Stay afloat using AWS Security Hub and Splunk to find, fix, and prevent security leaks

splunk> turn data into doing™

aws

Table of contents

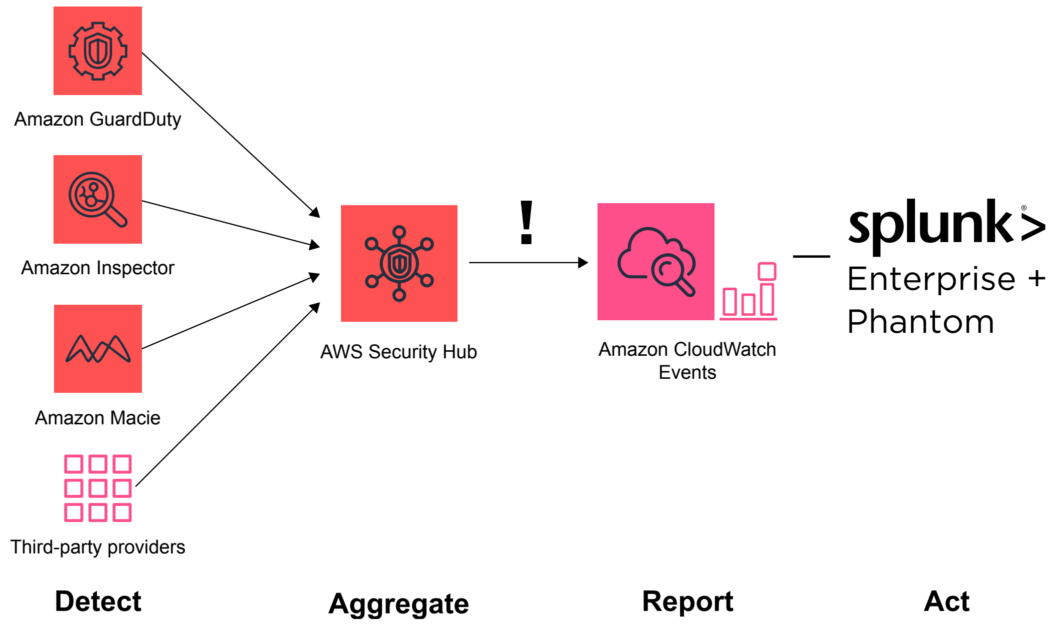
Is data threatening to knock you off your feet?

With each new cloud service you adopt, another wave of data swells into your business. Depending on how you approach it, the data could be your ride to the top, or it could crush you on the rocks. In no other area is this as obvious or immediate as it is in security.

Amazon Web Services (AWS) offers a wide range of tightly integrated security services, such as Amazon GuardDuty, Amazon Inspector, and Amazon Macie, that monitor the security posture of your AWS accounts.

AWS Security Hub aggregates, organizes, and prioritizes security findings from AWS security services and third-party providers across all your AWS environments.

Splunk, the data to everything platform, integrates with AWS to deliver solutions that offer real-time visibility into your cloud applications, infrastructure, and accounts. The platform's automated, intelligent assistance helps you act quickly and efficiently to stop security threats.



Turn the crush of security data into powerful insights using Splunk with AWS

AWS Security Hub enables a centralized security approach

- Aggregate security findings across your AWS environments
- Take action against security findings by directing them to the appropriate target for processing the finding
- Perform industry compliance checks against your AWS environments
- Pinpoint areas that require attention via Insights
- See security insights and alerts quickly through visual displays

