PUBLIC SECTOR SUMMIT ONLINE

Using AWS security services to achieve advanced threat detection

Brad Dispensa
Principal Solutions Architect
Worldwide Public Sector
Amazon Web Services

aws PUBLIC SECTOR SUMMIT ONLINE

Agenda

- Threat detection service overview
- Attack patterns and mitigations
- Frameworks that can help you

Threat detection service overview

aws PUBLIC SECTOR SUMMIT ONLINE

AWS Foundational and Layered Security Services


AWS Organizations


AWS Security Hub

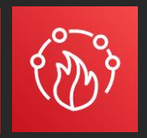

AWS Shield

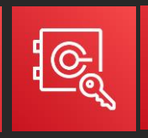

AWS Certificate Manager

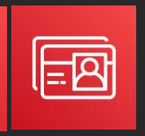

KMS

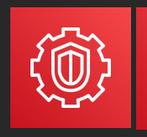

Amazon Cloud Directory

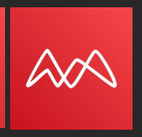

AWS WAF

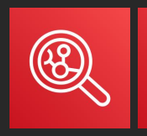

AWS Firewall Manager

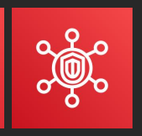

AWS CloudHSM


AWS Directory Service


Amazon GuardDuty

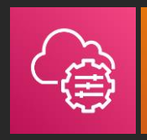

Amazon Macie

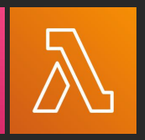

Amazon Inspector


AWS Security Hub


Amazon CloudWatch


AWS Step Functions


AWS Systems Manager


AWS Lambda


AWS OpsWorks


AWS CloudFormation

Identify → Protect → Detect → Respond → Recover

Automate

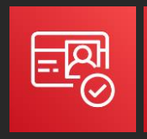
Investigate


AWS Config


AWS Trusted Advisor

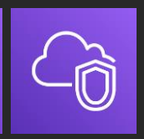

AWS Systems Manager

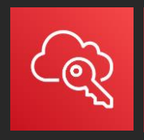

AWS Control Tower


Amazon Cognito

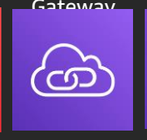

IAM


AWS Transit Gateway


Amazon VPC

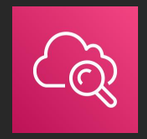

AWS Single Sign-On

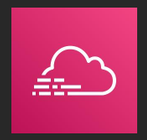

AWS Secrets Manager


Amazon VPC PrivateLink


AWS Direct Connect


Amazon Detective


Amazon CloudWatch


AWS CloudTrail


Amazon S3 Glacier


Snapshot


Archive

Threat detection: log data inputs

AWS CloudTrail

Track user activity and API usage

Flow logs

IP traffic to and from network interfaces in a VPC

Amazon CloudWatch

Monitor applications using log data; store and access log files

DNS logs

Log of DNS queries in a VPC when using the VPC DNS resolver

Threat detection: Machine learning

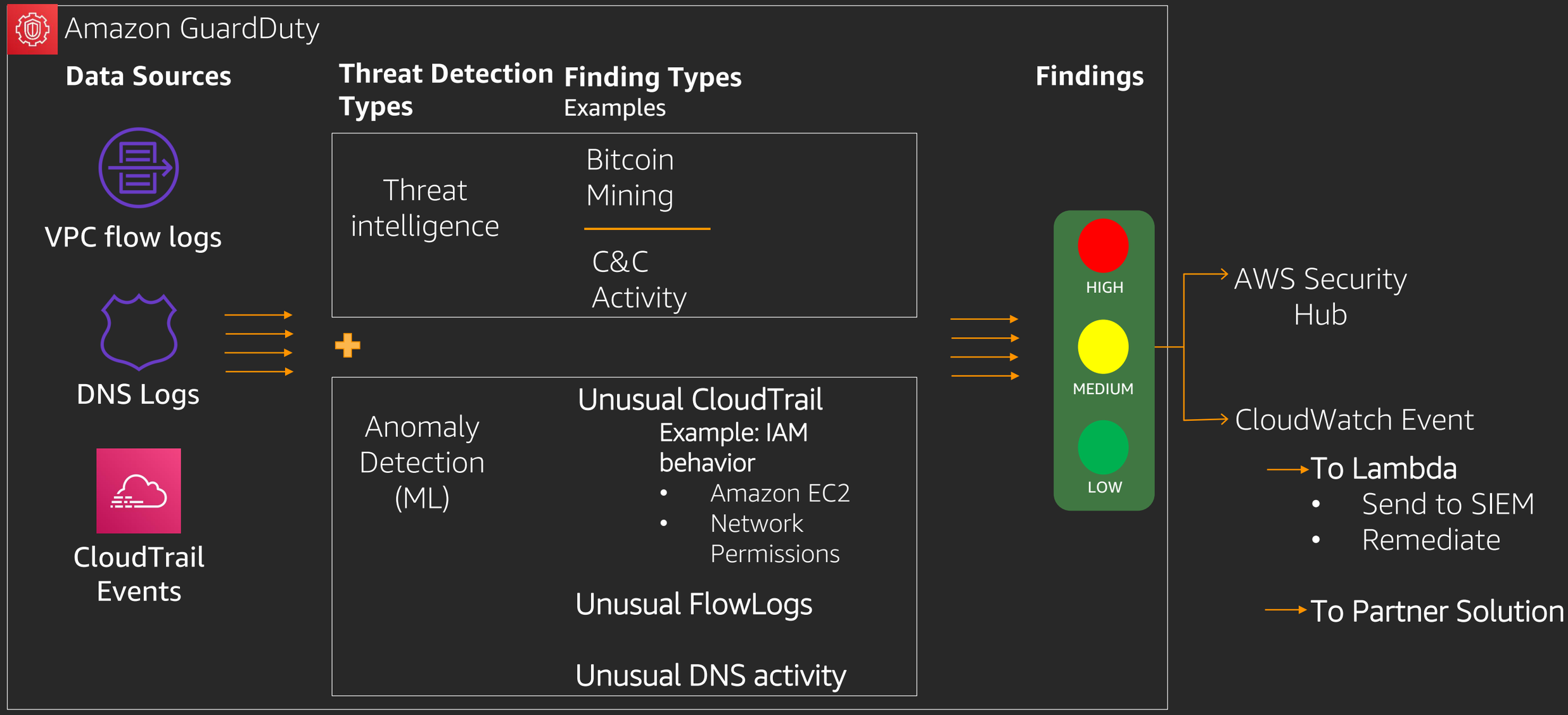
Amazon GuardDuty

Intelligent threat detection and continuous monitoring to protect your AWS accounts and workloads

