splunk> | amazon web services

WHITE PAPER

SECURITY INVESTIGATION AND RAPID RESPONSE USING SPLUNK AND AMAZON WEB SERVICES (AWS)

Security Investigation and Rapid Response with Splunk Enterprise, Splunk Cloud and Splunk App for AWS

It's what keeps you up at night. You're successfully delivering high quality IT services and protecting critical assets at your company. You receive an alert that some incident or breach may have occurred that is impacting your organization and your customers may be affected or their data may have been compromised. To complicate matters, your company recently migrated a portion of IT services to the cloud. So what do you do?

This scenario can happen at any time and can have a severe impact on any organization. When an issue or unsuspected attack occurs, IT teams often find out too late—learning only when the company is affected, or when an asset or device has had an unauthorized config change. Reputations are at stake as well – in many cases, notifications come from the individuals or institutions consuming these services.

Investigation and rapid response for day-to-day alerts are just as critical as hunting or addressing a breach situation. In all of these cases, response time is critical. The faster a security team can verify a threat, scope the impact across both on-premises and cloud, and plot and initiate the right course of action, the more likely that damage will be minimal. That's why security teams and IT professionals need to find and remediate security problems as soon as possible. However, it is extremely difficult to investigate efficiently and with enough depth when the story must be stitched together manually from many different IT "silos."

The Need for Security Investigation

Security investigation requires gathering foundational knowledge around alerts or notifications and analyzing that information as quickly as possible to determine what's behind the most critical issues. An analyst must quickly find the required information to determine the who, what, where, when and how of the security threat, the impacts it might have on the company, and what action to take.

Specific items to investigate are: who is associated with the alert and activity, where is the device or activity located (on-premises or on a public or private cloud), what the alert is saying, what activities are associated and related to the attack or alert, when did the attack start, and how to contain or disrupt the threat. Analysts also need ways to determine if the system has been infected or compromised, determine if the attack progressed beyond the infected system or how far it reached. Whether for alerts, hunting for an unknown threat or in a breach situation, investigations can prove challenging for anyone—whether a dedicated analyst or person that plays multiple roles.

Data typically lives in siloed locations, and can come from many different security technologies like firewalls, intrusion prevention systems, web proxies, email protection systems, anti-malware, endpoint protection suites, endpoint threat detection, and identity access management. Data can also come from non-security technologies like asset databases, network infrastructure, document repositories, card readers, servers, applications, and more. The number of silos increases with cloud deployments – between cloud services, virtualized and hosted workloads, and off-prem cloud investigations. All this data that is created is known as machine data and is relevant for security investigations, hunting, and rapid response.

While machine data presents an opportunity to gain security insights, the manual process of verifying an alert and investigating the root cause and impact of a breach across various locations can be challenging and time-consuming. By centralizing and analyzing your machine data across silos, teams gain the knowledge necessary to assess, drill down into the specifics of why and where an incident occurred, verify, and take action quickly, through a single pane of glass.

While having visibility across silos is a great starting point, verifying and addressing threats over the long term requires a more comprehensive approach.

Security Investigation Defined

Security investigation is the ability to centralize, analyze, correlate, and visualize machine data to verify and mitigate threats that pose harm, and to alert and report on those threats in order to build a strong defense against future attacks.

Basic Principles of Investigation

Security investigation requires multi-step analysis. There is a need to explore and interact with data in order to identify evidence of infection or an attack. It often starts with a small clue and then the user must find relationships, common themes, associations, and correlations in the data to determine the impact and appropriate course of action. The analysis consists of the following steps:

- Search for patterns across any data from cloud, on-prem or hybrid environments using a variety of methods – this allows the analyst to look for set terms or related terms in different technologies.
- Change the search pattern quickly by adding or removing the pattern from the search – this allows the analyst to work through their hypothesis on what to look for and follow the indicators of compromise.
- Look at the information provided by each and all data sources and then add or remove those fields from the display.
- Change the analysis timeframe to look back in time, to fixed time windows or in real time – this allows the analyst to understand activity sequencing and potential cause and effect relationships.
- Apply different statistical operations to the search results to aggregate, count, order the results to determine anomalies.
- Apply different visualization techniques to the search results to look for trends, patterns or both.

These steps are often repeated in any order and in any combination to allow the analyst to find the relationships across activities to determine what is malicious and what is normal. And once any search criteria is established, the analyst will set up a dashboard to monitor for that condition or set up an alert to be notified when the condition is encountered.

Enter Splunk

Splunk Enterprise and Splunk Cloud provide an analytics-driven approach to security on the AWS Cloud that enables organizations to quickly and efficiently perform security investigations, hunt for unknown threats, and embrace a rapid response program. Organizations can index and store all machine data from any source regardless of format or location – key security data sources include network, endpoint, identity, and threat intelligence as examples.

Any combination of search criteria and transformation, filtering, and analytical commands can be cascaded so a series of analysis can be performed. For example, in Splunk Enterprise, a user can search for an infected IP address, count all the results, filter by the top 10, and then graph

the results – all in a single Search Processing Language™ (SPL) command. SPL enables a high degree of processing speed – for example, users can directly pipe the result of any analytic step to another command for more efficient analysis.