AWS GuardDuty detects and monitors AWS workloads

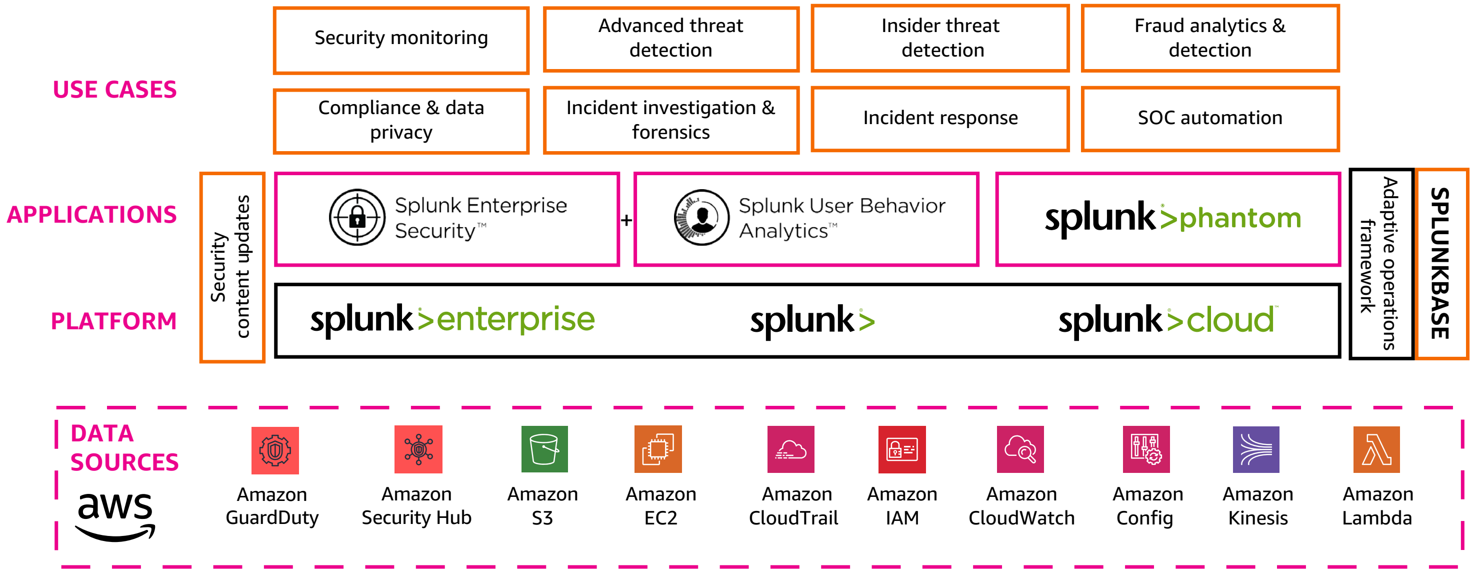
- Accurate and highly available threat detection with severity level prioritization
- Set automated threat response and remediation
- Integrates with AWS Security Hub for improved security findings

Find secure footing using Splunk with AWS Security Hub

The Splunk platform provides real-time, end-to-end visibility into your AWS environment to help you organize, display, and take action on your security alerts.

AWS Security Hub makes it possible to aggregate security findings from AWS and third-party sources and export them to Splunk through a single point of integration—even as you continue to add new data sources. Through the configuration options in AWS Security Hub, you can specify which, if not all, of your security findings are sent to Splunk and modify your settings as needed.

Splunk Phantom allows you to automate responses to your findings using machine learning and AI capabilities. The integration between Splunk and AWS makes it easy for you to detect future security threats and free up your security personnel for higher value activities.



USE CASES

Security monitoring | Advanced threat detection | Insider threat detection | Fraud analytics & detection

Compliance & data privacy | Incident investigation & forensics | Incident response | SOC automation

APPLICATIONS

Splunk Enterprise Security™ + Splunk User Behavior Analytics™ | splunk>phantom

PLATFORM

splunk>enterprise | splunk> | splunk>cloud

Security content updates

Adaptive operations framework

SPLUNKBASE

DATA SOURCES

aws

Amazon GuardDuty | Amazon Security Hub | Amazon S3 | Amazon EC2 | Amazon CloudTrail | Amazon IAM | Amazon CloudWatch | Amazon Config | Amazon Kinesis | Amazon Lambda

To get started with Splunk and AWS Security Hub, follow the four key steps:

1. Create a point of integration using the **Splunk Add-on for AWS**
2. Add Security Orchestration, Automation, and Response (SOAR) services with Splunk Phantom
3. Automate security actions using Splunk Phantom playbooks
4. Oversee security remediation from Phantom Mission Control

Let’s explore these steps in more detail. →

Step 1:

Create a point of integration using the Splunk Add-On for AWS

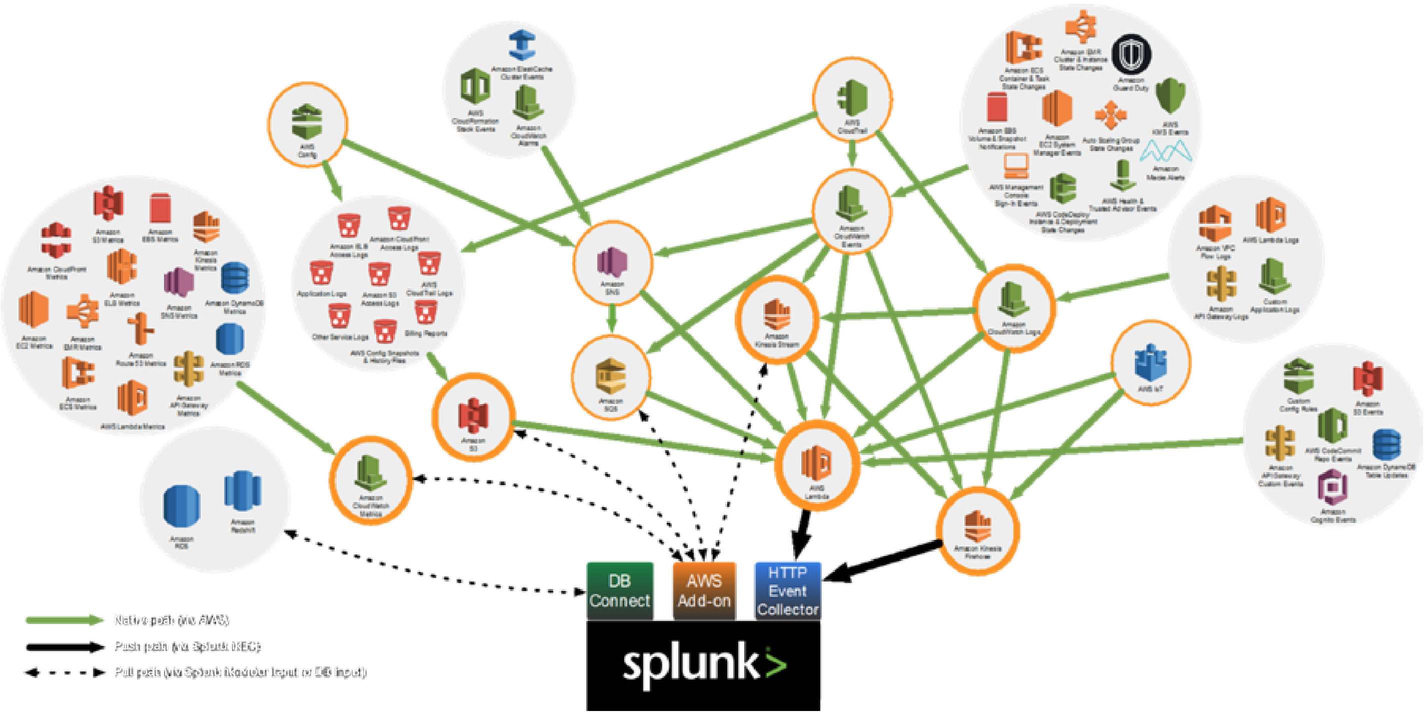
To create a point of integration between the platform and AWS, use the Splunk Add-On for AWS. You can download the whitepaper about Getting Data Into (GDI) Splunk From AWS for technical guidance setting up the Add-On.

As a best practice for using Splunk with your AWS environment, we recommend deploying either Splunk Enterprise or Splunk Cloud as the data integration point for AWS and using Splunk Phantom to apply rules, automation, and intelligence to your data.

Splunk Enterprise is the software deployment of Splunk's complete data platform that's perfect for any organization with data analytics needs. Unlike alternatives, Splunk enables you to easily access, investigate and combine structured and unstructured data generated by your IT, security and business systems, apps and devices, as well as monitor and analyze these environments using artificial intelligence and machine learning, and act in near real-time to achieve business value.

Splunk Cloud is an AWS-based service that delivers the benefits of Splunk Enterprise with the flexibility of a cloud service.

Bring AWS data into Splunk using the Splunk Add-On for AWS


DB Connect
AWS Add-on
HTTP Event Collector
splunk>
Native path (via AWS)
Push path (via Splunk HEC)
Pull path (via Splunk Modular Input or DB input)

*Some organizations may use Splunk Phantom without Splunk Enterprise. Please consult your Splunk account manager for advice on when this scenario may be right for you.

