AWS Incident Response

AWS Security Workshop

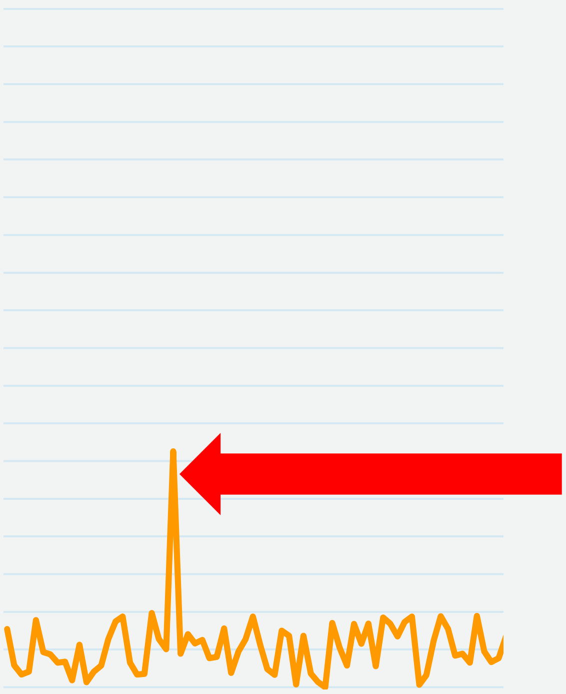
Agenda

- Different types of incidents
- Infrastructure related incidents
- Service related incidents
- Incident management

Goals

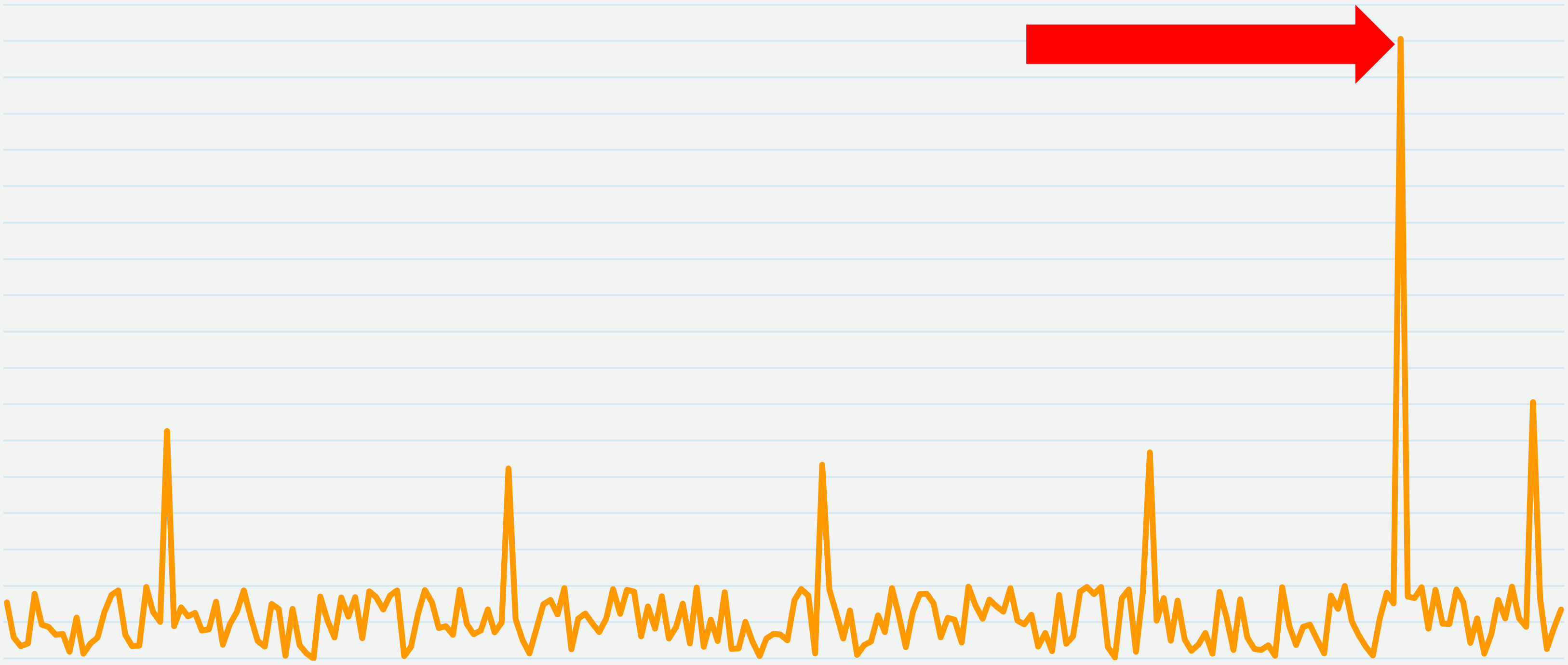
- Become aware of indicators of security incidents
- Classify incident types
- Discover sources of information to respond to an incident
- Understand incident response workflows
- Learn to prepare for incidents

