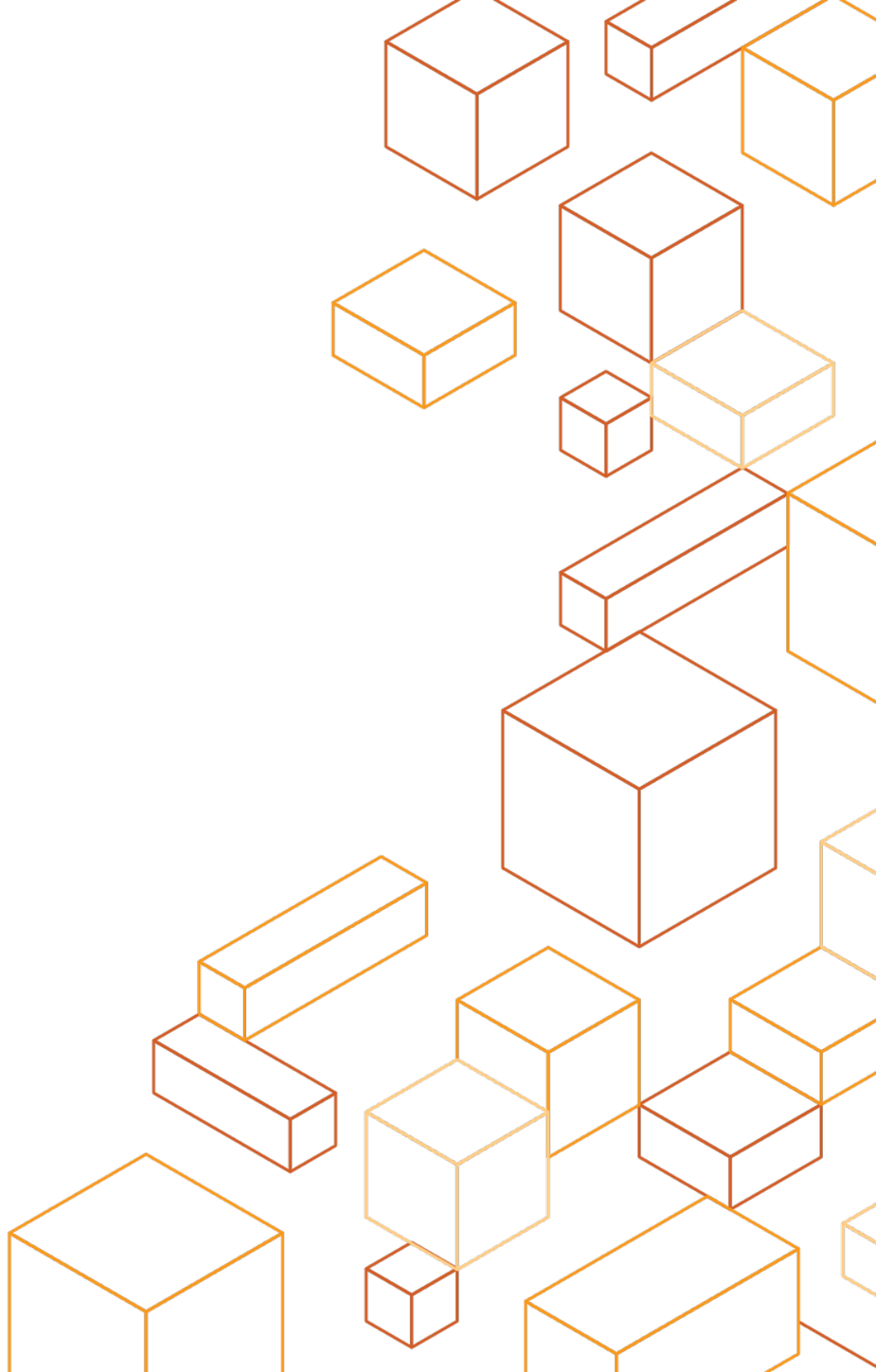
aws professional services

Incident Response



Agenda

- **Foundations** of Incident Response
- **Educating** security operations and incident response staff
- **Preparing** your incident response team
- **Simulating** security events
- **Iterating** on simulation outcome

Goals

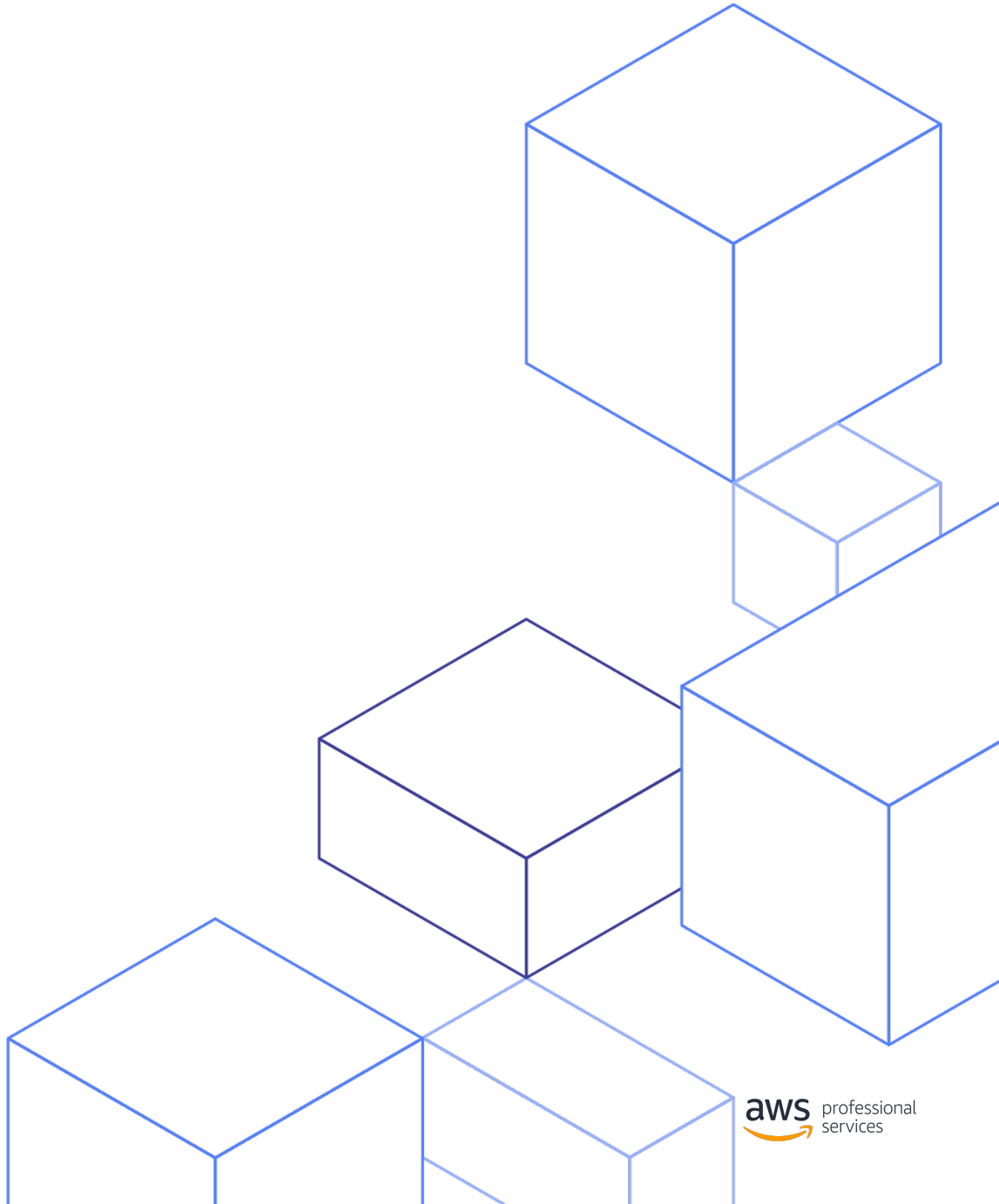
- Understand principles of incident response in the cloud
- How to prepare for incident response – people and technology
- Become aware of indicators of security incidents
- Classify incident types
- How to simulate and prepare for security incidents
- Automation of incident response

Outcomes

- Decision on who will be responsible for Incident Response on AWS
- Decision what (3rd party) tools will be used and/or developed to perform incident response in a cloud native way
- Decision on whether to schedule (regular) incident response simulations

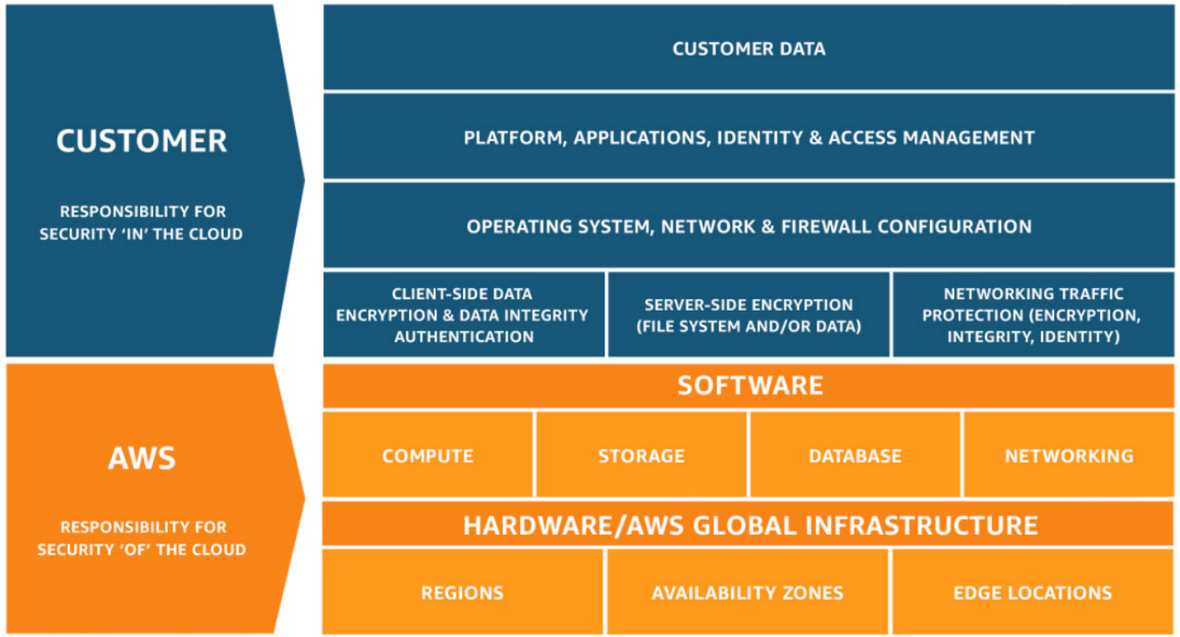
Educate

Incident Response

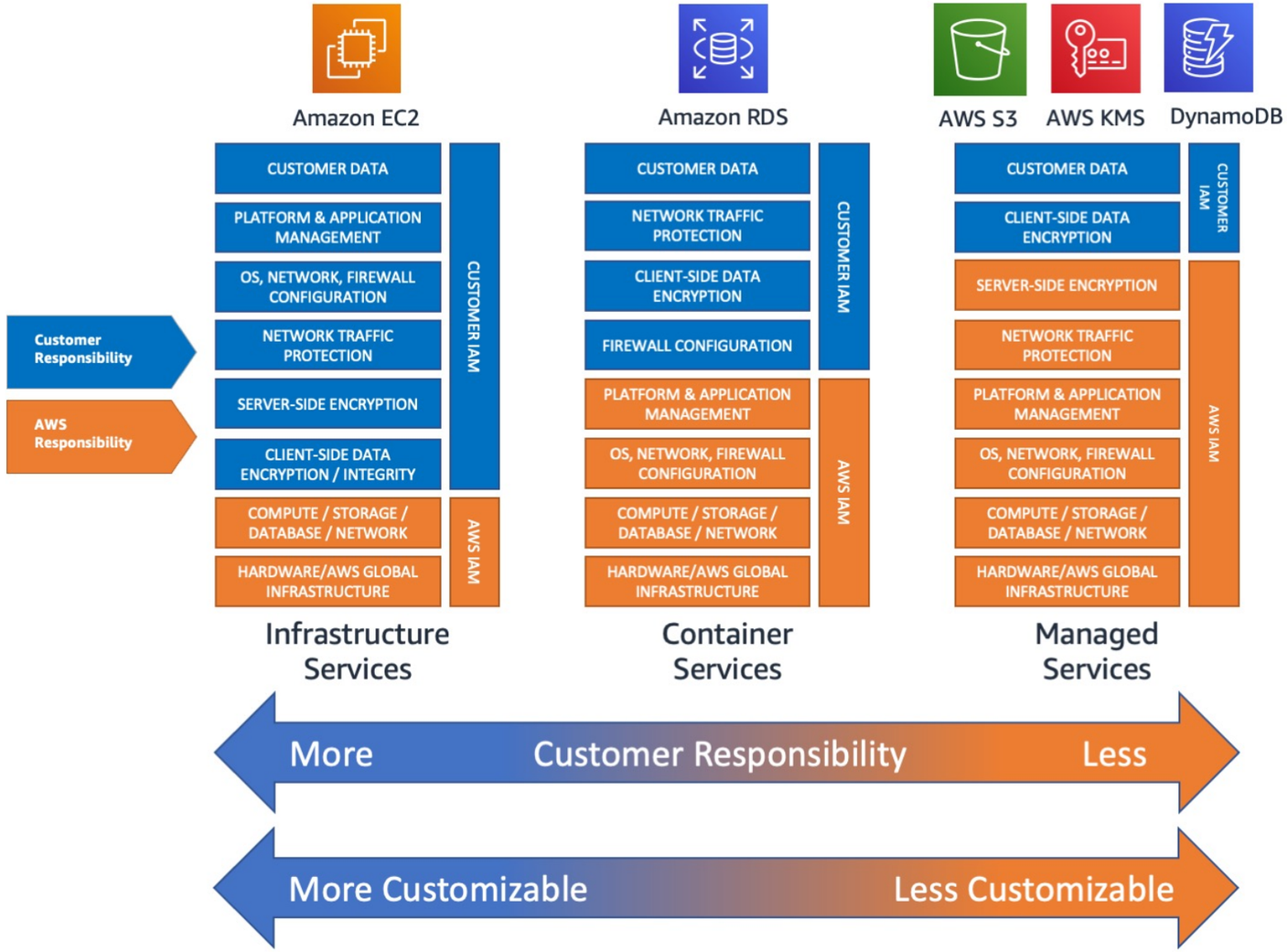


Incident Response - Shared Responsibility

- General shared responsibility model still applies
- Model varies depending on actual services used
- Incident response model needs to reflect actual operating model based on services used and internal organization (see next slide)



