CYBER GUARDIANS

Midterm Ops 401d6

Agenda

1. Team Member Introductions
2. Problem Domain & Project Overview
3. Team Process & Documentation
4. Application Demonstration
5. Q&A

Our Team

Dericus Horner

Dylan Dempsey

Anthony Wall

Geneva Knott

Alexander Echols

Alexander Echols

- Co Founder of Cyber Guardians
- Cybersecurity Professional
- Physical penetration tester
- Does various accents

LinkedIn

Dericus Horner

- US Army Veteran
- Master's degree in Business Administration
- Current IT Property Specialist
- Detail Oriented/Critical Thinker

Connect With Me

Linked in

Geneva Knott

- Marine Corps Veteran- 0621 Communications
- 9 yo LE/Criminal Investigator -Violent Crimes w/ Bachelors in Criminal Justice
- working on Associates in Cyber Defense

LinkedIn

CompTIA ITF+

aws certified Cloud Practitioner FOUNDATIONAL

Candidate (ISC)²

Dylan Dempsey

CompTIA

ITF+

CERTIFIED

Dylan Dempsey | LinkedIn

- Navy Veteran (STG2)
- Security Clearance
- Real Estate Agent/ Investor
- Expert at identifying risks and opportunities

Anthony G Wall

Persistent and goal oriented

- Former USMC Infantry team leader
- Licensed and registered Loan officer
- CompTIA ITF+ Certified
- Aspiring cyber security professional

CompTIA ITF+ CERTIFIED

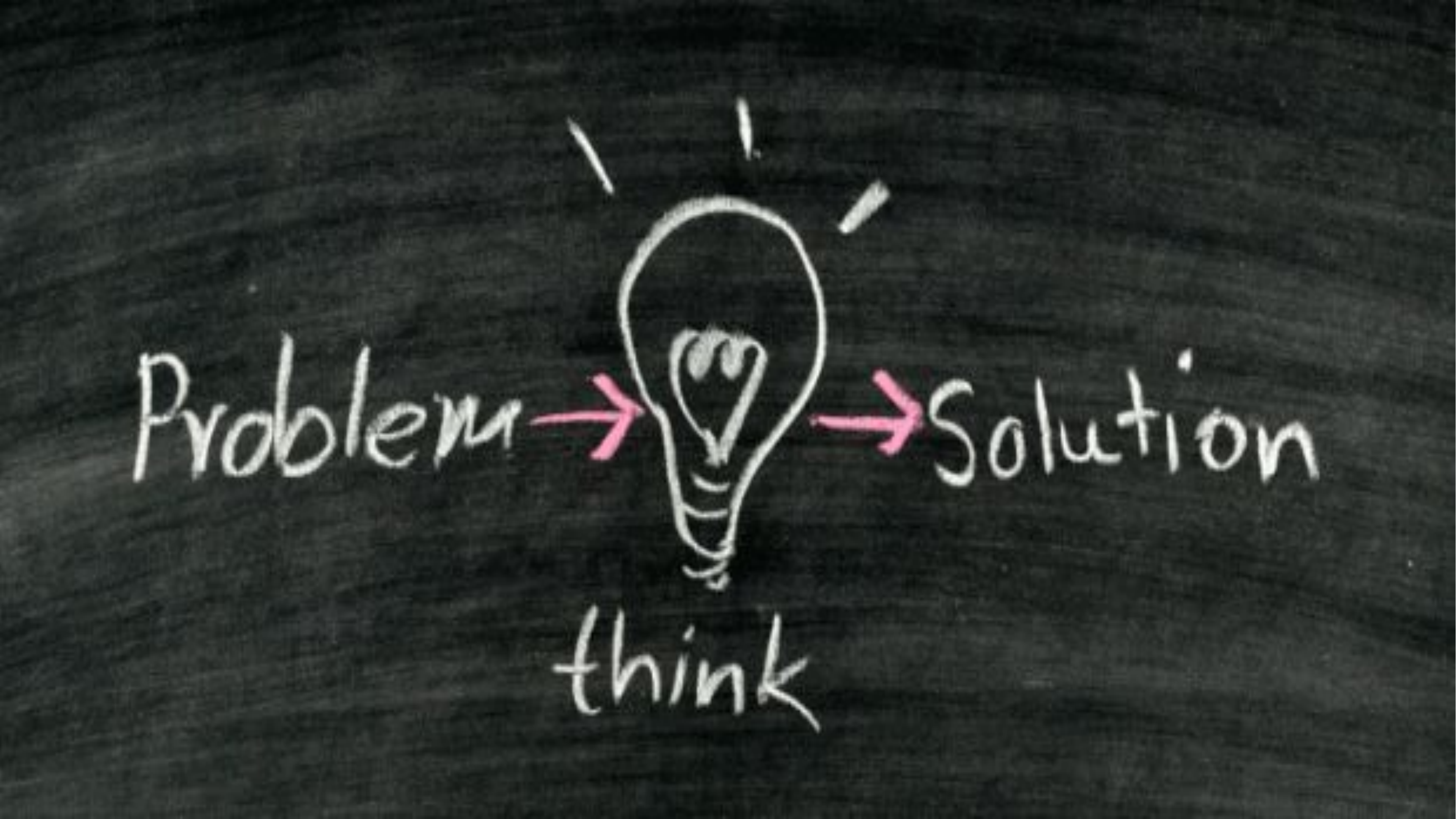
Scan to connect with me on Linkedin:

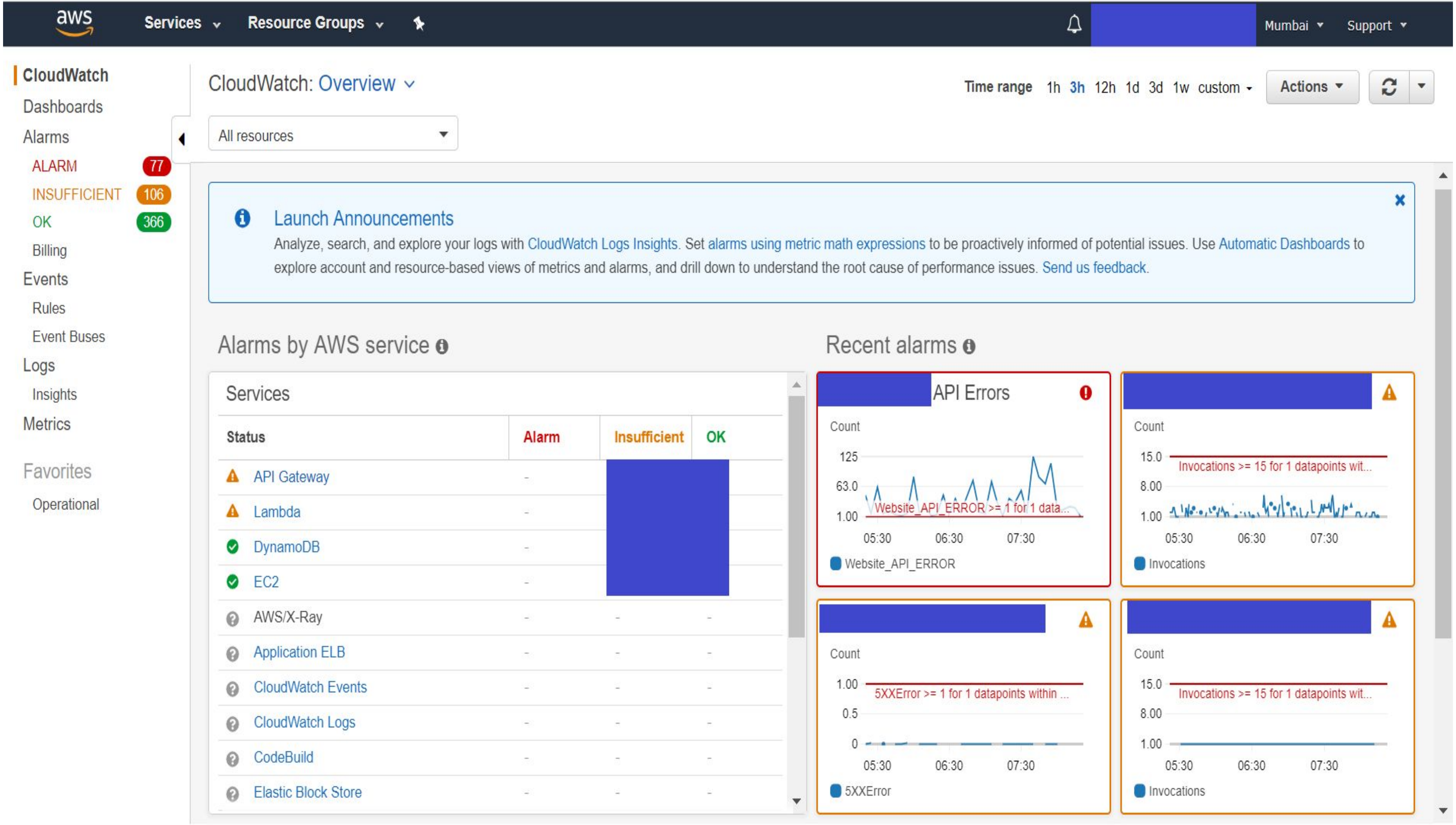
Problem Domain

Cyber Guardians has been contracted to improve the cybersecurity processes and systems for the clients company.

