

# How to Perform a Security Investigation in AWS

Sponsored by  
 aws marketplace

# Today's Speakers

- Kyle Dickinson – SANS Instructor, Analyst and Author; Cloud Security Architect, Koch Industries
- David Aiken – AWS Marketplace, Specialist Solutions Architect

# Agenda

---

Incident Response (IR) Planning

---

Incident Data Sources

---

Amazon EC2 Instance Metadata and Forensic Acquisition

---

Use Cases

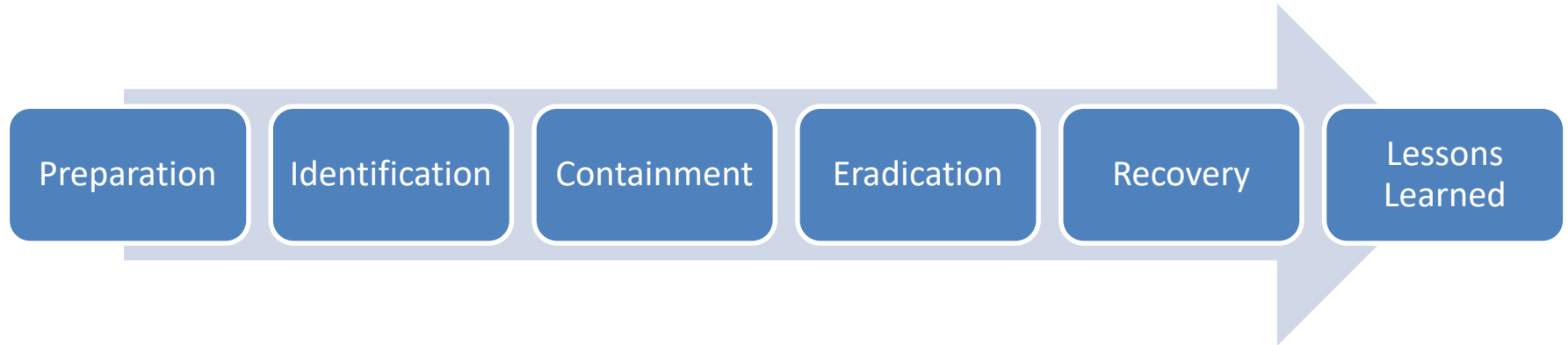
---

AWS Marketplace Solutions

---

AWS Marketplace Success Stories

# Incident Response (IR) Planning



SANS Six-Step Incident Response Methodology

# Cloud-Specific IR Planning

## 1. Preparation

- What cloud service provider is being used?
- What is the deployment model? (Public? Hybrid? Private?)
- What is the cloud model? (SaaS, PaaS, IaaS?)

## 2. Identification

- Is there unusual activity in the audit logs?
- Did something get misconfigured?

## 3. Containment

- Can we disable a user's access?
- Can we isolate the VM or subnet?
- How do we acquire an image?

## 4. Eradication

- Can we remove affected systems?
- Can we remove/replace compromised credentials?

## 5. Recovery

- Can we restore normal business operations?
- Is a business continuity plan available?
- Did that plan need to be implemented?

## 6. Lessons Learned

- What gaps in coverage did we discover?
- How do we close those gaps?

# VPC Traffic Mirroring

- “Spanport-as-a-Service”
- Mirror traffic of selected instances to a target
  - Elastic Load Balancer
  - Amazon EC2 instance
    - Suricata
    - Zeek
    - Third-party SaaS tool

# AWS CloudTrail Events

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDAZDEVHULLOJ65ACNU",
    "arn": "arn:aws:iam::90123456789:user/Marc_the_Intern",
    "accountId": "90123456789",
    "userName": "Marc_the_Intern"
  },
  "eventTime": "2019-09-04T23:00:13Z",
  "eventSource": "signin.amazonaws.com",
  "eventName": "ConsoleLogin",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "11.22.33.44",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_0; rv:61.0) Gecko/20100101 Firefox/61.0",
  "requestParameters": null,
  "responseElements": {
    "ConsoleLogin": "Success"
  },
  "additionalEventData": {
    "LoginTo": "https://console.aws.amazon.com/console/home",
    "MobileVersion": "No",
    "MFAUsed": "No"
  },
  "eventID": "734f86de-ff17-47ef-8e60-5e6186fe041d",
  "eventType": "AwsConsoleSignIn",
  "recipientAccountId": "90123456789"
}
```

The **userIdentity** used for the event:

- type:** Shows if a Role, or User was used
- principalId:** Unique identifier for this specific user (Think SID.)
- arn:** Amazon Resource Name
- accountId:** What account ID was logged into
- userName:** User that authenticated

Additional details:

- eventTime:** Zulu time for when the event occurred
- eventSource:** How the API was called
- eventName:** One of many API calls that can be used within AWS
- awsRegion:** Which region the console was set to log in to (can vary depending on how the login was initiated; good source to determine if activity is occurring outside of normal regions)
- sourceIPAddress:** The IP address which the request was sent from
- userAgent:** Fingerprint of what was used (browser or CLI version)
- requestParameters:** What was included in the request
- responseElements:** If the API delivers a response, this section contains additional details

# Amazon EC2 Instance Metadata

---

AMI ID

---

IAM data

---

Instance ID

---

Instance type

---

Public hostname



# Forensic Acquisition

- Create a Security Group that does not allow outbound traffic.
- Attach to compromised Amazon EC2 instance.
- Create snapshot of Amazon EC2 instance.
- Perform memory acquisition, if possible.
- Share snapshot with Security Account (if using one).
- Create volume from snapshot.
- Attach volume to SIFT EC2 instance.

# Use Case 1

- **Scenario:** Amazon EC2 instance is communicating to unusual destinations.
- **AWS services to use:**
  - AWS CloudTrail
    - Was something modified to permit this traffic?
  - Amazon VPC Flow Logs/Amazon Traffic Mirroring
    - Details of network communication
  - Amazon EC2 Snapshot
    - If additional review is required of instance

# Use Case 2

- **Scenario:** Administrative activity is occurring from multiple IP Addresses.
- **AWS services to use:**
  - AWS CloudTrail
    - Understand additional activity
  - AWS Identity and Access Management (IAM)
    - Temporarily disable key while investigation is underway to understand anomalous behavior

# Next Steps

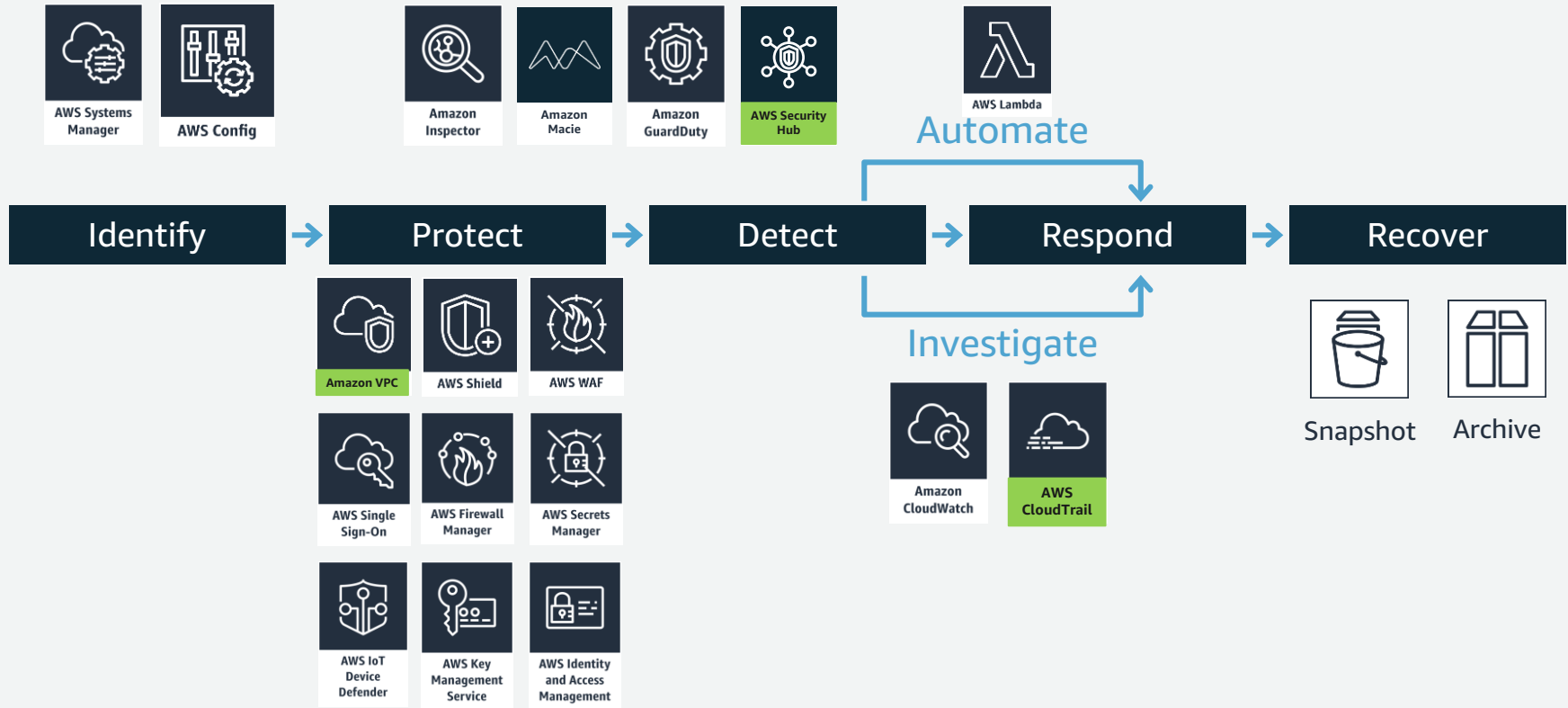
- Create an IaaS-specific incident response plan.
- Formulate exercises.
- Identify training opportunities.




# Enabling a Security Investigation in AWS





# AWS services that enhance security investigations





# Data sources that support contextual investigations

 AWS Cloud

 CloudTrail logs

 VPC Flow logs

 VPC Traffic Mirroring

 DNS Logs

Filter: Read only false Time range: Select time range

Event time	User name	Event name	Resource type
2019-10-17, 01:28:22 AM	i-0f27009005fac557a	AssignPrivateIpAddresses	EC2 NetworkI
2019-10-17, 01:28:22 AM	i-0ca8602fb23b79bfb	CreateNetworkInterface	EC2 SecurityG

```
2018-07-26T02:27:11.000Z 2 684778767920 eni-1146f345 5.8.54.27 172.31.79.58 49
2018-07-26T02:27:30.000Z 2 684778767920 eni-1146f345 172.31.79.58 66.135.44.92
2018-07-26T02:27:30.000Z 2 684778767920 eni-1146f345 188.92.74.189 172.31.79.5
2018-07-26T02:27:30.000Z 2 684778767920 eni-1146f345 159.203.158.197 172.31.79
2018-07-26T02:27:30.000Z 2 684778767920 eni-1146f345 190.195.96.12 172.31.79.5
2018-07-26T02:27:30.000Z 2 684778767920 eni-1146f345 172.31.79.58 159.203.158
2018-07-26T02:27:30.000Z 2 684778767920 eni-1146f345 66.135.44.92 172.31.79.58
```

tms-079df7621c213da49: MirrorSession01

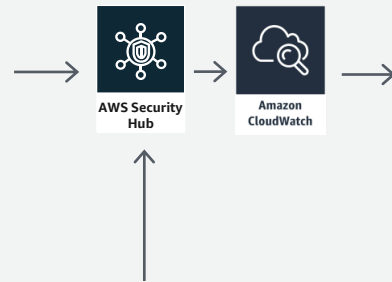
**Details**

Name	Session ID
MirrorSession01	tms-079df7621c213da49

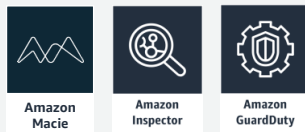
```
1.0 2017-12-13T08:16:02.130Z Z123412341234 example.com A NOERROR UDP FRA6 192.168.
1.0 2017-12-13T08:15:50.235Z Z123412341234 example.com AAAA NOERROR TCP IAD12 192.
1.0 2017-12-13T08:16:03.983Z Z123412341234 example.com ANY NOERROR UDP FRA6 2001:d
1.0 2017-12-13T08:15:50.342Z Z123412341234 bad.example.com A NXDOMAIN UDP IAD12 19
1.0 2017-12-13T08:16:05.744Z Z123412341234 txt.example.com TXT NOERROR UDP JFK5 18
```

# Integrations that support effective investigations

## AWS forwarding findings into AWS Security Hub



## AWS Security Services forwarding findings into AWS Security Hub



## "Taking Action"





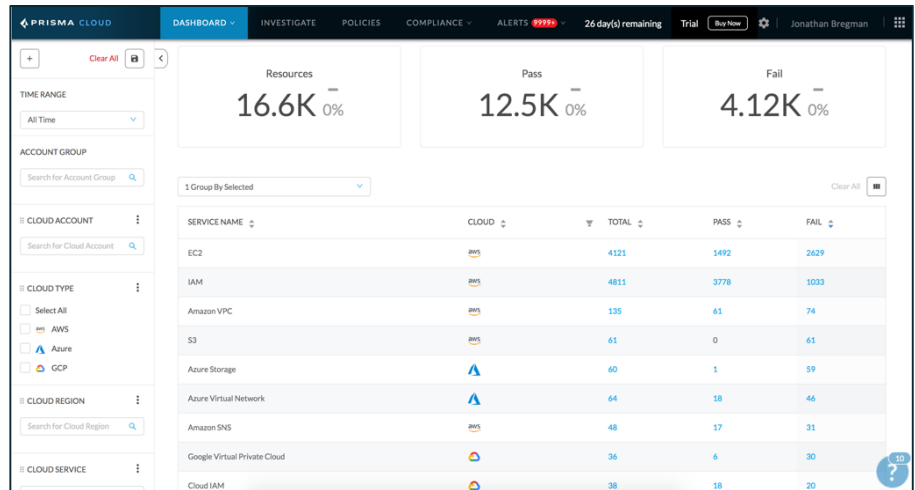
# How are AWS customers leveraging Palo Alto Networks?



Expedite security investigations

Automate responses to security threats

Remediate findings



# Pokémon improves SOC efficiencies

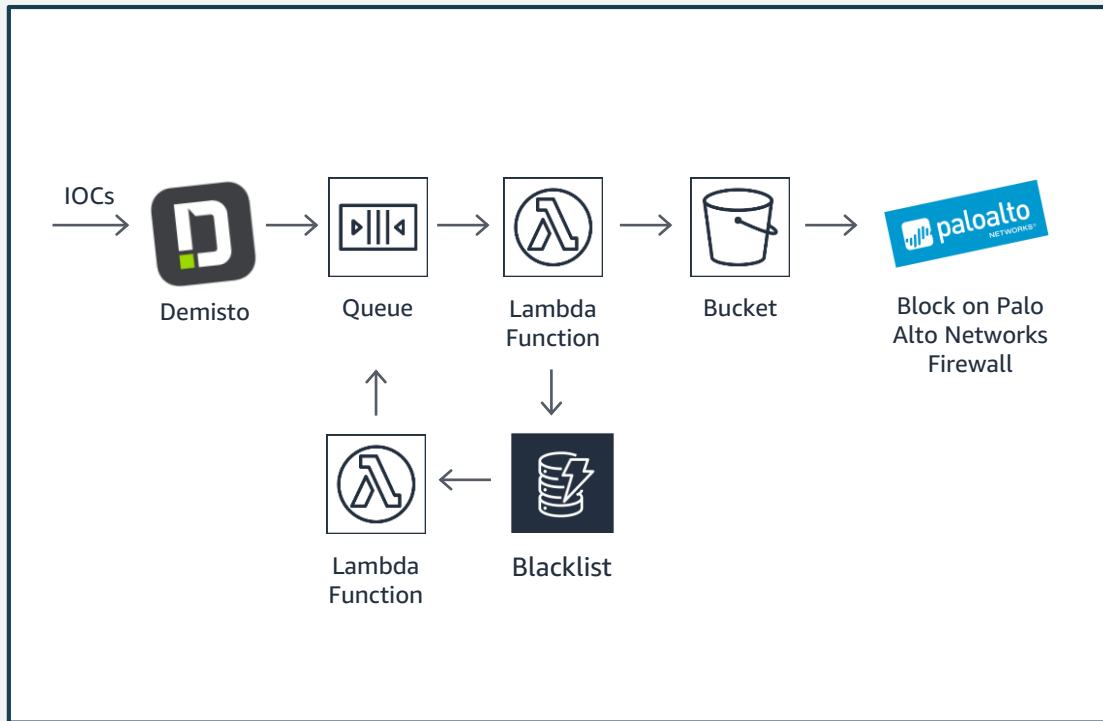
DEMISTO  
A Palo Alto Networks COMPANY



By adopting Demisto's SOAR Platform

## Benefits:

- Provided scaling for cloud environment
- Automated repetitive tasks, enabling SecOps analysts to focus on critical operations
- Active use cases include phishing enrichment and response, employee onboarding, and EC2 & account compromise

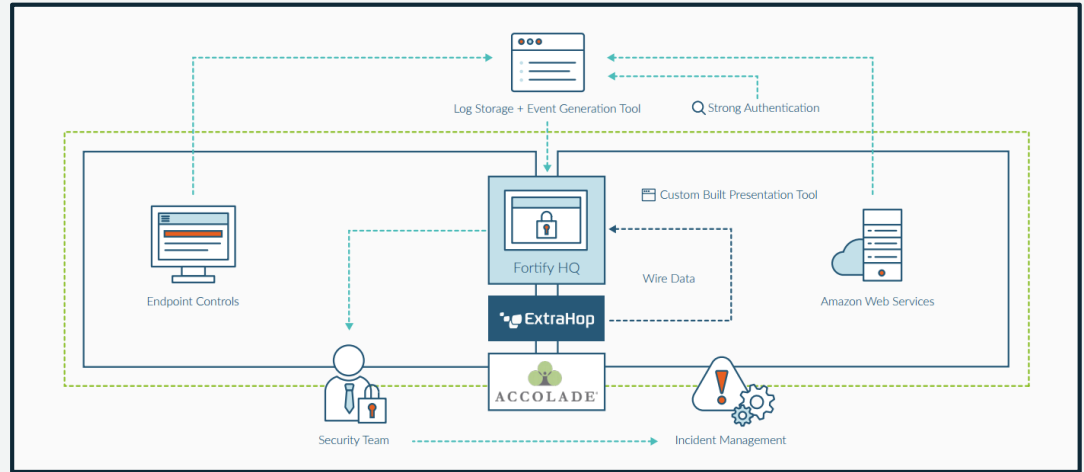


# Accolade audits security hygiene in real-time

By leveraging wire data from ExtraHop Reveal(x)

## Benefits:

- Real-time, cross-tier visibility into all East-West traffic
- Identifying and remediating any security incident
- Reduced annual IT security monitoring spend nearly 60%




# St. Jude streamlines security investigations

With Recorded Future's real-time threat intelligence

## Benefits:

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

CVE-2014-6271 (Shellshock) - Vulnerability [↗](#)



**Very Critical**  
Risk Score 99  
10 of 13 Risk Rules Triggered

Print  
Request Data Review  
Add to List

**EXPORT ENTITIES**

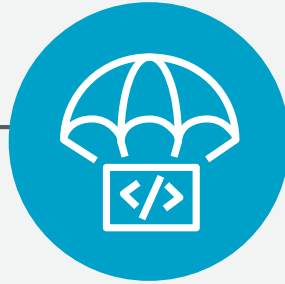
10 000+ References to This Entity  
First Seen Jul 17, 2010  
Last Seen Jun 9, 2016  
★ Curated Entity

Show all events involving CVE-2014-6271 in [Table](#) | [▼](#)

# Why AWS Marketplace?



**Flexible consumption  
and contract models**



**Quick and  
easy deployment**



**Helpful humans  
to support you**

# How can you get started?

## Find



**A breadth of security solutions:**



Recorded Future

ExtraHop



Barracuda

splunk >

Qualys



## Buy



**Through flexible pricing options:**

Free trial

Pay-as-you-go

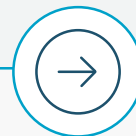
Hourly | Monthly | Annual |  
Multi-Year

Bring Your Own License (BYOL)

Seller Private Offers

Channel Partner Private Offers

## Deploy



**With multiple deployment options:**

SaaS

Amazon Machine Image (AMI)

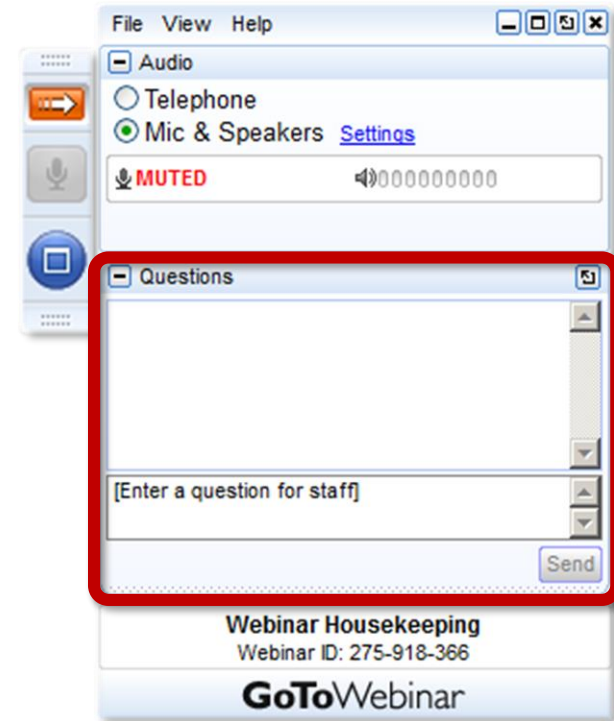
CloudFormation Template

Amazon Elastic Container Services (ECS)

# Q&A

Please use **GoToWebinar'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:



To our special guest: David Aiken

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