AWS Security Best Practices

CSA SoCal Chapter Forum 2018

Mary Wang, CISSP, CEH, CNDA

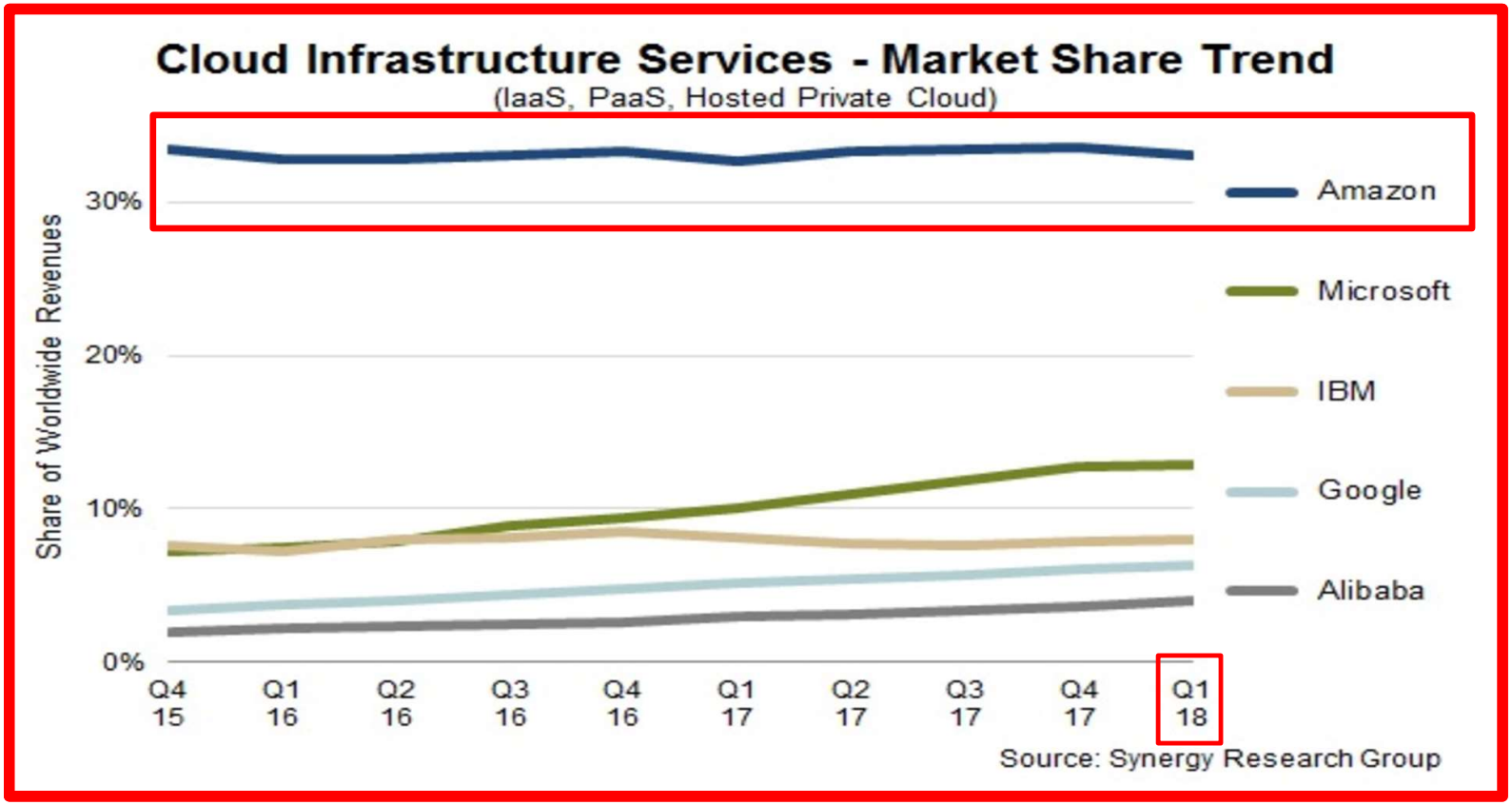
December 6, 2018

Why Am I Studying AWS Certified Solutions Architect (CSA) Associate Certification Exam?

NORTHROP GRUMMAN

Studying for : Amazon Web Service Certified Solutions Architect – Associate Certification

Cloud Market Share form Quarter 4 2015 – Quarter 1 2018



Three Cloud Computing Models

NORTHROP GRUMMAN

- All-in Cloud
  - Design and deploy all applications in a public cloud – using an AWS
    - New application in the cloud
    - Migrating existing applications to cloud
- Hybrid
  - Host some applications in the cloud
  - Host some applications at your own premises
    - Connect seamless together
  - Embrace cloud - the quickest way
  - Leave the legacy applications at the premises first

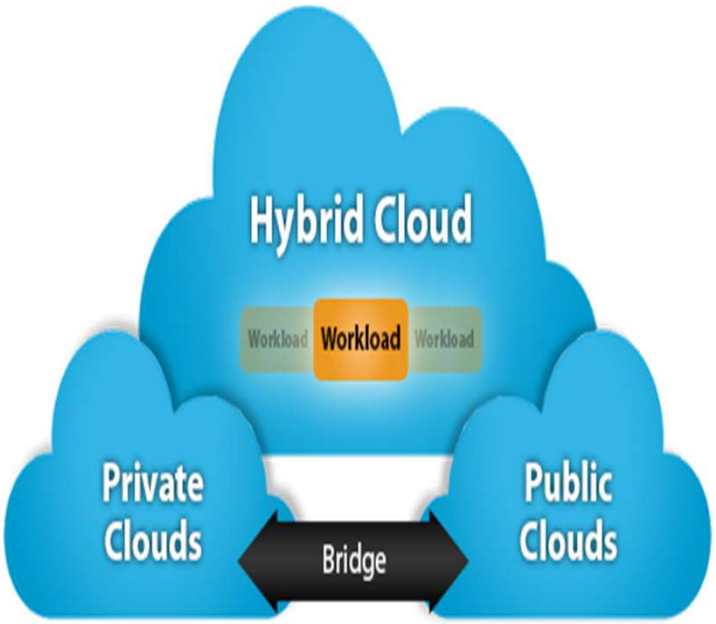


Image source: Rittal Encosures Blog https://blog.rittal.us/blog/hybrid-cloud-solutions-0

Three Cloud Computing Models (cont.)

NORTHROP GRUMMAN

- On-Premise or Private
  - Do get advantages of a public cloud (not all of them)
  - Segregate your resources and can meter them and charge back to business units
  - Establish a migration strategy journey – on premise data center with a implementation of cloud

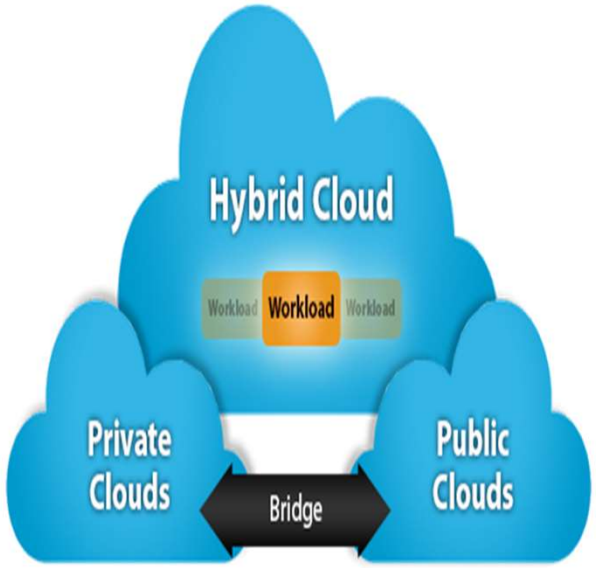
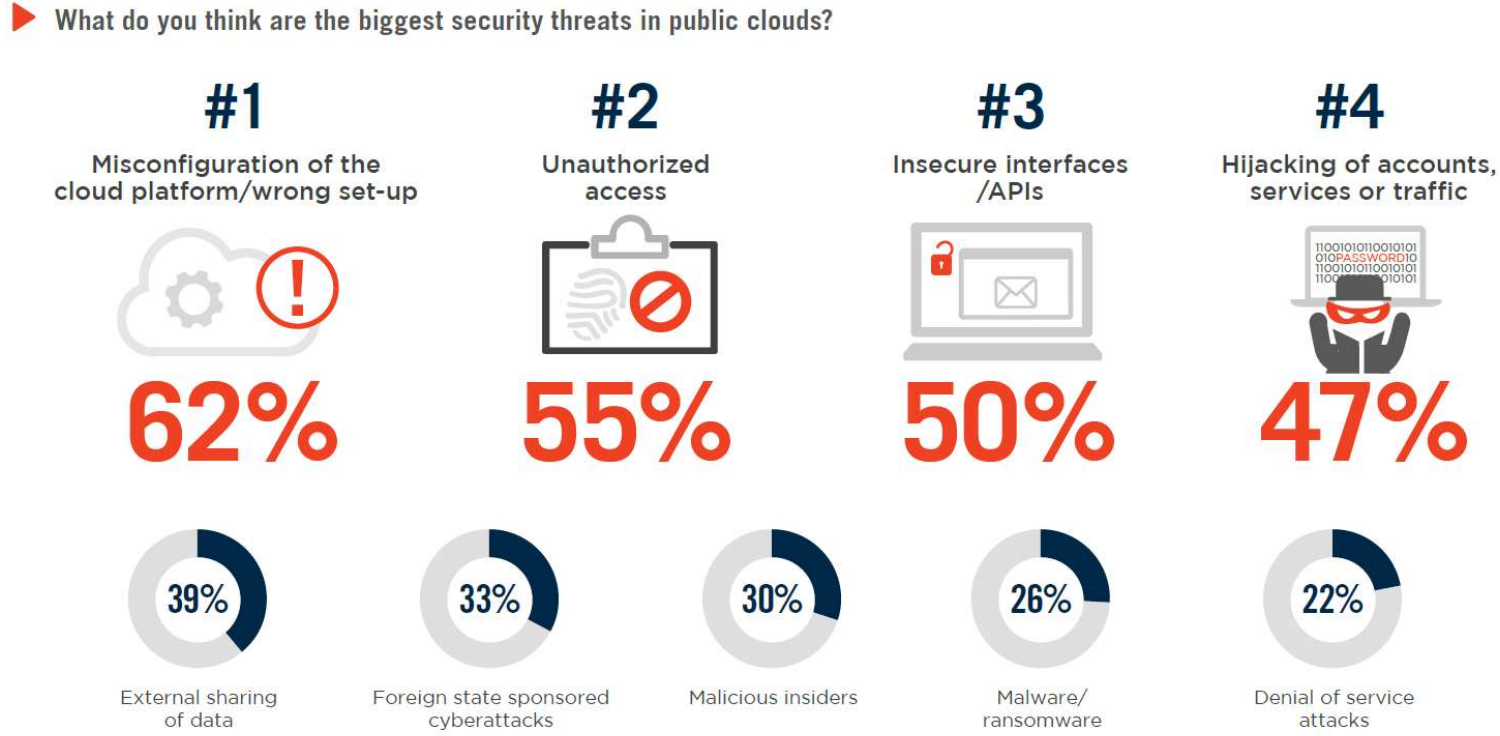