Splunk security solutions give organizations the ability to investigate more alerts, faster and more accurately. Splunk software enables organizations to:

- Index all machine data regardless of format or location into a centralized view and extract fields to easily find patterns, relationships, and meaning. This is important to verify malicious activity and progression within an attack.
- Achieve better verification with guided multi-step processing of data to gain deep insights by searching data without schema or limitations.
- Interact with data quickly and easily – with the field extractions and search result interactions users can refine the search criteria, while searching across all data irrespective of format to determine next actions.
- Search and investigate by a variety of techniques across any data set more quickly – refine a search by simply adding or removing SPL commands to get the desired "search criteria," providing the ability to remove non-relevant fields and respond rapidly to the incident.
- Understand sequences of activities – users can change the time display of the analysis in real time to look at historical data or a specific time window – this can help develop correlations of possible relationship cause and effect.
- Gain complete control of analysis, based on time – the user can customize and describe the parameters of the timeline to understand when and possibly why an incident might have occurred.
- Aggregate, count, and order the results with a drop-down menu and apply different statistical analysis of the search results to determine anomalies.
- Create visualizations and dashboards of the search results to look for trends, patterns of activity and share the information with a broader range of people to collaborate and respond quickly.
- Monitor their entire infrastructure – cloud, hybrid, and on-premises – with custom alerts and the visualizations that can be created, teams can make more informed decisions and eventually preempt issues before they happen.
- Monitor cloud account activity –– using the Splunk App for AWS, cloud and security teams gain critical insights into their AWSaccount(s), enabling them to add real-time visibility of various AWS service components into their investigative process to help mitigate risk, maintain compliance and conduct audits.

When used for security investigation, the Splunk platform helps users gain a range of analytical capabilities, including visual analysis, graphical representation of thresholds, alarms, and indicators. Security knowledge and workflow can be extended to broader data sets that can capture and deliver insights to any team using applications that are integral to your business. This helps teams collaborate and address the shortage of skills and empower less technical staff to easily solve problems using their data.

By making it easy to collect and analyze data from nearly any source, IT professionals and security analysts can improve investigation and workflow effectiveness. Looking at all the data and performing analytics allows security teams to get a better view of their entire infrastructure and take the necessary steps to reduce risks.

Managing Risk and Time

With Splunk security solutions, teams can more effectively manage risks to get back to focusing on business needs without having to continually look for and solve the same issues. This enables security practitioners to spend their time on priority security issues and strengthening the overall security posture rather than getting bogged down in manual data gathering or trying to manually stitch the story together between what's happening on-prem vs on the AWS Cloud. Further, operations teams will have improved collaboration and workflow and can document knowledge of issues that arise.

Splunk Enterprise and Splunk Cloud can provide users the power to understand their challenge, determine what actions to take, and investigate efficiently to quickly determine if there is a critical issue, so that security teams can focus on analyzing and visualizing security insights to share and plan so the same issue doesn't continue to happen. Splunk enables teams to collaborate and gain end-to-end visibility across the entire infrastructure to help minimize damage and disruption to the business.

Splunk and AWS

Splunk has closely aligned with AWS to deliver solutions that offer real-time visibility into your cloud applications, infrastructure and AWS account. With these solutions, you can monitor your AWS deployment using Splunk as well as deploy Splunk software as an AWS-based cloud service.

Splunk solutions, including the free **Splunk App for AWS**, enable you to:

- Seamlessly transform data from your AWS environment (including AWS CloudTrail, AWS Config, Config Rules, Amazon CloudWatch, AWS Billing and Cost Management, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Block Store (Amazon EBS), Amazon Simple Storage Service (Amazon S3), Elastic Load Balancing, Amazon Virtual Private Cloud (Amazon VPC) Flow Log, Amazon Inspector, Amazon Relational Database Service (Amazon RDS), and Metadata inputs) into real-time security insights across users and resources.
- Gain instant insight through pre-built dashboards and reports.
- Identify and resolve AWS security risks
- Fulfill your role in the AWS shared responsibility model – ensuring security of workloads and applications running on AWS.
- Analyze full audit trail of all user activity with data from AWS CloudTrail for real-time monitoring of critical security related events – including changes to security groups, unauthorized user access, and changes to admin privileges.
- Gain real-time monitoring and topology visualization of all your AWS resources – enabling you to view your entire environment in a single topology diagram, monitor instance start/stops, and gain end-to-end visibility across all network configuration changes.

Try Splunk now, no software installation required – **try hands-on basic techniques** with a guided walkthrough of investigating a real "threat" in an online sandbox environment

Learn more about the **Splunk App for AWS** and see how it can help you gain visibility into your AWS accounts

Simplify your procurement process today and **subscribe** to Splunk Cloud on the AWS Marketplace

WP-Splunk-Security-Investigation-Splunk-and-AWS-cobranded-101