Incident Response – Understanding Normal

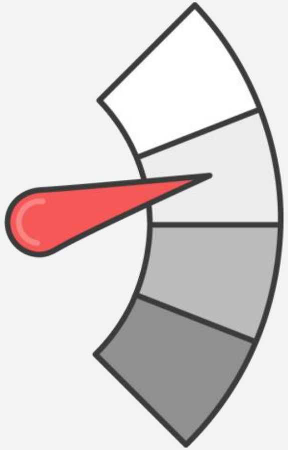


Incident: deviation from your [security] baseline

Incident Response – Understanding Normal

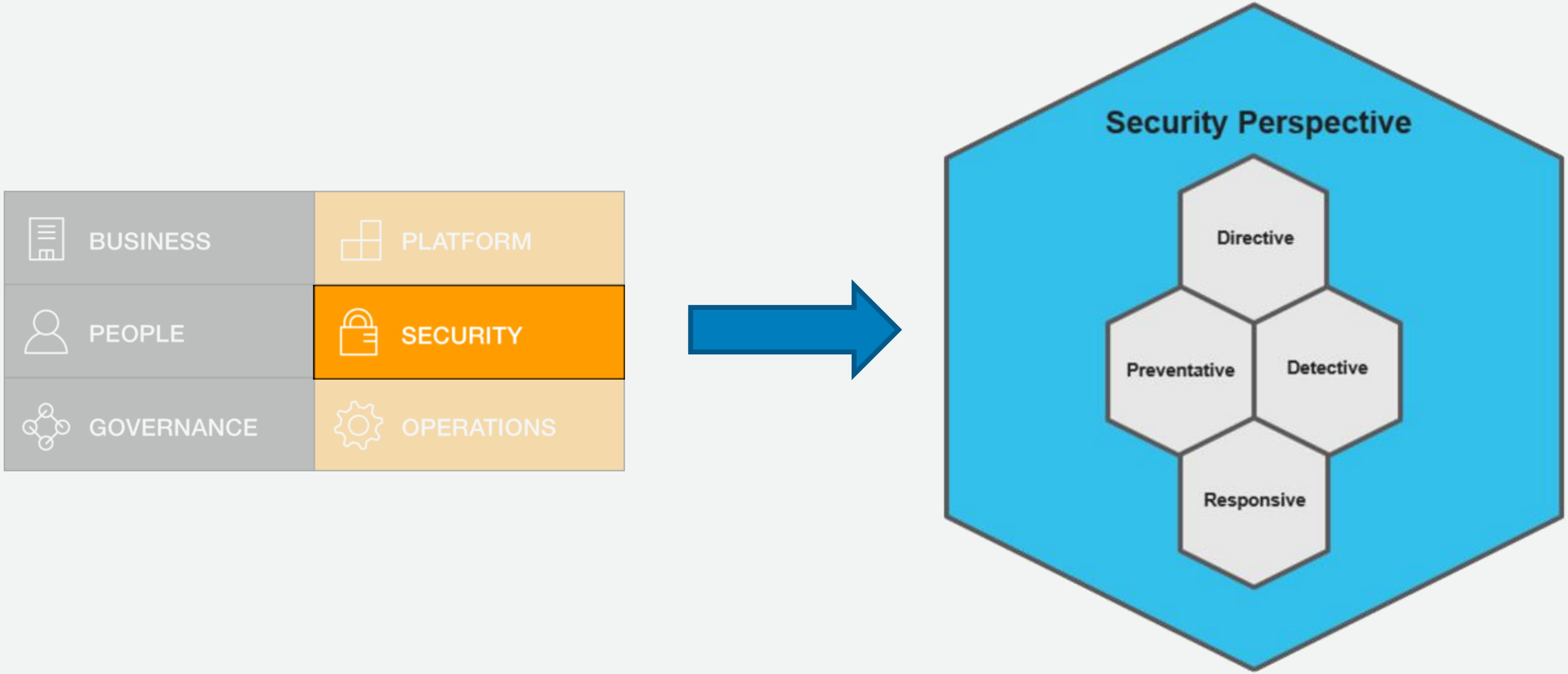


Incident Response – Indicators



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

Incident Response – Cloud Adoption Framework



BUSINESS

PLATFORM

PEOPLE

SECURITY

GOVERNANCE

OPERATIONS

Security Perspective

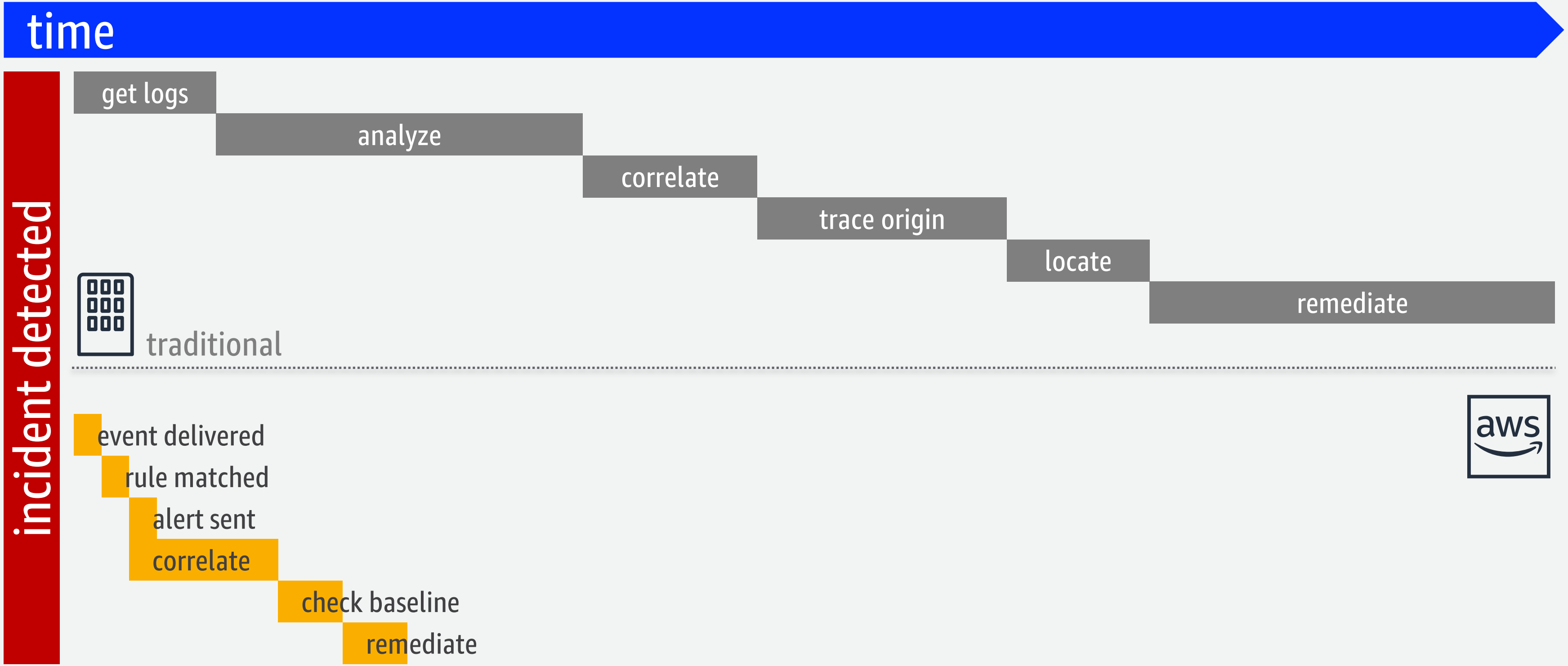
Directive

Preventative

Detective

Responsive

Incident Response – Time Comparison (example)



time

incident detected

get logs

analyze

correlate

trace origin

locate

remediate

traditional

event delivered

rule matched

alert sent

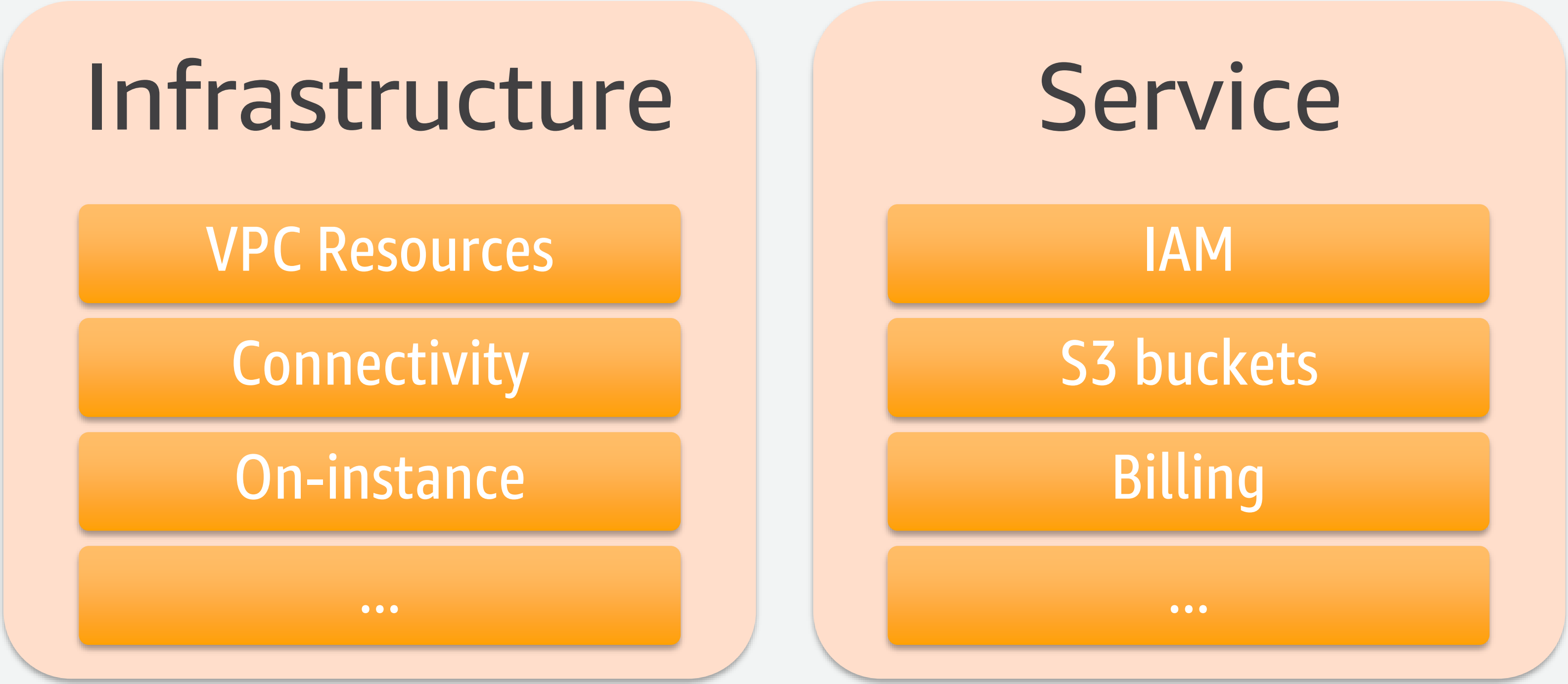
correlate

check baseline

remediate

aws

Incident Response - Domains



Infrastructure

- VPC Resources
- Connectivity
- On-instance
- ...

