Continuous Threat Detection and Monitoring

Brian Galloway
Security Leader, Solutions Architecture
AWS Worldwide Public Sector

Agenda

AWS Worldwide Public Sector US Education and State & Local Government (EDU | SLG)

SLG | Education Regulations and Standards

Challenges and Threats in EDU and SLG

Mitigation with Frameworks and Guiding Principles

Cloud Native Approach to Threat Detection and Monitoring

Worldwide Public Sector
US Education and State & Local Government

WWPS US EDU/SLG

- Our **Mission** is to enable and support our SLG and EDU customers and partners in their journey with AWS.

State & Local Government

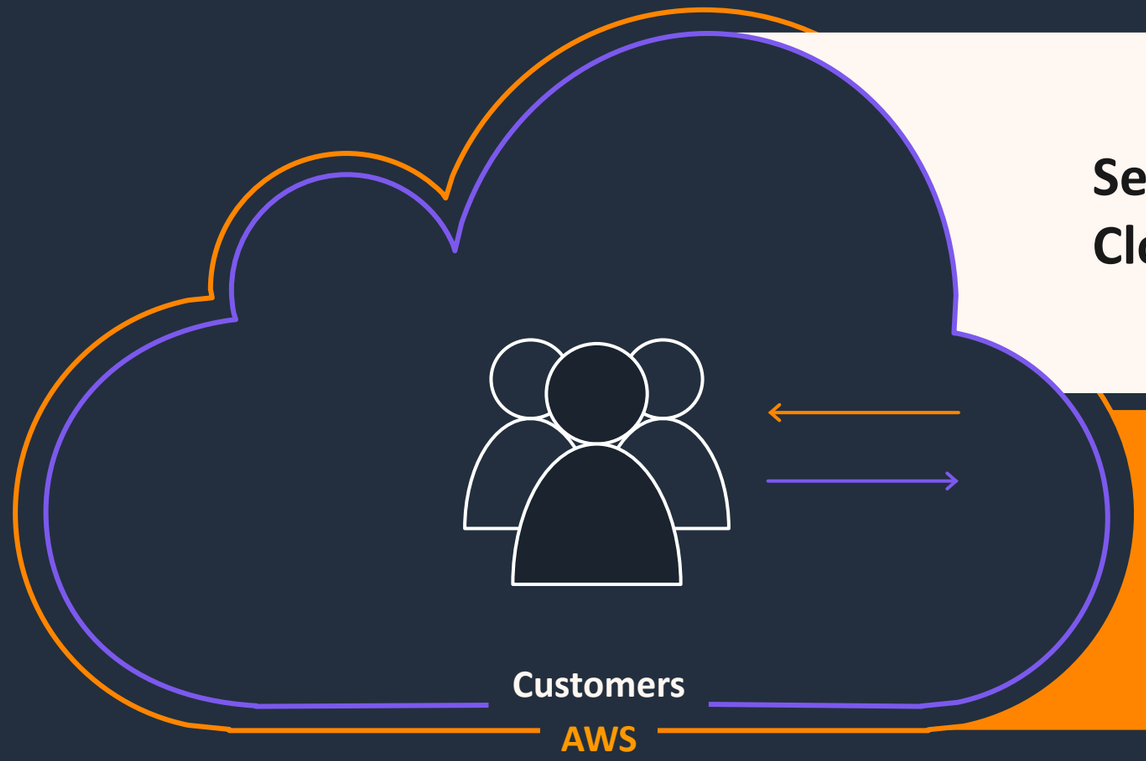
Elections	Health & Human Services
Justice & Public Safety	Transportation
Finance & Administration	Public Utilities

