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
» SECURITY «
Dericus Horner
Dylan Dempsey
Anthony Wall
Geneva Knott
Alexander Echols

Dylan Dempsey

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

Dylan Dempsey | LinkedIn

Alexander Echols

- Co Founder of Cyber Guardians
- Cybersecurity Professional
- Physical penetration tester
- ITF+ Certified
- 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 LinkedIn

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

Anthony G Wall

-Persistent and Goal Oriented

- Former USMC Infantry team leader

- Licensed and registered Loan officer

- CompTIA ITF+ Certified

- Aspiring cyber security professional

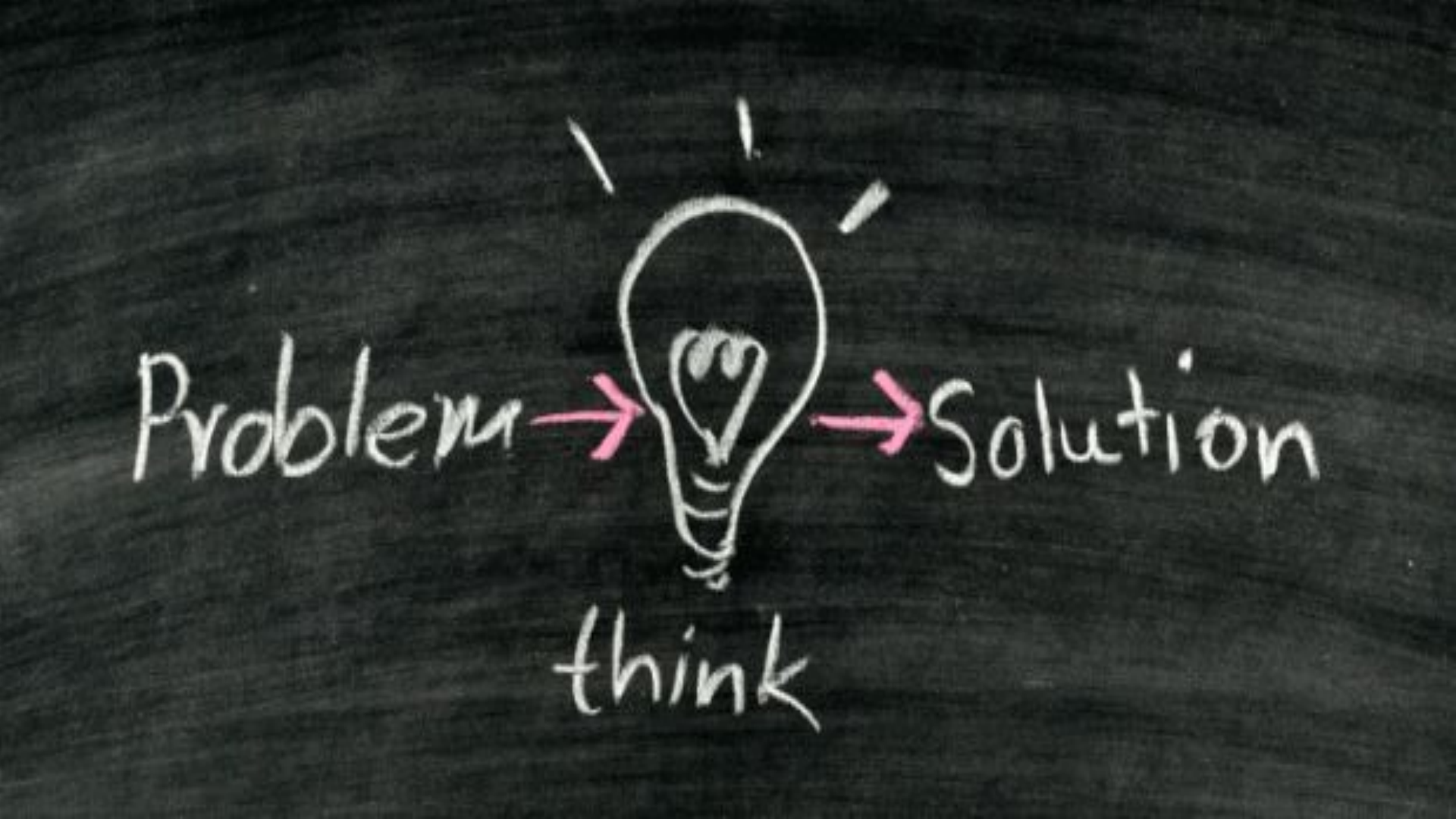
Scan to connect with me on Linkedin:

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

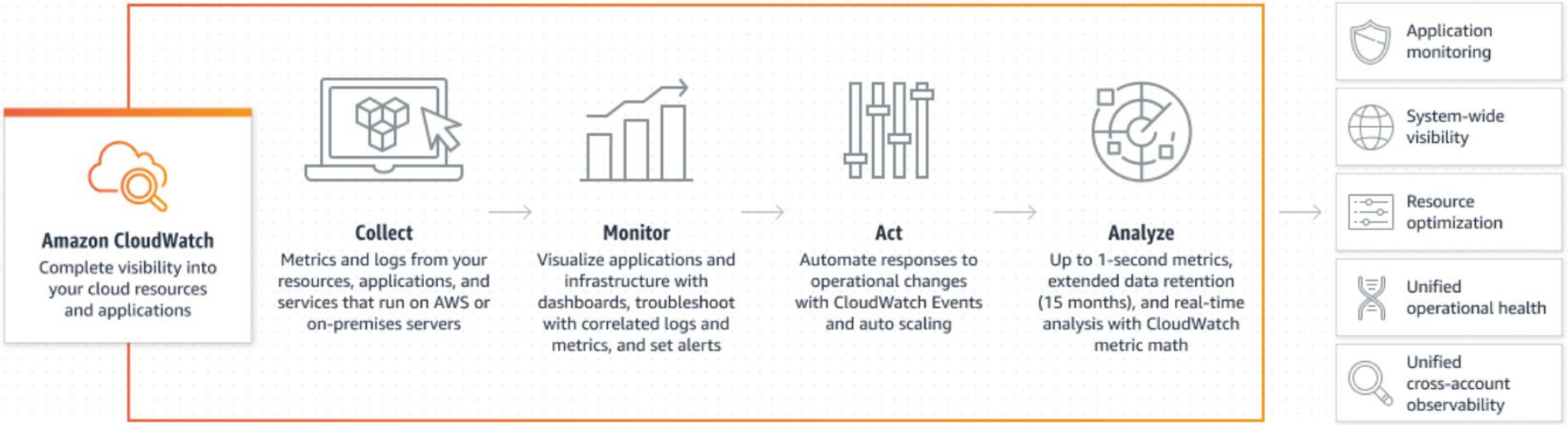
How we Met Compliance?