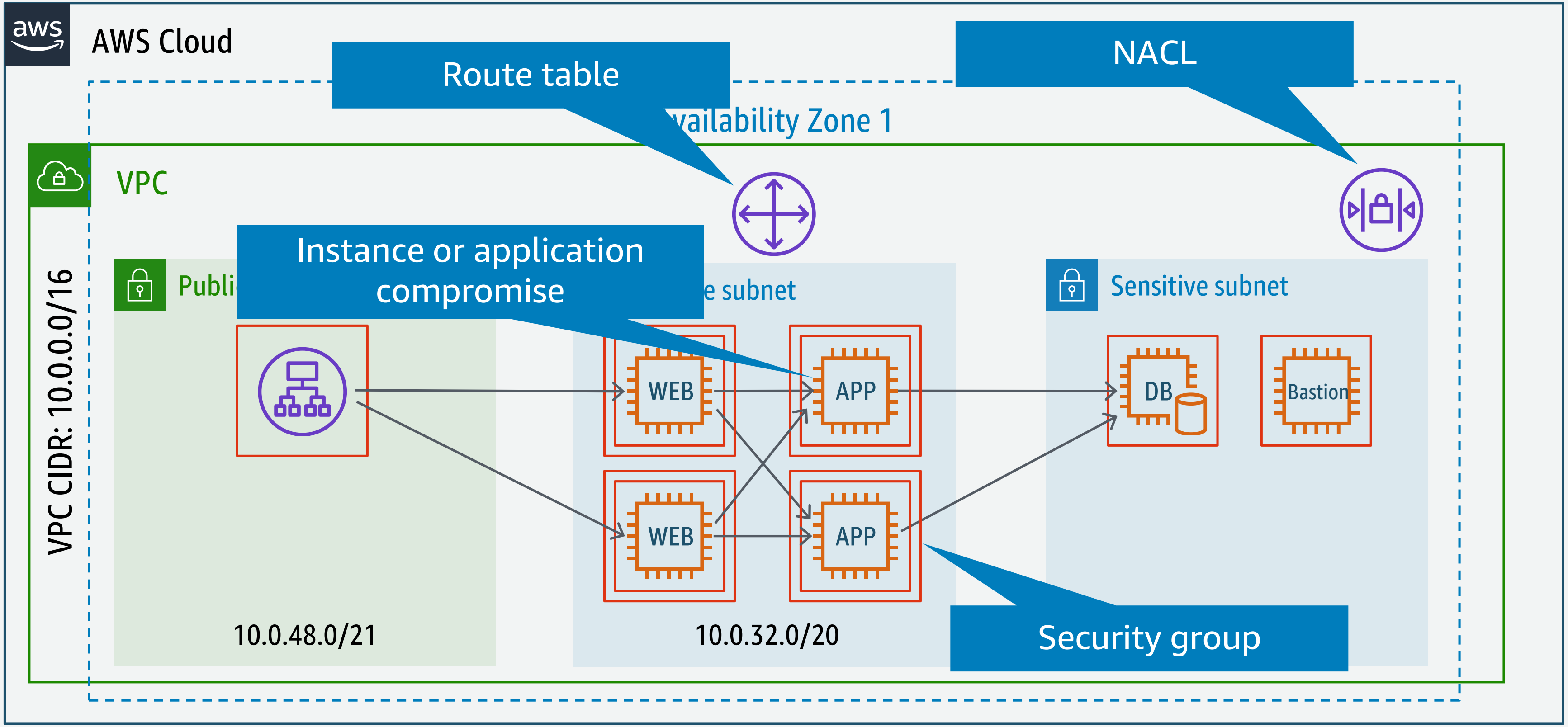
Service

- IAM
- S3 buckets
- Billing
- ...

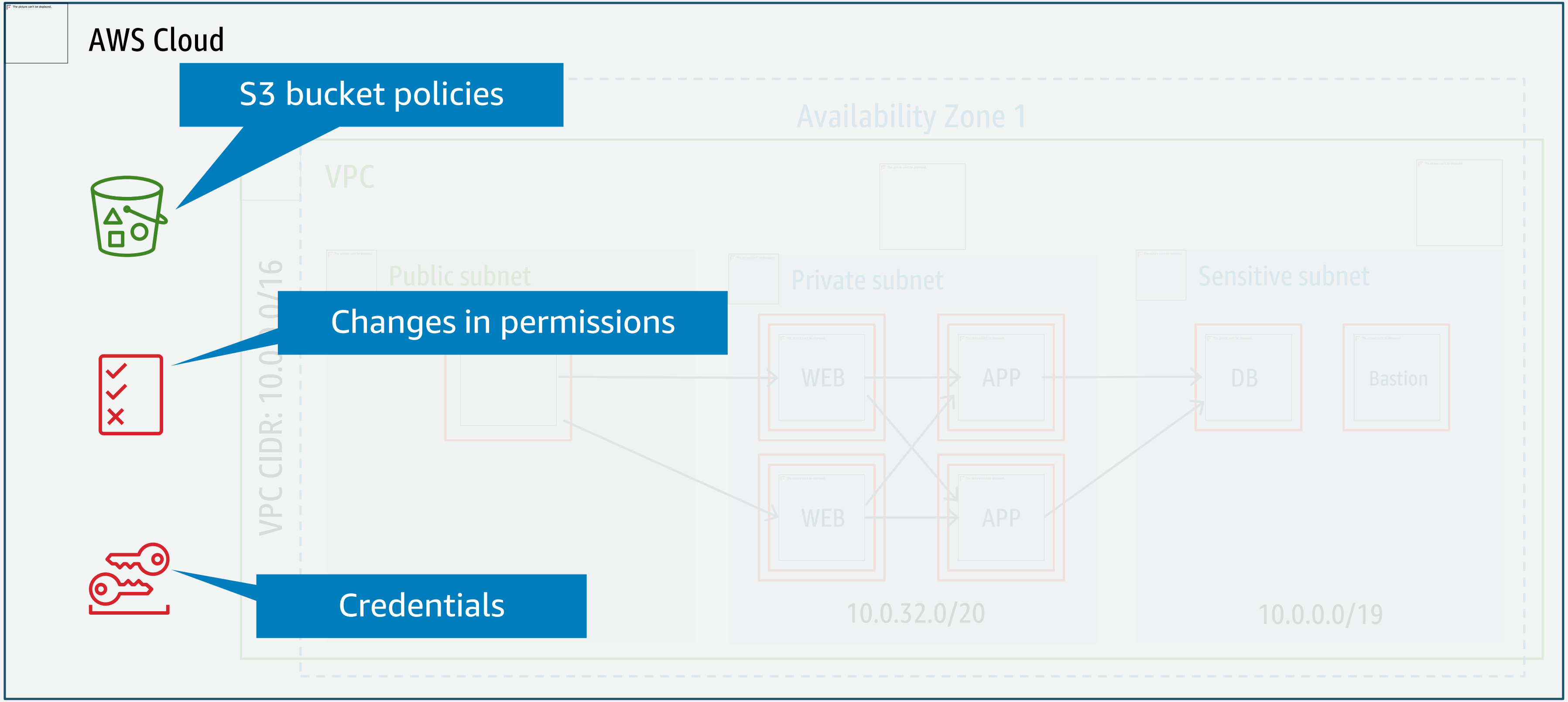
Incident Response – Incident Types

- Compliance variance
- Service disruption
- Unauthorized resources
- Unauthorized access
- Privilege escalation
- Persistence
- Excessive permissions
- Information exposure
- Credentials exposure

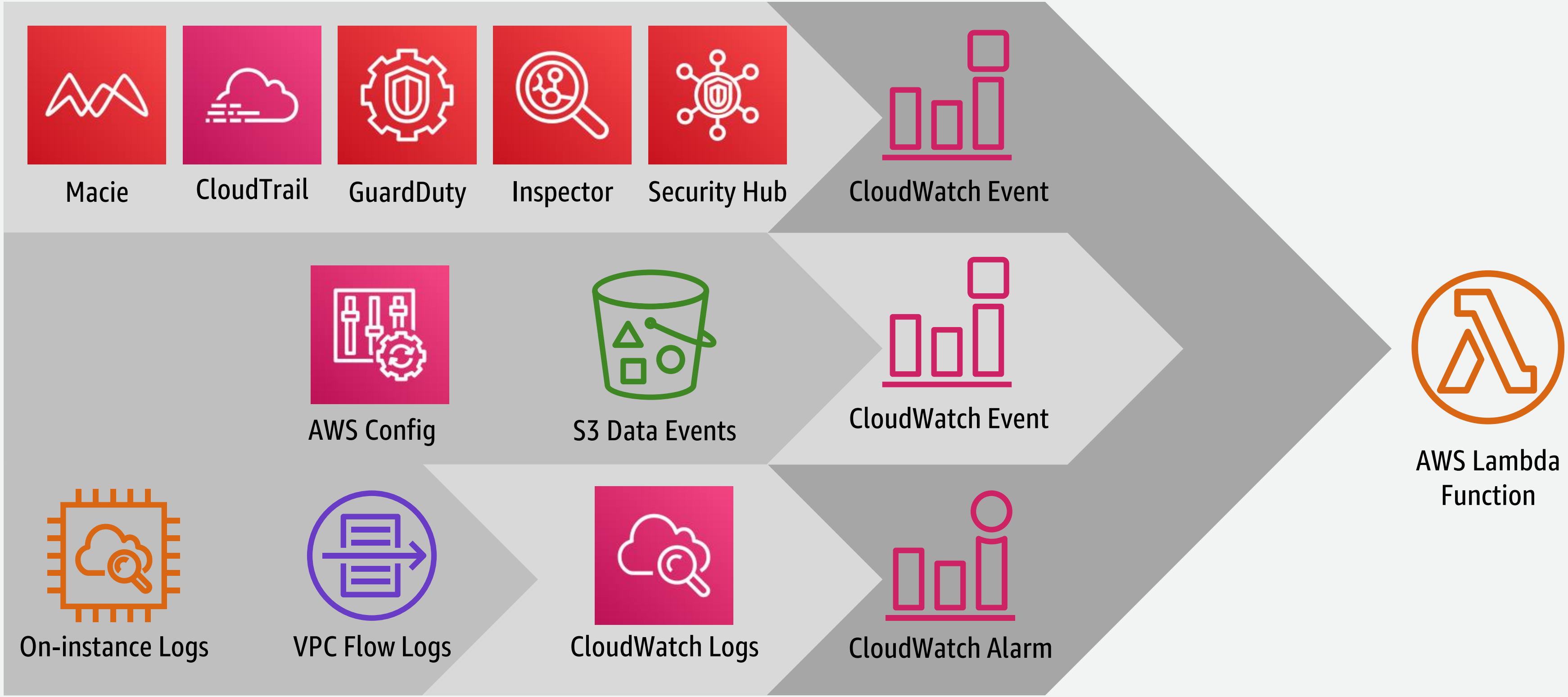
Incident Response – Infrastructure Domain