Education

Academic Medical Centers	Higher Education
K12	Research

Regulations and Standards

Shared responsibility model



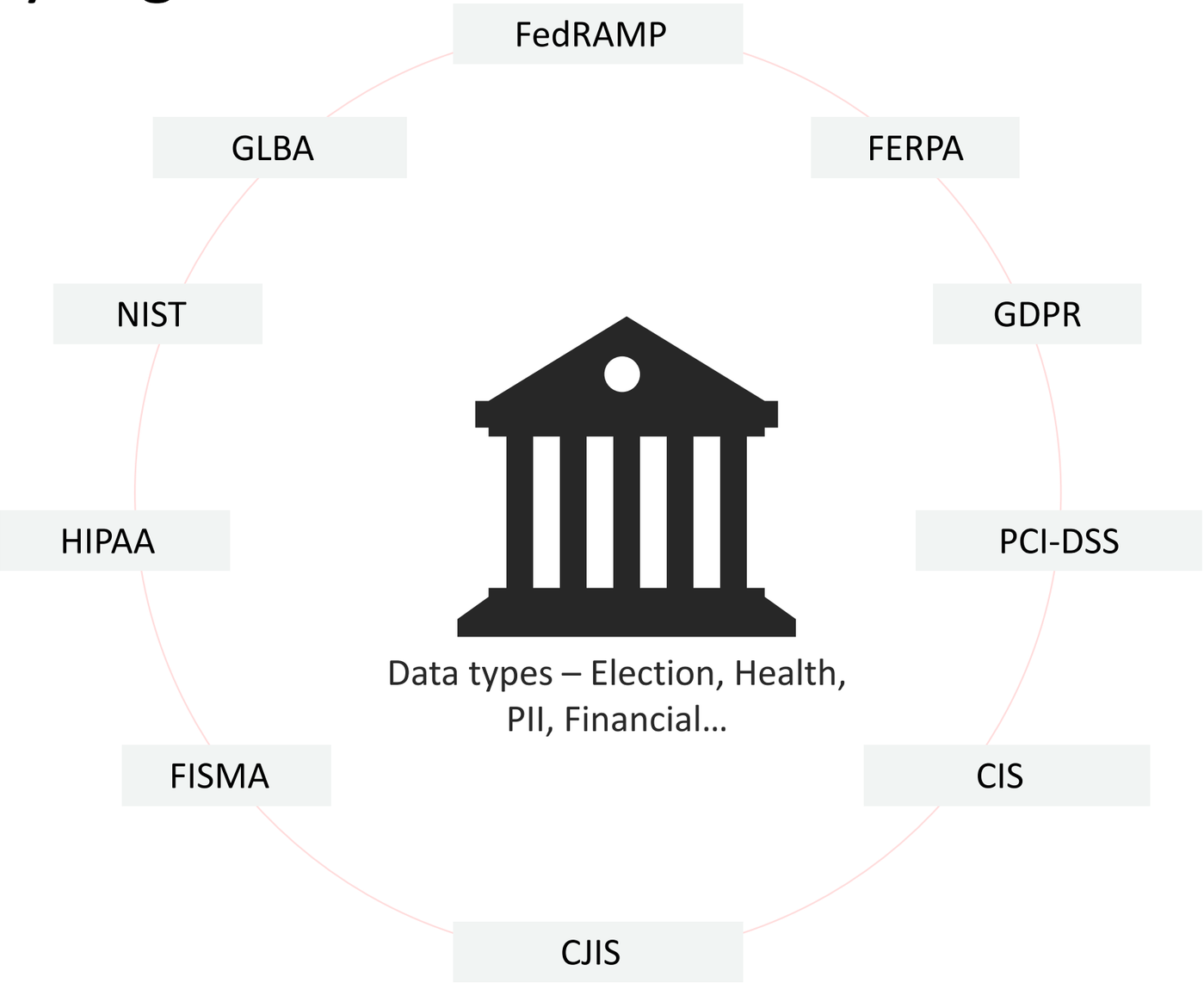
Security IN the Cloud

Customer responsibility is determined by the AWS Cloud services a customer selects.

Security OF the Cloud

AWS is responsible for protecting the infrastructure that runs all the services offered in the AWS Cloud.

SLG | EDU Key Regulations and Standards



Inherit global security and compliance controls

CSA cloud security alliance℠	CyberGRX exchange member THIRD-PARTY CYBER RISK MANAGEMENT	ISO 9001 International Organization for Standardization	ISO 22301 International Organization for Standardization	ISO 27001 International Organization for Standardization	ISO 27017 International Organization for Standardization
ISO 27701 International Organization for Standardization	ISO 27018 International Organization for Standardization	PCI Security Standards Council PARTICIPATING ORGANIZATION™	AICPA SOC SOC 1	AICPA SOC SOC 2	AICPA SOC SOC 3
CCCS PIPEDA	CJIS	FR FedRAMP	FERPA	FIPS 140-2 CRYPTOGRAPHY	FISMA FEDERAL INFORMATION SECURITY MANAGEMENT ACT
GxP	HIPAA	International Traffic in Arms Regulations Compliant ITAR	MPAA	SEC Rule 17a-4(f)	VPAT Section 508
FINTECH	FISC	irap	정보보호 관리체계 인증 ISMS Information Security Management System	iDA SINGAPORE	FFIEC Federal Financial Institutions Examination Council
C5	CISPE data protection COMPLIANCE	CYBER ESSENTIALS PLUS	CERTIFICACIÓN DE CONFORMIDAD CON EL ens Esquema Nacional de Seguridad Categoría ALTA RD 3/2010	G-Cloud	TISAX ENX ASSOCIATION

Challenges and Threats in EDU and SLG

Key Terms and Definitions

- A **Threat** is any circumstance or event with the potential to adversely impact organizational operations, organizational, assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification, and/or denial or service.

- **Risk** is a measure of the extent to which an organization is threatened by a potential circumstance or event. Typically a function of adverse impacts, likelihood, and frequency.

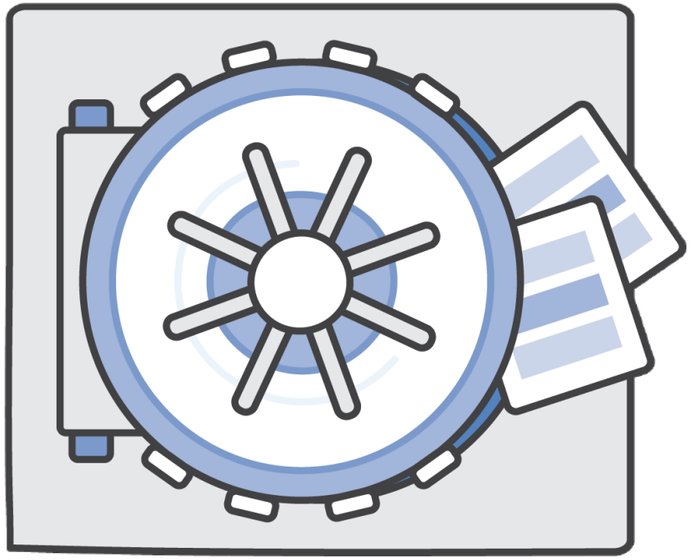
- Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source is a **Vulnerability.**

- **Mitigation** is a decision, action, or practice intended to reduce the level of risk associated with one or more threat events, threat scenarios, or vulnerabilities.