Incident Response - Shared Responsibility by service type

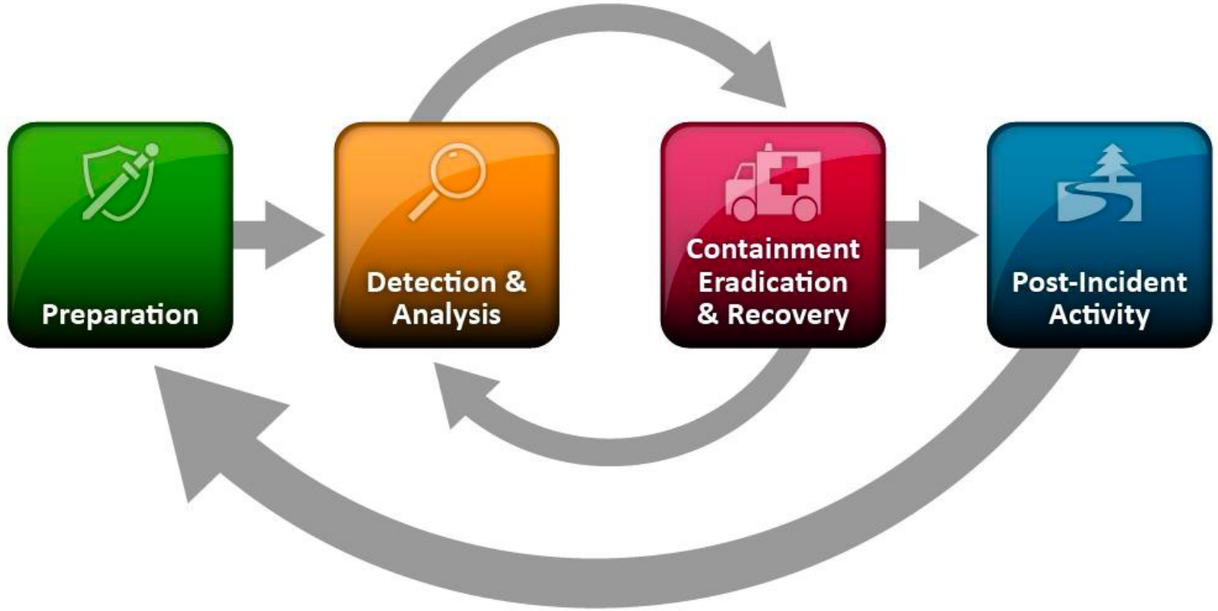


aws professional services

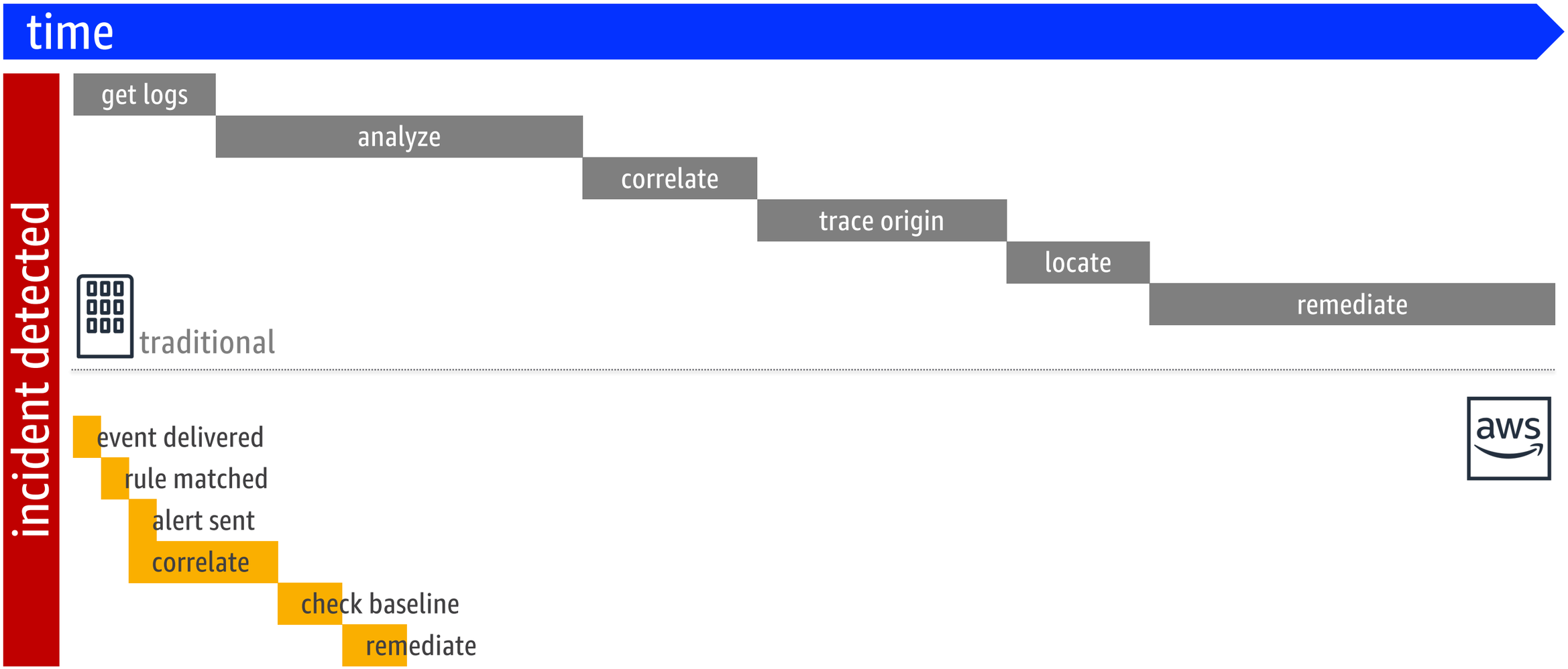
Incident Response – Design Goals of Cloud Response

General processes of IR remain true (see NIST SP 800-61), but some cloud specific points apply

- Establish response objectives
- Respond using the cloud
- Know what you have and what you need
- Use redeployment mechanisms
- Automate where possible
- Choose scalable solutions
- Learn and improve processes

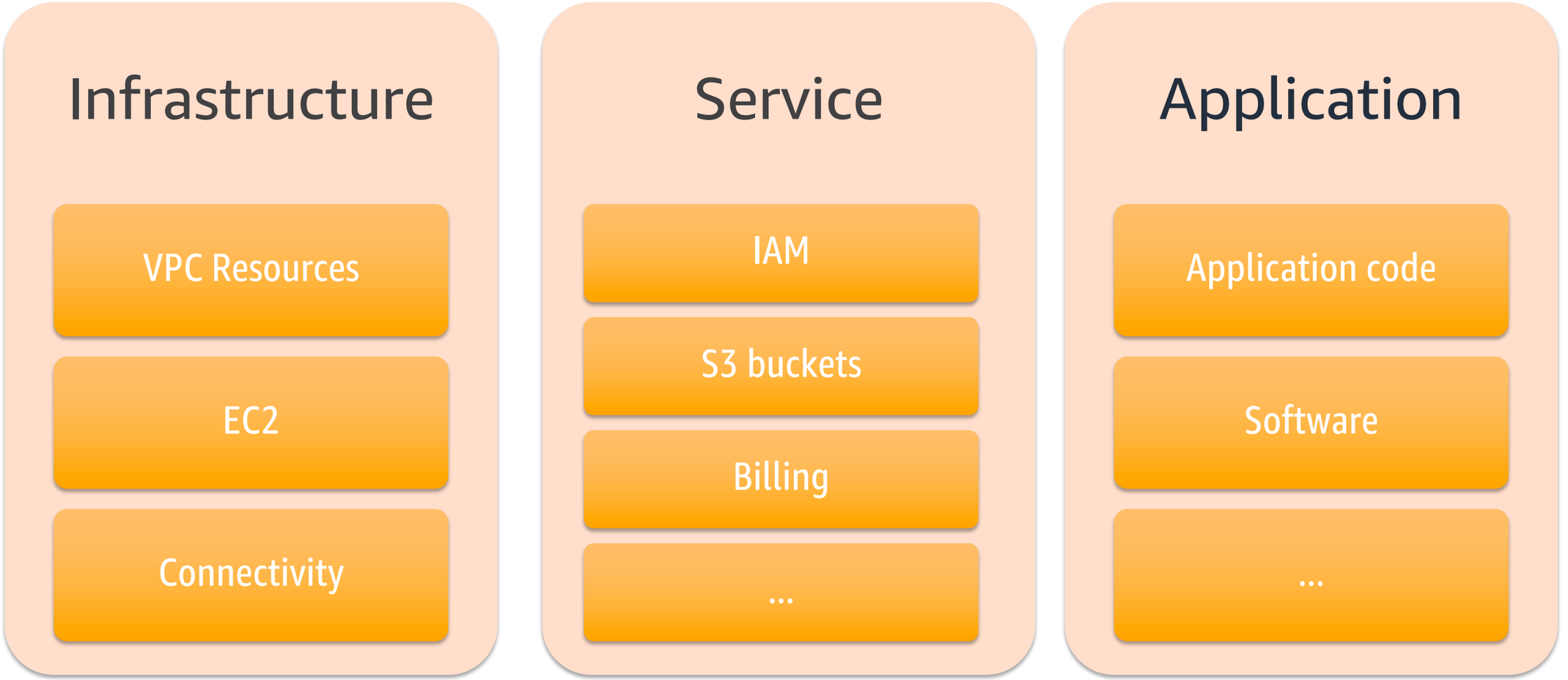


Incident Response – Time Comparison (example)



