AWS re:Inforce

JUNE 10 – 12, 2024 | PHILADELPHIA, PA

splunk>

TDR226-S

SPONSORED BY SPLUNK

Building a better lake: Federated search for Amazon Security Lake

Colin Gibbens

Director Product Manager
Splunk

Forward-Looking Statements

This presentation may contain forward-looking statements regarding future events, plans or the expected financial performance of our company, including our expectations regarding our products, technology, strategy, customers, markets, acquisitions and investments. These statements reflect management's current expectations, estimates and assumptions based on the information currently available to us. These forward-looking statements are not guarantees of future performance and involve significant risks, uncertainties and other factors that may cause our actual results, performance or achievements to be materially different from results, performance or achievements expressed or implied by the forward-looking statements contained in this presentation.

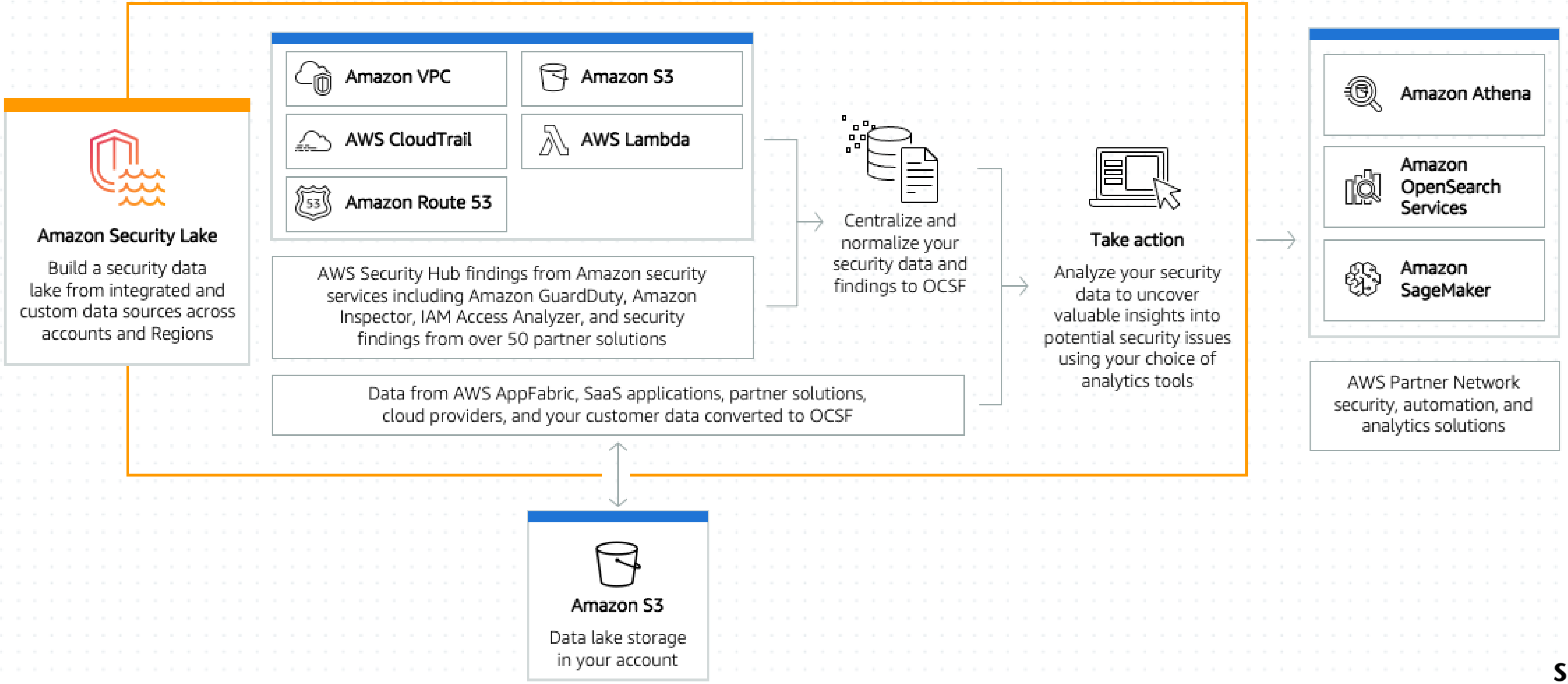
For additional information about factors that could cause actual results to differ materially from those described in the forward-looking statements made in this presentation, please refer to our periodic reports and other filings with the SEC, including the risk factors identified in our most recent quarterly reports on Form 10-Q and annual reports on Form 10-K, copies of which may be obtained by visiting the Splunk Investor Relations website at www.investors.splunk.com or the SEC's website at www.sec.gov. The forward-looking statements made in this presentation are made as of the time and date of this presentation. If reviewed after the initial presentation, even if made available by us, on our website or otherwise, it may not contain current or accurate information. We disclaim any obligation to update or revise any forward-looking statement based on new information, future events or otherwise, except as required by applicable law.

