AWS Digital Forensics Automation @ Goldman Sachs

Ryan Tick
Cloud Security Architect
Goldman Sachs

Vaishnav Murthy
Cloud Security Architect
Goldman Sachs

Logan Bair
Cloud Security Architect
AWS – Professional Services

Agenda

1. Learning Objectives
2. Problem Space
3. How GS Solved Forensic Artifact Collection
4. Getting Started Resources
5. Q & A

What You'll Learn

Importance of having a digital forensics evidence collection workflow

How to effectively leverage AWS security services in your solution

Advantages of using multi-threading / concurrency to efficiently scale your solution

Problem Statement

Planetary Scale

- 3000+ accounts spanning 3 OUs
- Range of configuration requirements
- New accounts on-boarded regularly
- Easier to scale technology vs. people

Multiple Data Sources

- Different cloud native services need to be monitored
- Option to integrate with third-party sources

Critical MTTD & MTTR

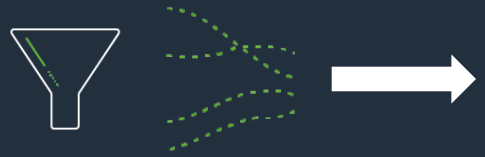
- MTTD and MTTR must be as low as possible
- Response actions need to have minimal business and forensic evidence impact

aws financial services

Our Solution

Leverages Security Hub

- Stores security findings centrally
- Leverages ASFF to aggregate event sources
- Acts as a trigger for notification and response actions



Consolidates Data Sources

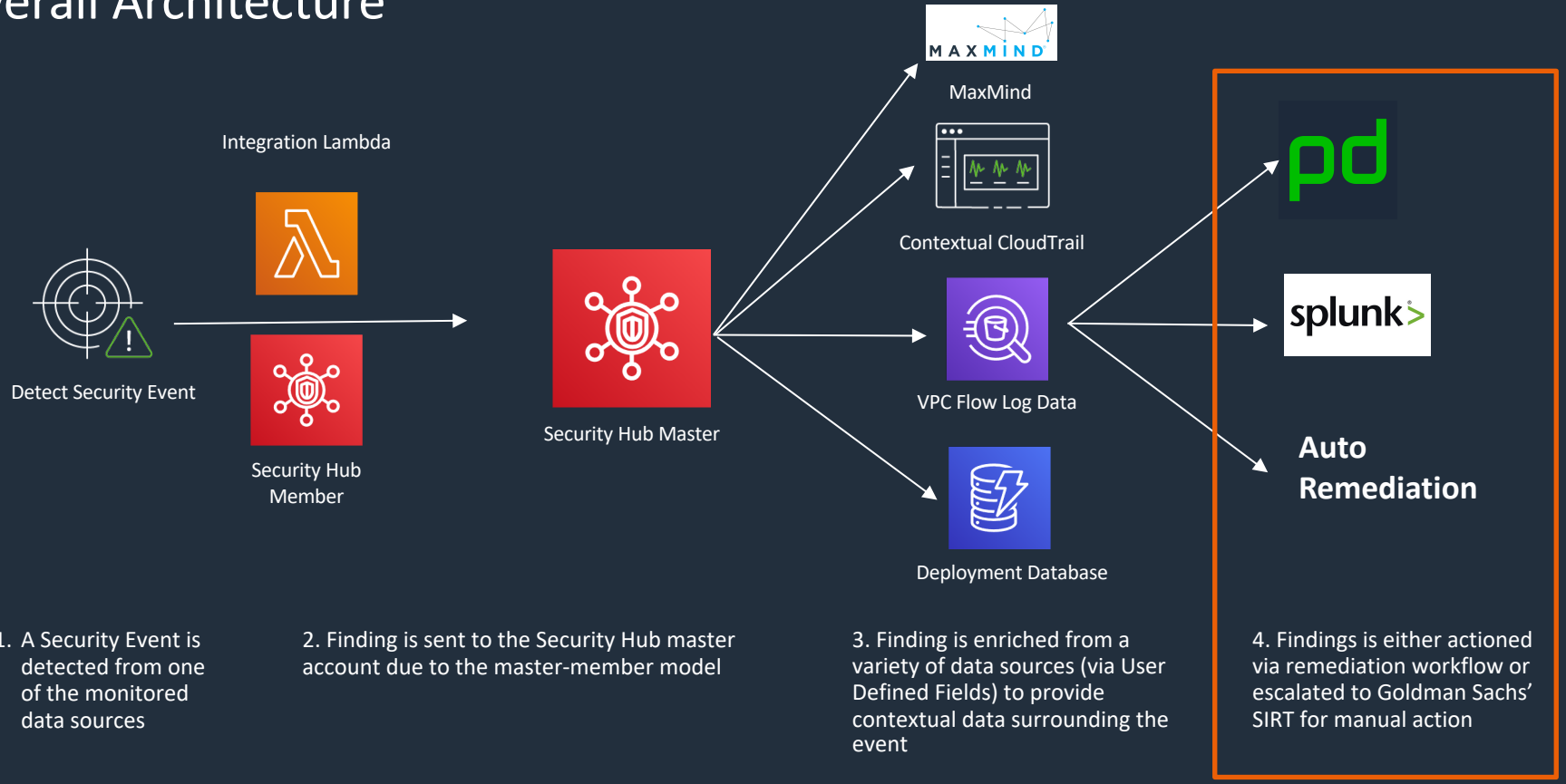
- Supports custom detections on top of AWS CloudTrail, AWS Config, AWS VPC Flow Logs, etc.
- Allows Goldman Sachs' SIRT to trigger an investigation manually

