AWS Security Best Practices

Course objectives

After completing this course, you will be able to do the following:

- Design and implement a secure network infrastructure.
- Design and implement compute security.
- Design and implement a logging solution.

Security Overview

AWS Security Best Practices

Module 1

Objectives

By the end of this module, you will be able to do the following:

- Differentiate security responsibilities according to the AWS shared responsibility model.
- Identify organizational challenges and threats.
- Describe a standards-based approach to best practices.

Agenda

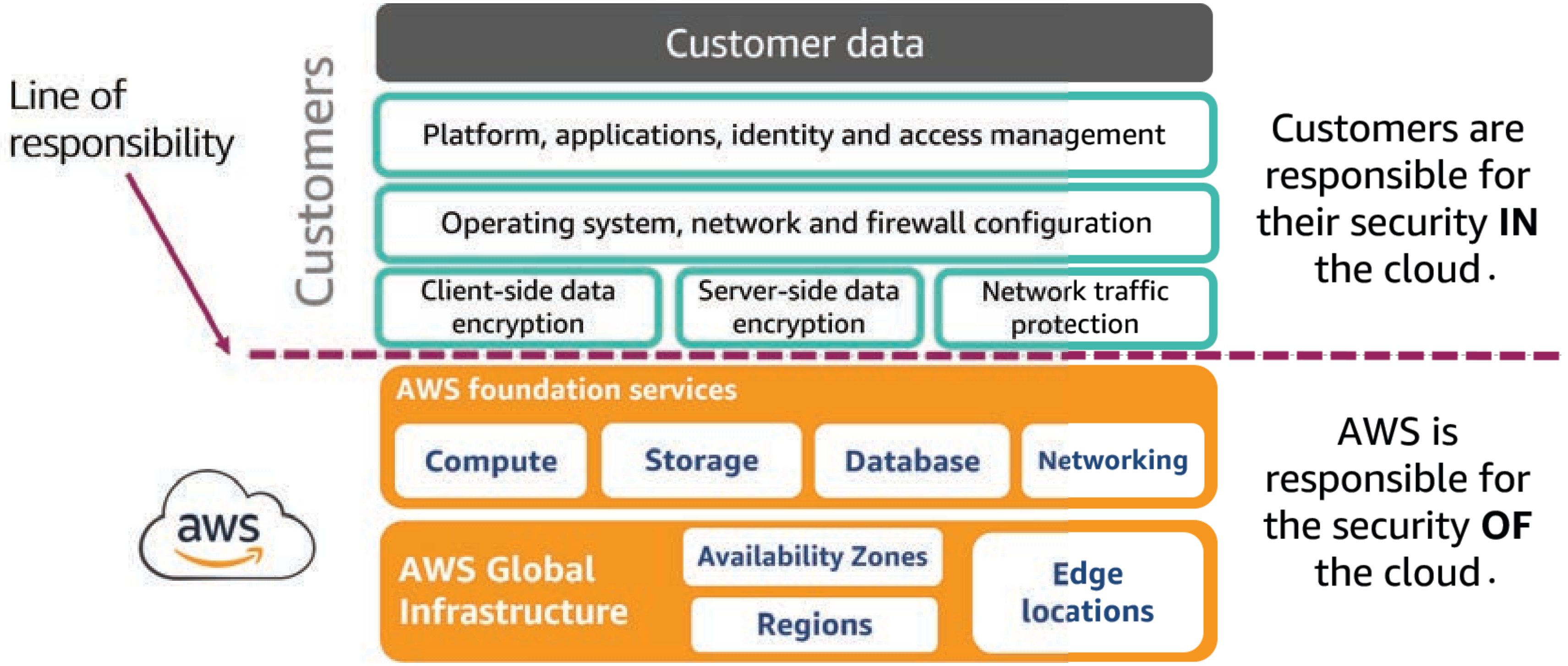
This module is organized into the following sections:

- Shared responsibility model
- Customer challenges
- Frameworks and standards
- Establishing best practices
- Compliance in AWS

Shared responsibility model

Section 1 of 5

Shared responsibility model review


Line of responsibility
Customers
Customer data
Platform, applications, identity and access management
Operating system, network and firewall configuration
Client-side data encryption
Server-side data encryption
Network traffic protection
AWS foundation services
Compute
Storage
Database
Networking
aws
AWS Global Infrastructure
Availability Zones
Regions
Edge locations

Customers are responsible for their security **IN** the cloud.

AWS is responsible for the security **OF** the cloud.

Customer challenges

Section 2 of 5

Customer challenges

To protect and safeguard data, you must consider the following:

- Technology changes in size and complexity
- Resources and workforce limitations
- Evolving threats and expanding threat surfaces
- Changes to legal and regulatory requirements

Vulnerability, threat, and risk

- A *vulnerability* is a weakness.
- A *threat* is a possibility for an event or act to exploit a vulnerability.
- A *risk* is the potential for loss, damage, or destruction of resources due to a threat.

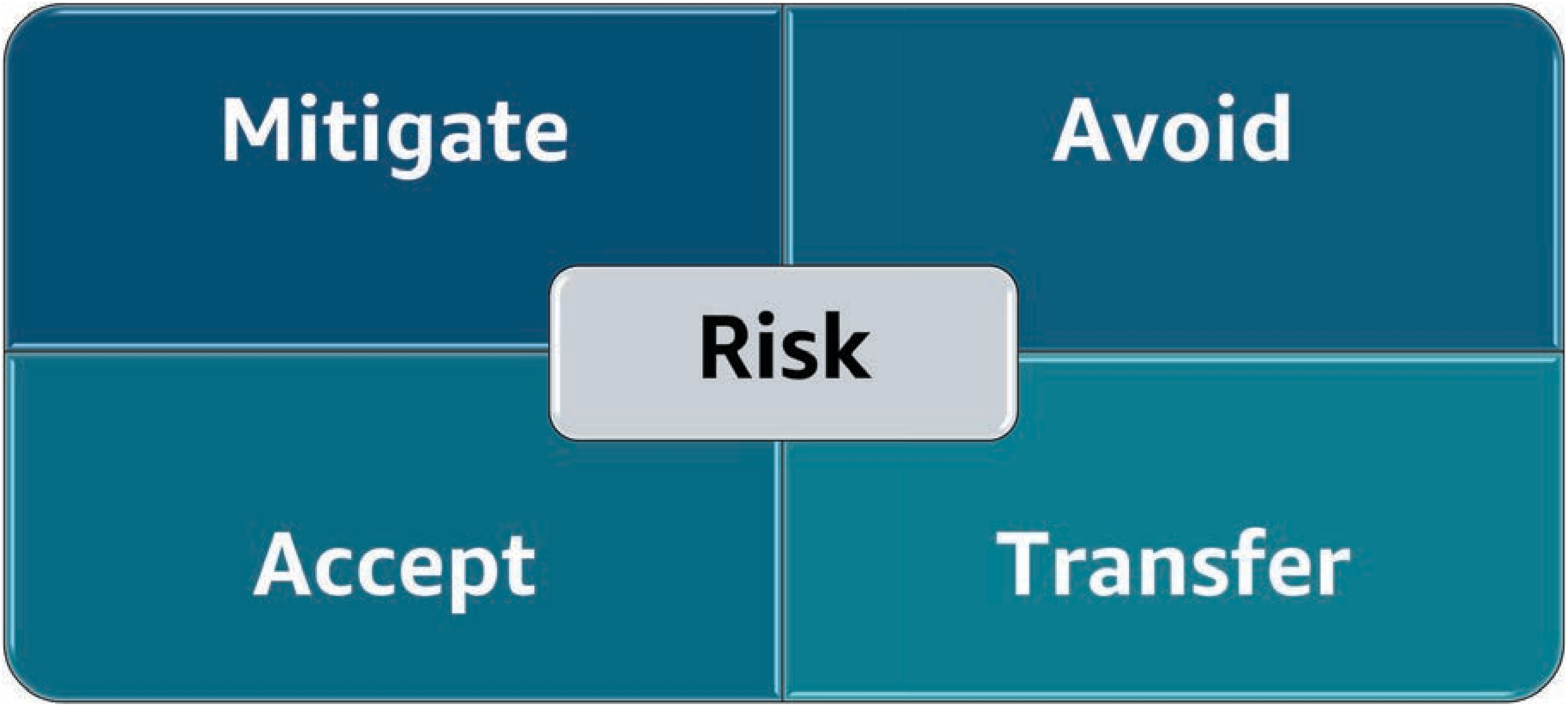
Threats in the cloud

- Denial-of-service attacks
- Malware infections
- Unauthorized access or insider threats
- Misconfigurations and poor change control

Assessing risk

- Also known as *risk analysis*
- Based on different values or judgements
- Point-in-time snapshot
- Use quantitative measurements or qualitive measurements

Addressing threats: Risk management



Mitigate

Avoid

Risk

Accept

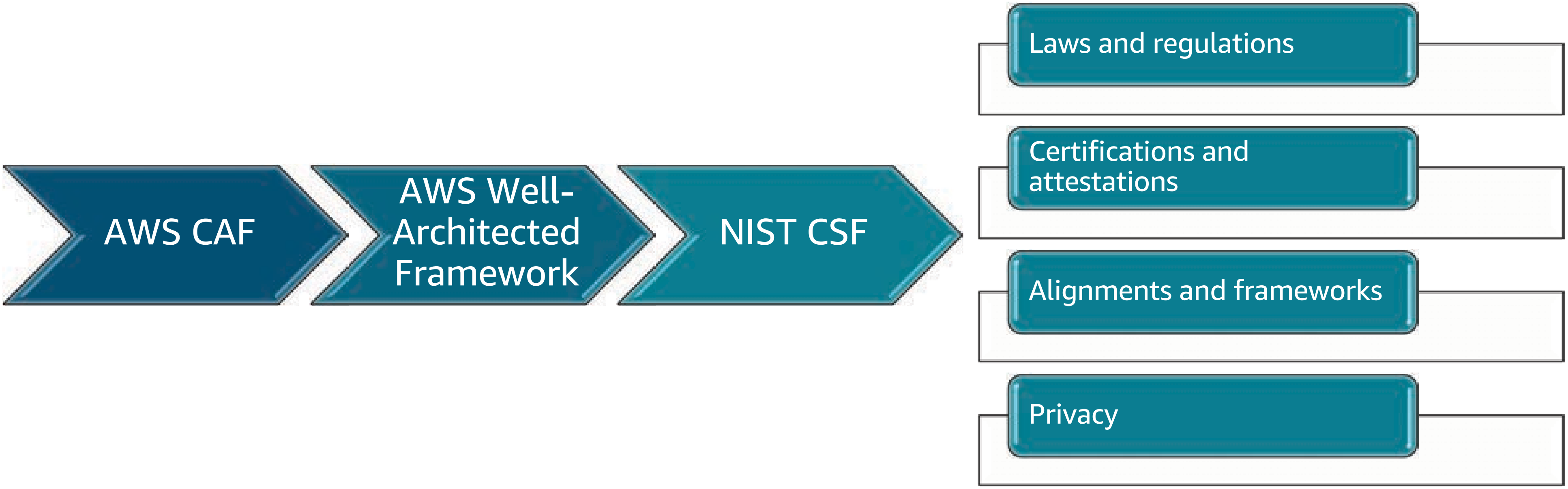
Transfer

Frameworks and standards

Section 3 of 5

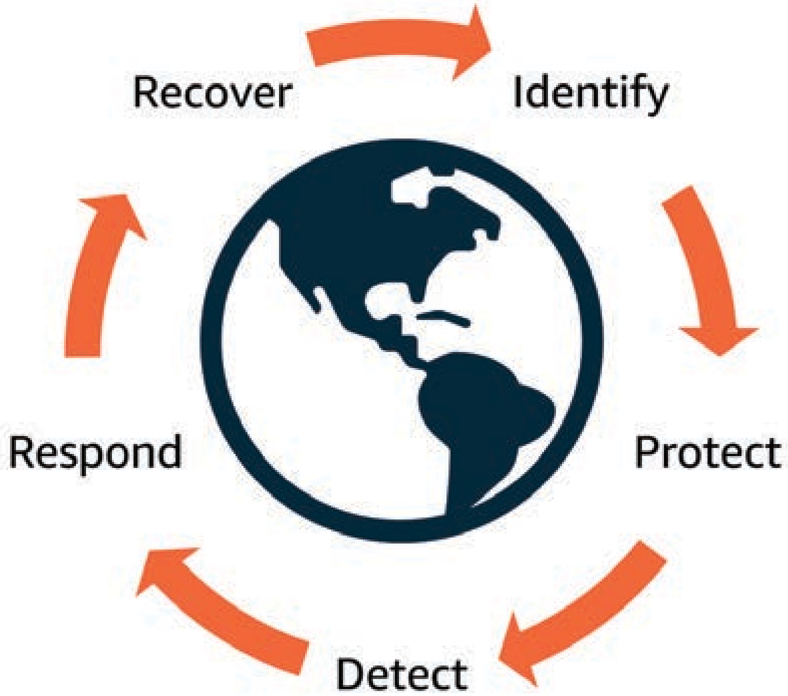
Standards-based approach

Organizations must employ effective security controls to **identify**, **protect**, **detect**, **respond**, and **recover** from destructive security events.

