Tackle AWS Security Automatically with Phantom

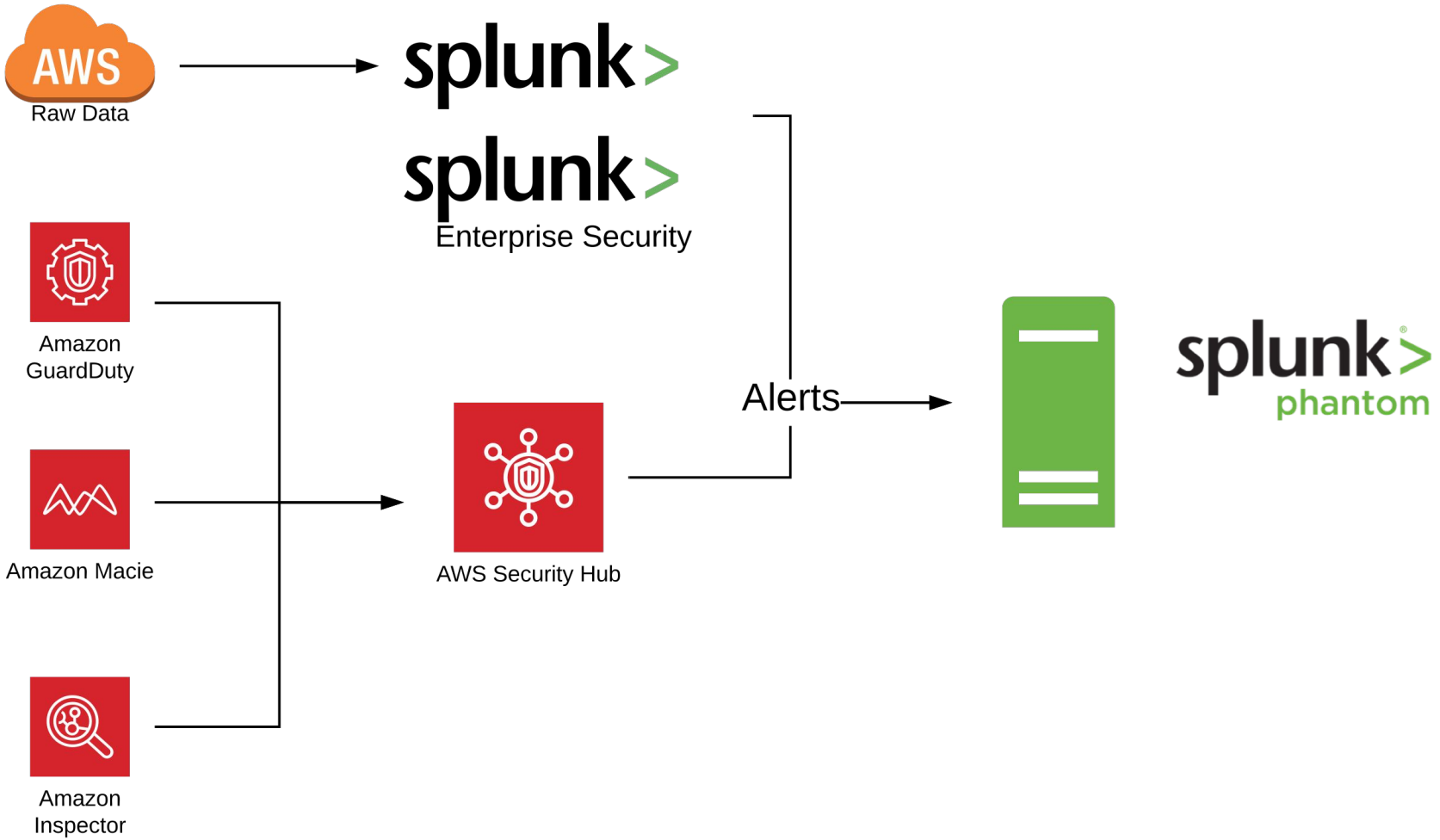
Matt Tichenor
Product Manager | Splunk

splunk> .conf19

> We also offer detection services that add another layer our customers can deploy to protect their resources.
>
> …We have a service called Macie that automatically classifies data into different buckets of sensitivity, and then **sends customers alarms…**
>
> …We have a service called GuardDuty that **alerts customers** when there are unusual Application Programming Interface (API) calls…