Step 2:

Add SOAR services with Splunk Phantom

Combine nearly all your data with Phantom's 1,200+ APIs and 225+ app integrations.

After transferring your security findings from AWS Security Hub to Splunk, you need to quickly make sense of the data.

Splunk Phantom is our security orchestration, automation, and response (SOAR) service that gives you full access to the contents of your security data for the purposes of automated decision making.

You can use Phantom's automation framework to translate AWS Security Hub findings into immediate action. The combined power of AWS Security Hub and Phantom dramatically reduces response times for everything from SSH brute force attempts on AWS EC2 instances to AWS IAM credential compromise attacks.

Phantom integrates with 8 AWS services and more than 250 other security tools that can be launched via the AWS Marketplace such as automation playbooks for out-of-the-box use with AWS Security Hub findings.

Trigger Phantom into action using any type or source of security data—including incidents, threat indicators, vulnerabilities, emails, and more. With Phantom, you can either push data into it or pull from an externally supported SIEM or analytics tool.

Splunk Phantom supports six key functions of the Security Operations Center (SOC)

Automation:
Codify your workflows into automated playbooks using our visual editor (no coding required) or the integrated Python development environment.

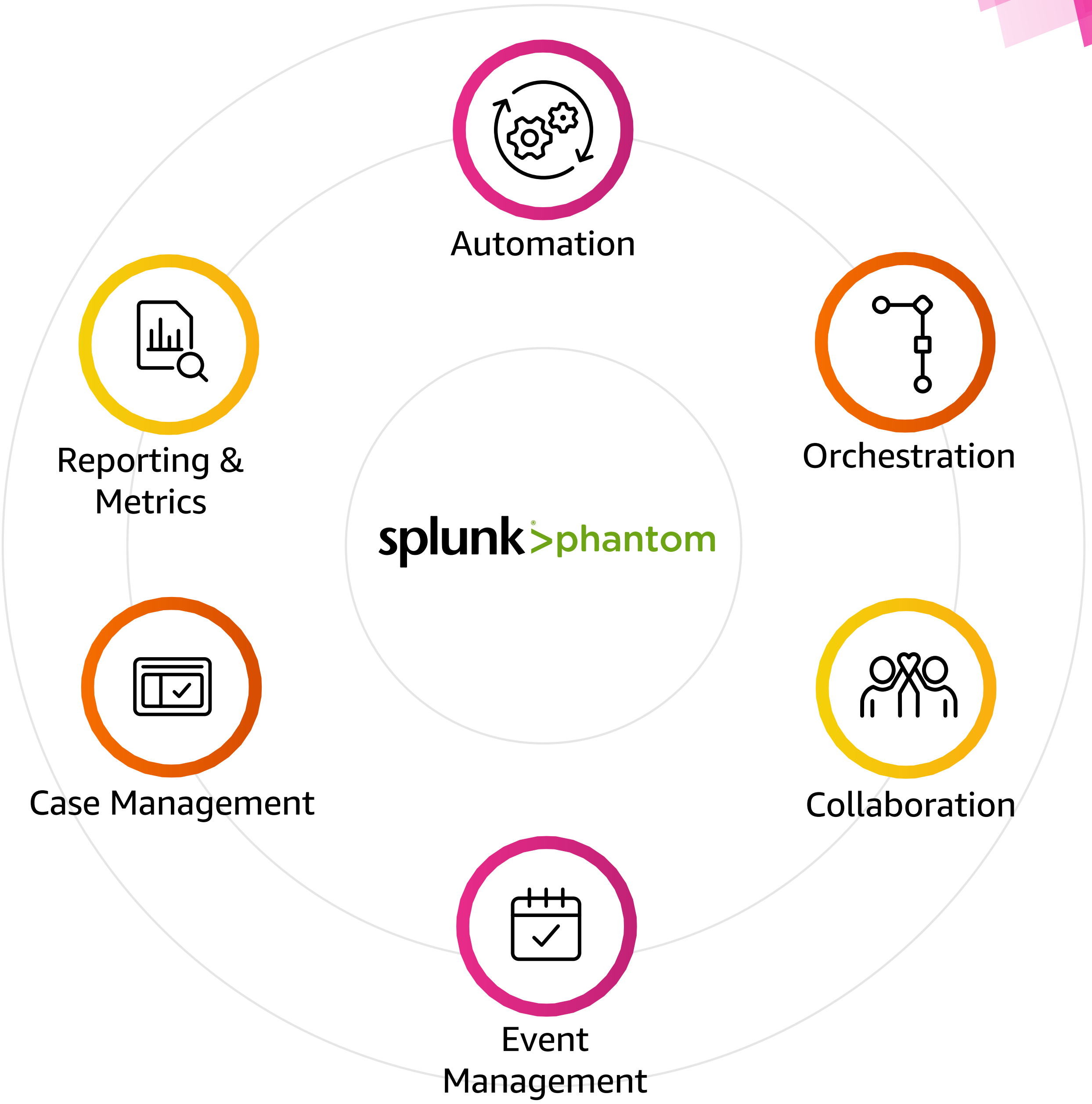
Orchestration:
Connect and coordinate complex workflows across your team and tools through integration with hundreds of apps and thousands of APIs.