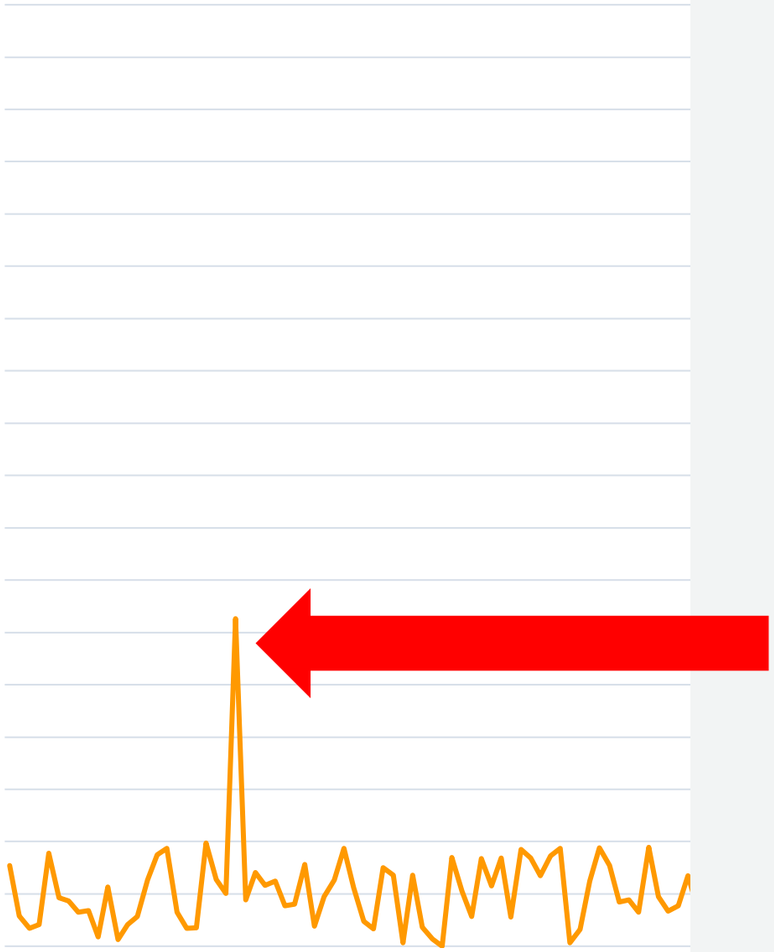
aws professional services

Incident Response - Incident Domains



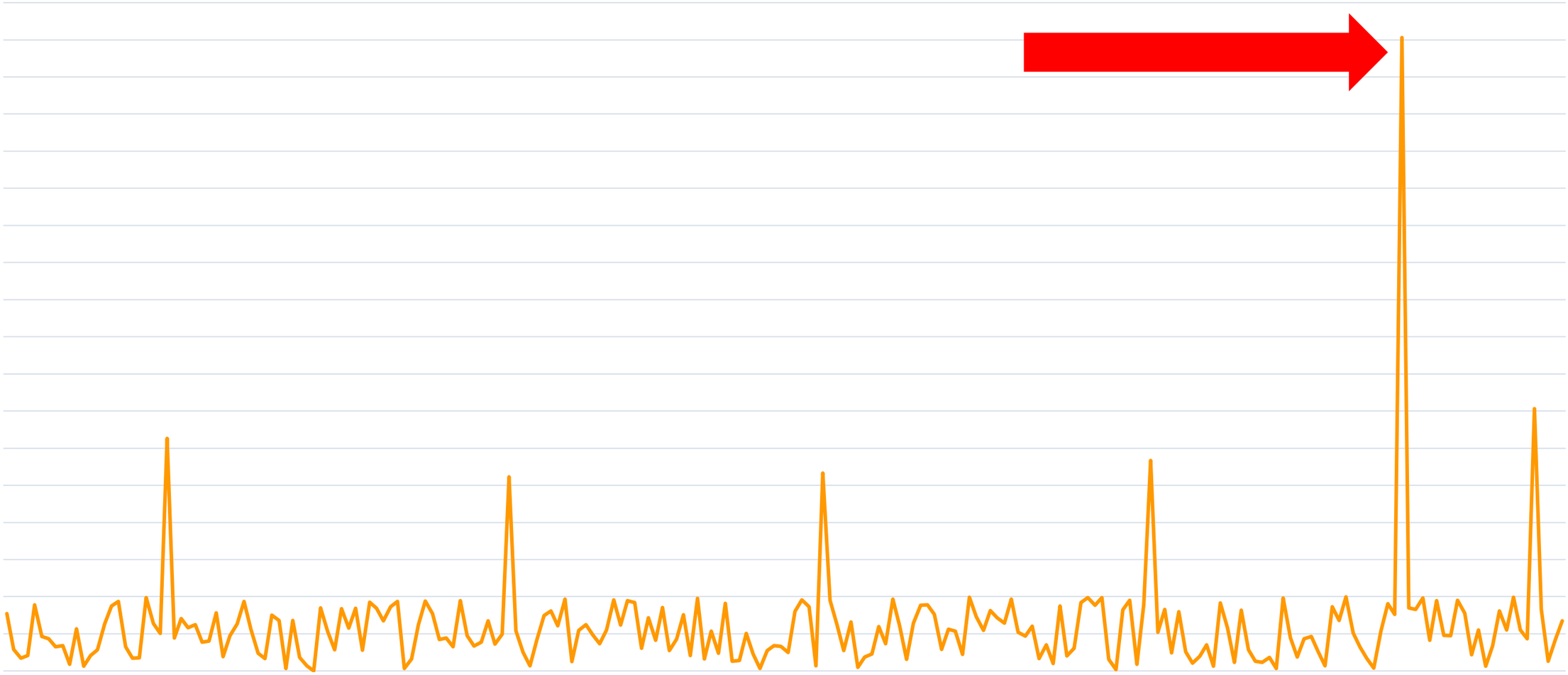
aws professional services

Incident Response – Understanding Normal



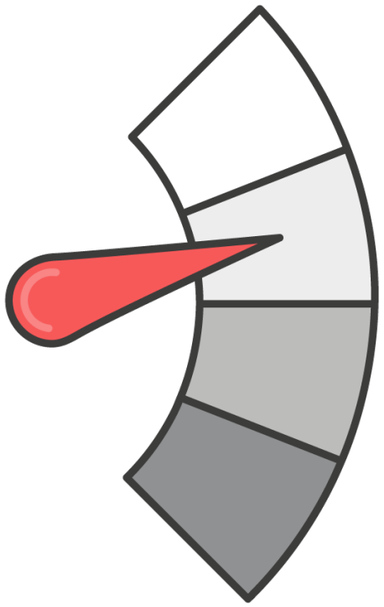
Incident: deviation from your [security] baseline

Incident Response – Understanding Normal



aws professional services

Incident Response – Indicators

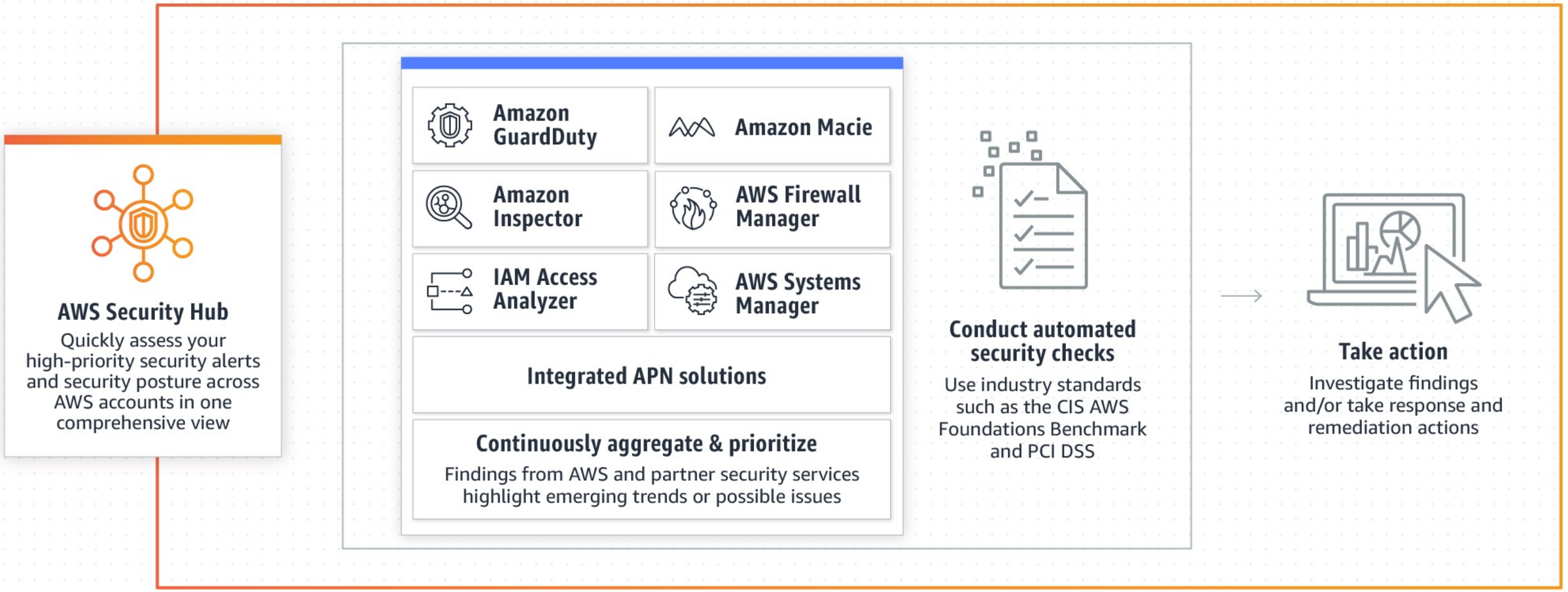


- Logs and Monitors
- Billing Activity
- Threat Intelligence
- AWS Outreach
- Ad Hoc Contact

Incident Response – Security Hub

AWS Security Hub is a cloud security posture management service that performs security best practice checks, aggregates alerts, and enables automated remediation.

Incident Response – Security Hub

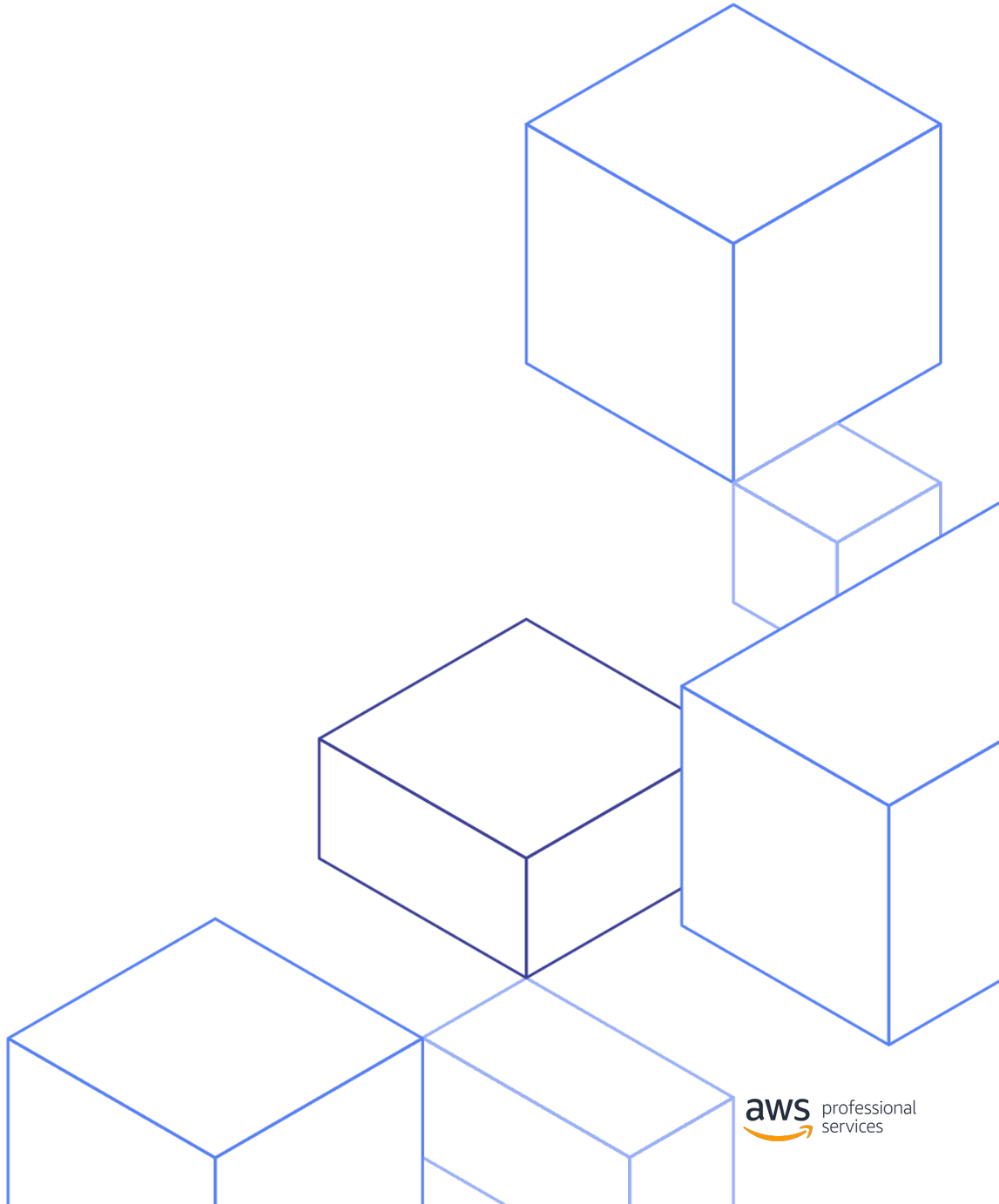


Incident Response – Cloud Capabilities

- Data Privacy
    - Limitations of AWS access to customer content
- Abuse and Compromise
    - Abuse activities include malicious, offensive, or illegal behaviours
    - Compromised resources, unintentional and secondary abuse, false complaints
- Contact
    - Root email and secondary email addresses
        - Distribution lists

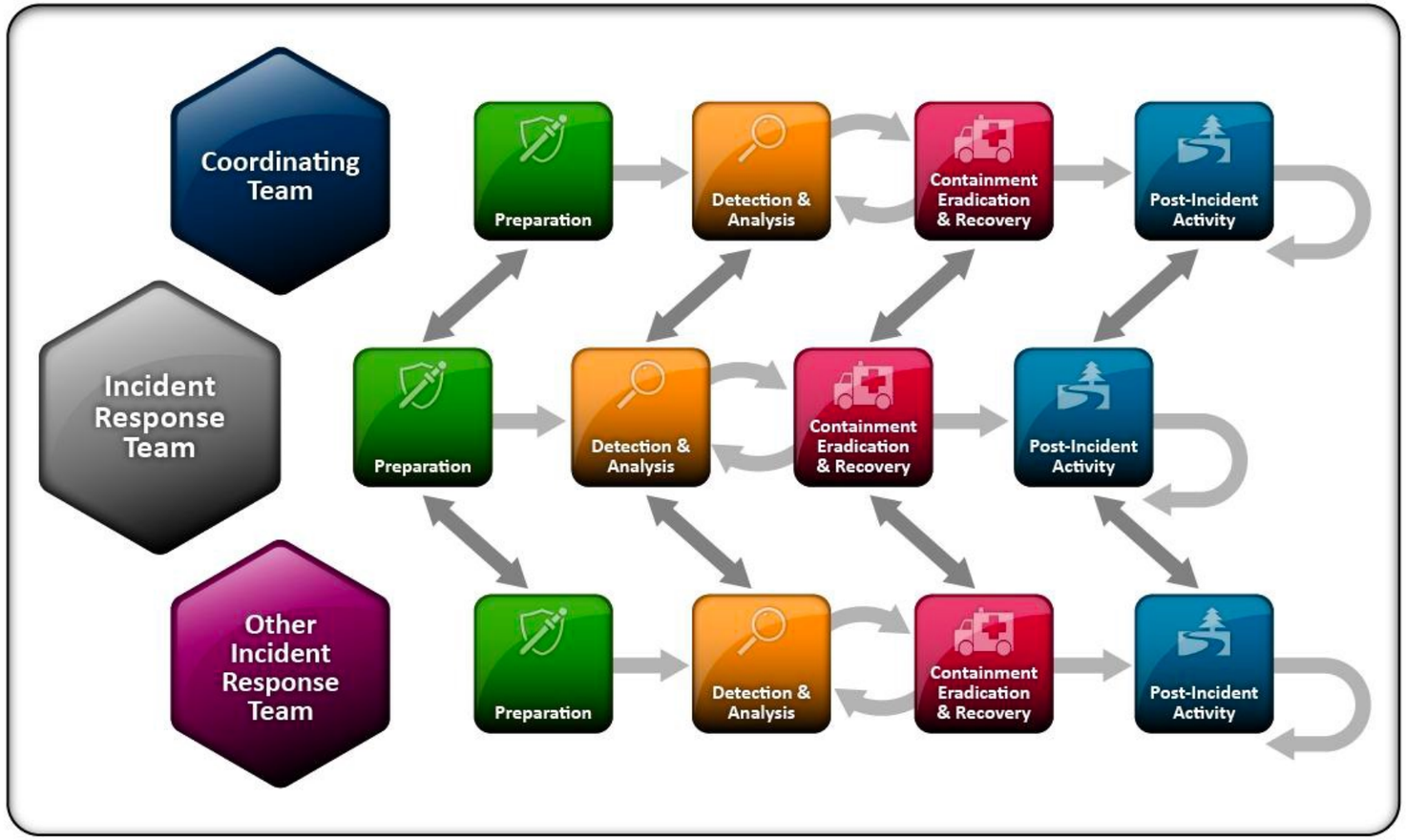
Prepare - People

Incident Response



Incident Response – Roles and Responsibilities

- Develop organization wide RACI model
- Use automation for repetitive tasks
- Develop strong relationships and practice between application owners and IT team
- Don’t forget third parties and trusted partners



