TECH BRIEF

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

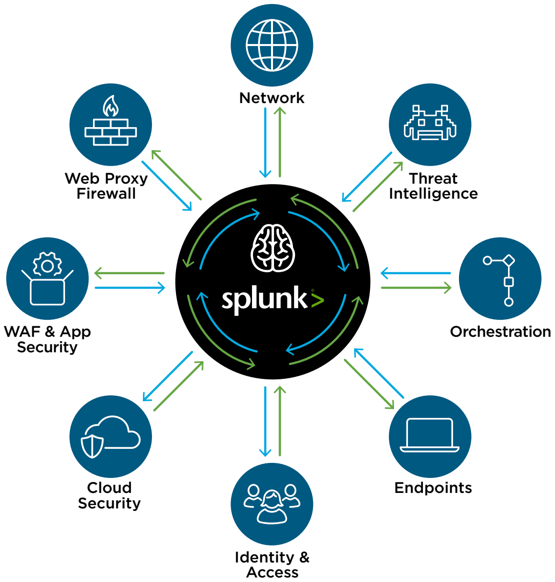
Splunk Adaptive Response enables security analysts—from hunters to less skilled security staff—to better handle threats by speeding the time to make decisions and actions when responding and adapting to them.

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 Splunk 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 Splunk ES. Following is a list of partner integrations.

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.

accenture

Using Accenture's Adaptive Response action clients can enrich and contextualize data by leveraging iDefense service to augment events in Splunk Enterprise Security. This creates the next level of detail needed to diminish false positives and get truly actionable information.

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.

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.

ATLASSIAN

The Atlassian Adaptive Response action creates a JIRA issue kicked off from an incident investigation and response workflow in Splunk Enterprise Security to create a ticket that tracks the progress of an incident investigation and response.

AWAKE

The Awake Security Adaptive Response action allows analysts using Splunk to pivot on an IP address, email or domain name and get detailed context and analytics on them. For instance, Awake identifies the actual device involved, operating system, device owner, associated risk as well as a forensic timeline of threat activity.

aws

The integration will tag, ssh lock-down and make a backup of an AWS EC2 instance flagged by a notable event. In addition, an email will be sent asking if the instance should be shut down. Once an approve/deny link is clicked in the email, the state of the instance will be changed.

Carbon Black.

The Carbon Black Response app for Splunk includes Adaptive Response actions to isolate endpoints, ban files, and terminate running processes. Each of these actions can be performed either on an ad-hoc basis on a notable event surfaced in Splunk ES, or on an automated basis as part of a Splunk correlation search.

The Carbon Black Defense app for Splunk includes an Adaptive Response action to change the security policy associated with a device enrolled in Carbon Black Defense. The related Carbon Black Defense add-on for Splunk automatically forwards all alert and incident information from the Carbon Black Defense console into Splunk.

Booz | Allen | Hamilton

Cyber4Sight for Splunk is a human-curated threat intelligence solution, which provides actionable intelligence, context and uses Splunk Adaptive Response actions to rapidly prioritize alerts and help speed threat response.

CISCO

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

CISCO Cisco Umbrella

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.

CISCO Cisco 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.

COFENSE

Cofense (formally PhishMe) Intelligence allows for the querying of the Cofense Intelligence API for indicators of phishing. The API queries provide enrichment and will return results on human-verified phishing domains, URLs, IPs and hashes. These malware indicators are associated with criminal phishing infrastructure. Analysts can centrally-view payload, C2 and drive-by download locations that correspond with severity ratings. Human-readable contextual reports are available to understand the attacker's tactics and techniques.

Corvil

Integration triggers a capture of all communications (packet capture) for a compromised host and enables contextual click-over investigation and analysis of traffic to expedite and improve efficacy of an investigation. It also enriches Splunk with intelligence about users, devices and indicators of compromise (IOCs).

CROWDSTRIKE

CrowdStrike customers can take advantage of three Adaptive Response actions that allow them to change the status of a CrowdStrike detection within the Splunk console, search for endpoints that have run an IOC identified within Splunk and upload IOCs from Splunk to the CrowdStrike Falcon platform for real-time detection and alerts.