In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. We undertake no obligation either to develop the features or functionalities described, in beta or in preview (used interchangeably), or to include any such feature or functionality in a future release.

splunk>

Amazon Security Lake (JT), 5 minutes

Overview



Amazon Security Lake

Build a security data lake from integrated and custom data sources across accounts and Regions

Amazon VPC

Amazon S3

AWS CloudTrail

AWS Lambda

Amazon Route 53

AWS Security Hub findings from Amazon security services including Amazon GuardDuty, Amazon Inspector, IAM Access Analyzer, and security findings from over 50 partner solutions

Data from AWS AppFabric, SaaS applications, partner solutions, cloud providers, and your customer data converted to OCSF

Centralize and normalize your security data and findings to OCSF

Take action

Analyze your security data to uncover valuable insights into potential security issues using your choice of analytics tools

Amazon Athena

Amazon OpenSearch Services

Amazon SageMaker

AWS Partner Network security, automation, and analytics solutions

Amazon S3

Data lake storage in your account

Overview

Splunk and Amazon Security Lake

- **To be a SIEM or not – that is the question**
  - Splunk is designed and built to be a SIEM for customers to store data and query to look for security findings and/or to build dashboards and reports in near real time in a performant manner
  - Amazon Security Lake is designed to be a data lake to store information for a long period of time in a cost-effective manner, but it would be more costly and not sufficiently performant for a customer to try and use it as a SIEM
- **A SIEM consists of several components**
  - **Data storage:** Stores data that is indexed and can be queried very fast to look for security-related issues
  - **Rules engine:** Provides OOTB security content or the ability to create new security content to run against the data to look for matches in a performant manner in real to near real time using simple to complex queries
  - **Incident management:** A frontend that the SOC uses to manage an incident (detection) once a rule fires, detecting a match
  - **Dashboard and reporting:** OOTB or custom dashboards and reports used by the SOC to report on security posture and risk
  - **Security event analysis (link analysis):** A graphical representation of a security event from when it started to completion
  - **Other SIEM components**
    - Workflow engines (SOAR) to automate response actions
    - Threat intelligence integrations to pull down indicators for IoC matching
    - User behavior analytics to monitor for suspicious user activity

Main Use Cases

Splunk and Amazon Security Lake Use Cases

Splunk

- Data collector and aggregator of log sources from all types of devices and data producers from IT to security, from on-premises to cloud devices
- A highly performant reporting engine that allows customers to use OOTB or create custom reports, dashboards, visualizations, graphing, and analytical views across the data in a near real-time manner
- Provides the ability to create or use prebuilt applications on top of the data stored in the platform
- Correlates, runs detections, and analyzes the data, looking for patterns and security-related risk

Amazon Security Lake

- Data lake to store Amazon or third-party data for long periods of time for compliance, auditing, and integration with other third-party vendors to provide value on the data; data stored in Security Lake is normalized using OCSF
- Low-cost storage for storing large amounts of data for a long period of time
- Compliance and audit storage for meeting internal and external requirements for storing data in long-term storage
- Data lake for third-party tools to integrate with to provide reporting, searching, and analytics on top of the data
- Additional AWS applications (Amazon Athena, Amazon SageMaker, Amazon OpenSearch Service, etc.) can be used to provide additional capabilities