Enriches & Auto-Remediates

- Security Hub Findings enriched via User Defined fields
- Cloud Watch Event Rules allow for a targeted response

aws financial services

Overall Architecture



1. A Security Event is detected from one of the monitored data sources

2. Finding is sent to the Security Hub master account due to the master-member model

3. Finding is enriched from a variety of data sources (via User Defined Fields) to provide contextual data surrounding the event

4. Findings is either actioned via remediation workflow or escalated to Goldman Sachs' SIRT for manual action

aws financial services

Why It’s Important

- Disk evidence: point in time copy of all volumes attached to the compromised instance. Can potentially answer questions such as:
  - When was the Bitcoin miner installed or executed for the first time?
  - How did the Bitcoin miner get on the system?
  - Is there any evidence of sensitive data exfiltration?
  - Are there any other known bad programs or files on the system?

- Memory evidence: point in time copy of memory (RAM) associated with the compromised instance. Can potentially answer questions such as:
  - What process is running the Bitcoin software?
  - What parent process executed the Bitcoin software?
  - Are there any established network connections?
  - Where is the attacker sending the mined Bitcoin?

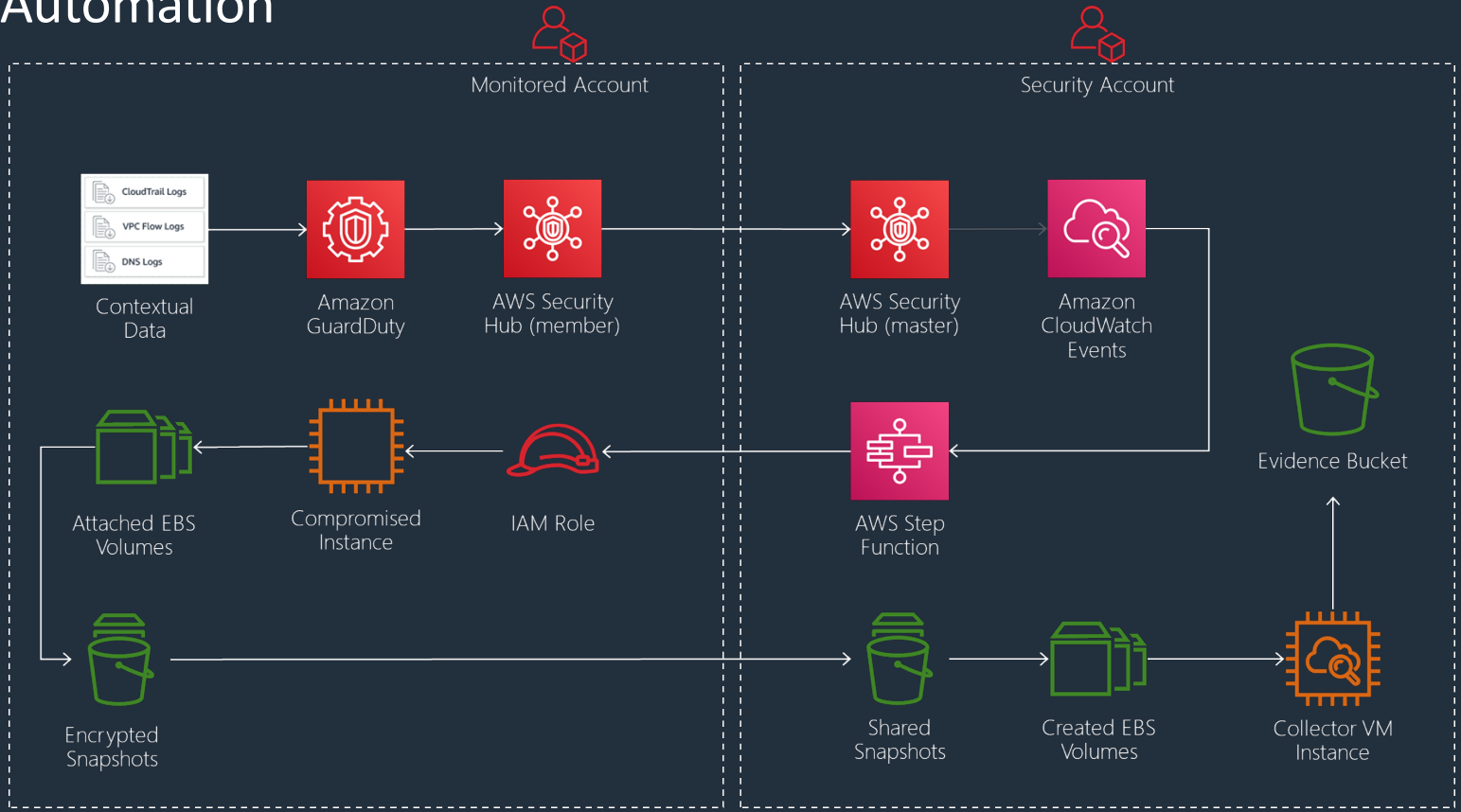
Disk Collection Workflow

aws financial services

Before Automation

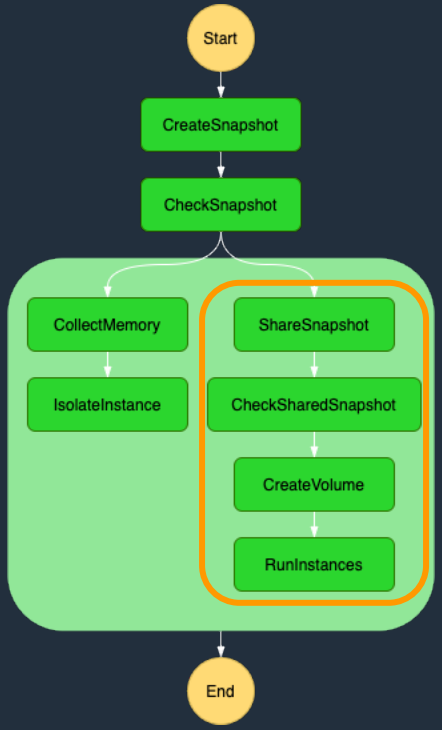
aws financial services

After Automation



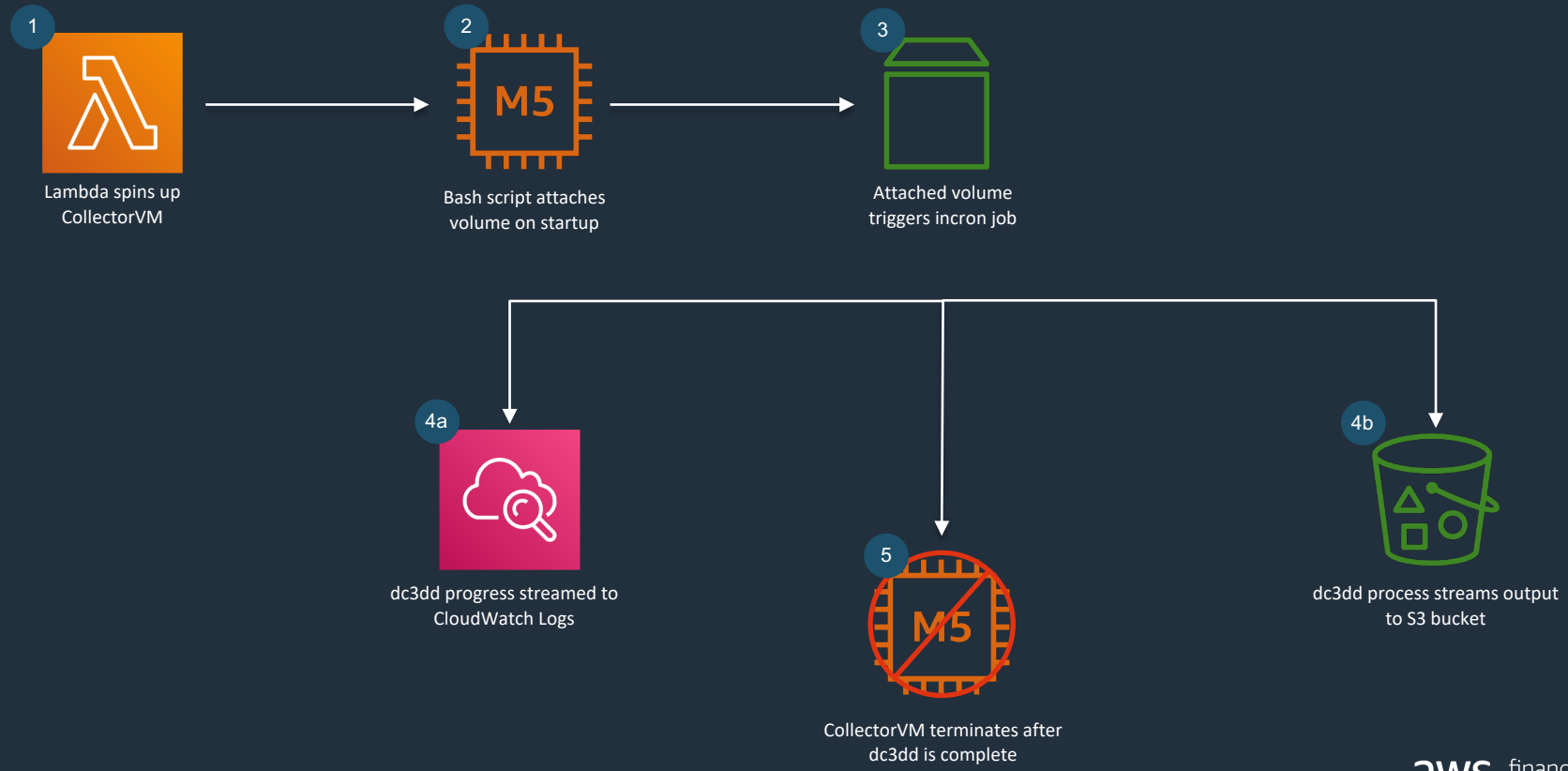
aws financial services

Step Function – Disk



aws financial services

