Analytics-based Investigation & Automated Response with AWS + Splunk Security Solutions

Scott Ward

Principal Solutions Architect | Amazon Web Services

Wissam Ali-Ahmad

Lead Solutions Architect | Splunk

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or plans of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results may differ materially. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, it may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements made herein.

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. Splunk undertakes no obligation either to develop the features or functionalities described or to include any such feature or functionality in a future release.

Scott Ward

Principal Solutions Architect | Amazon Web Services

splunk> .conf20

Wissam Ali-Ahmad

Lead Solutions Architect | Splunk

splunk> .conf20

Agenda

"The speed of the cloud waits for no one, least of all the CISO" – Gartner

1) **AWS Security Principles**
   - Shared responsibility model
   - Security architectures

2) **Getting AWS Security Data Into Splunk**
   - AWS Data Sources
   - Scalable Cloud to Cloud Integrations

3) **Achieving heathy security posture of your AWS workloads**
   - Use Cases for detection and investigation using modern SIEM Demo

4) **Responding faster to cloud incidents**
   - Automated response using SOAR

5) **Next Steps**
   - Resources

.conf20

splunk>

AWS Security Principles

Security is our top priority

Shared Responsibility Model

Customers have their choice of security configuration **ON** the Cloud

- CUSTOMER DATA
- PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT
- OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION
- CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION
- SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)
- NETWORKING TRAFFIC PROTECTION (ENCRYPTION INTEGRITY, IDENTITY)

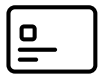
splunk>

AWS is responsible for the security **OF** the Cloud

- SOFTWARE
  - COMPUTE
  - STORAGE
  - DATABASE
  - NETWORKING
- HARDWARE/AWS GLOBAL INFRASTRUCTURE
  - REGIONS
  - AVAILABILITY ZONES
  - EDGE LOCATIONS

splunk> .conf20

AWS Security, Identity, and Compliance Solutions



Identity and Access Management

- AWS Identity & Access Management (IAM)
- AWS Single Sign-On
- AWS Organizations
- AWS Directory Service
- Amazon Cognito
- AWS Resource Access Manager

Detection

- AWS Security Hub
- Amazon GuardDuty
- Amazon Inspector
- Amazon CloudWatch
- AWS Config
- AWS CloudTrail
- VPC Flow Logs
- ction

Infrastructure Protection

- AWS Firewall Manager
- AWS Shield
- AWS WAF – Web application firewall
- Amazon Virtual Private Cloud (VPC)
- AWS PrivateLink
- AWS Systems Manager

Data Protection

- Amazon Macie
- AWS Key Management Service (KMS)
- AWS CloudHSM
- AWS Certificate Manager
- AWS Secrets Manager
- AWS VPN
- Server-Side Encryption

Incident Response

- Amazon Detective
- CloudEndure DR
- AWS Config Rules
- AWS Lambda

Splunk & AWS Security Services

Amazon GuardDuty

VPC Flow Logs

AWS CloudTrail

AWS Security Hub

Successful security practices in AWS

Identify, investigate, and respond to threats in your AWS environments at scale

Use Case 1: Protecting Your AWS Account

APIs back how you interact with your AWS account.

Access to APIs and their usage are important controls.

- Are credentials being used from unusual locations?
- Are dormant credentials now being used?
- Are credentials being used in a way that is abnormal?

Use Case 1: Protecting Your AWS Account

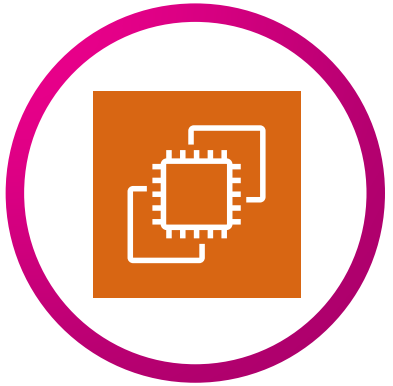
What to do with findings about your AWS account?

- Who do the IAM credentials belong to?
- What access do the credentials have?
- Impact if the credentials are blocked?
- Why is this happening?
- How should I respond?
- How do I prevent this in the future?

Use Case 2: Protecting Virtual Compute Resources

Amazon EC2 is a critical component for many customer workloads.

Understanding threats to EC2 based workloads is critical



- Is someone scanning my instances looking for a way in?
- Has an instance started acting in an unusual way?
- Has an instance started communicating with a known bad actor?

Use Case 2: Protecting Virtual Compute Resources

What to do with findings about your EC2 instances?

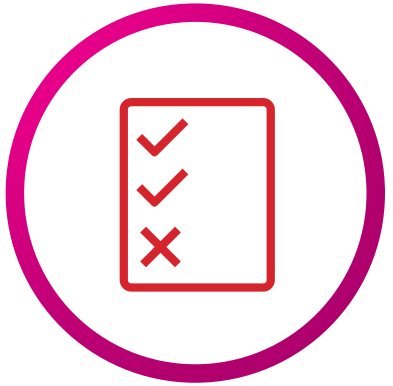
- What is the severity of the threat?
- What is the purpose of this instance?
- Why is this happening?
- What should my response be?
- How do I prevent this in the future?