Amazon Macie

Machine learning powered security service to discover, classify, and protect sensitive data

How Amazon GuardDuty works



Threat detection: AWS Security Hub

Insights and standards

- Comprehensive view of your security and compliance state within AWS
- Aggregates security findings generated by other AWS security services and partners
- Analyze security trends and identify the highest-priority security issues

AWS Security Hub

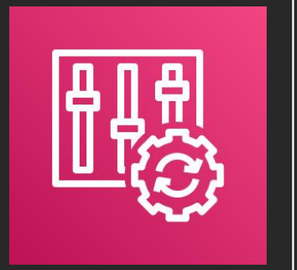
Findings

Security findings providers

Amazon Inspector

Amazon GuardDuty

Amazon Macie

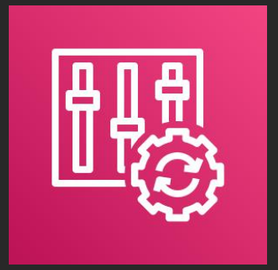


AWS Config

Partner solutions

Other

Threat detection: Evocations and triggers



AWS Config

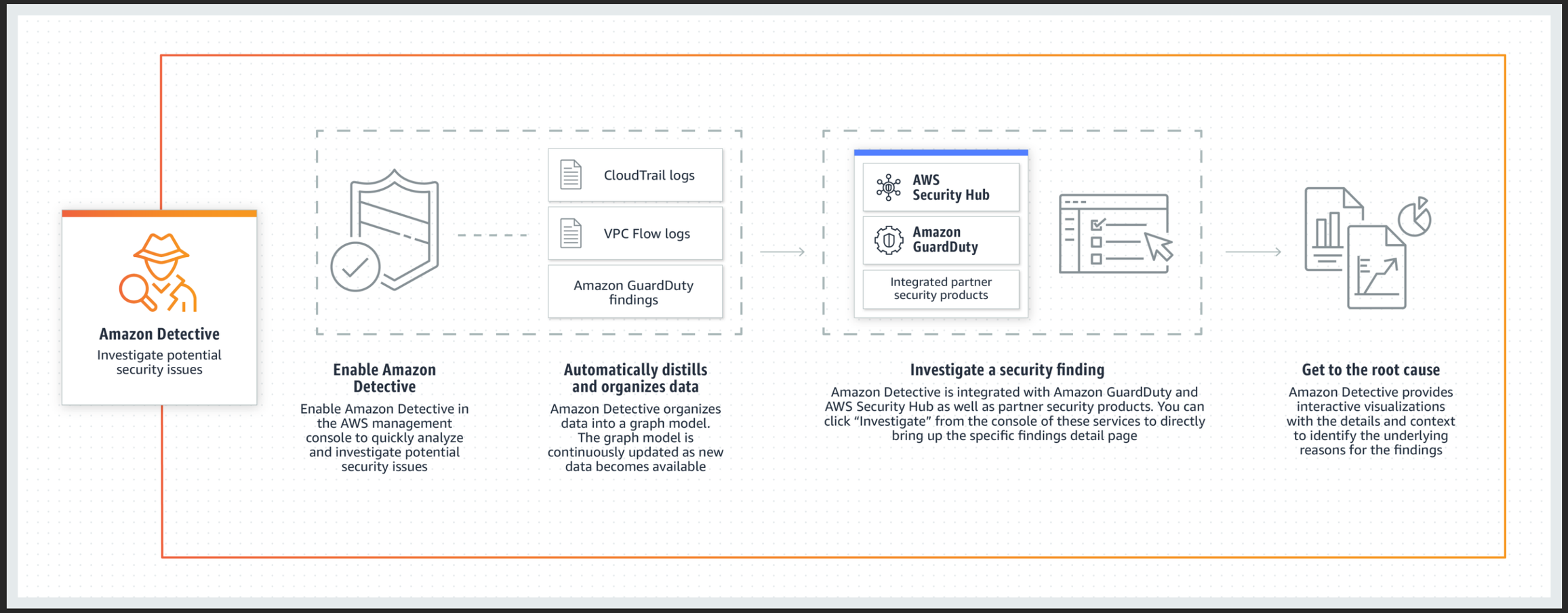
Continuously tracks your resource configuration changes and whether they violate any of the conditions in your rules

Amazon CloudWatch Events

Delivers a near real-time stream of system events that describe changes in AWS resources

What is Amazon Detective?

Protect your AWS accounts and workloads with intelligent threat detection and continuous monitoring