Focuses include:

- Logging-Cloud Trail
- Monitoring-Cloud Watch
- Detection of adversarial activity on cloud infrastructure.


Problem
Solution
think



CloudWatch: Overview

Launch Announcements

Analyze, search, and explore your logs with CloudWatch Logs Insights. Set alarms using metric math expressions to be proactively informed of potential issues. Use Automatic Dashboards to explore account and resource-based views of metrics and alarms, and drill down to understand the root cause of performance issues. Send us feedback.

Alarms by AWS service

Services

Status	Alarm	Insufficient	OK
⚠ API Gateway	-	[redacted]	[redacted]
⚠ Lambda	-	[redacted]	[redacted]
✓ DynamoDB	-	[redacted]	[redacted]
✓ EC2	-	[redacted]	[redacted]
? AWS/X-Ray	-	-	-
? Application ELB	-	-	-
? CloudWatch Events	-	-	-
? CloudWatch Logs	-	-	-
? CodeBuild	-	-	-
? Elastic Block Store	-	-	-

Recent alarms

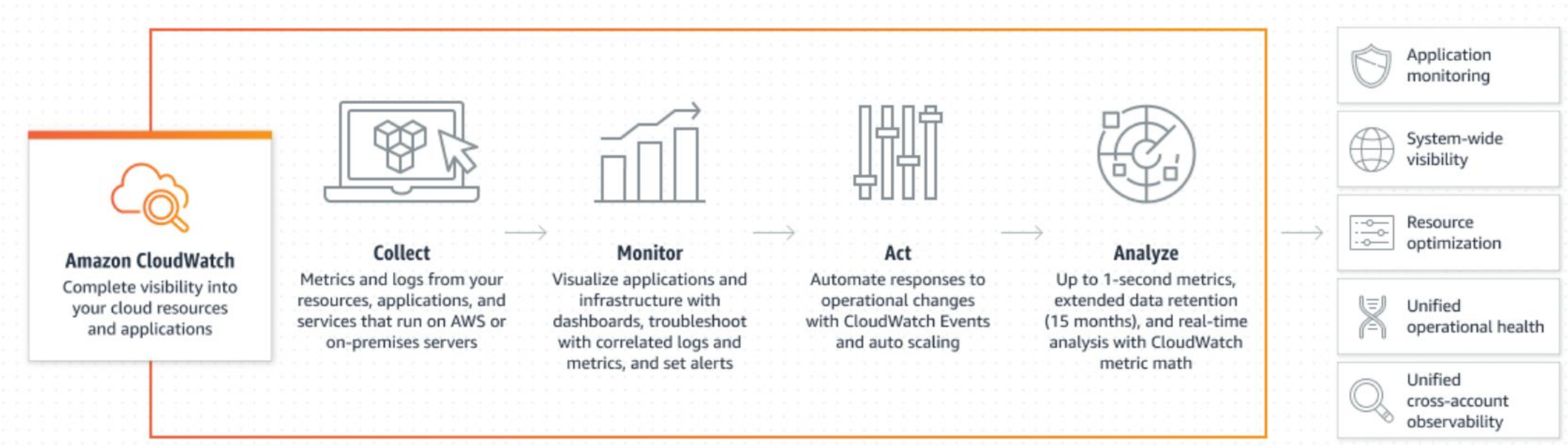
[redacted] API Errors

[redacted]

[redacted]

[redacted]