Incident Response – Typical Third Parties

Incident Response - Training

Cloud services

- Ensure familiarity with cloud platform
- Use runbooks and tabletop exercises

Online security workshops

- AWS or third party providers

AWS training and certification

- Digital and classroom training, APN partners, certifications

Incident Response - Response mechanisms and Culture

Governance, risk, and compliance (GRC) model

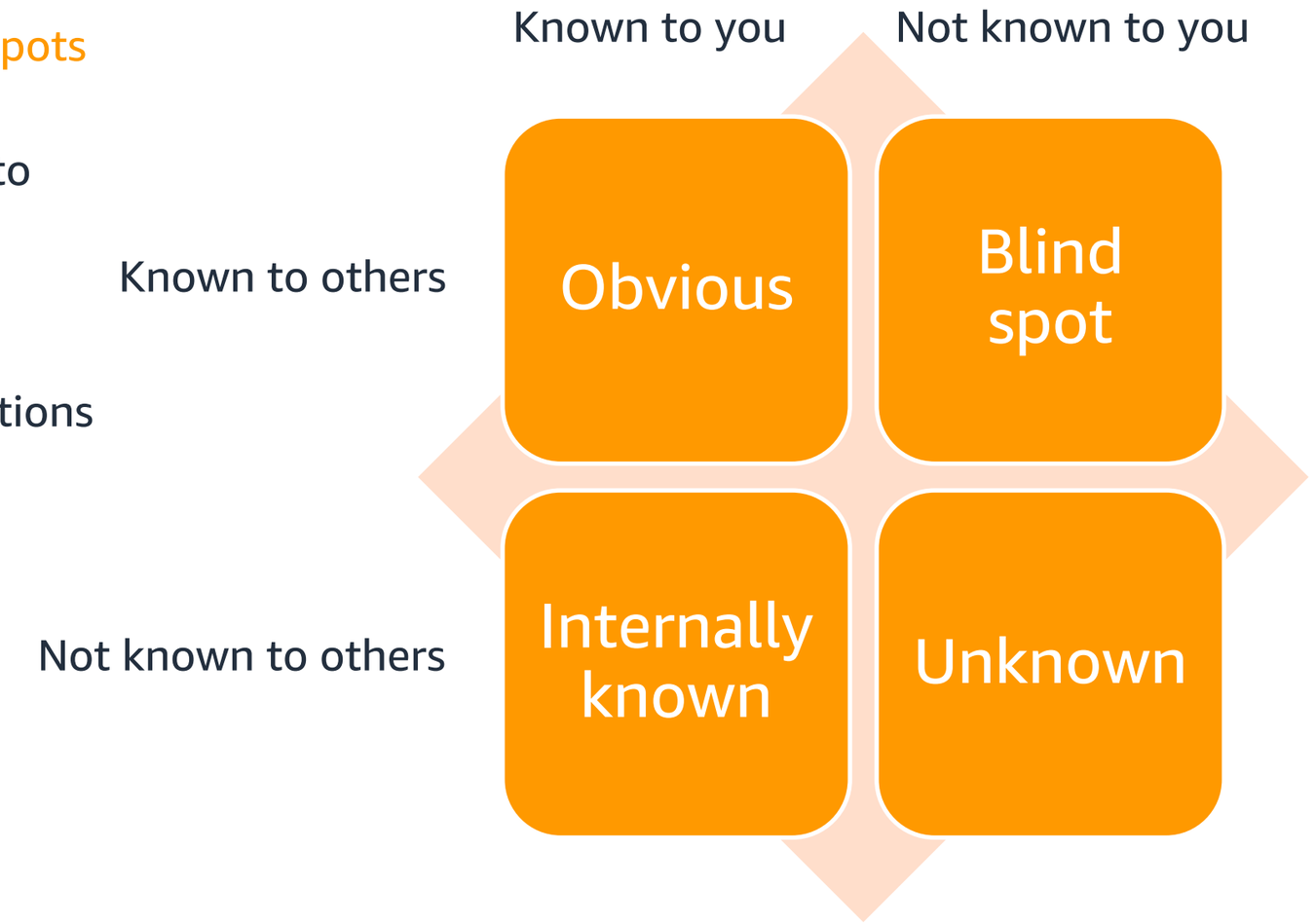
- Ideally before IR plan
- How to use AWS visibility and capabilities
- Documentation

Security culture

- Escalation and cooperation.
- No blame
- Everyone is part of security
- Continuous improvement

Incident Response – Partners and the Johari window

- Use partners' expertise to cover blind spots
- Use threat intelligence and modelling to reduce unknown risk
  - Finding new threats.
  - Defining new patterns.
  - Defining new automated acquisitions techniques.
  - Repeating these processes.



Prepare - Technology

Incident Response

aws professional services

Incident Response – Prepare access to AWS accounts

- Federation
- Cross-account access
- Authentication

- Indirect access
- Direct access
- Alternative access
- Automation access
- Managed Services access

Incident Response – Prepare processes

Define and prepare the related processes and playbooks necessary for investigation and remediation

- Decision Trees
- Use Alternative Accounts
- View or Copy Data
- Sharing Amazon EBS Snapshots
- Sharing Amazon CloudWatch Logs
- Use Immutable Storage
- Launch Resources Near the Event
- Isolate Resources
- Launch Forensic Workstations

Incident Response – Cloud provider support

AWS Managed Services (AMS)

- Ongoing management of your AWS infrastructure
- Automates common activities

AWS Support

- Range of support plans that provide access to tools and expertise to support operational health of AWS solutions.

DDoS response support

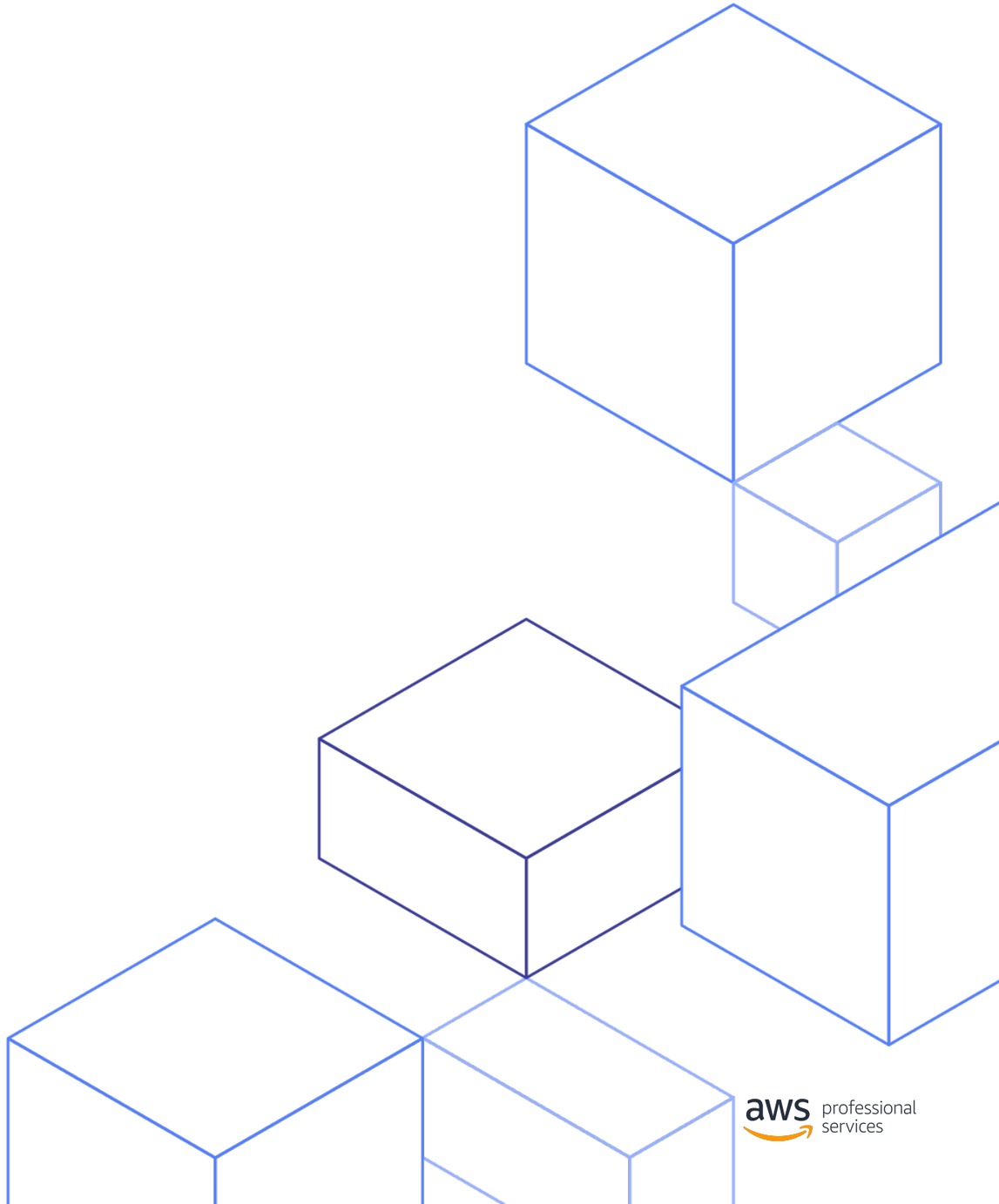
- AWS Shield
- AWS Shield Advanced - 24/7 access to the AWS DDoS Response Team

AWS Customer Incident Response team

- Specialized team that assists and advises customers during active security events on the customer's side of the AWS Shared Responsibility Model

Amazon Detective

Incident Response



Incident Response – Amazon Detective

1) Finding / Alert triage

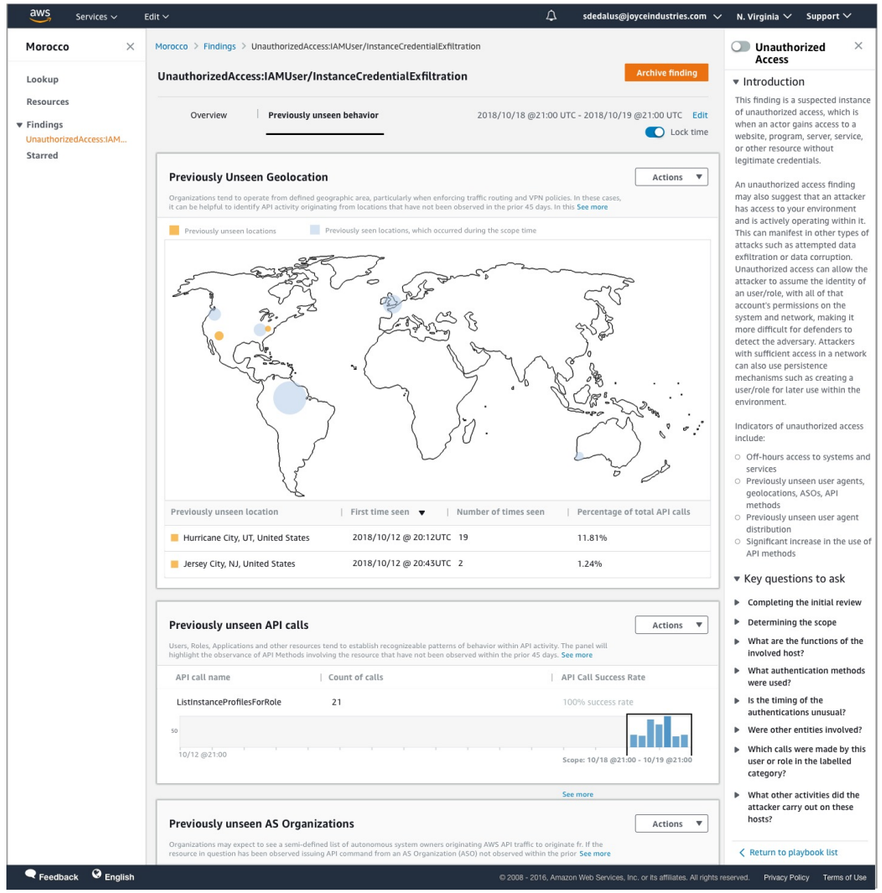
Accelerate triage and avoid unnecessary escalations

2) Incident Investigation

Improve context and surface correlated behavior

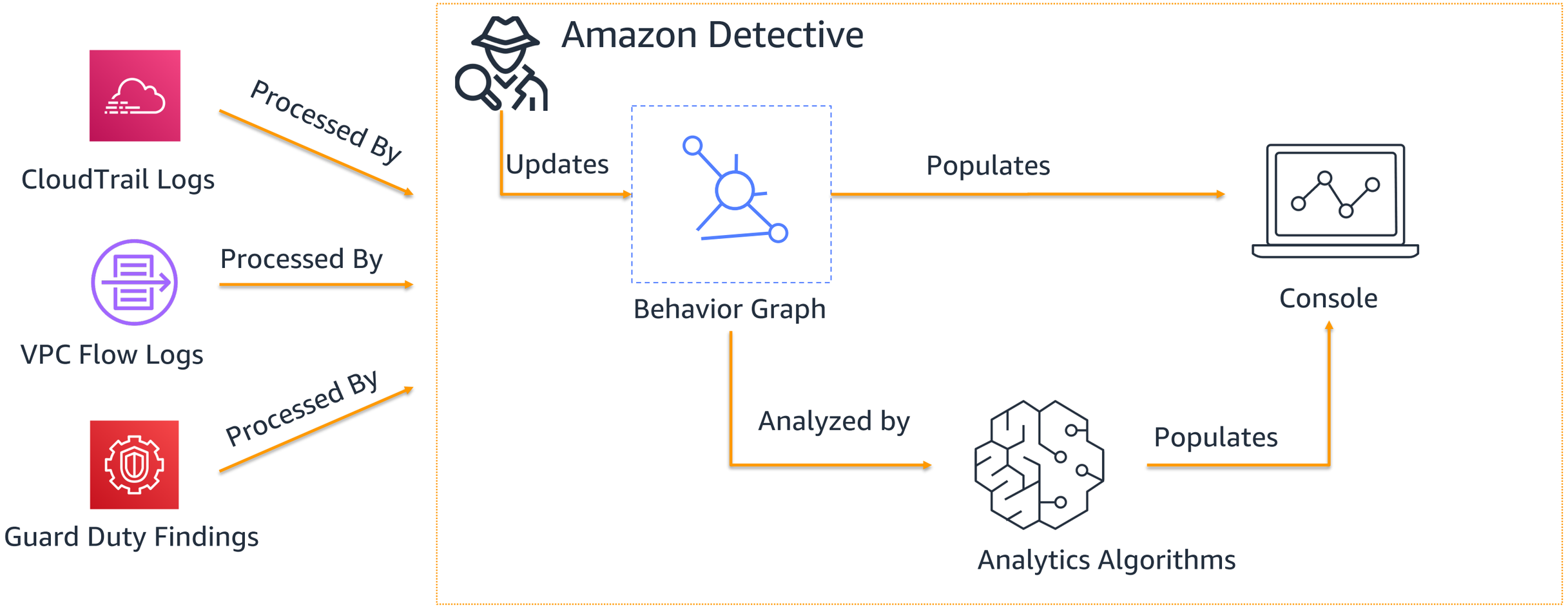
3) Threat Hunting

Simplify data collection, aggregation and pivoting



aws professional services

Incident Response – Amazon Detective



aws professional services

Incident Response Domains

Incident Response

aws professional services

Incident Response – Service Domain

Service domain incidents are typically handled through AWS APIs.

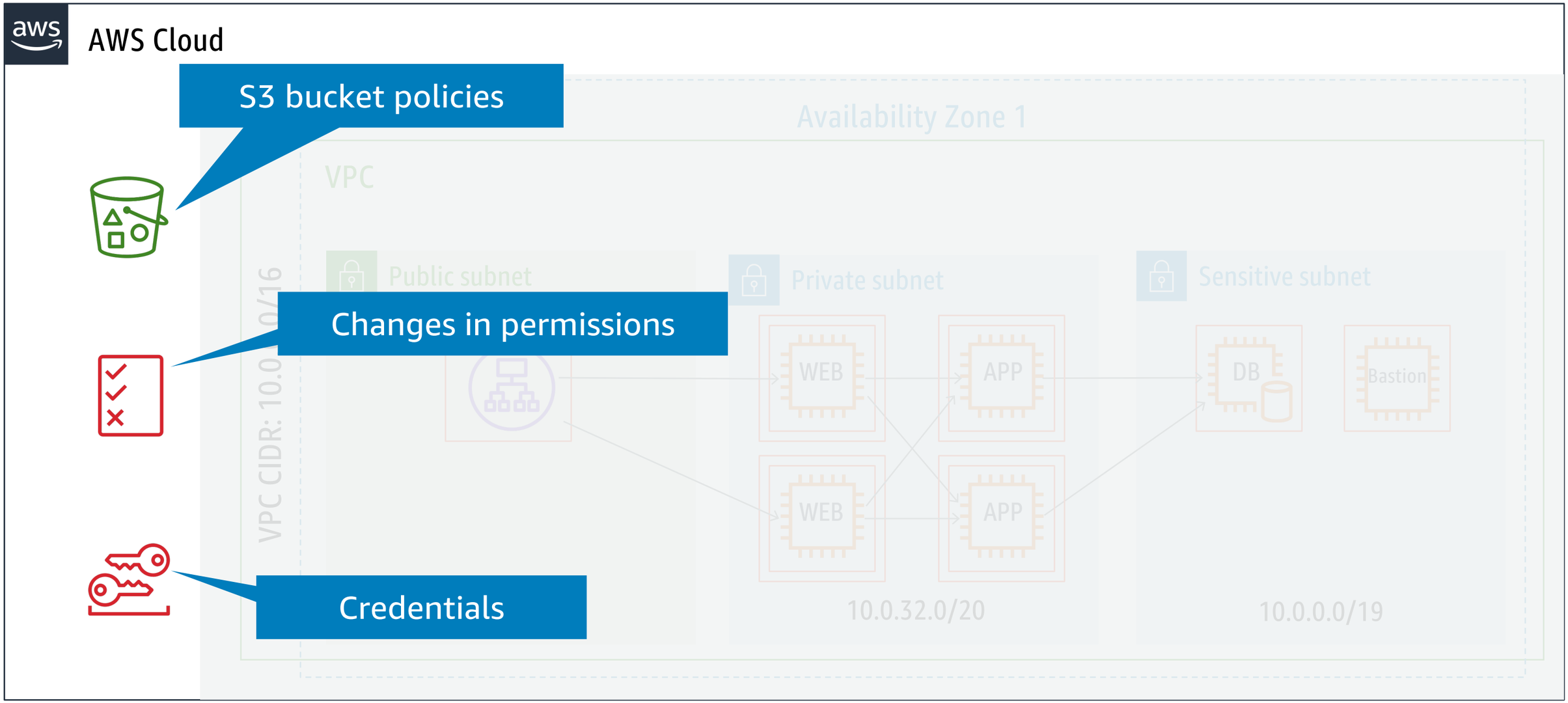
Identities

- Ensure identities follow least privilege model to prevent abuse of APIs
- Do not use root account unless essential
- Follow IAM best practice

Resources

- Ensure resources match how you intend to operate in the cloud
- Regularly check for security misconfigurations

Incident Response – Service Domain



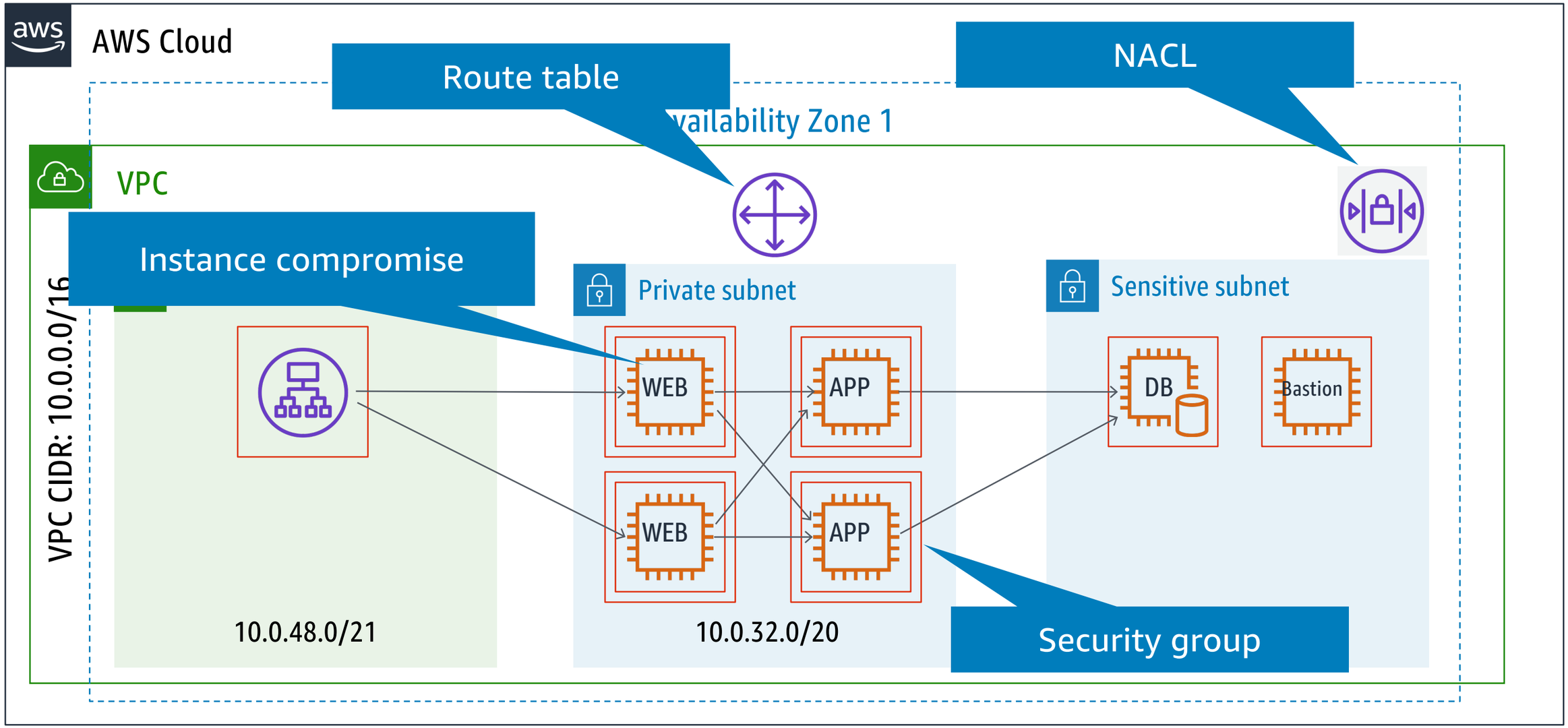
Incident Response – infrastructure & application domain

The infrastructure domain typically includes your application's data or network-related activity.

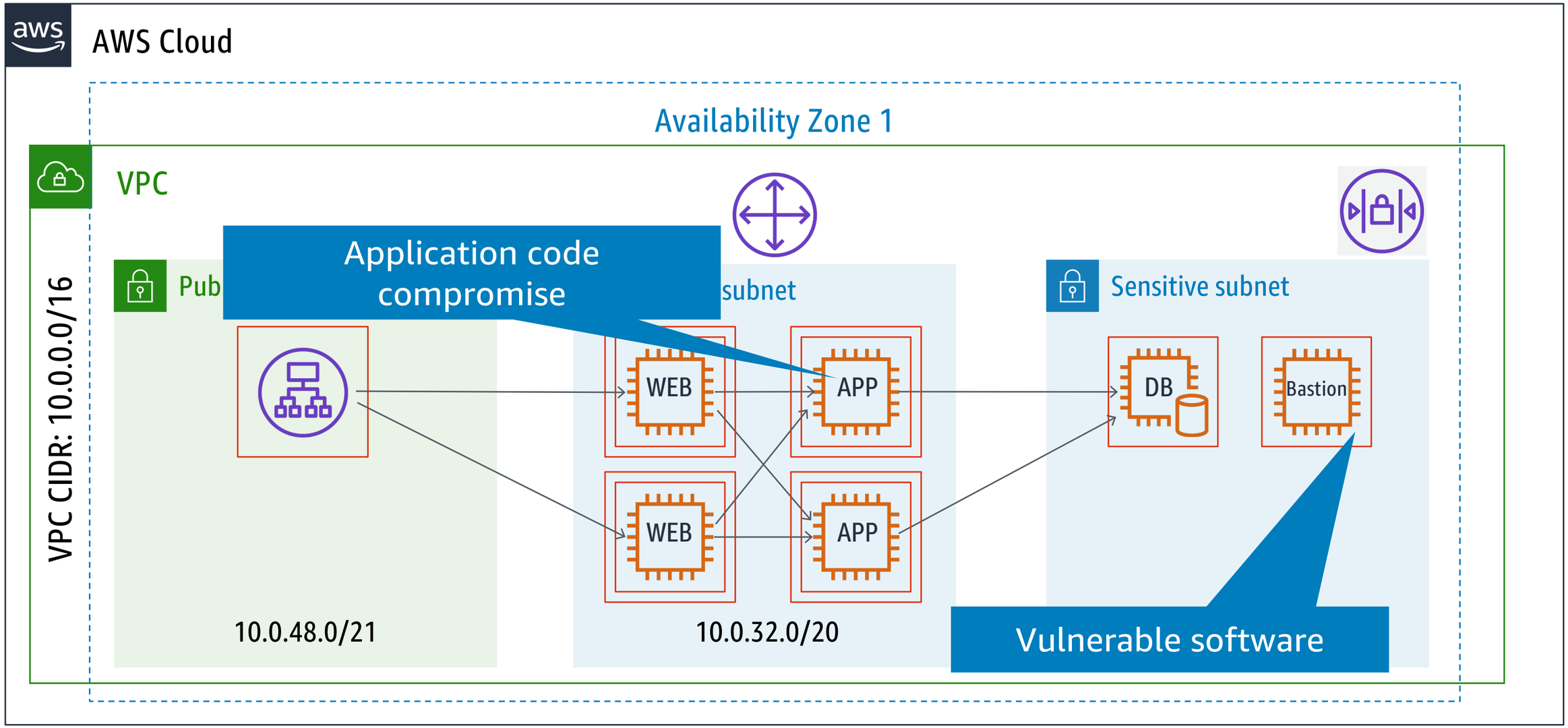
Typical steps to resolve an infrastructure incident:

- **Capture** the metadata from EC2 instance
- **Protect** the Amazon EC2 instance from accidental termination
- **Isolate** the Amazon EC2 instance by switching the VPC Security Group
- **Detach** the Amazon EC2 instance from any Auto Scaling groups
- **Deregister** the Amazon EC2 instance from any related Elastic Load Balancing service.
- **Snapshot** the Amazon EBS data volumes
- **Tag** the Amazon EC2 instance as quarantined for investigation

Incident Response – Infrastructure Domain



Incident Response – Application Domain



Incident Response – infrastructure & application domain

Investigation Decisions
- Offline or Online investigations

Capturing Volatile Data
- Manual connection vs automated tools

AWS Systems Manager
- Remotely and securely perform on-demand changes running Linux shell scripts and Windows PowerShell commands on a targeted instance

Automating capture
- Use tagging, SSM Agent, and CloudWatch events to trigger isolation and capture of memory