Collaboration:
Drive efficient communications through integrated chat to shared case notes and more and offers helpful suggestions throughout the process.

Event Management:
Rapidly triage low-level events or other security objects in an automated, semi-automated, or manual fashion.

Case Management:
Track and monitor case status and progress by aggregating and escalating confirmed events to cases using one of our case templates or your own.

Reporting and Metrics:
Simplify human oversight and auditing capabilities using dashboards and reports to consolidate the critical information needed to understand your security.



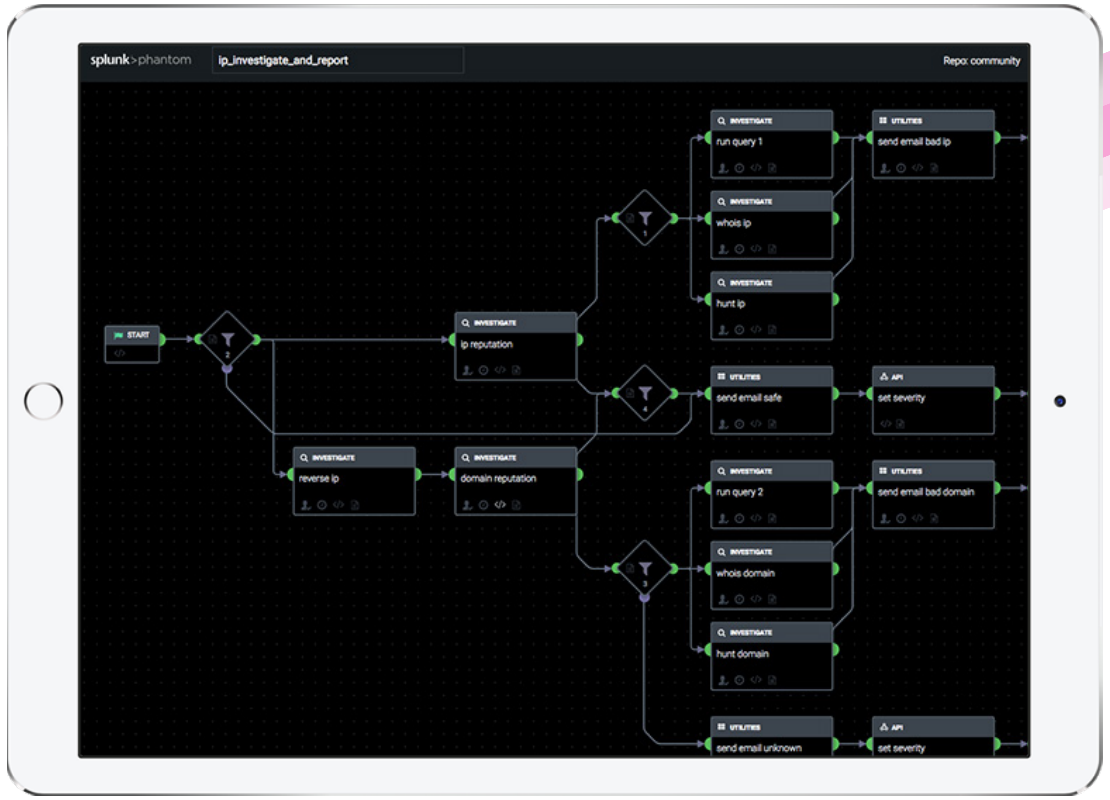
Step 3:

Automate security actions using Phantom playbooks

Splunk Phantom includes playbooks which are the codification of your Security Operations (SecOps) plan. In practice, they're high-level Python scripts that Phantom interprets in order to execute your mission. Playbooks hook into the Phantom Platform and its capabilities to execute actions for you and ensure a repeatable and auditable process around your security operations.