AWS CloudWatch



Amazon CloudWatch
Complete visibility into your cloud resources and applications

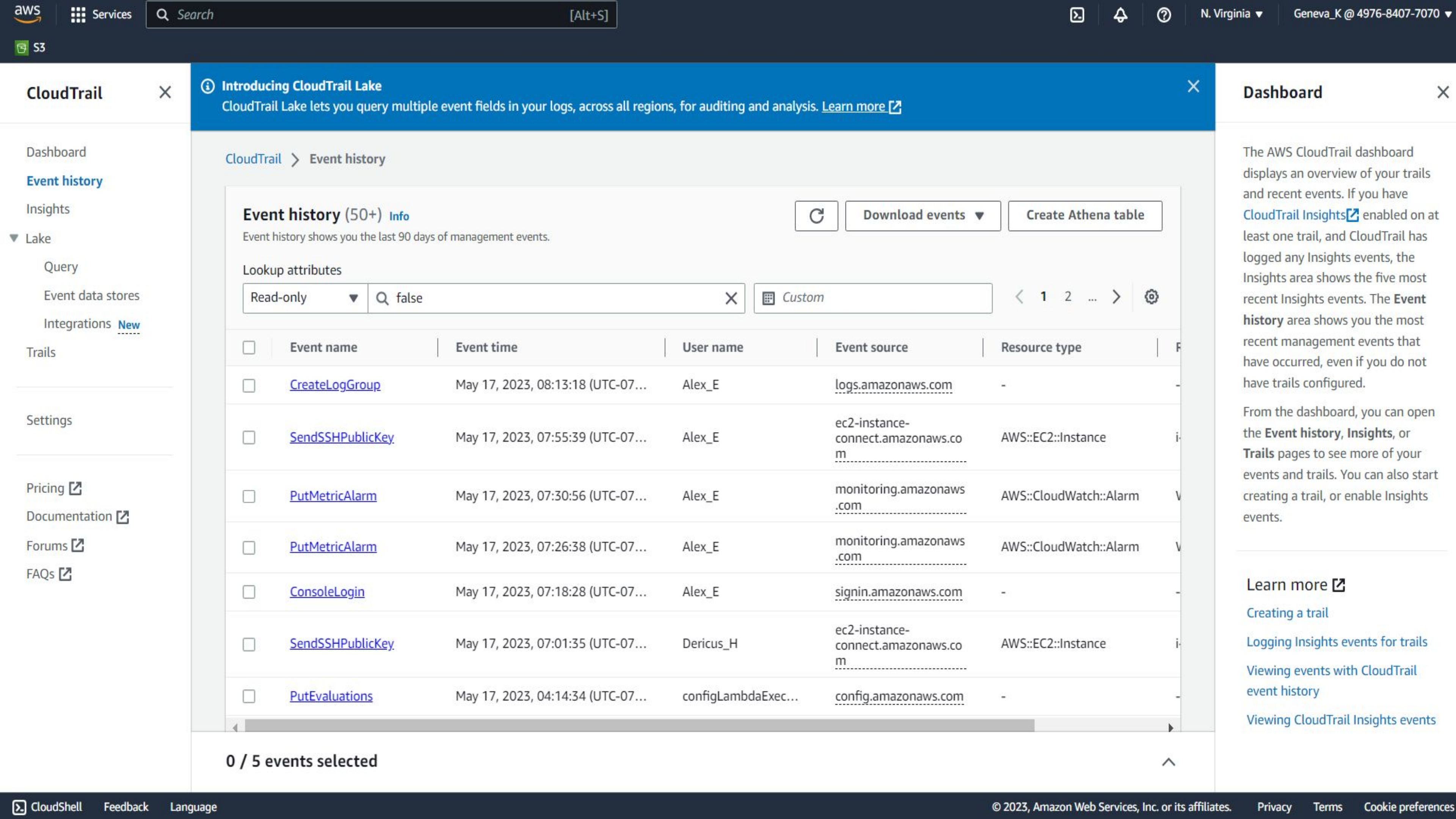
Collect
Metrics and logs from your resources, applications, and services that run on AWS or on-premises servers

Monitor
Visualize applications and infrastructure with dashboards, troubleshoot with correlated logs and metrics, and set alerts

Act
Automate responses to operational changes with CloudWatch Events and auto scaling

Analyze
Up to 1-second metrics, extended data retention (15 months), and real-time analysis with CloudWatch metric math

- Application monitoring
- System-wide visibility
- Resource optimization
- Unified operational health
- Unified cross-account observability



Introducing CloudTrail Lake

CloudTrail Lake lets you query multiple event fields in your logs, across all regions, for auditing and analysis. Learn more

CloudTrail > Event history

Event history (50+) Info

Event history shows you the last 90 days of management events.

