aws partnercast

Proactive Security

Defending against the modern day threats

6 June, 2023

Kirti Dhabhai, Technical Account Manager

Shagun Beniwal, Technical Account Manager

aws partnercast

Agenda

- Background
- Current Trends
- Shift Left Strategy
- Demo – Reactive vs Proactive approach
- Key Takeaways

Background

aws partnercast

Modern Day Threats

- **Zero Days:** A zero-day attack (also referred to as Day Zero) is an attack that exploits a potentially serious software security weakness that the vendor or developer may be unaware of.

- **Advanced Persistent Threats (APTs):** APTs are a covert cyber attack on a computer network where the attacker gains and maintains unauthorized access to the targeted network and remains undetected for a significant period.

- **Polymorphic Malware:** It is a type of malware that is programmed to repeatedly mutate its appearance or signature files through new decryption routines. This makes many traditional cybersecurity tools, which rely on signature based detection, fail to recognize and block the threat.

aws partnercast

Security: Reactive vs Proactive

- **Reactive:** It is everything you do after an attack occurs. Reactive measures do aim to mitigate an attack's harm on the organization, but as the name implies, they are reacting to an event.

- **Proactive:** It is everything you do before an attack takes place. Proactive security measures are all processes and activities performed periodically and continuously within the organization, focused on identifying and eliminating vulnerabilities within the network infrastructure, preventing security breaches, and evaluating the effectiveness of the business security posture in real-time.