Incident Response – Service Domain



Incident Response - Wrangling Information Sources



Infrastructure Domain

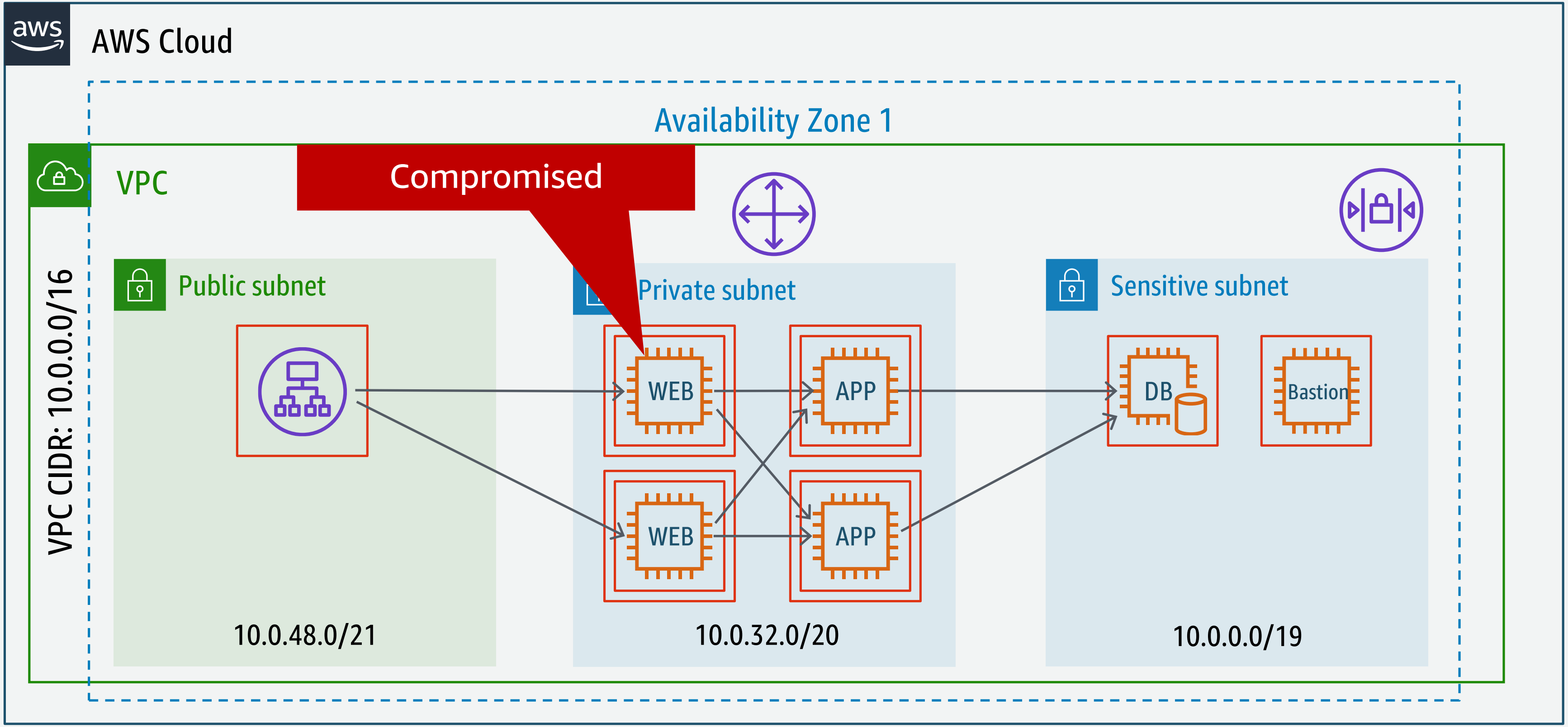
Incident Response – Infrastructure Domain

Two options for forensic analysis in the infrastructure domain:

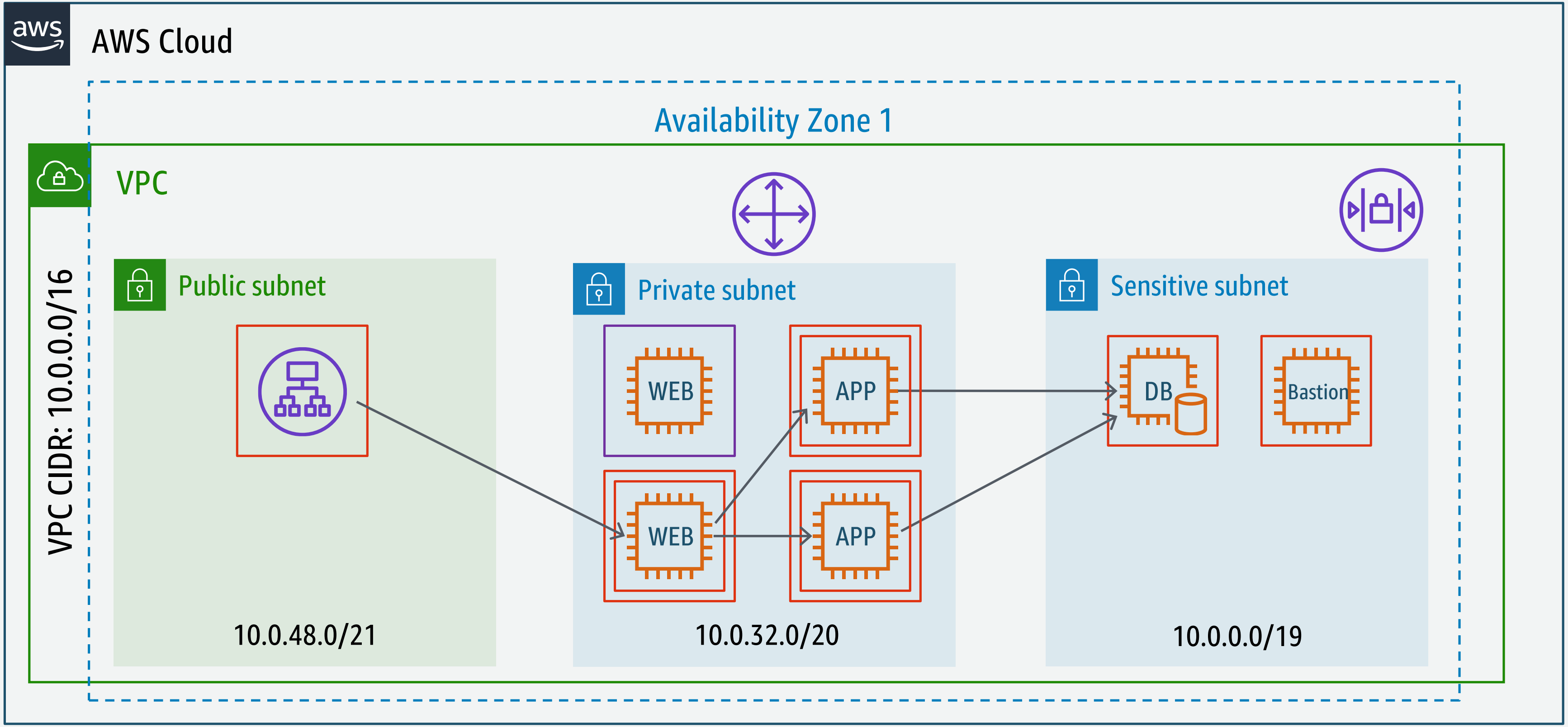
- Online analysis
- Offline analysis

You can do either or both

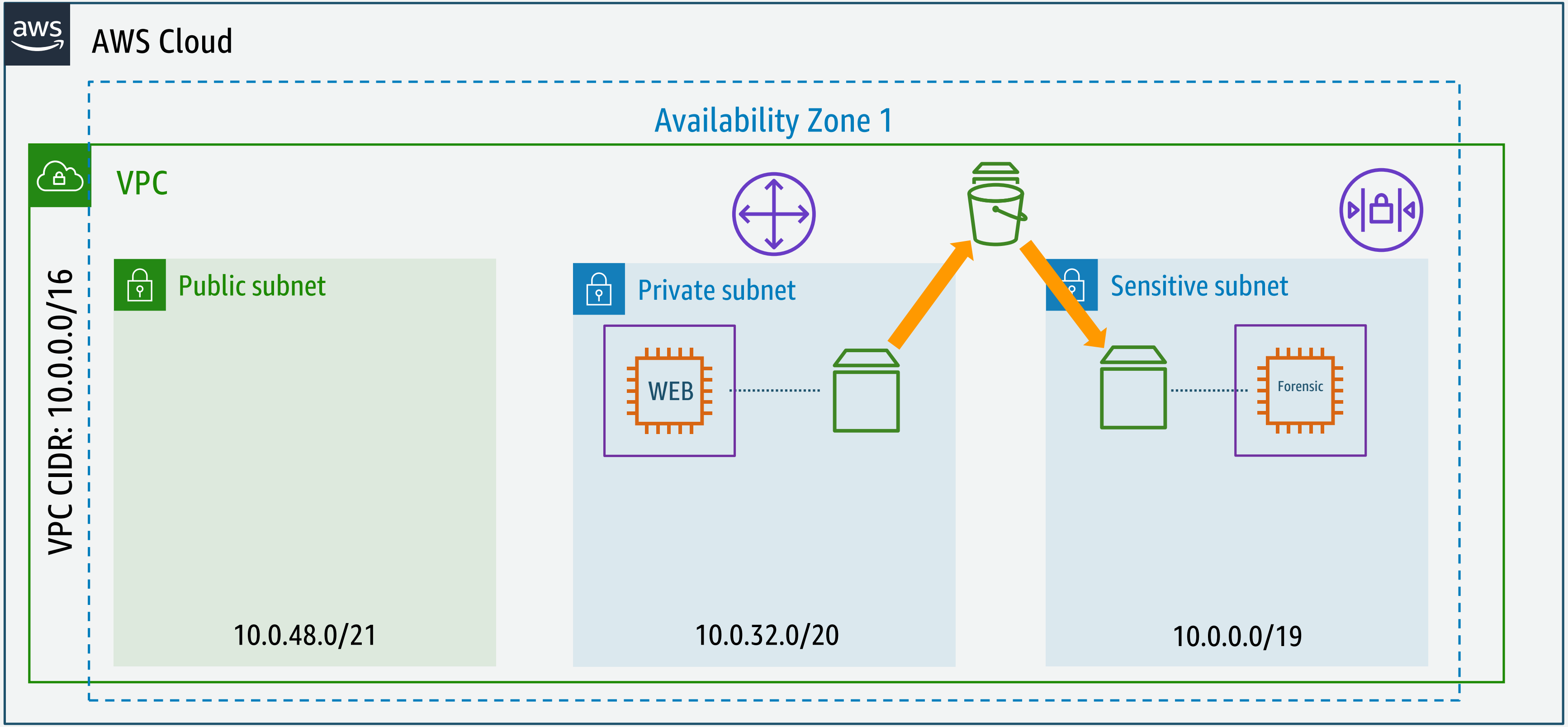
Incident Response – Offline Analysis EC2



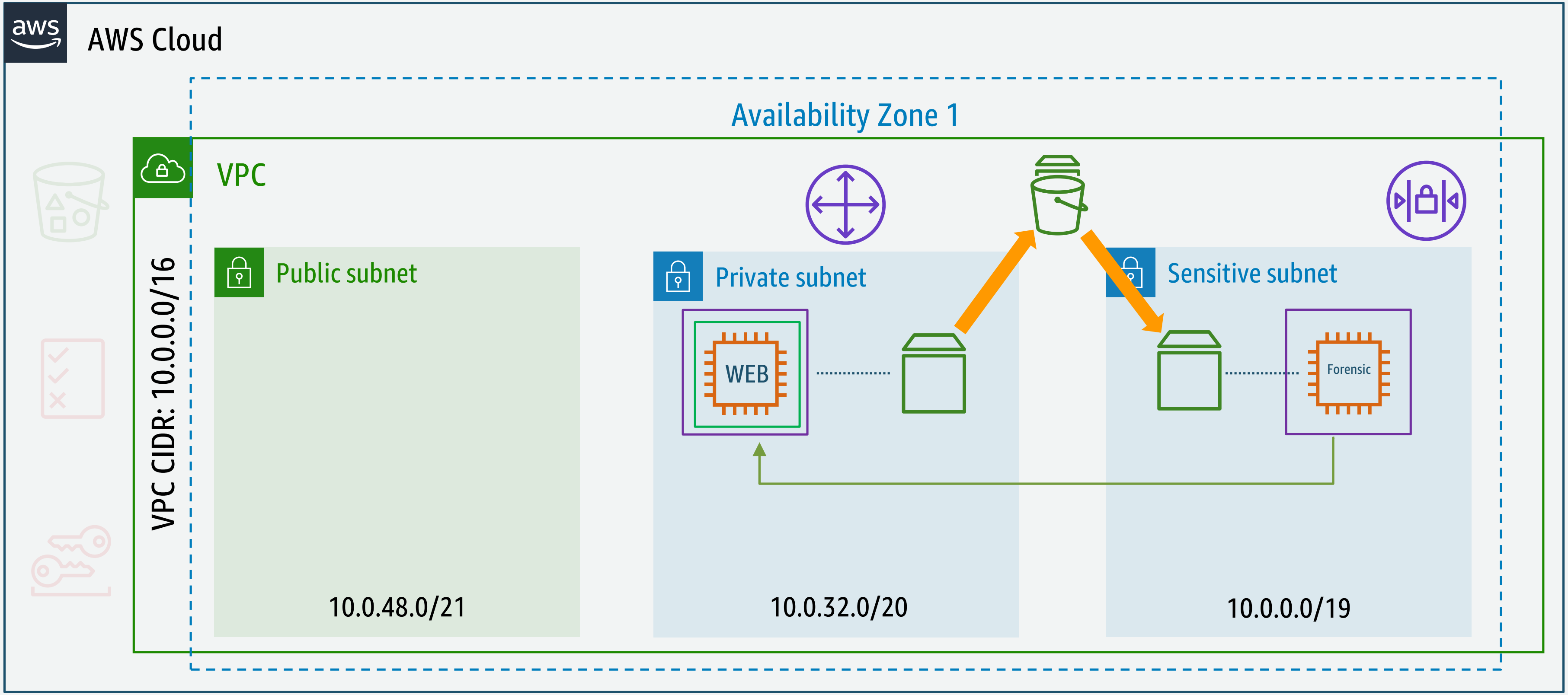
Incident Response – Offline Analysis EC2



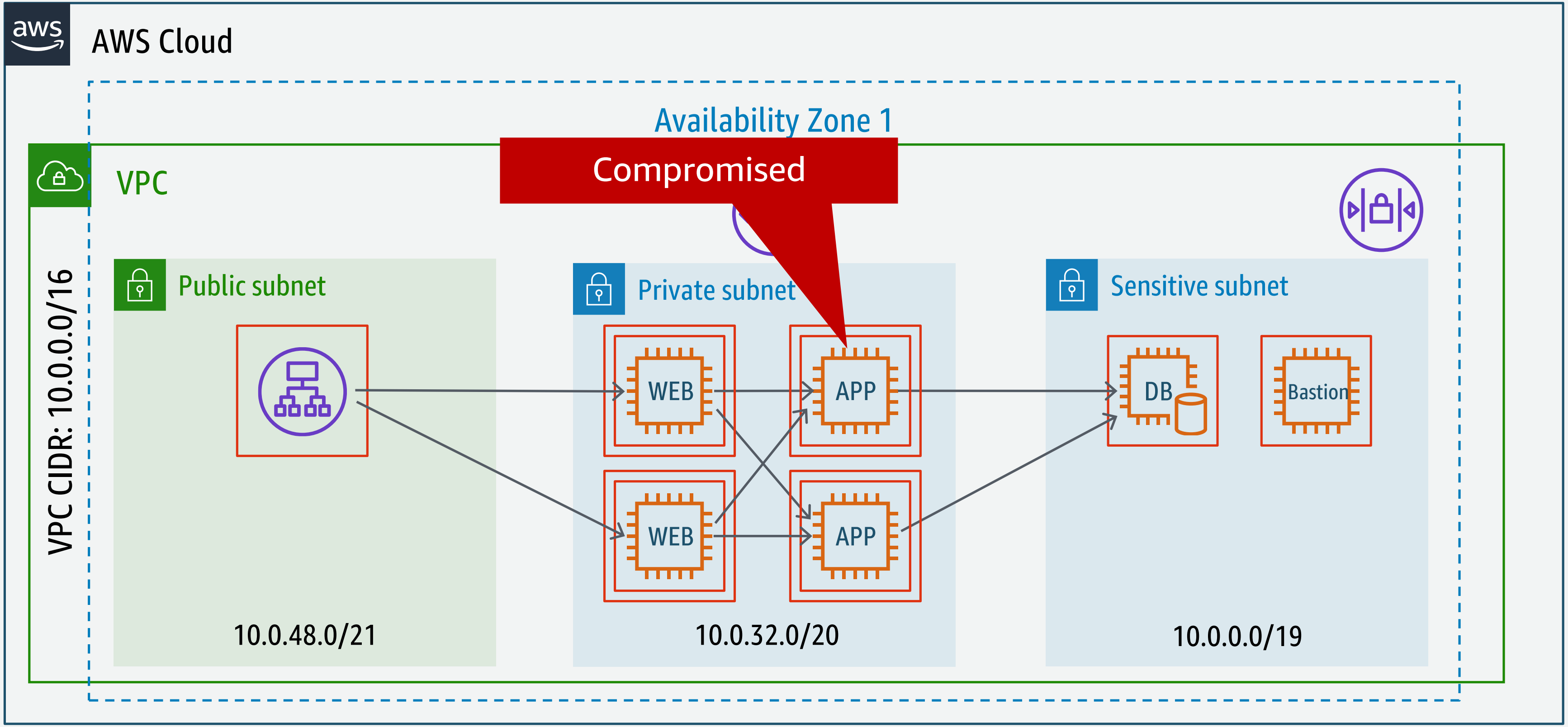
Incident Response – Offline Analysis EC2