Investigations are resource intensive & time consuming

Collect and combine terabytes of log data

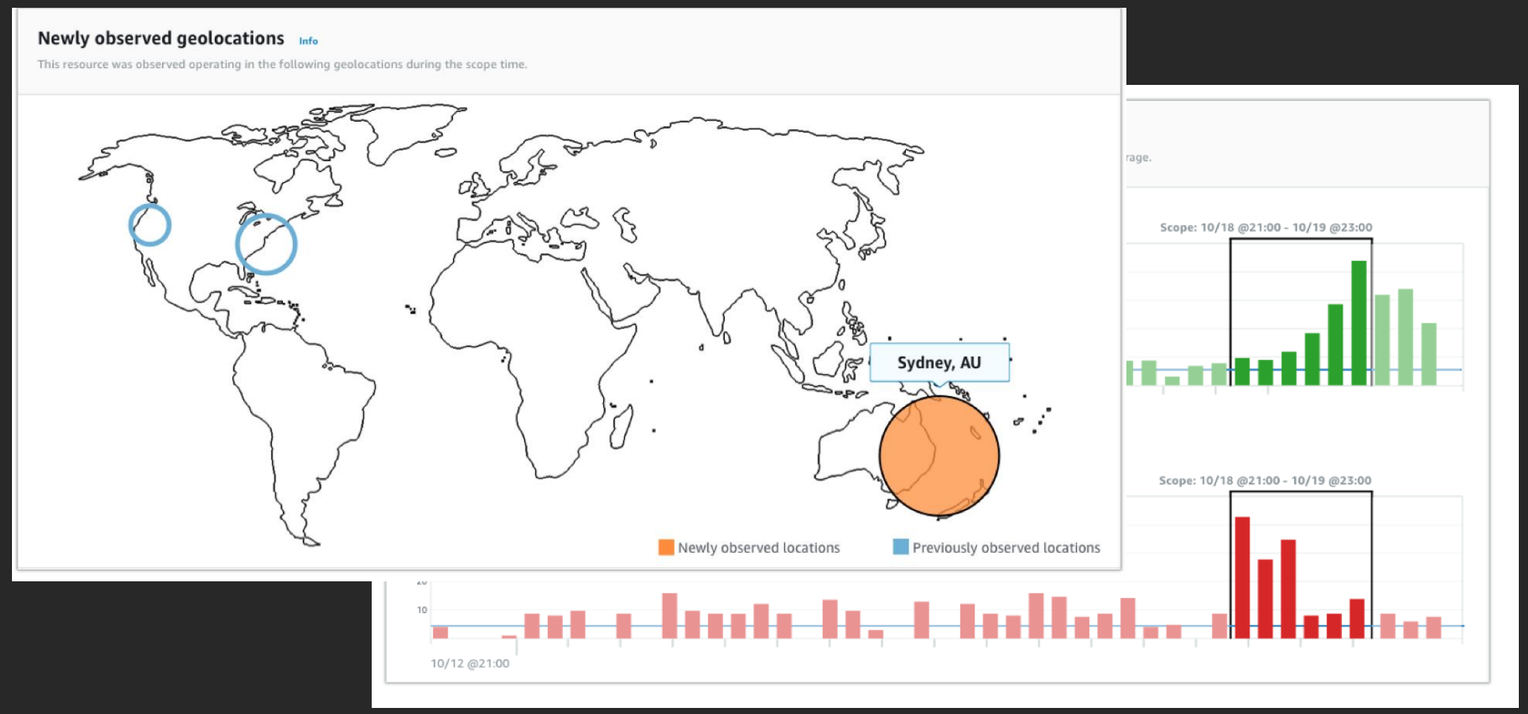
Transform the data using ETL tools, custom scripting

Finding right set of visualization tools to view the data

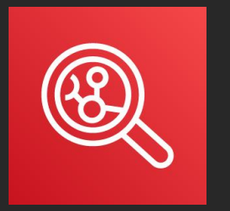
Translate investigation questions into queries to help answer questions

Amazon Detective

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



What is Amazon Inspector?



Automated security assessment service

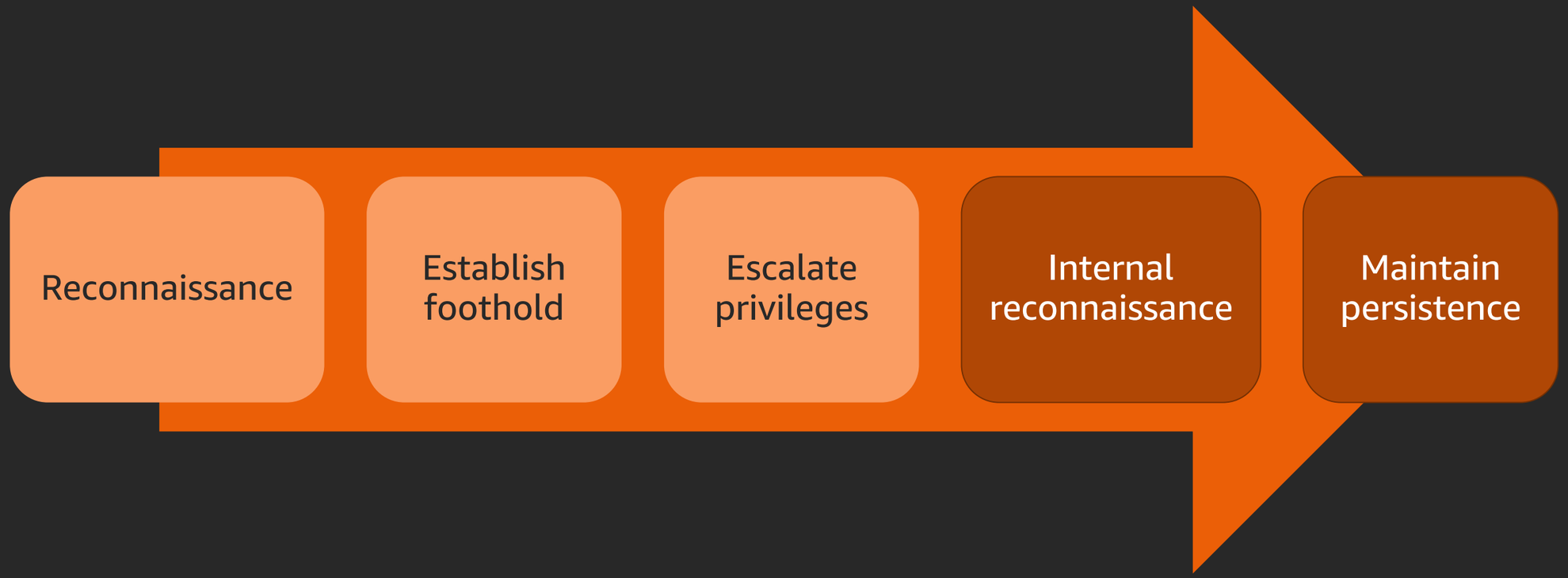
- Automatically assesses applications for vulnerabilities or deviations from best practices.
- Produces a detailed list of security findings prioritized by level of severity
- Agent-based, API-driven, and delivered as a service

Layer	Sample issues
Web Application	**SQL injection** **Cross-site scripting** **OS command injection** **Parameter manipulation**
OS/middleware	**OS/MW exploit** **Misconfiguration** **Weak passwords**
Network	**Port scans** **Unused listeners** **Exposed services**