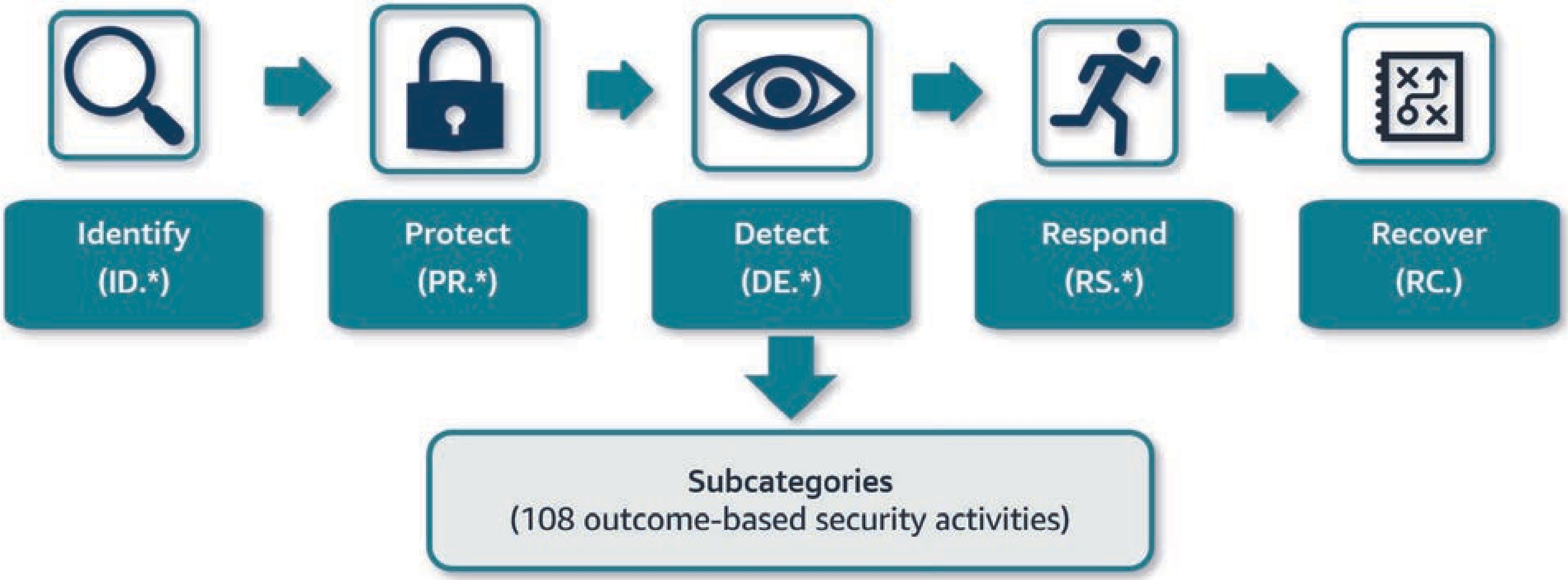

AWS CAF
AWS Well-Architected Framework
NIST CSF
Laws and regulations
Certifications and attestations
Alignments and frameworks
Privacy

Referencing NIST CSF

- The CSF is designed to be size, sector, and country agnostic.
- It references globally accepted standards, guidelines, and practices.
- Organizations across the world can use it to efficiently operate in a global environment



CSF core security functions



Identify
(ID.*)

Protect
(PR.*)

Detect
(DE.*)

Respond
(RS.*)

Recover
(RC.)

Subcategories
(108 outcome-based security activities)

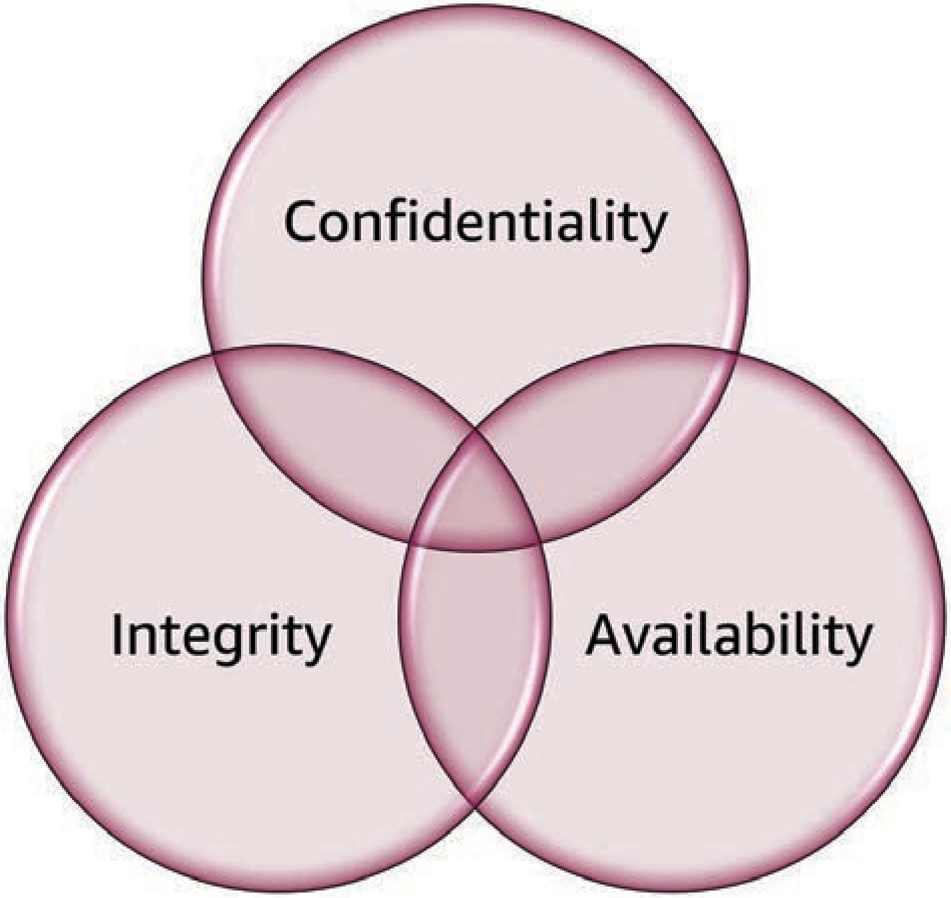
Establishing best practices

Section 4 of 5

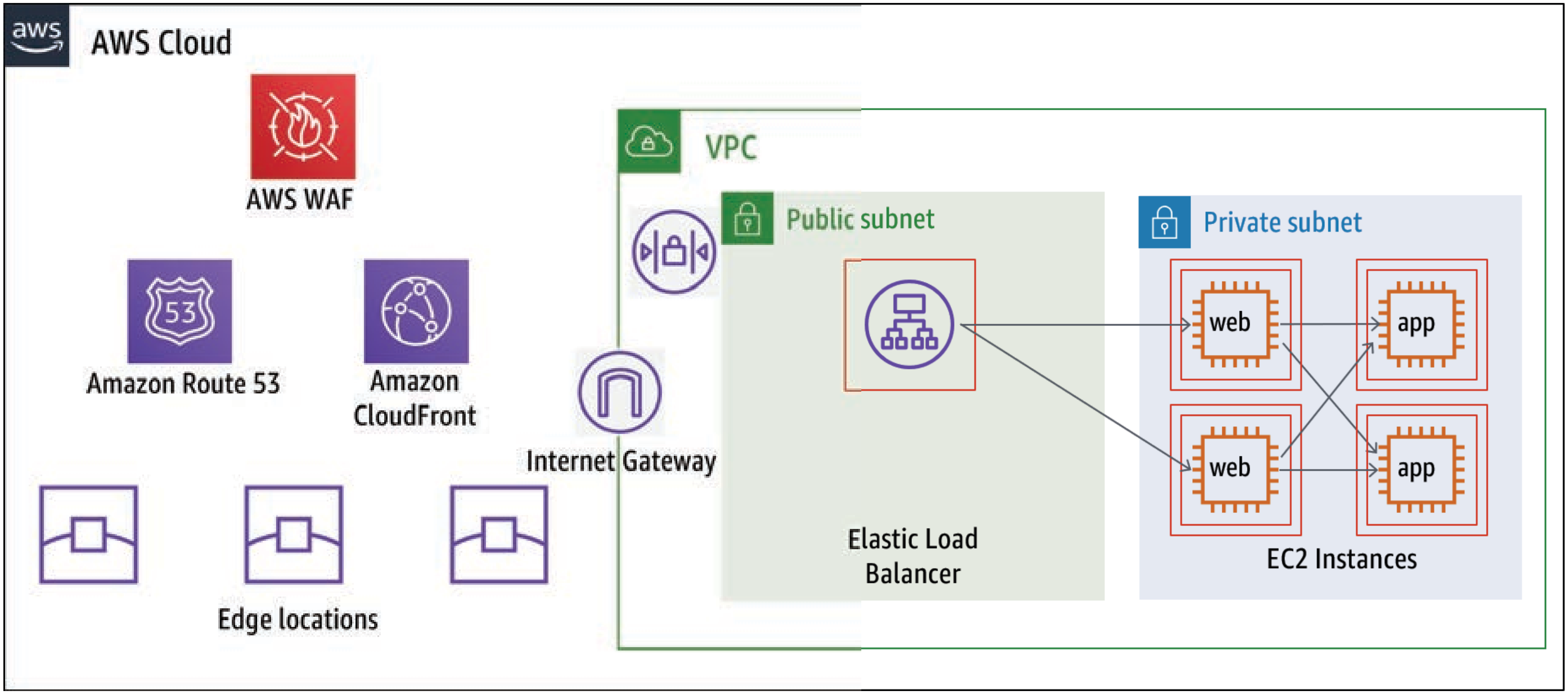
CIA triad

AWS examples:

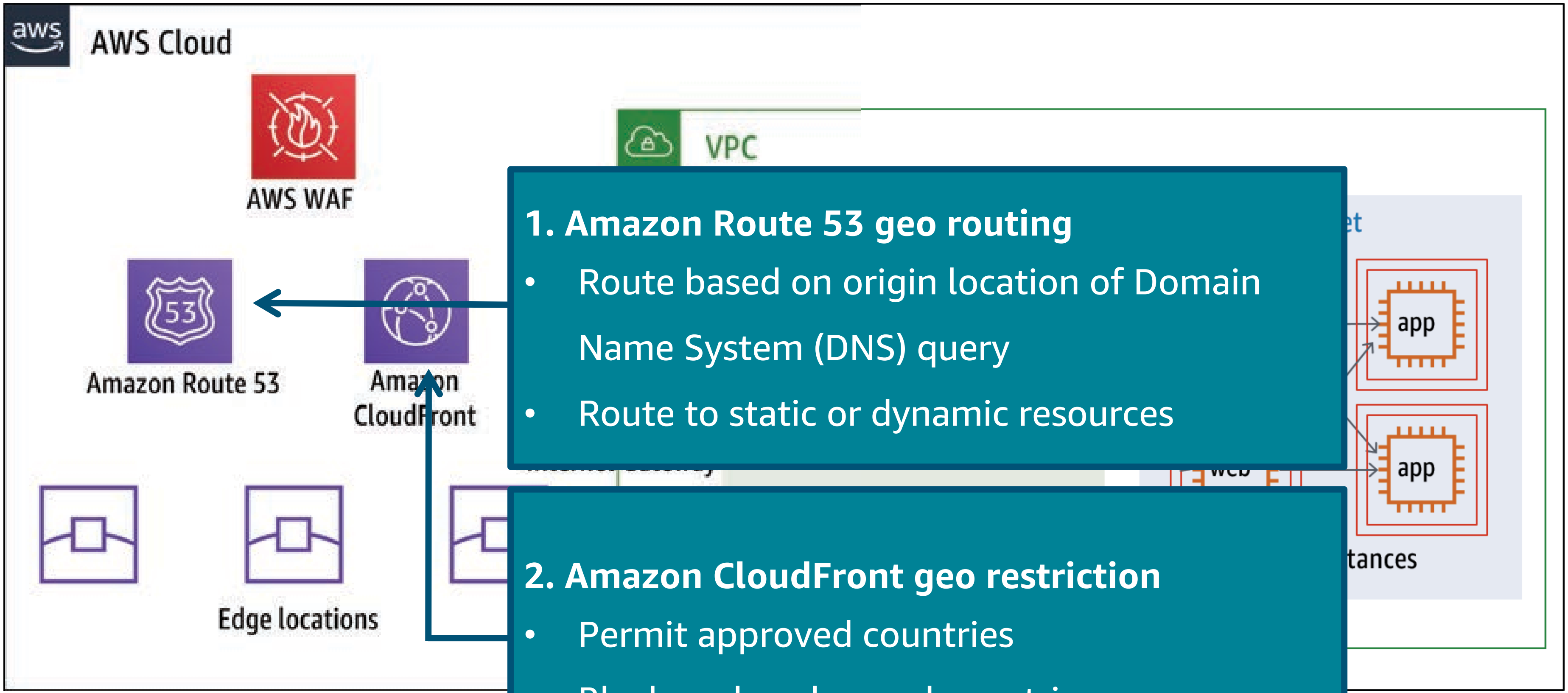
- Confidentiality: Amazon Elastic Block Storage (EBS) encryption
- Integrity: AWS CloudTrail log file validation
- Availability: Elastic Load Balancing (ELB)



Layering defense: Castle analogy



Global concerns (the moat)