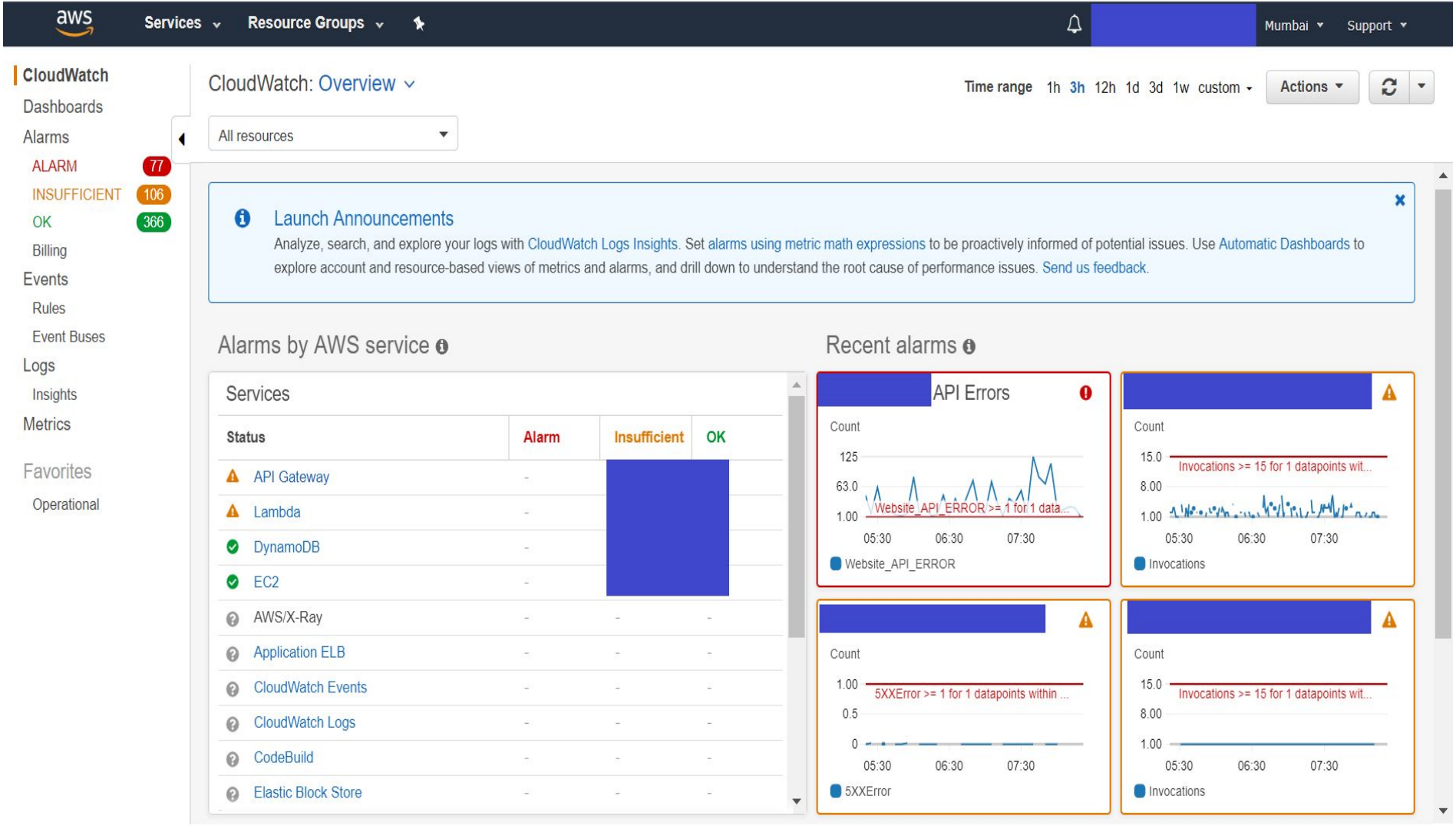
- CIS-compliant Windows Server DC hosted on a private subnet of a VPC and accessible only via VPN tunneling
- CIS-compliant Data Server

Security systems requirements

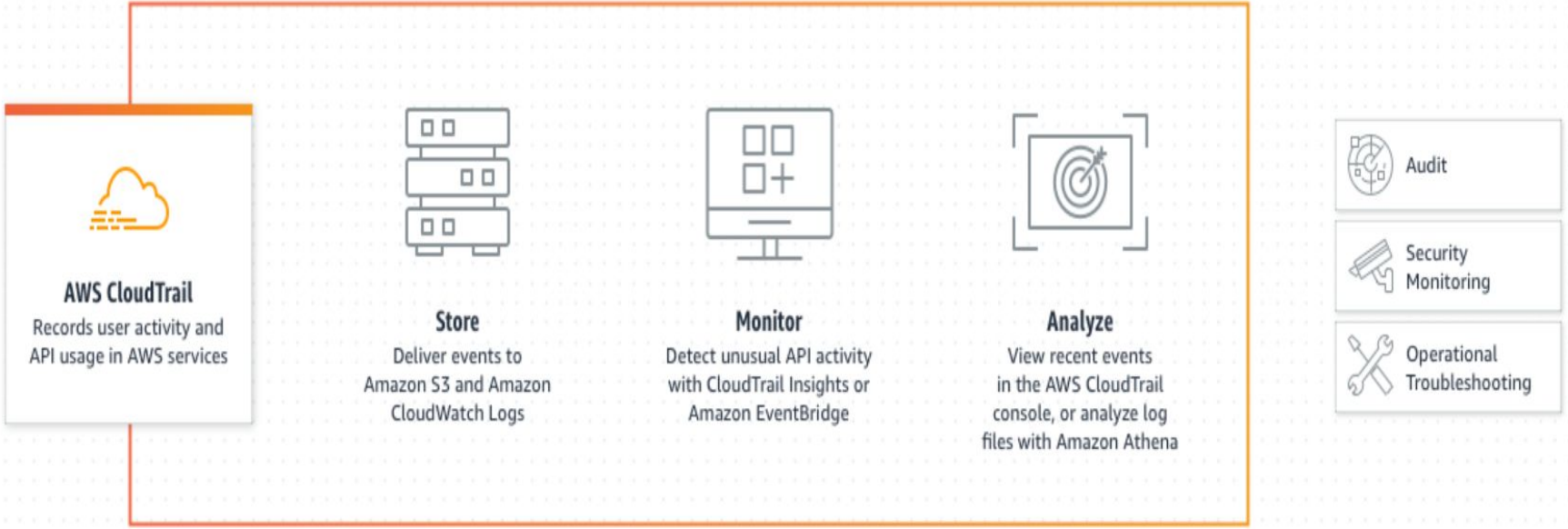
- Identity and Access Management (IAM)
- Network and Infrastructure Security
- Data Protection and Encryption
- Security Monitoring and Incident Response
- Security Auditing and Compliance
- Vulnerability Management and Patching
- Secure Configuration Management

AWS CloudWatch




aws
Services
Resource Groups
Mumbai
Support
CloudWatch
Dashboards
Alarms
ALARM 77
INSUFFICIENT 106
OK 366
Billing
Events
Rules
Event Buses
Logs
Insights
Metrics
Favorites
Operational
CloudWatch: Overview
All resources
Time range 1h 3h 12h 1d 3d 1w custom
Actions
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
Lambda
DynamoDB
EC2
AWS/X-Ray
Application ELB
CloudWatch Events
CloudWatch Logs
CodeBuild
Elastic Block Store
Recent alarms
API Errors
Count
125
63.0
1.00
Website_API_ERROR >= 1 for 1 data...
05:30
06:30
07:30
Website_API_ERROR
Count
15.0
8.00
1.00
Invocations >= 15 for 1 datapoints wit...
05:30
06:30
07:30
Invocations
Count
1.00
0.5
0
5XXError >= 1 for 1 datapoints within ...
05:30
06:30
07:30
5XXError
Count
15.0
8.00
1.00
Invocations >= 15 for 1 datapoints wit...
05:30
06:30
07:30
Invocations

AWS CloudTrail



CloudTrail
Dashboard
Event history
Insights
Lake
Query
Event data stores
Integrations New
Trails
Settings
Pricing
Documentation
Forums
FAQs

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.

Download events | Create Athena table

Lookup attributes

Read-only | false | Custom | 1 2 ...

Event name	Event time	User name	Event source	Resource type
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
PutMetricAlarm	May 17, 2023, 07:30:56 (UTC-07...	Alex_E	monitoring.amazonaws.com	AWS::CloudWatch::Alarm
PutMetricAlarm	May 17, 2023, 07:26:38 (UTC-07...	Alex_E	monitoring.amazonaws.com	AWS::CloudWatch::Alarm
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
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. Privacy Terms Cookie preferences

AWS Lambda

Invoked in Response to the Events

S3 Events

Dynamo DB

Kinesis

SNS Events

Cloudtrail Events

Cognito Events

Custom Events

Execute Only When Needed, Automatic Scale

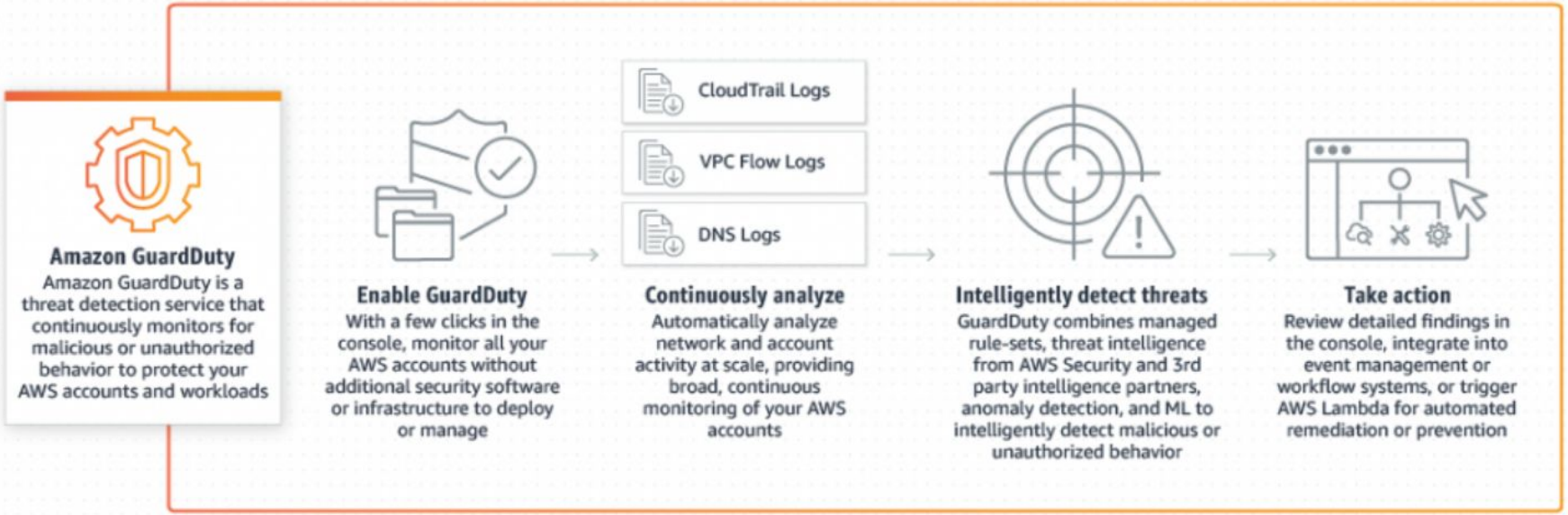
Lambda Functions

Access Any Service

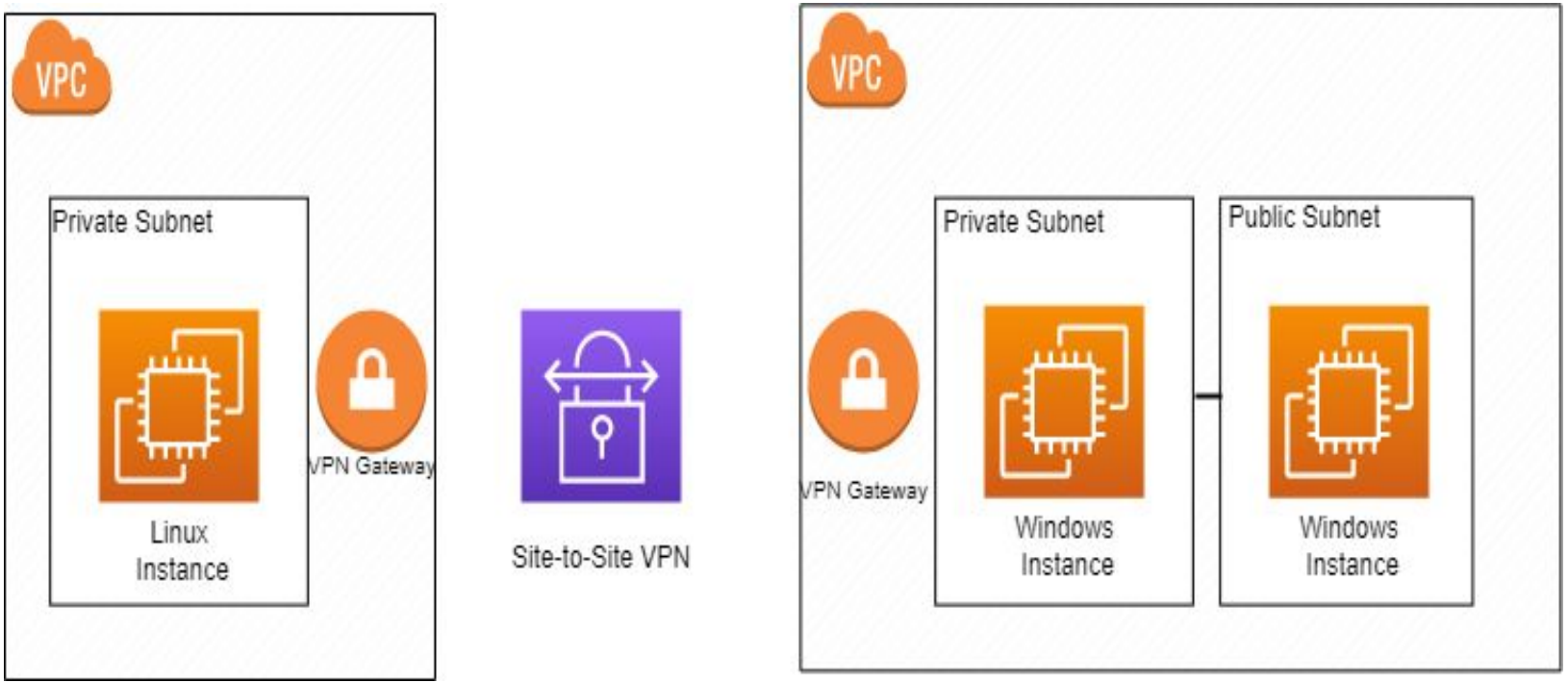
Any Custom Services

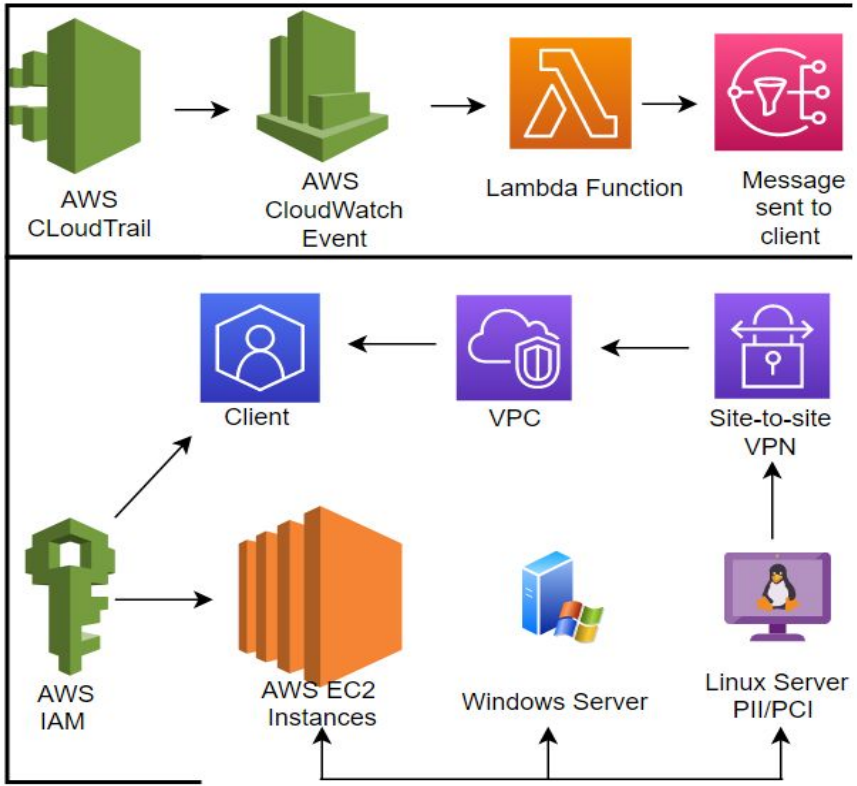
Any AWS Services

AWS GuardDuty



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!

Questions