aws partnercast

Current Trends

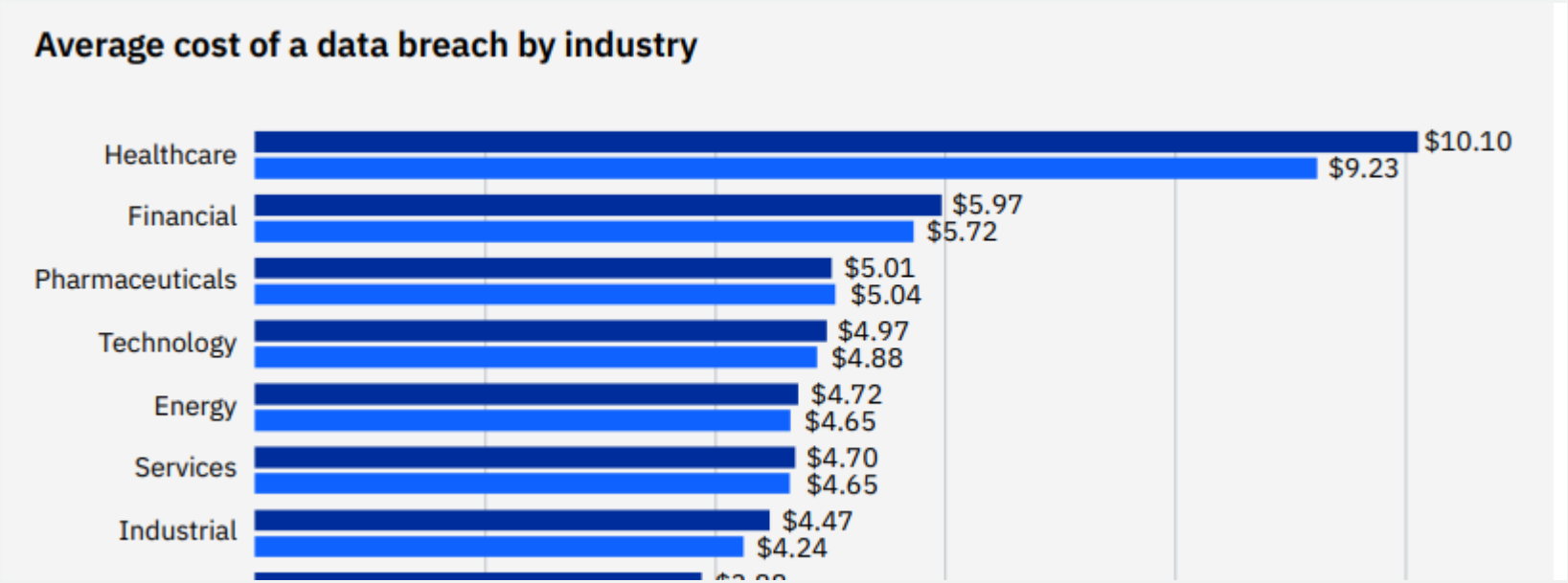
aws partnercast

Average cost of a data breach

$4.35 million
Average total cost of a
data breach

$4.54 million
Average cost of a
ransomware event

$4.82 million
Average cost of a
critical infrastructure data breach

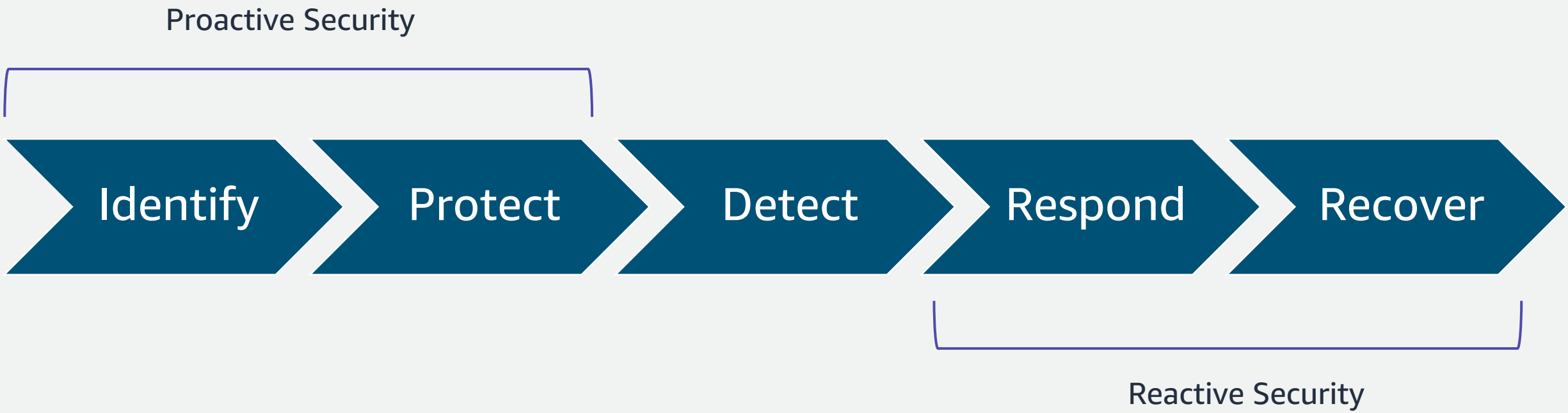


* Measured in USD millions

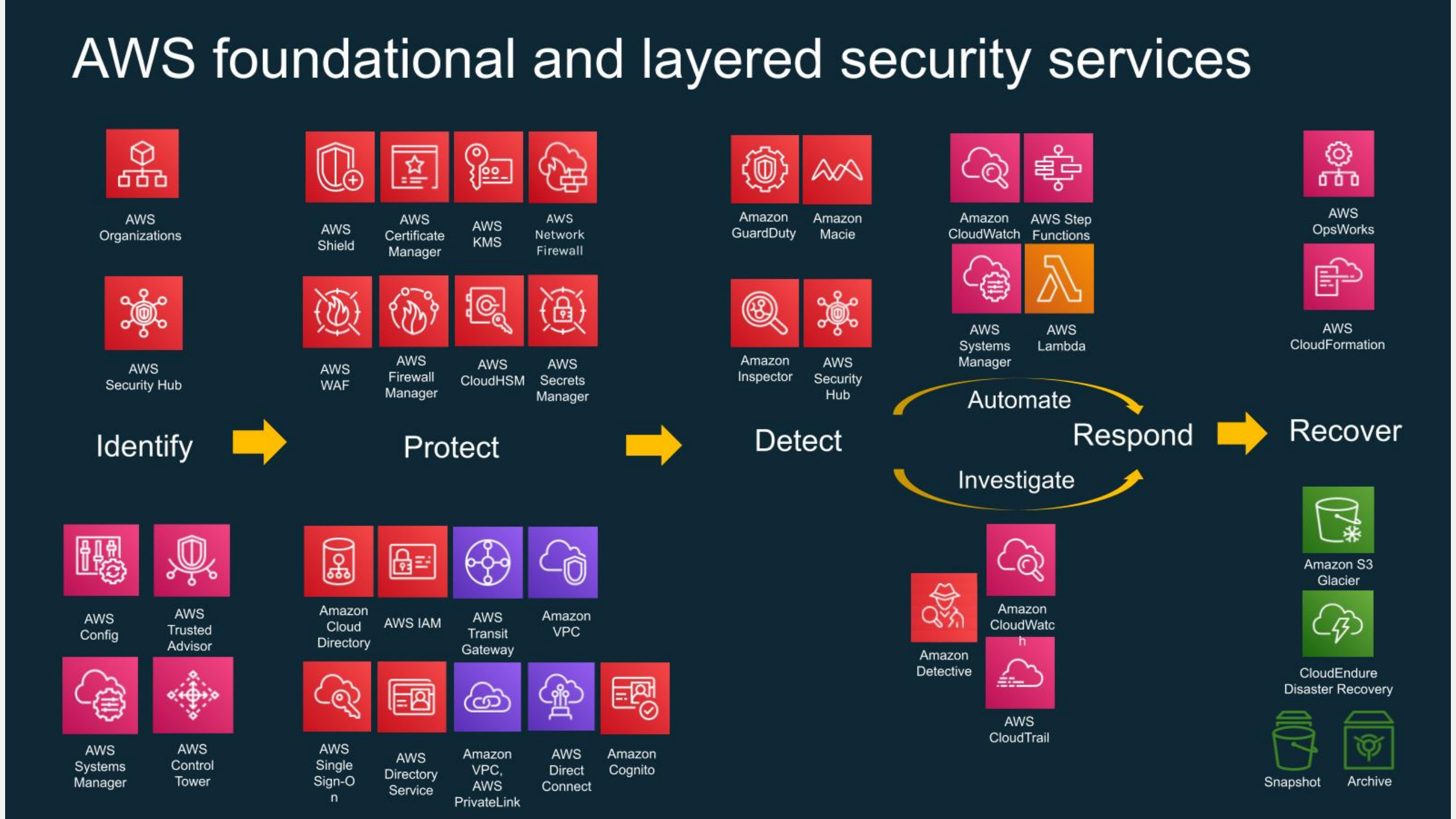
Source: IBM

aws partnercast

NIST Cyber Security Framework

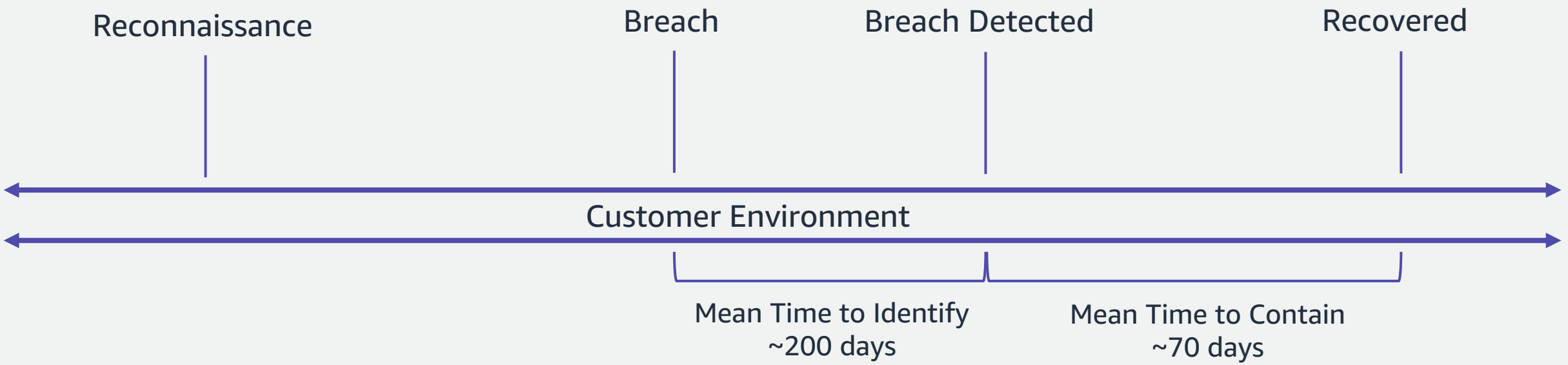


AWS foundational and layered security services



aws partnercast

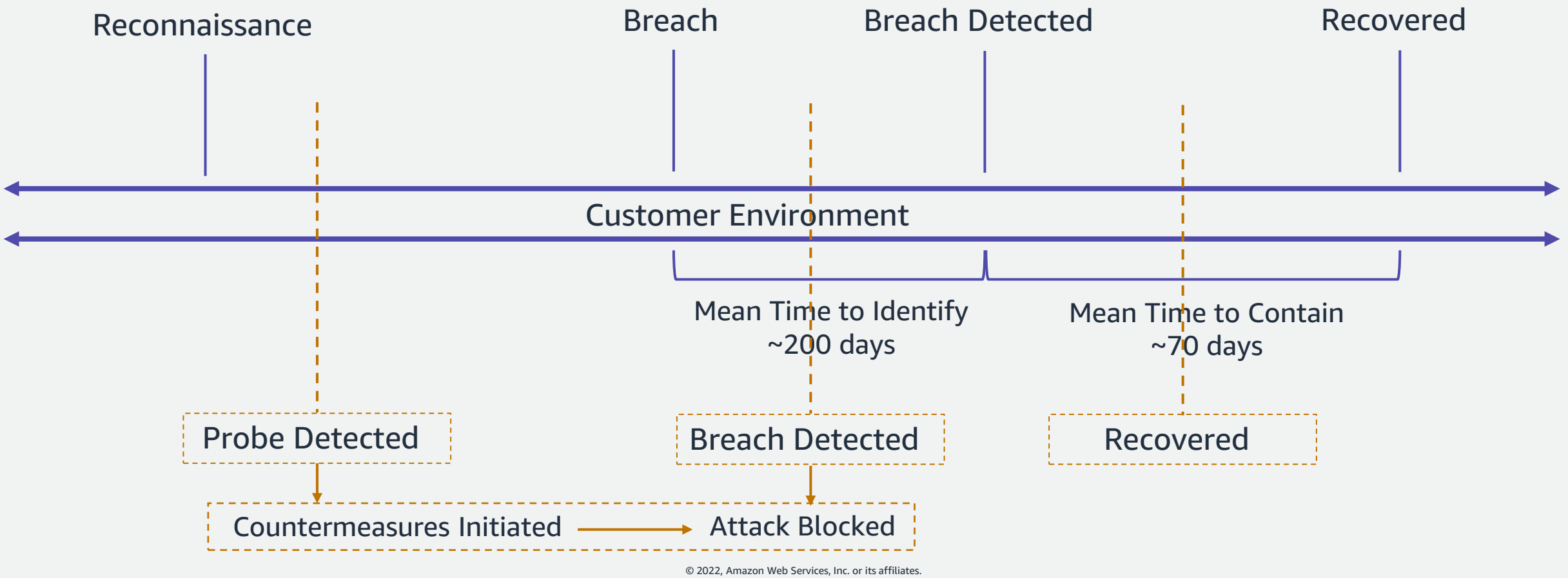
Cyber Attack Chronology – Reactive



aws partnercast

Cyber Attack Chronology – Proactive

Shifting Left helps become proactive.

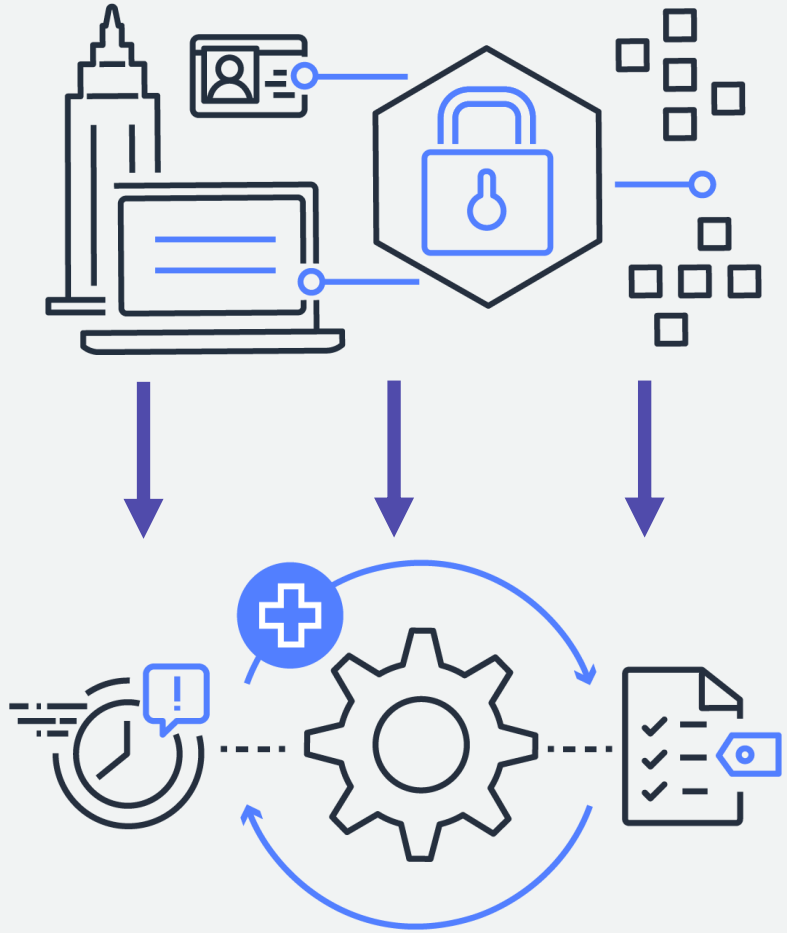


aws partnercast

Identifying attacks faster

To identify attacks and probe attempts we will use a bunch of sources –

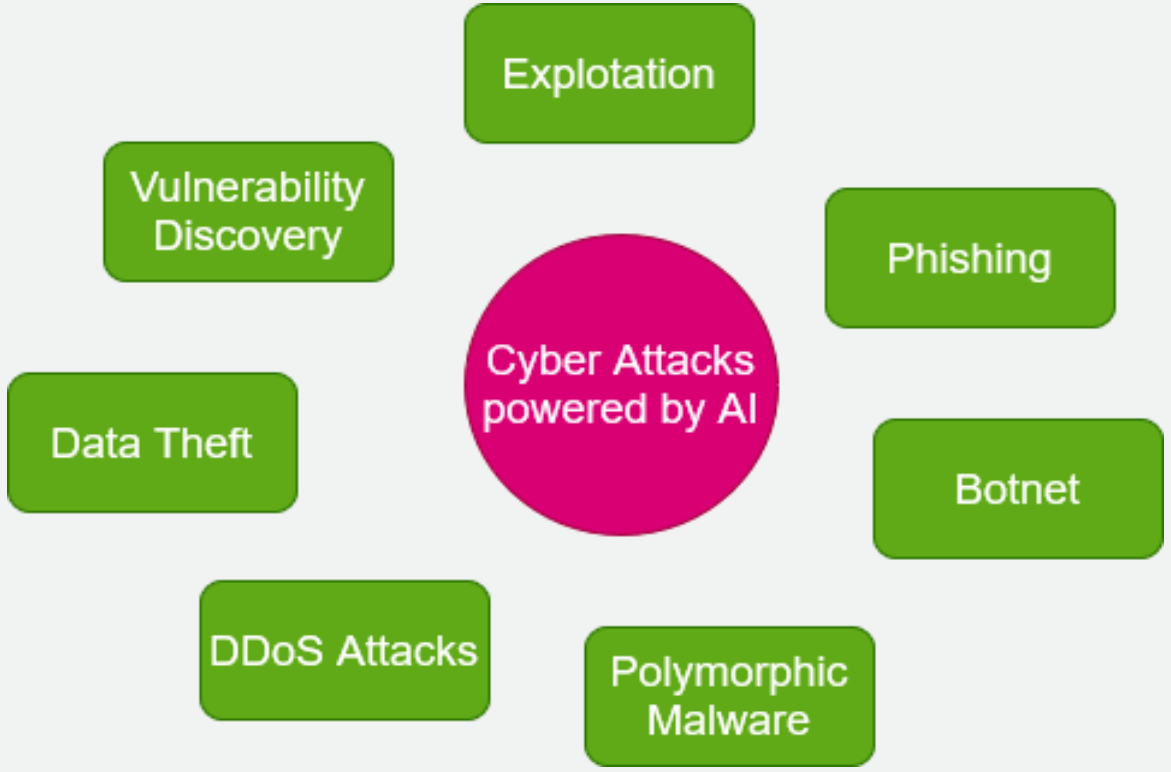
- Indicators of Compromise (IoC)
- Indicators of Attack (IoA)
- Security/Threat Intelligence
- Vulnerability Scans
- Red team exercises
- Tooling
  - Extended Detection & Response (XDR)
  - Security Information & Event Management System (SIEM)
  - User Behaviour Analytics (UBA)
  - Artificial Intelligence & Machine Learning capabilities



aws partnercast

How AI/ML are fueling cyberattacks?

- Use AI to identify fresh vulnerabilities in networks, devices and applications.
- AI can learn to spot patterns in behavior and increase effectiveness of any social engineering attacks.
- AI-based botnets can outpower defense systems to launch massive DDoS attacks. AI predicts the defense side strategies, which will help the botnet to devise new ways to exploit systems.



aws partnercast

Application Security - Shift Left Strategy

aws partnercast

Application testing

Shift left

Shift right

Testing new requirements

Testing new code

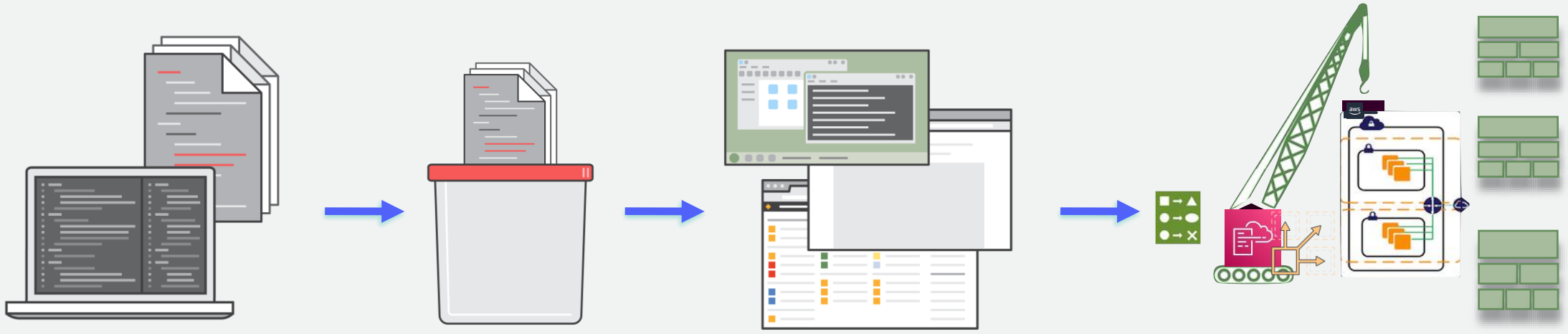
Test every build

Testing every deployment

Testing on production

How does this apply to Infrastructure as Code (IaC)?

Infrastructure as code – Recap



Code in YAML or JSON directly or use sample templates

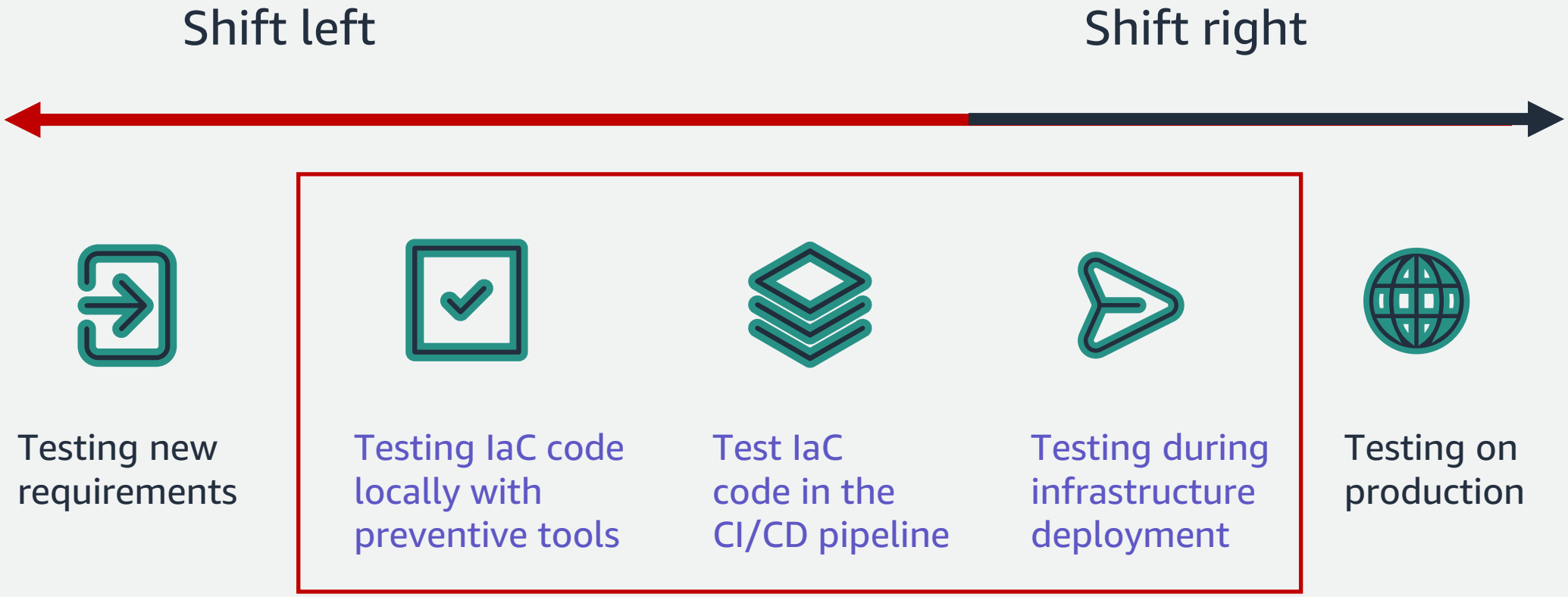
Upload local files or files from an Amazon S3 bucket

Create stack using console, API, or CLI

Stacks and resources are provisioned

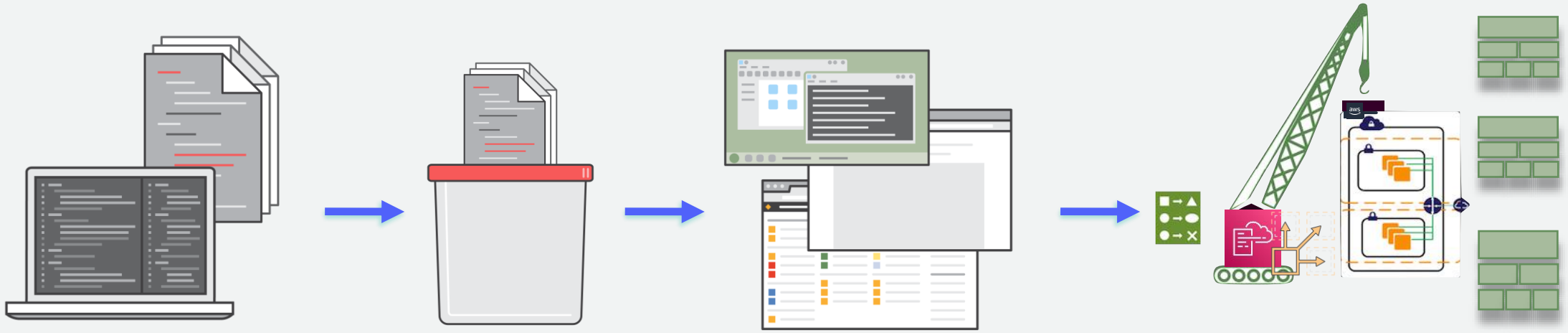
aws partnercast

Shift-left application testing



aws partnercast

Infrastructure as code – Expanded

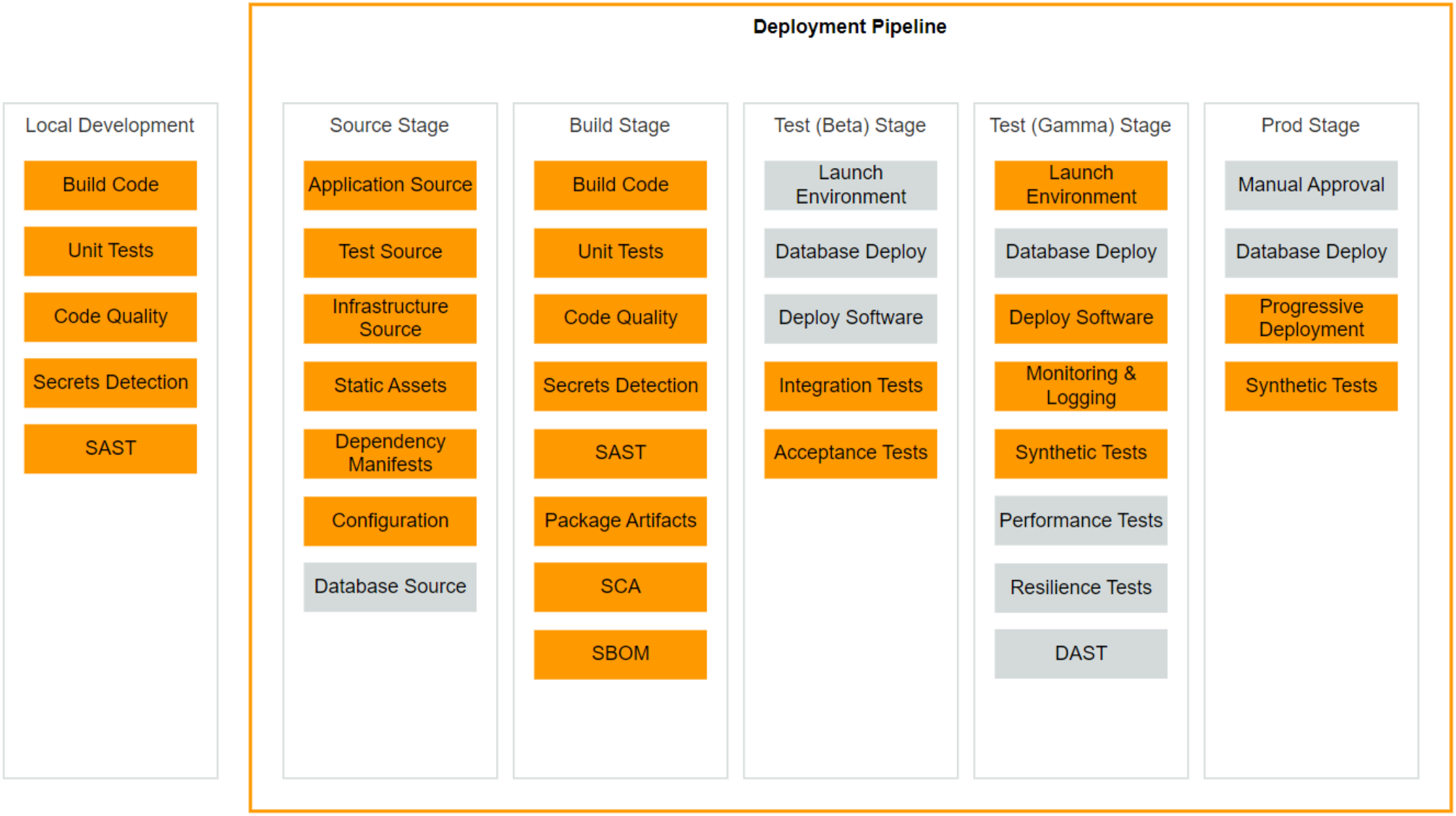


Testing IaC code locally with preventive tools

Upload local files or files from an Amazon S3 bucket

Test IaC code in the CI/CD pipeline

Testing during infrastructure deployment


Deployment Pipeline
Local Development
Build Code
Unit Tests
Code Quality
Secrets Detection
SAST
Source Stage
Application Source
Test Source
Infrastructure Source
Static Assets
Dependency Manifests
Configuration
Database Source
Build Stage
Build Code
Unit Tests
Code Quality
Secrets Detection
SAST
Package Artifacts
SCA
SBOM
Test (Beta) Stage
Launch Environment
Database Deploy
Deploy Software
Integration Tests
Acceptance Tests
Test (Gamma) Stage
Launch Environment
Database Deploy
Deploy Software
Monitoring & Logging
Synthetic Tests
Performance Tests
Resilience Tests
DAST
Prod Stage
Manual Approval
Database Deploy
Progressive Deployment
Synthetic Tests
Legend
Required
Recommended

aws partnercast

AWS CloudFormation hooks

- Proactive validation
- Automatic enforcement
- Prebuilt hooks
- Build your own
- ”Always on”

Testing during infrastructure deployment

Shift left

Shift right

aws partnercast

AWS CFN-Guard – Policy as code

- Open source policy-as-code tool
- Write rules to validate compliance
- Validate AWS CloudFormation
- Any JSON or YAML doc configuration
- Terraform state files
- Kubernetes configurations

Testing IAC code locally with preventive tools

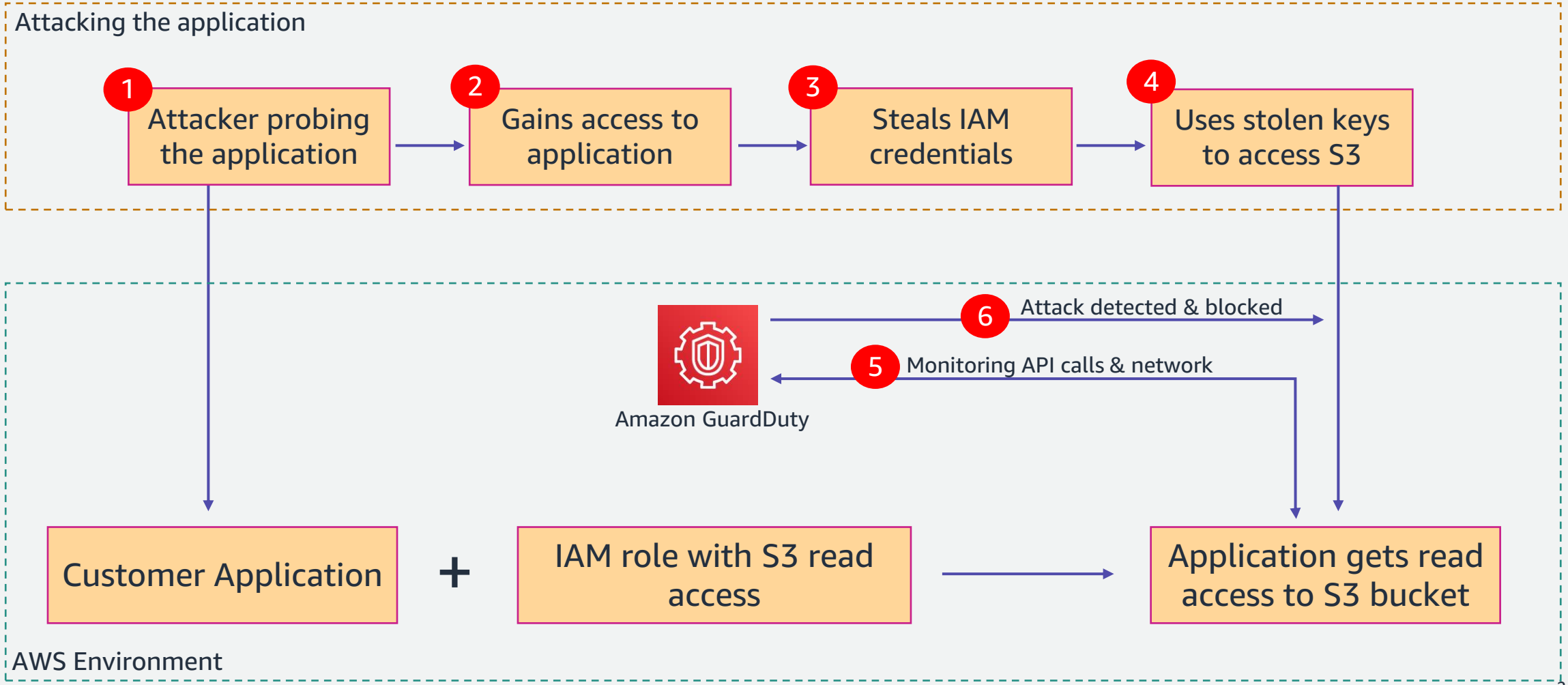
Shift left

Shift right

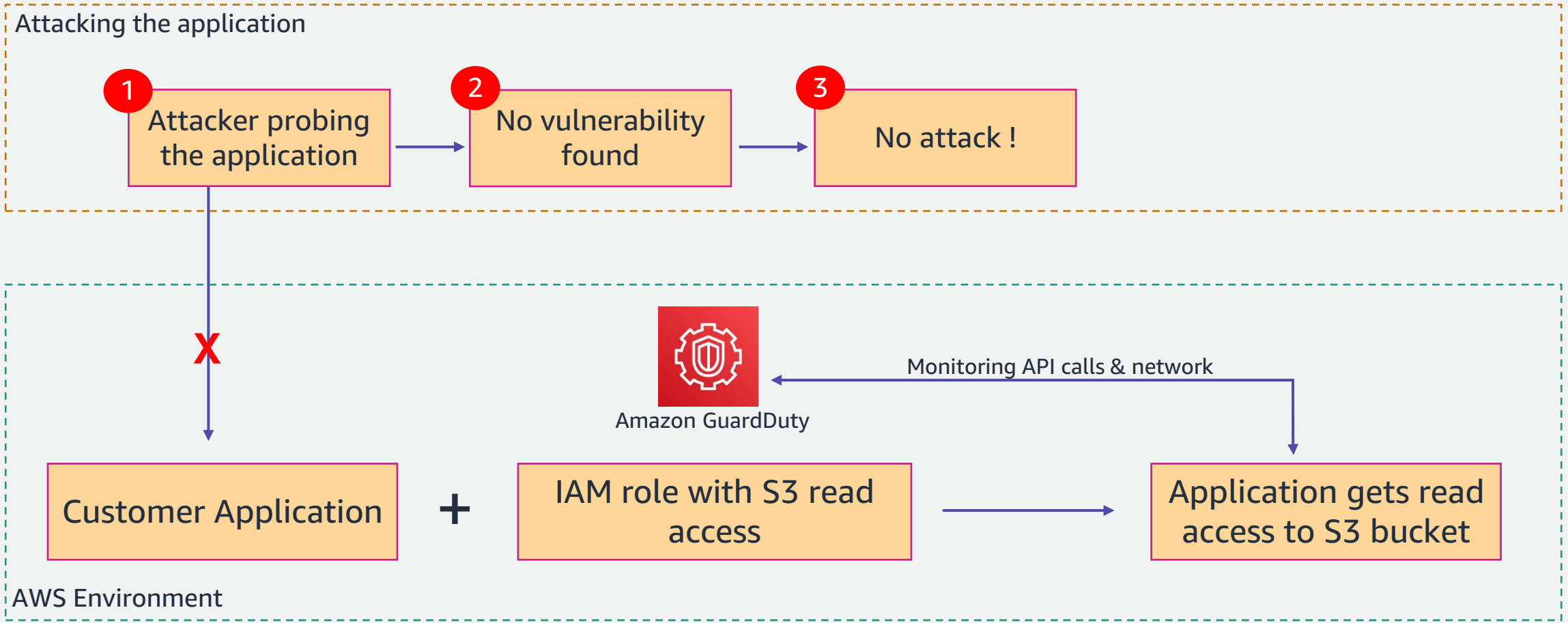
Demo

Stealing AWS access keys through misconfigured endpoints

Demo Scenario 1: Reactive Approach



Demo Scenario 2: Proactive Approach



aws partnercast

Jump to Demo

aws partnercast

Key Takeaways

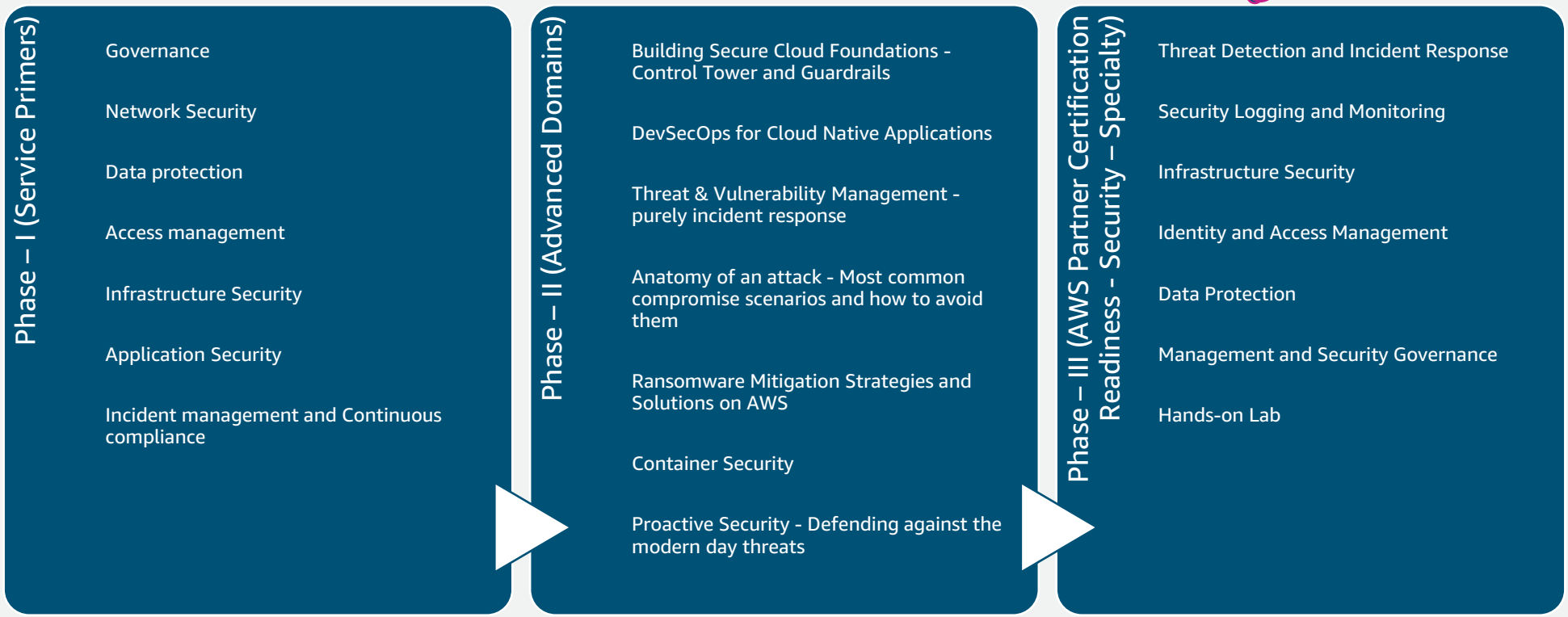
- Security is everyone’s job today, irrespective of the job role. It stands as the foundational and integral part of the digital age.
- Attackers have access to the same technology as we do – they can use AI/ML to launch more sophisticated and stronger attacks.
- Security is an integral part of Software Development & Deployment Lifecycle – We should aim to move from DevOps → DevSecOps.
- Reduce Mean Time to Identify and Mean Time to Recover by combining threat intel with IoCs, IoAs and existing security tooling.

aws partnercast

Call to Action

Register here!

Starts – Aug 2nd



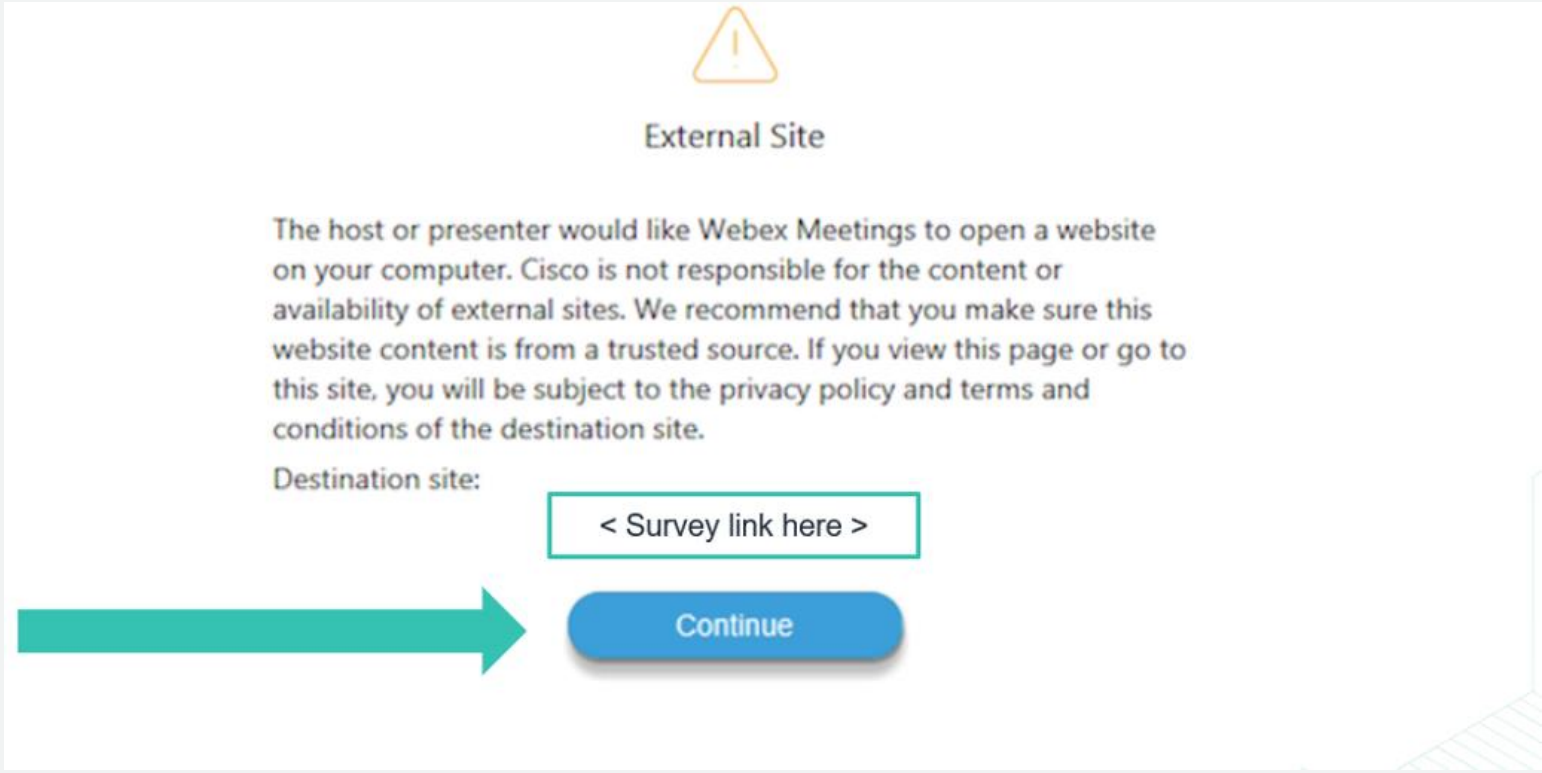
aws partnercast

Feedback

aws partnercast

Exit Survey

We appreciate your feedback! Please complete the survey at the end of this session. You will be automatically redirected via this screen:



aws partnercast

Shape the future of AWS Partner learning!

Scan this code to see how you can become an AWS Partner Training Feedback Contributor

aws partnercast

Thank you!

Please join us again for another PartnerCast session

https://aws.amazon.com/partners/training/partnercast/