARIA SDS allows for the detection of network-borne threats without reliance on logs. SOC analysts can set up the solution to automatically verify threats by redirecting entire live suspect conversations found with the NetFlow information to central detection tools like IPS and DLP. Those devices can both verify and, in many cases, stop the threats in real time. This is yet another way ingestion costs can be reduced by doing the work automatically without the need to ingest large amounts of costly logs from many sources. This is not to say log sources are no longer needed; however a core set of log sources can now be relied upon to provide the information needed to supplement what the NetFlows can't find or to complement with added context through correlation.

One of the big challenges pertaining specifically to SIEM platforms is the complexity of creating query strings. Security analysts must write a query string in order to use a SIEM to answer a specific question. This query string defines the question, which means it also defines whether the answer returned includes the desired data. This is not a trivial task and requires a very special skillset to accomplish.

Integration with ARIA SDS is valuable here as it reduces the number of query strings needed when looking for data related to network traffic analytics. This is where NetFlow collection by Splunk Stream helps – it identifies devices and port-level conversations, frequency, duration, and the amount of data passed. It's not difficult to write a query to see what types of devices are talking, how they attempt to talk, when, and how much. ARIA goes one step further and provides example queries to find lateral spreads and other threat behaviors. In addition, there are plays available which can be run to find such threats. These can be automated with the ARIA workflow tool or driven directly by a SOAR tool.

**ARIA Unsampled NetFlow Benefits:**

- Drastically reduces Splunk compute, indexer, and data ingestion costs
- Detect network-borne threats and attacks that would previously be missed
- Find threats faster as they are happening live across the network
- Reduce dependence on log ingestion by using NetFlow
- Correlate with existing source log data and threat intelligence to enrich alerts and reduce false positives
- Allow Splunk to see threats impacting IoT or critical production applications that cannot support an agent or full-blown EDR
- Remove complexity around threat query string creation

## 2. Capture selective data conversations to provide "definitive" threat confirmation

ARIA SDS classifies all traffic as it crosses the network. It then can redirect selected traffic data conversations based on filters like SRC/DST (live streams) for further inspection as noted above, or it can take a copy of the traffic to be ingested by Splunk Stream as requested to verify the details of the threat.

To reduce the volume of ingested data and save costs, ARIA SDS can redirect these copies to a packet recorder, which in turn will ingest and index these conversations for quicker searches. It thereby preserves the actual data and allows detailed searches to be performed on it as required by the SOC analysts. When completed it sends the desired output of these searches into Splunk Stream for a complete record of all details related to the threat.

This provides Splunk ES with definitive proof by capturing the actual threat data which, improves overall workflow processes and makes IR more effective. These capabilities allow for more effective incident response (IR) processes, allowing for improved IR work flows that create definitive proof by capturing the actual threat data. This approach speeds up both investigation and follow-on audit work. ARIA SDS can send copies of this traffic to other tools such as next-generation firewalls, IDS, UEBA, DLP, etc. for further action when required. In addition, ARIA SDS allows all process actions to be fully automated through use of the ARIA Automated WorkFlow (AWF) process tool, or via SOAR tools such as Demisto.

**Selective Packet Capture Benefits:**

- Eliminates the chance of false positives and provides more definitive proof
- Helps improve the IR process – easily validate and identify the specific threat type
- Minimizes the ingestion of network data for detailed analysis
- Helps eliminate the need and cost associated with other IR tools to find this information
- Aids in assuring compliance with increasingly stringent industry, federal, (FISMA, HIPAA) and all state regulations
- Reduces the time and cost of audits and third-party investigative analysis

## 3. Stop threats immediately without taking devices or application offline

Splunk's work typically stops at investigating threats. With ARIA SDS, the real benefit comes from how it automatically stops the threats from within the network, while doing the least harm.

Splunk, with ARIA SDS, can quickly find threats and verify them. ARIA uses its own user interface or APIs to stop the specific threat conversations as they cross the network. This adds critical new effective and efficient ways to stop attacks of all kinds. It joins the two other means that are used today. First, being firewalls, which can only block external sources from communicating inward. The second being endpoint detection and response (EDR) solutions, which can only run on the devices that can support them and for the limited set of threats it understands how to block, on a given machine. Therefore, EDRs create a quandary for many customers – they make sense for endpoint devices under the customer's control, but tend to be CPU-intensive and are very difficult to deploy in each VM and container that needs to be dynamically spawned and provisioned quickly. So, these surfaces tend not to be protected. For example, BYOD, IoT, and legacy OS devices in medical and industrial environments join this list of devices where EDRs don't typically work.