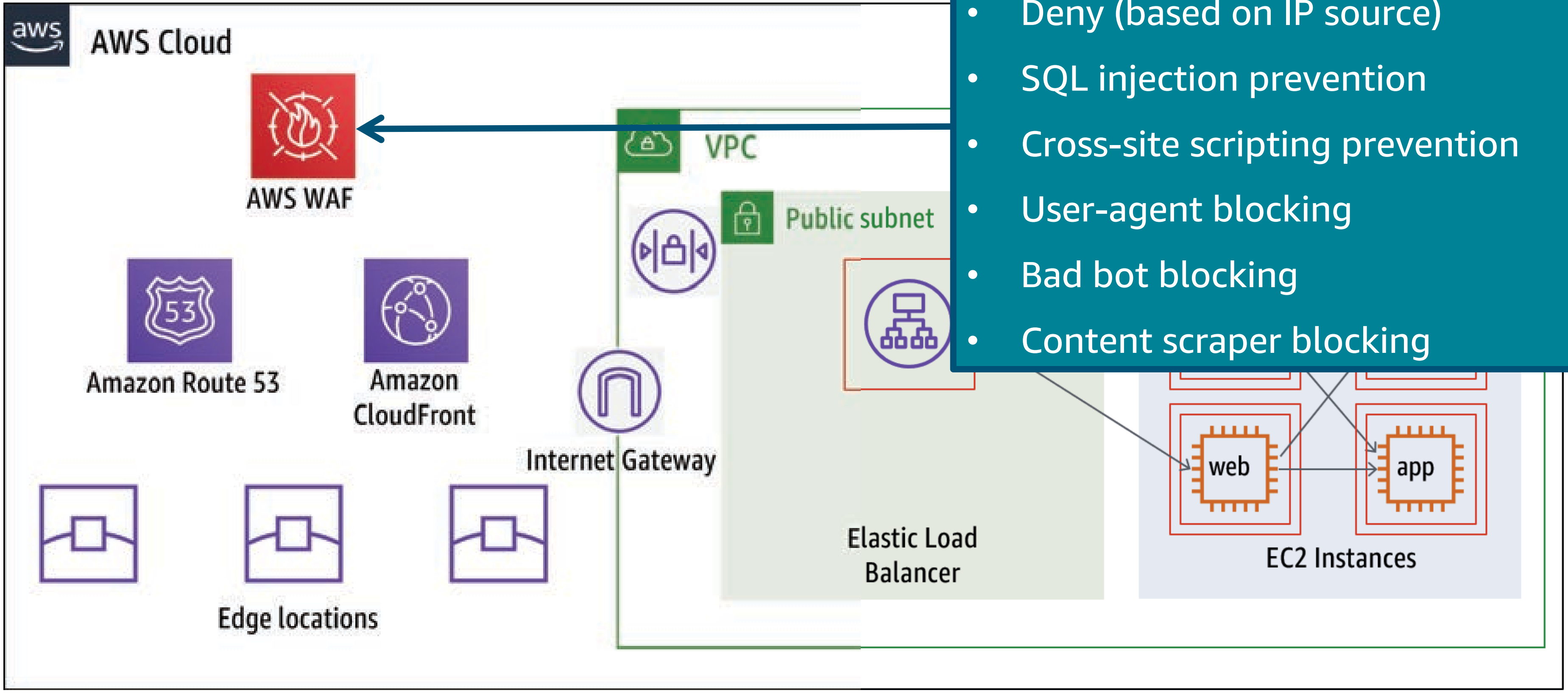
1. Amazon Route 53 geo routing

- Route based on origin location of Domain Name System (DNS) query
- Route to static or dynamic resources

2. Amazon CloudFront geo restriction

- Permit approved countries
- Block or deny banned countries

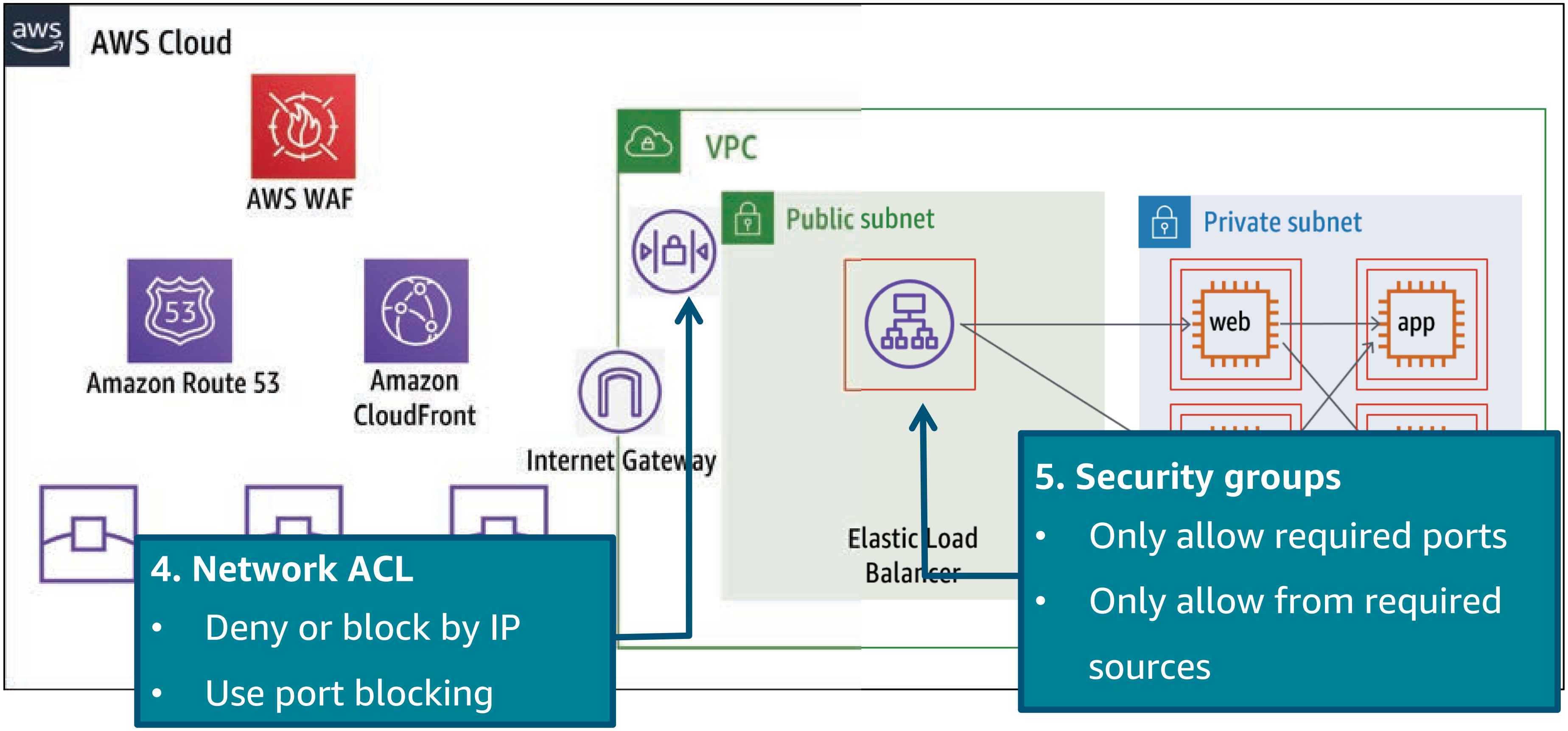
Global concerns (the outer wall)



3. AWS WAF rules

- Deny (based on IP source)
- SQL injection prevention
- Cross-site scripting prevention
- User-agent blocking
- Bad bot blocking
- Content scraper blocking

Global concerns (inside the castle)



4. Network ACL

- Deny or block by IP
- Use port blocking

5. Security groups

- Only allow required ports
- Only allow from required sources

Heterogeneous security layers

- Apply many layers of controls; target distinct layers with distinct controls.
- Diversify your signature sources and threat intelligence sources.
- Diversify technology.

Compliance in AWS

Section 5 of 5

Customer responsibilities

- Understanding what workloads must be regulated by which applicable standards
- Discovering applicable controls or checklist items that apply to workloads
- Mitigating risk and applying applicable controls
- Verifying that the applied controls are deployed and functionally tested against the workload

Compliance by region

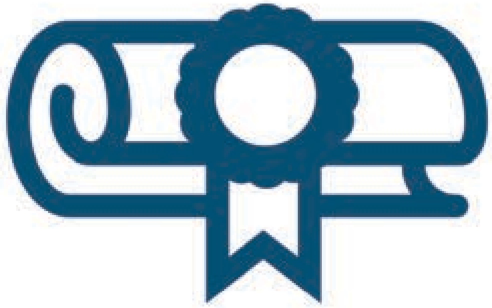
AWS is audited against a variety of global and regional security frameworks dependent on region and industry.

- Global
- US and North America
- Asia Pacific
- Europe, Middle East, and Africa

AWS compliance programs

The IT standards that AWS complies with are broken out by:

- Certifications and attestations
- Laws, regulations, and privacy
- Alignments and frameworks



AWS Artifact

- Reports on demand
- Global availability
- Straightforward identification
- Quick assessments
- Continuous monitoring
- Enhanced transparency

Module 1: Security Overview

Remember…

- The customer is responsible for everything *in* the cloud.
- Security frameworks can help:
  - AWS Well-architected Framework
  - AWS CAF
  - NIST CSF
- Defense-in-Depth is a layered approach to security.

Let’s take a look at what we will cover in the upcoming modules.

Protecting and detecting with AWS

NIST CSF Function and target	Module
Protect network infrastructure	Module 2 (Securing the network) explores best practices for protecting the network from threats.
Protect compute resources	Module 3 (Amazon EC2 Security) explores best practices for protecting your Amazon EC2 instances from threats.
Detect security events	Module 4 (Monitoring and alerting) explores best practices for detecting threats through monitoring and alerting in your AWS environment.

Additional resources

Finding resources

- AWS Marketplace
- AWS security bulletins
- AWS security documentation
- AWS Trusted Advisor

Securing the Network

AWS Security Best Practices

Module 2

Objectives

By the end of this module, you will be able to:

- Design a network for flexibility and security.
- Implement network security by controlling traffic at all layers and automating network protection.
- Select AWS services to secure network traffic and combat common security threats.
- Understand the benefits of third-party solutions offered through AWS Marketplace.

Agenda

This module is organized into the following sections:

- Flexible and secure
- Security inside the VPC
- Security services
- Third-party security solutions

Flexible and secure

Section 1 of 4

Starting with the Virtual Private Cloud (VPC)

Network architecture is your foundation.

A sound strategy for designing, building, and maintaining the network architecture provides the best foundation for scaling and security.

- A good design builds in security.
- Customers have full control over their VPC.
- Stakeholder input helps develop the strategy.

Security inside your VPC

Best practices

- Use subnets to isolate the tiers of your application (for example, web, application, and database) within a single VPC.
- Avoid opening Secure Shell (SSH) or Remote Desktop Protocol (RDP) between or within instances of the production environment whenever possible.

Designing a network

Monitor at boundaries

Subnet to create isolation

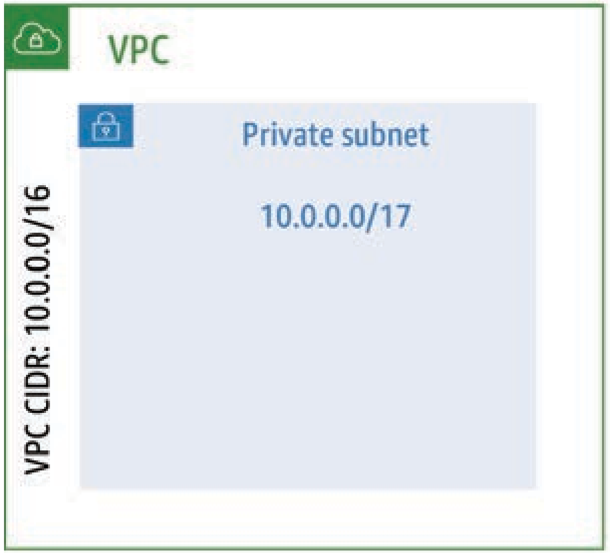
Connect externally
through protective devices

Network segmentation

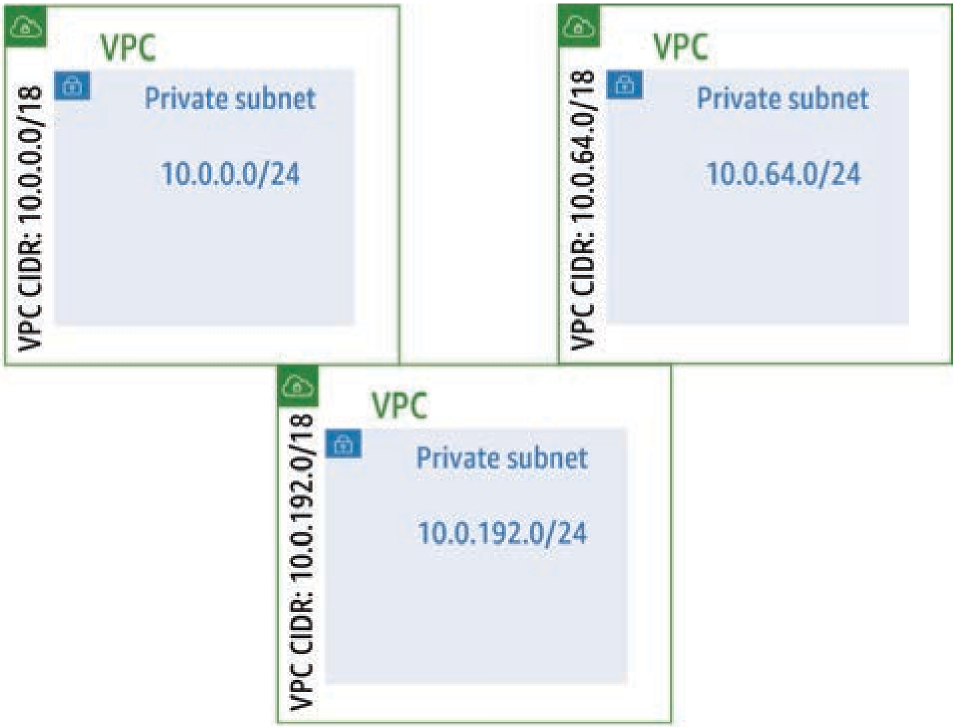
Advantages of using subnets for network segmentation include the following:

- Limiting the spread and damage of potential attacks by creating smaller impact areas
- Improving visibility and control over traffic movement, device access, and external access
- Reducing the scope when auditing for specific requirements

VPC and subnet strategy



Large VPC and subnets



Small VPC and subnets

Design best practices

- Inside the VPC:
  - Plan for unique CIDR for each VPC.
  - Use RFC 1918 addressing (class A/B/C).
  - Plan for growth and reserve spare IP ranges.

