# How to Improve Threat Detection and Hunting in the AWS Cloud Using the MITRE ATT&CK® Matrix

Sponsored by

aws marketplace

# Today's Speakers

- Dave Shackleford – SANS Analyst
- Ross Warren - Specialist Solution Architect at AWS

# Today's Agenda

- Introduction to TTPs and Threat Detection
- The MITRE ATT&CK Cloud Matrix
- Detection and Threat Hunting: Logging and Event Analysis
- Cloud-Native Options for Threat Detection
- Integrating Automation and SOAR
- A TTP Detection, Analysis and Response Case Study
- Solutions in AWS Marketplace
- Customer Success Stories

# Moving from IOCs to TTPs

- As more organizations build cloud infrastructure, attackers are taking notice. Can IOCs help?
- TTPs are more useful! Attackers *do* leave traces and exhibit recognizable patterns in many attacks. TTPs focus on:
  - **Tactics—**Tactics describe an overall approach to compromise.
  - **Techniques—**Techniques describe the specific and unique ways each phase of an attack is executed.
  - **Procedures—**Procedures describe a combination of varied approaches taken in both techniques and overall tactics.

*The views and opinions of the SANS Institute and their presenter, Dave Shackleford, are their own, and do not necessarily reflect the positions of AWS or AWS Marketplace.

# Cloud Threats and Security Challenges

Analyst Program

- To improve the state of security monitoring and response in the cloud, SOC teams should:
  - Perform more proactive threat hunting.
  - Rapidly investigate systems in cloud environments.
  - Assess workload and identity state and attributes quickly for response and investigation.
  - Rapidly align numerous cloud events to detect TTPs.
  - Adopt SOAR platforms and workflows to improve response efficiency and effectiveness.

*The views and opinions of the SANS Institute and their presenter, Dave Shackleford, are their own, and do not necessarily reflect the positions of AWS or AWS Marketplace.

# The MITRE ATT&CK Cloud Matrix

- The team at MITRE has updated and adapted its ATT&CK (Adversarial Tactics, Techniques and Common Knowledge) framework for cloud.
  - ATT&CK focuses on the tactics, techniques and procedures (TTPs) commonly used against enterprise environments.
- ATT&CK focuses on:
  - Adversary behaviors
  - Life-cycle models for attacks
  - Real-world attack applicability
  - Common attack taxonomy and nomenclature

*The views and opinions of the SANS Institute and their presenter, Dave Shackleford, are their own, and do not necessarily reflect the positions of AWS or AWS Marketplace.

# The MITRE ATT&CK Cloud Matrix

| Initial Access | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Collection | Exfiltration | Impact |
|---|---|---|---|---|---|---|---|---|
| Drive-by Compromise | Account Manipulation | Valid Accounts | Impair Defenses | Brute Force | Account Discovery | Data from Cloud Storage Object | Transfer Data to Cloud Account | Defacement |
| Exploit Public-Facing Application | Create Account | | Modify Cloud Compute Infrastructure | Steal Application Access Token | Cloud Service Dashboard | Data from Information Repositories | | Endpoint Denial of Service |
| Phishing | Implant Container Image | | Unused/ Unsupported Cloud Regions | Steal Web Session Cookie | Cloud Service Discovery | Data Staged | | Network Denial of Service |
| Trust Relationship | Office Application Startup | | Use Alternate Authentication Material | Unsecured Credentials | Network Service Scanning | Email Collection | | Resource Hijacking |
| Valid Accounts | Valid Accounts | | Valid Accounts | | Network Share Discovery | | | |
| | | | | | Permission Groups Discovery | | | |
| | | | | | Remote System Discovery | | | |
| | | | | | Software Discovery | | | |
| | | | | | System Information Directory | | | |
| | | | | | System Network Connections Discovery | | | |

Source: Adapted from https://attack.mitre.org/matrices/enterprise/cloud

*The views and opinions of the SANS Institute and their presenter, Dave Shackleford, are their own, and do not necessarily reflect the positions of AWS or AWS Marketplace.

# The MITRE ATT&CK Cloud Matrix: Initial Access

Analyst Program

- Initial access phase occurs when an initial means of ingress into cloud accounts or resources is found.
- Common methods to accomplish this include:
  - Exploiting public-facing applications
  - Discovering and exploiting trusted relationships
  - Discovering valid accounts to cloud environments

*The views and opinions of the SANS Institute and their presenter, Dave Shackleford, are their own, and do not necessarily reflect the positions of AWS or AWS Marketplace.

# The MITRE ATT&CK Cloud Matrix: Persistence

Analyst Program

- The persistence phase is where an attacker seeks to stage a foothold in the victim's environment to ensure they can return at will.
- Within a newly compromised cloud environment or asset, an attacker may use the following tactics:
  - Using account manipulation to grant later or ongoing access
  - Creating new accounts
  - Implanting container images for PaaS environments
  - Creating redundant access with network and identity controls
  - Continuing to leverage valid accounts

*The views and opinions of the SANS Institute and their presenter, Dave Shackleford, are their own, and do not necessarily reflect the positions of AWS or AWS Marketplace.