Actions are the high-level primitives available within Phantom playbooks, such as:

- **Detonate File**
  Detonate a file in a supported sandbox
- **Geolocate IP**
  Perform a geolocation lookup on a given IP address
- **Hunt File**
  Look for a particular file on endpoints
- **Block URL**
  Block a URL on perimeter devices
- **Quarantine Device**
  Disconnect a device from the network via NAC



Playbooks allow you to execute a series of actions across your security infrastructure in seconds, versus the hours it might take you to perform analogous tasks manually. You can codify your workflows into automated playbooks using our visual editor (no coding required) or the integrated Python development environment.

The Phantom Visual Playbook Editor (VPE) allows both developers and non-developers to construct and customize complex Phantom Playbooks graphically through a drag-and-drop interface. The VPE generates all the supporting code that's required behind the scenes and in real time.

You can also use the VPE to create a playbook using function blocks and connectors, which describe the order of operation.

Step 4:

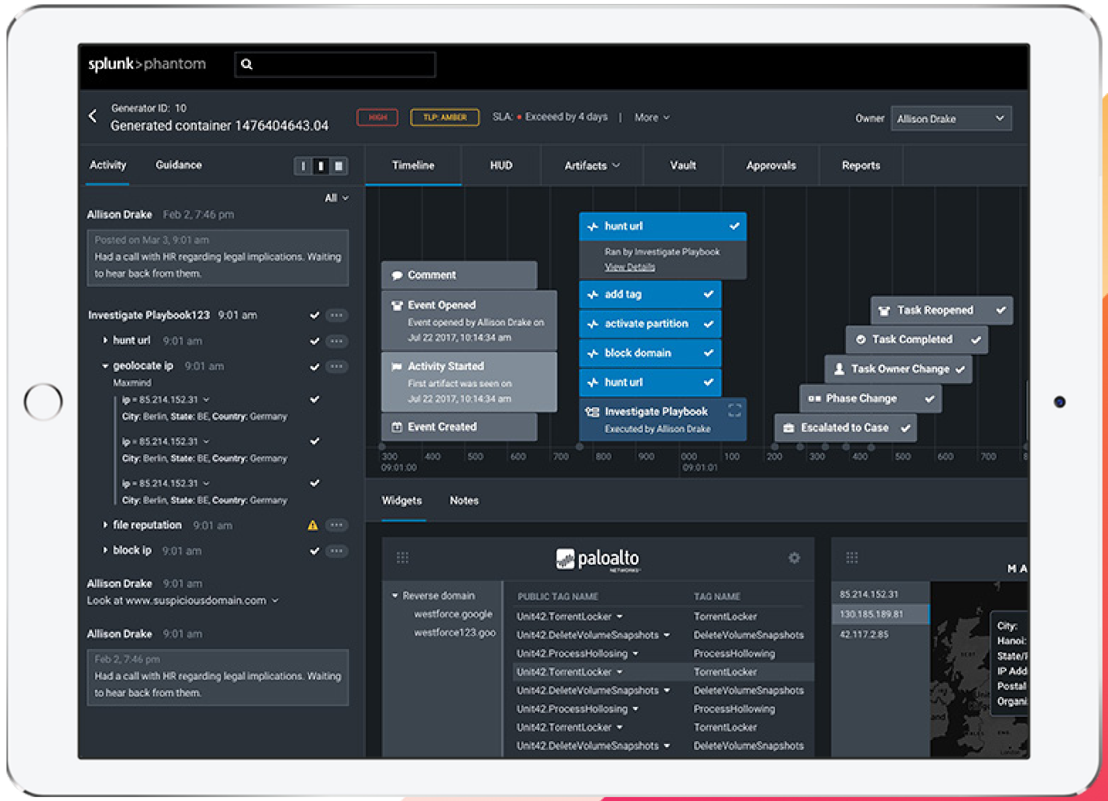
Oversee security remediation from Phantom Mission Control

Phantom Mission Control brings event data and SOC tools together into one consolidated view, to help your analyst understand, investigate, and act on an event without having to switch between different screens and tools. It complies the results of the playbook's actions (as described in step 3) into a single view, so you can decide what to do next.

