

Cloud Security: Navigating the Security Challenges of Cloud Computing

CISO Chicago Summit – July 18th, 2023



Michael Tayo
[/michaeltayo](https://www.linkedin.com/in/michaeltayo)

About



B.S. Information Technology, Marquette University

AVP, Cloud Vulnerability Management and Application Security – Principal Cloud Security Engineer, U.S. Bank

Research: Cloud Security, DevSecOps, Cyber Fusion, Security Operations, Leadership and Product Management

Author: Anomali - Collaborative Security to Defend the Modern Landscape

Hobbies: Traveling, Music Shows, Playing Sports



d0uble3L



Michael Tayo
/michaeltayo

Disclaimer

The opinions expressed in this presentation are my own and do not necessarily reflect the opinions of my employer or any other organization.

This presentation is for educational purposes only.

I am not affiliated with any of the products or services mentioned in this presentation, and I have not been paid to endorse any of them.

All tools and resources shown in this presentation are for reference purposes only.

I encourage you to do your own research before making any decisions.



Michael Tayo
/michaeltayo

Objectives & Key takeaways:



Learn about best practices for securing cloud environments.



Discuss strategies for managing cloud security risks.



Review methods for measuring and optimizing cloud security program effectiveness.



Michael Tayo
/michaeltayo



TABLE OF CONTENT

01

INTRODUCTION

02

CLOUD SECURITY
CHALLENGES

03

CLOUD SECURITY
BEST PRACTICES

04

MANAGING CLOUD
SECURITY RISKS

05

MEASURING A CLOUD
SECURITY PROGRAM

06

WRAP UP + Q/A



Michael Tayo
[/michaeltayo](https://www.linkedin.com/in/michaeltayo)





Michael Tayo
/michaeltayo



INTRODUCTION

A Brief History of Cloud Computing

By the mid-1970s, many groups of computers had been linked together in networks

In 2002, Amazon introduced its web-based retail services. It was the first major business to think of using only 10% of its capacity as a problem to be solved.

In 2010, companies like AWS, Microsoft, and OpenStack developed private clouds that were fairly functional.

By 2014, cloud computing had developed its basic features, and security had become a major concern.

In 2020, The coronavirus pandemic accelerated the use of the internet for e-commerce and working remotely.



Michael Tayo
/michaeltayo



Michael Tayo
/michaeltayo

If 70% of
businesses use
the cloud, and
90% of data
breaches involve
cloud services...



What does that mean for your
business?

63% will likely experience a breach*

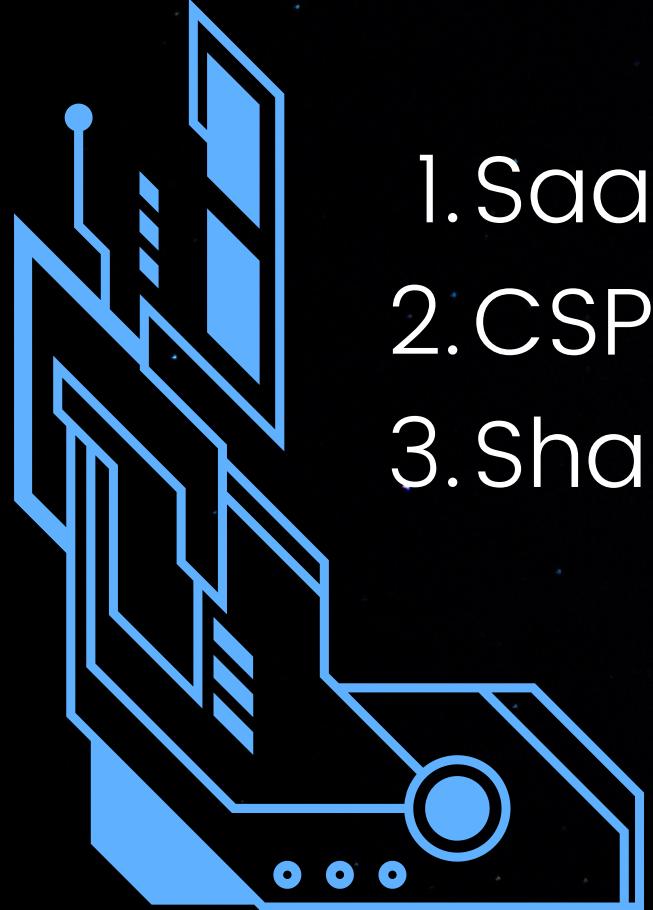
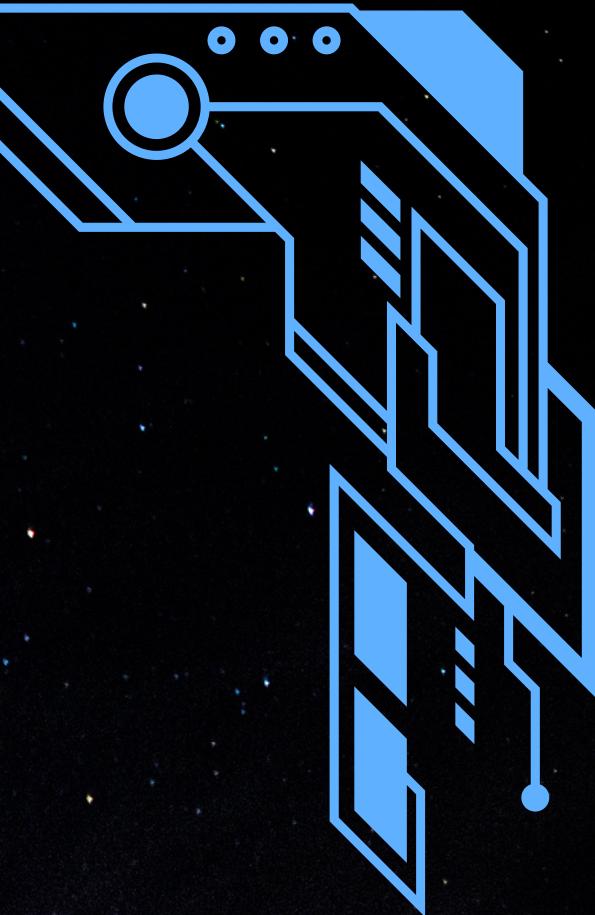


Michael Tayo
/michaeltayo

Why Does Cloud Security, Matter?