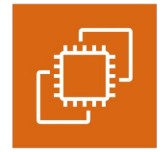
AWS Response to Senator Ron Wyden | August 13 2019

AWS Intel Sources



Responding to AWS Alerts

splunk> phantom



Amazon EC2

Amazon Simple Storage Service (S3)

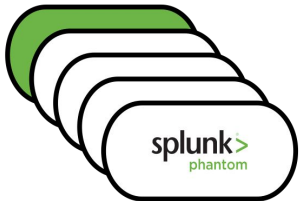
Amazon Athena

AWS Lambda

AWS Identity and Access Management (IAM)

AWS Systems Manager

AWS WAF



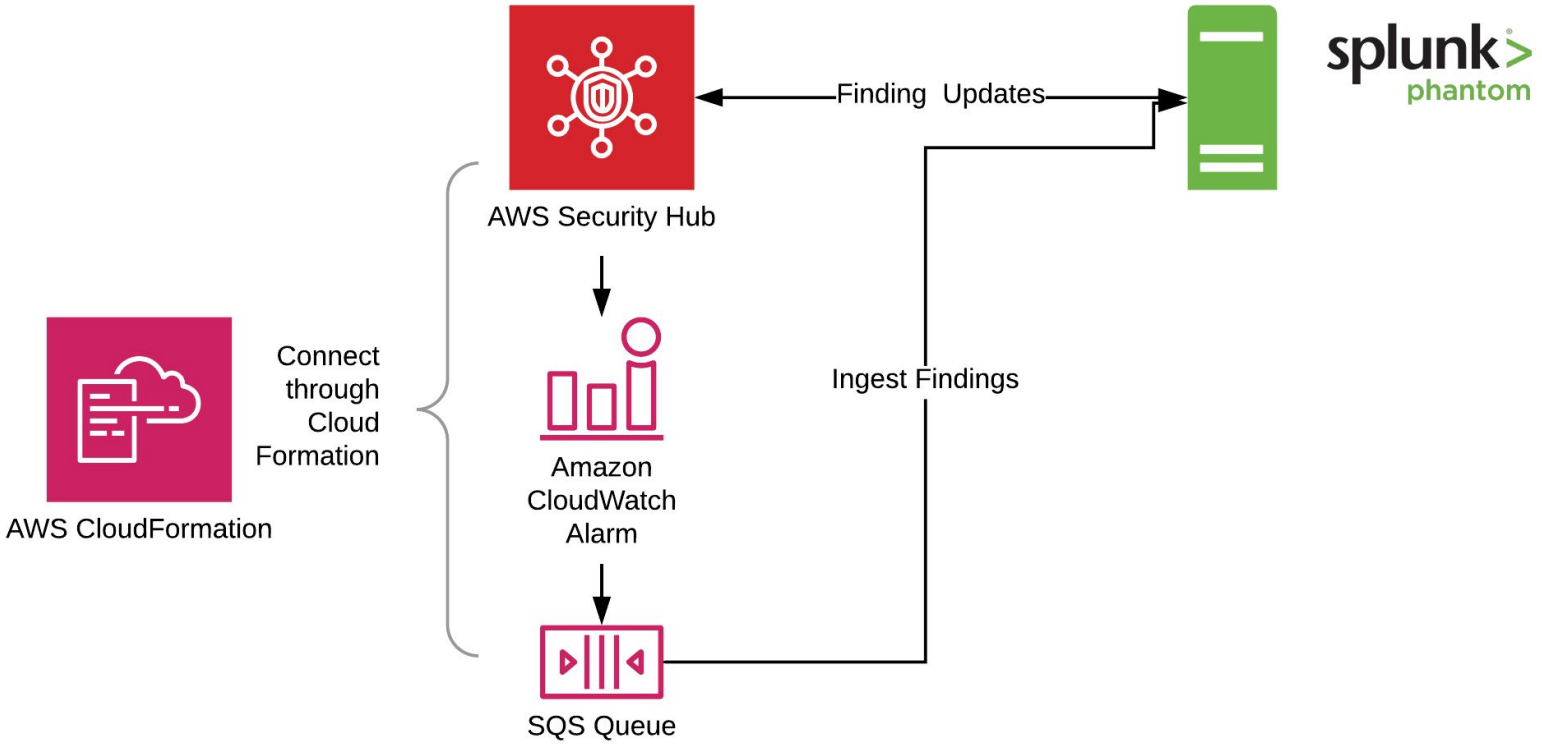
300+ Phantom Apps

splunk> .conf19

DEMO

Getting AWS Alerts into Phantom

https://splunk
/phantom-se



EC2 Investigation

☐	MEDIUM	Personal	Default	Unprotected port on EC2 instance i-0231c5ce402c67748 is being probed.	arn:aws:ec2:us-east-1:149665393462:instance/i-0231c5ce402c67748	AwsEc2Instance