- Inside the Availability Zone:
  - Use role-based addressing schemes.
  - Implement Route summarization.
  - Use separate route tables (based on subnet or security segments).

DNS operations and security

Amazon Route 53 using DNSSEC

- Domain Name Security Extensions (DNSSEC) helps prevent DNS attacks like DNS cache poisoning and DNS spoofing.

Store private keys in AWS KMS

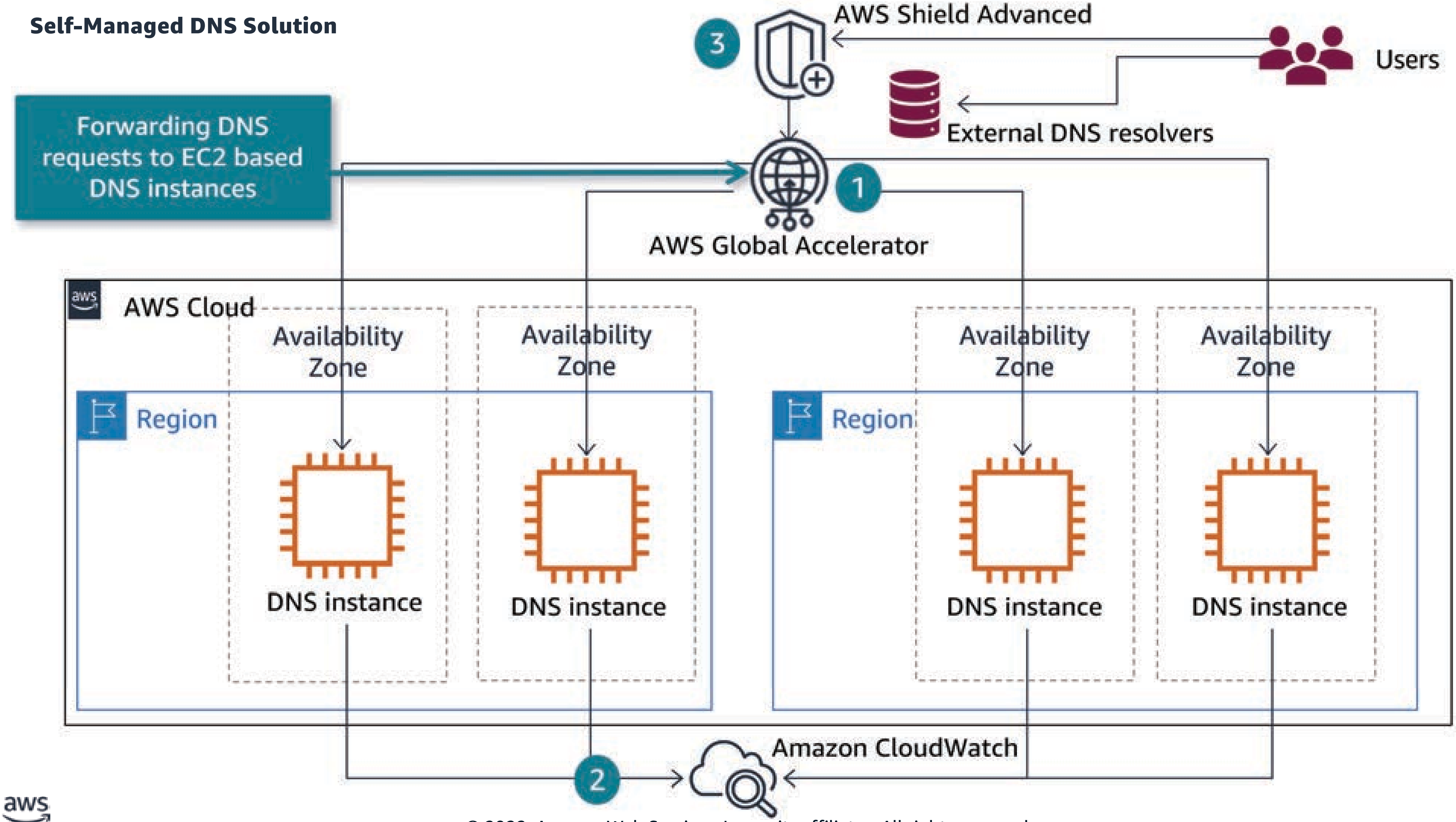
Sign public hosted zones or use DNSSEC validation

Use a single key across multiple public hosted zones

Route 53 Resolver DNS Firewall

- Define domain name filtering rules to control access to sites and block DNS-level threats
- Customize the responses for blocked DNS queries
- Filter on a domain names only (not an IP address)
- Filters User Datagram Protocol DNS traffic (not HTTPS, TLS, SSH or, other protocols)
- Centralize management with AWS Firewall Manager

Self-Managed DNS Solution



Security inside the VPC

Section 2 of 4

Overall network security guidance

Best practices

- Layer security groups and network ACLs together.
- Use multiple Availability Zone deployments and Elastic Load Balancing (ELB) for high availability.
- Use out-of-band management whenever possible.
- Use Amazon CloudWatch to monitor your VPC components *(covered in module 4).*
- Use flow logs to capture information about traffic in your VPC *(covered in module 4).*
- Always use Identity and Access Management (IAM) to limit access to your resources, including the VPC and related components.

Network filtering methods

Stateless

- Focus on the content of individual packets
- Generally use information from headers (IP source or destination, protocol, and so on) for filtering
- Generally fast and has no issue with heavy traffic loads
- Includes network access control lists

Stateful

- Track and filter all traffic that is part of a stateful associated (for example in the same TCP session)
- Can identify TCP connection stages, packet state, and other key statuses
- Includes security groups and firewalls

Network ACL review

- Provide stateless filtering for subnets
- Apply to one or more subnets
- Sequentially process rules
- Specify a traffic source with inbound rules
- Specify a destination with outbound rules
- Create rules using increments

Default mode: **explicit deny** and **implicit allow**

Using Network ACLs in your VPC

Best practices

- Remember the default network ACL.
- Monitor and audit network ACLs for ineffective “deny” rules.
- Consider limitations.
- Do not ignore outbound rules on network ACLs.

Test yourself: inbound access

Requirements:

- The DNS queries, HTTPS and SMTP traffic sourced from your on-premises network 192.0.2.0/28 are **allowed** to reach subnet A in your VPC.
- All other inbound traffic should be denied.

Rule #	Type	Protocol	Port range / ICMP Type	Source	Allow / Deny
10	UDP	ALL	ALL	192.0.2.0/28	ALLOW
20	TCP	HTTPS	443	10.0.0.0/17	ALLOW
30	TCP	SMTP	25	10.0.0.0/17	ALLOW
*	All IPv4 Traffic	ALL	ALL	0.0.0.0/0	DENY

How can you fix this network ACL?

- VPC subnet A—10.0.0.0/17
- VPC subnet B—10.0.128.0/17
- On-premises network: 192.0.2.0/28

Solution: source address misconfiguration

In this scenario, the network ACL is inbound, meaning that the source of traffic is outside the subnet.

- Rules 20 and 30 have the correct protocol, port number, and action, but their source network was mistakenly set to 10.0.0.0/17. This is the *destination* for traffic inbound to the subnet; the source in the on-premise network at 192.0.2.0/28.

Rule #	Type	Protocol	Port range / ICMP Type	Source	Allow / Deny
10	UDP	ALL	ALL	192.0.2.0/28	ALLOW
20	TCP	HTTPS	443	192.0.2.0/28	ALLOW
30	TCP	SMTP	25	192.0.2.0/28	ALLOW
*	All IPv4 Traffic	ALL	ALL	0.0.0.0/0	DENY

Test Yourself: outbound access

Requirements:

- SSH and RDP traffic sourced from your VPC must be **DENIED** to the on-premises network of 192.0.2.0/24.
- All other traffic from your VPC should be permitted through.

Rule #	Type	Protocol	Port range / ICMP Type	Destination	Allow / Deny
10	All IPv4 Traffic	ALL	ALL	192.0.2.0/28	ALLOW
20	TCP	RDP	3389	192.0.2.0/28	DENY
30	TCP	SSH	22	192.0.2.0/28	DENY
*	All IPv4 Traffic	ALL	ALL	0.0.0.0/0	DENY

How can you fix this network ACL?

- VPC subnet A—10.0.0.0/17
- VPC subnet B—10.0.128.0/17
- On-premises network: 192.0.2.0/28

Solution: rule order and processing

In this scenario, the first rule (10) allows all traffic, on all ports and protocols from your VPC outbound to the on-premise network. All traffic (including RDP and SSH) will match the first rule here, so rules 20 and 30 will not be processed and have no effect.

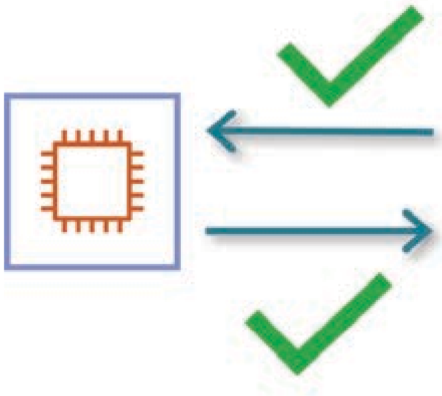
- You must first deny the specific traffic types you want to stop from reaching the on-premise network before allowing all other traffic.

Rule #	Type	Protocol	Port range / ICMP Type	Destination	Allow / Deny
~~10~~	~~All IPv4 Traffic~~	~~ALL~~	~~ALL~~	~~0.0.0.0/0~~	~~ALLOW~~
20	TCP	RDP	3389	192.0.2.0/28	DENY
30	TCP	SSH	22	192.0.2.0/28	DENY
40	All IPv4 Traffic	ALL	ALL	192.0.2.0/28	ALLOW
*	All IPv4 Traffic	ALL	ALL	0.0.0.0/0	DENY

Security group review

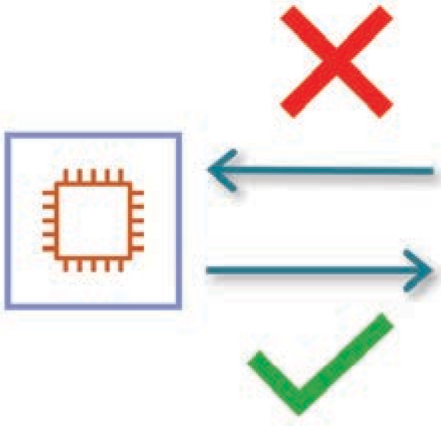
Default security group

- Permits all inbound traffic from members of the same security group (rule present)
- Permits all outbound traffic (rule present)



Custom security group

- Permits no inbound traffic (no rule present)
- Permits all outbound traffic (rule present)



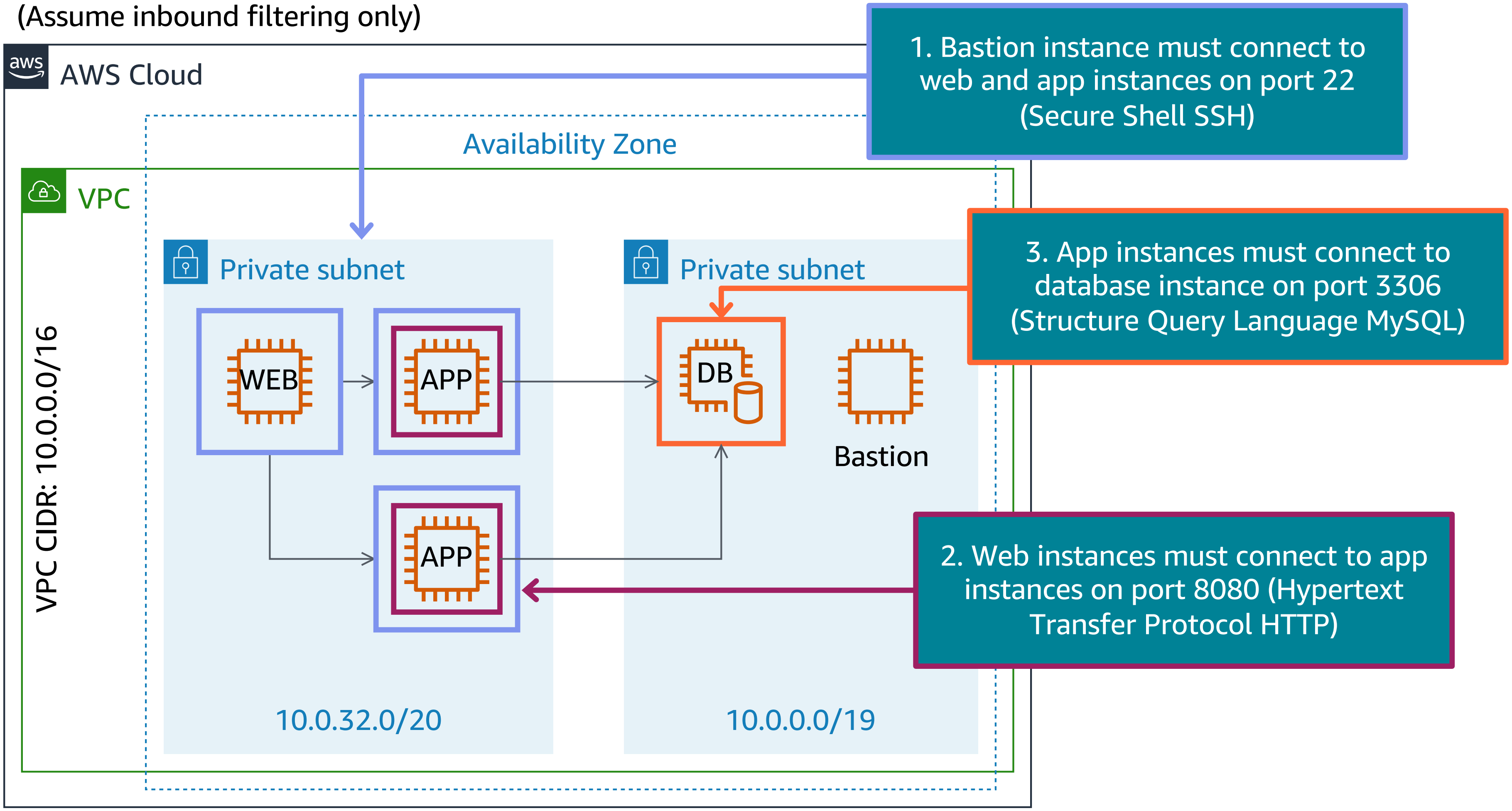
Using security groups in your VPC

Best practices

- Never keep unattached security groups.
- Track rate of change in production environments.
- Ensure that security groups do not have a large range of ports open.
- Use elastic load balancers with security groups to restrict access to the internet.
- Limit modifications to only certain IAM roles.
- Do not ignore outbound rules of security groups.