1. SaaS is more accessible
2. CSPs have billions of customers
3. Shared resources put us all at risk



The Benefits

Ability to save money

Improve scalability

Access powerful computing resources

Increase competitive edge

The Challenges

Shared responsibility model

Access Control

Data Privacy

Compliance and legal considerations

Data breaches and cyber attacks

The average data breach costs in 2022 is \$4.35 million, a 2.6% rise from 2021 amount of \$4.24 million.
- Upguard



Michael Tayo
/michaeltayo



Cloud Security Challenges



Michael Tayo
[/michaeltayo](https://www.linkedin.com/in/michaeltayo)



Michael Tayo
/michaeltayo



Real-world Examples and Case Studies

LastPass, 2022, October

- Compromised developer account (an IAM User)
- Unknown pivot point into a production environment.
- Gained access to data decryption keys
- Internal and customer data broadly compromised, including backups of the MFA database

Capital One, 2019, April

- "Misconfigured WAF" that allowed for a SSRF attack
- Over-privileged EC2 Role
- 100 million credit applications

DataDog, 2016, July

- CI/CD AWS access key and SSH private key leaked
- The attacker attempted to pivot with customer credentials
- 3 EC2 instances and a subset of S3 buckets

Shared Responsibility Model

Who's responsible for what?



Responsibility	On-Prem	IaaS	PaaS	SaaS
Data classification & accountability	Cloud Customer	Cloud Customer	Cloud Customer	Cloud Customer
Client & end-point protection	Cloud Customer	Cloud Customer	Cloud Customer	Cloud Provider
Identity & access management	Cloud Customer	Cloud Customer	Cloud Provider	Cloud Provider
Application level controls	Cloud Customer	Cloud Customer	Cloud Provider	Cloud Provider
Network controls	Cloud Customer	Cloud Provider	Cloud Provider	Cloud Provider
Host infrastructure	Cloud Customer	Cloud Provider	Cloud Provider	Cloud Provider
Physical security	Cloud Customer	Cloud Provider	Cloud Provider	Cloud Provider

Cloud Customer Cloud Provider



Michael Tayo
[/michaeltayo](https://www.linkedin.com/in/michaeltayo)

Identity Access Management

Complexity: Who has access to what?

Security: Which point of entry is the priority?

Compliance: Who governs access?