☐	MEDIUM	Personal	Default	Unprotected port on EC2 instance i-0231c5ce402c67748 is being probed.	arn:aws:ec2:us-east-1:149665393462:instance/i-0231c5ce402c67748	AwsEc2Instance
☐	MEDIUM	Amazon	GuardDuty	103.255.216.166 is performing SSH brute force attacks against i-0839e15e1ae0b768c.	arn:aws:ec2:us-east-1:149665393462:instance/i-0839e15e1ae0b768c	AwsEc2Instance
☐	MEDIUM	Amazon	GuardDuty	117.27.151.104 is performing SSH brute force attacks against i-0839e15e1ae0b768c.	arn:aws:ec2:us-east-1:149665393462:instance/i-0839e15e1ae0b768c	AwsEc2Instance

EC2 Alert Response Ideas

Investigate

- geolocate ip
- determine risk level of device
- contact resource owners
- list ssh sessions

Respond - Soft Touch

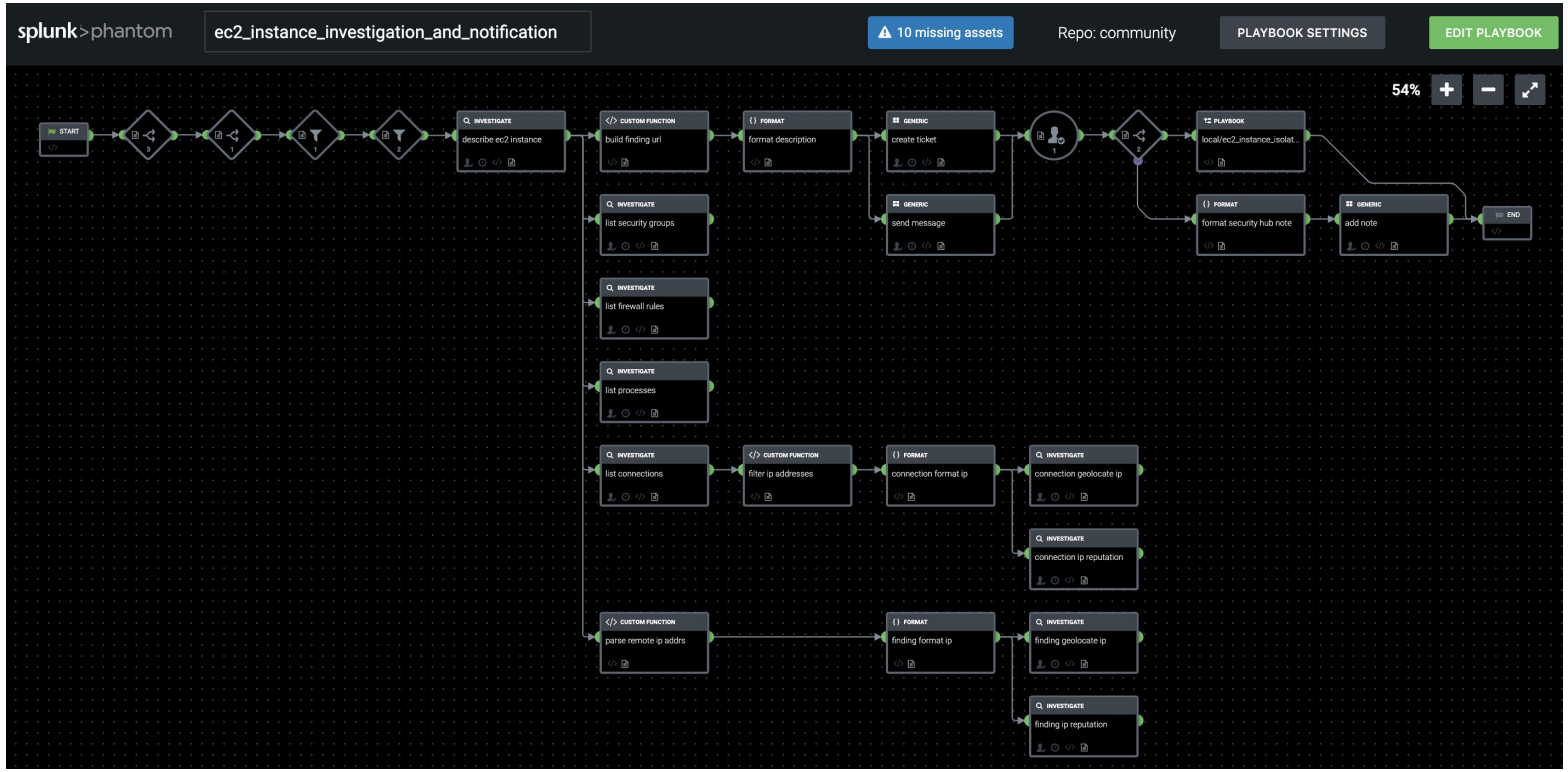
- File a ticket to resource owner
- Start a Slack chat with Security Team & Resource Owner

