USING SPLUNK ADAPTIVE RESPONSE

Automating verification and response actions in heterogeneous security architectures

- **Enable a multi-vendor adaptive security architecture**
- **Extract new insight from existing security architectures**
- **Improve investigations with more context from key security and IT domains**
- **Shorten security analytics cycle by enabling automation of actions**

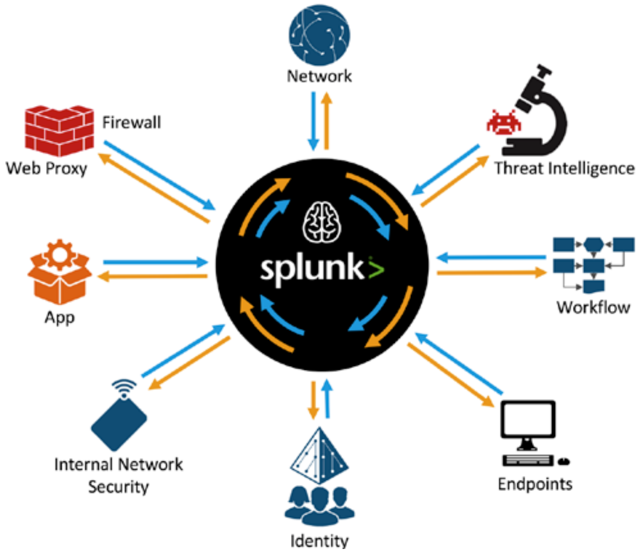
Splunk Adaptive Response enables security analysts—from hunters to less skilled security staff—to better handle threats by speeding the time to make decisions and actions when responding and adapting to them.

What is adaptive response?

Adaptive response consists of both the Splunk Adaptive Response Initiative and the Adaptive Response Framework.

The Splunk-led Adaptive Response Initiative represents the collective efforts of best-of-breed security vendors who are committed to providing a defense strategy for multi-layered, heterogeneous security architectures.

The Adaptive Response Framework resides within Splunk Enterprise Security (ES) and optimizes threat detection and remediation using workflow-based context. Analysts can automate actions or individually review response actions to quickly gather more context or take appropriate actions across their multi-vendor environment.



Adaptive Response Framework Capabilities

Splunk security analysts can leverage the incident investigation and response cycles within ES with capabilities such as:

- **Correlation search builder** – Configure, automate, queue responses and attach the results to notable events
- **Incident review** – Configure and execute responses and queries across multiple security domains; approve and follow through on semi-automated responses; review status and results from responses associated with an incident
- **Response audit** – Search and review responses taken and their results; manage workflow actions specific to domains

Adaptive Response Initiative – Partner Integrations

Adaptive response uses Splunk software as the “security nerve center” to bridge intelligence from multiple security domains. The initiative brings together vendors to provide the benefit of collective intelligence and coordinated response actions to customer security architectures. This makes it possible to better defend against threats by ensuring that the cycle of "insight to action" can be accelerated; that is, not hindered by data silos and inefficiencies from operating across multiple domains.

Partners develop integrations with Splunk to add actions to the adaptive response framework in ES. Following is a list of partner integrations.

Cloud Access Security Broker (CASB)

CloudLock

Integration allows for the updating of an app's "classification" from within Splunk. For example, if Splunk sees an odd behavior related to a specific cloud app or service—it can then reclassify that app as "Trusted," "Banned," "Restricted" or "Unclassified" in CloudLock.

Deception

ACALVIO

Provides a way for Acalvio to communicate deception events and IOCs to Splunk to take action on the network devices for quick remediation. It also allows Splunk to send notable events to Acalvio for automated confirmation using fluid deception.

Endpoint

CARBON BLACK
ARM YOUR ENDPOINTS

The integration will allow isolation of an endpoint via hostname, IP or Carbon Black sensor ID; and ability to ban a hash from running on any Carbon Black-managed endpoints (based on MD5 hash input). The integration also allows for process kill on endpoints, based on process name/ID.

CROWDSTRIKE

Integration allows for the querying of the Falcon Host API to determine the number of devices a specific IOC has been seen on. This includes support for file hashes, IPs and domains.

TANIUM™

Enables Splunk to ask a Tanium-specific question from a notable event and index the results.

ziften

Integration allows calling into the Ziften Extension Platform to execute any Ziften extension (PowerShell scripts that are code signed). This also allows the activation of ZFlow—turning on client-side netflow to be sent to Splunk on demand.