# The MITRE ATT&CK Cloud Matrix: Privilege Escalation

Analyst Program

- Escalating privileges is a common goal for many attackers once they've initially breached the environment.
- In a cloud setting, the most common method of privilege escalation is to:
  - Attempt access with, or to, *valid accounts* within the environment, *or*
  - Manipulate identity role assignment to then use these valid accounts.

*The views and opinions of the SANS Institute and their presenter, Dave Shackleford, are their own, and do not necessarily reflect the positions of AWS or AWS Marketplace.

# The MITRE ATT&CK Cloud Matrix: Defense Evasion

Analyst Program

- Once an attacker has gained access to a cloud account or environment, they will seek to avoid defenses.
- Common ways that attackers may seek to avoid defenses in a cloud environment include:
  - Avoiding detection via redundant access
  - Reverting cloud instances to a previous state
  - Establishing a presence in unused/unsupported cloud regions
  - Continuing to leverage valid accounts

*The views and opinions of the SANS Institute and their presenter, Dave Shackleford, are their own, and do not necessarily reflect the positions of AWS or AWS Marketplace.

# The MITRE ATT&CK Cloud Matrix: Credential Access



- One of the most common ways an attacker can advance in a focused campaign is by accessing and using varied types of cloud account and asset credentials.
- Several well-known types of credential access attackers attempt in the cloud include:
  - Using account manipulation to access credentials
  - Querying an identity role with a cloud instance's metadata API
  - Discovering credentials in files

*The views and opinions of the SANS Institute and their presenter, Dave Shackleford, are their own, and do not necessarily reflect the positions of AWS or AWS Marketplace.

# The MITRE ATT&CK Cloud Matrix: Discovery



- Attackers will focus on asset and service discovery, including:
  - Cloud service dashboards
  - Cloud service discovery (through network visibility, interaction with other services, and so on)
  - Network service scanning
  - Network share discovery
  - Remote system discovery
  - System information discovery
  - System network connection discovery


*The views and opinions of the SANS Institute and their presenter, Dave Shackleford, are their own, and do not necessarily reflect the positions of AWS or AWS Marketplace.

# The MITRE ATT&CK Cloud Matrix: Collection



- The goal of many attackers is to access and collect data and other assets of value. Their top focal areas are likely to include:
  - Data from cloud storage objects (e.g., items in S3 buckets)
  - Data from other cloud information repositories (databases or big data warehouses)
  - Data from local systems
  - Data staged in application scenarios

# The MITRE ATT&CK Cloud Matrix: Exfiltration



- Once an attacker has gained access to data, many attack campaigns lead to eventual exfiltration of data to a location under the attacker's control.
- In the ATT&CK framework, this is accomplished via the act of *transferring data to a cloud account*.
- Savvy attackers do this gradually and somewhat slowly to avoid detection of large, sudden data transfers.

# The MITRE ATT&CK Cloud Matrix: Impact

Analyst Program

- The final potential “stage” of the ATT&CK framework is eventual cloud service impact, which the current model categorizes as *resource hijacking*.

*The views and opinions of the SANS Institute and their presenter, Dave Shackleford, are their own, and do not necessarily reflect the positions of AWS or AWS Marketplace.

# Detection and Threat Hunting: Logging and Event Analysis

Analyst Program

- The first thing security analysts need to do is collect logs from all relevant cloud service environment systems and workloads.
- Second, the cloud service environment can also track events occurring across the infrastructure of the cloud platform itself, which security teams can monitor for unusual or suspicious activity.

*The views and opinions of the SANS Institute and their presenter, Dave Shackleford, are their own, and do not necessarily reflect the positions of AWS or AWS Marketplace.

# Detection and Threat Hunting: Logging and Event Analysis

Analyst Program

- An excellent example of a cloud control plane logging engine is AWS CloudTrail.
  - AWS CloudTrail generates cloud service event data that can feed log management and SIEM platforms already in use.
- SOC teams should also collect network monitoring patterns with network flow data, primarily for monitoring communications to, from and between workloads within VPCs.
  - Amazon VPC Flow Logs can be used to monitor and track network events and behaviors at a large scale.

*The views and opinions of the SANS Institute and their presenter, Dave Shackleford, are their own, and do not necessarily reflect the positions of AWS or AWS Marketplace.

# Detection and Threat Hunting: Logging and Event Analysis

Analyst Program

- Some interesting log/event examples that all security teams should initially focus on:
  - **Billing alarms—**If you have a reasonable idea of a monthly billing range, you can break this down to define “checkpoints” that your bill should be at any given time. If these thresholds are crossed, you can be alerted and investigate what is causing the additional cost. Tools like AWS Budgets provide simple alerting and reporting for cloud billing.
  - **IAM activity (logins, in particular)—**Monitor your user activity within the cloud.
  - **Cloud environment logs—**General API logs can tell you when workloads are created or changed, when storage attributes change, and so on.

*The views and opinions of the SANS Institute and their presenter, Dave Shackleford, are their own, and do not necessarily reflect the positions of AWS or AWS Marketplace.

# Cloud-Native Options for Threat Detection

Analyst Program

- **Cloud Security Analytics**
  - Amazon GuardDuty is a powerful security analytics service that analyzes a vast volume of log and intelligence data.
- **VPC Traffic Mirroring**
  - Amazon VPC Traffic Mirroring permits network traffic to be copied from any compatible system in a VPC to a suitable endpoint.