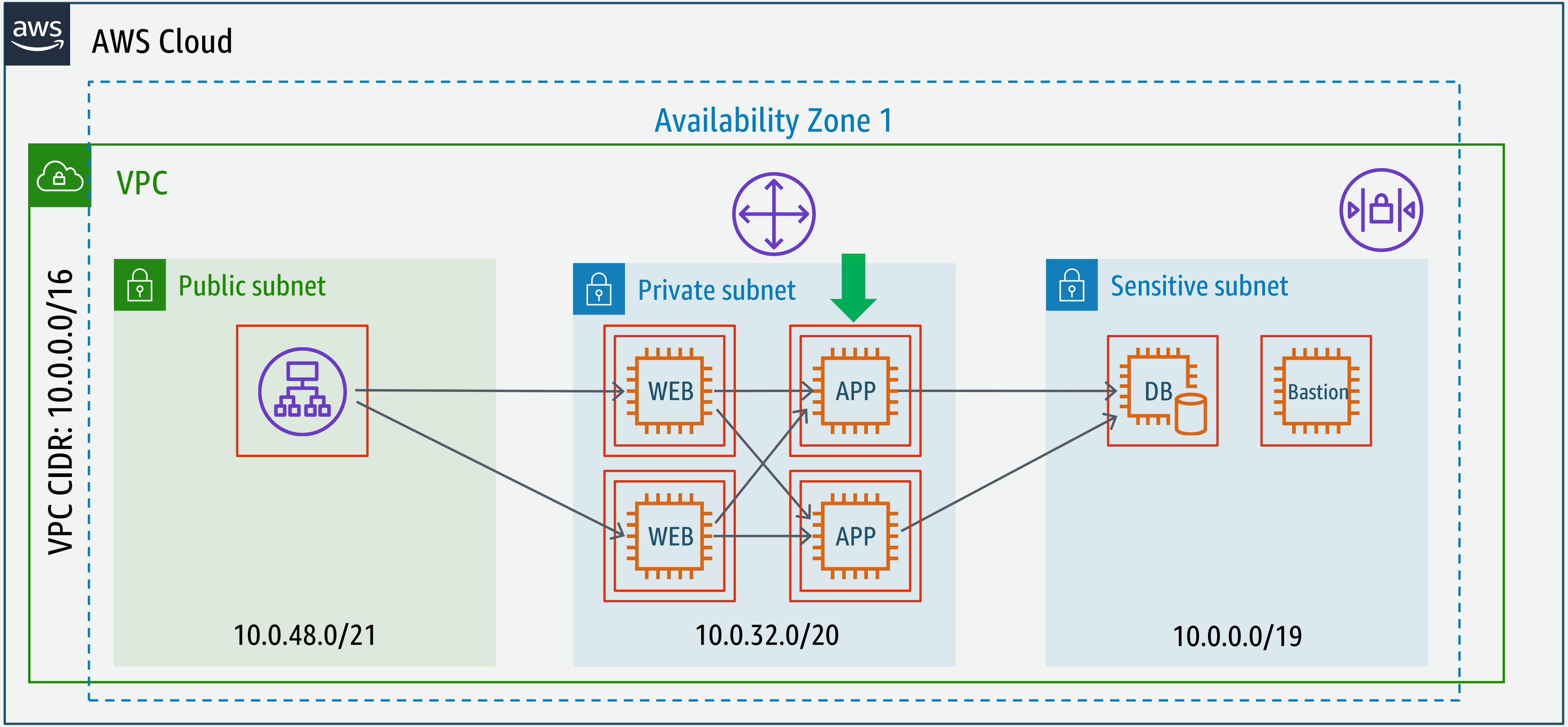
Incident Response – Offline Analysis EC2