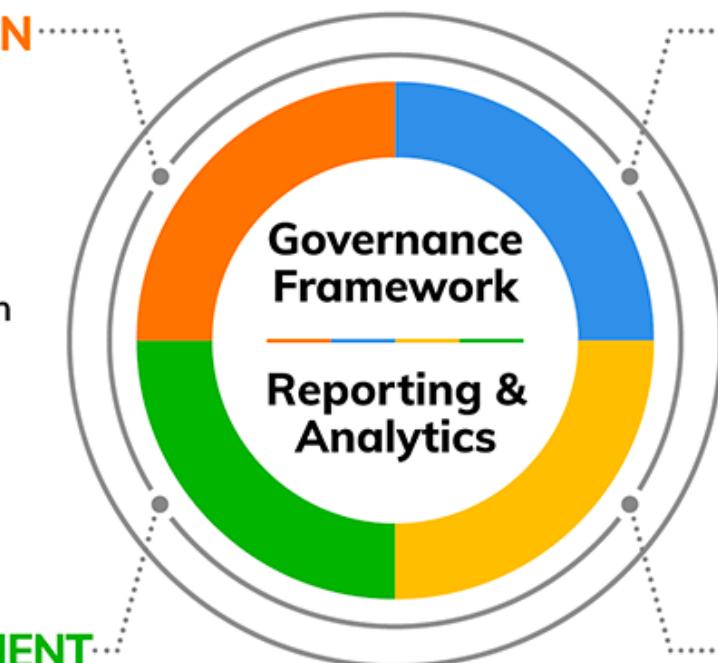
IAM service components

AUTHENTICATION SERVICES

- Single sign-on
- Multifactor authentication
- Session and token management

USER MANAGEMENT SERVICES

- Provisioning
- Deprovisioning
- Self-service
- Delegation



AUTHORIZATION SERVICES

- Roles
- Rules
- Attributes (e.g. metadata)
- Privileged access

DIRECTORY SERVICES

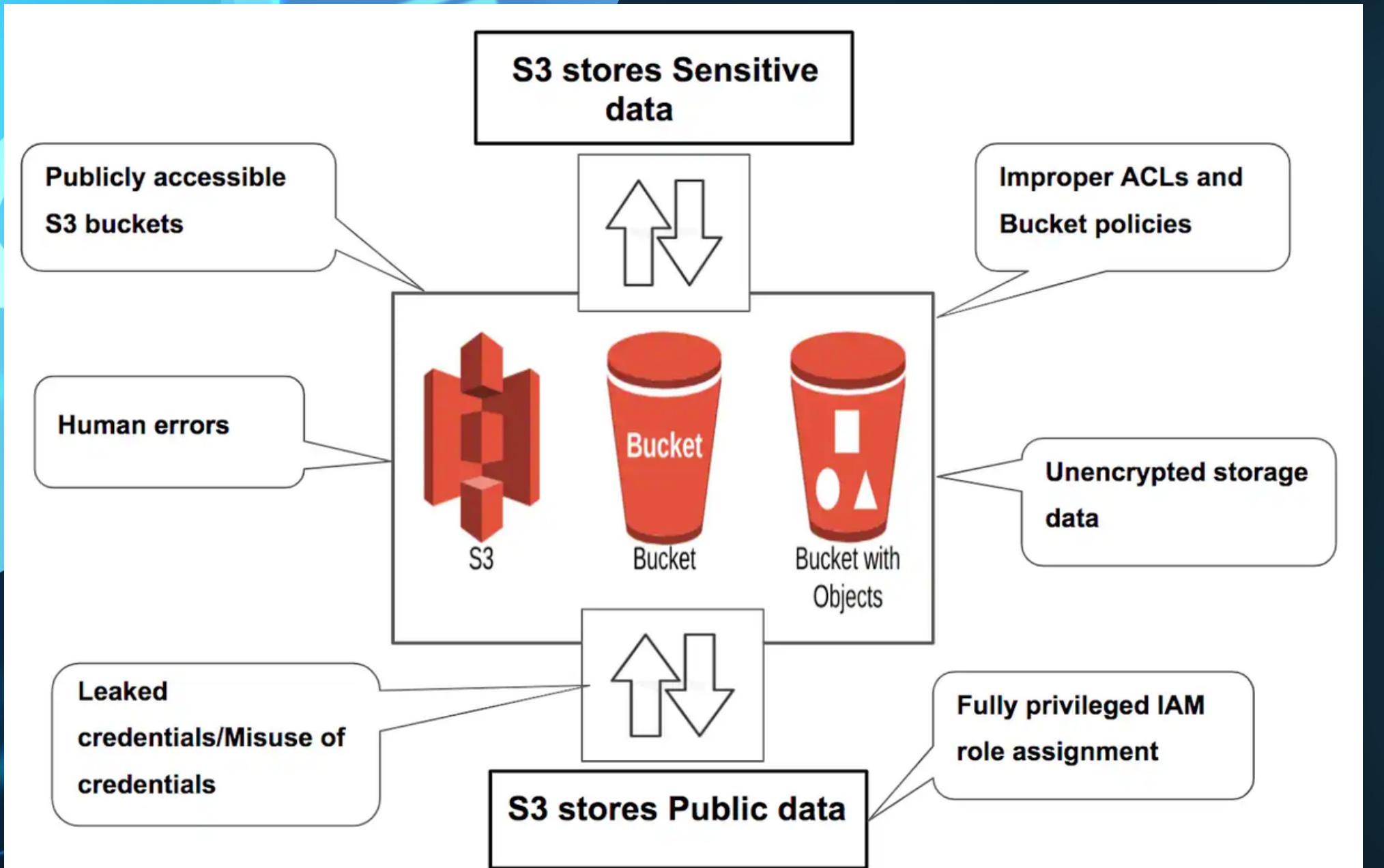
- Identity store
- Directory federation
- Metadata synchronization
- Virtual directory

Image source data courtesy of TechTarget

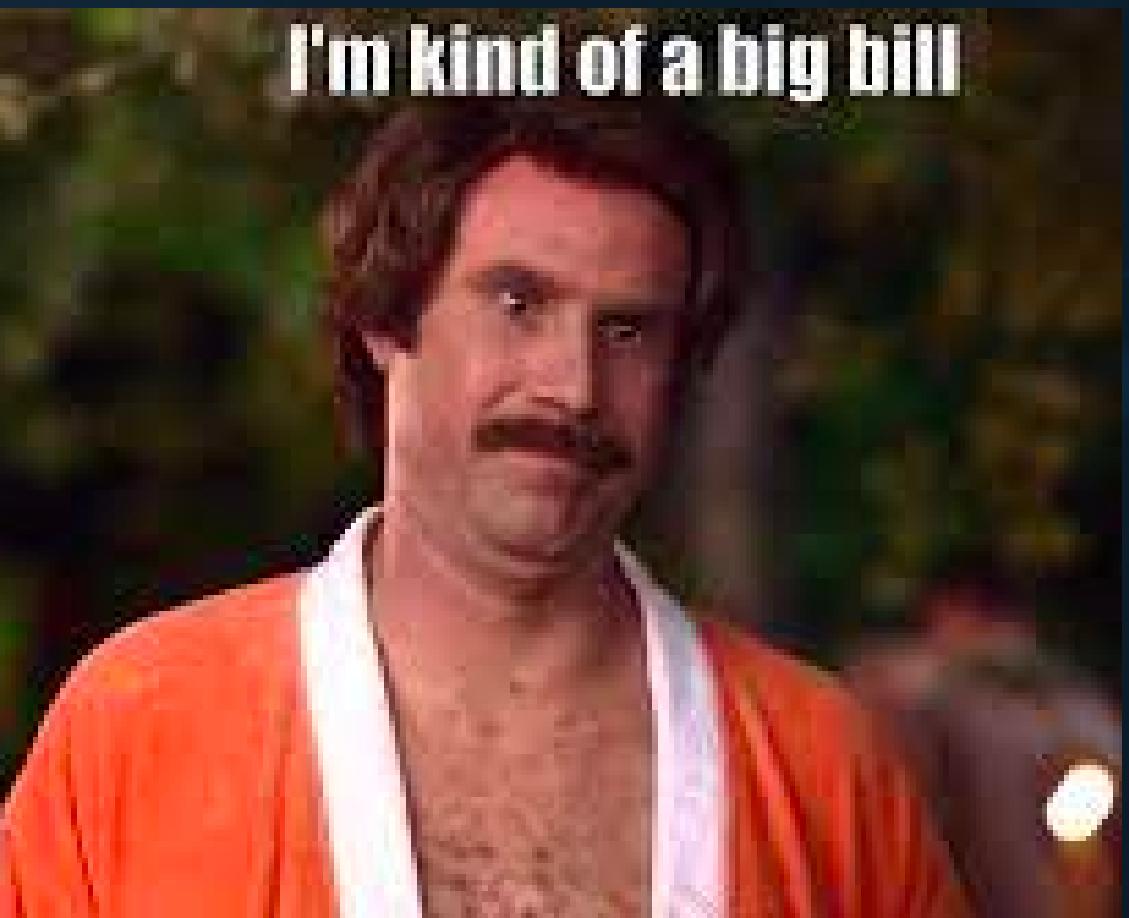


Michael Tayo
/michaeltayo

Data Protection



Michael Tayo
/michaeltayo



Governance, Risk and Compliance

Non-compliance can lead to financial penalties, regulatory fines, and reputational damage.