Use Case 3: Maintaining Compliance

Maintaining compliance against internal and/or external controls.

Being out of compliance puts me and my data at risk.

Need to maintain compliance across a broad set of AWS resources.



- Am I currently in compliance?
- Am I aligning with compliance best practices on AWS?
- I need to know as soon as I go out of compliance.
- I need to quickly fix things when I am out of compliance.

Use Case 3: Maintaining Compliance

What to do with findings related to compliance?

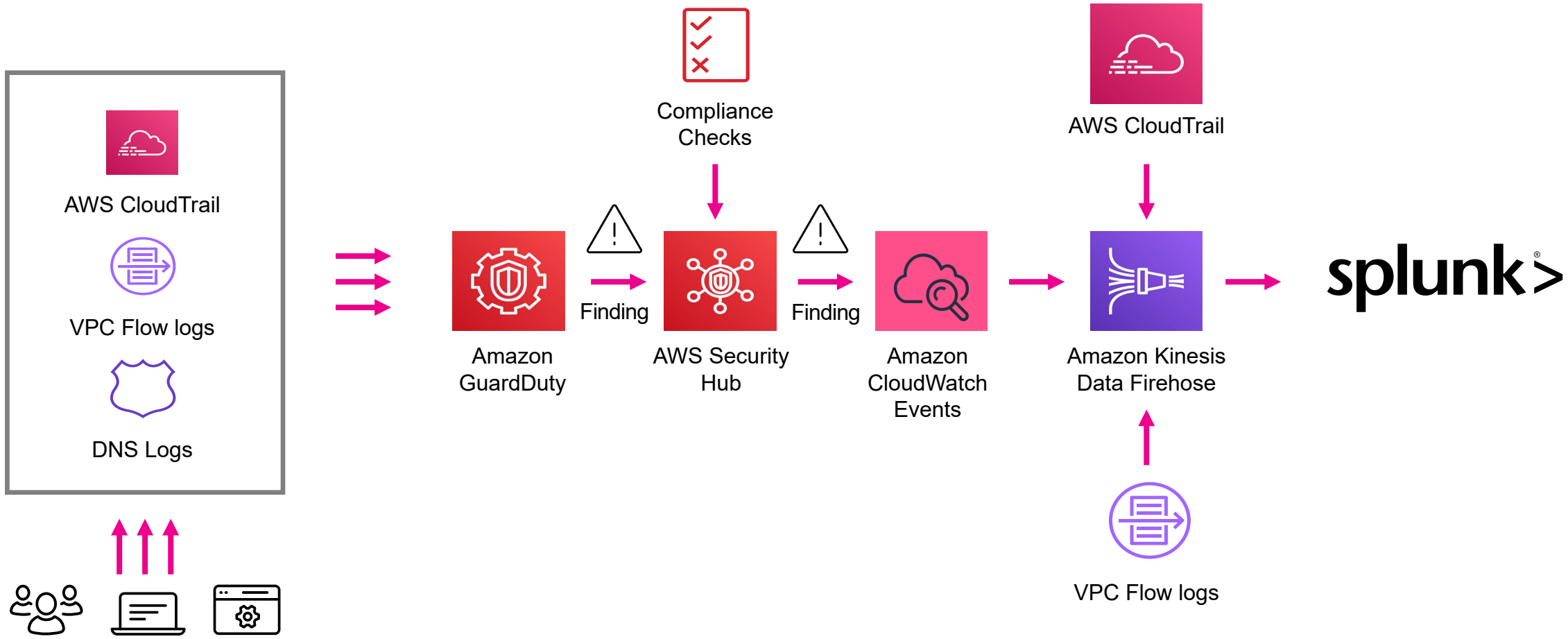
- What is out of compliance?
- How did I get out of compliance?
- How do I get back into compliance?
- How do I prevent this in the future?