Key Terms and Definitions - CIA security triad model

Confidentiality

- Data should be accessed only by authorized principles; it is imperative to maintain a strong data classification policy
- Prevent disclosure attacks, leakage, and theft



Integrity

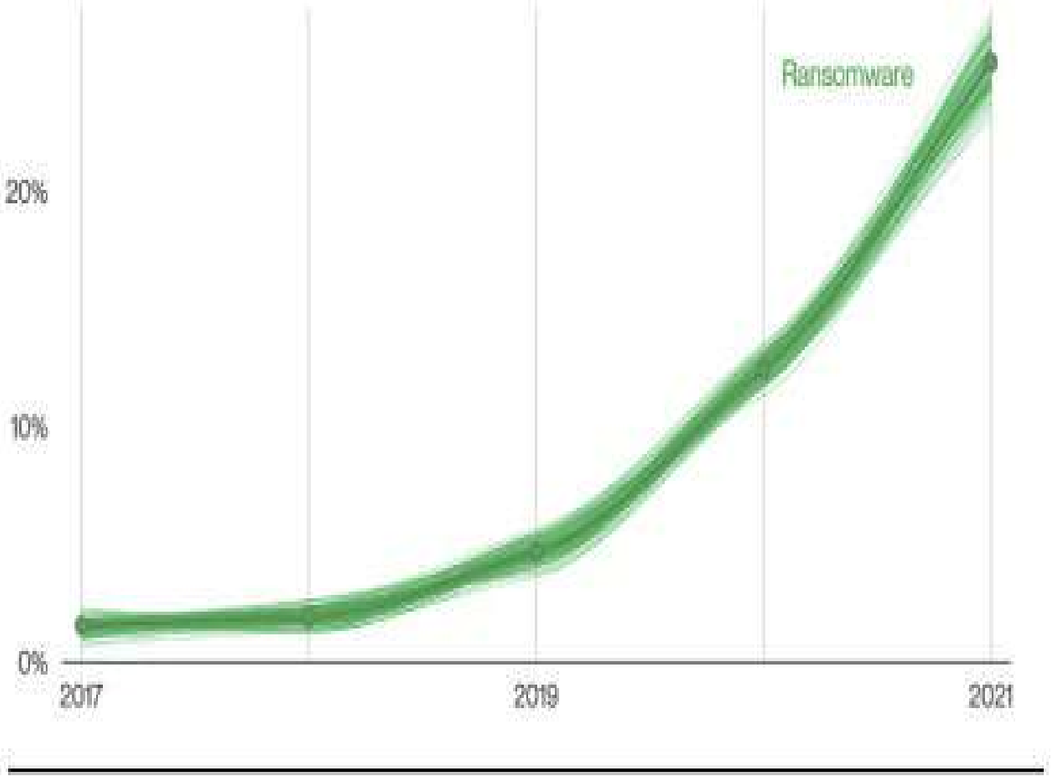
- Data are trustworthy, coherent, and modified only by authorized principles
- Prevent alteration attacks and unauthorized modification

Availability

- Provide reliable, timely access to data when required
- Prevent destruction attacks & denial of service at the data layer

Threats Facing SLG & EDU

- Supply Chain attacks/Third Party Risks
- Critical Infrastructure attacks
- Business Email Compromises
- Insider Threats
- Ransomware/Phishing attacks
- Emerging Threats – The unknown