*The views and opinions of the SANS Institute and their presenter, Dave Shackleford, are their own, and do not necessarily reflect the positions of AWS or AWS Marketplace.

# Cloud-Native Options for Threat Detection

Analyst Program

- **Security data aggregation and analysis**
  - Amazon Detective is a service that collects and aggregates logs across AWS resources and performs deep analysis on them to detect behavior anomalies and other events for faster and more efficient root cause analysis and threat hunting investigations.
- **Continuous monitoring**
  - AWS Security Hub offers basic continuous monitoring for AWS accounts by looking at CIS Benchmarks configuration checks (www.cisecurity.org/cis-benchmarks), AWS security best practices, and more.

*The views and opinions of the SANS Institute and their presenter, Dave Shackleford, are their own, and do not necessarily reflect the positions of AWS or AWS Marketplace.

# Integrating Automation and SOAR

Analyst Program

- Common activities that many teams consider for automation include:
  - Identifying and correlating alerts
  - Identifying and suppressing false positives
  - Performing initial investigation and threat hunting
  - Opening and updating incident tickets/cases
  - Producing reports and metrics

*The views and opinions of the SANS Institute and their presenter, Dave Shackleford, are their own, and do not necessarily reflect the positions of AWS or AWS Marketplace.

# Integrating Automation and SOAR



- Examples of security response automation include:
  - Automated DNS lookups of domain names never seen before
  - Automated searches for detected IOCs and TTP elements
  - Automated forensic imaging of disk and memory from a suspect system, driven by alerts triggered in network- and host-based anti-malware platforms and tools
  - Network access controls automatically blocking outbound command-and-control (C2) channels from a suspected system based on known TTP behaviors

# A TTP Detection, Analysis and Response Case Study

Analyst Program

| Attack Phase | TTP Elements |
|---|---|
| Initial Access | Discovering valid accounts to cloud environments |
| Persistence | Creating new accounts |
| Defense Evasion | Establishing a presence in unused/unsupported cloud regions<br>Continuing to leverage valid accounts |
| Credential Access | Querying an identity role with a cloud instance's metadata API<br>Discovering credentials in files |
| Discovery | Cloud service discovery (through network visibility, interaction with other services, and so on)<br>System information discovery<br>System network connection discovery |
| Collection | Data from cloud storage objects (items in S3 buckets, for example)<br>Data from local systems |
| Exfiltration | Outbound data to a cloud storage account elsewhere |

*The views and opinions of the SANS Institute and their presenter, Dave Shackleford, are their own, and do not necessarily reflect the positions of AWS or AWS Marketplace.

# A TTP Detection, Analysis and Response Case Study (Slide 1 of 2)

Analyst Program

| Attack Phase | TTP Elements | Detection/Response Controls |
|---|---|---|
| Initial Access | Discovering valid accounts to cloud environments | AWS CloudTrail event: Account login via AWS CLI or AWS Management Console (IAM account) |
| Persistence | Creating new accounts | AWS CloudTrail event: New IAM account created |
| Defense Evasion | Establishing a presence in unused/unsupported cloud regions | AWS CloudTrail event represented in Amazon GuardDuty or Amazon Detective: New API event in a previously unused region |
| | Continuing to leverage valid accounts | AWS CloudTrail event represented in Amazon GuardDuty or Amazon Detective: Account use in new region |
| Credential Access | Querying an identity role with a cloud instance's metadata API | AWS CloudTrail event represented in Amazon GuardDuty, third-party SIEM or Amazon Detective: Metadata service queried for new services and role permissions |
| | Discovering credentials in files | AWS CloudTrail event: Account login via AWS CLI or AWS Management Console |

*The views and opinions of the SANS Institute and their presenter, Dave Shackleford, are their own, and do not necessarily reflect the positions of AWS or AWS Marketplace.

# A TTP Detection, Analysis and Response Case Study (Slide 2 of 2)

Analyst Program

| Attack Phase | TTP Elements | Detection/Response Controls |
|---|---|---|
| **Discovery** | Cloud service discovery (through network visibility, interaction with other services, and so on) | Amazon GuardDuty event showing network or service scanning/interaction |
| | System information discovery | Local syslog or Windows event logs sent to SIEM or Amazon CloudWatch Logs |
| | System network connection discovery | Amazon GuardDuty event showing network or service scanning/interaction |
| **Collection** | Data from cloud storage objects (items in S3 buckets, for example) | AWS CloudTrail event: Account access to S3 attempting API requests like GetObject |
| | Data from local systems | Local syslog or Windows event logs sent to SIEM or Amazon CloudWatch Logs showing local data access and manipulation |
| **Exfiltration** | Outbound data to a cloud storage account elsewhere | Amazon VPC Flow Logs showing access to an external IP address or Amazon GuardDuty events showing numerous interactions with an external IP/domain |

*The views and opinions of the SANS Institute and their presenter, Dave Shackleford, are their own, and do not necessarily reflect the positions of AWS or AWS Marketplace.