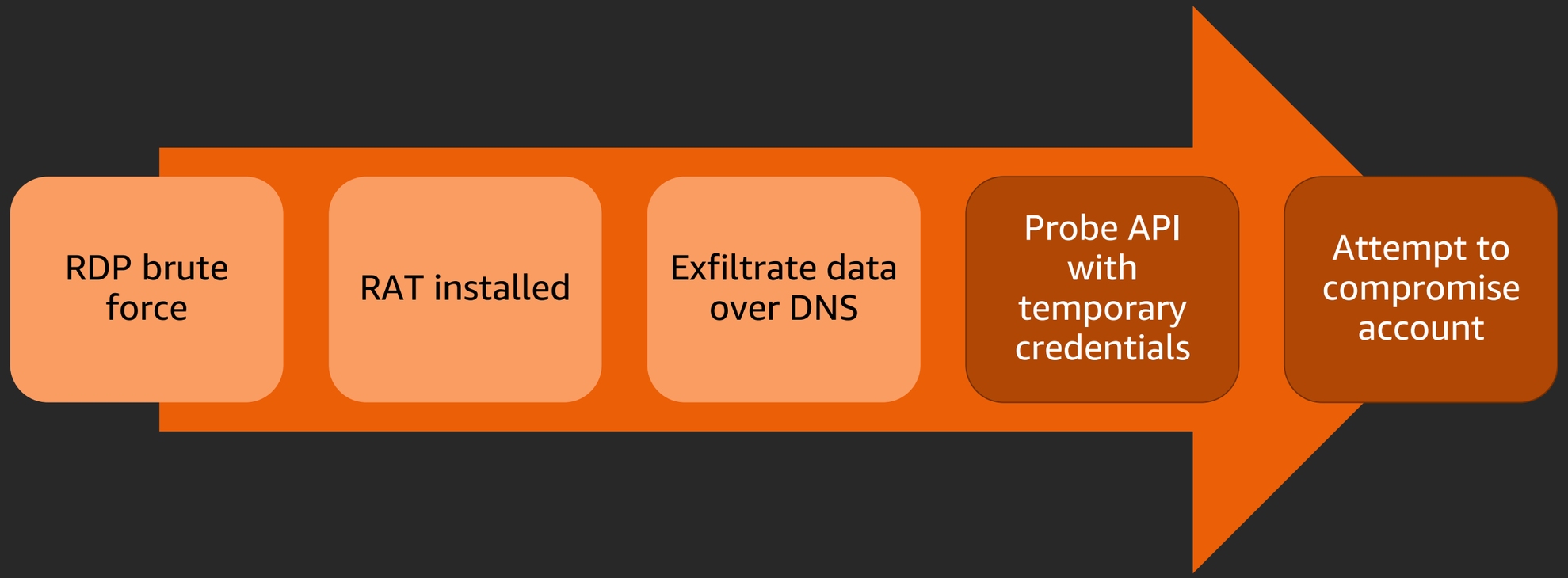
Attack patterns and mitigations

aws PUBLIC SECTOR SUMMIT ONLINE

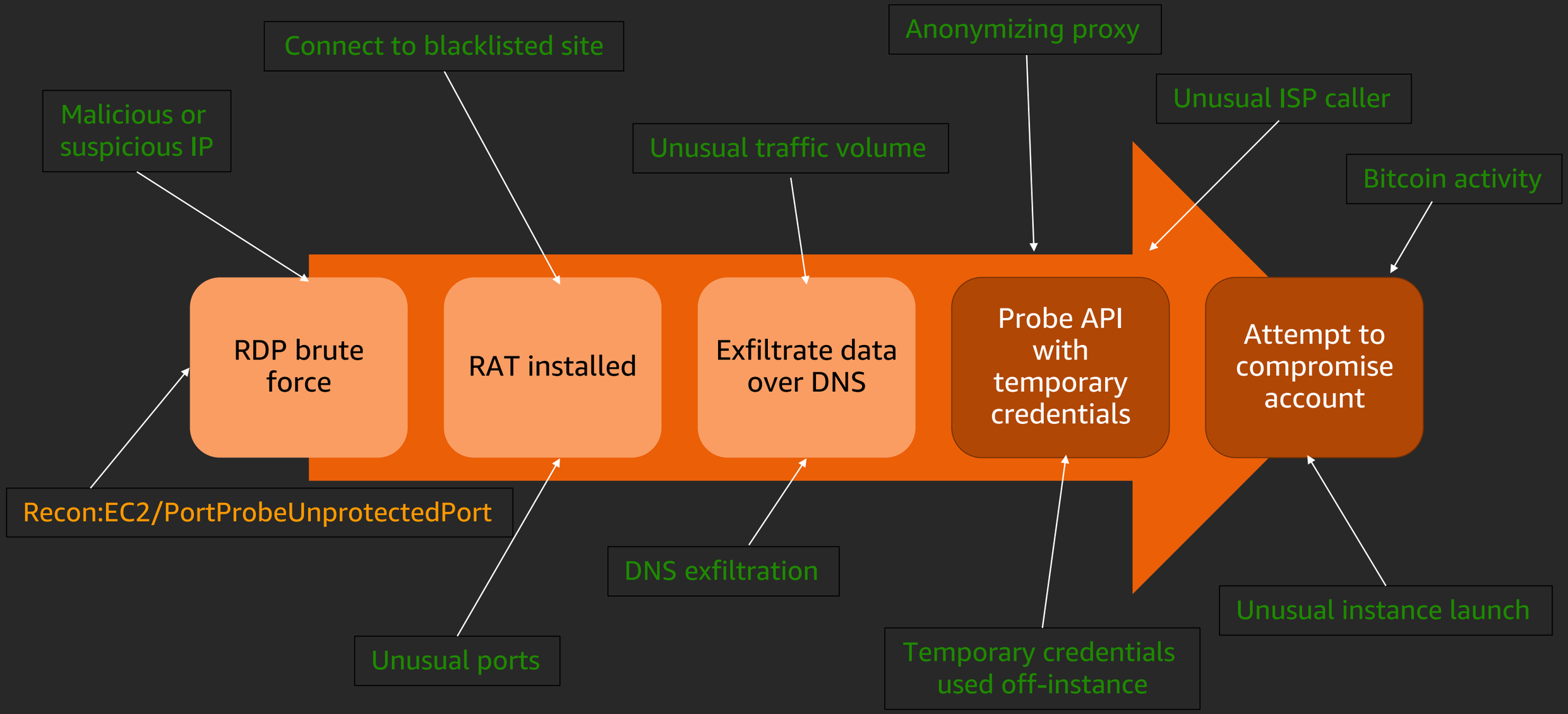
Attacker lifecycle: Stages



Attacker lifecycle: Attacker actions



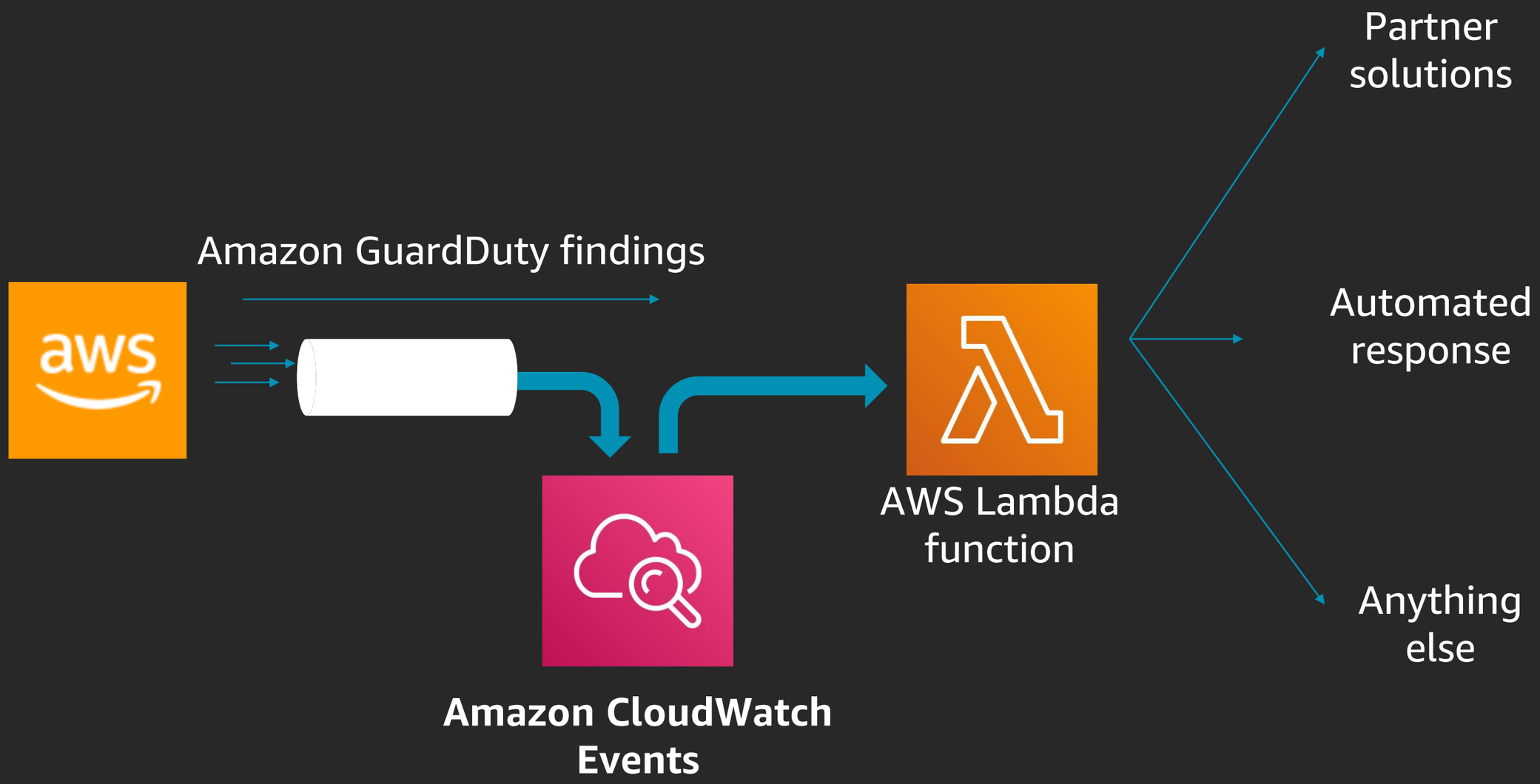
Attacker lifecycle: Amazon GuardDuty findings



Response

aws PUBLIC SECTOR SUMMIT ONLINE

Threat response: Amazon CloudWatch Events



Threat response: services

AWS Lambda

Run code for virtually any kind of application or backend service—zero administration