.conf20

splunk>

Getting AWS Security Data into Splunk

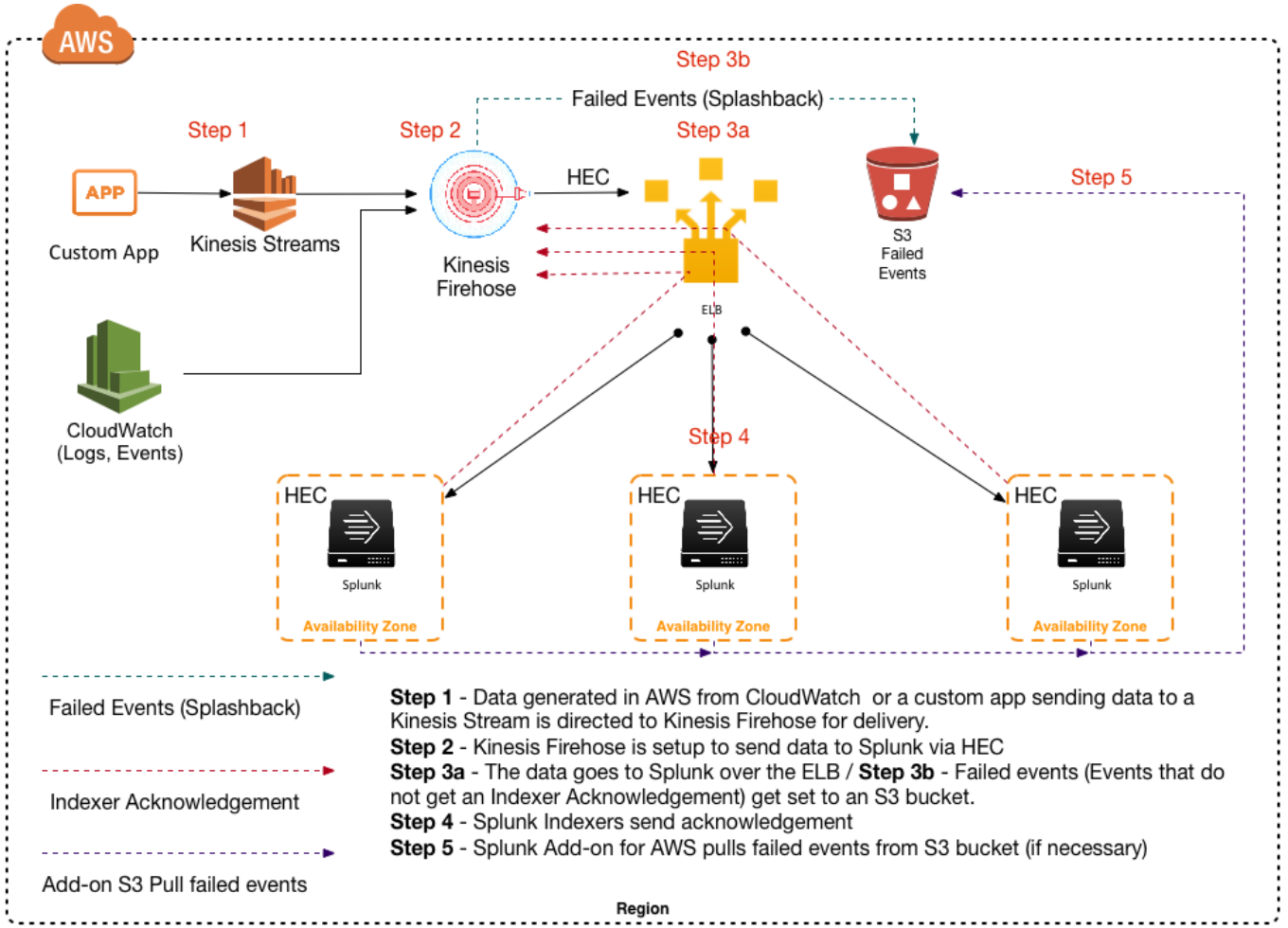
AWS Data Flow for Use Cases



Kinesis Data Firehose Benefits

Scalable architecture with event acknowledgement

- Push architecture allows for high volume data sent to Splunk without a forwarder
- Data stored in S3 if unable to send to Splunk
- Scales to large volume data sources, like CloudTrail, VPCFlow logs, Application Logs etc.
- Leverages Splunk HTTP Event Collector (HEC)
- Enables automation such as Project Grand Central
- Reduces complexity for data collection