# Next Steps

- To successfully build TTP detection capabilities in the cloud, SOC teams should follow these steps:

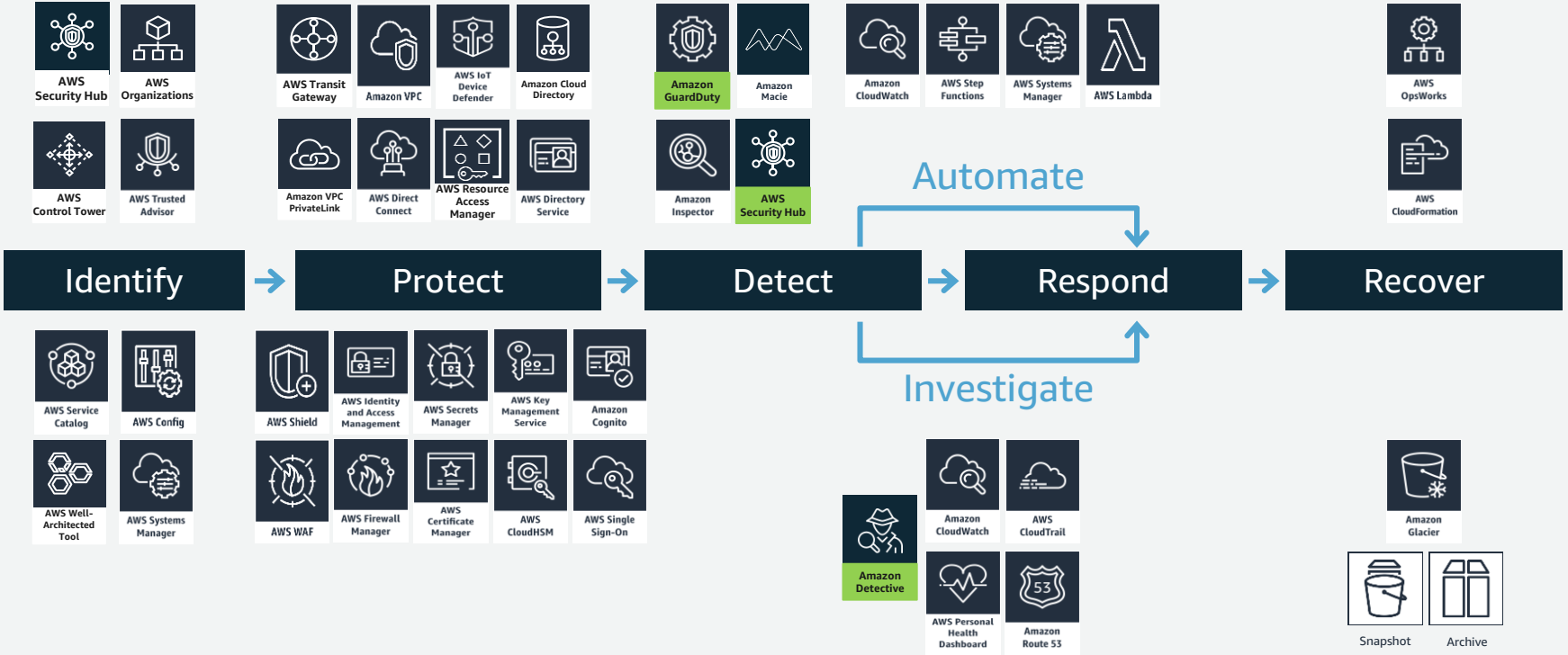
1. Use the MITRE ATT&CK Matrix for Cloud to build chained TTP scenarios in the AWS environment.
2. For each TTP technique or procedure, evaluate the exact events that would occur in AWS CloudTrail and determine the specific defensive services or tools that would capture them.
3. Analyze each event in conjunction with prior events and subsequent events to build a pattern of behavior that constitutes a legitimate TTP, versus singular IOCs.
4. Build automated alerting and response functions with AWS Lambda or other services that correspond to the different attack scenarios.
5. Ensure the SOC team has access to a practice account where they can generate these TTPs and test them independently, possibly through red/purple team testing scenarios.

*The views and opinions of the SANS Institute and their presenter, Dave Shackleford, are their own, and do not necessarily reflect the positions of AWS or AWS Marketplace.