Layering security groups: example topology

(Assume inbound filtering only)



1. Bastion instance must connect to web and app instances on port 22 (Secure Shell SSH)

2. Web instances must connect to app instances on port 8080 (Hypertext Transfer Protocol HTTP)

3. App instances must connect to database instance on port 3306 (Structure Query Language MySQL)

Service highlight: AWS Network Firewall

AWS Network Firewall is a managed network protection service that provides the following:

- Stateful firewall
- Web filtering
- Intrusion protection
- Central management and visibility
- Rule management and customization
- Partner integrations

Building for availability

Availability is an important part of the C-I-A triad.

Global availability

Regions
Coming Soon

Regions and Availability Zones

- AWS Global Infrastructure spans 84 Availability Zones within 26 geographic regions around the world.
- Announced Regions include the following:
  - Australia, India, Indonesia, Israel, New Zealand, Spain, Switzerland, and United Arab Emirates (UAE)

VPC and AZ availability

Elastic Load Balancing (ELB)

- ELB distributes traffic over a group of resources in one or more Availability Zone.
- Deploy ELB with AWS Application Auto Scaling, AWS Auto Scaling, or Amazon EC2 Auto Scaling.
- Choose the type of load balancing device you need.
- **(Best practice)** Use security groups to protect ELB.

Management traffic best practices

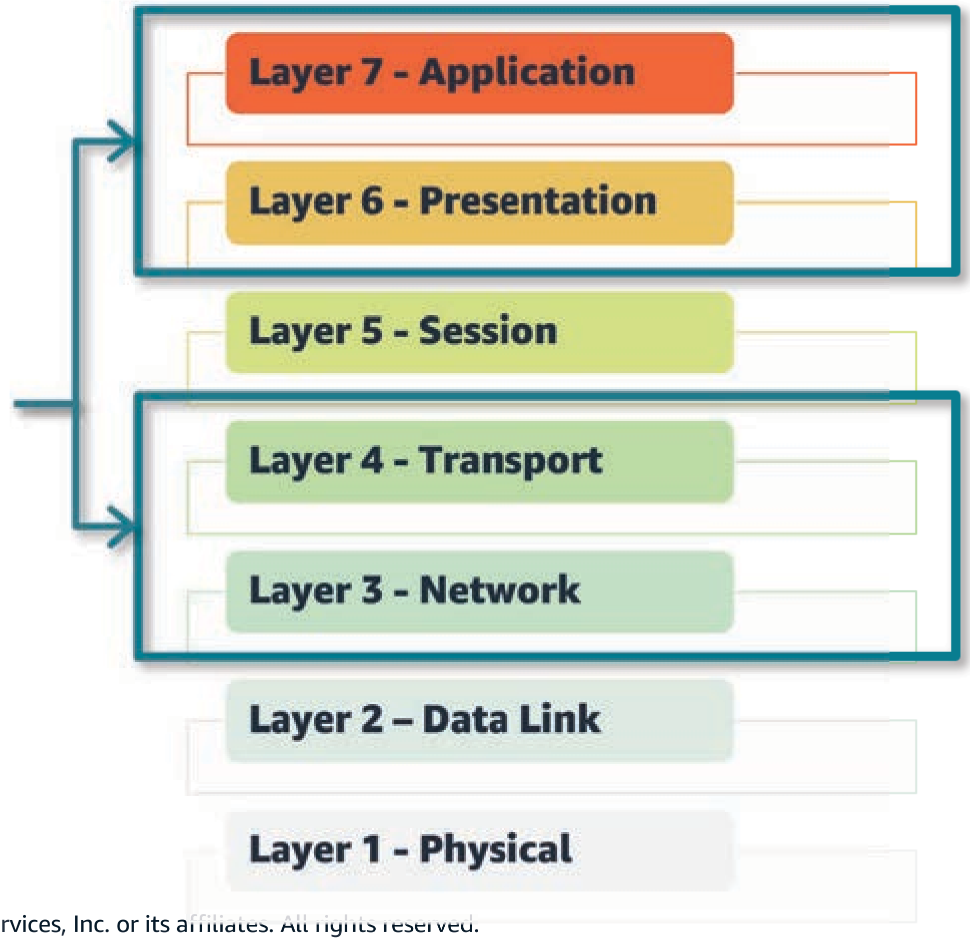
- Use additional security groups or network interfaces to control Amazon EC2 instance management traffic separately from regular application traffic.
- Implement special IAM policies for change control and auditing.

Security services

Section 3 of 4

Threat highlight: Distributed Denial of Service attack

DDoS are most common at the following Open Systems Interconnection (OSI) model layers:



Layer 7 - Application

Layer 6 - Presentation

Layer 5 - Session

Layer 4 - Transport

Layer 3 - Network

Layer 2 – Data Link

Layer 1 - Physical

AWS Shield

Standard Protection

- Available to all AWS Customers at **no additional cost**
- Automatic detection and mitigation
- Protection from most common DDoS attacks (SYN/UDP Floods, Reflection Attacks, etc.)

Advanced Protection

- Paid service that provides additional protection, features, and benefits.
- Includes Shield Response Team (SRT), AWS WAF for layer 7 DDoS attack mitigation, and AWS Firewall Manager

Shield Response Team (SRT)

- Shield Advanced includes the option to receive proactive support from the Shield Response Team (SRT).
- During a DDoS attack, the SRT will provide resolution support if necessary.

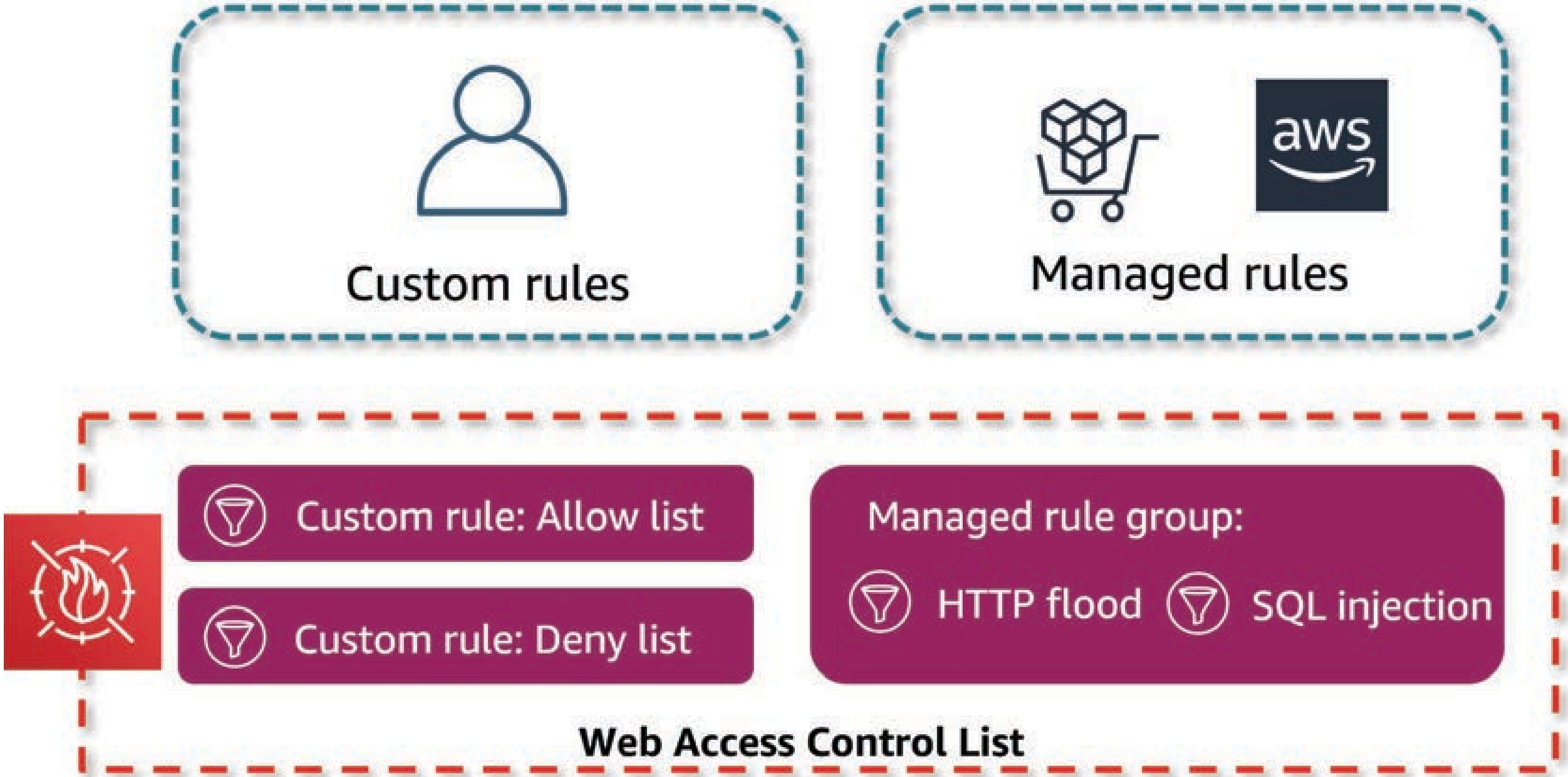
AWS Web Application Firewall (WAF)

AWS WAF filters traffic for your web applications based on the following criteria:

- IP address origin of the request
- Country of origin of the request
- String match or regular expression (regex) match in a part of the request
- Size of a particular part of the request
- Malicious SQL code or scripting

This service is provided to customers using AWS Shield Advanced for no additional cost and adds additional DDoS protection

AWS WAF rules and rule groups



AWS WAF

Demo Opportunity

AWS WAF supports many filtering options for stopping malicious http requests from reaching your resources. The lack of a User-Agent header in a request may indicate a bot or API based request.

- Task:
  - Create a rule that will block web requests using regex, or size constraint.

AWS Firewall Manager—benefits

Management

- Integrated with AWS Organizations
- Centrally managed global rules and account-specific rules

Compliance

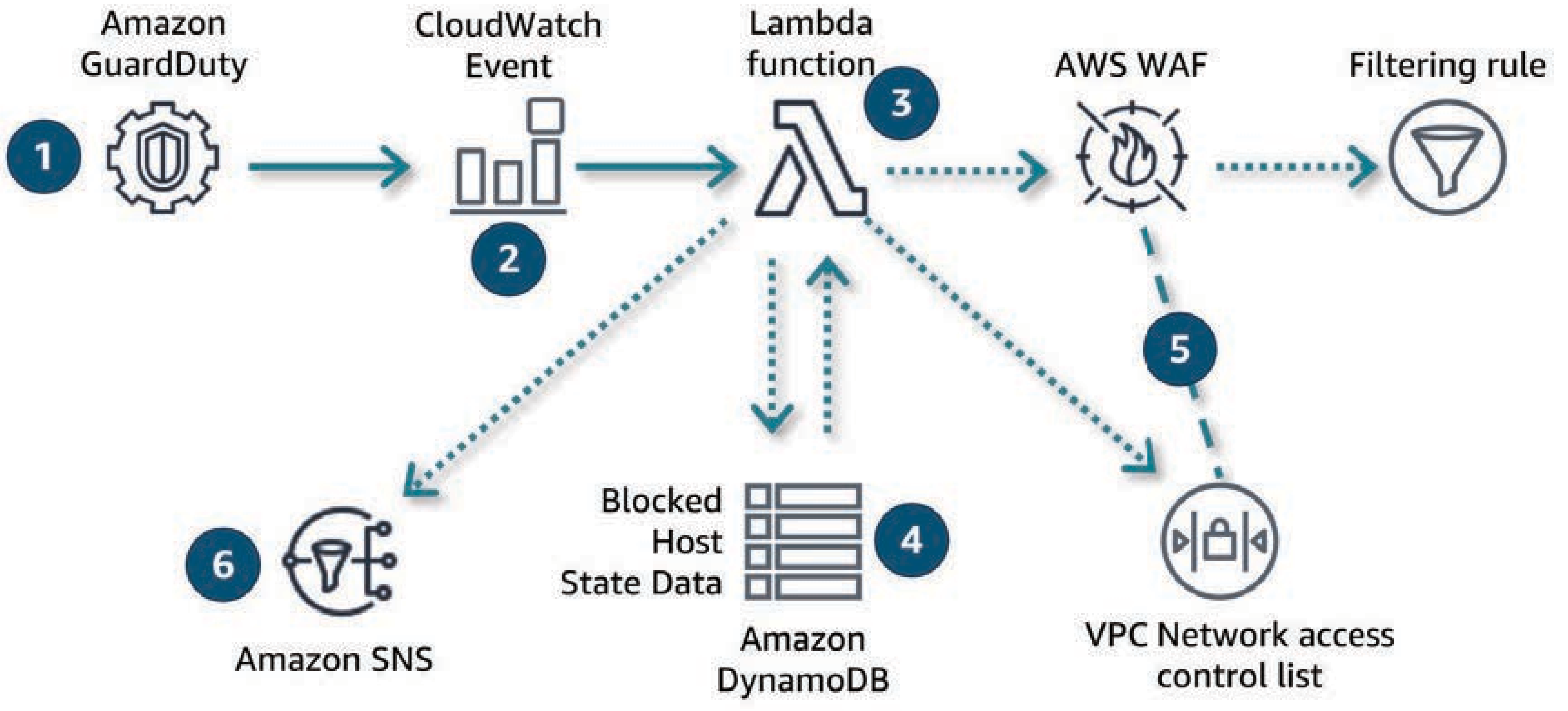
- Ensure that the entire organization adheres to a mandatory set of rules
- Apply protection, even when new accounts or resources are created

Visibility

Across the Organization:

- Central visibility of AWS WAF threats
- Consolidated AWS WAF operations
- Compliance dashboard for auditing

Example solution integration



"We saved about a million dollars per year in triage time for security operations, staffing, and licensing costs.”