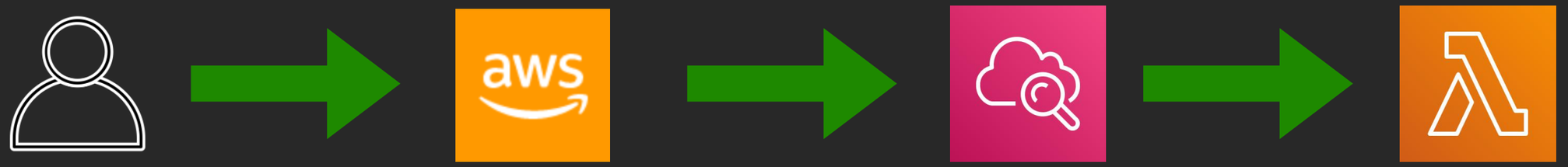
AWS Systems Manager

Gain operational insights and take action on AWS resources

Amazon Inspector

Automate security assessments of Amazon EC2 instances

Threat response: High-level playbook



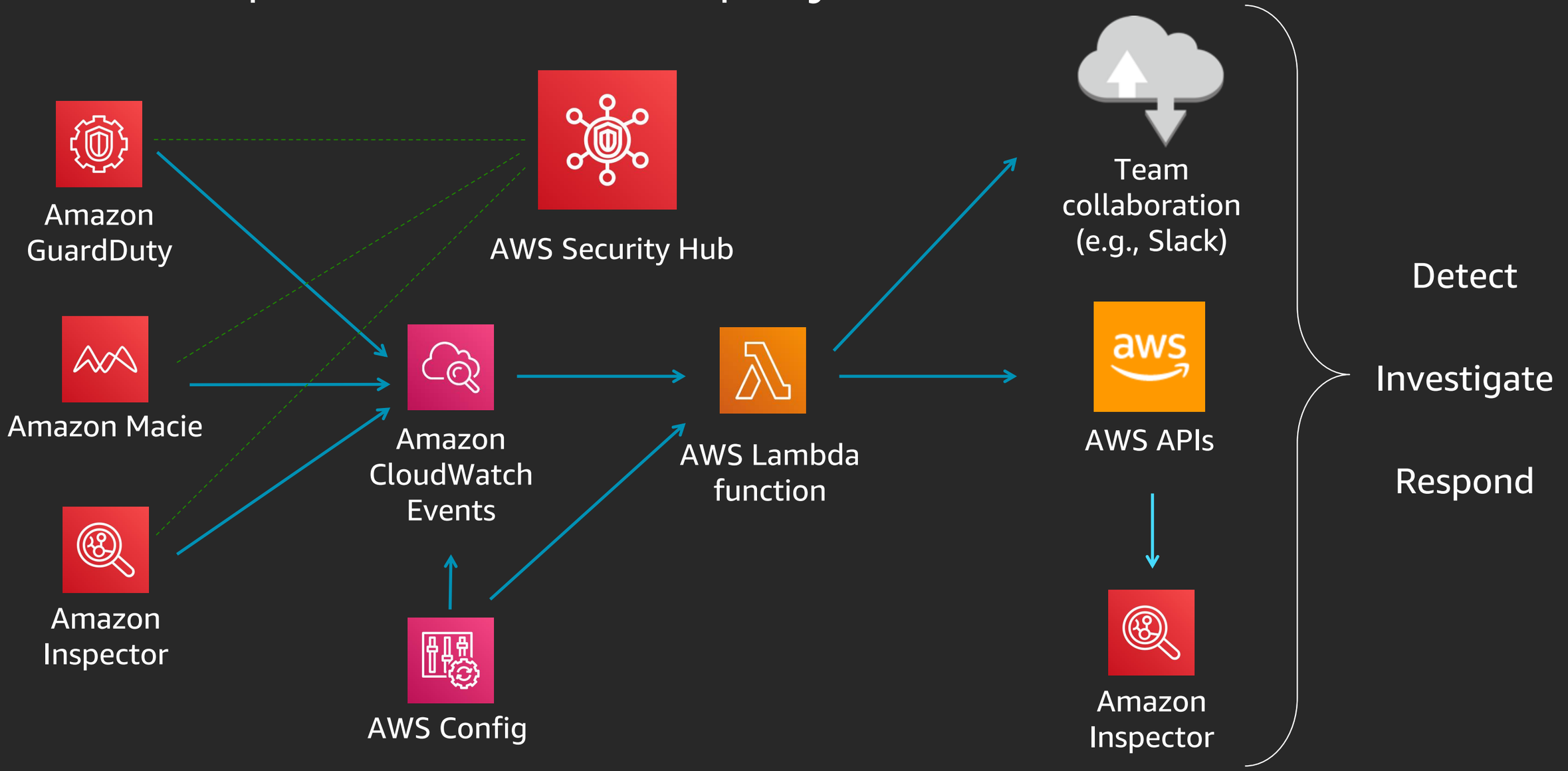
Adversary or intern

Your environment

Amazon CloudWatch Events

AWS Lambda function

Threat response: Detailed playbook



Frameworks that can help you

MITRE ATT&CK™

ATT&CK Matrix for Enterprise

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data Staged	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	CMSTP	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Information Repositories	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Local System	Data Encoding	Exfiltration Over Command and Control Channel	Endpoint Denial of Service
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Network Shared Drive	Data Obfuscation	Exfiltration Over Other Network Medium	Firmware Corruption

https://attack.mitre.org

LockheedMartin Kill Chain

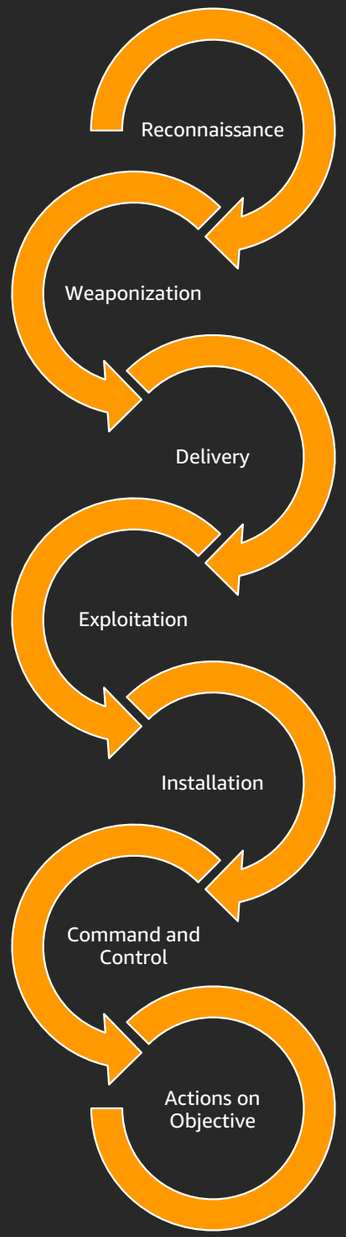


Table 1: Courses of Action Matrix

Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance	Web analytics	Firewall ACL				
Weaponization	NIDS	NIPS				
Delivery	Vigilant user	Proxy filter	In-line AV	Queuing		
Exploitation	HIDS	Patch	DEP			
Installation	HIDS	"chroot" jail	AV			
C2	NIDS	Firewall ACL	NIPS	Tarpit	DNS redirect	
Actions on Objectives	Audit log			Quality of Service	Honeypot	

https://lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf

Courses of action example: Exploitation

Detect

To discover or discern the existence, presence, or fact of an intrusion into information systems

Control Names	Descriptions
Amazon GuardDuty	Detects reconnaissance activity, such as unusual API activity, intra-VPC port scanning, unusual patterns of failed login requests, or unblocked port probing from a known bad IP
AWS WAF, WAF Managed Rules + Automation	Malicious sources scan and probe internet-facing web applications for vulnerabilities; they send a series of requests that generate HTTP 4xx error codes, and you can use this history to help identify and block malicious source IP addresses
Amazon VPC	Amazon VPC can help prevent attackers from scanning network resources during reconnaissance; Amazon VPC Black Hole Routes (as a whitelist or blacklist of network reachable assets before Security Groups or NACLs)
AWS Systems Manager State Manager, or third-party or OSS file integrity monitoring solutions on Amazon EC2	Automates the process of keeping your Amazon EC2 and hybrid infrastructure in a state that you define.
AWS Config	Assess, audit, and evaluate the configurations of your AWS resources
Third-party security tools for Containers	Implement advanced security protection and behavioral security solutions for containers
Third-party security tools for AWS Lambda functions	Implement advanced security protection and behavioral security solutions for Lambda functions
AWS Partner offerings – anti-malware protection	Detect and block malicious payloads
AWS Lambda Partners	Complement the security properties of Lambda functions
Container Partners – Security	Complement the security properties of containers solutions

Defined in 2006 version of JP 3-13, as documented in Mitre, "Characterizing Effects on the Cyber Adversary, A Vocabulary for Analysis and Assessment", https://www.mitre.org/sites/default/files/publications/characterizing-effects-cyber-adversary-13-4173.pdf

Courses of action example: Exploitation

Deny

To prevent the adversary from accessing and using critical information, systems, and services

Control Names	Descriptions
IAM Roles	Helps deny or contain the blast radius of attacks
Amazon S3 bucket policies, object policies	Control access to objects and prevent upload of that malicious object into the bucket
AWS Secrets Manager	Protect secrets needed to access your applications, services, and IT resources
Amazon EC2: Linux: SELinux - Mandatory Access Control	As non-overridable system policy mediating access to files, devices, sockets, other processes, and API calls
Amazon EC2: FreeBSD Trusted BSD – Mandatory Access Control	As non-overridable system policy mediating access to files, devices, sockets, other processes, and API calls
Amazon EC2: Linux, FreeBSD: Hardening and minimization	Disable/remove unused services and packages
Amazon EC2: Linux, Windows, FreeBSD: Address Space Layout Randomization (ASLR)	ASLR is a technology used to help prevent shellcode from being successful

Defined in 2006 version of JP 3-13, as documented in Mitre, "Characterizing Effects on the Cyber Adversary, A Vocabulary for Analysis and Assessment", https://www.mitre.org/sites/default/files/publications/characterizing-effects-cyber-adversary-13-4173.pdf

Courses of Action example: Exploitation

Disrupt

To break or interrupt the flow of information

Control Names	Descriptions
AWS WAF, WAF Managed Rules + Automation	Malicious sources scan and probe Internet-facing web applications for vulnerabilities; they send a series of requests that generate HTTP 4xx error codes, and you can use this history to help identify and block malicious source IP addresses
Amazon S3 bucket policies, object policies	Control access to objects and prevent upload of that malicious object into the bucket
AWS Secrets Manager	Protect secrets needed to access your applications, services, and IT resources
Amazon EC2: Linux: SELinux - Mandatory Access Control	As non-overridable system policy mediating access to files, devices, sockets, other processes, and API calls
Amazon EC2: FreeBSD Trusted BSD – Mandatory Access Control	As non-overridable system policy mediating accessto files, devices, sockets, other processes, and API calls
Amazon EC2: Linux, Windows, FreeBSD: Address Space Layout Randomization (ASLR)	ASLR is a technology used to help prevent shellcode from being successful

Defined in 2006 version of JP 3-13, as documented in Mitre, "Characterizing Effects on the Cyber Adversary, A Vocabulary for Analysis and Assessment", https://www.mitre.org/sites/default/files/publications/characterizing-effects-cyber-adversary-13-4173.pdf

Courses of action example: Exploitation

Degrade

To reduce the effectiveness or efficiency of adversary command and control (C2) or communications systems, and information collection efforts or means

Control Names	Descriptions
Amazon GuardDuty + AWS Lambda	Detects reconnaissance activities and modifies security configurations to degrade/block traffic associated with an attack
AWS WAF	Protects from common web exploits that could affect application availability, compromise security, or consume excessive resources
Load balancing	All entities providing the load-balanced service need to be compromised to guarantee a client interacting with a compromised instance
Immutable Infrastructure-short-lived environments	Rebuilt or refresh environments periodically to make it a harder task to make an attack payload persist

Deceive

To cause a person to believe what is not true; deception attempts to mislead adversaries by manipulating their perception of reality

Control Names	Descriptions
Honeypot and Honeynet Environments	Helps to deceive and contain the attack
Honeywords and Honeykeys	When an attacker attempts to use stolen false credentials, it helps detect, contain, and recover faster
AWS WAF + AWS Lambda	Trap endpoint to detect content scrapers and bad bots; when the endpoint is accessed a function add the source IP address to a block list

Defined in 2006 version of JP 3-13, as documented in Mitre, "Characterizing Effects on the Cyber Adversary, A Vocabulary for Analysis and Assessment", https://www.mitre.org/sites/default/files/publications/characterizing-effects-cyber-adversary-13-4173.pdf

Courses of Action example: exploitation

Contain

The action of keeping something harmful under control or within limits

Control Names	Descriptions
IAM Roles	Helps deny or contain the blast radius of attacks
AWS Organizations + Service Control Policies (SCPs) + AWS accounts	Implement strong least-privilege and need-to-know security principles for both users and services across a multi-account structure. Control administrators privileges in child accounts
Amazon EC2: Linux: SELinux - Mandatory Access Control	As non-overridable system policy mediating access to files, devices, sockets, other processes, and API calls
Amazon EC2: FreeBSD Trusted BSD – Mandatory Access Control	As non-overridable system policy mediating access to files, devices, sockets, other processes, and API calls
Amazon EC2: Linux, FreeBSD: Hardening and minimization	Disable/remove unused services and packages
Amazon EC2: Linux: Role based Access Control (RBAC) and Discretionary Access Control (DAC)	Implement least-privilege account profiles

Defined in 2006 version of JP 3-13, as documented in Mitre, "Characterizing Effects on the Cyber Adversary, A Vocabulary for Analysis and Assessment", https://www.mitre.org/sites/default/files/publications/characterizing-effects-cyber-adversary-13-4173.pdf

Courses of Action example: exploitation

Respond

Capabilities that help to react quickly to an adversary's or others' IO attack or intrusion

Control Names	Descriptions
Amazon GuardDuty Partners	Complement GuardDuty
Third-party security tools for Containers	Implement advanced security protection and behavioral security solutions for containers
Third-party security tools for AWS Lambda functions	Implement advanced security protection and behavioral security solutions for Lambda functions
AWS Partner offerings: behavioral monitoring/ response tools and services	Provides insights into the threats in your environment
AWS Managed Services	AWS Managed Services monitors the overall health of your infrastructure resources, and handles the daily activities of investigating and resolving alarms or incidents

Defined in 2006 version of JP 3-13, as documented in Mitre, "Characterizing Effects on the Cyber Adversary, A Vocabulary for Analysis and Assessment", https://www.mitre.org/sites/default/files/publications/characterizing-effects-cyber-adversary-13-4173.pdf

Courses of Action example: exploitation

Restore

To bring information and information systems back to their original state

Control Names	Descriptions
Autoscaling	Adjusts capacity to maintain steady, predictable performance
AWS Systems Manager state manager	Helps you define and maintain consistent OS configurations
AWS Partner offerings: File integrity monitoring	Help maintain the integrity of the operating system and application files
AWS CloudFormation + Service Catalog	Provision your infrastructure in an automated and secure manner; this file serves as the single source of truth for your cloud environment
Immutable infrastructure – short-lived environments	Rebuilt or refresh environments periodically to make it a harder task to make an attack payload persist

Defined in 2006 version of JP 3-13, as documented in Mitre, "Characterizing Effects on the Cyber Adversary, A Vocabulary for Analysis and Assessment", https://www.mitre.org/sites/default/files/publications/characterizing-effects-cyber-adversary-13-4173.pdf

What is the NIST Cybersecurity Framework?

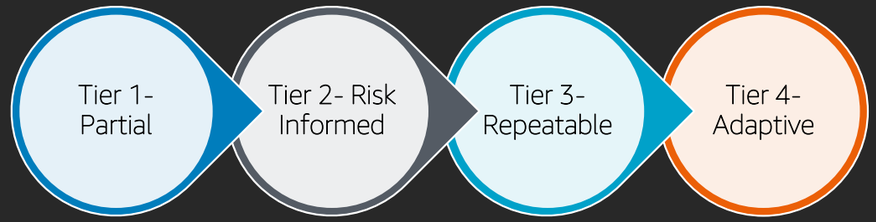
The CSF offers a simple-yet-effective risk-based, outcome-focused framework consisting of three elements – core, tiers, and profiles

Core

- The core represents a set of cybersecurity practices, outcomes, and technical, operational, and managerial security controls (referred to as informative references) that support the five risk management functions

Tiers

- Tiers characterize an organization's aptitude for managing cybersecurity risk



Profiles

- Profiles are intended to convey the organization's "as is" and "desired" risk posture

Current

Target

These three elements enable organizations to prioritize and address cybersecurity risks consistent with their business and mission needs

Aligning to the NIST CSF in the AWS Cloud

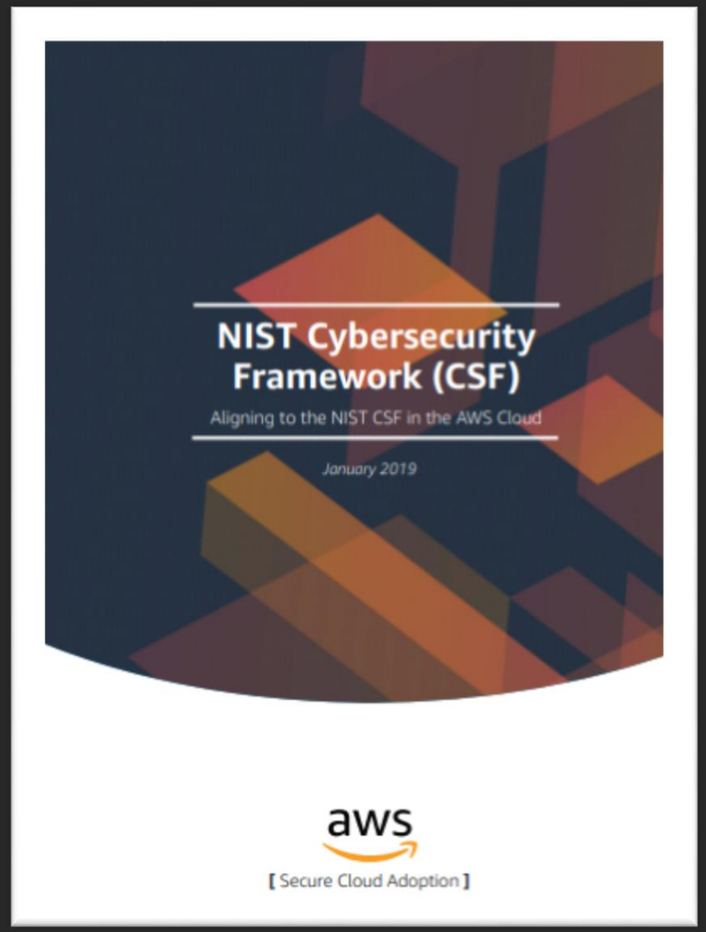
Two objectives with the whitepaper:

Security *of* the cloud

- Third-party attestation that AWS infrastructure and services conform to NIST CSF risk-management practices based on FedRAMP and ISO 27001 accreditations

Security *in* the cloud

- Detailed mapping of AWS services and resources (beyond FedRAMP and ISO 27001)
- Customer responsibilities
- AWS responsibilities



https://d1.awsstatic.com/whitepapers/compliance/NIST_Cybersecurity_Framework_CSF.pdf

https://aws.amazon.com/architecture/well-architected/

The Framework

Framework

This whitepaper introduces you to the AWS Well-Architected Framework, covering key concepts, design principles for architecting in the cloud, and the five pillars. The appendix includes the current questions for reviewing a workload using the Framework.

Framework whitepaper **PDF** | Kindle

Operational Excellence

The operational excellence pillar focuses on running and monitoring systems to deliver business value, and continually improving processes and procedures. Key topics include managing and automating changes, responding to events, and defining standards to successfully manage daily operations.

Operational Excellence whitepaper **PDF** | Kindle

Security

The security pillar focuses on protecting information & systems. Key topics include confidentiality and integrity of data, identifying and managing who can do what with privilege management, protecting systems, and establishing controls to detect security events.

Download the Security Pillar whitepaper **PDF** | Kindle

Reliability

The reliability pillar focuses on the ability to prevent, and quickly recover from failures to meet business and customer demand. Key topics include foundational elements around setup, cross project requirements, recovery planning, and how we handle change.

Download the Reliability Pillar whitepaper **PDF** | Kindle

Performance Efficiency

The performance efficiency pillar focuses on using IT and computing resources efficiently. Key topics include selecting the right resource types and sizes based on workload requirements, monitoring performance, and making informed decisions to maintain efficiency as business needs evolve.

Download the Performance Efficiency whitepaper **PDF** | Kindle

Thank you!

Brad Dispensa

aws PUBLIC SECTOR SUMMIT ONLINE