Image source: Rittal Encosures Blog https://blog.rittal.us/blog/hybrid-cloud-solutions-0

Security Concerns from 2018 Cloud Security Report



Source: 2018 Cloud Security Report from Securonix

AWS Shared Responsibility Model

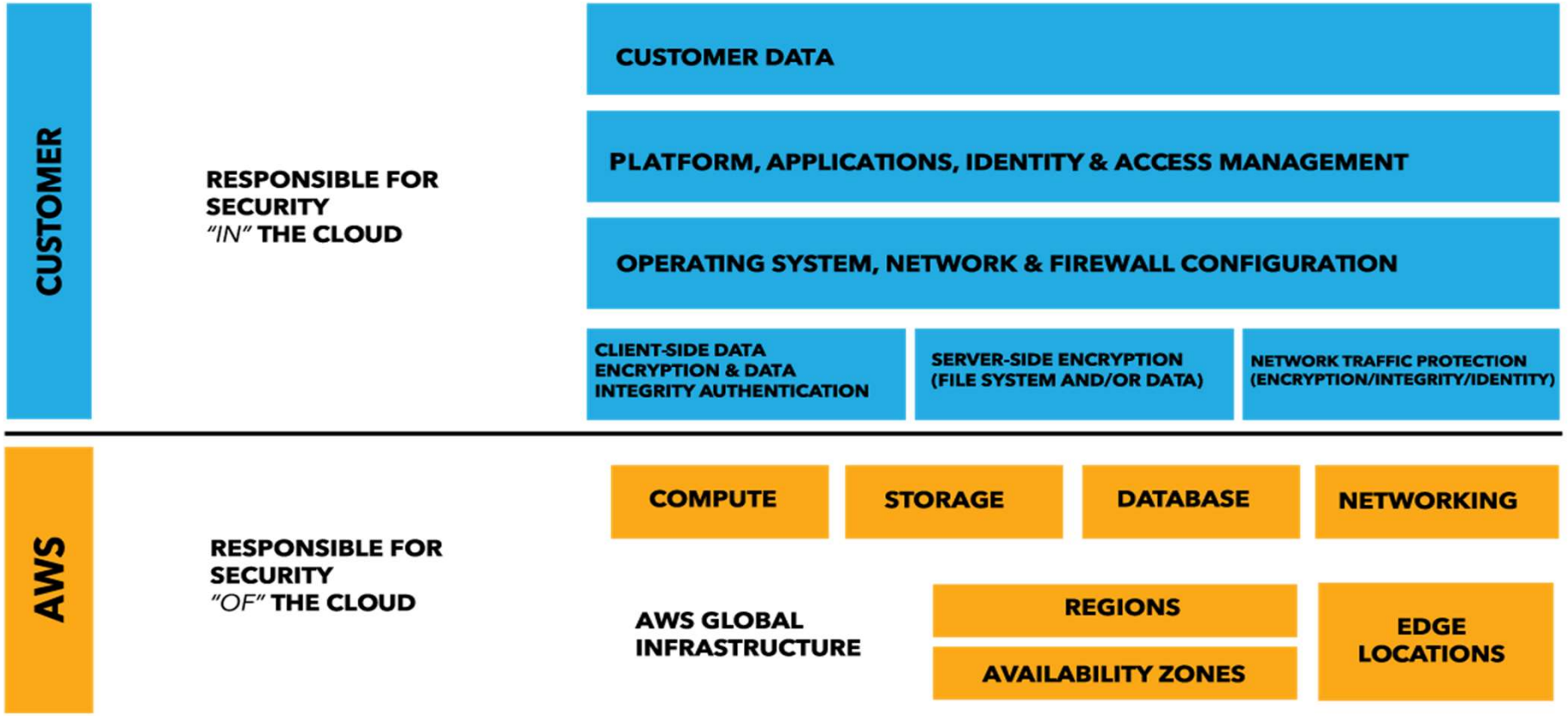


Image source: Amazon Shared Responsibility Model https://aws.amazon.com/compliance/shared-responsibility-model/

AWS Responsibility

NORTHROP GRUMMAN

- Physical security of data center
- Amazon EC2 security
  - Secure host operating systems
    - Customer has the full access or admin control over accounts, services and applications
    - AWS doesn't have any access rights to your instances or the guest OS
- Network security
- Configuration management - validate they are configured properly and all software are installed
- High available data center – all data centers are highly available at all times.
- Disk management – prevents customers from accessing each other's data
- Storage device decommissioning
  - Use DoD 5220.22-M and NIST 800-88
    - Data wiped and disks are degaussed and finally physically destroyed

Customer Responsibility

NORTHROP GRUMMAN

- Operating System (OS)
  - Management of the guest OS – OS is patched and has all security updates and bug fixes
- Application
  - Management of any application that you run on top of AWS
    - Encrypting data, managing application users and their privileges
    - Responsible for all security and compliance of the application
      - For example, if your application needs to be PCI compliant, you need to deploy al the steps for being PCI compliant from the application
- Firewall
  - Make sure to set up the proper firewalls at the OS level

Customer Responsibility (cont.)

NORTHROP GRUMMAN

- Network Configuration
  - For example, Amazon Virtual Private Cloud (VPC) gives the ability to run your private cloud, but you are still responsible for its configuration
- Service Configuration
  - What configurations are set on your systems
- Authentication and Account management
  - For both AWS users and application users

Best Practices (1) – Use Identity and Access Management (IAM)

NORTHROP GRUMMAN

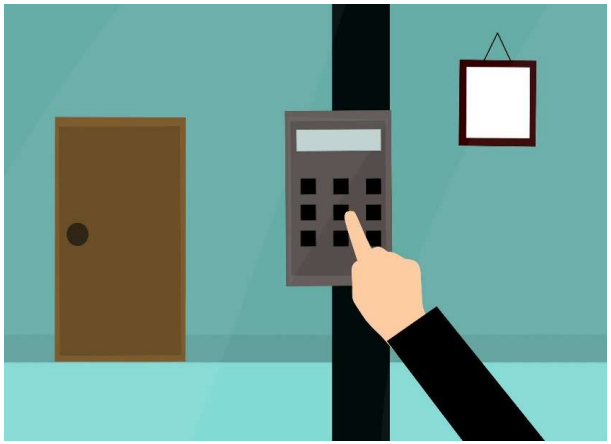
- Use Identity and Access management (IAM)
  - Make sure only those who are authorized can access the system
  - Can help in protecting the AWS account credentials
    - Provide fine-grained authorizations