aws marketplace

# Improving threat detection and hunting in AWS

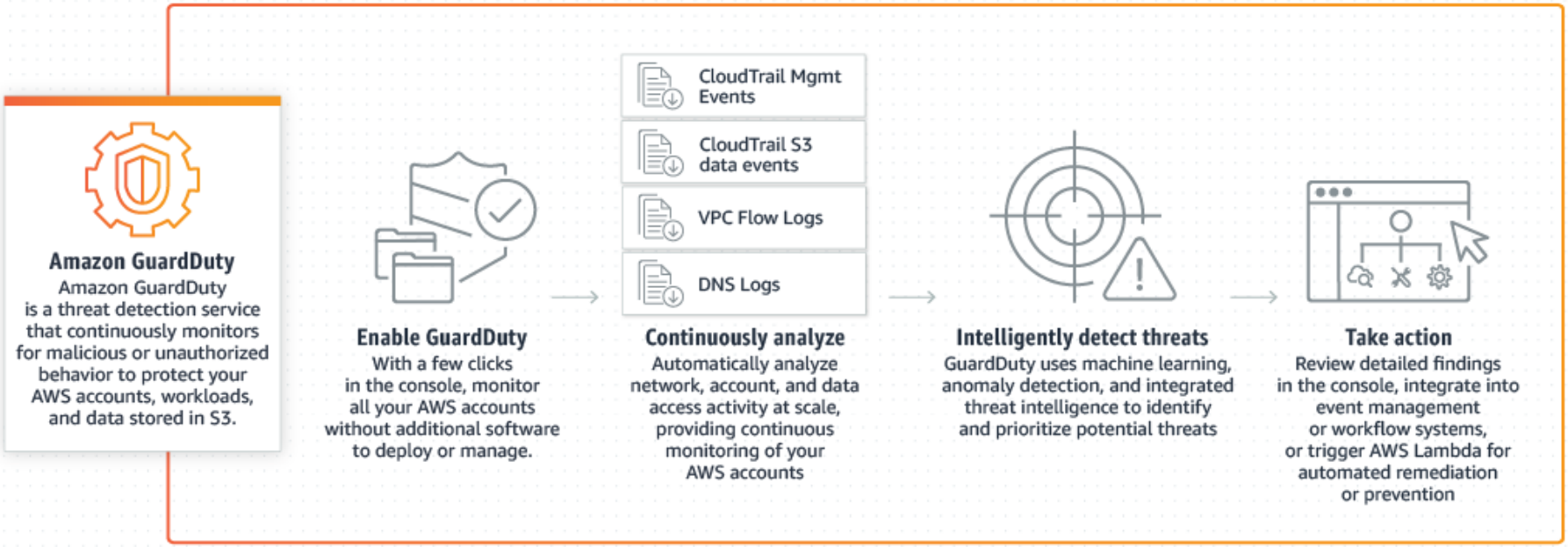
# AWS services that help improve threat detection and hunting






aws | aws marketplace

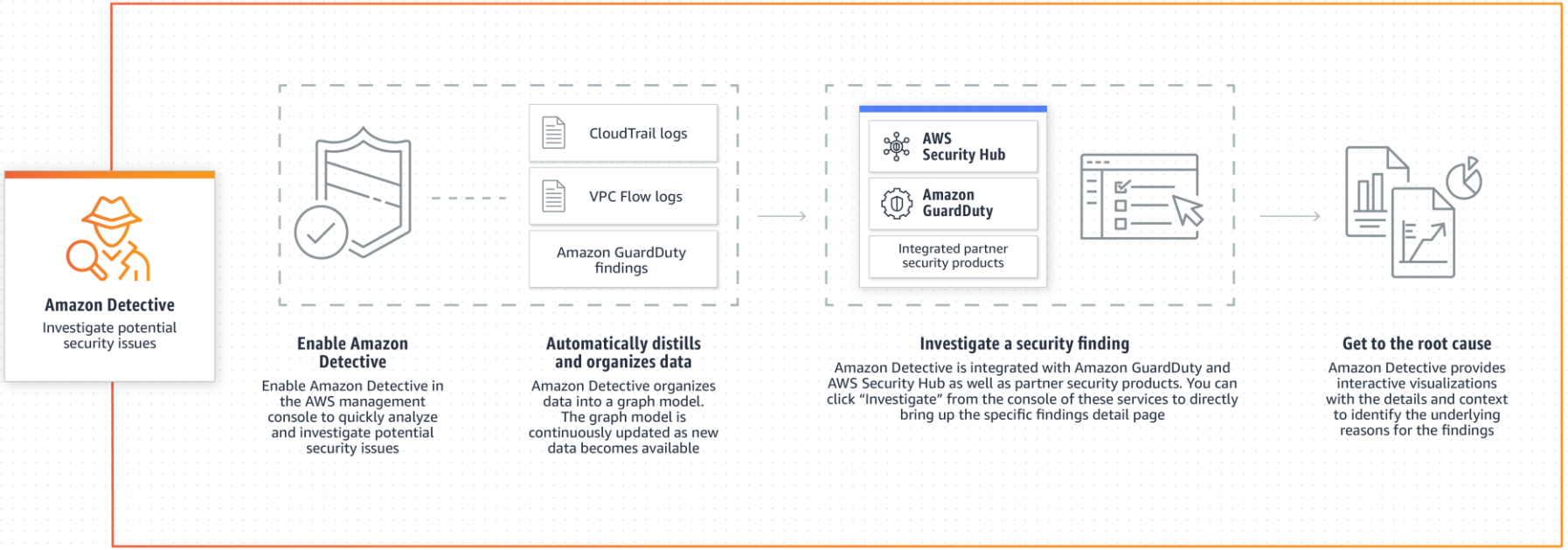
# Monitor for malicious activity and unauthorized behavior