Meta Technologies



SolarWinds



Morgan Stanley



\$35 M



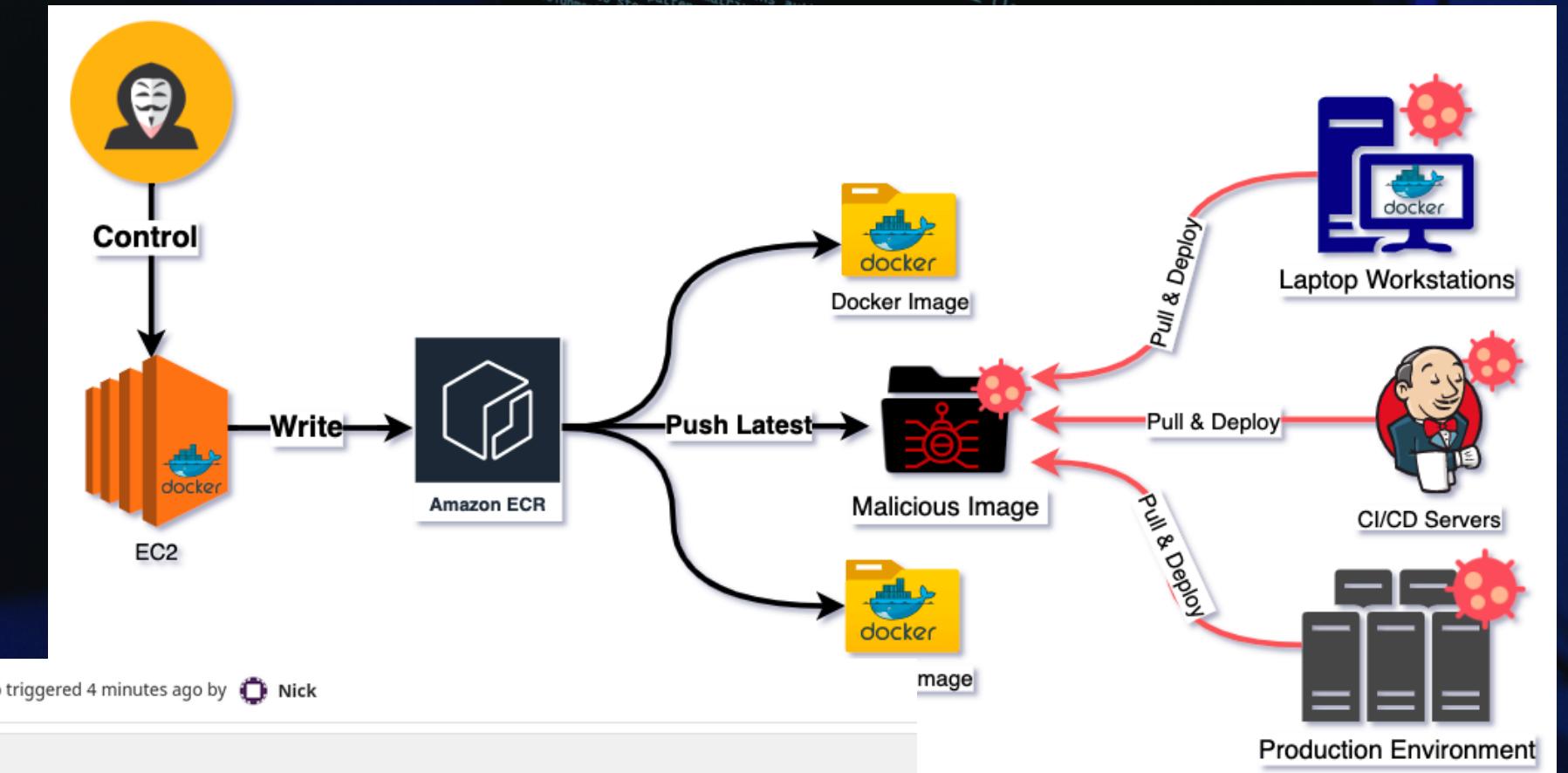
Michael Tayo
/michaeltayo

Data breaches and cyber attacks

The number of cloud security incidents increased by 600% between 2019 and 2021.

Cloud Security Alliance

```
current user: Xo_Bla..._ox
PREMIUM USER identified
dracut: rd_NO_MD: removing MD RAID activation
ata_piix 0000:00:01.1: version 2.13
ata_piix 0000:00:01.1: setting latency timer to 64
ata_piix 0000:00:01.1: PATA max MWDMA2 cmd 0x1f0 ctl 0x3f6 bmdma
ata_piix 0000:00:01.1: NODEV after polling detection
ata_piix 0000:00:01.1: ATA-7: QEMU HARDDISK, 0.121
ata_piix 0000:00:01.1: configured for MWDMA2
ata_piix 0000:00:01.1: Flushing to <...>
ata_piix 0000:00:01.1: Enabling assignment permissions
ata_piix 0000:00:01.1: Flushing to <...>
ata_piix 0000:00:01.1: Assignment matrix
ata_piix 0000:00:01.1: Flushing to <...>
```



passed Job build-job triggered 4 minutes ago by Nick

```
1 Running with gitlab-runner 14.7.0 (98daeee0)
2 on docker-runner JmPwzhaP
3 Preparing the "docker" executor
4 Using Docker executor with image ubuntu:latest ...
5 Pulling docker image ubuntu:latest ...
6 Using docker image sha256:54c9d81ccb440897908abdcaa98674db83444636c300...
53c1fd5768333f0d1dbc834f7c07a4dc93f474be ...
7 Preparing environment
8 Running on runner-jmpwzhaP-project-2-concurrent-0 via 5c6657d54ff5...
9 Getting source from Git repository
10 Fetching changes with git depth set to 20...
11 Initialized empty Git repository in /builds/ashley/mvp-docker/.git/
12 Created fresh repository.
13 Checking out b5866b75 as main...
14 Skipping Git submodules setup
15 Executing "step_script" stage of the job script
16 Using docker image sha256:54c9d81ccb440897908abdcaa98674db83444636c300...
53c1fd5768333f0d1dbc834f7c07a4dc93f474be ...
17 $ echo "Hey, $GITLAB_USER_LOGIN! This is the CI/CD Pipeline!"
18 Hey, Nick! This is the CI/CD Pipeline!
19 $ id
20 uid=0(root) gid=0(root) groups=0(root)
21 Job succeeded
```

```
root@kali: ~/Desktop/DDos-Attack
File Edit View Search Terminal Help
Author : HA-MRX
You Tube : https://www.youtube.com/c/HA-MRX
github : https://github.com/Ha3MrX
Facebook : https://www.facebook.com/muhamad.jabar222
IP Target :
```



Michael Tayo
/michaeltayo

CLOUD SECURITY BEST PRACTICES



Michael Tayo
[/michaeltayo](https://www.linkedin.com/in/michaeltayo)

Identity Access Management



Identity Privileged Access Management

Dedicated Cloud IAM

Never Trust, Always Verify

Data Protection



Encryption

Data Governance

Employee Training

82% of data breaches included human- elements, social attacks, mistakes, and abuse.

- Gartner

Security Baseling



Organizational Standards +
Industry Frameworks

Holistic Cloud Security
Solution(s)

Declarative Resource
Management

Managing Cloud Security Risk



OH, YOU USE CLOUD COMPUTING?

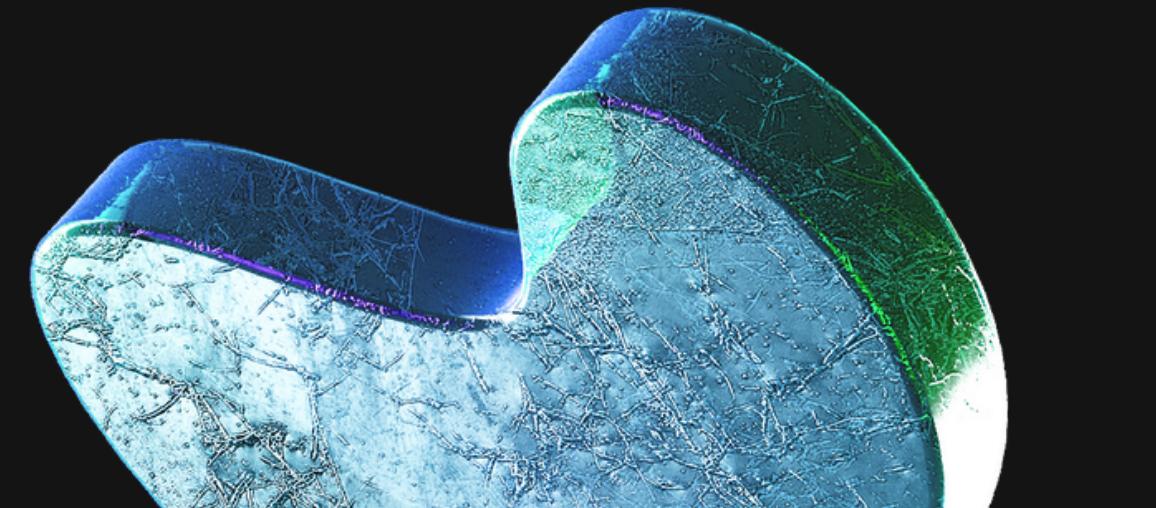
YOUR WORK MUST BE SO SECURE



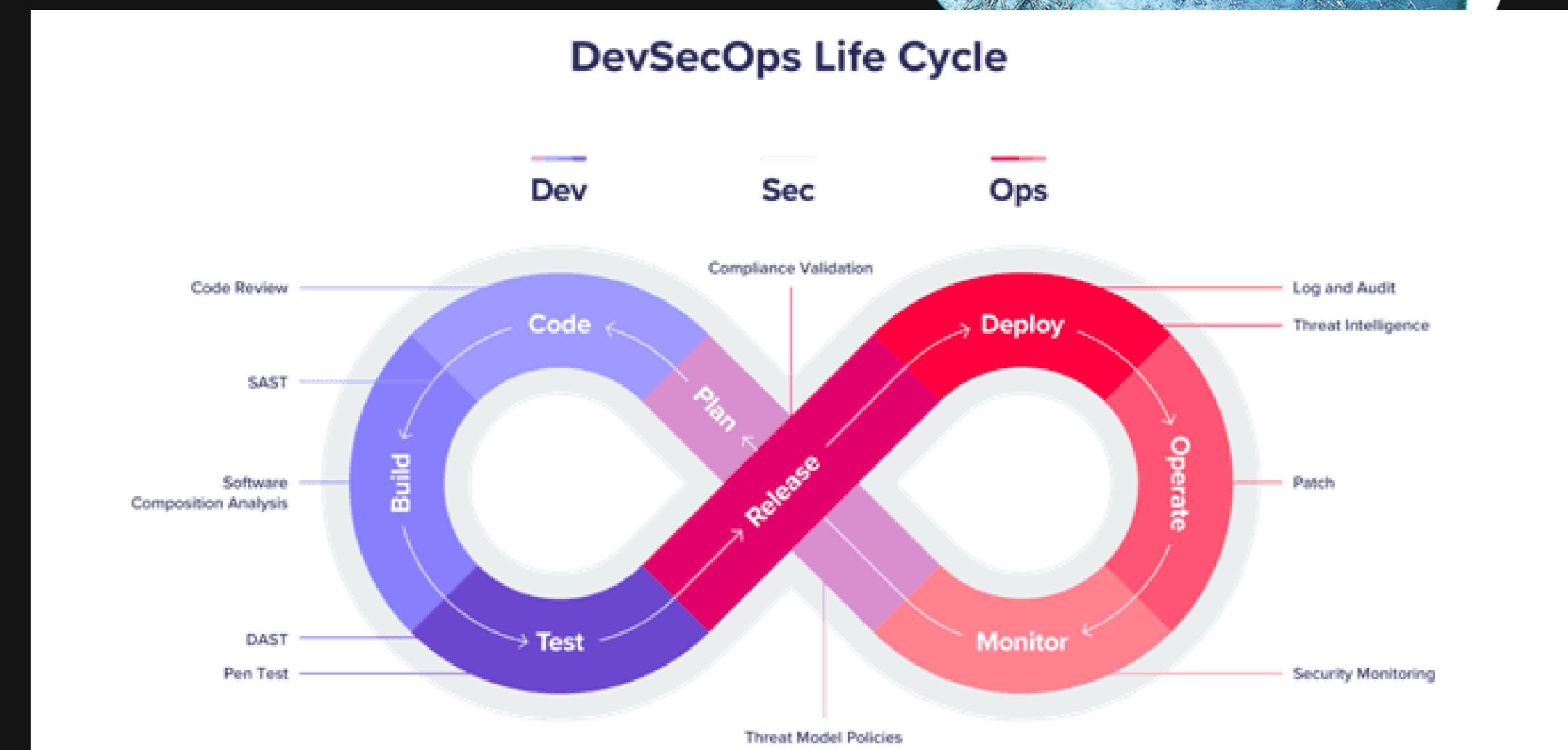
Michael Tayo
/michaeltayo

Shift Left Security

Embed security into the earliest phases of the software development lifecycle.



- Build security into new application development
- Integrate application and container security into the DevOps toolchain
- Combine scans to improve visibility and prioritization



Michael Tayo
/michaeltayo

Continuous Monitoring and Threat Detection

Security Signals that are Context-Driven and Risk-Based



Proactive Threat Intelligence
Stay ahead of threats and protect their data from attacks

SIEM & SOAR
Increase visibility and automate repetitive triage tasks

Posture Management & Workload Protection
Improve security posture and protect their data from attack.

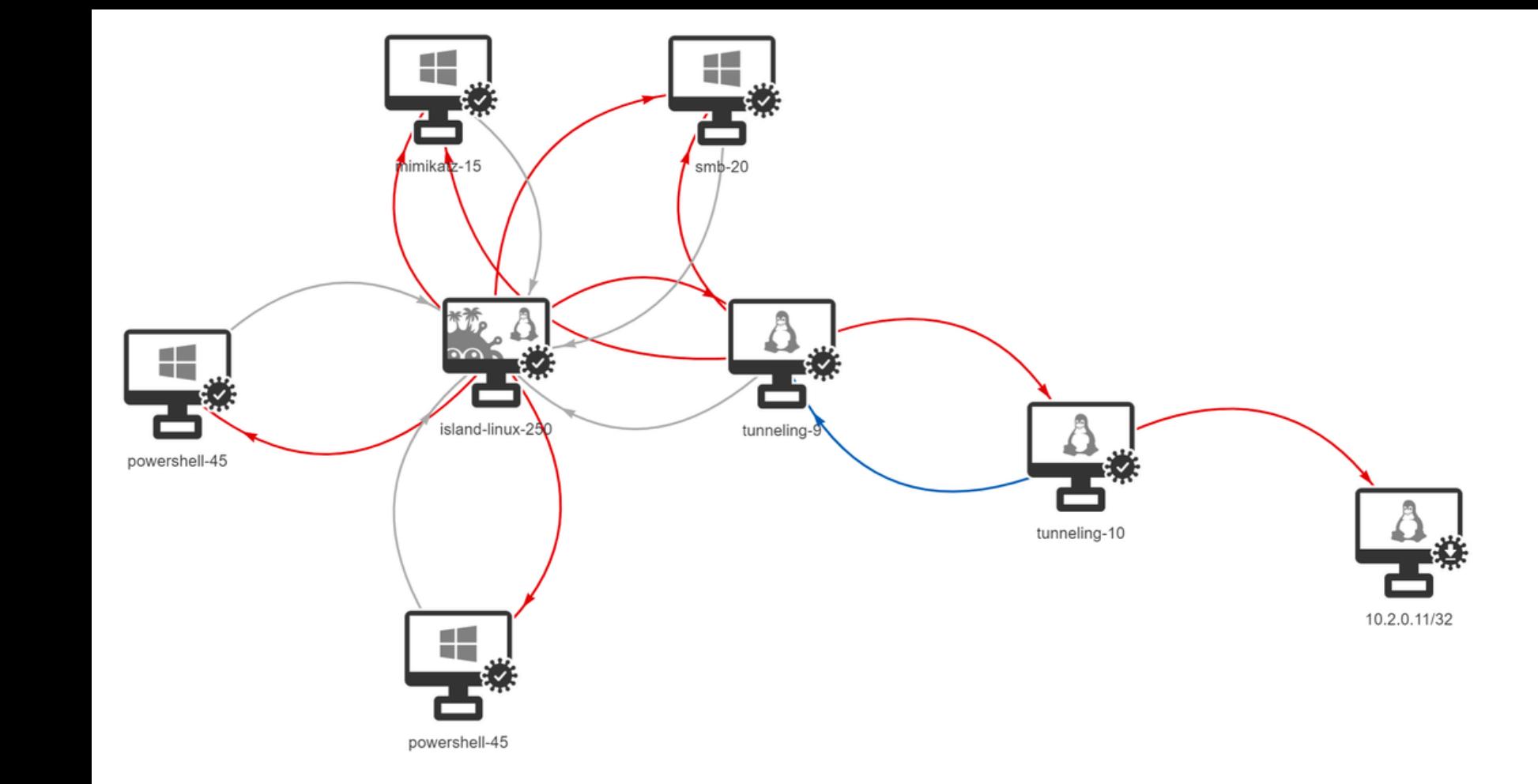
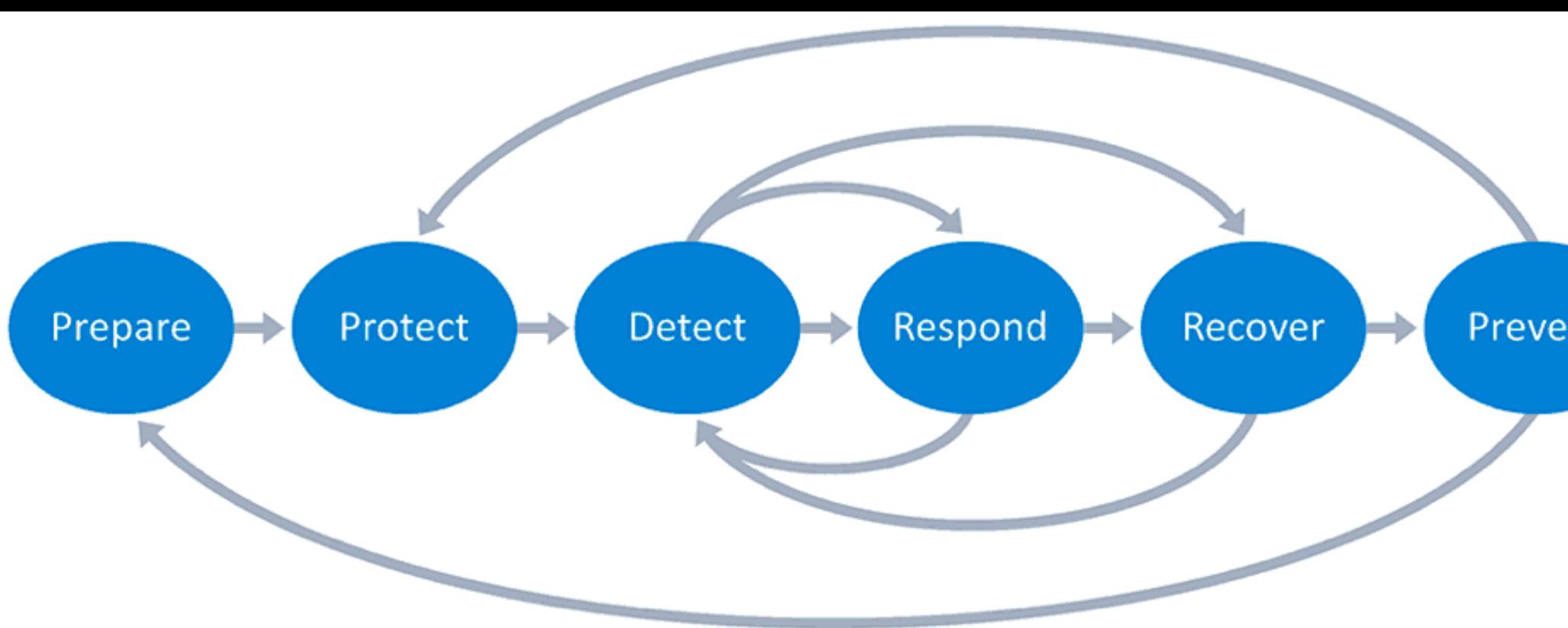


Michael Tayo
/michaeltayo



Incident Response and Recovery

Minimize the Impact of a Security Incident and Protect sensitive data.



Roles and Responsibilities

Communication protocols

Escalation procedures

Don't forget about Disaster Recovery and Business Continuity

Shift Left

How can you enable engineers by embedding security into the SDLC? Is this a security feature or a business blocker?

Scan Regularly

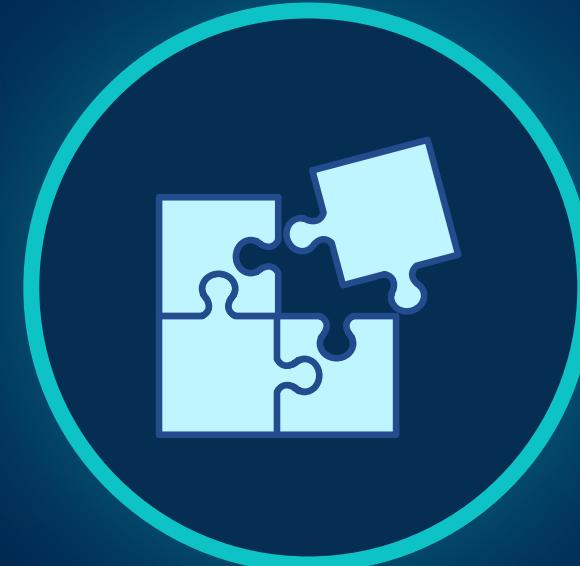
Are findings and recommendations up to date with the current infrastructure?

Has new risk been introduced into the environment?

Threat Model & Table Top

Where are threats being identified for remediation?

Is your plan effective? What could be improved?



Practical Tips and Recommendations

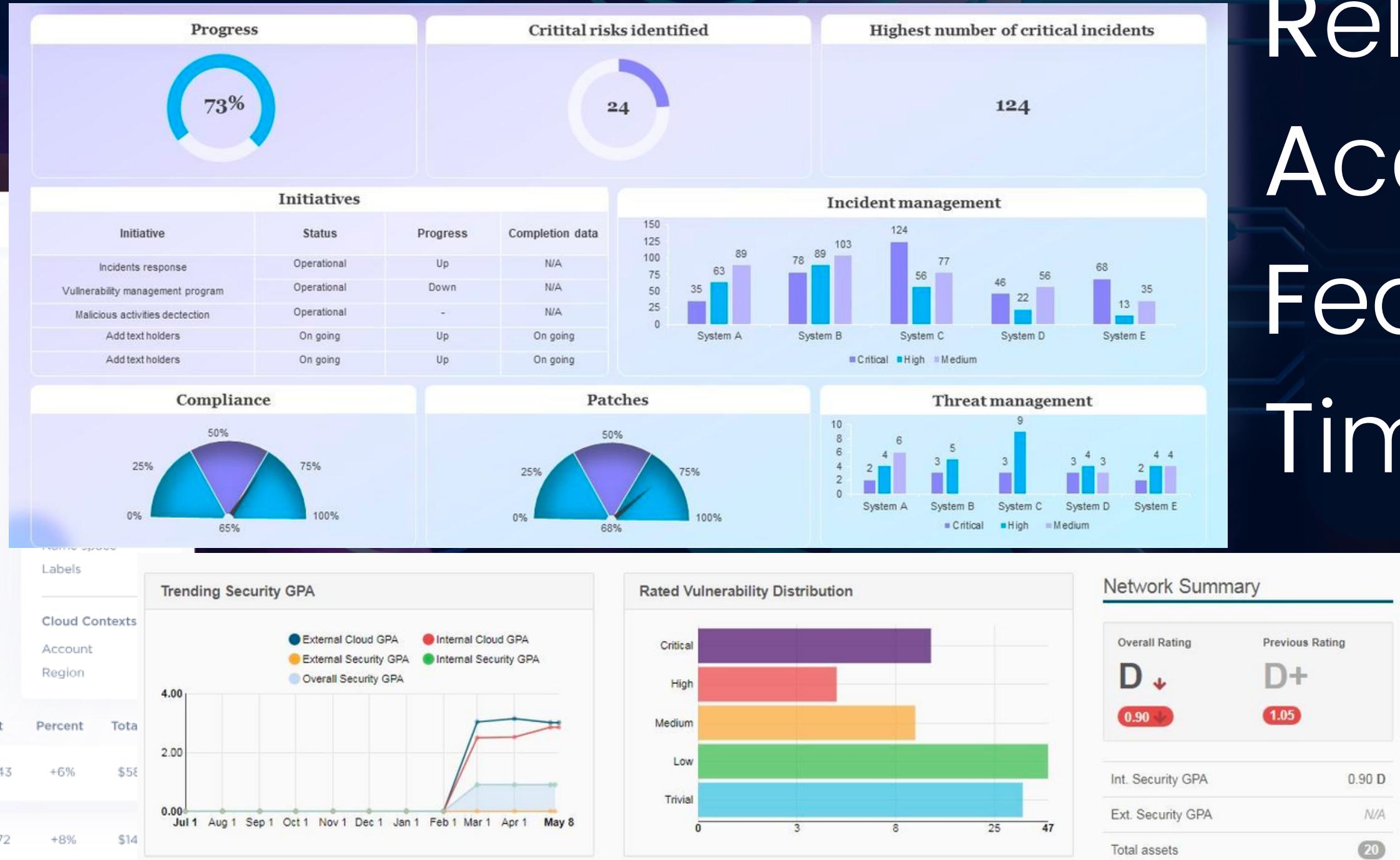


Michael Tayo
/michaeltayo

Measuring a Cloud Security Program

How do we know if we are on the right track?

Choose the right metrics



Relevant
Accurate
Feasible
Timely

"Not all metrics are created equal"



Michael Tayo
/michaeltayo

Key Metrics and Indicators

Performance & Posture

MTTD & MTTR

SLA Compliance (%)

Secure Score*

Budget

of Incidents

of Privileged Accounts

of Sensitive Data Exposures

of WAF Deny/Blocks

of Outdated SSL Certificates

of long-running VM instances

"Data is like garbage.
You'd better know what
you are going to do with
it before you collect it."

Mark Twain



Michael Tayo
/michaeltayo

Optimizing a Cloud Security Program

Rule #1: Don't try to boil the ocean

SET CLEAR GOALS AND OBJECTIVES

What do you want to achieve with your security program?

MEASURE THE RIGHT METRICS

Identify areas where you are doing well and areas where you can improve.

Focus on metrics that are relevant to your goals and objectives.

EVALUATE YOUR RESULTS

Make changes to your program based on the results of your measurements.

CONTINUOUSLY MONITOR AND IMPROVE

Cloud security is an ever-evolving landscape.

Make improvements as needed to ensure your program remains effective.



Michael Tayo
/michaeltayo



Summary

Cloud Security Best Practices

- The Shared Responsibility Model
- IAM & Data Governance
- Security Baselinging

Managing Cloud Security Risk

- Shift Left Security
- Continuous Monitoring & Threat Detection
- Incident Response and Recovery

Measuring & Optimizing Cloud Security

- RAFT
- Performance vs Posture
- Don't try to boil the ocean



Michael Tayo
[/michaeltayo](https://www.linkedin.com/in/michaeltayo/)

Thank You



Michael Tayo
[/michaeltayo](https://www.linkedin.com/in/michaeltayo)