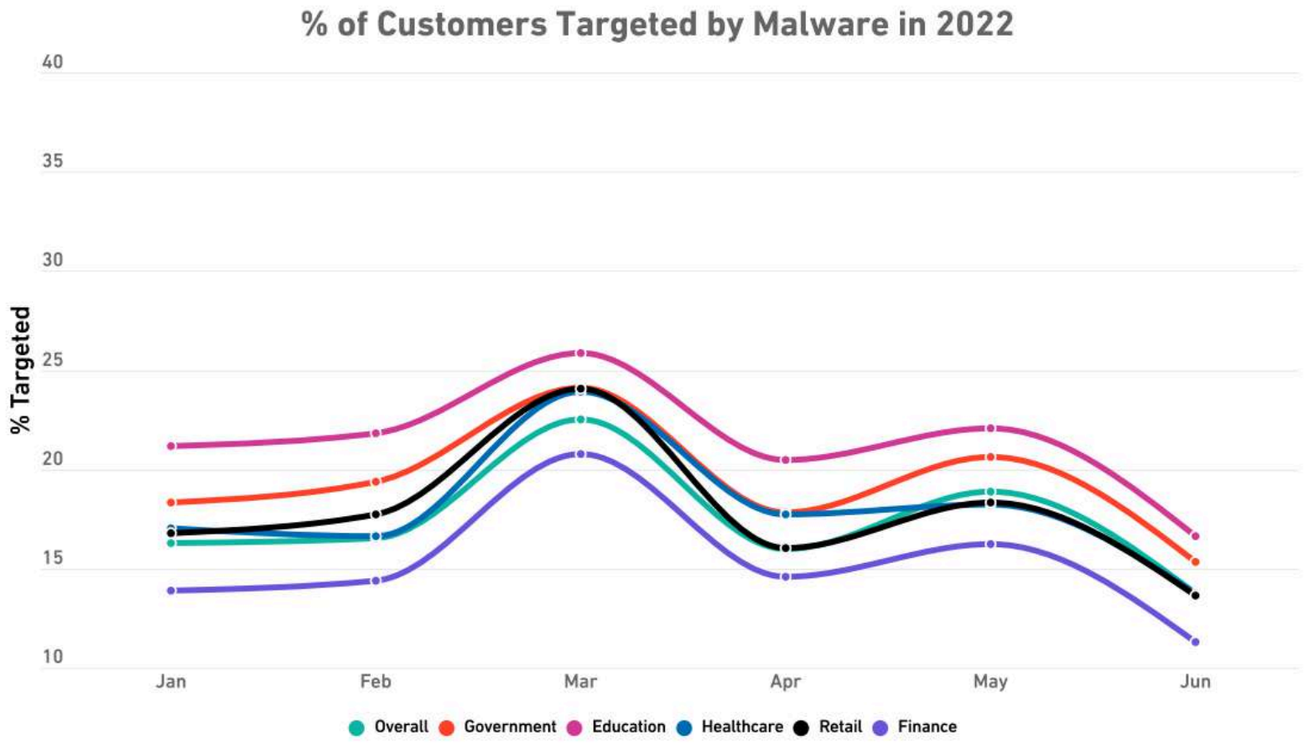


Source: 2022 Verizon Data Breach Investigations Report

Threats Facing SLG & EDU

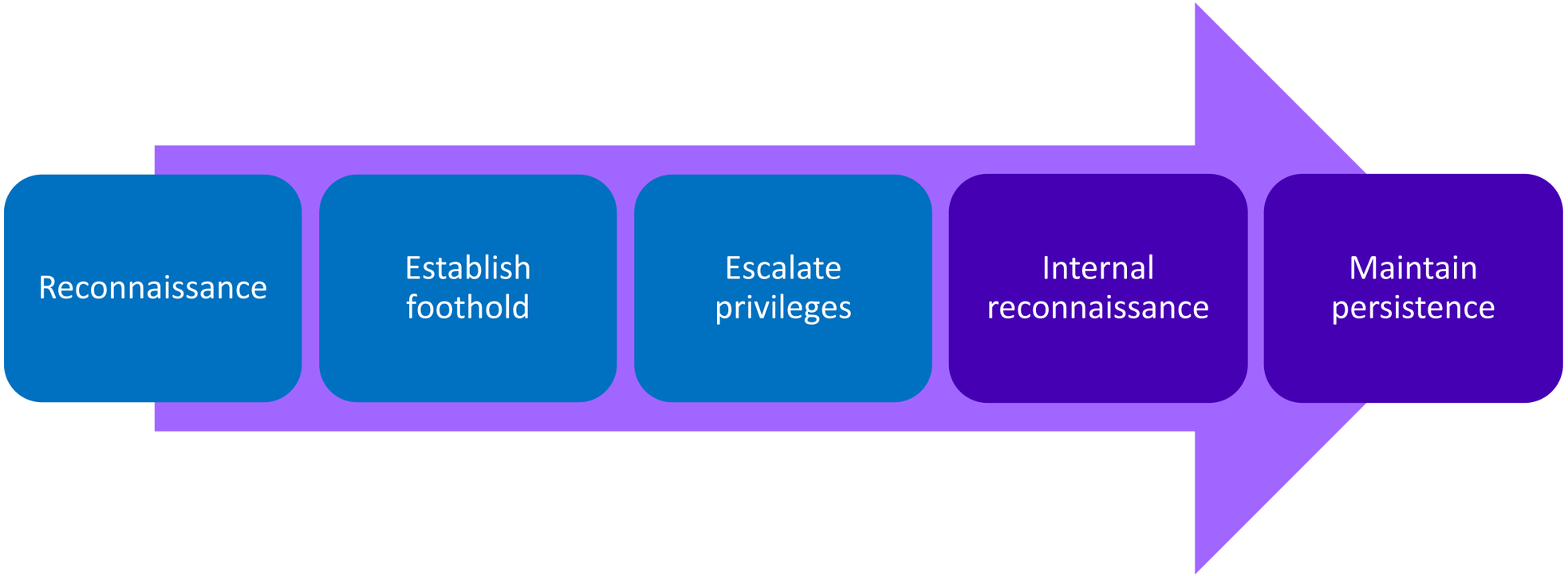
2020 Deloitte - NASCIO Cybersecurity Study identified these top barriers for States to overcome:

- Insufficient cyber budget
- Lack of skilled cyber professionals
- Legacy Infrastructure and solutions
- Inadequate availability of cybersecurity professionals
- Lack of recurring/dedicated cyber budget



Source: 2022 Sonicwall Cyber Threat Report

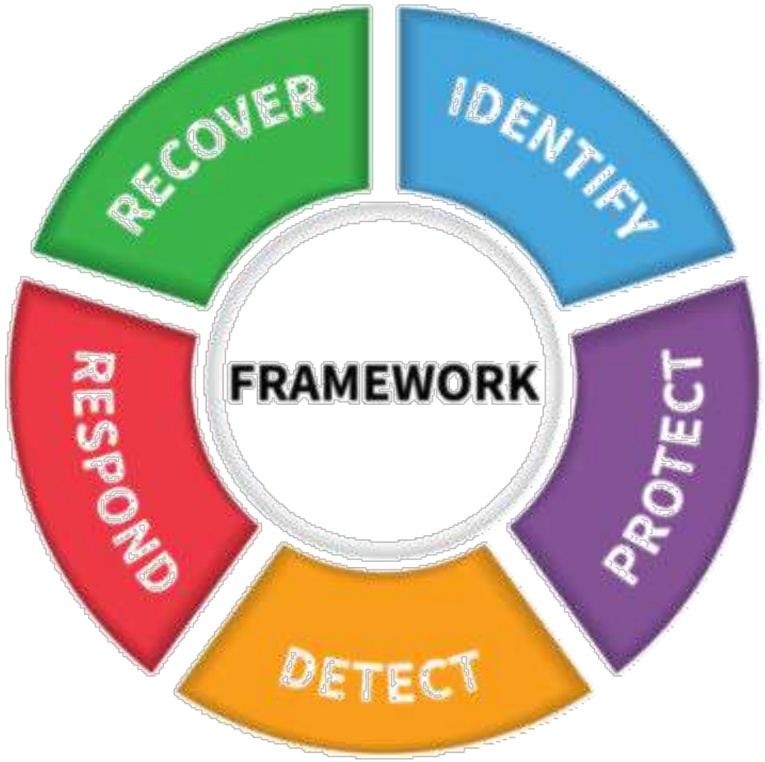
Intrusion life cycle: Stages



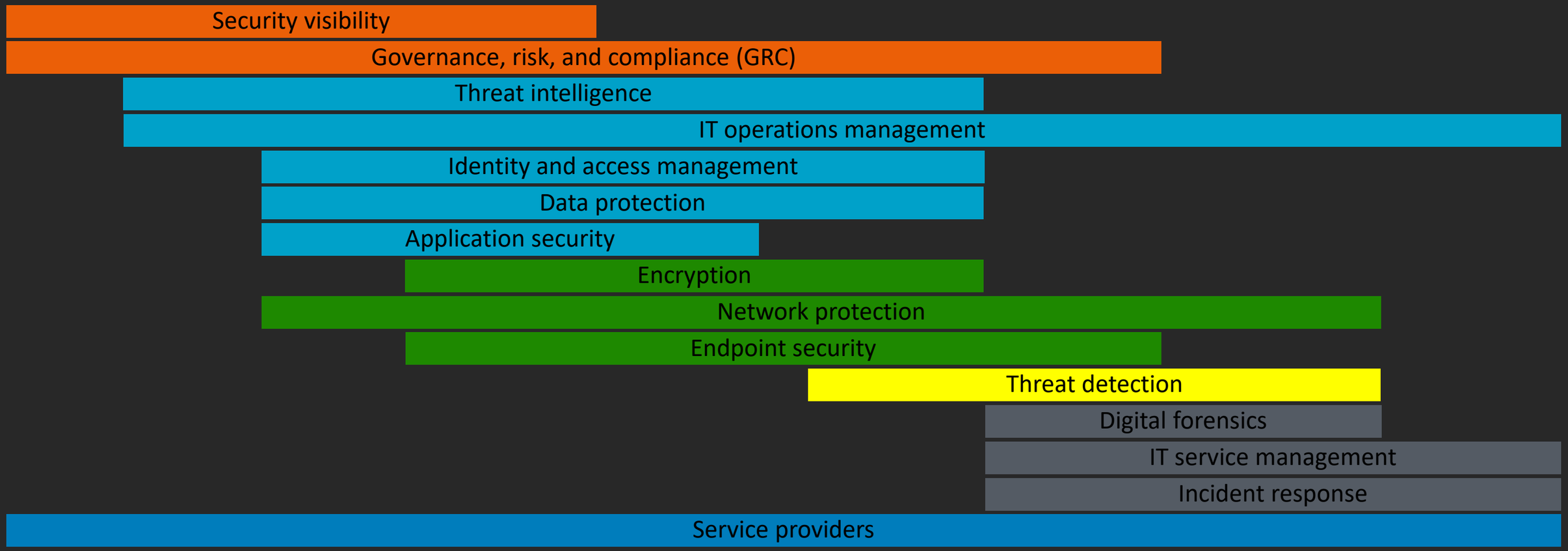
Mitigating threats with frameworks and guiding principles

NIST Cybersecurity Framework

- A **voluntary framework** comprised of **best practices** to help organizations of any size and in any sector improve the cybersecurity, risk management, and resilience of their systems



Security in the cloud (Using the NIST CSF)



Identify

Security fundamentally anchors on having sufficient knowledge of your world

Protect

The best defense is a good offense, but…

Detect

One must “assume breach” and have a strong defense

Respond/Recover

Knowing and being able to act swiftly is key in the cloud

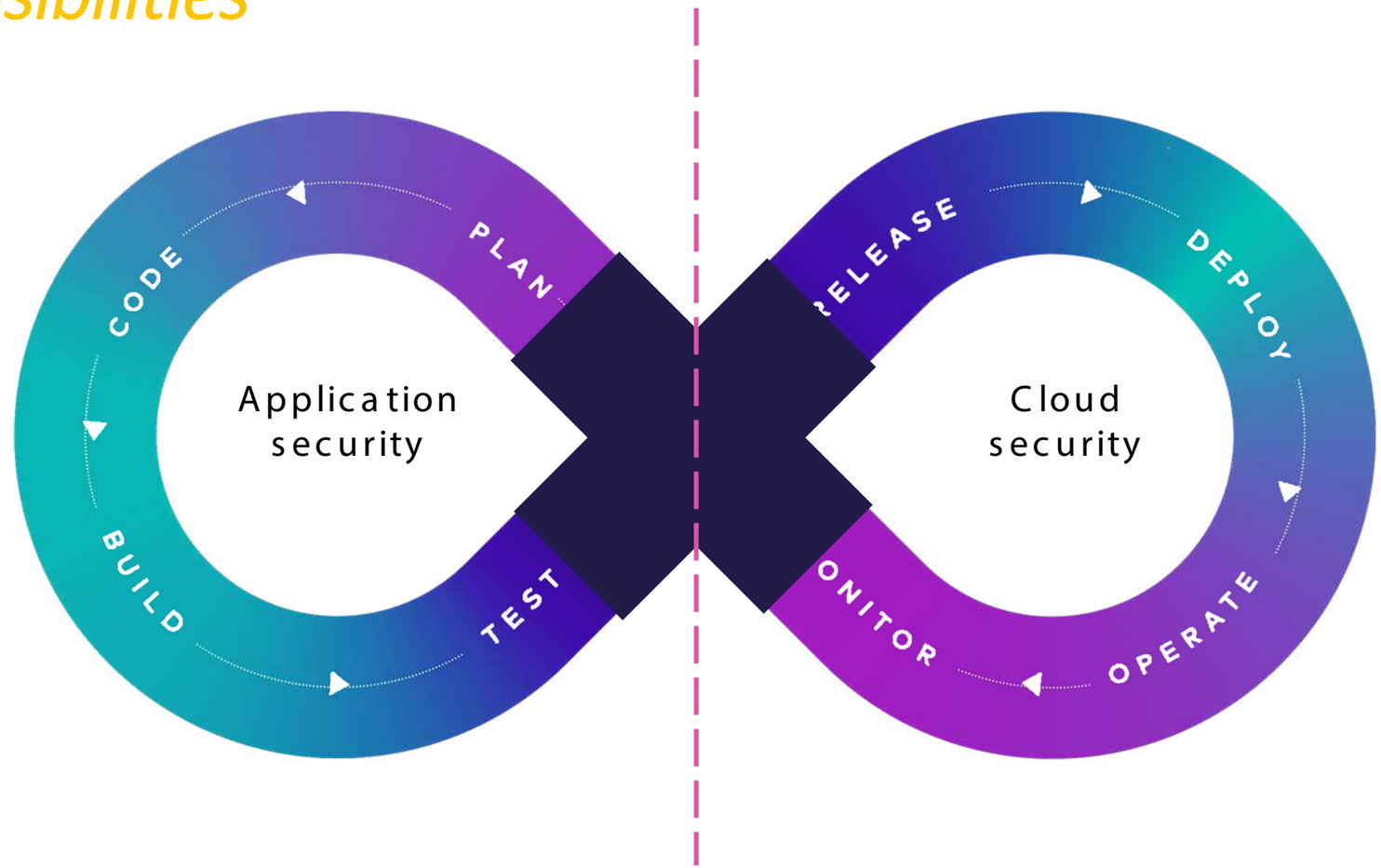
Web Application Security Checklist

- Error Handling and Logging
- Data Protection
- Configuration and Operations
- Authentication
- Session Management
- Input and Output
- Access Controls

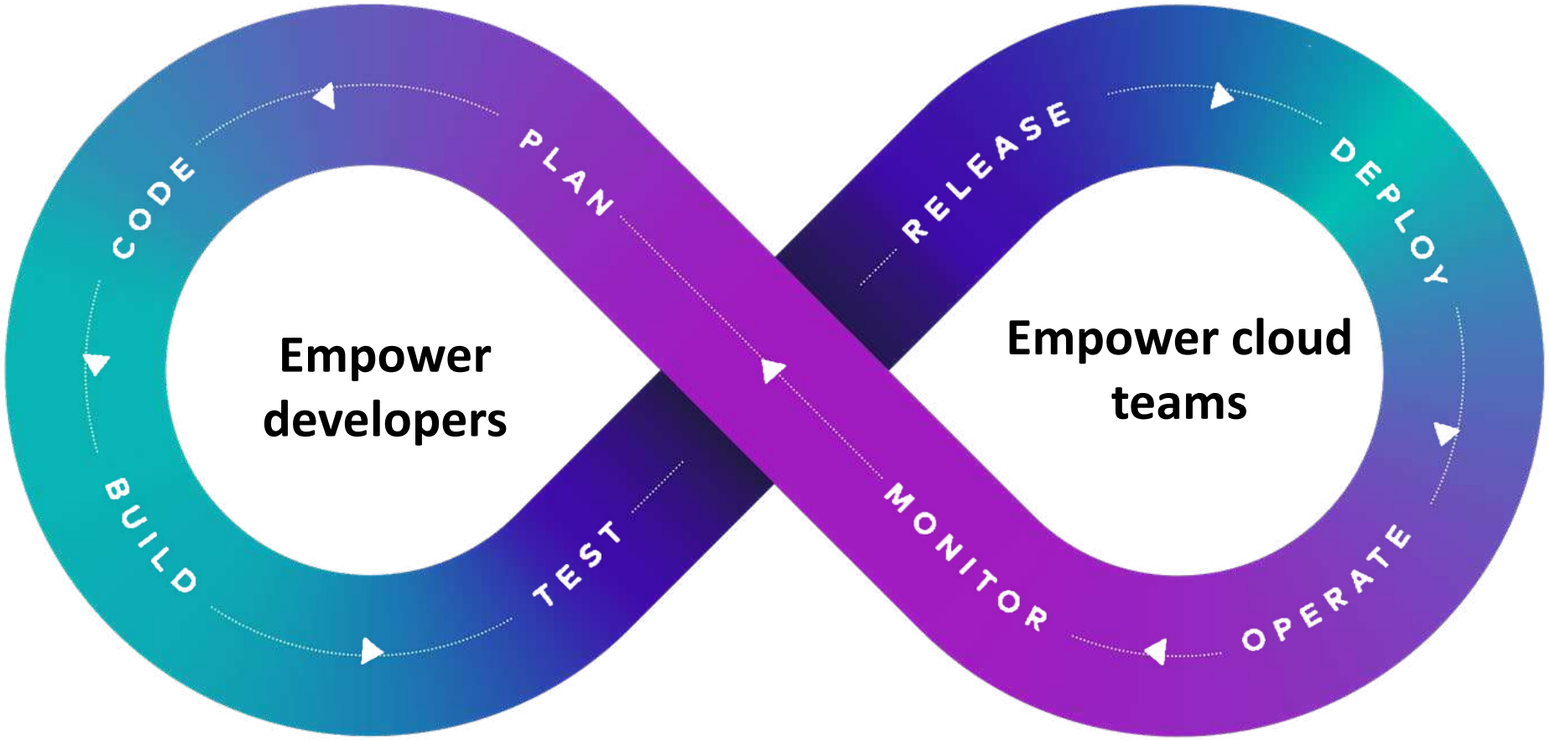
Source: https://www.sans.org/cloud-security/securing-web-application-technologies/

Employ DevSecOps

Applications and cloud are still often treated as siloed responsibilities



DevSecOps requires removing barriers between dev, ops, and security



Implement Zero Trust

A conceptual security model and associated set of mechanisms that focus on providing security controls around digital assets that do not solely or fundamentally depend on traditional network controls or network perimeters

Components

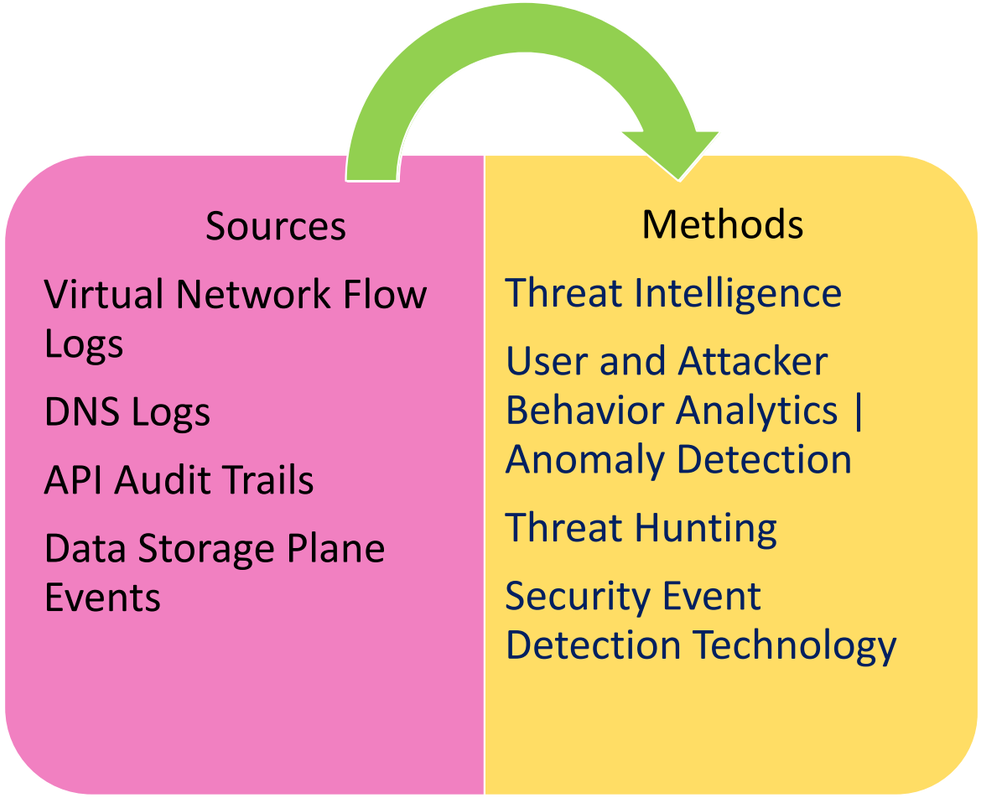
- Policies and Policy Engines
- Analytics and Confidence Scoring
- Decision Points and Enforcement Points

Guiding Principles

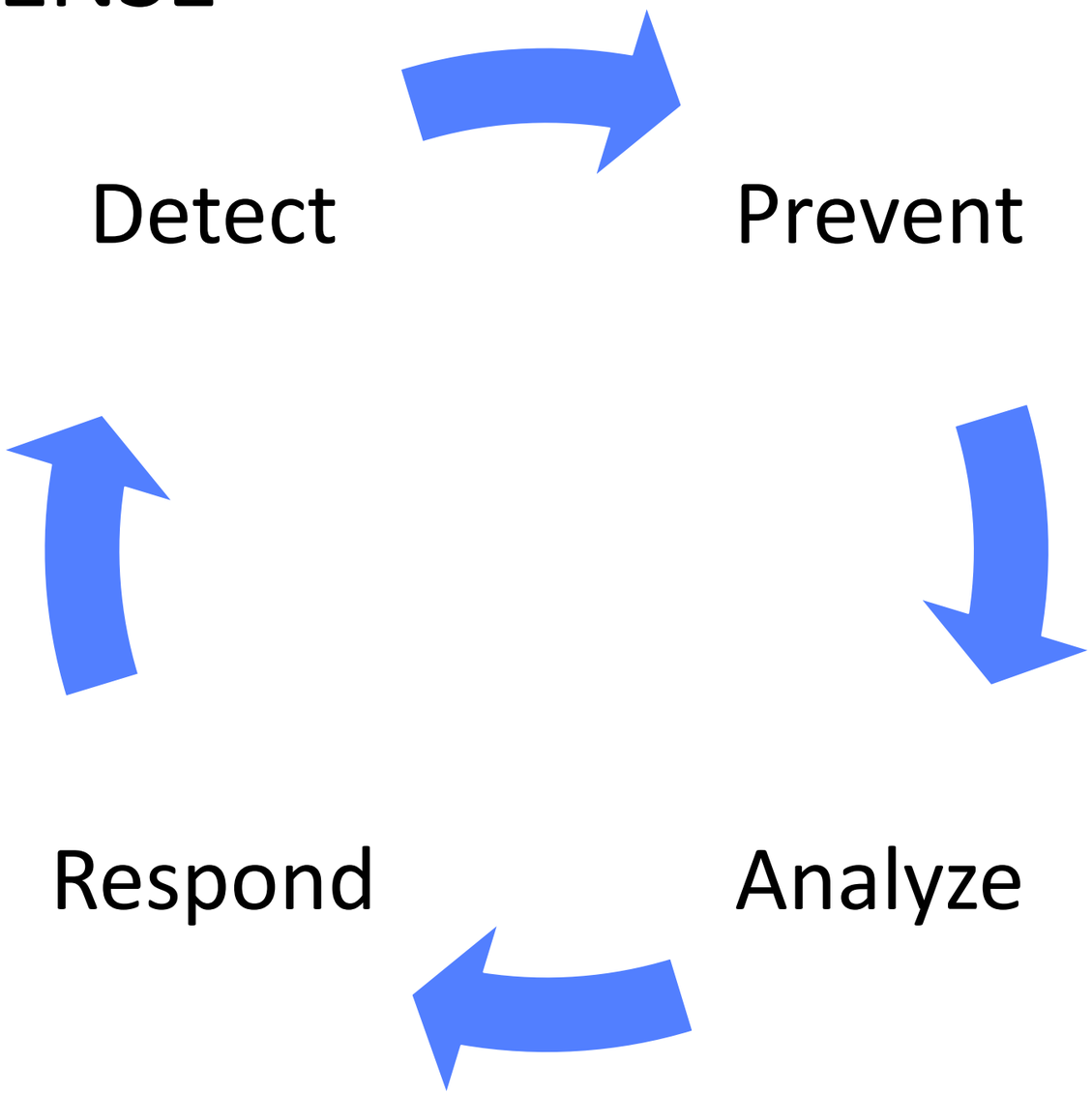
- Avoid a binary choice
- Focus on use cases