aws | aws marketplace

# Analyze and visualize data to discover root causes

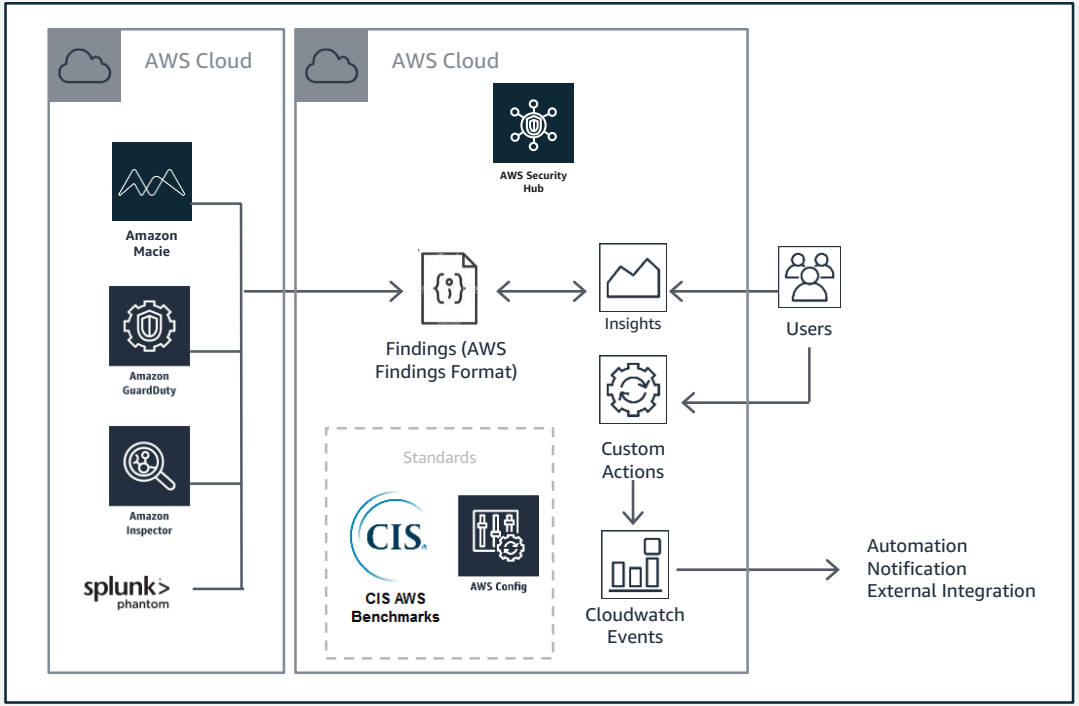





aws | aws marketplace

# Gain full visibility into data source output in your AWS environment

Generate security findings through native AWS services, such as Amazon GuardDuty, or AWS Marketplace solutions, such as Splunk Enterprise and Splunk Phantom.






aws | aws marketplace

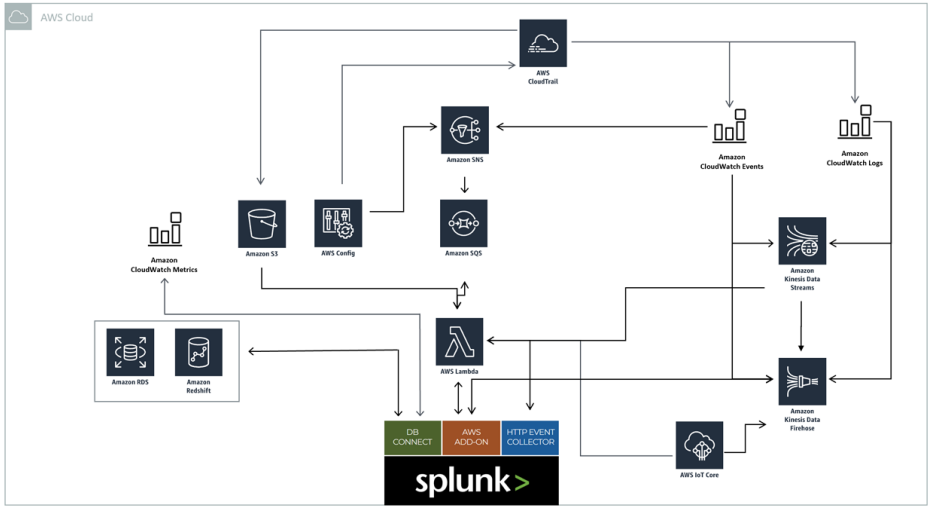
# How are AWS customers leveraging Splunk?

splunk>

Detect and aggregate security findings

Gain actionable threat intelligence

Reduce incident response time





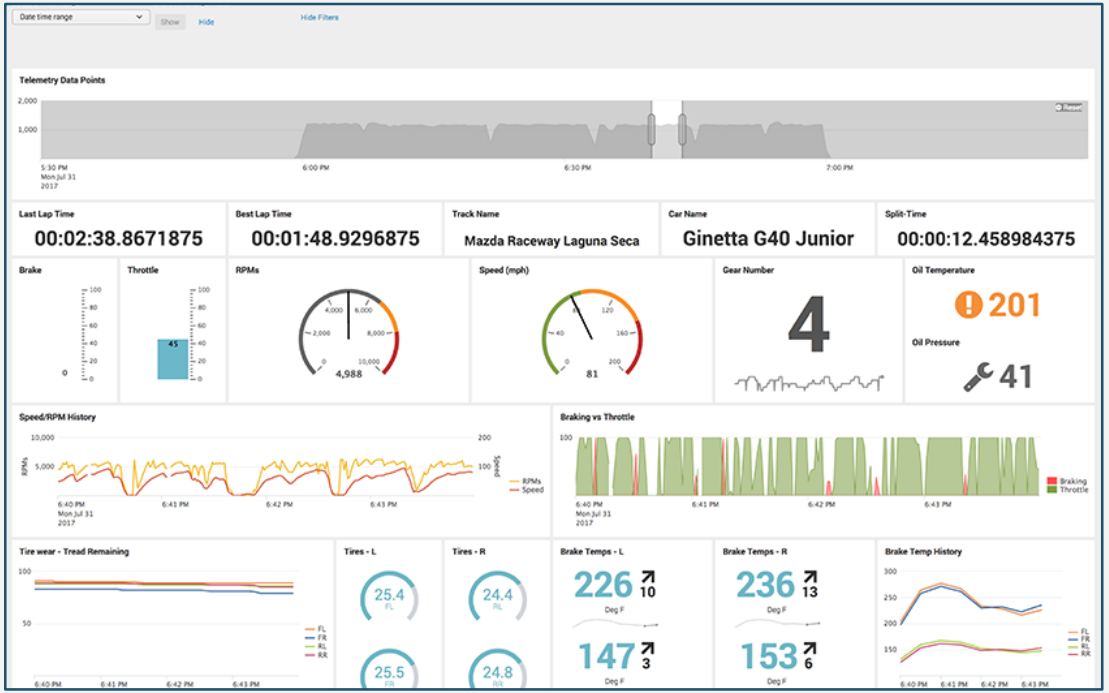

aws | aws marketplace

# Los Angeles enhances situational awareness

## Leveraging Splunk

**Benefits:**

- Established always-available, real-time situational awareness
- Increased ability to view and compare log data from multiple sources
- Reduced time to detect and respond to incidents

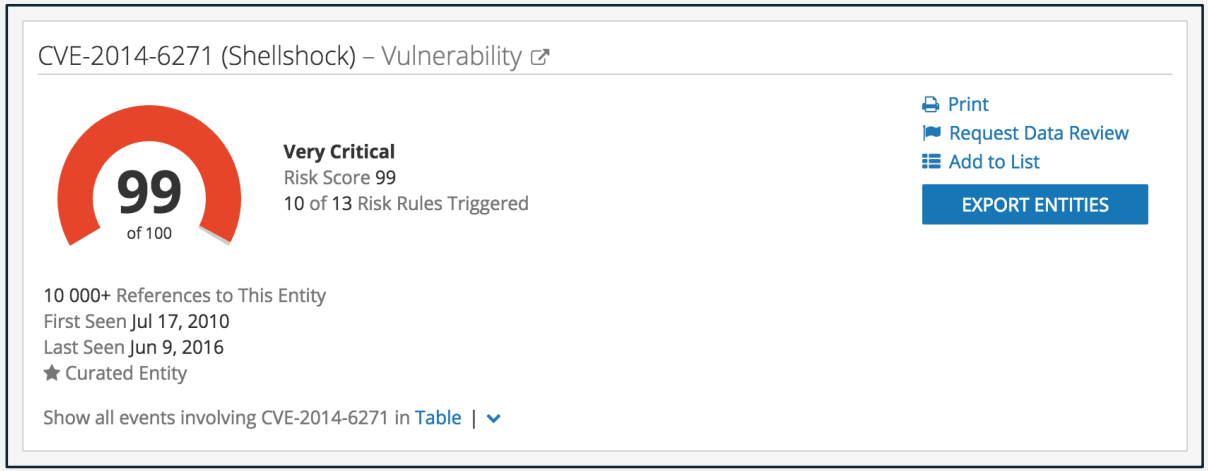


# St. Jude streamlines security investigations

## With Recorded Future

**Benefits:**

- 63% reduction on exploit kit traffic
- 28x better detection of botnet traffic
- 50% savings in analyst time for malicious IOC investigation