Incident Response – Online Analysis EC2



Incident Response – Online Analysis EC2



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

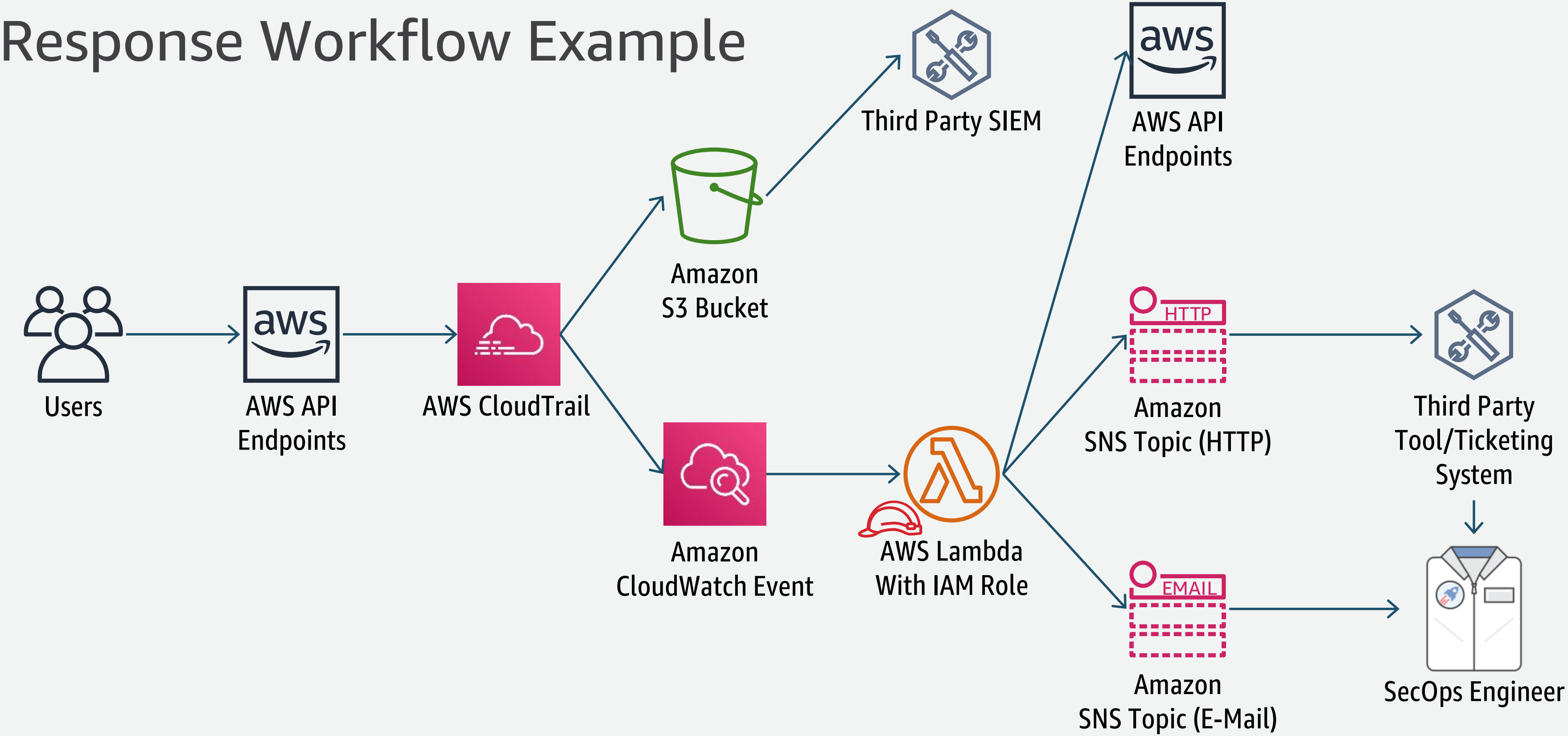
Memory Capture

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

Service Domain

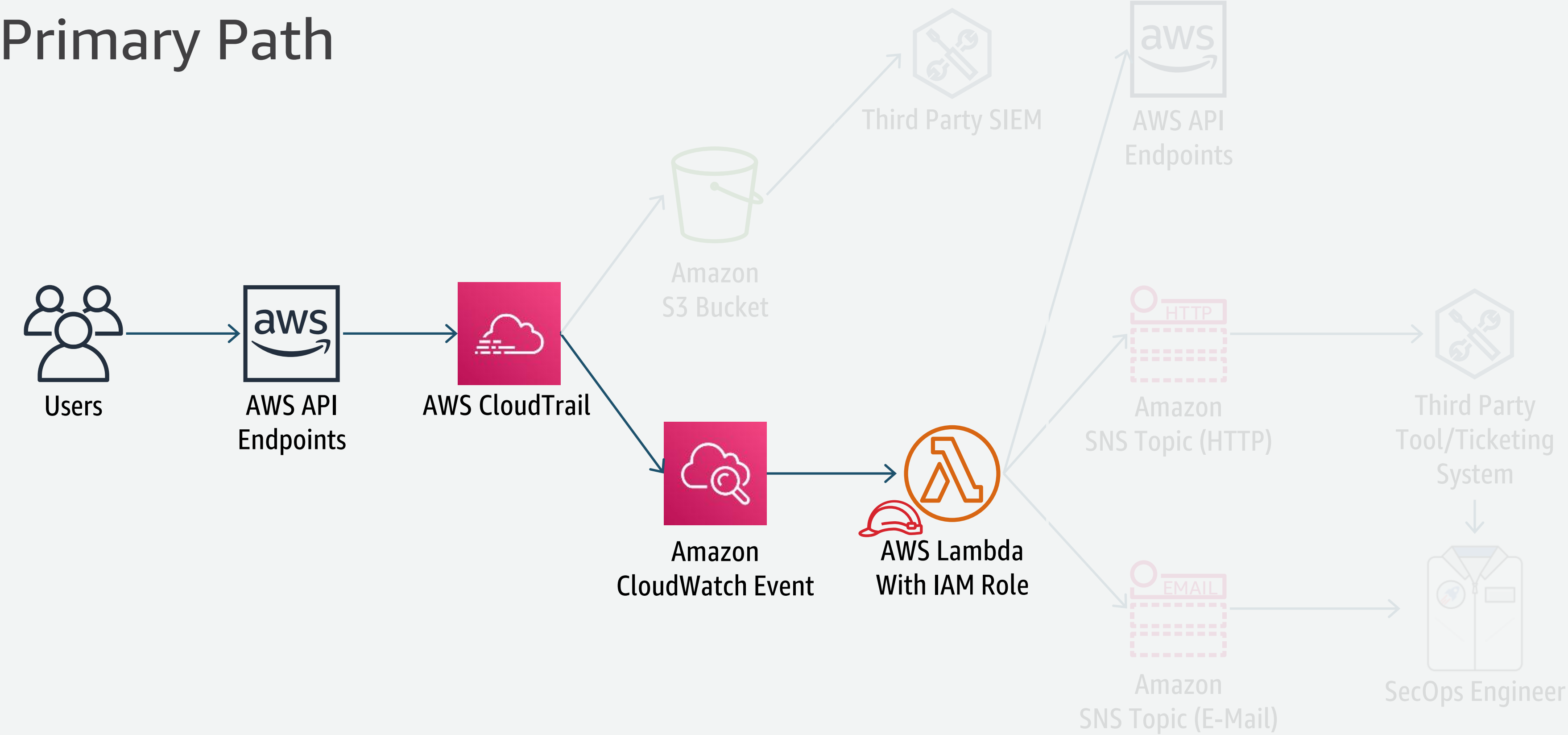
Incident Response – Service Domain

Response Workflow Example



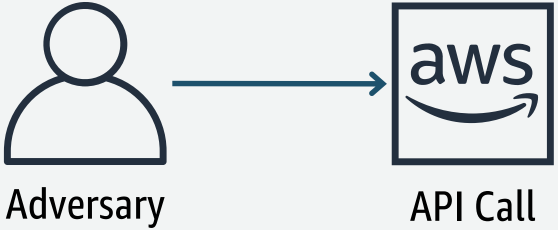
Incident Response – Service Domain

Primary Path



Incident Response – Service Domain

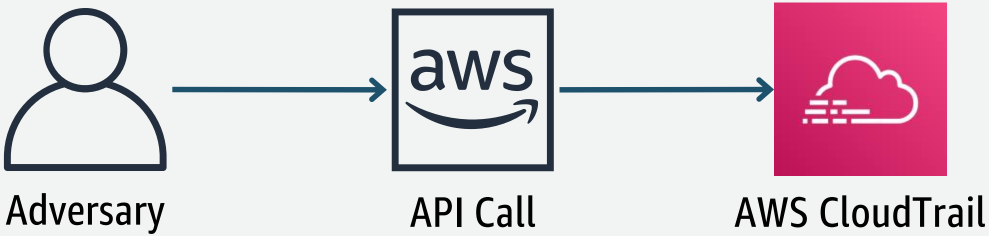
Example: CloudTrail gets turned off



```
$ aws cloudtrail stop-logging --name Trail1
```

Incident Response – Service Domain

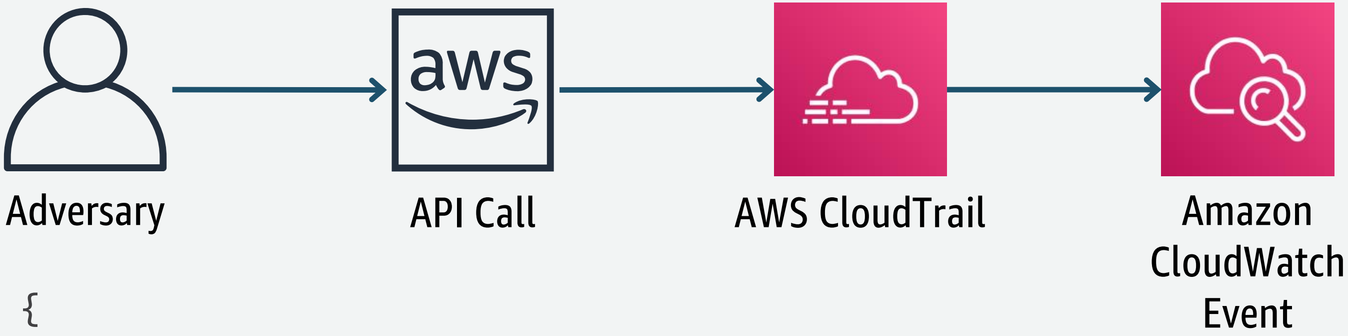
Example: CloudTrail gets turned off



```
cloudtrail:StopLogging
```

Incident Response – Service Domain

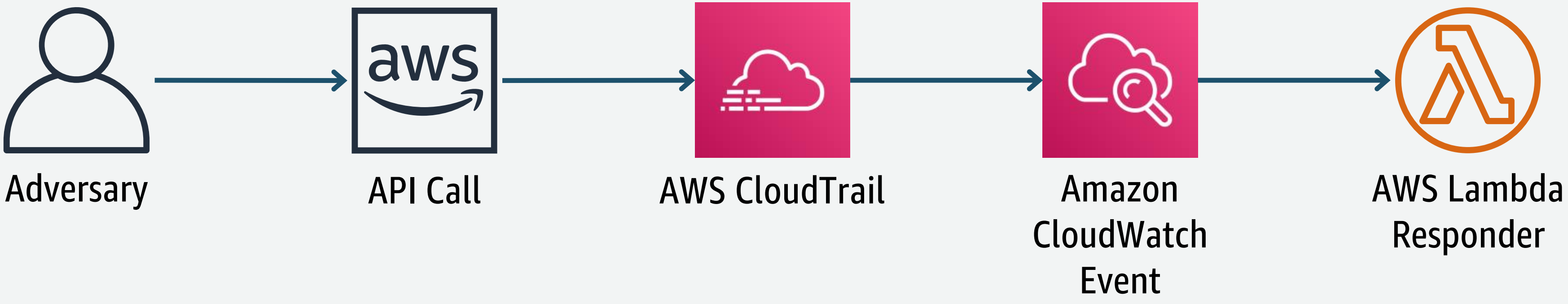
Example: CloudTrail gets turned off



```
{
    "detail-type": [ "AWS API Call via CloudTrail" ],
    "detail": {
       "eventSource": [ "cloudtrail.amazonaws.com" ],
       "eventName":   [ "StopLogging" ]
    }
}
```

Incident Response – Service Domain

Example: CloudTrail gets turned off



```
... ... ...
if "StopLogging" in event["detail"]["eventName"]:
                                ct_response = cloudtrail.start_logging(
                                    Name = trail_arn,
                                )
... ... ...
```