The interface includes access to all event activity history, contextual and interactive data views, a digital vault for attachments, as well as fully integrated automation and case management controls.

Integrated within Mission Control, Phantom Mission Guidance is an intelligent assistant that supports security operations analysts by offering suggestions to help investigate, contain, eradicate, and recover from a security event. It works by mapping security event data to your currently configured SOC tools and playbooks. Phantom Mission Guidance recommendations help educate newer analysts on steps to take and validate the choices of more experienced analysts.

The Activity Feed in the Phantom Mission Control interface displays all current and historical action and playbook activity that has acted on the currently displayed event. This allows you to quickly see the success, ongoing execution, and results of all automation operations for the event. The Activity Feed also provides team collaboration capabilities that are integrated inline with automation details and other data, forming a record of all relevant event information.



Allison Drake Feb 2, 7:46 pm

Posted on Mar 3, 9:01 am
Had a call with HR regarding legal implications. Waiting to hear back from them.

Investigate Playbook123 9:01 am
- hunt url 9:01 am
- geolocate ip 9:01 am
  Maxmind
  ip = 85.214.152.31
  City: Berlin, State: BE, Country: Germany
  ip = 85.214.152.31
  City: Berlin, State: BE, Country: Germany
  ip = 85.214.152.31
  City: Berlin, State: BE, Country: Germany
- file reputation 9:01 am
- block ip 9:01 am

Allison Drake 9:01 am
Look at www.suspiciousdomain.com

Allison Drake 9:01 am

Feb 2, 7:46 pm
Had a call with HR regarding legal implications. Waiting to hear back from them.

Event opened by Allison Drake on Jul 22 2017, 10:14:34 am

First artifact was seen on Jul 22 2017, 10:14:34 am

Ran by Investigate Playbook
View Details

Executed by Allison Drake

Reverse domain
westforce.google
westforce123.goo

PUBLIC TAG NAME	TAG NAME
Unit42.TorrentLocker	TorrentLocker
Unit42.DeleteVolumeSnapshots	DeleteVolumeSnapshots
Unit42.ProcessHollosing	ProcessHollowing
Unit42.TorrentLocker	TorrentLocker
Unit42.DeleteVolumeSnapshots	DeleteVolumeSnapshots
Unit42.ProcessHollosing	ProcessHollowing
Unit42.TorrentLocker	TorrentLocker
Unit42.DeleteVolumeSnapshots	DeleteVolumeSnapshots

85.214.152.31
130.185.189.81
42.117.2.85

Protect your AWS accounts with Splunk's proven solution

AWS Security Hub makes it easier than ever to aggregate alerts and potential threats inside your AWS environments. Its seamless integration with Splunk and Splunk Phantom makes it possible for you to take action quickly to enhance your security posture.

Splunk's competency has been recognized by AWS time and again through partner titles, including:

- **AWS Advanced Technology partner**
- **AWS Security competency**
- **AWS Data and Analytics competency**
- **AWS Cloud Management Tools competency**
- **AWS Container competency**
- **AWS DevOps competency**
- **AWS Education competency**
- **AWS Government competency**
- **AWS IoT competency**
- **AWS MSP Technology provider**
- **AWS Marketplace partner**
- **AWS Security Automation & Orchestration partner**
- **AWS SaaS Program partner**
- **AWS GovCloud (US) Skill partner**

Many of today's **leading global companies** choose Splunk as their security solution for their AWS accounts.

Accelerate deployment using Splunk Amazon Machine Images (AMIs)

Splunk offers AMIs to enable you to rapidly deploy standardized, preconfigured instances on Amazon EC2. Using a Splunk AMI, you can gain access to Splunk solutions with just a few clicks. AMIs are available on the AWS Marketplace for Splunk Enterprise, Splunk Insights for AWS Cloud Monitoring, as well as **Splunk Phantom AMI**.

For more information on Splunk and AWS solutions, visit the Splunk website or visit our AWS Marketplace website.

turn data into doing™

© 2019 Splunk Inc. All rights reserved. Splunk, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners.