SEC219-L

Continuous security improvement: Strategies and tactics

Steve Schmidt
Vice President and Chief Information Security Officer
Amazon Web Services

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

“There was a click, and the entire Universe was there in the box . . .”



Douglas Adams

Author, Hitchhiker’s Guide to the Galaxy

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Strategy: Lower the friction of security

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon GuardDuty

AWS Security Hub

Amazon Detective



Amazon GuardDuty

GuardDuty is a threat-detection service that uses machine learning, anomaly detection, and integrated threat intelligence to identify and prioritize potential threats

- Identify malicious and highly suspicious activity
- Protects AWS accounts, workloads, and data stored in Amazon S3

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

GuardDuty for Amazon S3 protection

Detect malicious and suspicious activities

With a single click, gain Amazon S3 protection



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Security Hub

CENTRALLY VIEW AND MANAGE SECURITY ALERTS AND AUTOMATE SECURITY CHECKS



Centralize across accounts, aggregate across Regions, and prioritize findings



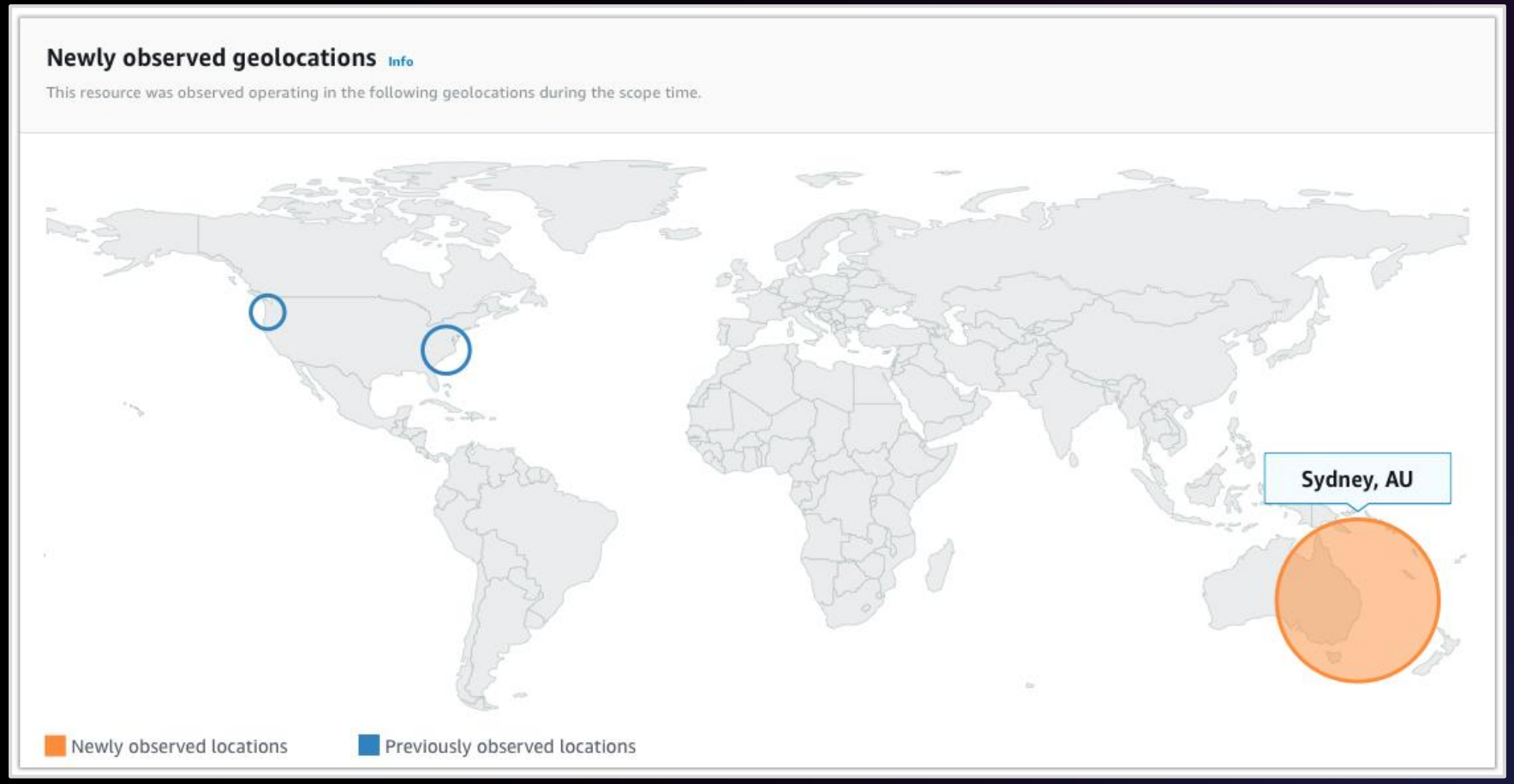
View security and compliance posture against key standards



Take automated or custom action on findings

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon Detective



Analyze and visualize security data to rapidly get to the root cause of potential security issues

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Strategy:
Remain focused on *tangible* ways to make customers safer

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Tactic

Cybersecurity Awareness Training

https://learnsecurity.amazon.com



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Tactic: Incident Manager

TRIGGER, NOTIFY, RESOLVE WITH AUTOMATION, AND REPORT FINDINGS IN AWS SYSTEMS MANAGER

- Create and automate response plans initiated by Amazon CloudWatch alarms or Amazon EventBridge events
- Define runbooks through AWS Systems Manager Automation to automate critical response and provide steps to first responders
- Automatically connect the correct people; engage through different contact methods and escalate through responders ensuring visibility and active participation during incidents

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Don’t let your security culture become “other”

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

"All opinions are not equal. Some are a very great deal more robust, sophisticated and well supported in logic . . ."



Douglas Adams

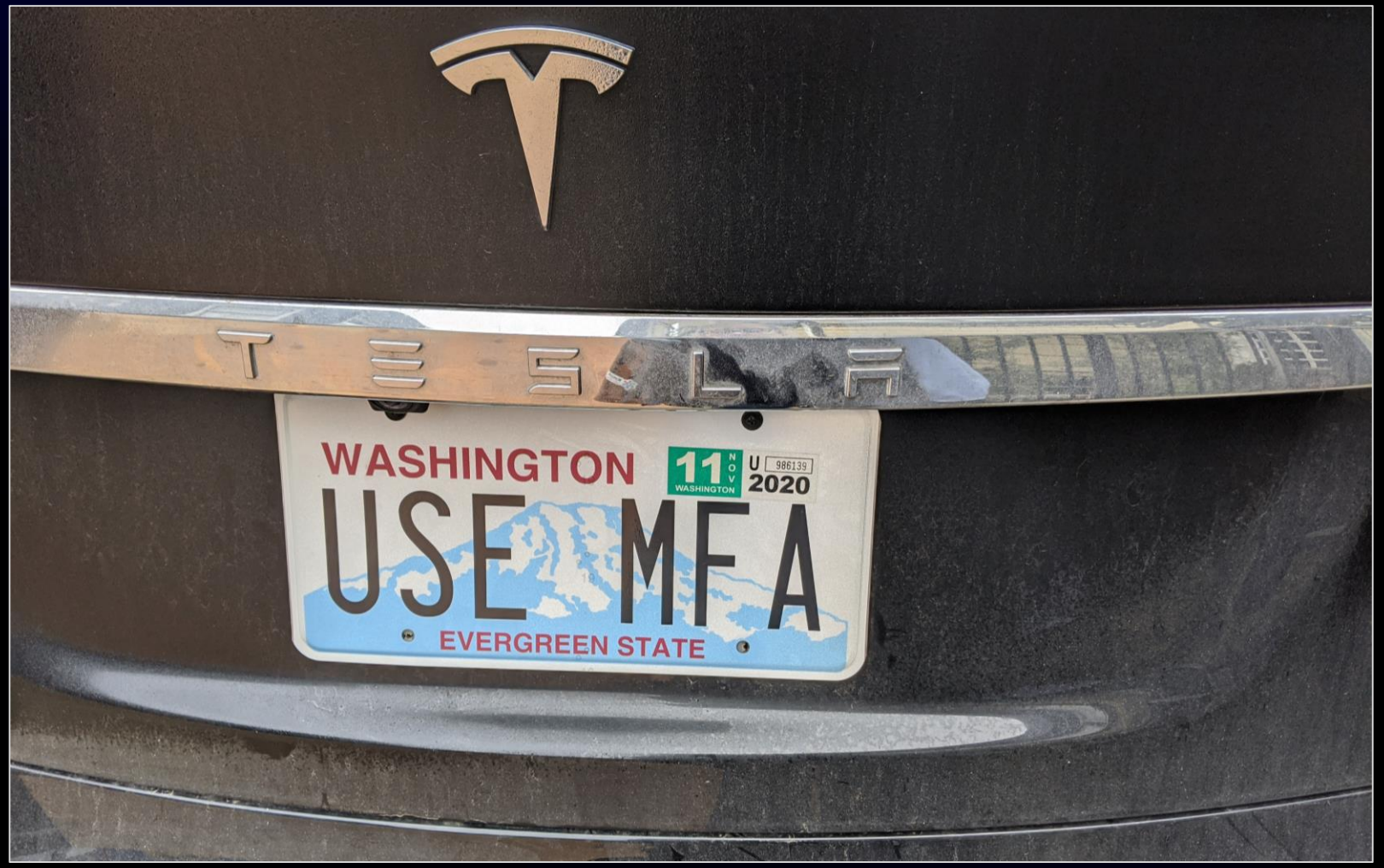
Author, *The Salmon of Doubt*

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Identity and access management

Sarah Cecchetti
Principal Product Manager
Amazon Web Services

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

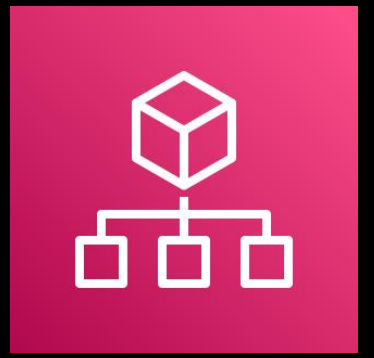


MFA

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Guidance

Use AWS Organizations and AWS Single Sign-On (SSO)





© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Guidance

Builder tools help establish your data perimeter

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS IAM Access Analyzer

Access Analyzer

Monitor access to resources

How it works



1 Create an analyzer

You can set the scope for the analyzer to an organization or an AWS account. This is your zone of trust. The analyzer scans all of the supported resources within your zone of trust.



2 Review active findings

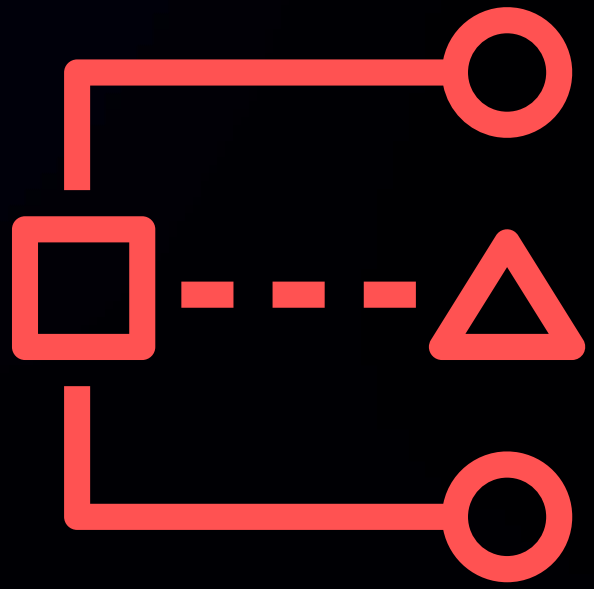
When Access Analyzer finds a policy that allows access to a resource from outside of your zone of trust, it generates an active finding. Findings include details about the access so that you can take action.



3 Take action

If the access is intended, you can archive the finding so that you can focus on reviewing active findings. If the access is not intended, you can resolve the finding by modifying the policy to remove access to the resource.

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Verify findings with IAM Access Analyzer

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Guidance

Restrict public and cross-account access

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Guidance

Validate your policies

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

Sarah Cecchetti

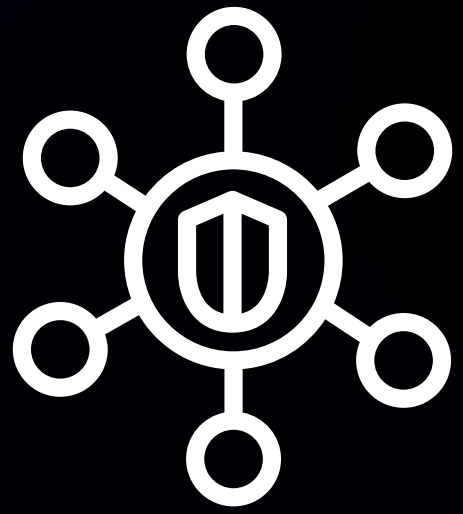
@AWSIdentity

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security services updates

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Updates

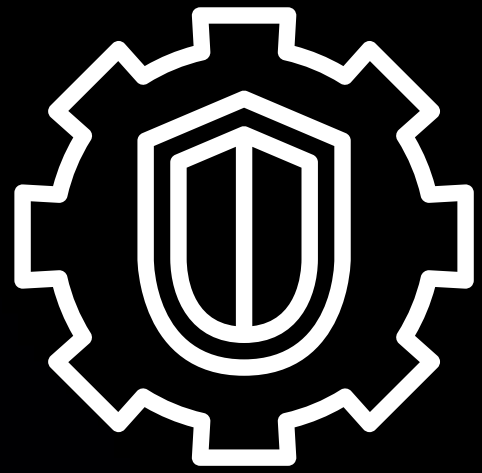


AWS Security Hub

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



+



Amazon Detective

Amazon GuardDuty

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

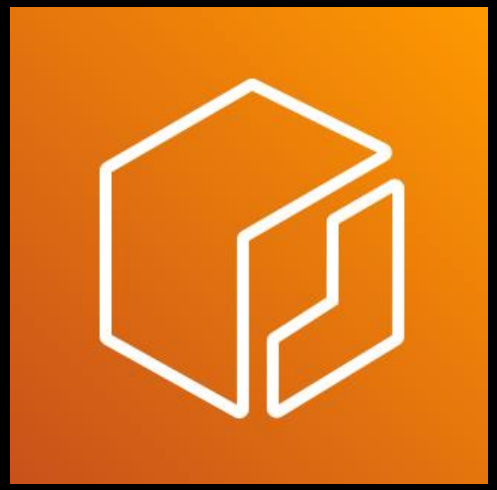
Launch: Automatic application layer DDoS mitigation

Automatic recommendation, testing, and deployment of custom AWS WAF rules for each incident

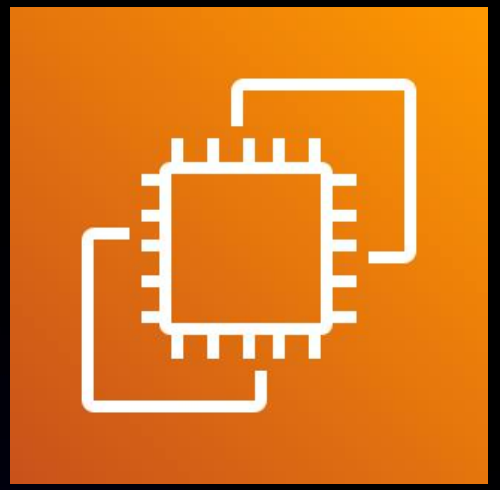
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Launch

Amazon Inspector







Amazon Elastic Container Registry (Amazon ECR)

Amazon Elastic Compute Cloud (Amazon EC2)

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Guidance

Update the alternate security contact across your AWS accounts for timely security notifications



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Guidance

Consider the Security Pillar of the AWS Well-Architected Framework



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security culture

Thomas Avant
Director
Amazon Web Services



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

“There is no problem so complicated that you can't find a very simple answer to it if you look at it right ...”



Douglas Adams

Author, *The Restaurant at the End of the Universe*

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

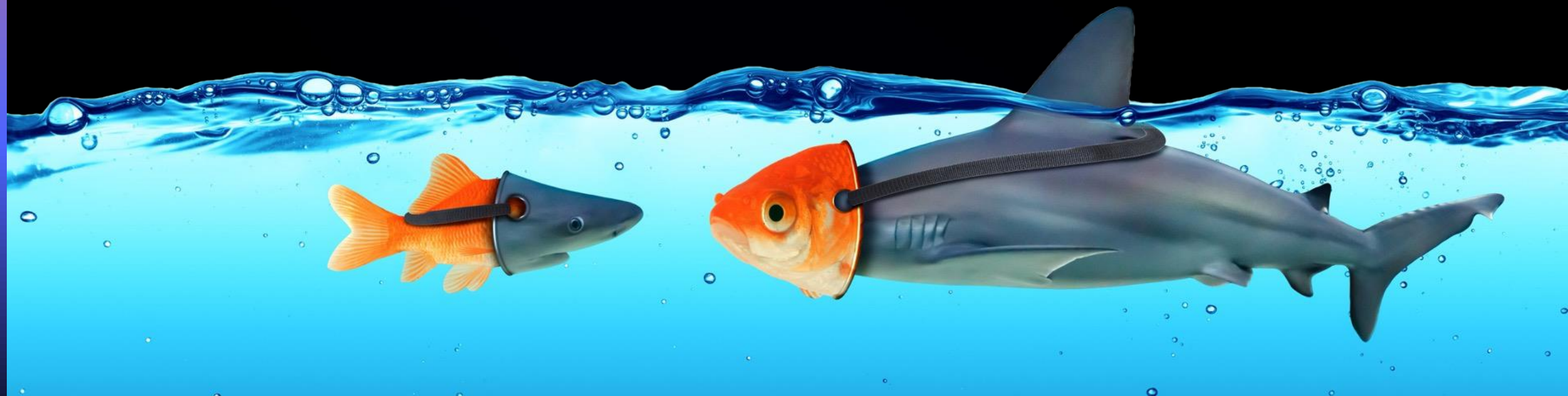
What my team does. . .



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Strategy

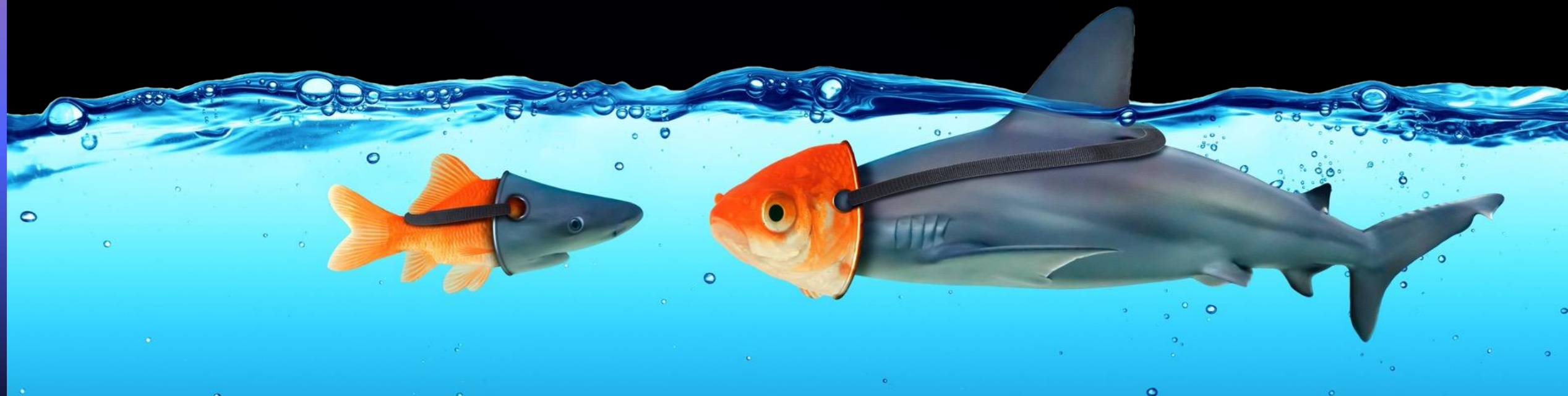
Security policies



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Strategy

Policies and people



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Strategy

Escalations – the right way



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Strategy

Culture – building trust



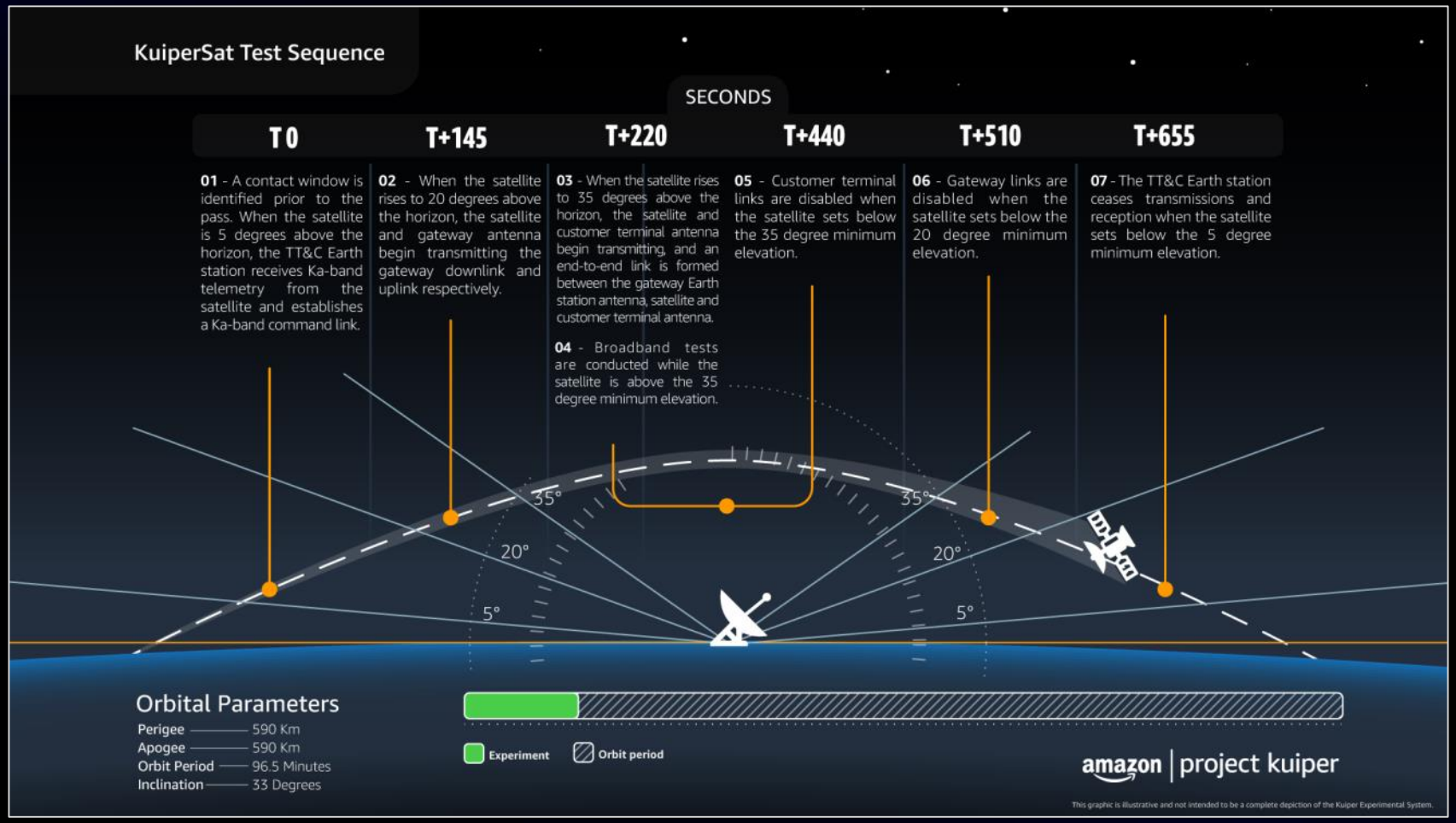
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Strategy

Access control increases and becomes more stringent as we get closer to customer data

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Future state



Low earth satellites

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

“What we really want is just stuff that works.”



Douglas Adams

Author, *Life, the Universe, and Everything*

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Containers and code

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Launches

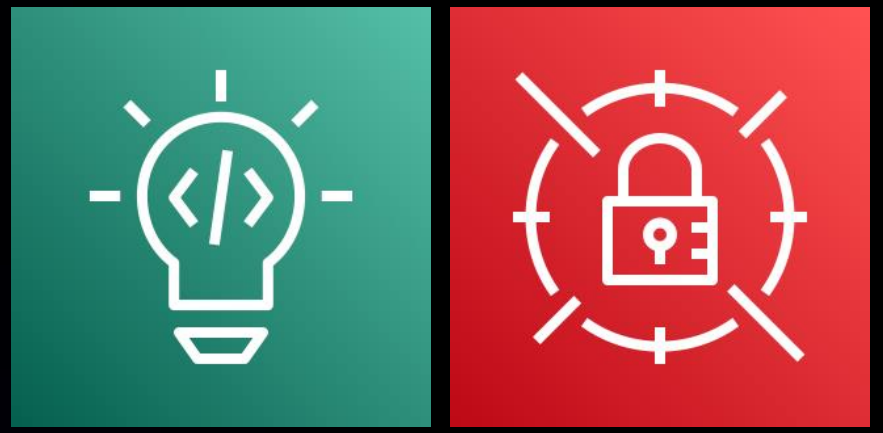
Amazon CodeGuru



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Launches

Amazon CodeGuru + AWS Secrets Manager



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Launch





Amazon GuardDuty and. . .

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Strategy







Containers need security tools too

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Where to enforce security boundaries? Philosophically, for AWS the answer is, “Yes.”



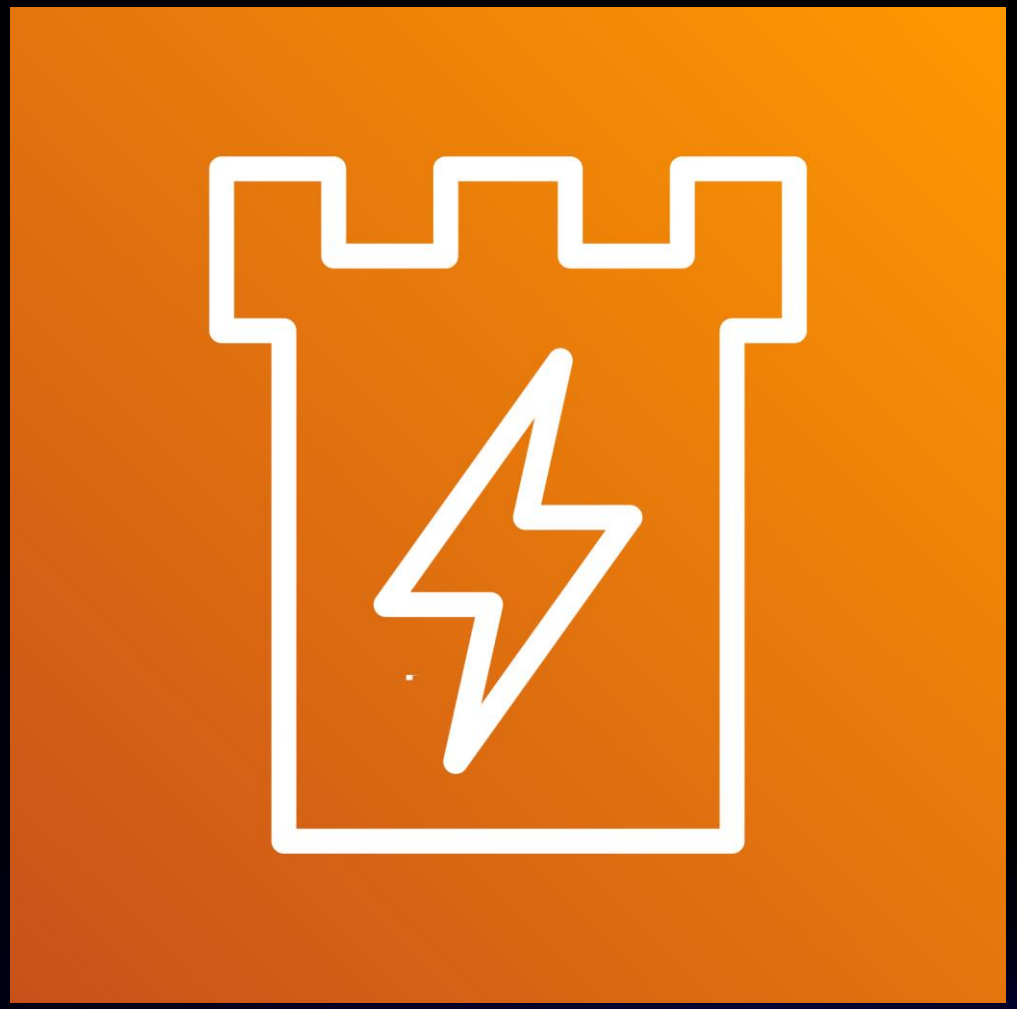
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Nitro System

Designed to provide strong isolation between AWS and the customer

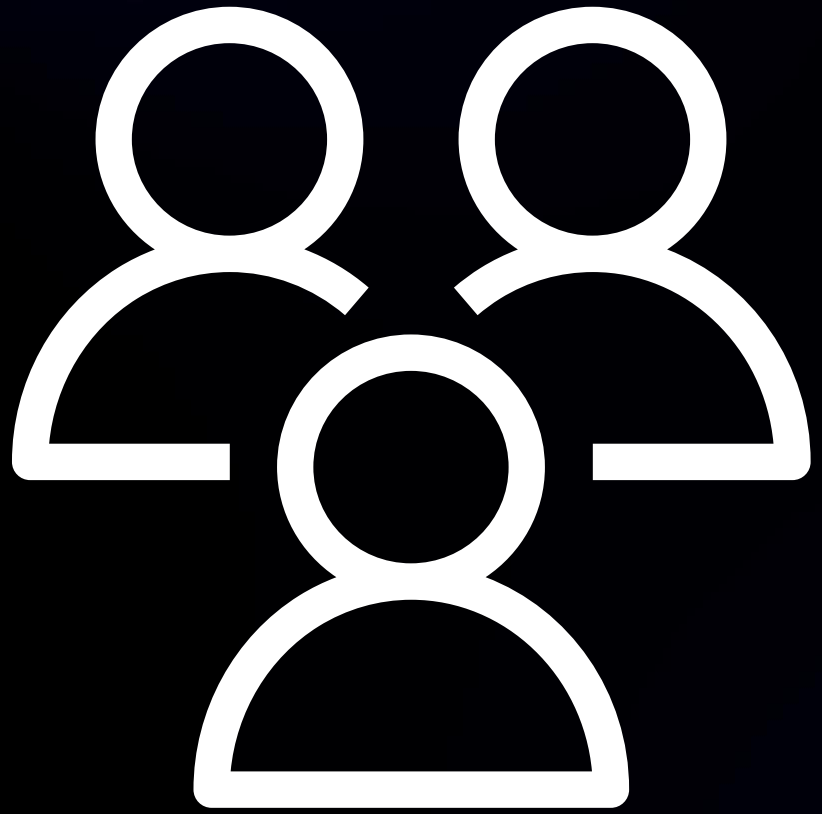
AWS Nitro Cards are physically separate from the hardware running customer instances

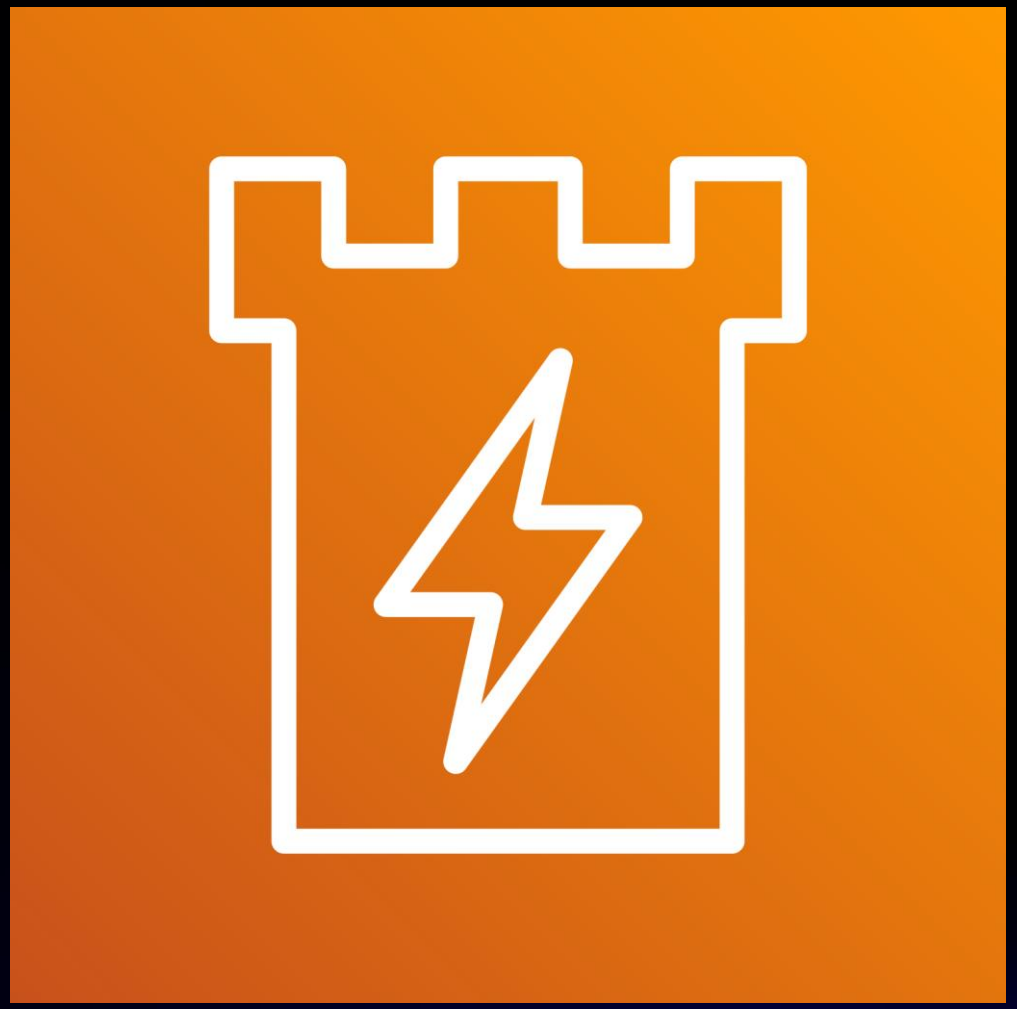
Dedicated CPU, memory, and hardware security chip



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Nitro Enclaves





© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Security Partners

Network and infrastructure security

ALERT LOGIC, APPGATE, ARMOR, Barracuda, Check Point, CISCO, ExtraHop, FORTINET, Guardicore, paloalto NETWORKS, PROTECTWISE, SKinfosec co.,ltd., SOPHOS, zscaler

Host and endpoint security

CROWDSTRIKE, SentinelOne, Symantec, TREND MICRO

Application security

Barracuda, Checkmarx, f5, imperva, pwc, VERACODE

Identity and access control

Auth0, CLOUDKNOX, CYBERARK, okta, onelogin, Ping Identity, SailPoint, SAVIYNT

Vulnerability and configuration analysis

bridgecrew, CloudHealth by vmware, ExtraHop, orca security, paloalto NETWORKS, Qualys., RAPID7, tenable, threat stack

Logging, monitoring, SIEM, threat detection, and analytics

ALIEN VAULT, LACEWORK, McAfee Together is power., SECURONIX Security Analytics. Delivered., splunk>, sumo logic

Data protection & encryption

CYBERARK, DataSunrise Data & Database Security, gemalto security to be free, HashiCorp, PRIVITAR, THALES, sonraí SECURITY

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Security Partners

Security engineering

8K Miles
accenture — High performance. Delivered.
AllCloud
>CMD SOLUTIONS
CLOUDZONE by matrix
CLOUDTEN
Deloitte.
ECCOii
escala 24x7
FOGHORN
GUIDEPOINT SECURITY
HELECLOUD
Hewlett Packard Enterprise
Itoc
lightstream
logicworks
NRI
pwc
Smartronix CLOUD ASSURED
Telefónica
VERSENT
direktgruppe
HITACHI Inspire the Next

Governance, risk, and compliance

Booz | Allen | Hamilton
Cloudgatech
cavirin
CloudCheckr
CloudHealth by vmware
CloudPassage
COALFIRE
DivvyCloud
ECCOii
NTT DATA Services
KindlyOps
OPTIV
pwc
ScaleSec
Telos
TREND MICRO
turbot
wirewheel
direktgruppe
stackArmor
KPMG
1Strategy
REPLY

Security operations and automation

Cloudreach
ECCOii
eCloud valley
IBM Security
Mphasis stelligent — The Next Applied
pwc
SAMSUNG SDS

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Managed Security Service Providers

Level 1 MSSP Competency Launch Partners



Marketplace MSSP Category Launch Sellers



aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

re:Inforce 2022
June 28 and 29 – Houston, TX



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

“Working out who you can trust and why is what a very large part of our brain has evolved to do.”



Douglas Adams

“How to stop worrying and learn to love the internet”
The Sunday Times, August 29, 1999

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.