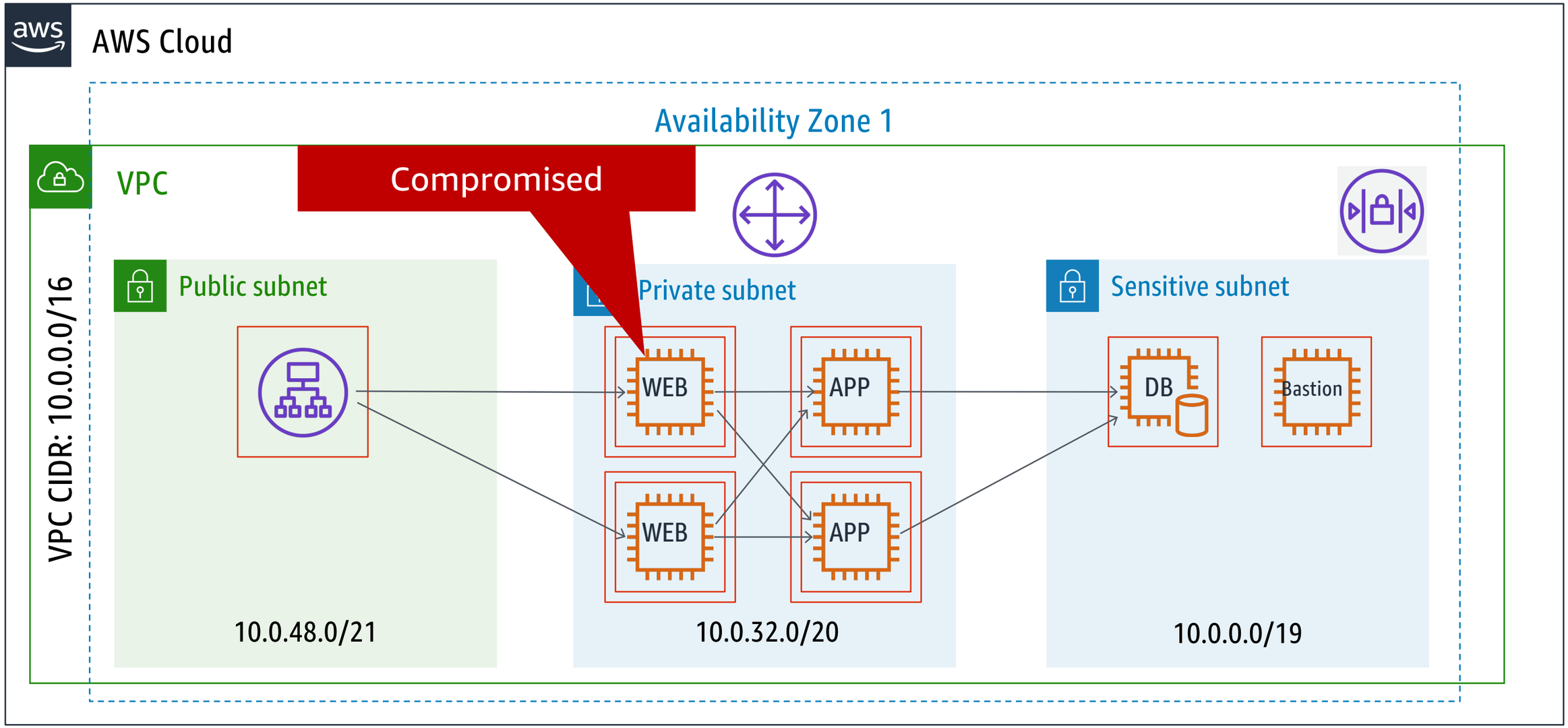
Incident Response – infrastructure & application domain

Two options for forensic analysis in the infrastructure domain:

- Online analysis
- Offline analysis

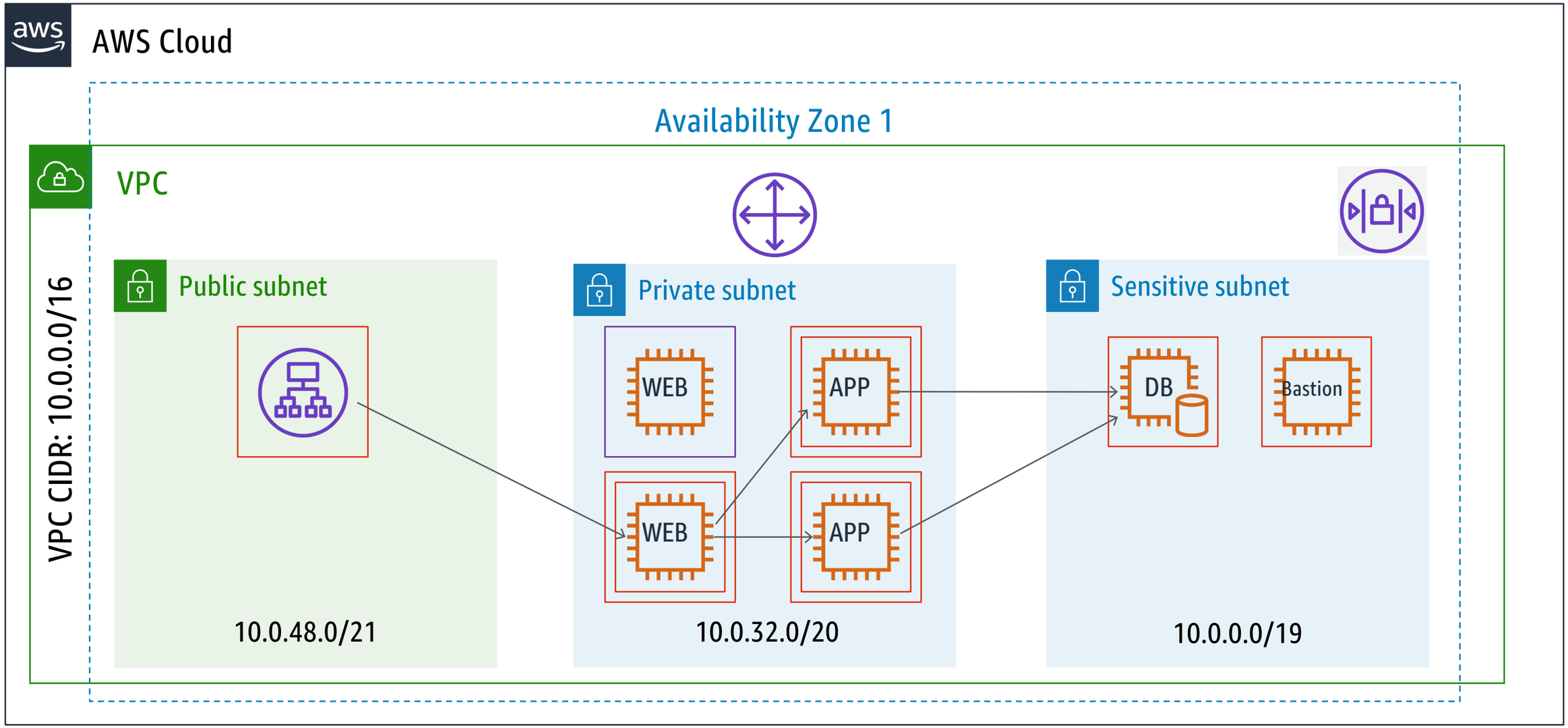
You can do either or both

Incident Response – Offline Analysis EC2



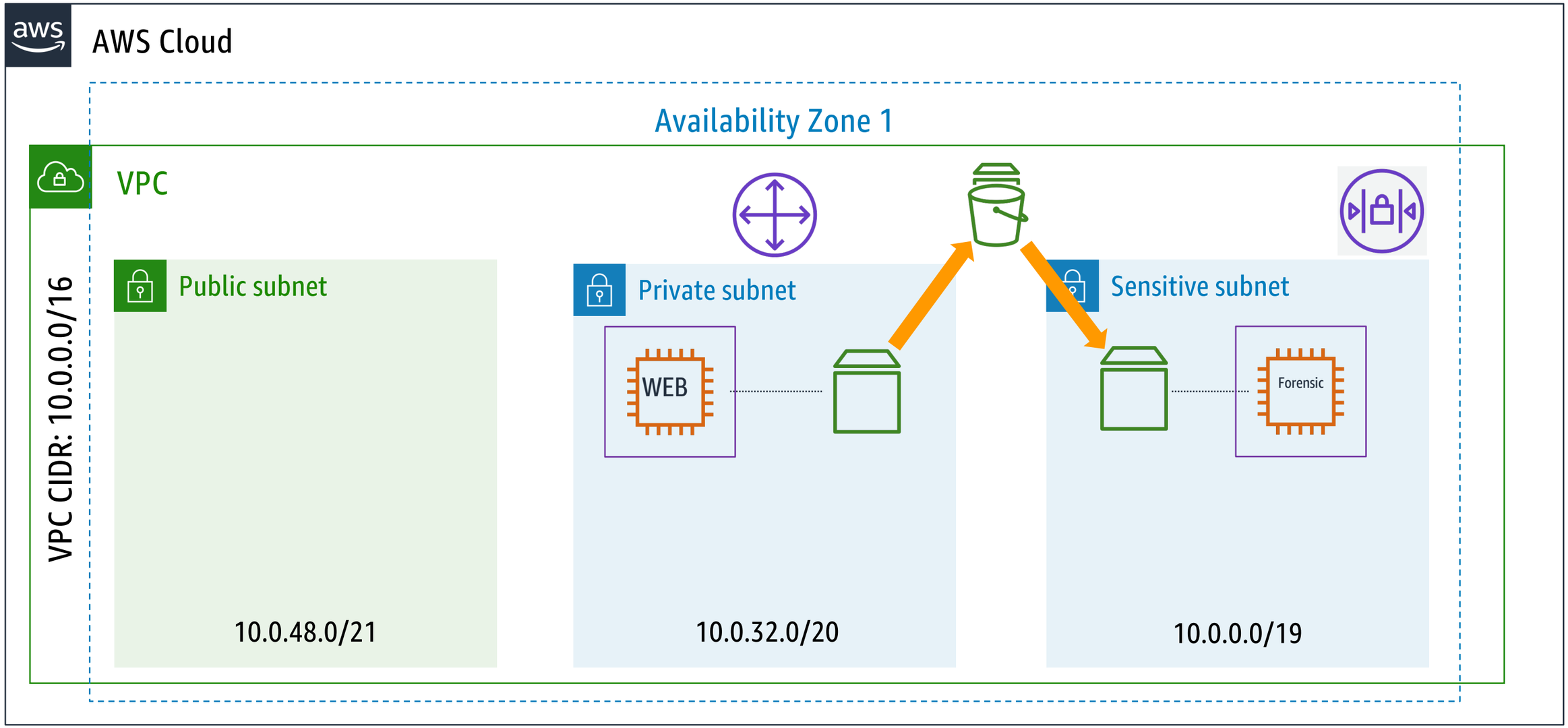
aws professional services

Incident Response – Offline Analysis EC2

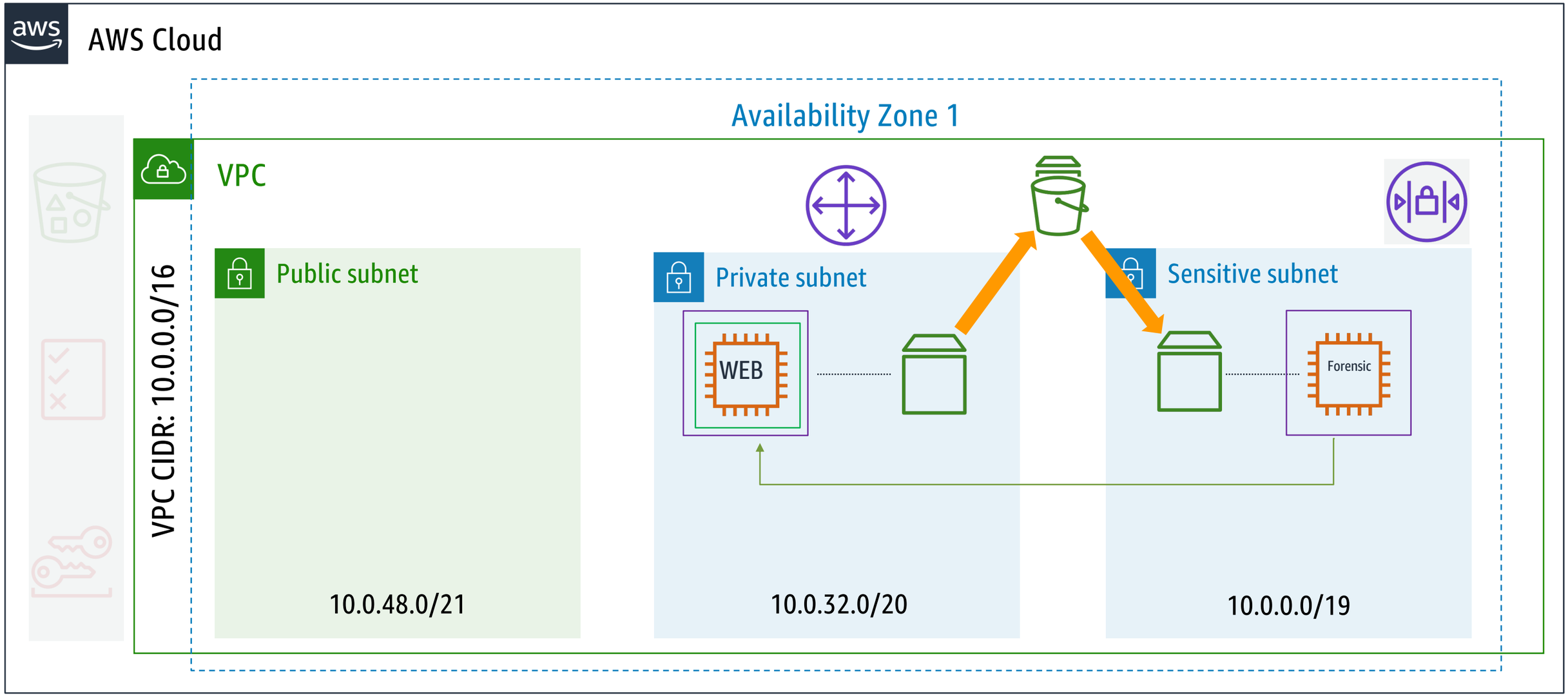


aws professional services

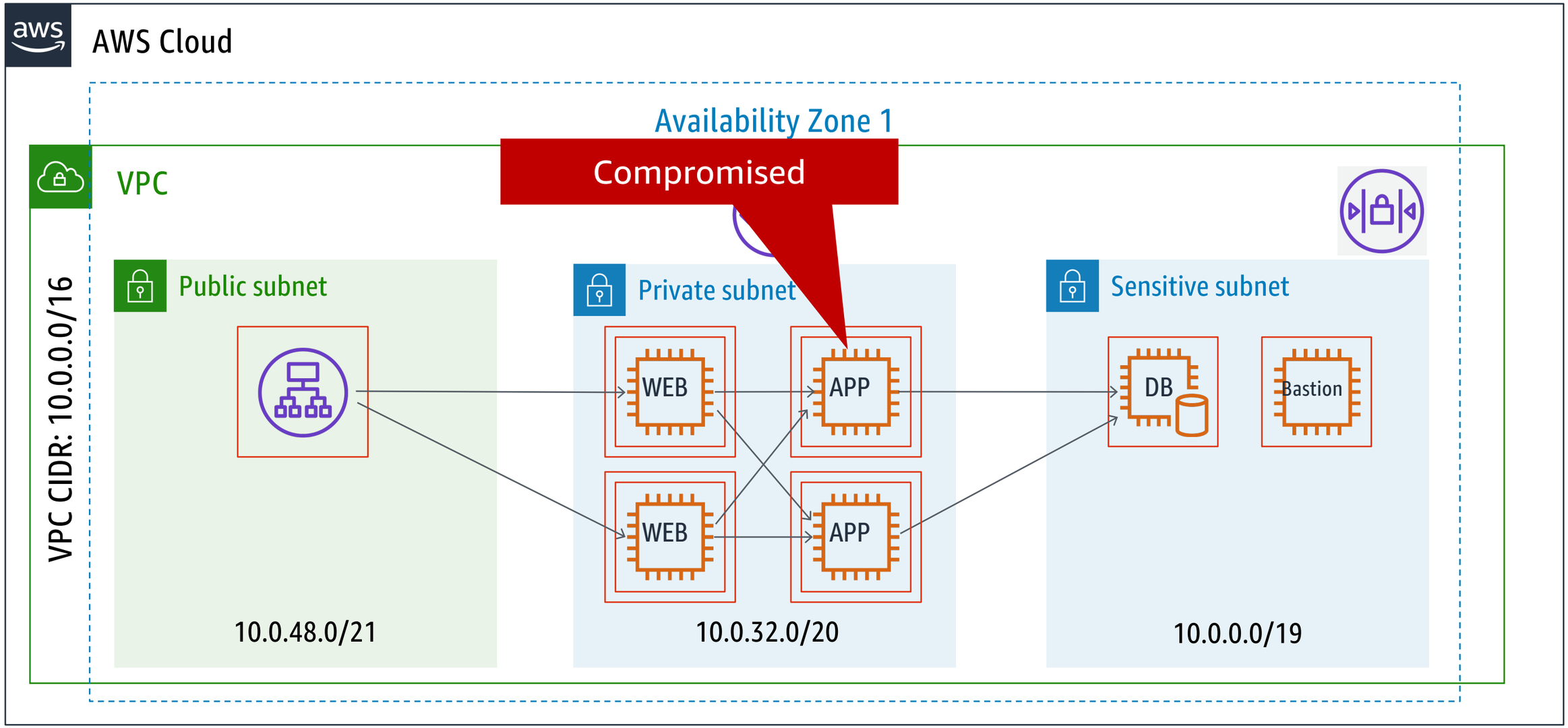
Incident Response – Offline Analysis EC2



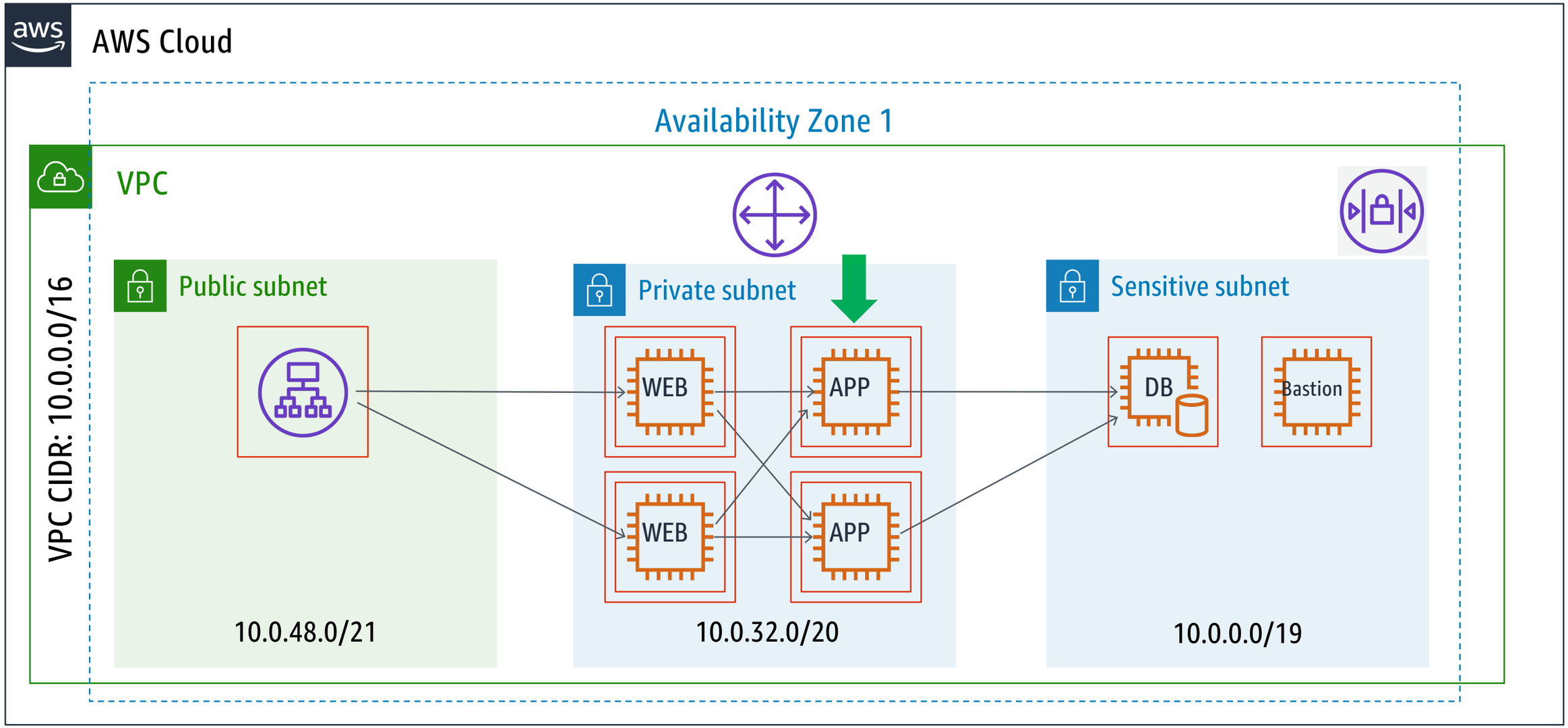
Incident Response – Offline Analysis EC2



Incident Response – Online Analysis EC2



Incident Response – Online Analysis EC2



aws professional services

Incident Response – Preparation

- Keep a pre-configured forensics AMI on hand
- Decide on the forensic procedure
- Create IAM role for incident responders and for the forensic workstation

Incident Response – Third Party Tools

Response

- AWS IR (ThreatResponse)

Case Management

- Incident Pony (ThreatResponse)

Networking

- Moloch
- Wireshark

Enterprise

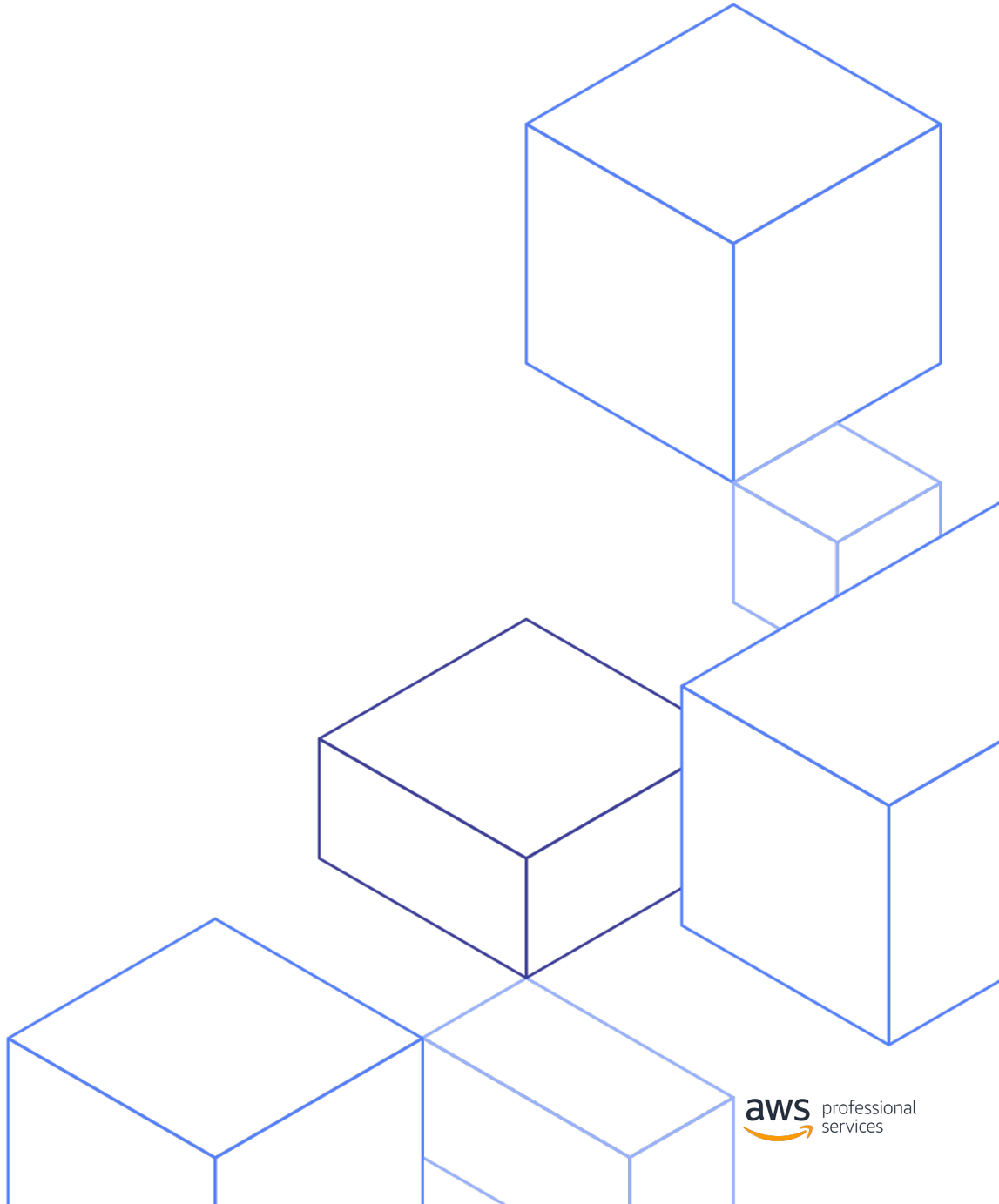
- Mandiant
- EnCase
- Forensic Tool Kit
- Google Rapid Response

Memory Capture

- Fastdump
- FTK Imager
- LiME
- Margarita Shotgun (ThreatResponse)

Simulate

Incident Response



Incident Response - Security Incident Response Simulations (SIRS)

Internal events that provide a structured opportunity to practice your incident response plan and procedures during a realistic scenario.

Value for customers:

- Validate readiness
- Develop confidence – learning opportunity and train staff
- Following compliance or contractual obligations
- Generate artifacts for accreditation
- Be agile – incremental improvement with focus
- Improving speed and tools
- Refine escalation and communication
- Develop comfort with the rare and the unexpected
- Identify areas for improvement

Incident Response - Preparing for a simulation

NB – AWS customers are welcome to carry out security assessments or penetration tests against their AWS infrastructure without prior approval for 8 services, listed at the link below. If you are planning a Security Incident Response Simulation (SIRS), see link below for further details of where prior approval might be required

https://aws.amazon.com/security/penetration-testing/

aws professional services

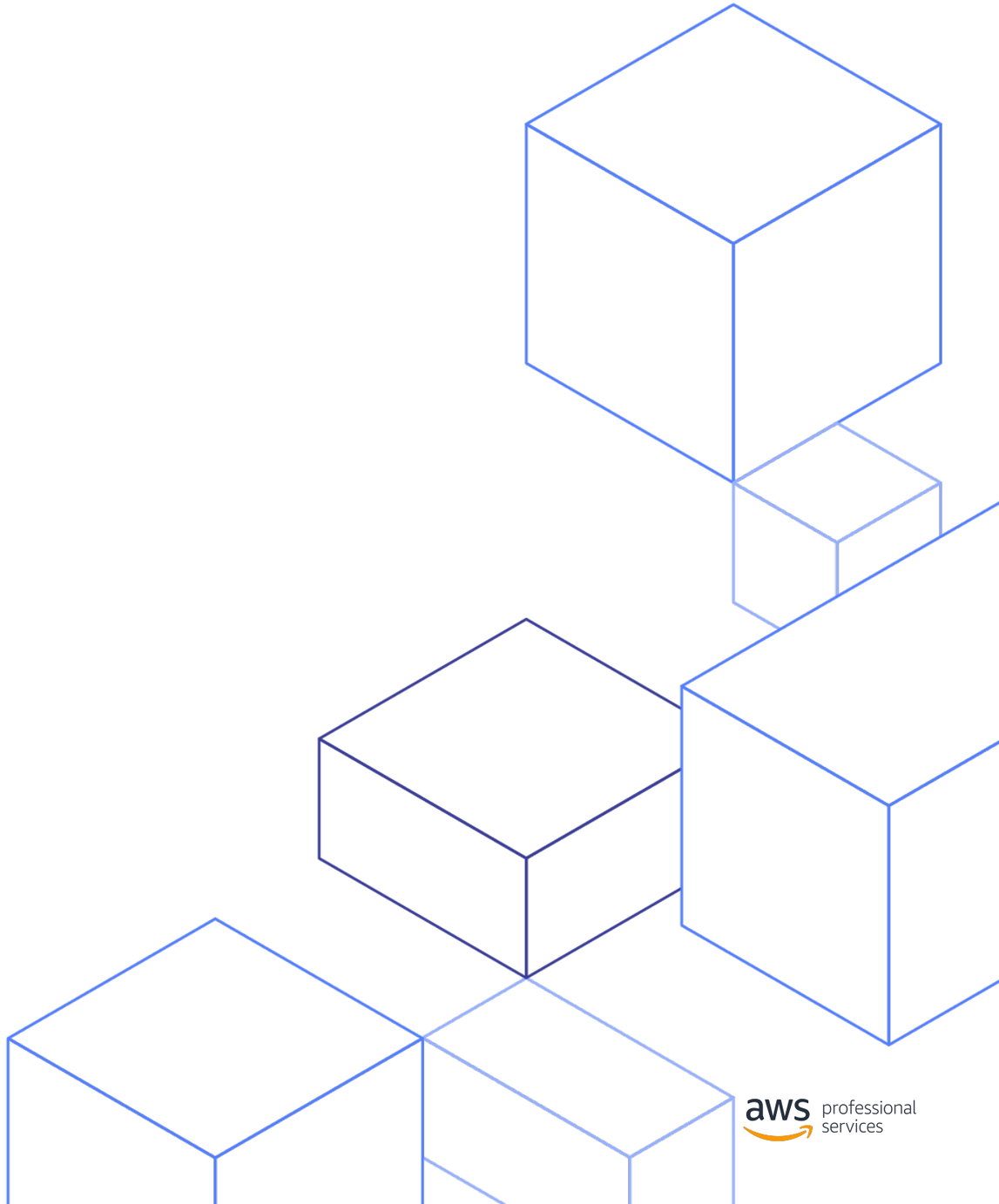
Incident Response – Simulation Examples

Security simulations must be realistic to provide the expected value. For example:

- Unauthorised changes
- Public exposure of credentials
- Sensitive content exposed publicly
- Web server communicating with malicious IP addresses

Iterate

Incident Response



Incident Response - Runbooks

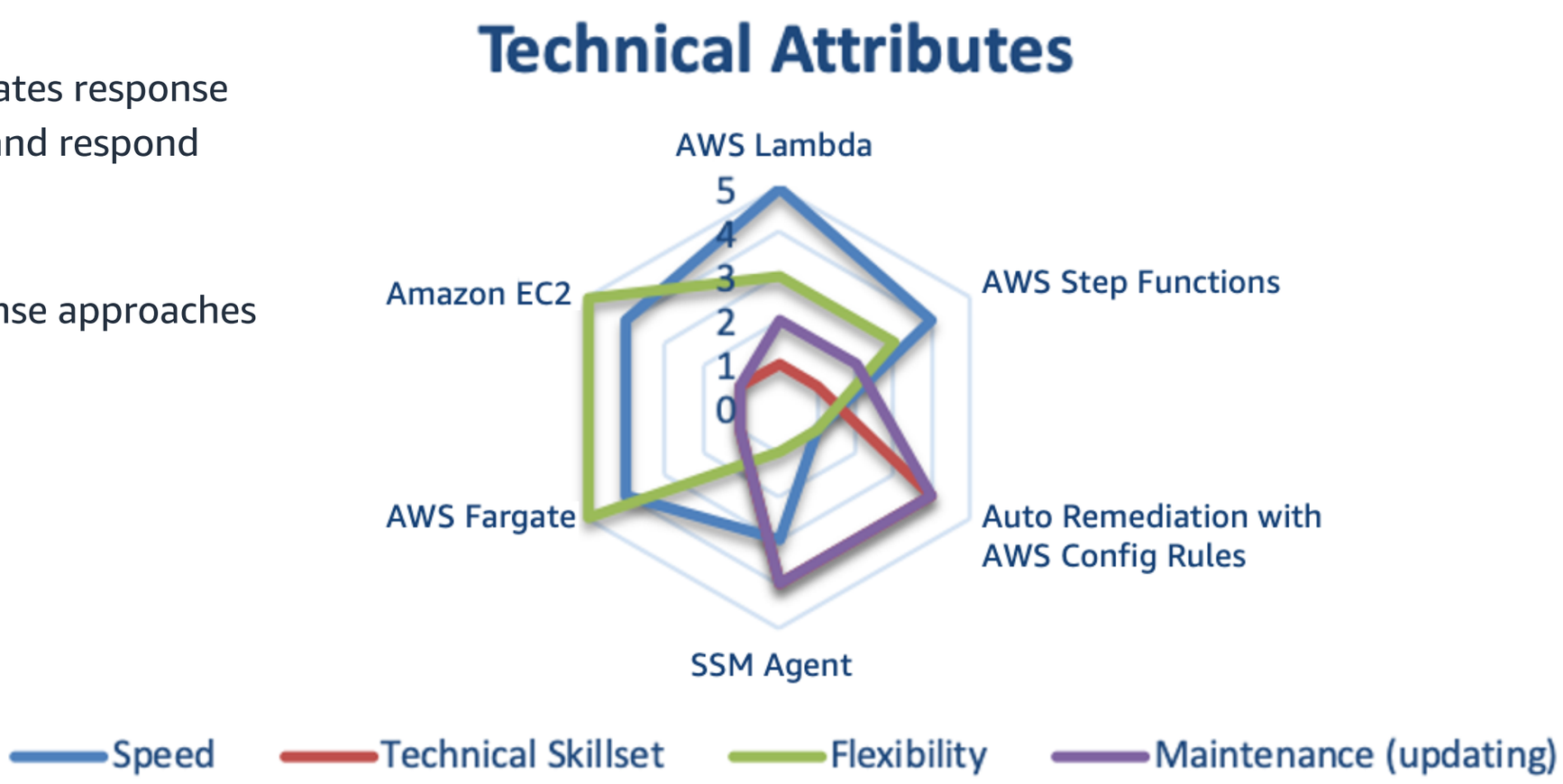
Documented form of an organization's procedures for conducting a task or series of tasks

- Start by focussing on current alerts
- Useful tools – AWS Trusted Advisor, Security Hub, AWS Config rules
- Test processes and iterate
- Determine exceptions
- Convert logic to code

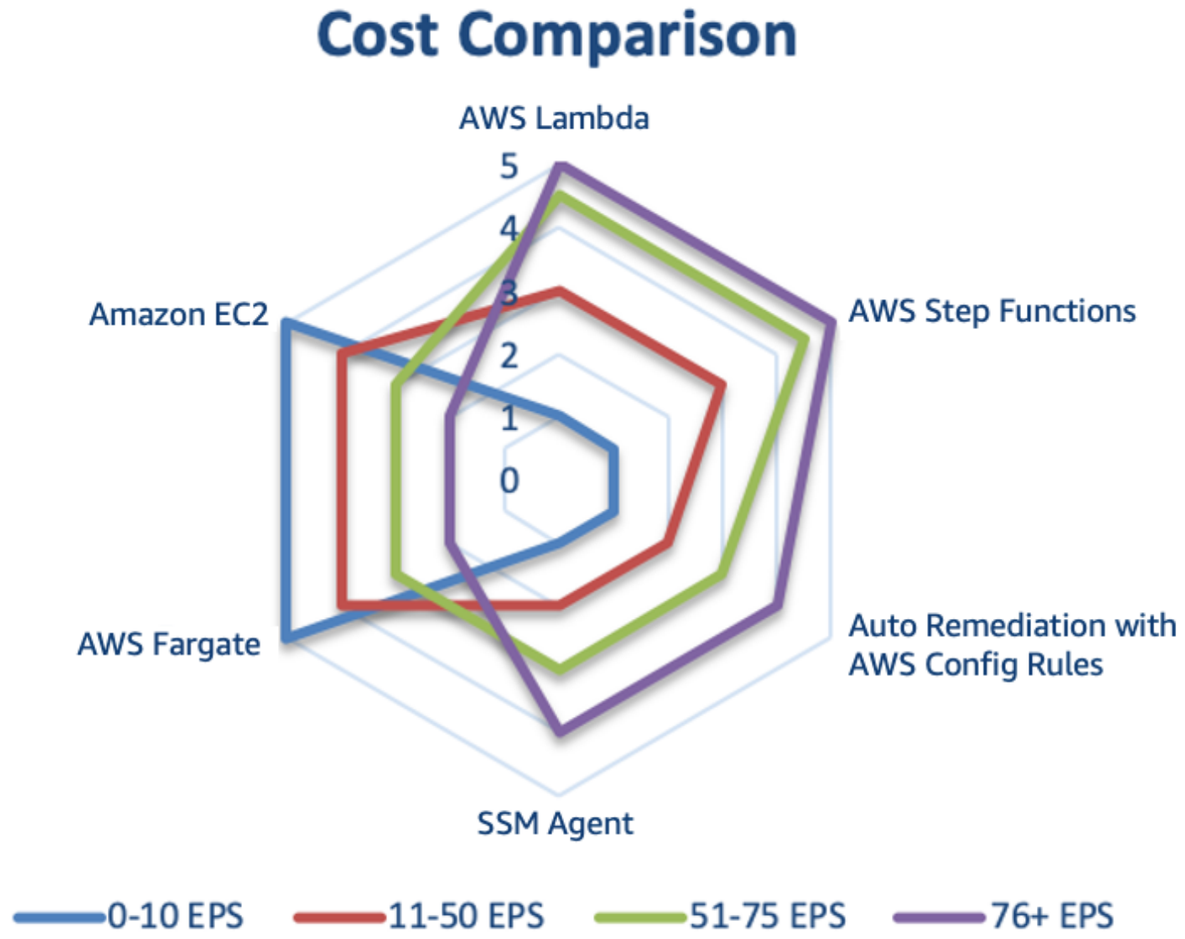
Incident Response – Comparison of automation technical approaches

- AWS tools and APIs
- System monitors, reviews, initiates response
- Reduces time between detect and respond

Several options to automate response approaches



Incident Response – Cost comparison of scanning methods



Incident Response – Centralized vs decentralized approach

Centralization refers to a central account that drives all of the detection and remediation for an organization.

	Centralization	Decentralization
Pros	Simple configuration management Unable to cancel or modify response	Simple architecture Faster initial setup
Cons	Increased complexity in architecture Onboarding/offboarding accounts and resources	More resources to manage Difficulty maintaining a software baseline

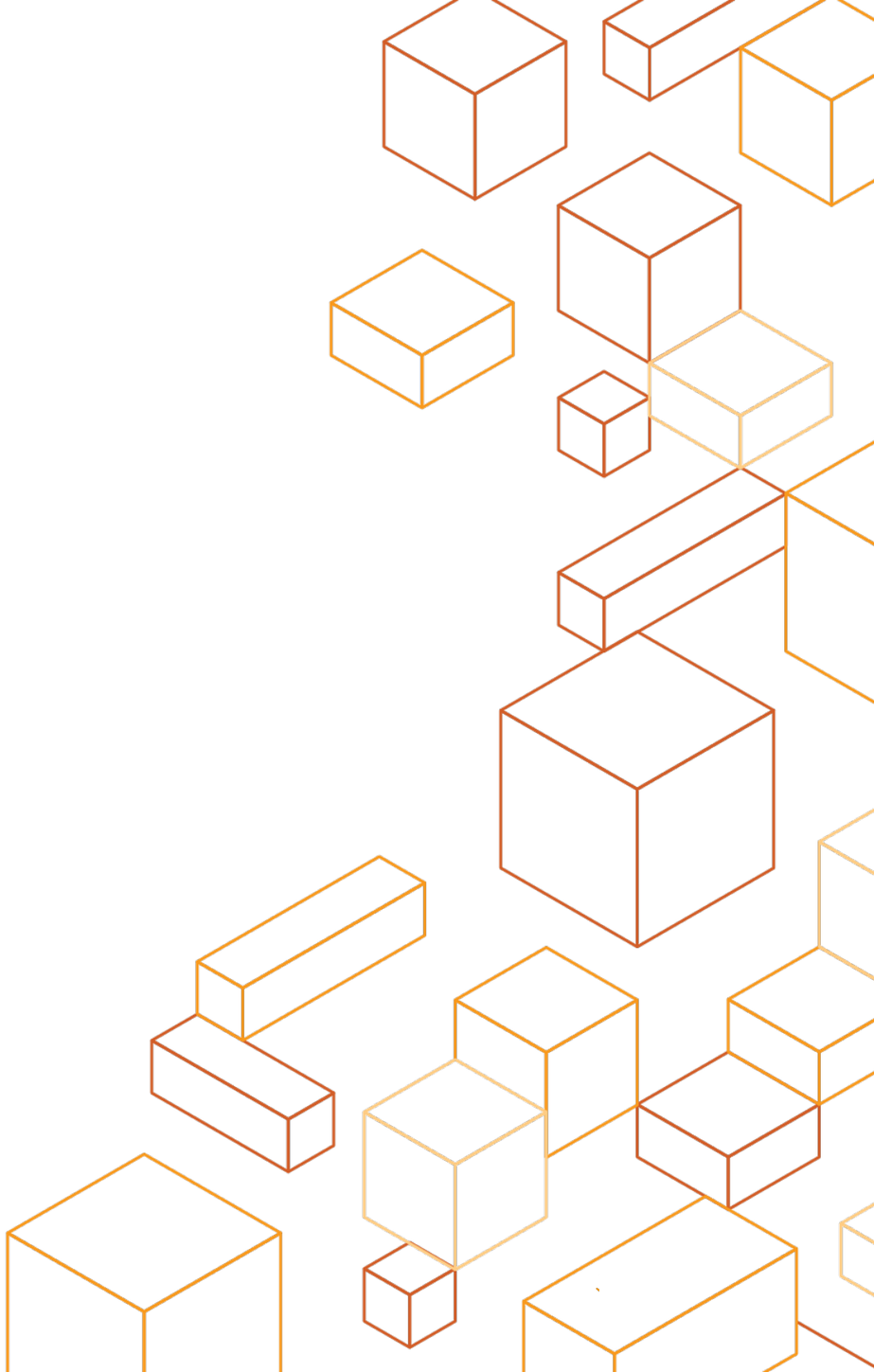
Incident Response – Event-driven response example

With an *event-driven response* system, a detective mechanism triggers a responsive mechanism to automatically remediate the event.

- Reduces time between detect and respond
- Uses AWS Lambda (serverless compute service)
- E.g. use CloudWatch Events to monitor for events and Lambda to handle response
- Lambda function can perform response tasks and notify responder

aws professional services

Questions



Appendix A - Resources

Incident Response Whitepaper

https://d1.awsstatic.com/whitepapers/aws_security_incident_response.pdf

Sample playbook framework

https://github.com/aws-samples/aws-customer-playbook-framework