Mark Dorsi

Director of Security, HelloSign

Use case—HelloSign

The security benefits realized include the following:

- Averted 12 DDoS security events
- Saved roughly 120 hours of work time per week through automation
- Gained visibility into security posture
- Implemented security best practices
- Customized security tools
- Automated security features within 3 months

Third-party security solutions

Section 4 of 4

AWS Marketplace enterprise solutions

Solution categories include the following:

- Network firewalls
- Protection solutions from software as a service (SaaS) or cloud delivery network providers
- Network IDS solutions

Module 2: Securing the network

Remember…

Control traffic at all layers using the following:

- Network ACLs, Security Groups, AWS Network Firewall

- Availability is an important part of securing the VPC.
- AWS services to secure network traffic and combat common security threats include the following:
  - AWS Shield Standard and Shield Advanced
  - AWS WAF
  - AWS Firewall Manager
- Third-party solutions offered through AWS Marketplace are available.

Let's check our knowledge with a few questions.

Question 1

Which statement is true about security groups?

A. Each subnet is required to be associated with only one security group.

B. A security group can be applied to one or more subnets.

C. Security groups allow for "allow" and "deny" rules.

D. Security groups are stateful.

Answer 1

Which statement is true about security groups?

A. Each subnet is required to be associated with only one security group.

B. A security group can be applied to one or more subnets.

C. Security groups allow for "allow" and "deny" rules.

D. (Correct) Security groups are stateful.

Question 2

Which AWS services or features are examples that BEST provide availability for your resources? (Select TWO.)

A. Regions and Availability Zones

B. Elastic Load Balancing (ELB)

C. Security Groups

D. Traffic mirroring

E. Network access control lists

Answer 2

Which AWS services or features are examples that BEST provide availability for your resources? (Select TWO.)

A. (Correct) Regions and Availability Zones

B. (Correct) Elastic Load Balancing (ELB)

C. Security Groups

D. Traffic mirroring

E. Network access control lists

Lab 1: Controlling the Network

By the end of this lab, you will be able to do the following:

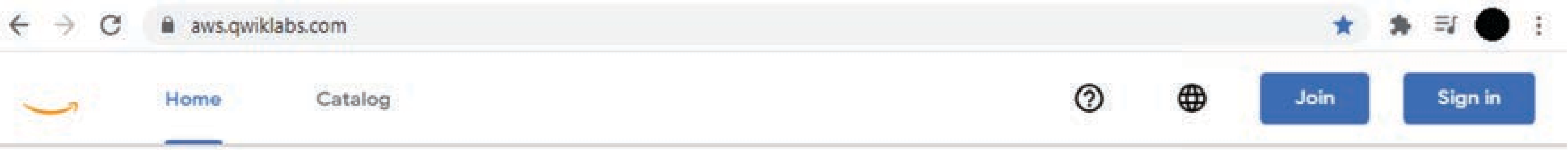
- Create a three-security zone network infrastructure
- Implement network segmentation using security groups, network ACLs, and public and private subnets
- Monitor network traffic to EC2 instances using VPC flow logs

Lab duration: 35 minutes

Labs

1 Log in at https://aws.qwiklabs.com/.

2 Existing users: **Sign in**
New users: **Join**



Amazon EC2 Security

AWS Security Best Practices

Module 3

Objectives

By the end of this module, you will be able to:

- Describe common compute security vulnerabilities.
- Construct a secure Amazon Elastic Compute Cloud (Amazon EC2) instance based on industry best practices.
- Use Amazon Elastic Block Store (Amazon EBS) encryption to secure volume data.
- Perform vulnerability management.

Agenda

This module is organized into the following sections:

- Compute hardening
- Amazon EBS encryption
- Secure management and maintenance
- Detecting vulnerabilities
- Using AWS Marketplace

Compute hardening

Section 1 of 5

Common vulnerabilities

Some examples of common vulnerabilities include the following:

- Unintentionally exposing Amazon Elastic Cloud Compute (EC2) instances to the public
- Sensitive information in metadata
- Unused or unneeded services or software
- Outdated or nonpatched OS or installed software
- Application configuration weaknesses (such as startup and configuration scripts containing sensitive information)
- Overly permissive identity and access management policies

Hardening your systems

Examples of hardening:

- Changing default passwords
- Removing or disabling unnecessary software or services
- Removal of unnecessary user names or logins
- Installing anti-malware and host intrusion detection and prevention systems (HIDS/HIPS)
- Using AWS Systems Manager Agent (**SSM** Agent) for remote access

AWS Services that can help

- AWS Systems Manager
- Amazon Inspector
- AWS Config

“Do I really need endpoint protection on my cloud resources?”

Consider this:

- Every OS has built-in malware protections and they’re all pretty good.
- All major OSs have vulnerabilities.
- It is important that you choose the appropriate software to help layer security (defense in depth) and protect your resources.

Hardening with benchmarks

Best practice

- Create an Amazon Machine Image (AMI) from your instance to save the configuration as a template for launching future instances.

-or-

- Use EC2 Image Builder to create and maintain images.
- Use benchmarks (from CIS and others) to harden common vulnerabilities and help minimize the attack surface.

CIS Benchmarks purpose

Benchmarks something to compare to and can help with the following.

- Using industry best practices
- Removing the guesswork in hardening
- Consistently evaluating against a known baseline
- Reducing complexity in risk management and auditing for critical, audited, and regulated systems

CIS Benchmarks alignment

CIS Benchmarks align closely with, or map to, regulatory frameworks including the following:

- National Institute of Standards and Technology Cybersecurity Framework (NIST CSF)
- Payment Card Industry Data Security Standard (PCI DSS)
- Health Insurance Portability and Accountability Act (HIPAA)
- International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC 2700)

Level 1, Level 2, and STIG profiles

Level 1 profile

- Practical and prudent
- Provides clear security benefit
- Does not inhibit utility or performance
- Intended for servers

Level 2 profile

- For environments or use cases where security is paramount
- Defense-in-depth measure
- Can negatively inhibit utility or performance
- Intended for servers

STIG profile

- Replaced the Level 3 profile
- Meets all STIG-specific recommendations, which overlap recommendations from Level 1 and Level 2

Amazon EBS encryption

Section 2 of 5

Amazon EBS backed instances

Best practices

- Use separate Amazon EBS volumes for the OS and your data.
- Encrypt EBS volumes and snapshots.
- Understand the implications of the root device type for data persistence, backup, and recovery.

Encryption by default

Encryption by default is a best practice to ensure security of data at rest.

- Encryption by default is a Region-specific setting.
- You can launch an instance only if the instance type supports Amazon EBS encryption.
- Do not use encryption by default while using automated migration services.

Encryption and snapshot copying

When you copy a snapshot, you can do the following:

- Keep it encrypted with the same KMS key as the original (incremental snapshot).
- Change the KMS key (full copy).
- Change the encryption status (full copy).
  - Full copies can incur greater data transfer and storage charges.

AWS KMS

Demo opportunity

AWS KMS supports many of the security best practices discussed in this course, providing centralized and secure management of cryptographic keys. This demo provides a quick look at so important features within AWS KMS.

- Prerequisites:
  - IAM user with appropriate AWS KMS permissions

Secure management and maintenance

Section 3 of 5

Management and maintenance

Best practices

- Limit access and authorization for connecting to instances *(Session Manager)*
- Securely manage instances at scale (using Run Command).
- Regularly patch and update with defined maintenance windows *(using Patch Manager).*
- Automate monitoring and remediate of configuration drift *(using State Manager).*
- Secure, monitor, and rotate secrets *(using Secrets Manager or Parameter Store).*