Since ARIA SDS is already sitting inline, it can be directed to intercept and stop the threat conversations on the network as they are identified by the SOC team manually or automatically via SOARs leveraging ARIA APIs. Taking out the threat conversations is a much better approach than taking critical devices or VMs offline as normal approaches dictate. ARIA allows critical devices to continue to operate until backups can be safely brought up online.

Once threats are found, ARIA SDS can be used to stop such threats permanently by implementing network-based microsegmentation. By creating device-level connectivity, white or blacklists can ensure devices that should not have been communicating at all or not communicating over a certain port or with a particular application – never do so in the future.

### Inline Threat Conversation Containment Benefits:

- Keeps critical processes safely running – blocking the threat while providing time for remediation action plans to be put in place
- Provides agentless threat containment for environments like IoT, VMs, and containers
- Provides a surgical means to stop threat conversations anywhere on network – north/south or east/west
- Improves SecOps' ability to stop threats quicker without having to wait for devices to be taken offline.
- Stops threats within minutes of detection (when automated)
- Provides a simple means to create and enforce network-based microsegmentation connectivity polices

## 4. Automatically detect and stop data breaches while further controlling Splunk ES ingest

Integrating an ARIA Cybersecurity Solutions Packet Recorder with Splunk ES has tremendous upfront value. As new threats are identified, any recorded metadata can be revisited to immediately find all of the impacted devices. Alternatively, the recorder can be used to capture and then feed only select data into Splunk upon request, greatly limiting ingest.

The recorder can be driven by plays and automation from the ARIA AWF or SOAR tools. It can also be used to capture and store anything from NetFlow metadata, to logs, to network traffic, thus allowing control of what goes into Splunk. Captured data feeds can be replayed such as those recoded against critical assets housing files or PII/PHI – back through applications such as SQL or through tools like Wireshark. This process can identify which exact records were exposed during a data breach.

In fact, the packet recorder can run the ARIA Automated Investigative Response (AIR) application to automatically search, detect, and auto-extract entire data breach conversations. The ARIA AIR application ingests threat intelligence alerts sent to it by third-party tools such as firewalls or IDS/IPS tools to trigger its automated process. As a result, it alerts of a confirmed data breach along with the complete copy of the data exfiltrated. This process can be tied into the plays above for SOC teams to follow the containment process to stop these data breaches immediately as they are discovered.  In fact, the entire process can be fully automated to stop the data breach without human intervention.

### Recording Network Traffic Benefits:

- Automatic identification of the exact records and devices exposed during a data breach
- Go back in time to help determine root cause of threats and patient zero
- Optimize Splunk with triggered, filtered ingestion, yielding better results at lower cost
- Gain a more effective data breach IR process
- Detect and stop critical data breaches automatically

## 5. Reduce data sets with filtering for improved cost and better results

Remember in the beginning when it was mentioned that an ingestion-based system is only as good as the data it brings in?  The ARIA SDS data filters also have advanced options to further reduce the data sent for certain conversation types into Splunk and other detection tools.

First, ARIA SDS can classify Splunk's packet data ingestion by ports, protocols, or applications for every packet on network – at wire rate. Also, the unnecessary classified traffic is filtered out to reduce the load and get Splunk the information it needs to do its job faster. Finally, data sets are further narrowed down by shunting streaming applications like Spotify or Netflix that can clog up ingestion and raise costs.

The point is less can be more and it's definitely faster – ARIA SDS gives you all options for the ultimate in flexibility of optimizing your Splunk network ingestion.

### Filtering Network Traffic Ingestion Benefits:

- Reduce ingestion costs
- Reduce false positives
- Create quicker search results
- Implement more effective, lower cost IR processes

## ARIA SDS provides a clear advantage to Splunk users

The issues covered here have definitely been felt by anyone who uses Splunk ES, or any modern SIEM for that matter. Adding ARIA SDS feeds Splunk better data to find internal network threats and allows Splunk customers to reduce the number of log sources that must be ingested. The result: Splunk runs searches quicker, and with the right data, finds previously missed threats early in the kill chain. The reduced ingestion and the reduction in indexers typically pay for the ARIA platform in a matter of three to six months – driving a substantial ROI in cost reduction alone over the platform's lifetime.

**Contact Us Today: sales@ariacybersecurity.com or 800.325.3110**

### 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 01854

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

aria CYBERSECURITY SOLUTIONS    ariaSDS    nVoy SECURITY APPLIANCES    Myricom NETWORK ADAPTERS