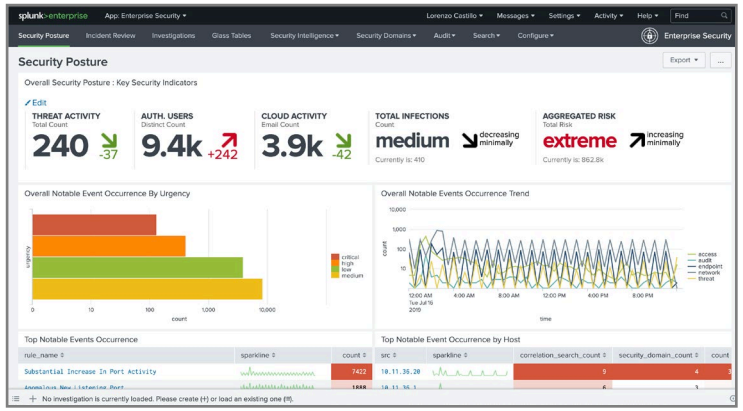


.conf20

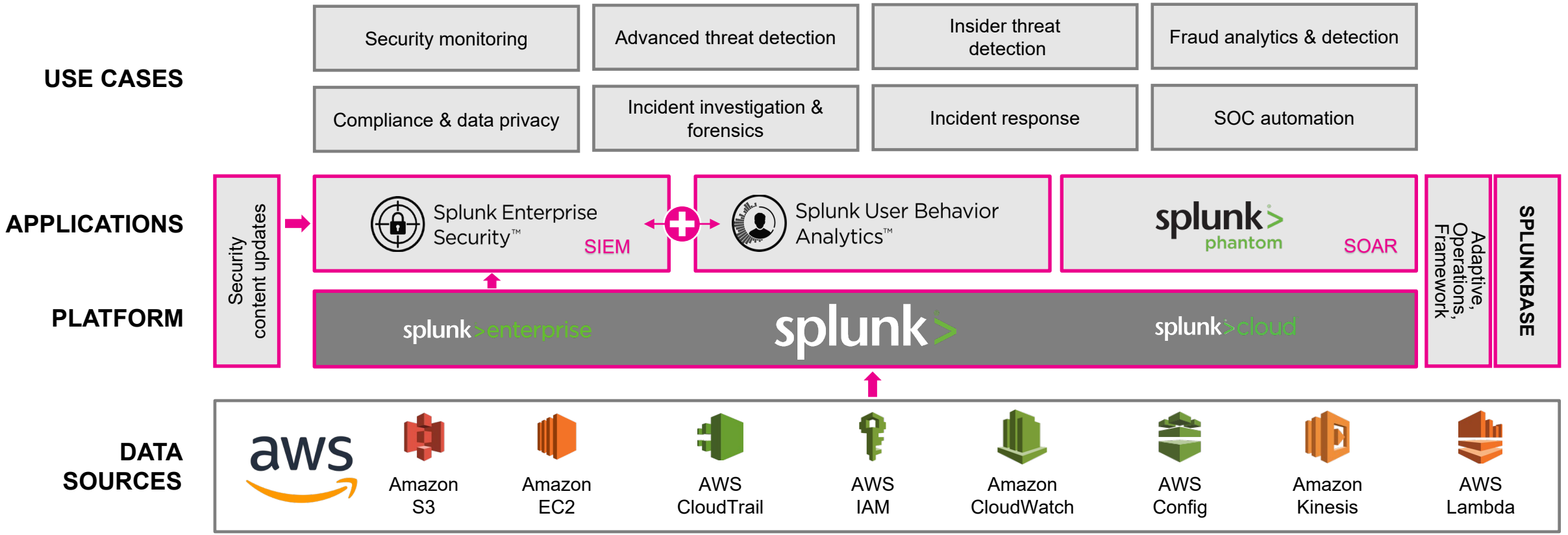
splunk>

Security posture of your AWS workloads

Detection and Investigation Use Cases



Splunk Security Operations Suite



Let's look first at some detection and investigation use cases with **AWS** and **Splunk Enterprise Security (SIEM)**

splunk> .conf20

Use Case 1: Account Protection

Essential data mapping and detection rules

AWS Data Source	Source type in Add-on	CIM Model	Detection in Splunk ES
CloudTrail	aws:cloudtrail aws:kinesis:firehose	Authentication Change Analysis	Any AWS Account Activity Notable in ES Use Case library ES Content Update pack
GuardDuty	aws:cloudwatch:guardduty	Alert Intrusion Detection	GuardDuty Finding as Notable Event in ES – common ones: UnauthorizedAccess:EC2/MaliciousIPCaller* UnauthorizedAccess:IAMUser/MaliciousIPCaller* Recon:IAMUser/MaliciousIPCaller Policy:IAMUser/RootCredentialUsage

Use Case 2: Defending Compute Resources

Essential data mapping and detection rules

AWS Data Source	Source type in Add-on	CIM Model	Detection in Splunk ES
VPCFlow logs	aws:cloudwatchlogs:vpcflow	Network_Traffic	Port Scanning activity Detect Spike in blocked Outbound Traffic from your AWS AWS Network Access Control List Created with All Open Ports
CloudTrail	aws:cloudtrail	Change Analysis	EC2 Instance Started In Previously Unseen Region EC2 Modified by Previously Unseen User All AWS activities from
GuardDuty	aws:guardduty	Alert Intrusion Detection	GuardDuty Finding – common rules: Recon:EC2/Portscan UnauthorizedAccess:EC2/SSHBruteForce Trojan:EC2/DNSDataExfiltration Backdoor:EC2/C&CActivity.B!DNS CryptoCurrency:EC2/BitcoinTool.B!DNS

Use Case 3: Maintaining Compliance

Essential data mapping and detection rules

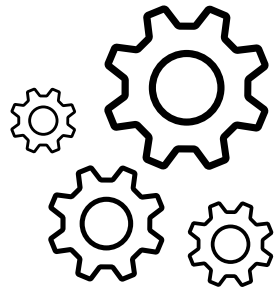
AWS Data Source	Source type in Add-on	CIM Model*	Detection in Splunk ES
SecurityHub	aws:securityhub*	Alert Inventory Change	SecHub Findings based on 1. CIS AWS Foundations Benchmark controls – e.g. Password policies Security Groups controls 2. PCI DSS 3. Data Protection controls 4. Secure network configs
CloudTrail	aws:cloudtrail	Change Authentication	S3 Bucket Exposed EC2 Instance changes Asset Ownership unspecified High Number of Hosts Unpatched
Config Rules	aws:config:rules	Alerts	ES Investigation Support