CYBERARK

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

CYBERSPONSE
ADAPTIVE SECURITY

CyberSponse Splunk Technology add-on enables you to automatically forward Splunk events and notables as alerts or incidents to CyOPs™ and leverage the CyOPs™ automation and orchestration capabilities to run further investigation on them using automated workflows. It also keeps track of changes to the notable status, urgency or assignment and updates the same into the CyOPs™ record thereby seamlessly synchronizing records across Splunk and CyOPs™. The AR action "CyberSponse: Run Playbook" enables you to run CyOPs™ playbooks directly from Splunk Enterprise Security. The CyberSponse Adaptive Response action provides the capability to invoke any CyOPs playbooks from Splunk ES.

CYLANCE

This enhanced integration allows incident responders to investigate and take defensive action on Cylance protected endpoints. This includes, but is not limited to, gathering insight on malicious activity detected on the endpoint, dynamically changing and enforcing stricter security policy settings, and actively responding to real time threats detected by Cylance.

datiphy™

Datiphy can detect and label comprehensive database security and compliance breaches in near real time. This integration with Splunk ES and the Adaptive Response action provides user capability to dispatch notable events data to Datiphy service for analysis. Additionally, related security context detected by Datiphy is returned back to Splunk ES.

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.

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.

ForeScout®

ForeScout provides continuous visibility of connected devices to Splunk to better identify, prioritize and respond to incidents. The integration also enables getting and storing of ForeScout actions in Splunk. Policy-driven actions can be triggered by Splunk and executed through ForeScout for immediate incident response. ForeScout sends result of actions to Splunk to facilitate closed loop remediation.

FORTINET®

Integration allows blocking of IP addresses directly from notable events.

Gigamon®

This integration allows automated changes to Gigamon's Visibility Platform. Traffic can be automatically blocked or copied to any connected security tool based on Source IP, Destination IP, Destination Service or Transaction. Combine with Gigamon Metadata Application for Splunk to accelerate identification and response to security threats using network metadata.

graphistry

The integration turns any Splunk security event into an interactive graph-based visual investigation. Graphistry automatically reveals how triggered events connect to other events and entities across a variety of data sources. Analysts can follow proven visual investigation fast paths, and click on identified entities to send commands and annotations back into Splunk.

illumio

Illumio allows for improved visibility of east-west traffic. Security operations center (SOC) staff can detect unauthorized activity, quickly pinpoint potential attacks and identify compromised workloads. Illumio's Adaptive Response integration enables quarantining the workload, while allowing forensic access.

LogicHub

LogicHub automates threat hunting, alert triage and incident response analysis. The Adaptive Response action triggers the automated analysis and investigation of notables using LogicHub's intelligent threat analysis flows, and returns threat ranking scores and explanations back in Splunk.

netskope

Netskope Adaptive Response actions allow incident investigators to populate either a running, custom blacklist file with bad URL or an updated, custom malware file hash. The Adaptive Response actions enable the analyst to pivot from discovery in the Splunk Enterprise Security dashboard to customized policy enforcement in the Netskope Cloud Security platform.

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.

paloalto NETWORKS

Palo Alto Networks actions are two-fold: First, customers can tag IP addresses within Splunk to send to the firewall for automated policy enforcement, for example to quarantine a particular host. Second, customers can submit a URL that points to Wildfire. The Wildfire results are later accessible in search with custom search commands.

Phantom

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

Pinn AuthX

Pinn AuthX goes beyond identity management, biometrics, and multi-factor authentication. AuthX technology effortlessly and continually identifies who's interacting with an application. Part of this is physical identification through voice recognition, face-mapping or touch id. Our Adaptive Response integration provides IT admins with greater visibility into identity across their networks and the ability to audit suspicious authentication requests.

proofpoint

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

Qualys

Continuous Security

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

Recorded Future

Recorded Future, the leader in real-time threat intelligence powered by machine learning, offers an Adaptive Response "Enrichment Action," which can be applied to any IP address, domain, hash or cyber vulnerability. This Adaptive Response action pulls in rich context, including Recorded Future risk scores, for notable events.