Splunk/Amazon Security Lake Integration

Splunk Add-on for AWS V7 or Later

- Available on **Splunkbase – splunkbase.splunk.com/app/1876**
- Ingests data from AWS data sources and Amazon Security Lake in OCSF
- OOTB content for enterprise security for OCSF AWS detections available

Splunk Add-on for Amazon Security Lake

- Available on **Splunkbase – splunkbase.splunk.com/app/6684**

Splunk and Amazon Security Lake

Category	Use Case	Solution
ETL (extract, transform, and load)	**Data ingesting and normalization**	Data from Amazon Security Lake can be collected, normalized, and stored in Splunk through the Splunk Add-On for AWS Customers will be able to search the normalized data from Security Lake using Splunk Federated Search
Reporting	**Creation of reports, dashboards, and visualizations**	Via ingestion into Splunk indexes, selected data sources from Security Lake can be reported on using the Splunk Add-on for AWS Via Federated Search, customers can perform reporting against data resident in Amazon Security Lake
Threat detection	**Real to near real-time running of detection content to look for security risk**	Via ingestion into Splunk, the data sources from Security Lake can be continuously analyzed using detection content Via Federated Search (Indexer), customers can run detection rules against data indexed from Security Lake
Threat hunting	**Searching for indicators or findings in data**	Via ingestion into Splunk, data from Security Lake can be searched Via Federated Search (Amazon Athena, Indexer), customers can perform ad-hoc and IoC searches against data resident in Security Lake or that has been indexed
Compliance data storage	**Long-term data storage to meet regulations**	Customers can pull data into Splunk from Amazon Security Lake to run reports and detections against the data but store it long-term in Amazon Security Lake for audit purposes Customers can store data in Amazon Security Lake long-term and query data using Splunk via federated search
Retrospective searching	**Searching for security findings (IoC, artifacts) in historical data that is not in Splunk**	Customers can run federated search queries for indicators across current and long-term data – this could be the standard 90 days worth of data stored in Splunk Cloud and historical data that is in Security Lake
User behavior analytics	**Analytics/ML to look for suspicious patterns**	Customers are able to run federated search queries for indicators across current and long-term data

splunk>

Running Security Analytics on Security Lake Data

Goal: Run cost- and performance-optimized security detections and threat hunting searches on Security Lake data. Expand Splunk horizons to high-volume security datasets directly ingested into Security Lake, due to cost and low signal-to-noise nature of the data.

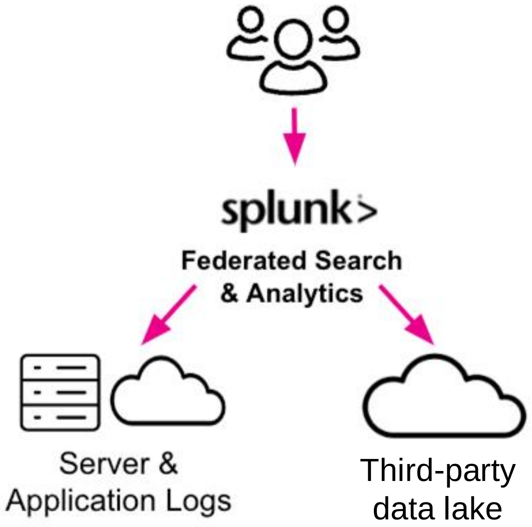
Provide premade and turnkey AWS security detection content to customers to rapidly derive value from data stored in Security Lake from supported AWS services that generate security events, like AWS CloudTrail and AWS Security Hub.

Data Profile

- Schematized security data
- Six primary schema categories

Use Cases

- **Threat detection:** Iterative high-frequency detections on near real-time short time range data
- **Threat hunting:** Infrequent ad-hoc threat hunting searches on long time range datasets
- Run iterative high-frequency detections on specific old/historical datasets



OOTB (Security Lake) Detections

AWS Identity and Access Management (IAM) Privilege Escalation

- asl aws createaccesskey
- asl aws iam delete policy
- asl aws password policy changes