Best Practices (2) - Use Infrastructure Protection

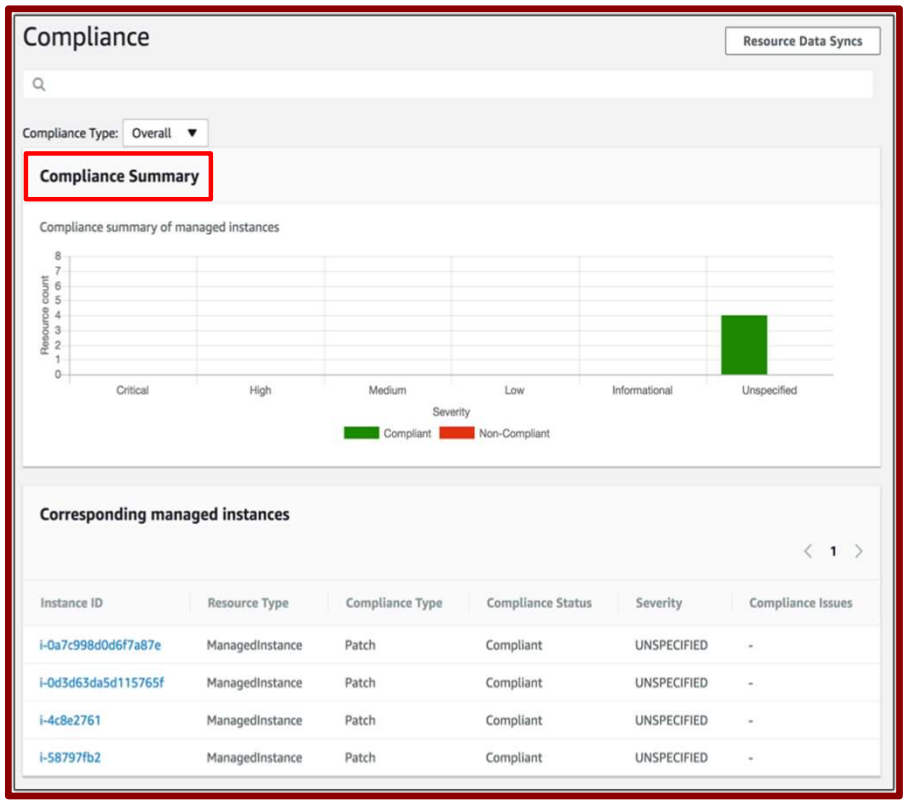
NORTHROP GRUMMAN

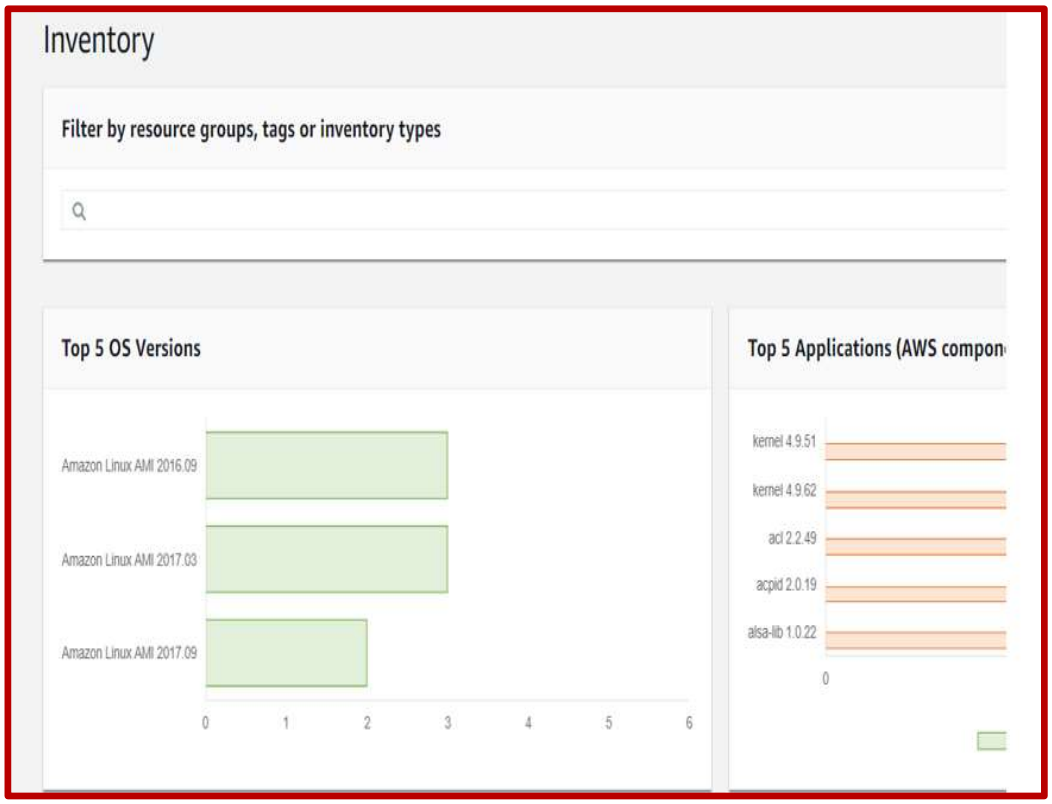
- Protect network and host level boundaries by applying appropriate configurations
  - Virtual private cloud, subnets, routing tables, network access control list (ACLs), gateways and security groups

- Use AWS Systems Manager
  - Give you the visibility and control of your infrastructure on AWS
  - View operational data from multiple AWS services
    - Monitoring
    - Trouble shooting



AWS System Manager Dashboard

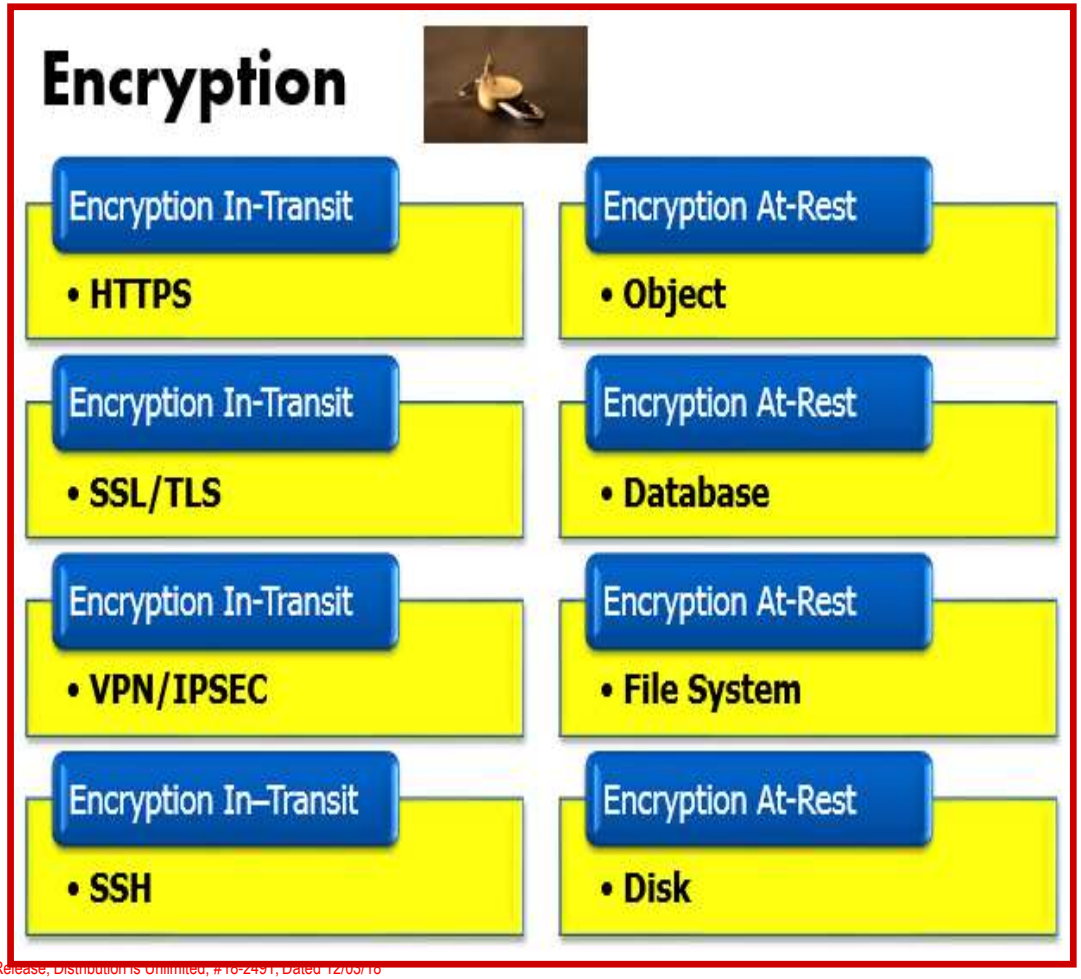




Best Practices (3) – Use Data Protection

NORTHROP GRUMMAN

- Data needs to be classified according to the level of sensitivity
- Meet regulatory compliance
  - Encryption in-Transit
  - Encryption at Rest
- Have backups, disaster strategy and replication



Best Practices (3) – Use Data Protection (cont.)

NORTHROP GRUMMAN

Volume Encryption

EBS Encryption, OS Tools

Object Encryption

S3 Server Side Encryption (SSE), S3 SSE with Customer Provided Keys, Client-side Encryption

Database Encryption

RDS MSSQL TDE, RDS ORACLE TDE/HSM, RDS MySQL KMS, RDS PostgreSQL KMS, Amazon Redshift Encryption

Best Practices (4) – Use Incident Response

NORTHROP GRUMMAN

- Have an incident response plan
- Should be able to respond to it quickly
- Routinely practice the incident response plan

Best Practices (5) – Use Detective Controls

Image Source: AWS

Amazon CloudWatch

AWS CloudTrail

AWS Config

Amazon Inspector

VPC FlowLogs

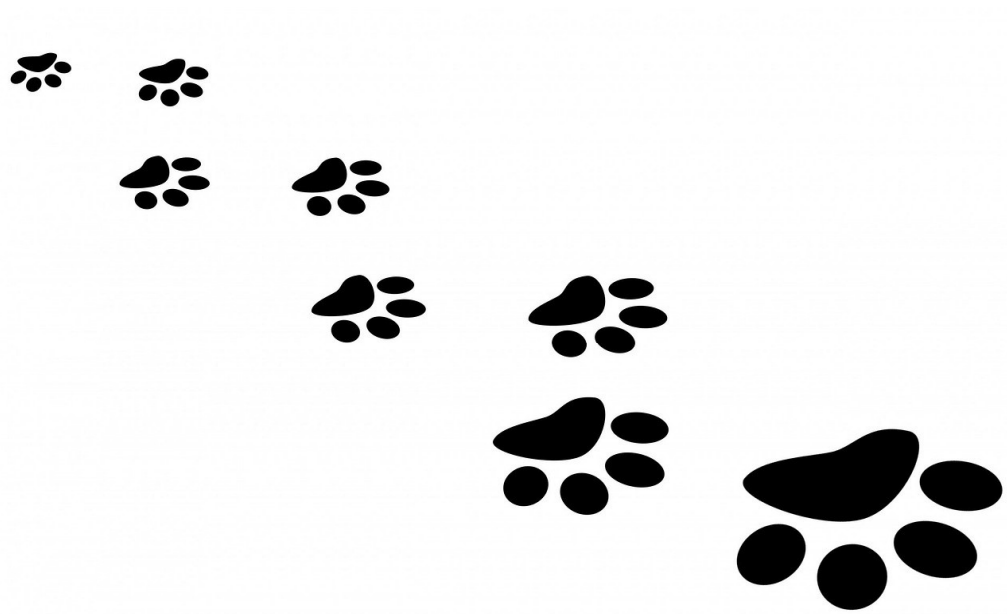
Amazon GuardDuty

Amazon Macie

Detective Controls 1 - CloudTrail

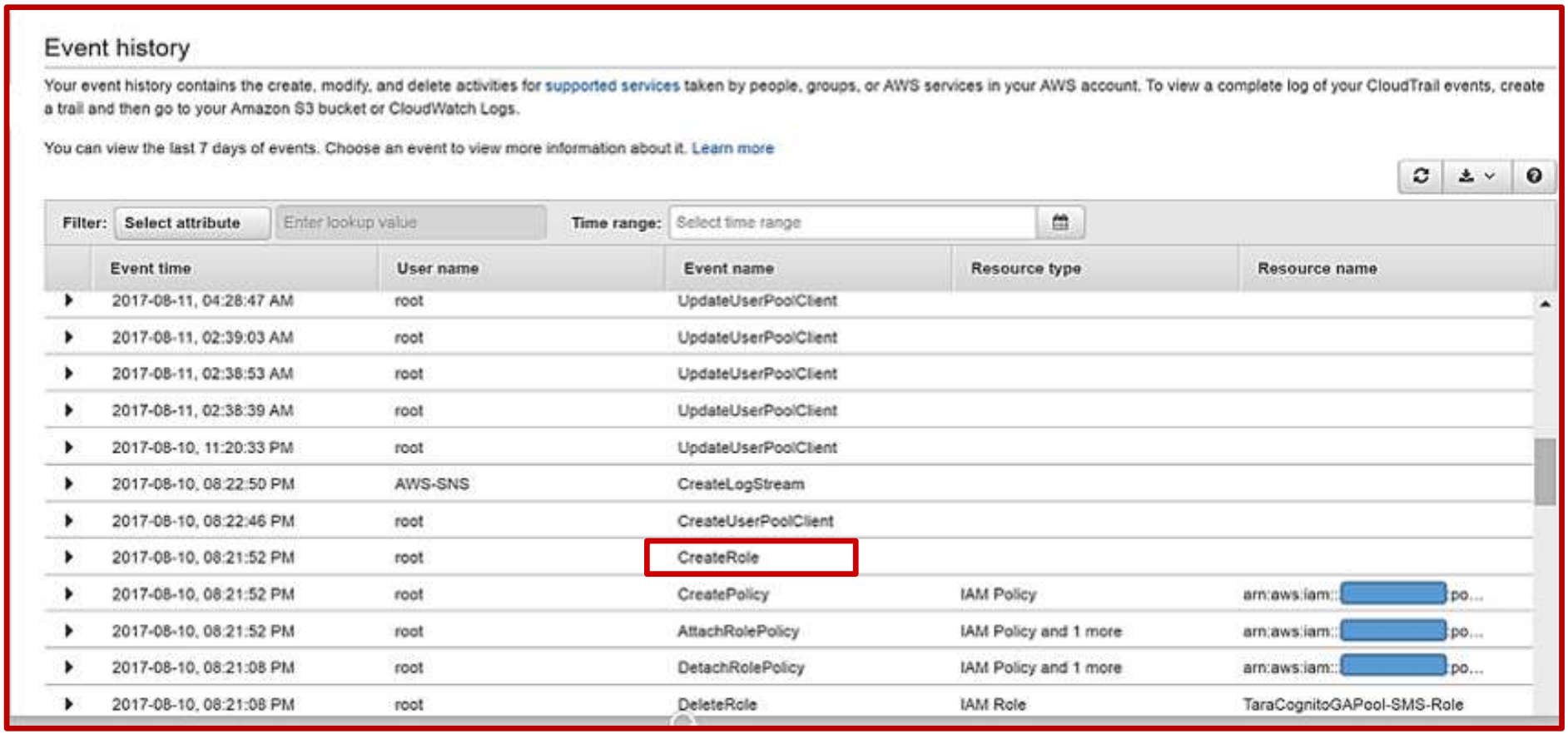
NORTHROP GRUMMAN

- Capture and record the activities – record API calls
- Discover and troubleshoot security and operation issues



AWS CloudTrail Logs (1)

NORTHROP GRUMMAN



Event history

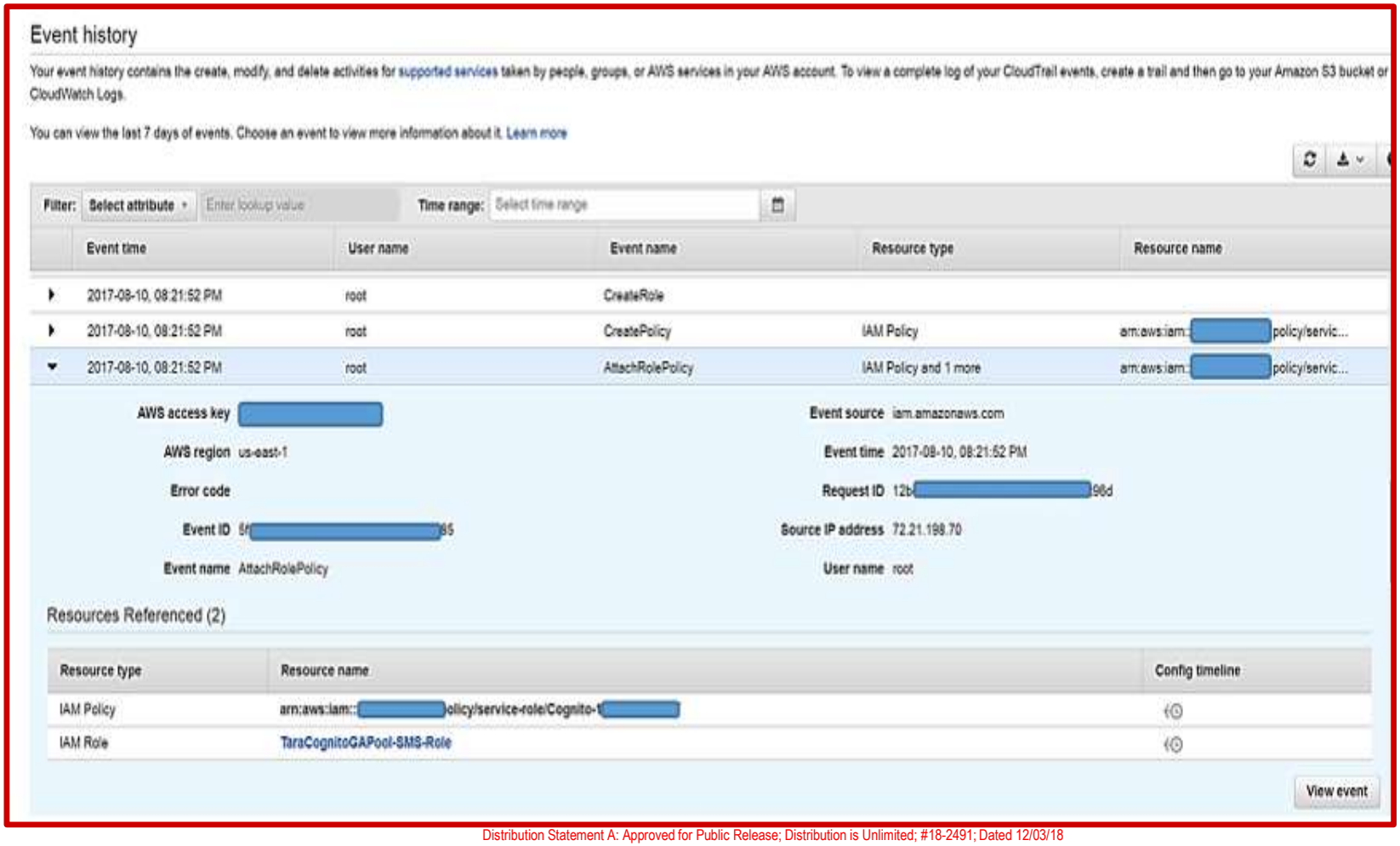
Your event history contains the create, modify, and delete activities for supported services taken by people, groups, or AWS services in your AWS account. To view a complete log of your CloudTrail events, create a trail and then go to your Amazon S3 bucket or CloudWatch Logs.

You can view the last 7 days of events. Choose an event to view more information about it. Learn more

Filter: Select attribute | Enter lookup value | Time range: Select time range

Event time	User name	Event name	Resource type	Resource name
2017-08-11, 04:28:47 AM	root	UpdateUserPoolClient		
2017-08-11, 02:39:03 AM	root	UpdateUserPoolClient		
2017-08-11, 02:38:53 AM	root	UpdateUserPoolClient		
2017-08-11, 02:38:39 AM	root	UpdateUserPoolClient		
2017-08-10, 11:20:33 PM	root	UpdateUserPoolClient		
2017-08-10, 08:22:50 PM	AWS-SNS	CreateLogStream		
2017-08-10, 08:22:46 PM	root	CreateUserPoolClient		
2017-08-10, 08:21:52 PM	root	CreateRole		
2017-08-10, 08:21:52 PM	root	CreatePolicy	IAM Policy	arn:aws:iam::[redacted]:po...
2017-08-10, 08:21:52 PM	root	AttachRolePolicy	IAM Policy and 1 more	arn:aws:iam::[redacted]:po...
2017-08-10, 08:21:08 PM	root	DetachRolePolicy	IAM Policy and 1 more	arn:aws:iam::[redacted]:po...
2017-08-10, 08:21:08 PM	root	DeleteRole	IAM Role	TaraCognitoGAPool-SMS-Role

AWS CloudTrail Logs (2)



Detective Controls 2 - CloudWatch

NORTHROP GRUMMAN

- Monitor your applications
  - Understand system-wide performance changes
  - Optimize resource utilization
  - Collect data from logs, metrics and events
- You can use CloudWatch
    - Take automated actions
    - Troubleshot issues
    - Discover and optimizes applications
- Ensure they are running smoothly

AWS CloudWatch Dashboard

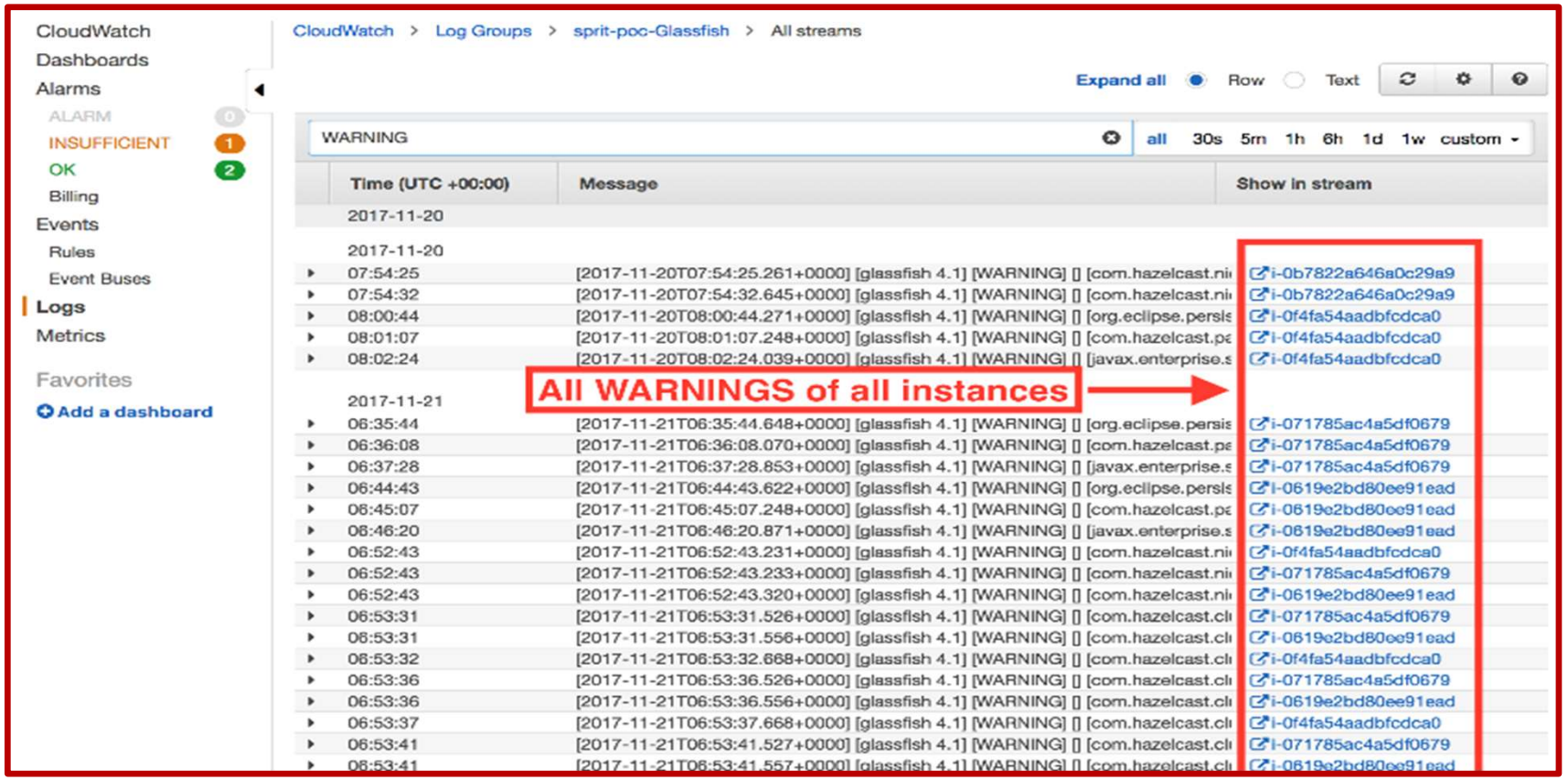


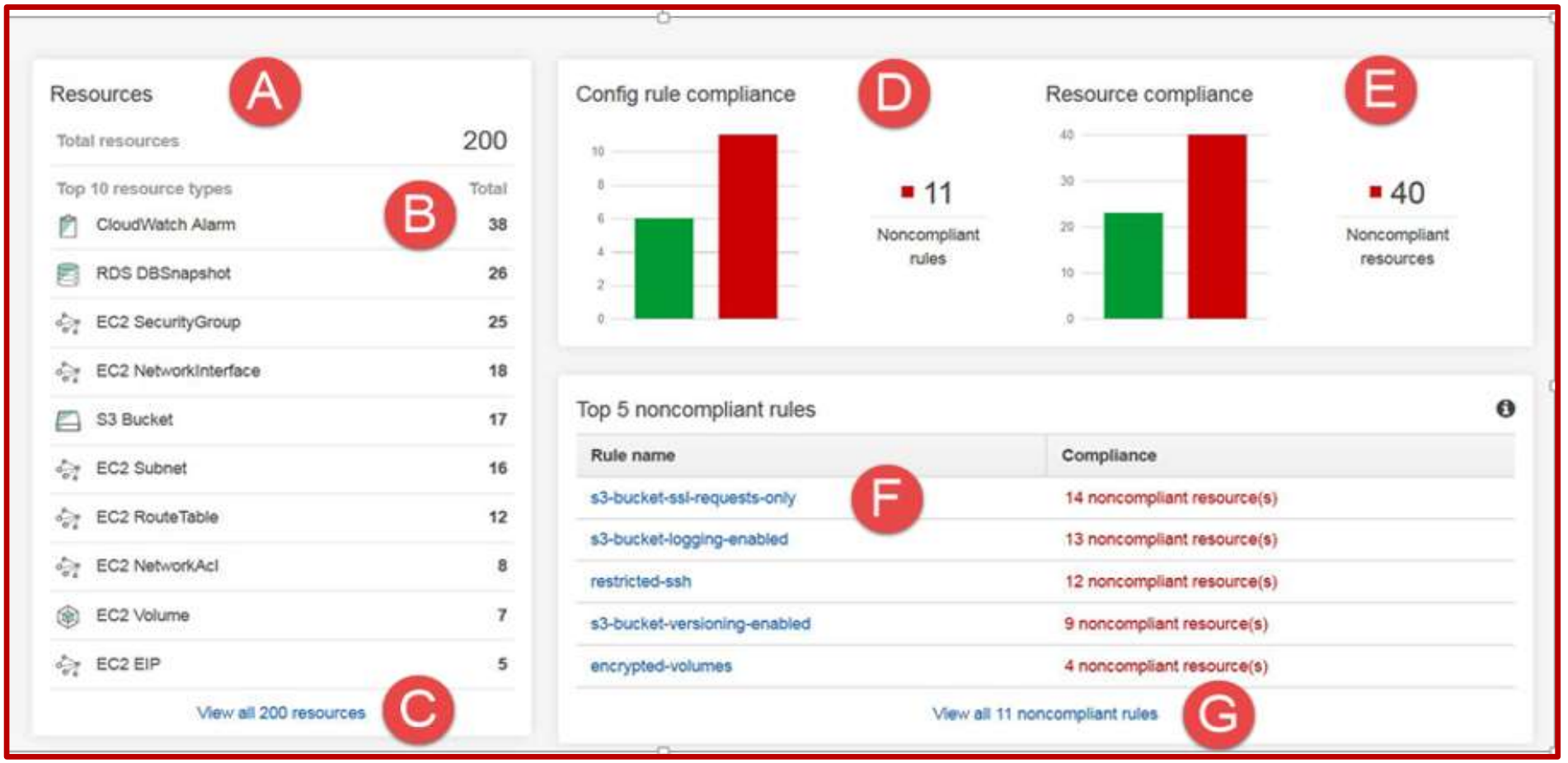
Image Source: https://blog.novatec-gmbh.de/check-your-logs-with-cloudwatch/

Detective Controls 3 - AWS Config

NORTHROP GRUMMAN

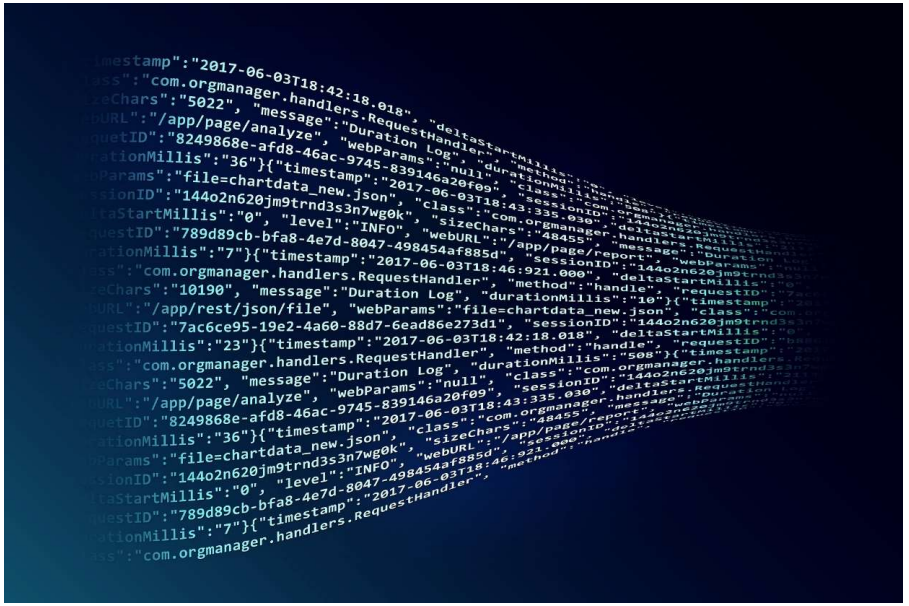
- Provide an inventory resources of your AWS resources
- Set up AWS SNS to notify you of configuration changes
- Specify an AWS S3 bucket to receive configuration information
- Add AWS Config managed rules to evaluate the resource types
- Let you audit the history of the configurations for those resources

AWS Config Dashboard



Detective Controls 4 - VPC Flow Logs

- Capture information about the IP traffic going to and from network
- Can publish flow log data to Amazon CloudWatch logs and Amazon S3
- Troubleshoot any specific traffic is not reaching an instance



VPC Flow Log Dashboard

NORTHROP GRUMMAN

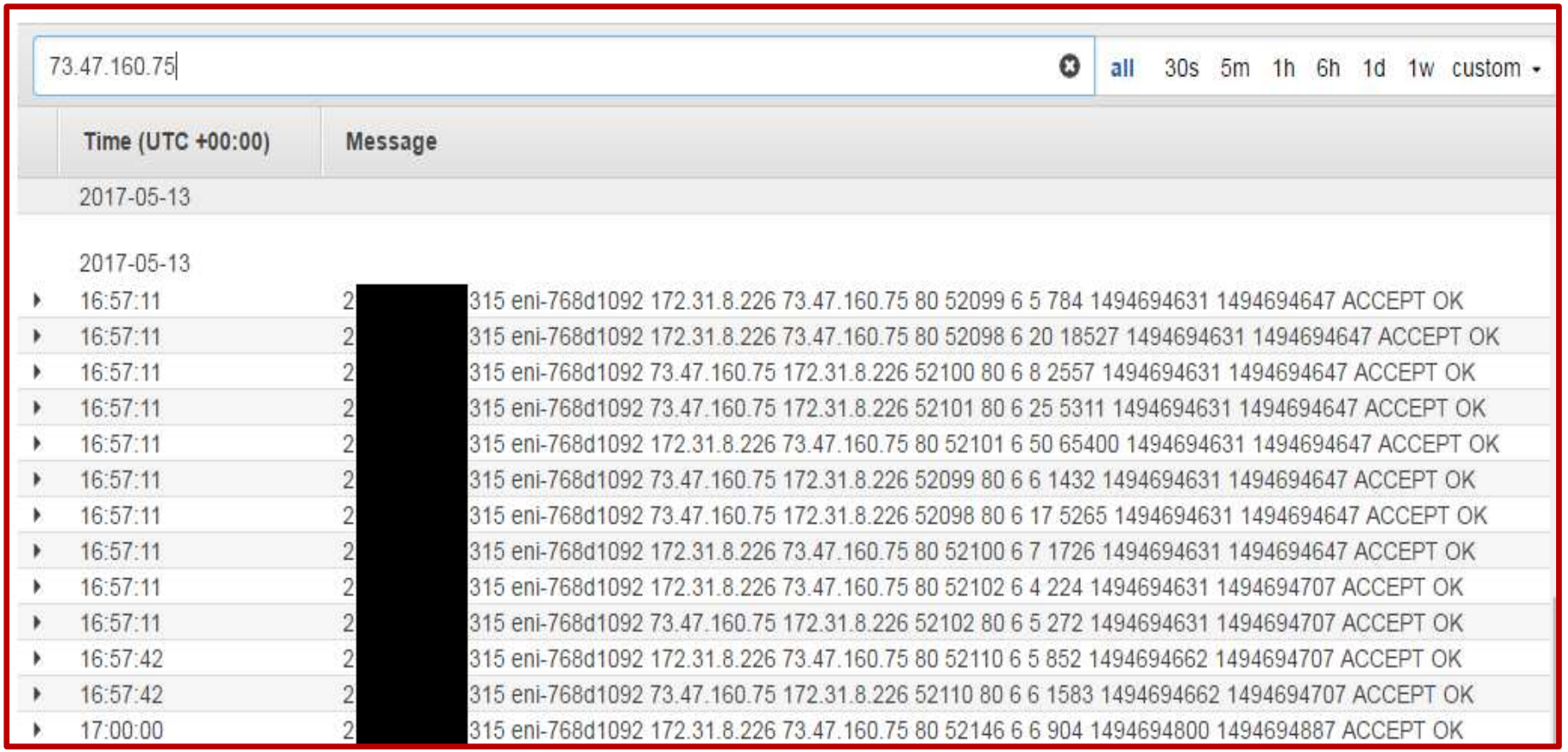


Image Source : https://www.flowtraq.com/author/chris/

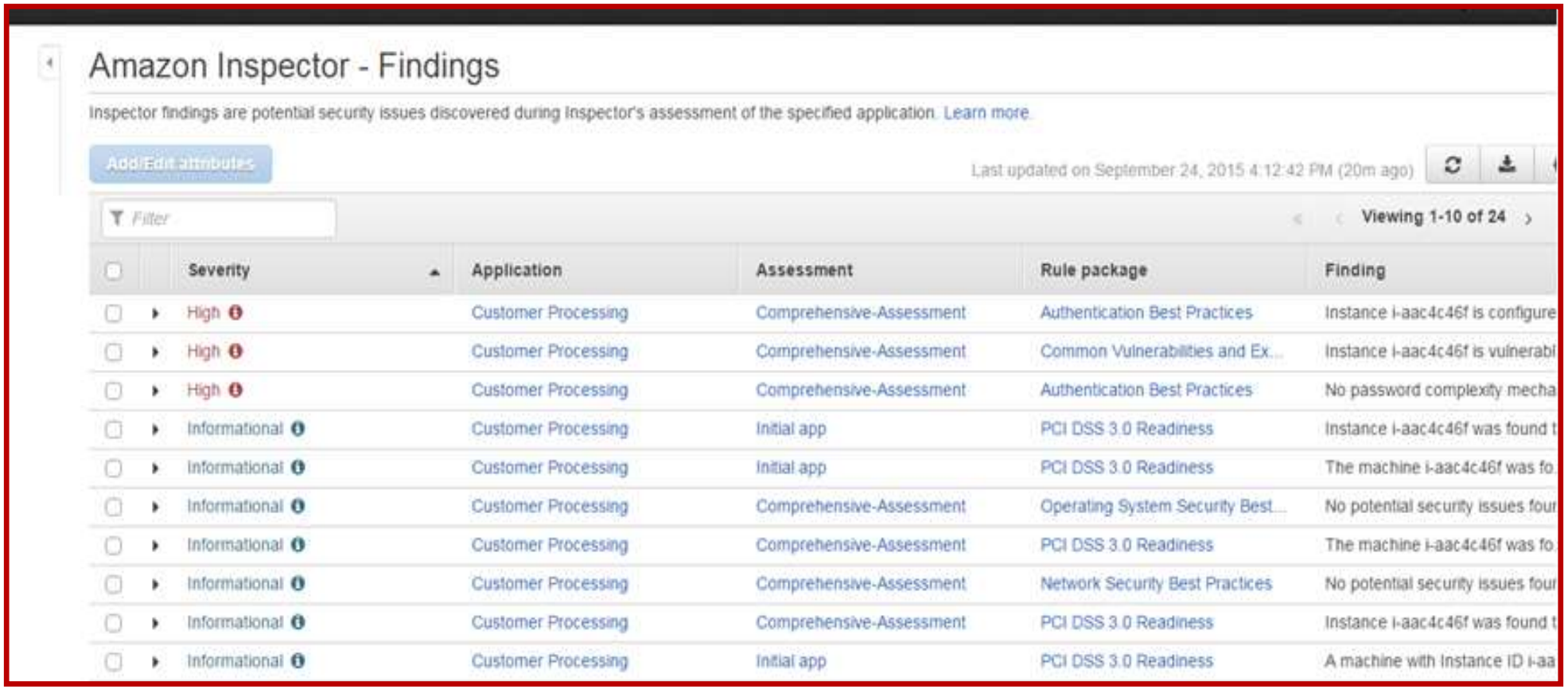
Detective Controls 5 - Amazon Inspector

NORTHROP GRUMMAN

- Provide Security Assessments
  - Check unintended network accessibility of Amazon EC 2 instances
  - Produce a detailed security findings
  - Help to improve compliance of applications deployed on AWS
  - Integrate security into DevOps

Amazon Inspector Log

NORTHROP GRUMMAN



Amazon Inspector - Findings

Inspector findings are potential security issues discovered during Inspector's assessment of the specified application. Learn more

Add/Edit attributes

Last updated on September 24, 2015 4:12:42 PM (20m ago)

Filter

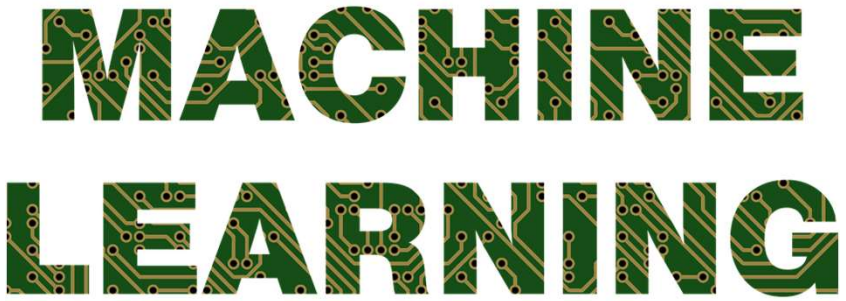
Viewing 1-10 of 24

Severity	Application	Assessment	Rule package	Finding
High	Customer Processing	Comprehensive-Assessment	Authentication Best Practices	Instance i-aac4c46f is configure
High	Customer Processing	Comprehensive-Assessment	Common Vulnerabilities and Ex...	Instance i-aac4c46f is vulnerabl
High	Customer Processing	Comprehensive-Assessment	Authentication Best Practices	No password complexity mecha
Informational	Customer Processing	Initial app	PCI DSS 3.0 Readiness	Instance i-aac4c46f was found t
Informational	Customer Processing	Initial app	PCI DSS 3.0 Readiness	The machine i-aac4c46f was fo
Informational	Customer Processing	Comprehensive-Assessment	Operating System Security Best...	No potential security issues four
Informational	Customer Processing	Comprehensive-Assessment	PCI DSS 3.0 Readiness	The machine i-aac4c46f was fo
Informational	Customer Processing	Comprehensive-Assessment	Network Security Best Practices	No potential security issues four
Informational	Customer Processing	Comprehensive-Assessment	PCI DSS 3.0 Readiness	Instance i-aac4c46f was found t
Informational	Customer Processing	Initial app	PCI DSS 3.0 Readiness	A machine with Instance ID i-aa

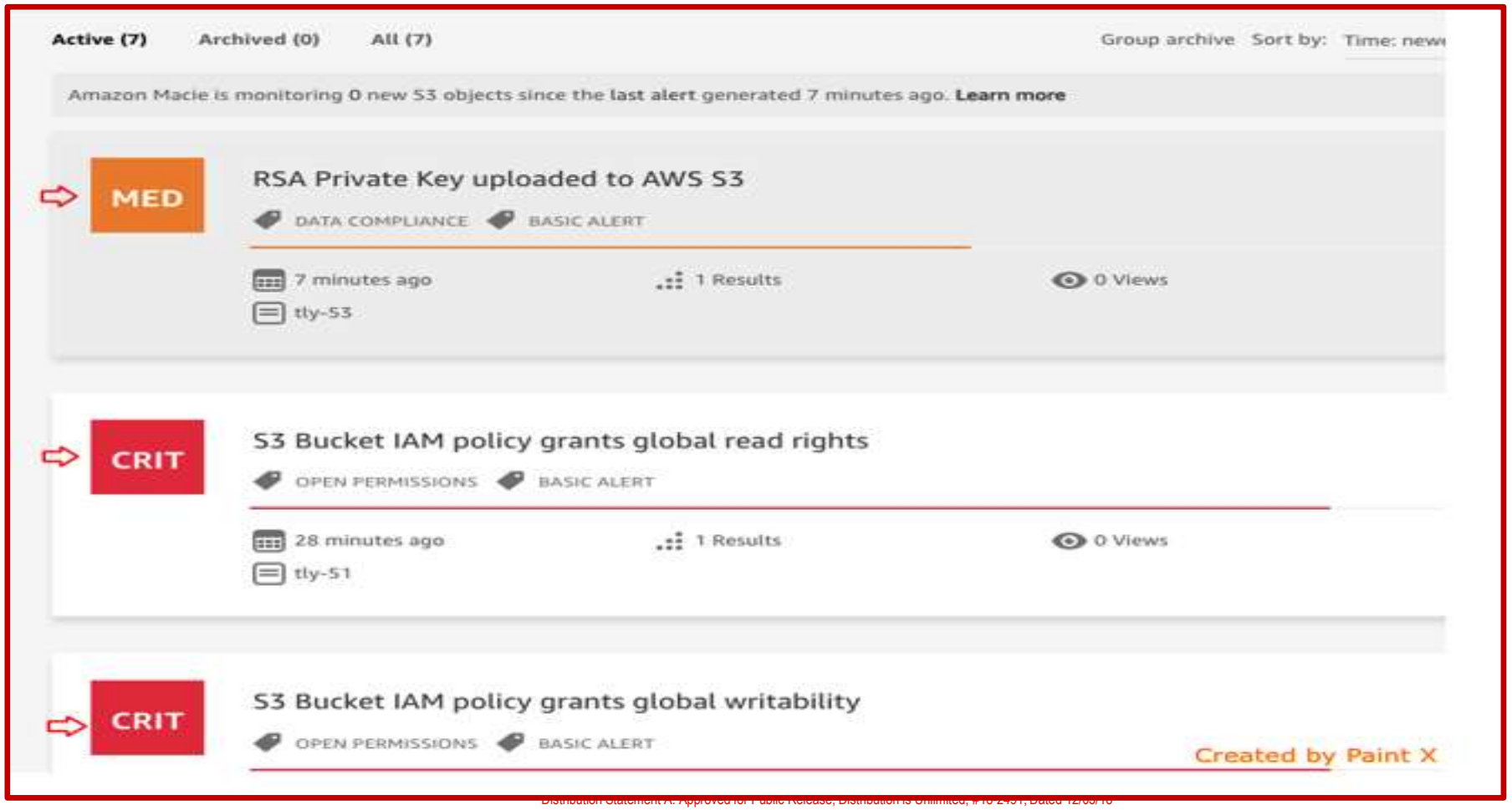
Detective Controls 6 - AWS Macie

NORTHROP GRUMMAN

- Use Machine Learning
  - Monitor how data is accessed and to look for any anomalies
  - Alert users of any activity that looks suspicious
  - Detect certain data types like full names, address, credit card numbers, IP address, driver license and social security number and birth dates
  - Flow into a central dashboard
    - Highlight high-risk files
  - Apply to S3 buckets



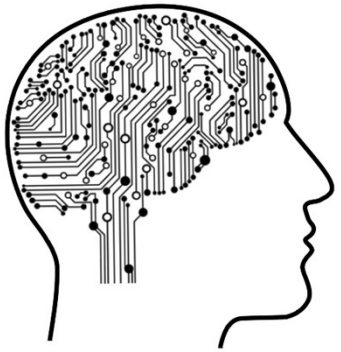
AWS Macie Dashboard



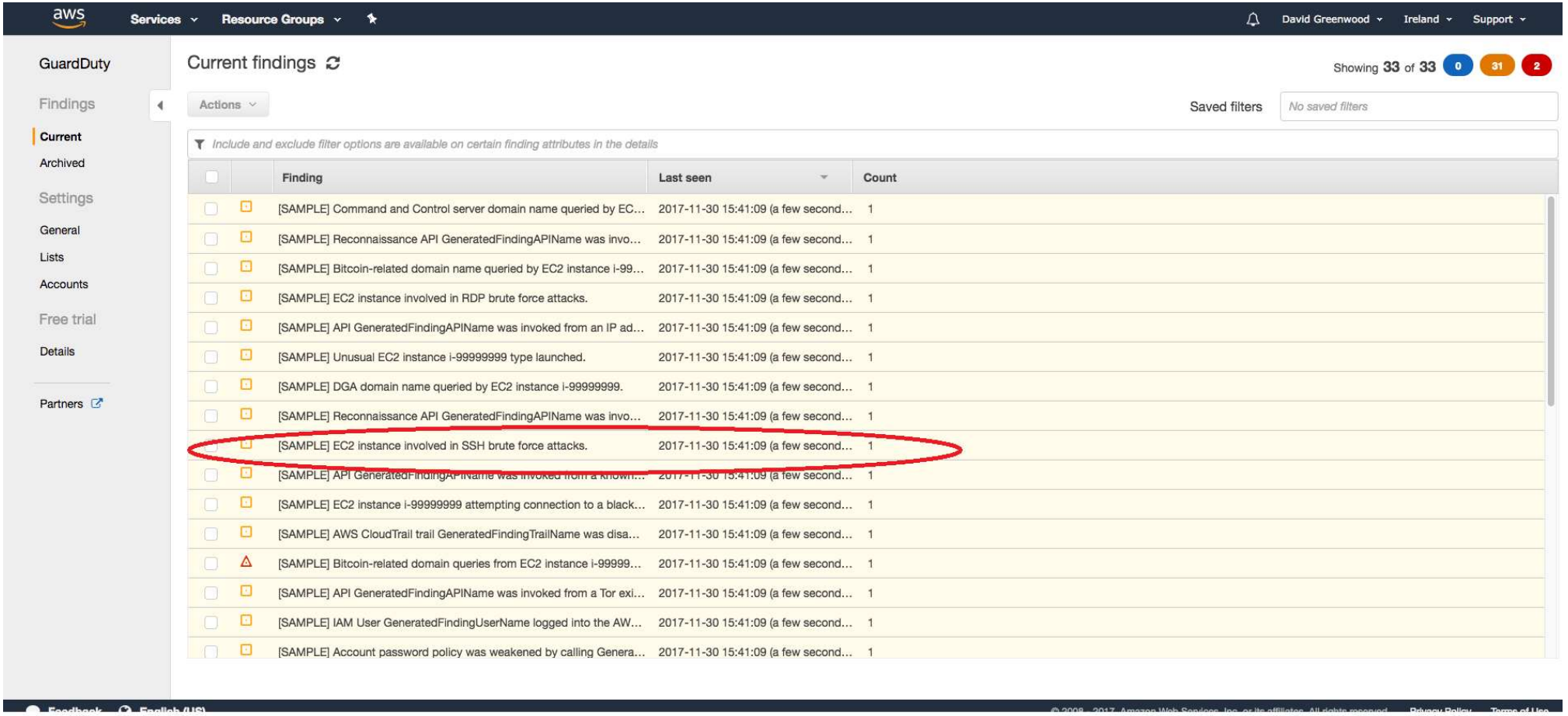
Detective Controls 7 - GuardDuty

NORTHROP GRUMMAN

- Threat Detection Service
  - Continue monitors for malicious or authorized behavior
  - Immediately begin analyzing billions of events
    - Signs of risk
- Use AI/Machine Learning , Anomy Detection and Threat Intelligence
- Send Detailed Alerts



GuardDuty Dashboard (Example of a Threat List)



In Summary

NORTHROP GRUMMAN

- Use more established AWS services; newer services might have more security vulnerabilities
- Implement security at **all layers – defense in depth!**
- Implement **AWS Security Best Practices**
- **Automate, automate and automate for security!**
  - Set up alerts for all important actions if something goes wrong
- Plan for security events
- Understand all the services come with AWS
  - How they integrate with the other AWS security services
- Design loosely coupled services is better
- Train your employees (get AWS certified)!!
- **Monitor, monitor and monitor**
  - **Oh, of course READ YOUR LOGS !!!**

Final Thoughts… Design Systems with “Failure” in Mind

NORTHROP GRUMMAN

- Remove Single Points of Failure
  - Can withstand the failure of an individual or multiple components
  - Think about ways to automate recovery and reduce disruption at **every layer of your AWS cloud architecture**
  - **Introduce redundancy**

- **Can Handle Failure in a Graceful Manner**

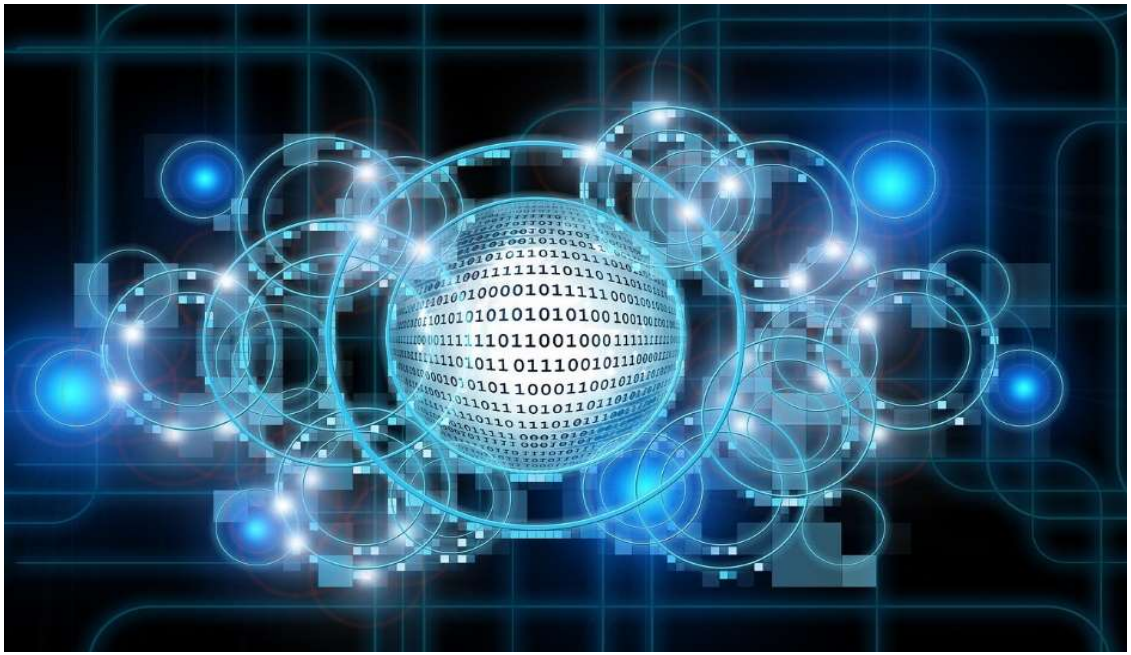
More Final Thoughts … Build Cyber Resilient Systems!!

NORTHROP GRUMMAN

"***Protecting critical systems and assets and making them cyber resilient…***"

"***The ability to anticipate, withstand, recover from and adapt to adverse conditions ……***"

- Dr. Ron Ross – Fellow at NIST



Mary Wang Biography

Ms. Mary Wang is a senior principal information assurance engineer at Northrop Grumman. She has a combined 20 years of software engineering and information assurance experience. She holds a Bachelor of Science degree in Computer Science and Master's in Business Administration from California State Polytechnic University, Pomona. Her certifications include an ISC^2 Certified Information Systems Security Professional (CISSP), EC-Council Certified Ethical Hacker (CEH), EC-Council Certified Network Defense Architect (CNDA) and CompTIA Security+. She is also an active SoCal chapter leader at Women's Society of Cyberjutsu (WSC).

Ms. Wang has given multiple software engineering presentations at technical symposiums and cybersecurity presentations at local security groups. She is an active member of OWASP, ISSA, Cloud Security Alliance (CSA), SB WASP, LETHAL and WSC organizations / groups.

References

- Banerjee, Joyjeet (2018) . AWS Certified Solutions Architect Associate All-in-One Exam Guide (Exam SAA-C01)
- Overview of Amazon Web Services White Paper (2018) https://docs.aws.amazon.com/aws-technical-content/latest/aws-overview/aws-overview.pdf?icmpid=link_from_whitepapers_page
- AWS Security Best Practices (Aug 31, 2016) https://aws.amazon.com/whitepapers/aws-security-best-practices/
- Architecting for The Cloud: Best Practices (Feb 10, 2016) https://aws.amazon.com/whitepapers/aws-security-best-practices/
- AWS Well-Architected Framework (June 2018) https://d1.awsstatic.com/whitepapers/architecture/AWS_Well-Architected_Framework.pdf
- Synergy Research Group (April 27, 2018) Cloud Growth Rate Increased Again in Q1; Amazon Maintains Market Share Dominance https://www.srgresearch.com/articles/cloud-growth-rate-increased-again-q1-amazon-maintains-market-share-dominance
- SECURONIX (2018) 2018 Cloud Security Report http://pages.securonix.com/Cloud-Security-Report-2018.html

THE VALUE OF PERFORMANCE.

NORTHROP GRUMMAN