Lookup attributes

Read-only ▾ false

Custom

< 1 2 ... >

□	Event name	Event time	User name	Event source	Resource type	R
□	CreateLogGroup	May 17, 2023, 08:13:18 (UTC-07...	Alex_E	logs.amazonaws.com	-	-
□	SendSSHPublicKey	May 17, 2023, 07:55:39 (UTC-07...	Alex_E	ec2-instance-connect.amazonaws.com	AWS::EC2::Instance	i-
□	PutMetricAlarm	May 17, 2023, 07:30:56 (UTC-07...	Alex_E	monitoring.amazonaws.com	AWS::CloudWatch::Alarm	V
□	PutMetricAlarm	May 17, 2023, 07:26:38 (UTC-07...	Alex_E	monitoring.amazonaws.com	AWS::CloudWatch::Alarm	V
□	ConsoleLogin	May 17, 2023, 07:18:28 (UTC-07...	Alex_E	signin.amazonaws.com	-	-
□	SendSSHPublicKey	May 17, 2023, 07:01:35 (UTC-07...	Dericus_H	ec2-instance-connect.amazonaws.com	AWS::EC2::Instance	i-
□	PutEvaluations	May 17, 2023, 04:14:34 (UTC-07...	configLambdaExec...	config.amazonaws.com	-	-

0 / 5 events selected

Dashboard

The AWS CloudTrail dashboard displays an overview of your trails and recent events. If you have CloudTrail Insights enabled on at least one trail, and CloudTrail has logged any Insights events, the Insights area shows the five most recent Insights events. The **Event history** area shows you the most recent management events that have occurred, even if you do not have trails configured.

From the dashboard, you can open the **Event history**, **Insights**, or **Trails** pages to see more of your events and trails. You can also start creating a trail, or enable Insights events.

Learn more

Creating a trail

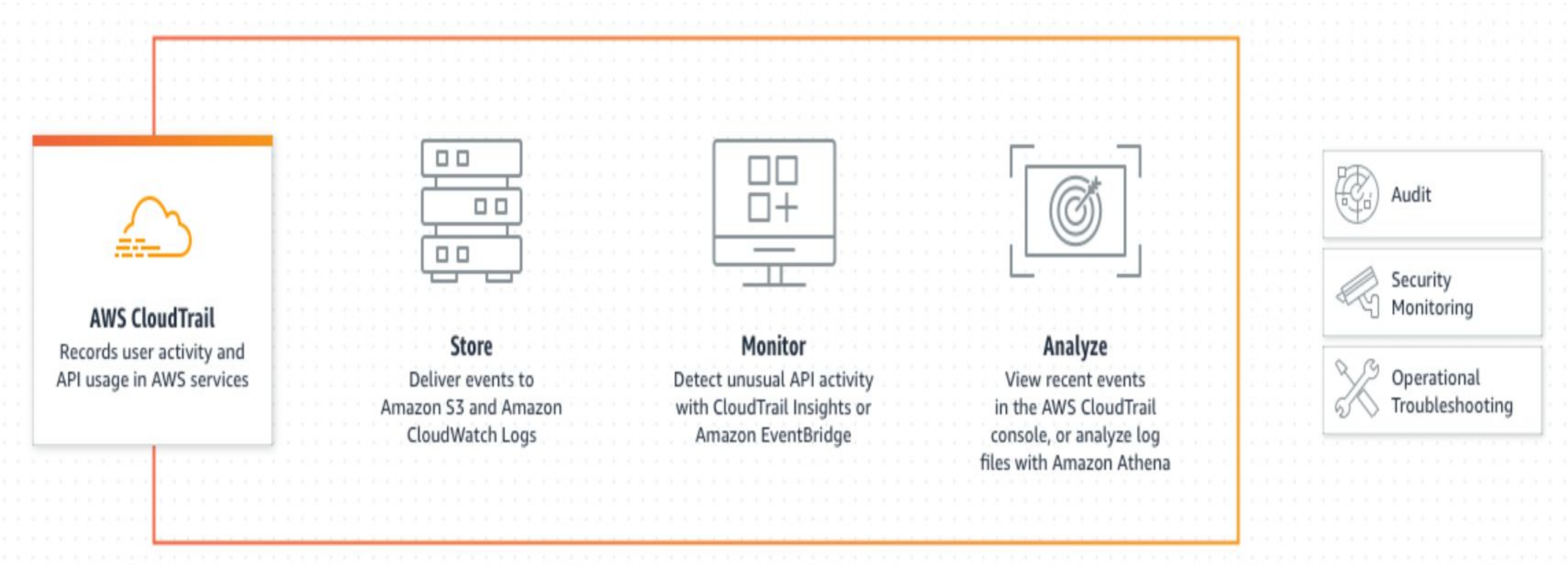
Logging Insights events for trails

Viewing events with CloudTrail event history

Viewing CloudTrail Insights events

© 2023, Amazon Web Services, Inc. or its affiliates.