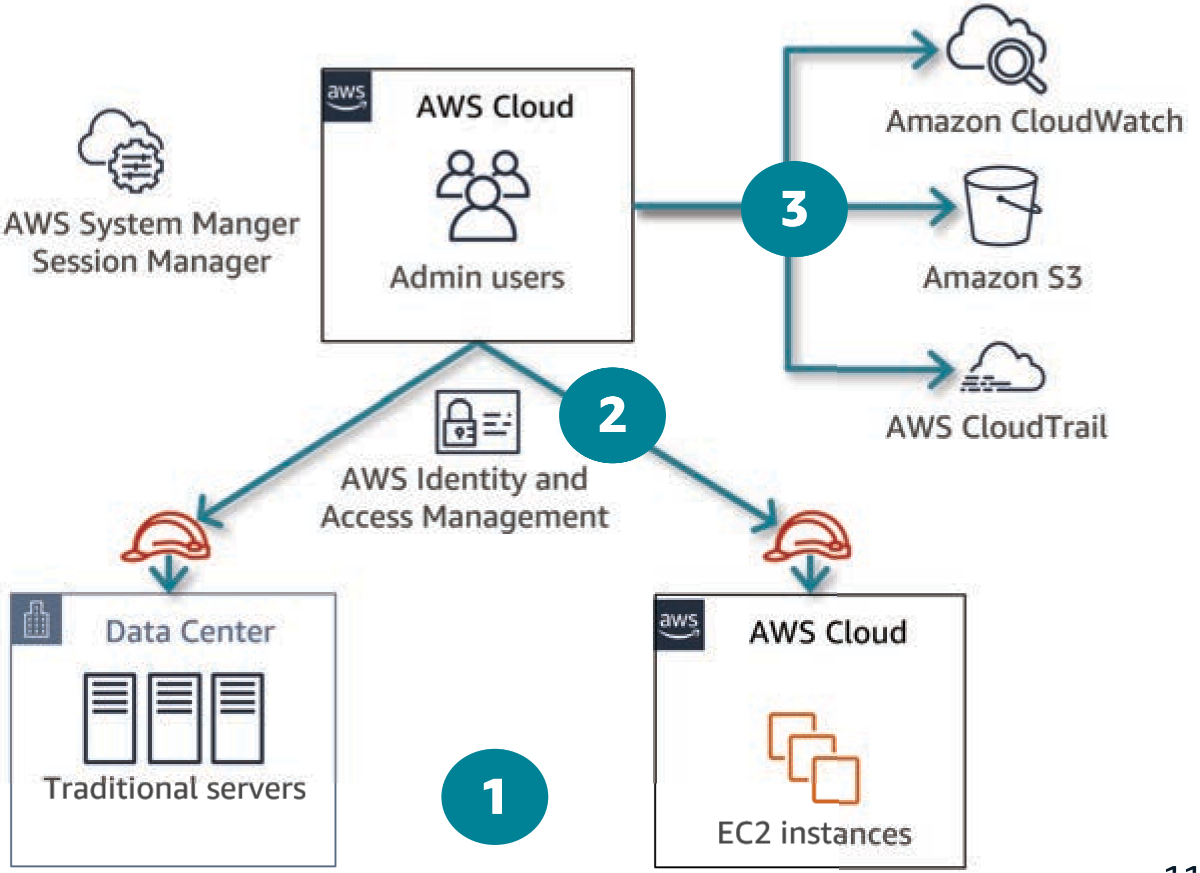
AWS Systems Manager

Node Management Highlights

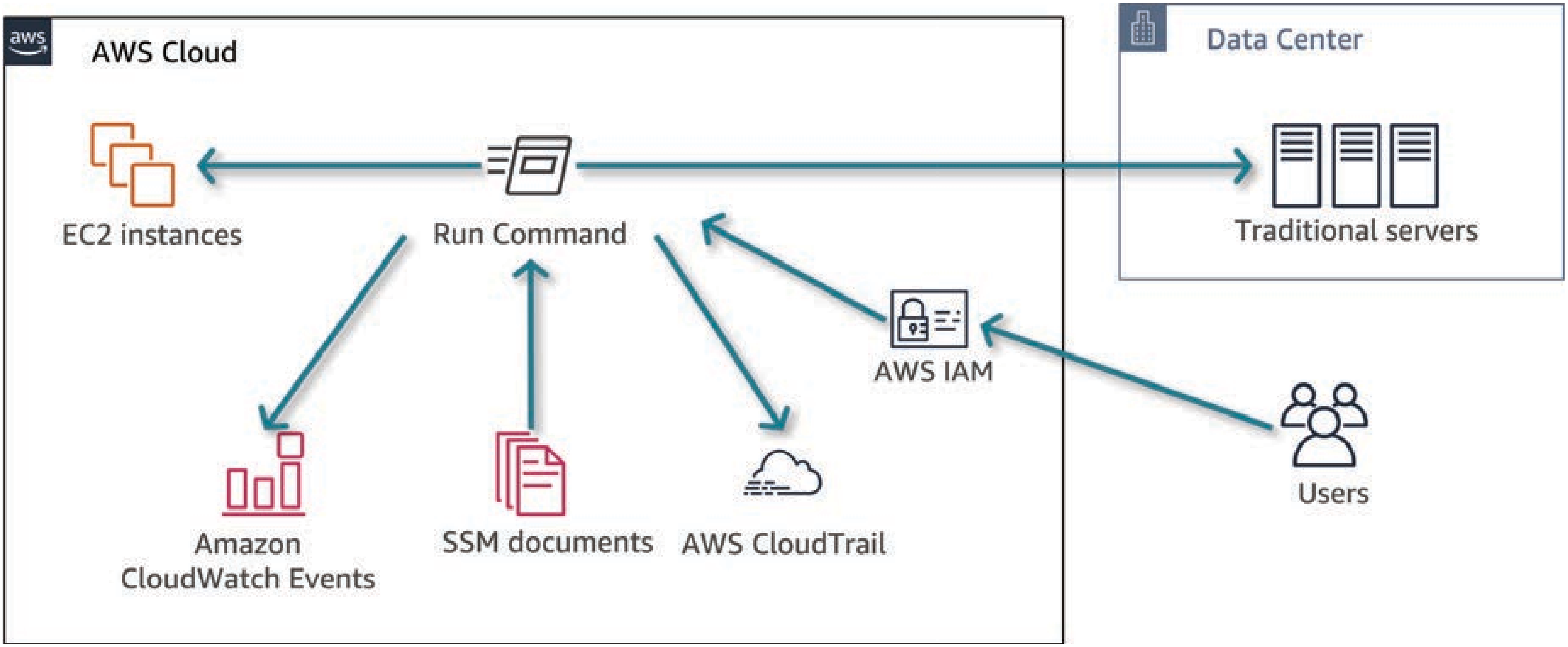
- Session Manager
- Run Command
- State Manager
- Patch Manager
- Parameter Store (compared to AWS Secrets Manager)

Session manager

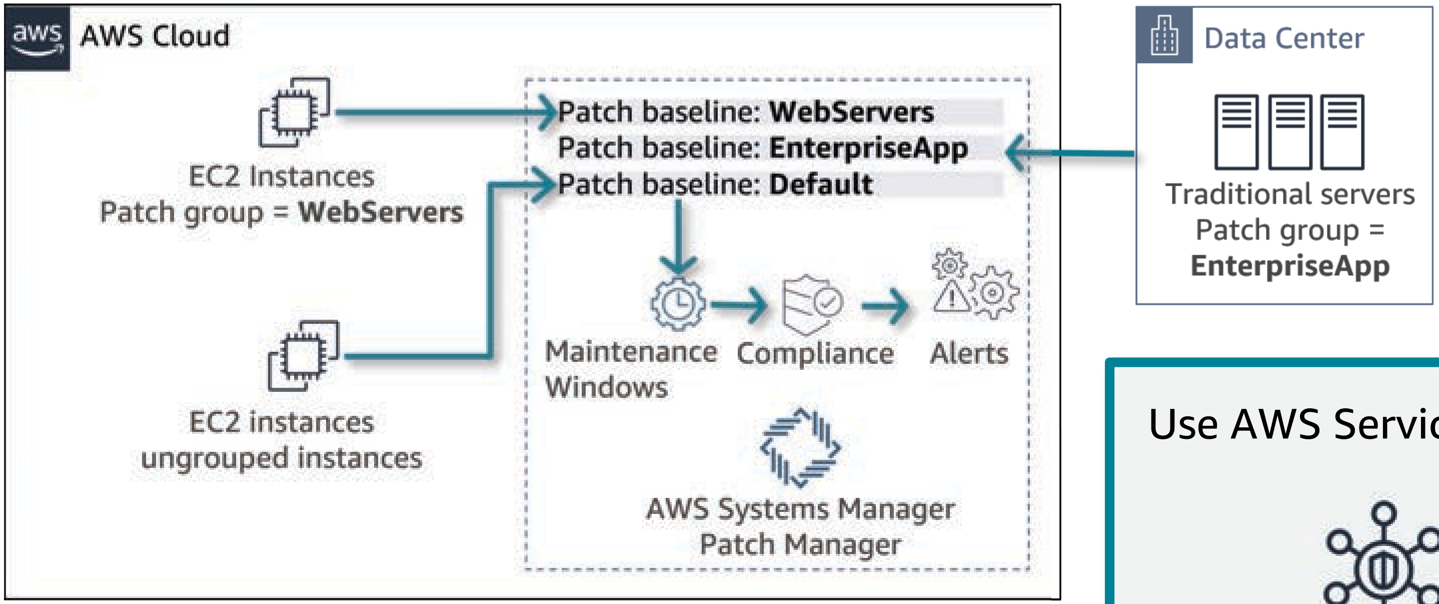
- Centralized access control to managed nodes using IAM policies
- No open inbound ports and no need to manage bastion hosts or SSH keys
- Logging and auditing session activity



Run command


AWS Cloud
EC2 instances
Run Command
Amazon CloudWatch Events
SSM documents
AWS CloudTrail
AWS IAM
Data Center
Traditional servers
Users

Patching best practices



- Deploy patches at scale.
- Schedule dedicated maintenance periods.
- Test patches in a nonproduction environment.

Use AWS Service Integrations

AWS Security Hub

AWS Config

State Manager

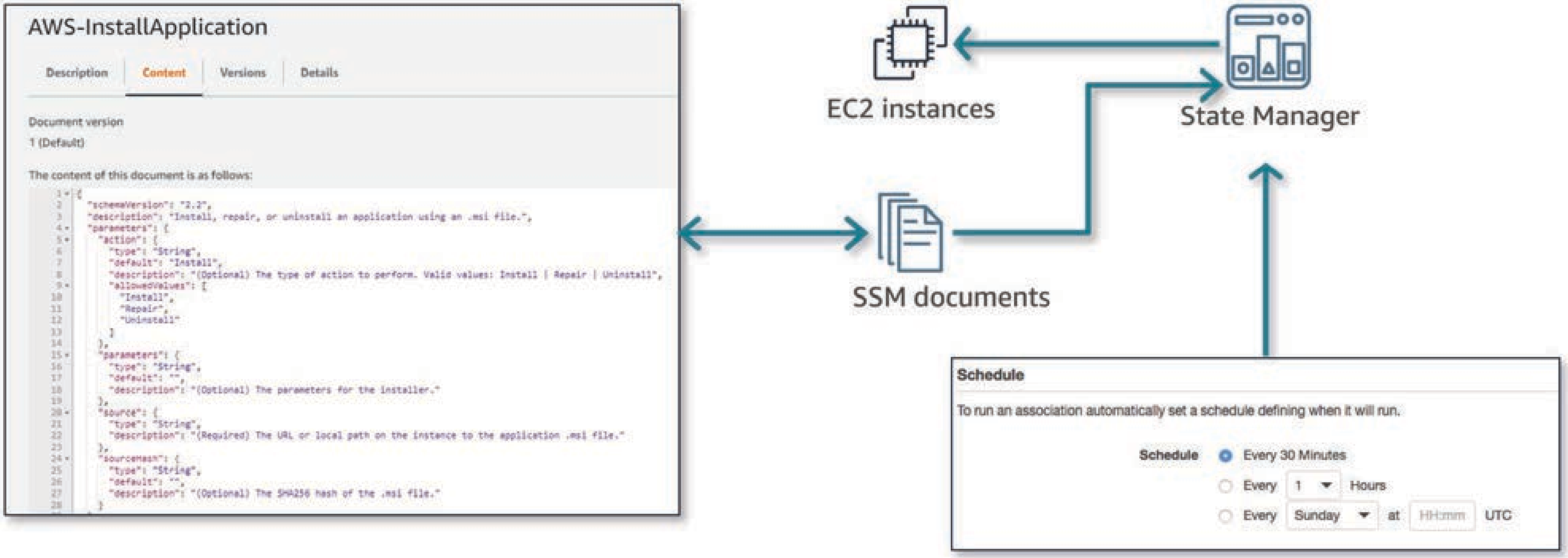
Usage

- Maintain visibility over system states.
- Apply configurations based on policies.
- Create and push alerts when configuration drifts are detected.
- Query statuses for on-demand visibility into compliance status.

Best practices

- Update SSM Agent using the preconfigured AWS-UpdateSSMAgent document.
- Use tags to create groups then target nodes using the targets parameter.
- Use a centralized configuration repository for your SSM documents, and share it across your organization.

State Manager example



AWS-InstallApplication

Document version

1 (Default)

The content of this document is as follows:

```
{
  "schemaVersion": "2.2",
  "description": "Install, repair, or uninstall an application using an .msi file.",
  "parameters": {
    "action": {
      "type": "String",
      "default": "Install",
      "description": "(Optional) The type of action to perform. Valid values: Install | Repair | Uninstall",
      "allowedValues": [
        "Install",
        "Repair",
        "Uninstall"
      ]
    },
    "parameters": {
      "type": "String",
      "default": "",
      "description": "(Optional) The parameters for the installer."
    },
    "source": {
      "type": "String",
      "description": "(Required) The URL or local path on the instance to the application .msi file."
    },
    "sourceHash": {
      "type": "String",
      "default": "",
      "description": "(Optional) The SHA256 hash of the .msi file."
    }
```

Schedule

To run an association automatically set a schedule defining when it will run.

Schedule ● Every 30 Minutes

○ Every 1 ▾ Hours

○ Every Sunday ▾ at HH:mm UTC

Parameter Store and Secrets Manager

Parameter Store

- Can notify you of expiring secrets but cannot rotate them for you
- Can be referenced from AWS CloudFormation templates
- Supports storing values under a name or key, encryption of secrets, and versioning

Secrets Manager

In addition to the capabilities of Parameter Store:

- Provides full key rotation integration with Amazon RDS
- Randomly generates passwords in CloudFormation and stores the password in Secrets Manager
- Shares secrets across different AWS accounts
- Can exceed storage capacity of Parameter Store, but has costs associated to storage of secrets and API calls

Exploring AWS Systems Manager

You explored just a few of the node management capabilities of AWS Systems Manager. There are many other features available that can help to operate and maintain your environment securely:

- Distributor
- Fleet Manager
- Parameter Store
- Many more…

Detecting vulnerabilities

Section 4 of 5

Amazon Inspector

- Amazon Inspector continuously scans your resources to help you do the following:
  - Prioritize patch remediation.
  - Meet compliance requirements.
  - Identify zero-day vulnerabilities sooner.
- Amazon Inspector integrates with AWS Organizations, AWS Security Hub, and Amazon EventBridge.

Amazon Inspector findings

Package vulnerability

- Identify software packages in your environment that are exposed to common vulnerabilities and exposures (CVEs).
- Findings can lead to compromise of the confidentiality, integrity, or availability of data or systems.

Network reachability

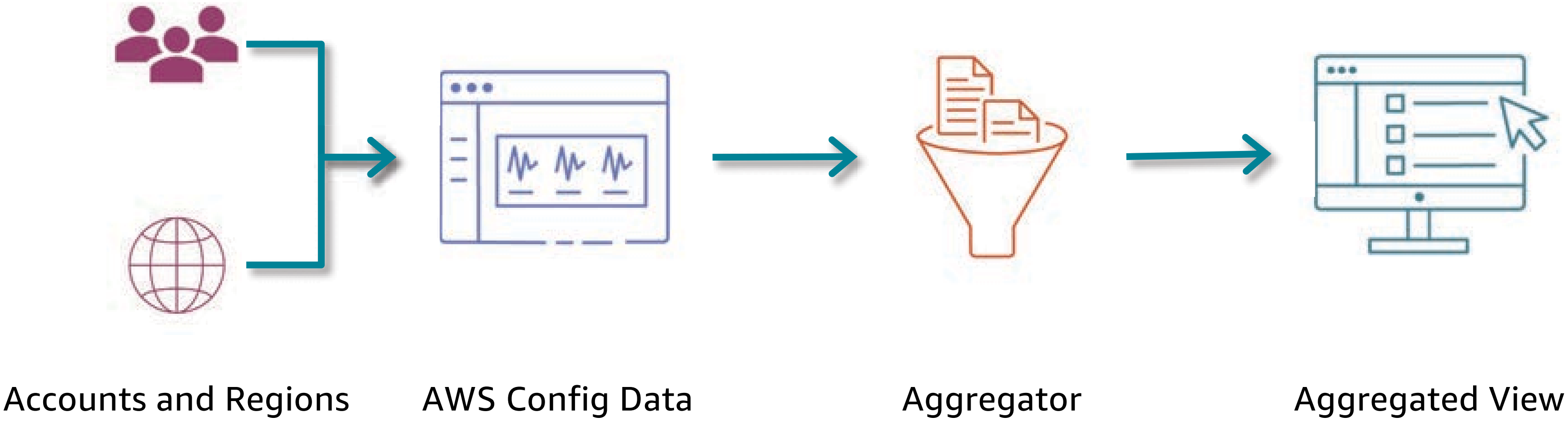
- Indicate that there are allowed network paths to EC2 instances in your environment.
- Indicate overly permissive paths over TCP or User Datagram Protocol (UDP) ports at virtual private cloud (VPC) edges that allow for potentially malicious access.

AWS Config benefits

- Automatically discover resources.
- Record the current state of a resource.
- Track changes; collect a historical record of the changes .
- Evaluate configuration changes against compliance policies.
- Automate remediation activities.
- Create real-time alerts using Amazon SNS and EventBridge.