Cloud Native Approach: Playing Defense

Threat Detection Sources and Methods



ADAPTIVE DEFENSE

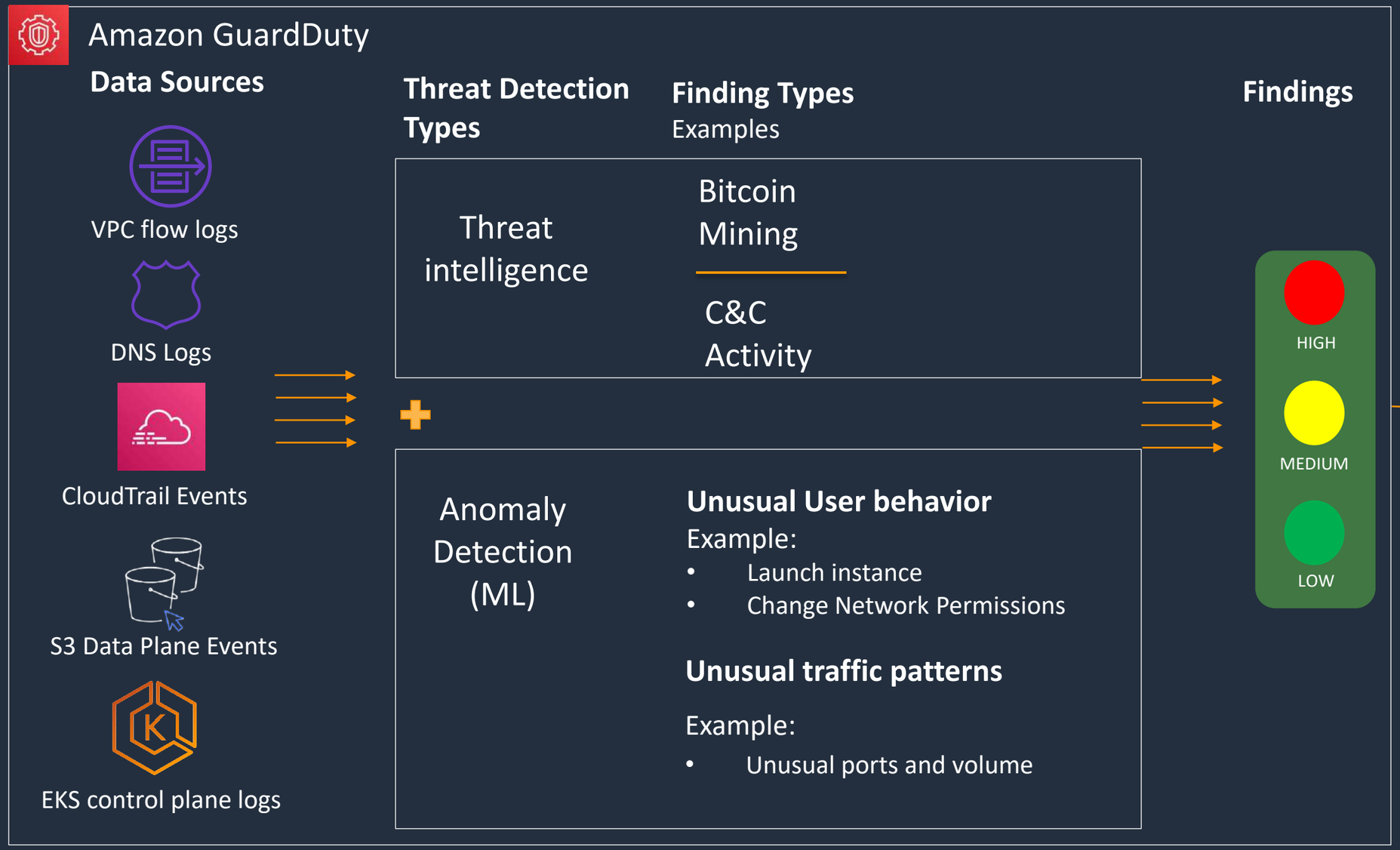


Threat Detection Finding Types

- Backdoor Finding Types
- Behavior Finding Types
- Crypto Currency Finding Types
- PenTest Finding Types
- Persistence Finding Types
- Policy Finding Types
- Privilege Escalation Finding Types
- Recon Finding Types
- Credential Access Finding Types
- Execution Finding Types

Cloud Native Approach: Example on AWS

Threat Detection and Monitoring on AWS



Amazon Detective

AWS Security Hub

CloudWatch Event

- Alert
- Remediate
- Partner Solutions
- Send to SIEM

Best Practices for Continuous Threat Detection and Monitoring

- Record workload configurations and measure drift/deviation from established ”gold” standard baselines
- Continuously measure security posture by checking against benchmarks (CIS Benchmarks)
- Use DevOps automation and Infrastructure as Code (IaC) to provide continuous compliance across accounts and regions.
- Enabled AI-based threat and malware detection using various log sources
- Centralized findings across workloads and regions

Call to Action

- Please reach out to your AWS account team or myself to deeply explore threat detection and monitoring on AWS
  - Account Team – Heather Kirk (heakirk@amazon.com); Steve Evernham (sweve@amazon.com)
  - Well-Architected Reviews
  - Amazon GuardDuty and AWS Security Hub Demonstrations
  - Proof of Concepts

Thank you!

Brian Galloway
bgallow@amazon.com