Respond - Hammer

- Quarantine Security Group
- Stop Device
- Kill Process

DEMO

Investigating an EC2 Alert



splunk> .conf19

Other Phantom Playbook Ideas

IAM Alerts

- Account created with excessive permissions
- Attempt to compromise account credentials
- Account login from new location

Sensitive Data Access

- Unusual Activity in S3
- PII uploaded to Public S3 Bucket

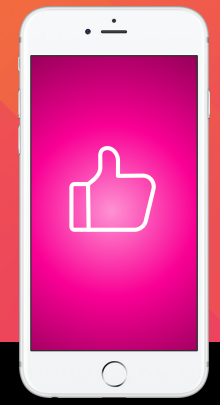
.conf19

splunk>

Thank You !

Go to the .conf19 mobile app to

RATE THIS SESSION



ATT&CK

Last Modified: 2019-07-01 17:29:19.726000

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	Command-Line Interface	.bash_profile and .bashrc	Exploitation for Privilege Escalation	Binary Padding	Bash History	Account Discovery	Application Deployment Software	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	Exploitation for Client Execution	Bootkit	Process Injection	Clear Command History	Brute Force	Browser Bookmark Discovery	Exploitation of Remote Services	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
Hardware Additions	Graphical User Interface	Browser Extensions	Setuid and Setgid	Compile After Delivery	Credential Dumping	File and Directory Discovery	Remote File Copy	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Spearphishing Attachment	Local Job Scheduling	Create Account	Sudo	Disabling Security Tools	Credentials in Files	Network Service Scanning	Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Spearphishing Link	Scripting	Hidden Files and Directories	Sudo Caching	Execution Guardrails	Exploitation for Credential Access	Network Sniffing	SSH Hijacking	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Spearphishing via Service	Source	Kernel Modules and Extensions	Valid Accounts	Exploitation for Defense Evasion	Input Capture	Password Policy Discovery	Third-party Software	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Endpoint Denial of Service
Supply Chain Compromise	Space after Filename	Local Job Scheduling	Web Shell	File Deletion	Network Sniffing	Permission Groups Discovery		Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Firmware Corruption
Trusted Relationship	Third-party Software	Port Knocking		File Permissions Modification	Private Keys	Process Discovery		Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Inhibit System Recovery
Valid Accounts	Trap	Redundant Access		Hidden Files and Directories	Two-Factor Authentication Interception	Remote System Discovery		Input Capture	Domain Generation Algorithms	Scheduled Transfer	Network Denial of Service
						System					