Incident Response – AWS Security Partner Solutions

ARMOR™

ALIEN VAULT

threat stack

SecureWorks®

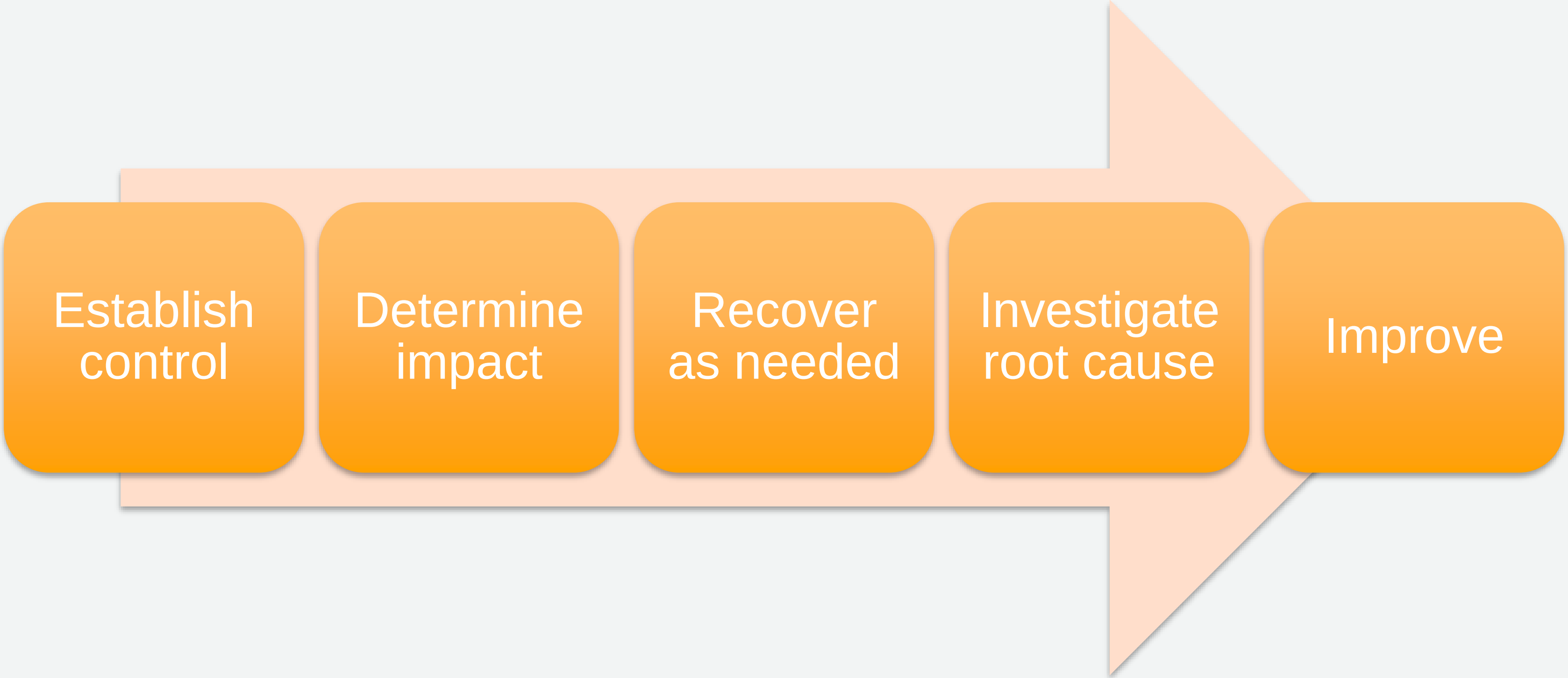
splunk>®

ALERT LOGIC®

sumologic

Incident Management

Incident Management - Lifecycle



Incident Management - AWS Support Escalation Path

In situations where an escalation is required, customers can follow a pre-defined escalation path:

- Submit a Support Case
- Technical Account Manager
- On-call Operation Manager
- Global Enterprise Support Manager
- Director of Support Engineering
- VP of AWS Support

Incident Management – IR Principles

- Establish Goals
- Respond using the cloud
- Know what you have and what you need
- Do things that scale
- Use redeployment mechanisms
- Iteratively automate the mundane
- Learn and improve your process

Security Incident Response Simulations (SIRS)

What is a SIRS?

- Security Incident Response Simulations (SIRS) are internal events that provide a structured opportunity to practice your incident response plan during a realistic scenario.
- SIRS events are fundamentally about being prepared and iteratively improving your response capabilities.

Working back from customers

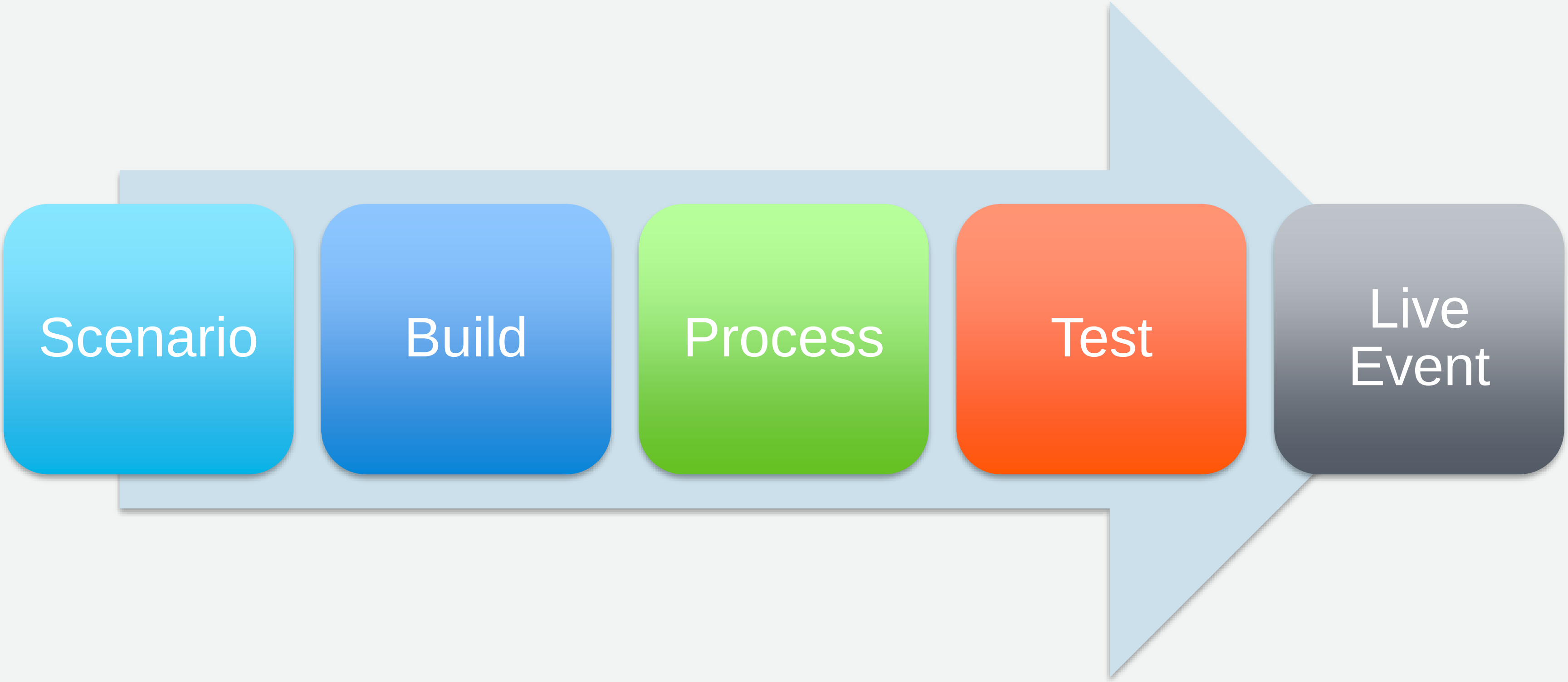
Customers voice the following reasons why they want to perform SIRS:

- **Validate readiness**
- **Develop confidence – Learn from and train staff**
- Generate artifacts for accreditation
- Be agile – Incremental improvement with laser focus
- Become faster and improve tools
- Refine escalation and communication
- Develop comfort with the rare and the creative

Preparing for a simulation

1. Find an issue of importance.
2. Find skilled security geeks.
3. Build a realistic model system.
4. Build and test the scenario elements.
5. Invite other security geeks and real people.
6. Run the simulation live.
7. Get better and repeat.

Key Simulation Elements



Scenario

Build

Process

Test

Live Event

When should I contact AWS?

If you are planning SIRS:

- Obtain permission to perform penetration testing/scanning. The following services do not need prior approval:
  - Amazon EC2 instances, NAT Gateways, and Elastic Load Balancers
  - Amazon RDS
  - Amazon CloudFront
  - Amazon Aurora
  - Amazon API Gateways
  - AWS Lambda and Lambda Edge functions
  - Amazon Lightsail resources
  - Amazon Elastic Beanstalk environments
- Confirm the SIRS does not violate the AWS Acceptable Use Policy.

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

Questions?

Appendix A - Incident Response Whitepaper

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