.conf20

splunk>

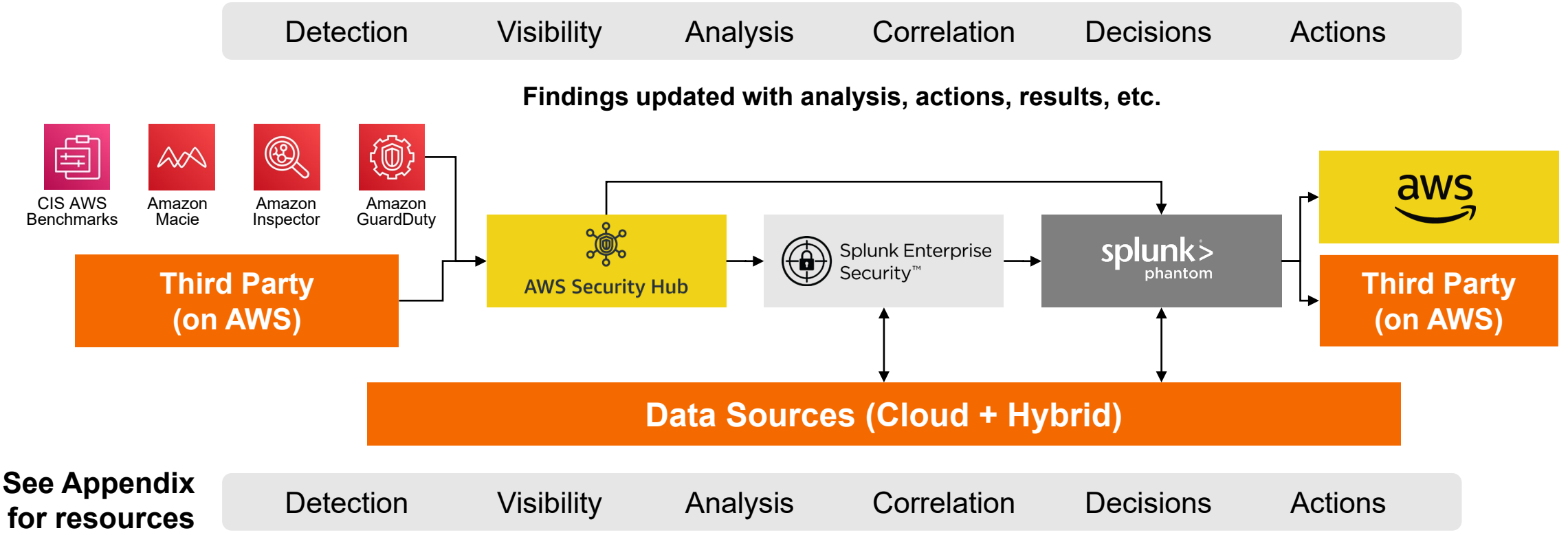
Automated Threat Mitigation

Automated decision making and response with AWS and Splunk



Automated Cloud Security Incident Response

End-to-End SecOps By Combining AWS Services with Splunk ES/SIEM and Phantom/SOAR



splunk> .conf20

Cloud SOAR Use Case

Automated Response in Splunk Phantom to a SecurityHub finding

Observe

1

AWS SecurityHub

- SecHub detects potential threat with an exposed **EC2 instance**
- SecHub **triggers a findings** as a CloudWatch event
- Cloudwatch event rule forwards the findings to an SQS Queue
- **Phantom App for SecurityHub** collects events from SQS Queue

Decide

2

Playbook: EC2 Instance Investigation

- Automated steps to **gather**:
  - Finding **risk level** and **details**
  - EC2 instance **configuration**
  - Host activity
- Get connections probing instance
  - Check IP reputation
  - Check Geolocation
- Create **service ticket**
- Send a **Slack message**
  - Notify security team