AWS User Monitoring

- asl aws excessive security scanning

AWS IAM Account Takeover

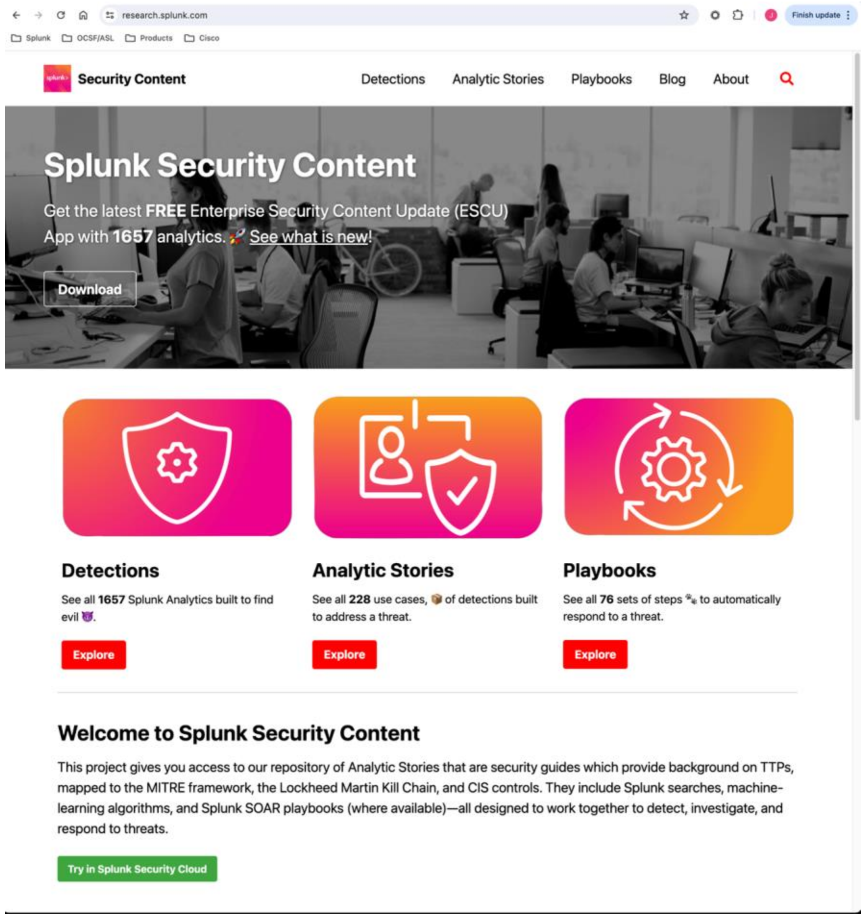
- asl aws concurrent sessions from different ips
- asl aws multi factor authentication disabled
- asl aws new mfa method registered for user

AWS Defense Evasion

- asl aws defense evasion delete cloudtrail
- asl aws defense evasion delete cloudwatch log group
- asl aws defense evasion impair security services

Compromised User Account

- asl aws concurrent sessions from different ips
- asl aws password policy changes



Splunk Security Content

Get the latest **FREE** Enterprise Security Content Update (ESCU) App with **1657** analytics. 🚀 See what is new!

Detections

See all **1657** Splunk Analytics built to find evil 😈.

Analytic Stories

See all **228** use cases, 📦 of detections built to address a threat.

Playbooks

See all **76** sets of steps 🐾 to automatically respond to a threat.

Welcome to Splunk Security Content

This project gives you access to our repository of Analytic Stories that are security guides which provide background on TTPs, mapped to the MITRE framework, the Lockheed Martin Kill Chain, and CIS controls. They include Splunk searches, machine-learning algorithms, and Splunk SOAR playbooks (where available)—all designed to work together to detect, investigate, and respond to threats.

Threat Detection and Hunting (Future)

Enterprise Security Detection

- Customer stores Amazon VPC and AWS CloudTrail data in Amazon Security Lake
- Enterprise Security (ES) runs federated search detections against Security Lake
- Enterprise Security generates a risk-based alerting (RBA) alert showing multiple suspicious activities from the CloudTrail data related to the Amazon EC2 instance in a short period of time
- The RBA alerts show unusual login activity on the EC2 instance
- ES detection matching search rule runs against the indexed VPC Flow Log data in Security Lake – detects outbound traffic to a C&C server
- The analyst sees an incident with several RBA findings and the IP addresses that were matched to threat intelligence

Q&A and Demo

splunk>