
AWS
re:Invent
NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

SEC321

Building your forensics capabilities on AWS

Jonathon Poling

Principal Security Consultant, AWS Professional Services
Amazon Web Services

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

Why forensics?

Setting up your forensics lab

Acquiring evidence

Analyzing evidence

Learning from investigations

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

About me

- Career in digital forensics and incident response (DFIR)
- Windows/Linux/Mac forensics SME
- Long-time DFIR community member/contributor and public presenter on DFIR (in the cloud)
- Lead threat detection and incident response (TDIR) offering development and delivery in AWS Professional Services (AWS ProServe)

@JPoForenso
jonpolin@amazon.com

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Why forensics?

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Why forensics?

- What is forensics?
  - Methodology
  - What it isn’t
- Why do it?
  - Purpose driven

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Setting up your forensics lab

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Setting up your forensics lab

- Forensics account
  - What's the structure?
  - Multiple accounts?
- Storage
  - What needs to be stored and how?
  - What type of folder/structure?

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Setting up your forensics lab

- Permissions/roles
  - What roles are needed?
  - What permissions?
- Analysis tools/setup
  - AMIs?
  - CI/CD?

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Setting up your forensics lab

BEST PRACTICES

- Forensics account
  - Have a dedicated OU and account(s) for forensics
- Storage
  - Establish a storage structure that facilitates data segregation, security, and access
- Permissions/roles
  - Implement specific roles (such as responder, investigator, data custodian, admin) with least-privilege permissions for collecting data, analyzing data, managing data, and performing administrative actions (role/policy/key creation)
- Analysis tools/setup
  - Leverage prebuilt AMIs (instrumented with forensic tooling) using a dedicated CI/CD pipeline for testing/deploying forensic analysis systems at (secure) scale

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Acquiring evidence

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Acquiring evidence

- Evidence in AWS
  - Services/control plane
  - Systems
  - Logs
- Acquisition methods
  - Traditional agents vs. cloud-native
  - Data transfer/storage

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Acquiring evidence

BEST PRACTICES

- Evidence in AWS
  - Understand the variety of data sources within the service/control plane
  - Ensure all appropriate/required data sources are configured/enabled to provide comprehensive data needed for investigations
- Acquisition methods
  - Have a plan, methodology, and tooling for accessing and acquiring the various types of data sources
  - Determine if/when proactive (pre-compromise) versus reactive (post-compromise) data collection is merited
  - Ensure data is being collected to a centralized and well-structured repository

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Analyzing evidence

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Analyzing evidence

- Resources
  - Amazon EC2 instances (Amazon EBS volumes)
  - Databases
- Logs
  - AWS CloudTrail
  - AWS Config
  - DNS (Amazon Route 53)
  - Load balancer (application/network)
  - Amazon VPC Flow Logs

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Analyzing evidence

BEST PRACTICES

- Resources
  - Ensure your analysis systems can directly and efficiently access the data for analysis
  - Understand which resources will need specialized data extraction/access techniques (databases)
  - Ensure you have the appropriate tooling to parse/extract information needed for investigations
- Logs
  - Understand how the service/control plane works (API calls) and how resources interact
  - Ensure each log source (format, structure, and content) is well understood to effectively analyze, interpret, and incorporate it into investigations
  - Ensure you have a log search/analysis capability, using cloud-native mechanisms as best as possible (for example, Amazon S3 ←→ Amazon Athena)

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Learning from investigations

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Learning from investigations

- Indicators of compromise (IOCs)
  - Extracting
  - Storing
  - Leveraging
- Tooling
  - Testing/research
  - Improving
- Process
  - Playbooks
- Lessons learned
  - Process/methodology

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Learning from incidents

BEST PRACTICES

- Indicators of compromise (IOCs)
  - Implement mechanisms to collect, store, and proactively apply IOCs from investigations
- Tooling
  - Ensure you have appropriate tooling needed to analyze all available resources/logs
  - Identify gaps in tooling and address them in advance
  - Implement a testing/research methodology for new/custom tooling
- Process
  - Implement alert/situation–specific IR playbooks to efficiently scale knowledge and processes
- Lessons learned
  - Incorporate a lessons-learned methodology into every investigation
  - Ensure you are getting better from every incident/response

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Key takeaways

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Key takeaways

- Preparation is paramount
  - Hours/minutes/seconds matter amid a compromise
- Account structure matters
  - Do not comingle the forensics account(s)
- Forensics requires multiple duties (roles/permissions)
  - Permissions must be clearly defined, separate, and least permissive
- Learning from incidents is transformative
  - The only way to get better (avoid repeating mistakes) is to comprehensively understand (investigate) incidents

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

Jonathon Poling
@JPoForenso
jonpolin@amazon.com



Please complete the session survey in the **mobile app**

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.