AWS CloudTrail



AWS CloudTrail

Records user activity and API usage in AWS services

Store

Deliver events to Amazon S3 and Amazon CloudWatch Logs

Monitor

Detect unusual API activity with CloudTrail Insights or Amazon EventBridge

Analyze

View recent events in the AWS CloudTrail console, or analyze log files with Amazon Athena

Audit

Security Monitoring

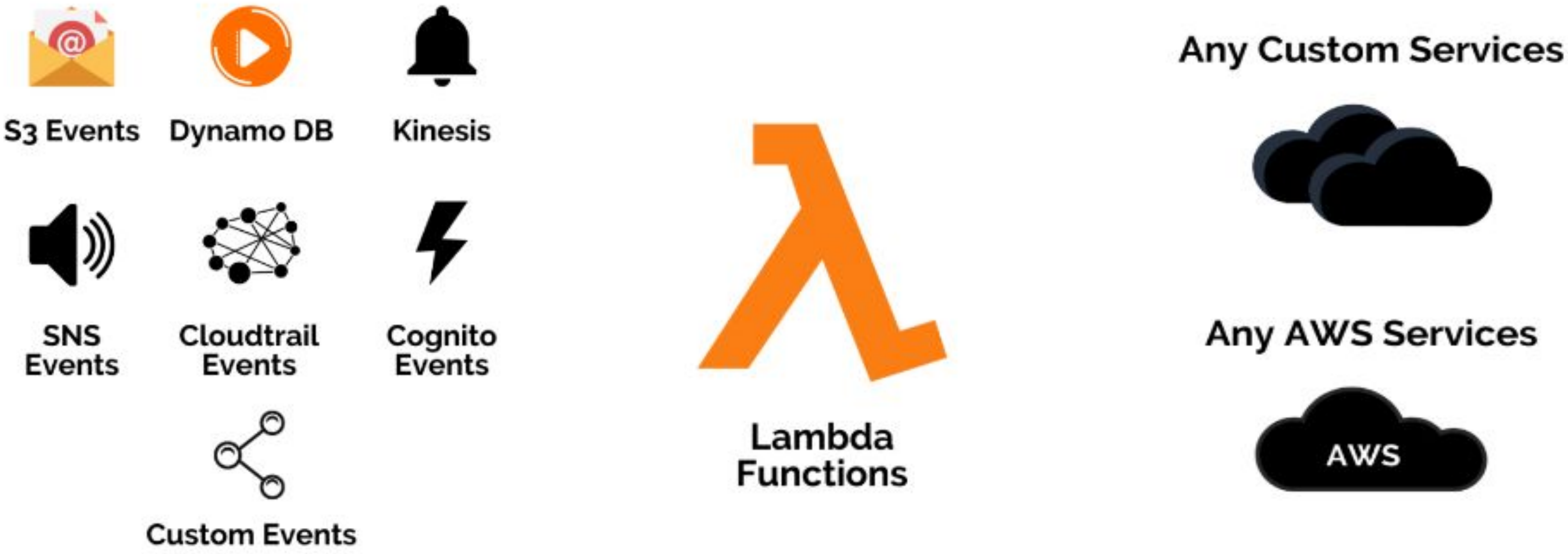
Operational Troubleshooting

AWS Lambda

Invoked in Response to the Events

Execute Only When Needed, Automatic Scale

Access Any Service



S3 Events

Dynamo DB