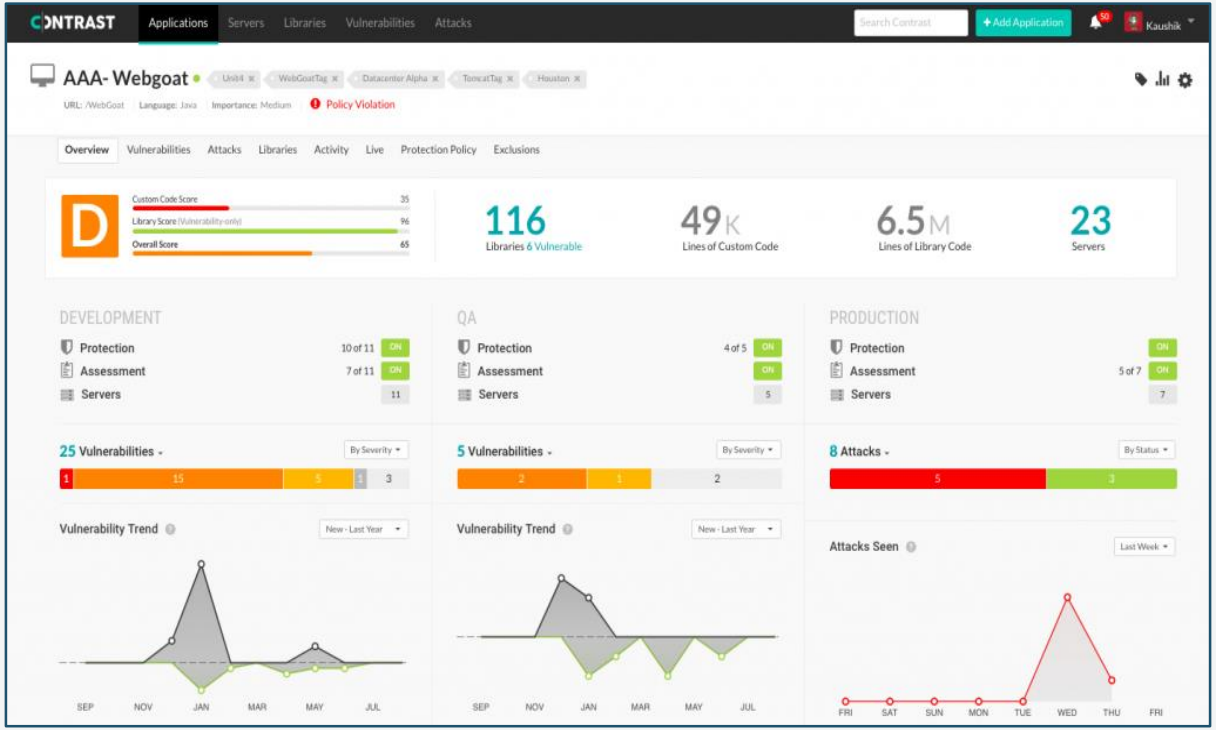


# Grasshopper Bank improved threat detection

## By adopting Contrast Security

**Benefits:**

- Improved threat detection and minimized false positives
- Virtual patching allows for a rapid security response to all applications
- Adds additional security features for strengthened security posture



# Why AWS Marketplace?

**Flexible consumption and contract models**

**Quick and easy deployment**

**Helpful humans to support you**



aws | aws marketplace

# How can you get started?

## Find

**A breadth of security solutions:**

splunk> · Recorded Future® · CONTRAST SECURITY · paloalto NETWORKS · sumo logic · FORTINET · TREND MICRO · CROWDSTRIKE

## Buy

**Through flexible pricing options:**

- Free trial
- Pay-as-you-go
- Hourly | Monthly | Annual | Multi-Year
- Bring Your Own License (BYOL)
- Seller Private Offers
- Channel Partner Private Offers

## Deploy

**With multiple deployment options:**

- Software as a Service (SaaS)
- Amazon Machine Image (AMI)
- AWS CloudFormation (Infrastructure as Code)
- Amazon Elastic Container Service (ECS)
- Amazon Elastic Kubernetes Service (EKS)



aws | aws marketplace

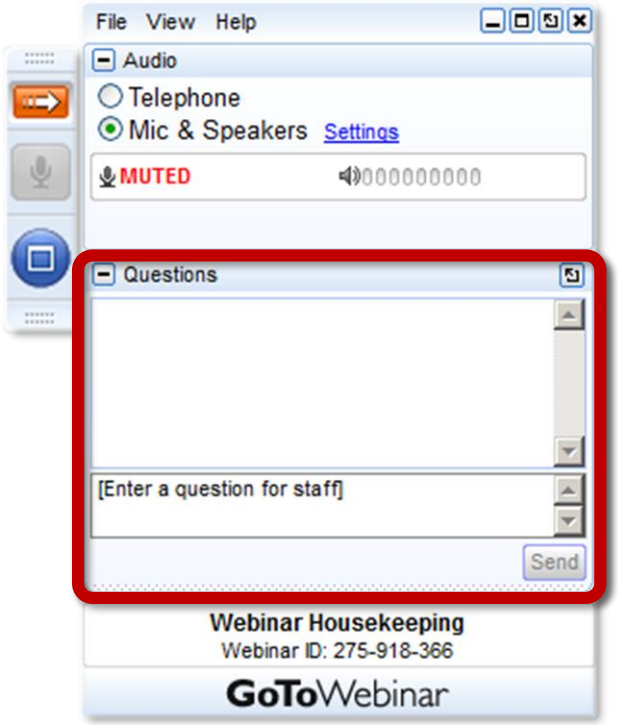
# Webinar summary

- Tracking TTPs is a valuable effort for any mature security team.
- Leverage AWS Services that integrate with your AWS environment and can enhance your network segmentation capabilities.
- Current tools? Bring your own license to leverage benefits of AWS Marketplace.
- New tools? Select solutions in AWS Marketplace for a curated list proven on AWS.

# Q&A

Please use **GoTo**Webinar's Questions tool to submit questions to our panel.

Send to "Organizers" and tell us if it's for a specific panelist.



# Acknowledgments

Thanks to our sponsor:

aws marketplace

To our special guest: Sagar Khasnis

And to our attendees, thank you for joining us today!