Identity and Access Management

okta

Integration allows for the disabling of a user ID from Splunk as well as moving a user into or out of a 2FA enabled group within Okta. Thus having the effect of enabling or disabling 2FA on a user.

Network Admission / Access Control

CISCO

Integration allows for quarantine or unquarantine of an IP address in a notable event via pxGrid/ Cisco ISE integration.

ForeScout

Integration dynamically gets a list of ForeScout actions and stores them in Splunk. Actions can then be executed on CounterACT via policy. CounterACT will also send back the action status to Splunk—synchronously or asynchronously. Both are supported.

REDSEAL

Delivers actionable intelligence from RedSeal's network modeling and risk scoring platform directly into Splunk Enterprise Security's (ES') "notable events" to accelerate incident response. Within minutes and without leaving notable events, ES users can locate L2 data for the source, identify access paths to high risk targets, and pinpoint the exact firewall and configuration rules to mitigate risk.

Next-Generation Firewall

FORTINET

Integration allows blocking of IP addresses directly from notable events.

paloalto NETWORKS

Allows tagging of IP addresses within Splunk to send to the firewall for automated policy enforcement, e.g. to quarantine a particular host.

Network Forensics

Symantec.

Provides Splunk users a single pane-of-glass to security and forensic information gathered from Symantec Advanced Threat Protection and Security Analytics platforms allowing extended visibility into endpoint and network control points to automate IR response tasks.

Orchestration and Incident Response

algosec

Integration with Splunk ties security incidents directly to the actual business processes that are or potentially will be impacted, including the applications, servers, network and traffic flows, and security devices. Once identified, AlgoSec can neutralize the attack by automatically isolating any compromised or vulnerable servers from the network.

DEMISTO

Allows for triggering notable event specific playbooks for gathering information about Splunk ES Incident fields or take actions based on incident severity and manage complete incident lifecycle within Demisto Enterprise.

Phantom

Call Phantom playbooks and actions directly from notable events. Notable events can also be sent directly to Phantom to generate buckets in Phantom.

RESOLVE SYSTEMS

Find it with Splunk, Fix it with Resolve. Resolve provides a process-driven and automated approach to incident response with standards based playbooks, process guidance, human-guided and closed loop automation reducing the amount of time that it takes organizations to investigate, contain and remediate security incidents.

Privileged Account Security

CYBERARK

Integration allows for the triggering of authentication actions—step up authentication, step down authentication, rotate password—from a notable event.

Threat Intelligence

ANOMALI

Integration allows for dispatching of notable event data to Anomali for further analysis. Additionally, if there are kill chain staged detected by Anomali, they will be written back to the Splunk investigation timeline automatically.

DOMAINTOOLS

Auto-enriches a notable event with DomainTools' domain intelligence. Allows setting alerts on a specific registrant email address, a suspect registrar, or an actor's preferred name server, among other options.

proofpoint

Integration allows for the submission of a domain from Splunk for analysis to the Investigate API. This will return reputation data and other security context such as domain age or domain neighborhood reputation.

OpenDNS

Integration allows Splunk user to auto-enrich notable events with threat data from ProofPoint Emerging Threats Intelligence, e.g. IP and domain reputation.

Recorded Future

Provides a means to auto enrich data from a notable event with threat intelligence from Recorded Future.

THREAT CONNECT

Allows calling of ThreatConnect playbooks/ blueprints to execute orchestration actions from Splunk notable events. Also allows for auto-enrichment and indicator sharing with ThreatConnect threat intelligence platform.

Vulnerability Management

QUALYS

Integration allows for the instantiation of a WAS scan based on the WAS ID of a device from within Splunk.

Try Splunk Enterprise Security Now Experience the power of Splunk Enterprise Security – with no downloads, no hardware set-up and no configuration required. The Splunk Enterprise Security Online Sandbox is a 7-day evaluation environment with pre-populated data, provisioned in the cloud, enabling you to search, visualize and analyze data, and thoroughly investigate incidents across a wide range of security use cases. You can also follow a step-by-step tutorial that will guide you through the powerful visualizations and analysis enabled by Splunk software. **Learn more** about Adaptive Response.

splunk>

Learn more: www.splunk.com/asksales

www.splunk.com