Kinesis

SNS Events

Cloudtrail Events

Cognito Events

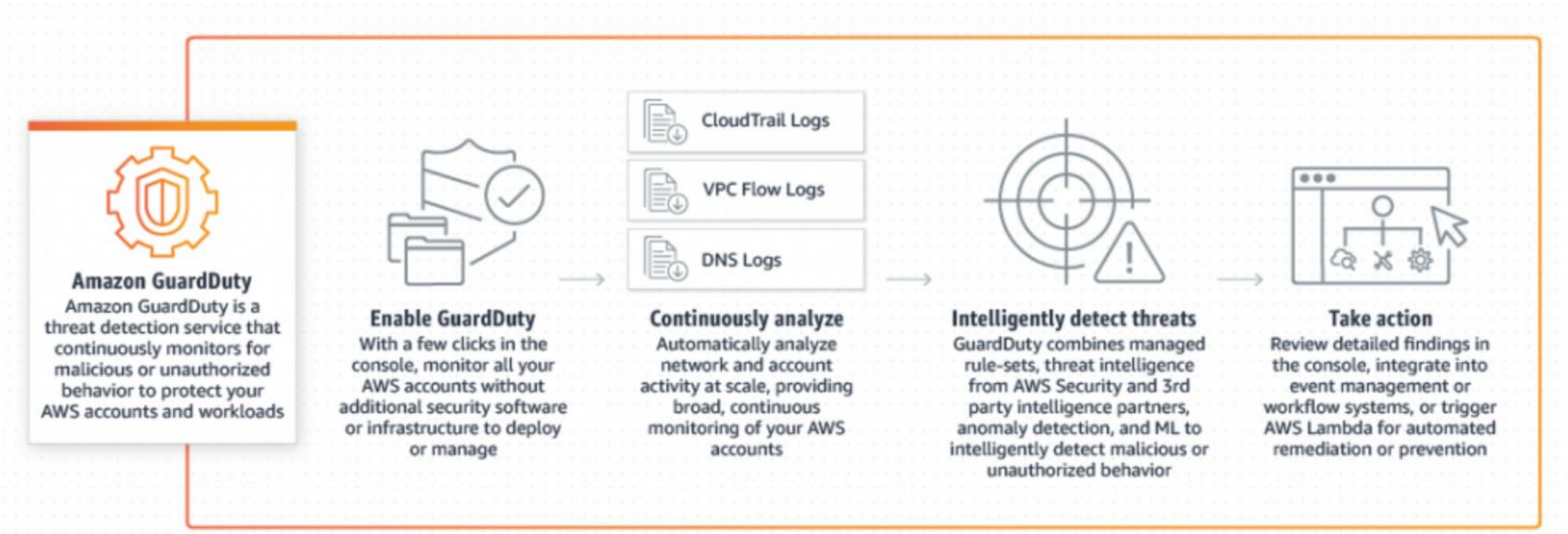
Custom Events

Lambda Functions

Any Custom Services

Any AWS Services

AWS GuardDuty



Amazon GuardDuty
Amazon GuardDuty is a threat detection service that continuously monitors for malicious or unauthorized behavior to protect your AWS accounts and workloads

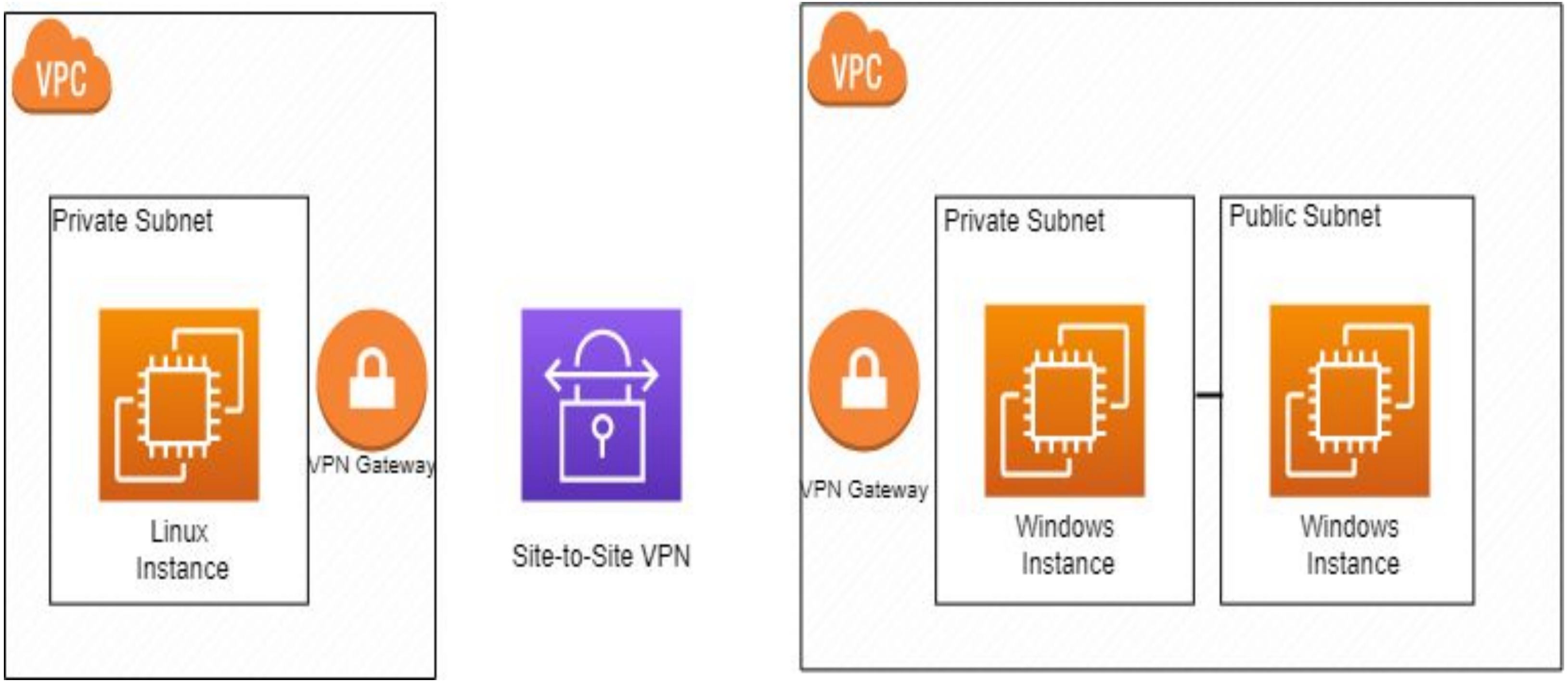
Enable GuardDuty
With a few clicks in the console, monitor all your AWS accounts without additional security software or infrastructure to deploy or manage