Custom Collection AMI



aws financial services

Getting Started – Disk Workflow

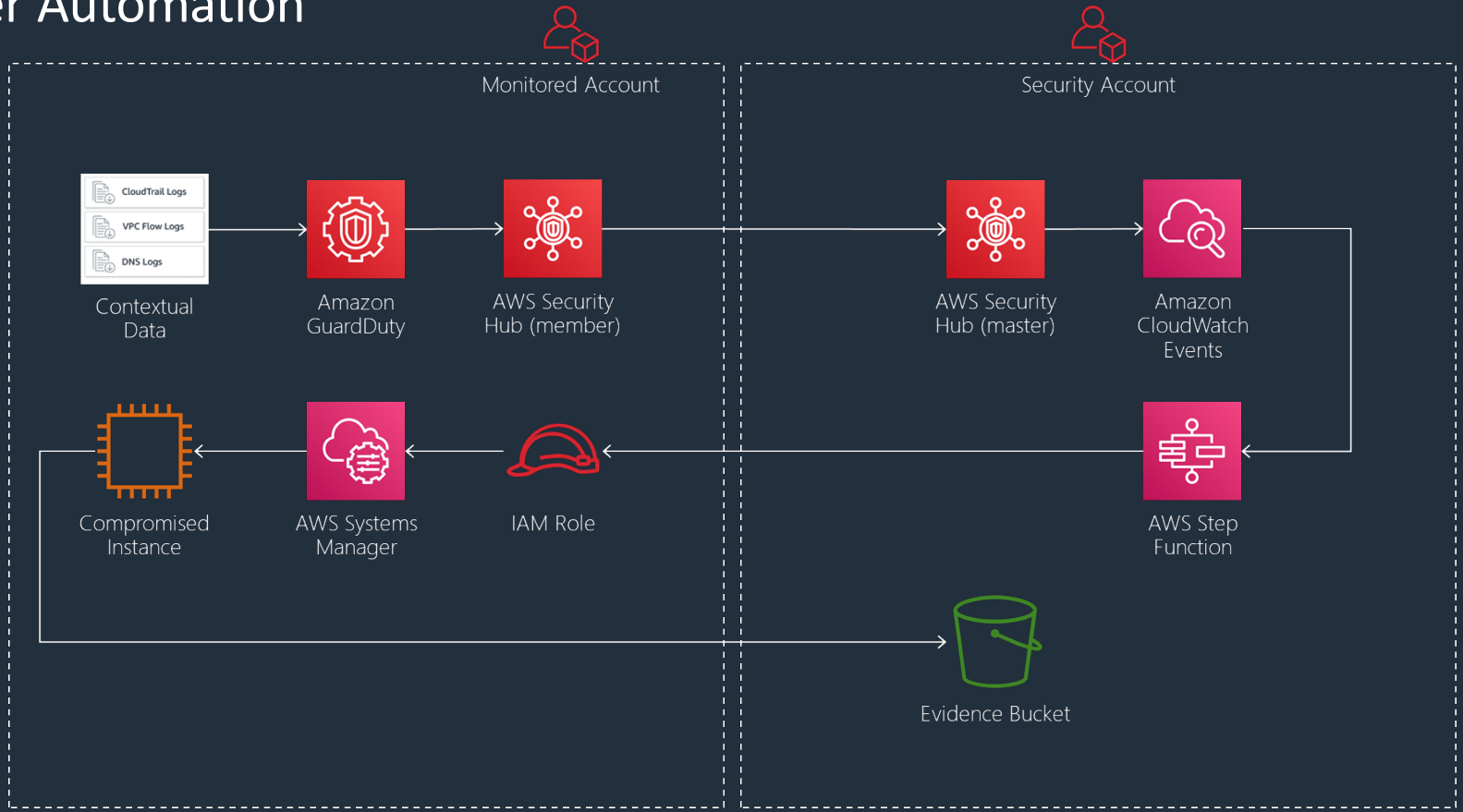
- Leverage and compare multi-threading and concurrent execution with Lambda
- Determine the necessity for a full disk collection vs. a triage collection
- Stream dc3dd output directly to S3
- Leverage VPC endpoints wherever possible
- Consider the tradeoff between cost and collection speed
- Remember that instance store data is not collected during an EC2 snapshot
- Restore EBS snapshots to HDDs (as opposed to SSDs) for hash verification