REDSEAL

Delivers actionable intelligence from RedSeal's network modeling and risk scoring platform directly into Splunk Enterprise Security's notable events to accelerate incident response. Within minutes, and without leaving notable events, Splunk 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.

IBM Resilient

The Resilient Incident Response Platform (IRP) easily allows customers to automate the incident response processes and mitigate alerts faster and more intelligently.

RESOLVE

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.

SailPoint

SailPoint allows Splunk administrators to automate Adaptive Response remediation actions when identity and application-based security alerts are received, such as revoking and de-provisioning an identity's access due to the detection of malicious or risky behavior.

INTERNET STORM CENTER

The SANS ISC Adaptive Response action allows an analyst to send an IP address, port number or autonomous system number (ASN) to the SANS ISC Api. The information contained within provides context around how many attacks seen by this IP, port or ASN and how many blocked firewall events.

SentinelOne

The integration leverages SentinelOne APIs to provide the response actions of isolating devices and quarantining threats. The threat classification capabilities enables responders to identify threats at machine speed, shortening the time from detection to response and yielding significant time savings.

SHODAN

The Shodan Adaptive Response action sends IP addresses from your alerts up to the Shodan API. The information provided back to Splunk includes what technologies are running, what services are present, what ports are open and the geolocation data for a given IP address.

Signal Sciences

This integration allows taking a blacklisting action in the Signal Sciences platform based on correlation search results from Splunk Enterprise Security or manual search actions from Splunk Enterprise. It's easy to extend capability to also whitelist IPs, paths, or parameters from network traffic logs ingested into Splunk.

SWIMLANE

Swimlane's Adaptive Response action can create Swimlane cases pre-populated with Splunk Enterprise Security alert and notable event data. Swimlane then automatically applies workflow, automation and orchestration to the cases, enriching them and performing actions against any third-party system. This includes initiating additional Splunk searches and updating notable events in Splunk.

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.

SYNCURITY

Syncurity's first Adaptive Response action provides the ability for Splunk and Syncurity customers to forward either an alert or a Splunk Enterprise Security notable event to IR-Flow for triage and investigation. Syncurity can automatically enrich these alerts as they progress through triage and incident workflows using a variety of automated steps, including Splunk saved searches. Look for future Adaptive Response actions, as well as expanded capabilities for IR-Flow to send results back to Splunk.

TANIUM

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

TCELL

The Splunk Adapative Response initiative and tCell provide security and operations professionals with real-time blocking of application layer attacks. tCell is a next-generation cloud waf that monitors and defends applications at runtime. Our Adaptive Response action allows customers to incorporate threat intelligence and create flexible blocking rules for automatic blocking against attacks like the OWASP Top 10, XSS, SQLi, command injection, remote command execution and account takeover. If you're looking for active protections against hackers, Splunk Adaptive Response and tCell gives you the power to defend your applications in real time with no impact on your end-users' experience.

Tenable's Adaptive Response actions allow customers to get current vulnerability summaries, schedule vulnerability scans and kick off remediation scans.

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

Valimail stops email impersonation attacks with automated DMARC enforcement. The Valimail Adaptive Response action can mitigate the threat posed by fraudsters and criminals impersonating your domains. By alerting on these primary vectors of cyberattack, Valimail's Adaptive Response action provides an early risk indicator directly back into Splunk.

VMRay Adaptive Response action allows for end-users to submit URLs from Splunk to VMRay Analyzer. VMRay will dynamically analyze the file or website connected to the URL. Analysis results are ingested back into Splunk, allowing end-users to aggregate threat intelligence associated with the URL including: IOCs, threat indicators, a high-level severity and additional analysis information.

WALKOFF is an automation platform enabling plug and play integration of devices through apps. The Adaptive Response integration with Splunk makes the actions and playbooks available on both platforms available to each other and improves interoperability throughout the industry. The WALKOFF initiative is sponsored by the NSA.

The integration between the Zscaler Cloud Security Platform and Splunk automates security operations tasks, such as maintaining block lists with the latest IOCs for effective enforcement. This enables automation of workflows across a range of common SOC functions, such as incident response and threat intel management, to efficiently and effectively manage IT security.

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

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.