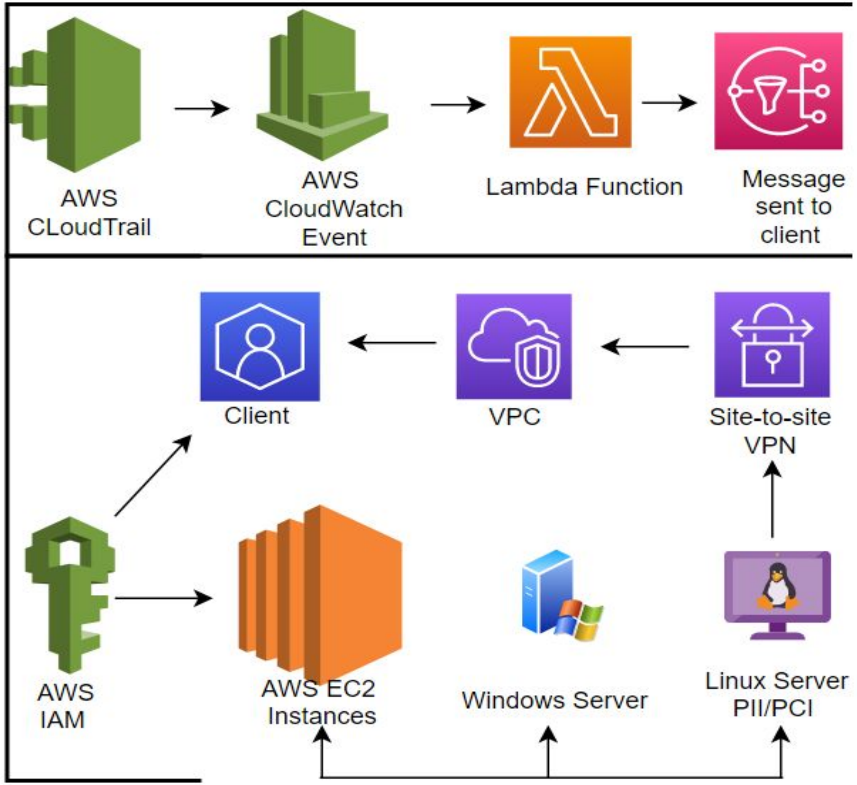
Continuously analyze
Automatically analyze network and account activity at scale, providing broad, continuous monitoring of your AWS accounts

Intelligently detect threats
GuardDuty combines managed rule-sets, threat intelligence from AWS Security and 3rd party intelligence partners, anomaly detection, and ML to intelligently detect malicious or unauthorized behavior

Take action
Review detailed findings in the console, integrate into event management or workflow systems, or trigger AWS Lambda for automated remediation or prevention

Quick View


VPC
Private Subnet
Linux Instance
VPN Gateway
Site-to-Site VPN
VPC
VPN Gateway
Private Subnet
Windows Instance
Public Subnet
Windows Instance


AWS CLoudTrail
AWS CloudWatch Event
Lambda Function
Message sent to client
Client
VPC
Site-to-site VPN
AWS IAM
AWS EC2 Instances
Windows Server
Linux Server PII/PCI

Demo!

Resources & Thanks

We would like to thank the 401 cohort, to include staff, instructors, TA and peers for collectively helping us grow and learn and all the family members who support us!

Lambda Functions Trello GitHub Windows Server aws Linux

Questions?