Memory Collection Workflow

Before Automation

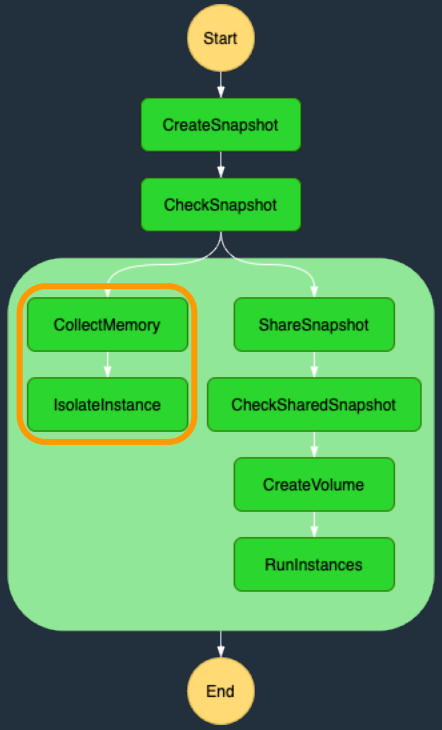
aws financial services

After Automation



aws financial services

Step Function – Memory



aws financial services

Getting Started – Memory Workflow

- Stream directly to S3 and include the expected size flag
- Consider the potential business impact of collecting memory
- Research the complexities of gateway VPC endpoints
- Leverage a file integrity monitoring (FIM) solution where possible
- Verify memory evidence before stopping or terminating the original host
- Understand the difference between tracked and untracked connections

Aligning to the AWS Well Architected Framework

Cost Optimization

- Manual processes relied on persistent infrastructure
- Automated workflow leverages dynamic resources and AWS managed services

Performance Efficiency

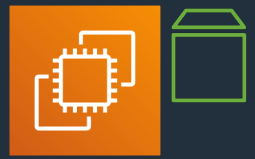
- New approach scales with volume, while manual process does not scale
- Automated workflow reduced collection/clean up times by ~85% at scale
- New approach allowed MTTR to become more real time

Reliability

- Not feasible to manually collect disk and memory for every finding in Security Hub
- Automated workflow provides consistent and auditable approach, increasing collection scope by ~90%

aws financial services

Time Savings



Scenario 1: EC2 Instance with 1 8GB volume

- **Automated Workflow:** 11 minutes
- **Manual Workflow:** 15 minutes

Scenario 2: EC2 Instance with 4 8GB volumes

- **Automated Workflow**: 11 minutes end to end
- **Manual Workflow**: 1 hour 10 minutes

Scenario 3: 4 EC2 Instances with 1 8GB volume each

- **Automated Workflow:** 11 minutes end to end
- **Manual Workflow:** 1 hour 20 minutes

aws financial services

Summary

- Discussed the challenges faced by enterprises in the digital forensics space
- Reviewed memory and disk collection strategies used by Goldman Sachs
- Demonstrated the importance of scale in forensic artifact collection

Thank You

AWS Digital Forensics Automation @ Goldman Sachs

Ryan Tick
Cloud Security Architect
Goldman Sachs

Vaishnav Murthy
Cloud Security Architect
Goldman Sachs

Logan Bair
Cloud Security Architect
AWS – Professional Services

aws financial services