Act

3

Playbook: Instance Isolation

- Automated step to:
- Add instance to an **isolated security group**

splunk> .conf20

Key Takeaways

1) Understand key security-relevant data in AWS services

2) Become familiar with getting AWS data into Splunk

3) Use cases to detect and investigate key cloud threats

4) Cloud incident automation uses cases

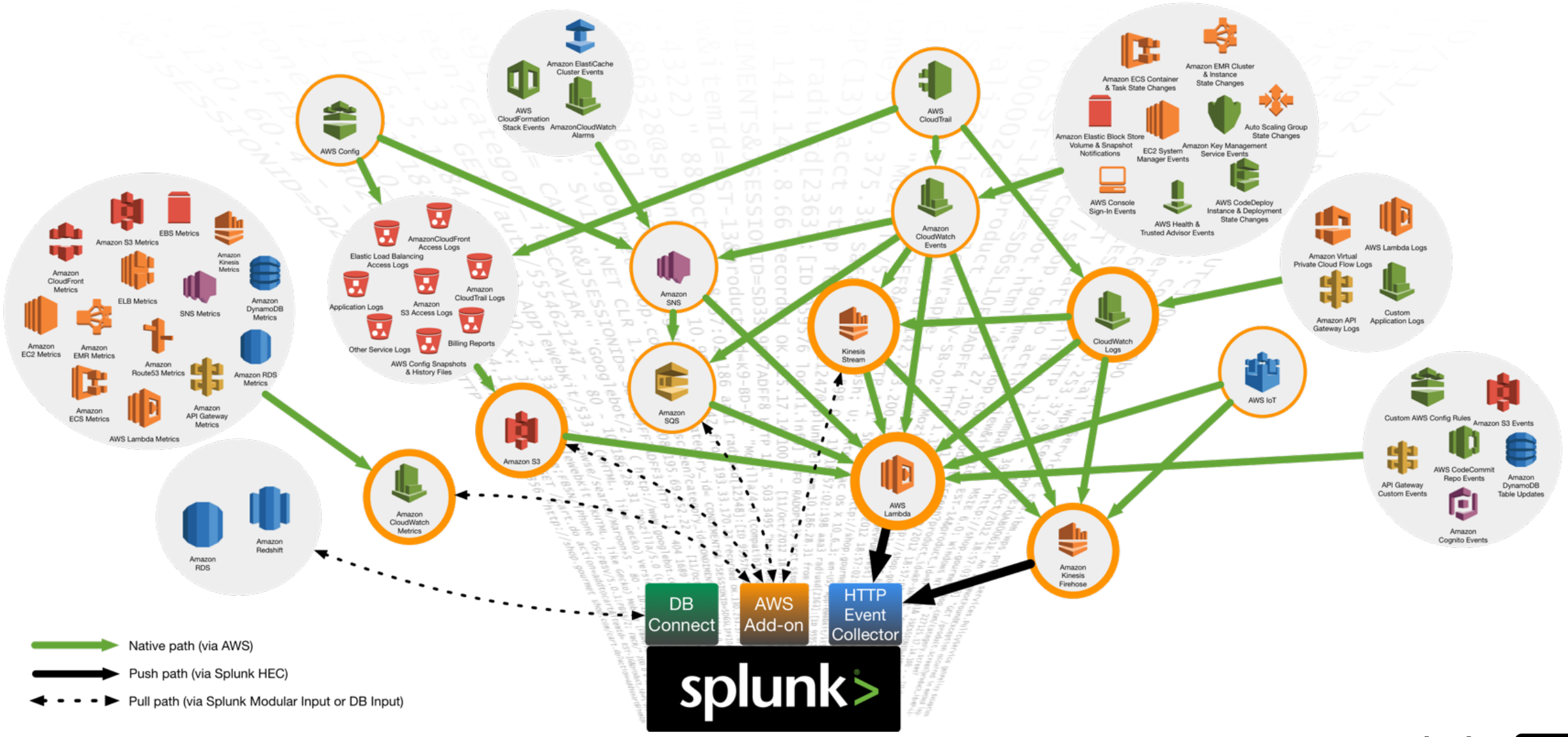
Thank You

Please provide feedback via the

SESSION SURVEY

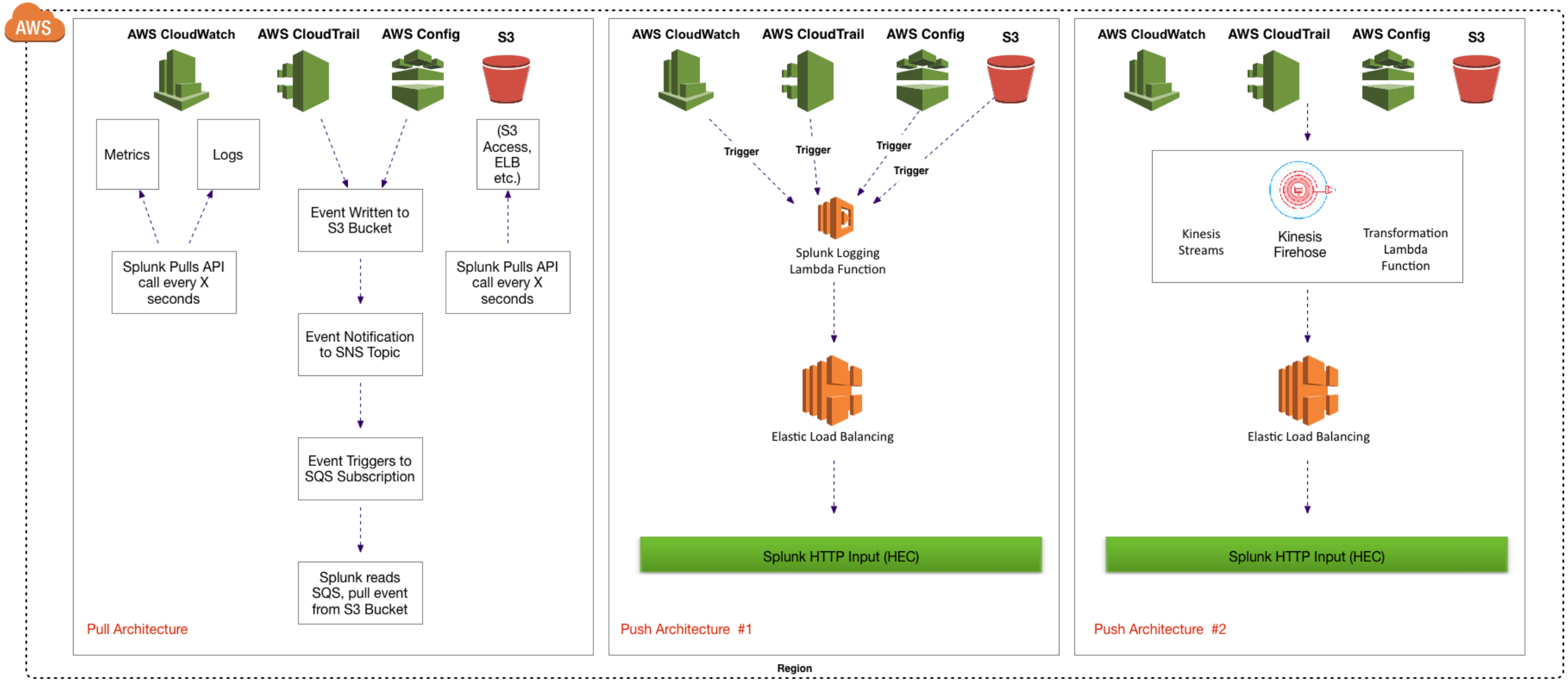
Appendix

End State: Comprehensive AWS Visibility



splunk> .conf20

Integrating AWS with Splunk



AWS reference content

AWS Security: https://aws.amazon.com/security/

AWS Security Services: https://aws.amazon.com/products/security/?nc=sn&loc=2

AWS Incident Response Whitepaper: https://d1.awsstatic.com/whitepapers/aws_security_incident_response.pdf

AWS Security Whitepapers: https://aws.amazon.com/whitepapers/

AWS Security Workshops: https://awssecworkshops.com/

Essential Splunk Apps & Add-ons for AWS

Splunk Add-on for Amazon Web

11624 Installs

Splunk Add-on for Amazon Kinesis

5643 Installs

Splunk App for AWS

6932 Installs

https://splunkbase.splunk.com/apps/#/search/aws/

App for AWS Billing

29 Installs

Amazon AWS SQS Monitoring

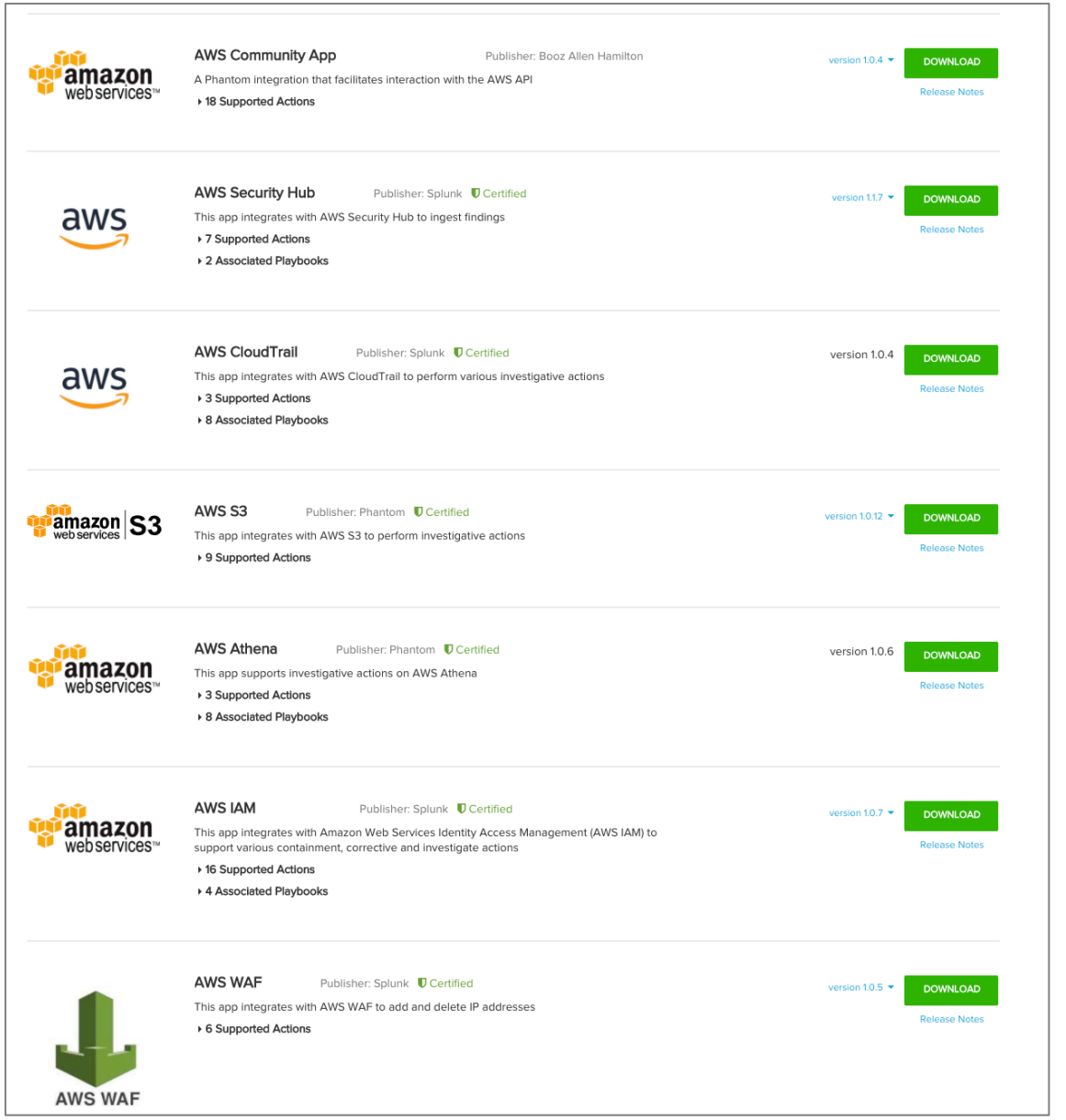
16 Installs

AWS Web Application Firewall

408 Installs

AWS Apps for Phantom

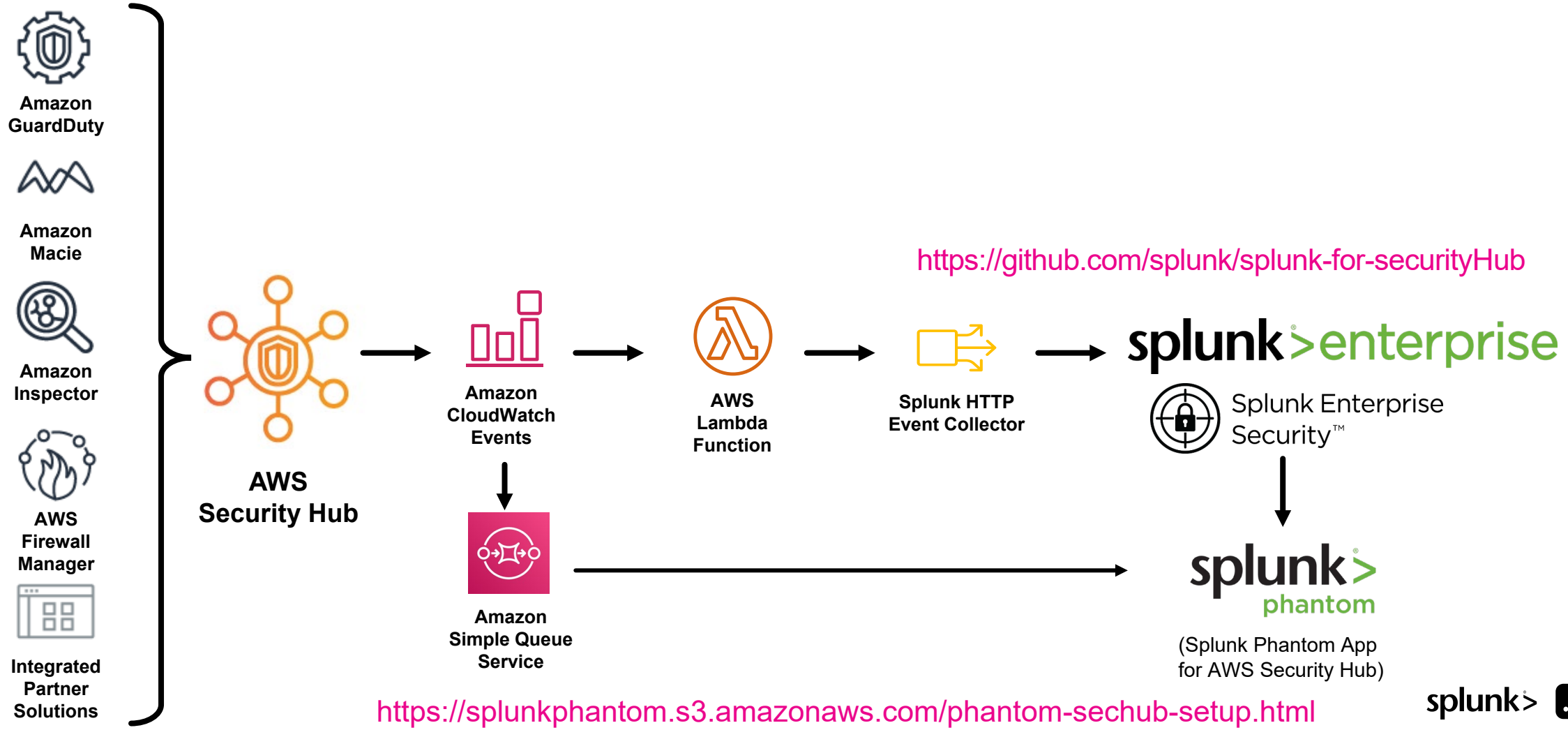
my.phantom.us/apps



splunk> .conf20

Splunk + AWS Security Hub

Investigate findings and/or respond with remediation actions



https://github.com/splunk/splunk-for-securityHub

https://splunkphantom.s3.amazonaws.com/phantom-sechub-setup.html