AWS Config at scale

- Use the multi-account, multi-Region data aggregation feature in AWS Config.
- Aggregate based on your organization or invite individual AWS accounts.
- Provides aggregate resource configurations and AWS Config rule compliance data.



Using AWS Marketplace

Section 5 of 5

Using AWS Marketplace AMI products

Ways to use:

1. AMI subscriptions
2. AMI products with contract pricing
3. Metering-enabled AMI products
4. No cost, community AMIs

AWS Marketplace: AMI security requirements

- AMIs must not contain known vulnerabilities or malware.
- AMIs must use current OSs and software packages.
- AMIs must not request or use secret keys.
- Linux-based AMIs must not allow SSH password authentication.
- Instance access must be key pair based (no password-based authorization).

Comparing Community and AWS Marketplace AMIs

Community AMIs

- Whenever an AWS user creates an AMI, they can add permissions to it to make it public. In that case, it becomes accessible through community AMIs. These AMIs come from AWS users and are not verified by AWS.

AWS Marketplace AMIs

- All AMIs in AWS Marketplace are verified by AWS.

Module 3: Compute Security

Remember…

- Harden against compute vulnerabilities.
  - Hardening with benchmarks
  - AMIs or image security
- Protect data on your instances.
  - Encryption on Amazon EBS
  - AWS Systems Manager for management and maintenance
  - Secure secrets storage
- Detect vulnerabilities.
  - Amazon Inspector
  - AWS Config

Let’s check our knowledge with a few questions.

Question 1

Which tasks does Amazon Inspector help you perform? (Select TWO)

A. Prioritize patch remediation.

B. Speed up deployment of databases.

C. Run Amazon EC2 instances without the use of antivirus software.

D. Identify zero-day vulnerabilities sooner.

E. Disable unnecessary services.

Answer 1

Which tasks does Amazon Inspector help you perform? (Select TWO)

A. (Correct) Prioritize patch remediation.

B. Speed up deployment of databases.

C. Run Amazon EC2 instances without the use of antivirus software.

D. (Correct) Identify zero-day vulnerabilities sooner.

E. Disable unnecessary services.

Question 2

What is a good reason to use an Amazon Elastic Block Store (Amazon EBS) backed root volume for your Amazon EC2 instance?

A. You only pay when the instance is running.

B. Data is persistent.

C. The root device is temporary.

D. The boot time is slower.

Answer 2

What is a good reason to use an Amazon Elastic Block Store (Amazon EBS) backed root volume for your Amazon EC2 instance?

A. You only pay when the instance is running.

B. (Correct) Data is persistent.

C. The root device is temporary.

D. The boot time is slower.

Lab 2: Controlling the Endpoint

By the end of this lab, you will be able to do the following:

- Create a custom AMI
- Deploy a new EC2 instance from a custom AMI
- Patch an EC2 instance using AWS Systems Manager
- Encrypt an EBS volume
- Understand how Amazon EBS encryption works and how it impacts other operations, such as snapshots

Lab duration: 60 minutes

Monitoring and Alerting

AWS Security Best Practices

Module 4

Objectives

By the end of this module, you will be able to do the following:

- Configure service and application logging.
- Analyze logs, findings, and metrics centrally.
- Automate response to events as much as possible.

Agenda

This module is organized into the following sections:

- Logging network traffic
- Logging user and API traffic
- Visibility with Amazon CloudWatch
- Enhancing monitoring and alerting
- Verifying your AWS environment

Logging network traffic

Section 1 of 5

VPC Flow Logs

What they are

VPC Flow Log capture packet metadata like the source IP address, destination IP address, ports, protocol, packet size and other metadata.

- Flow Logs cannot monitor packet contents (payload or application layer data).
- They are not real-time, they use aggregation interval for capture.
- Some types of traffic traversing your network are **NOT** captured by Flow Logs.
- They have no affect on network throughput or latency.

Best practices

- **VPC flow logging should be enabled for packet rejects for all VPCs.**
- Flow logging is instrumental to network traffic investigations.
- AWS Config has a rule to check if a VPC has flow logging enabled.

Anatomy of a log

Default format

- You cannot customize or change the default format.

Custom format

- Specify fields and order included in flow log records (any number, but at least one field is required).
- Simplify log processing.

Default format example

	1	2	3	4	5	6						7	
2	123…0	eni-12ab…9	172.31.9.2	172.31.1.6	49761	3389	6	20	4249	141…1	141..9	REJECT	OK

Longer fields in the example above have been truncated using "…" to allow the entire log to be shown on a single line.

Traffic Mirroring

Using traffic mirroring provides a detective control that allows you to send your traffic to out-of-band security appliances for the following:

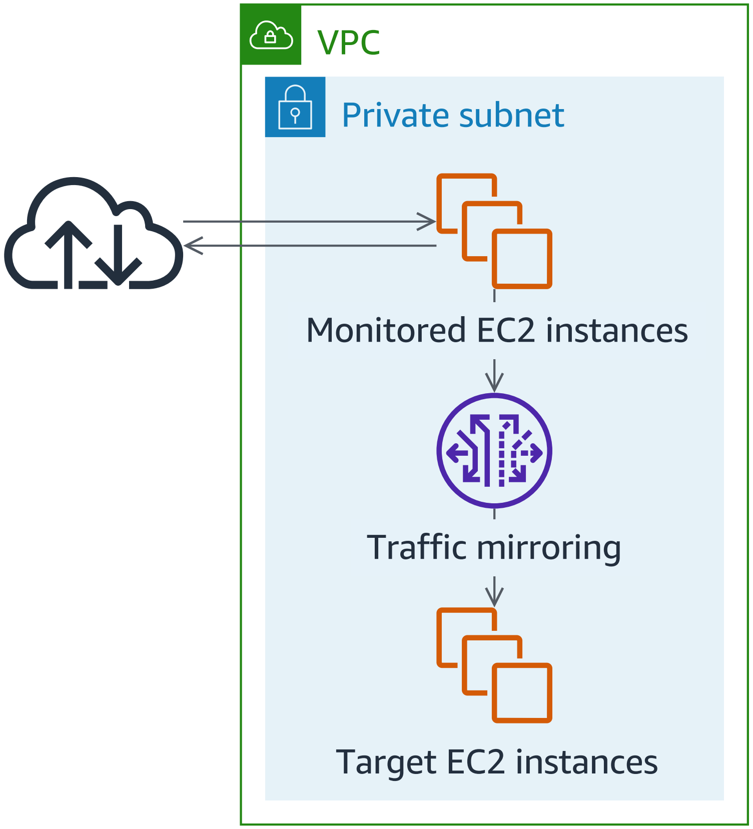
- Content inspection
- Threat monitoring
- Troubleshooting

Reasons for Traffic Mirroring

- Detect network and security anomalies
  - You can extract traffic of interest from any workload in a VPC and route it to the detection tools of your choice. You can detect and respond to attacks more quickly than is possible with traditional log-based tools.
- Implement compliance and security controls
  - You can meet regulatory and compliance requirements that mandate monitoring, logging, and so forth.

Traffic Mirroring components

- Target—The destination for mirrored traffic. A single instance, appliance, or a load balancer connecting to a fleet
- Filter—A set of rules that defines the traffic that is of interest. Traffic that will be copied in the traffic mirror session
- Session—An entity that describes Traffic Mirroring from a source to a target using filters



Logging user and API traffic

Section 2 of 5

AWS CloudTrail functions

- Simplify compliance audits by automatically recording and storing activity logs for an AWS account.
- Increase visibility into user and resource activity.
- Discover and troubleshoot security and operational issues by capturing a comprehensive history of changes that occurred in an AWS account.

AWS CloudTrail tracks the who, what, where, and when of activity that occurs in your AWS environment and records this activity in audit logs.

Security benefits and uses

- Perform security analysis and detect behavior patterns by ingesting CloudTrail API call history into log management and analytics solutions
- Maintain compliance with internal policies or regulatory standards
- Detect malicious activities and integrate other AWS services to automate remediation

CloudTrail configuration

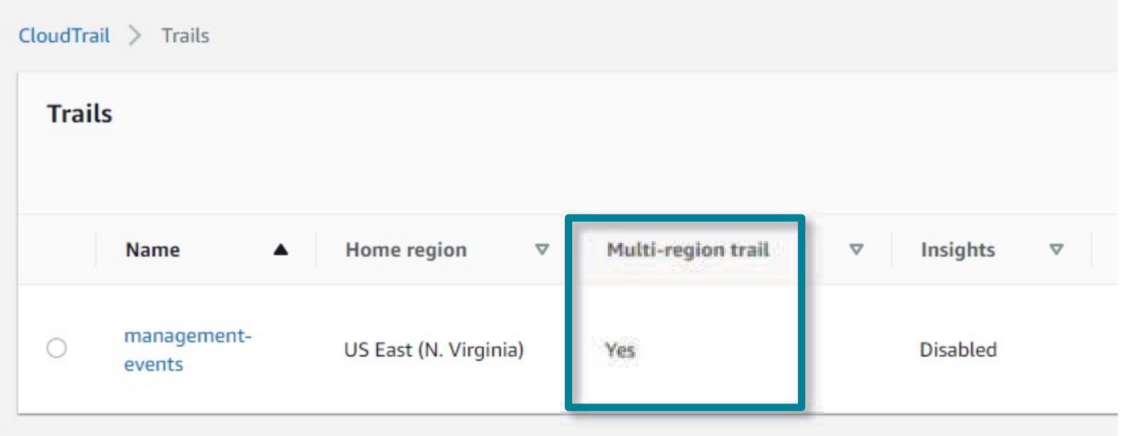
You can configure two types of “trails”:

1. A trail that applies to one Region
2. A trail that applies to all Regions

- This is the default setting when you create a trail in the CloudTrail console.
- **This is a best practice recommendation.**

Best practice: Multi-Region configuration

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": false,
    "S3BucketName": "my-bucket"
}
```



Trails

	Name ▲	Home region ▽	Multi-region trail ▽	Insights ▽
○	management-events	US East (N. Virginia)	Yes	Disabled

AWS CloudTrail best practices

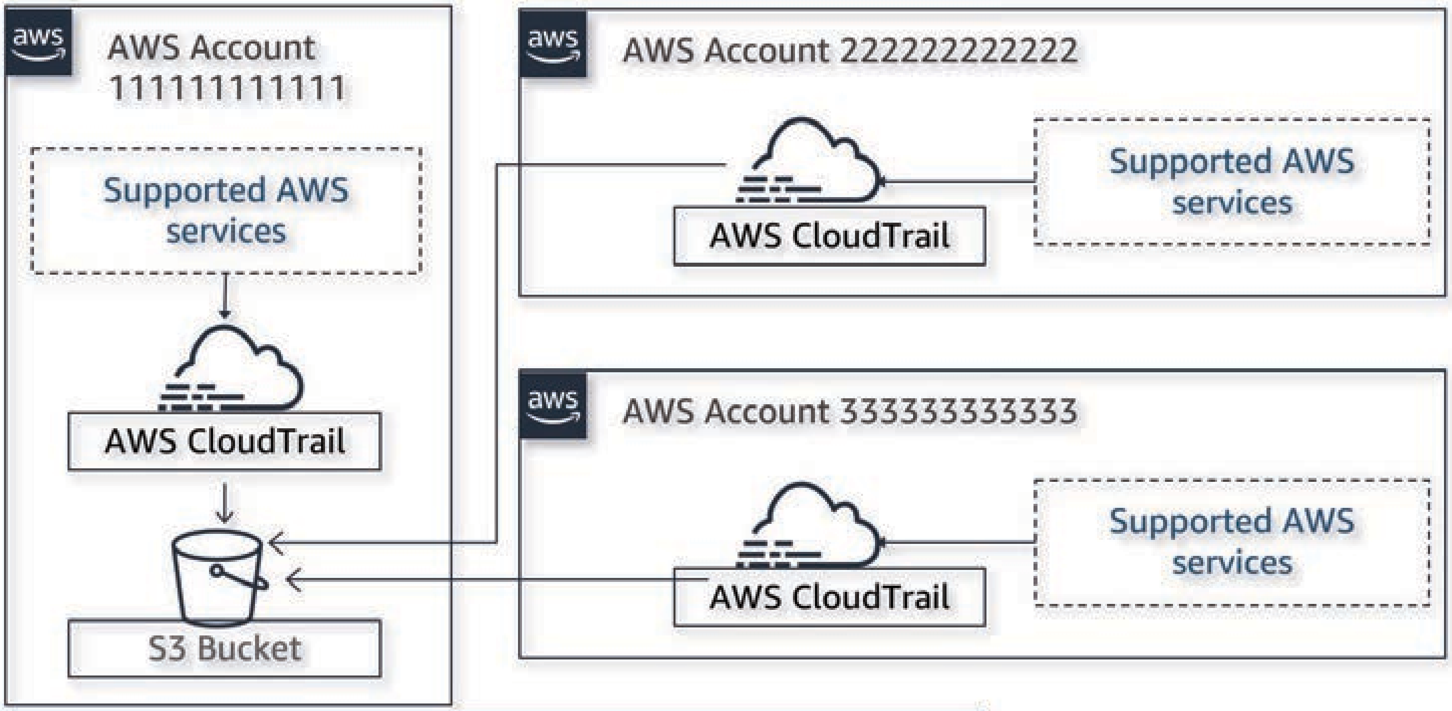
Centralizing multi-account CloudTrail logging

Many-to-one centralization

- Use AWS Organizations to centralize logging;
  - From multiple Regions into one S3 bucket (all-Regions/one-account)
  - From multiple accounts into one account's Amazon Simple Storage Service (S3) bucket
- AWS Control Tower centralizes logging for AWS Organizations by default.

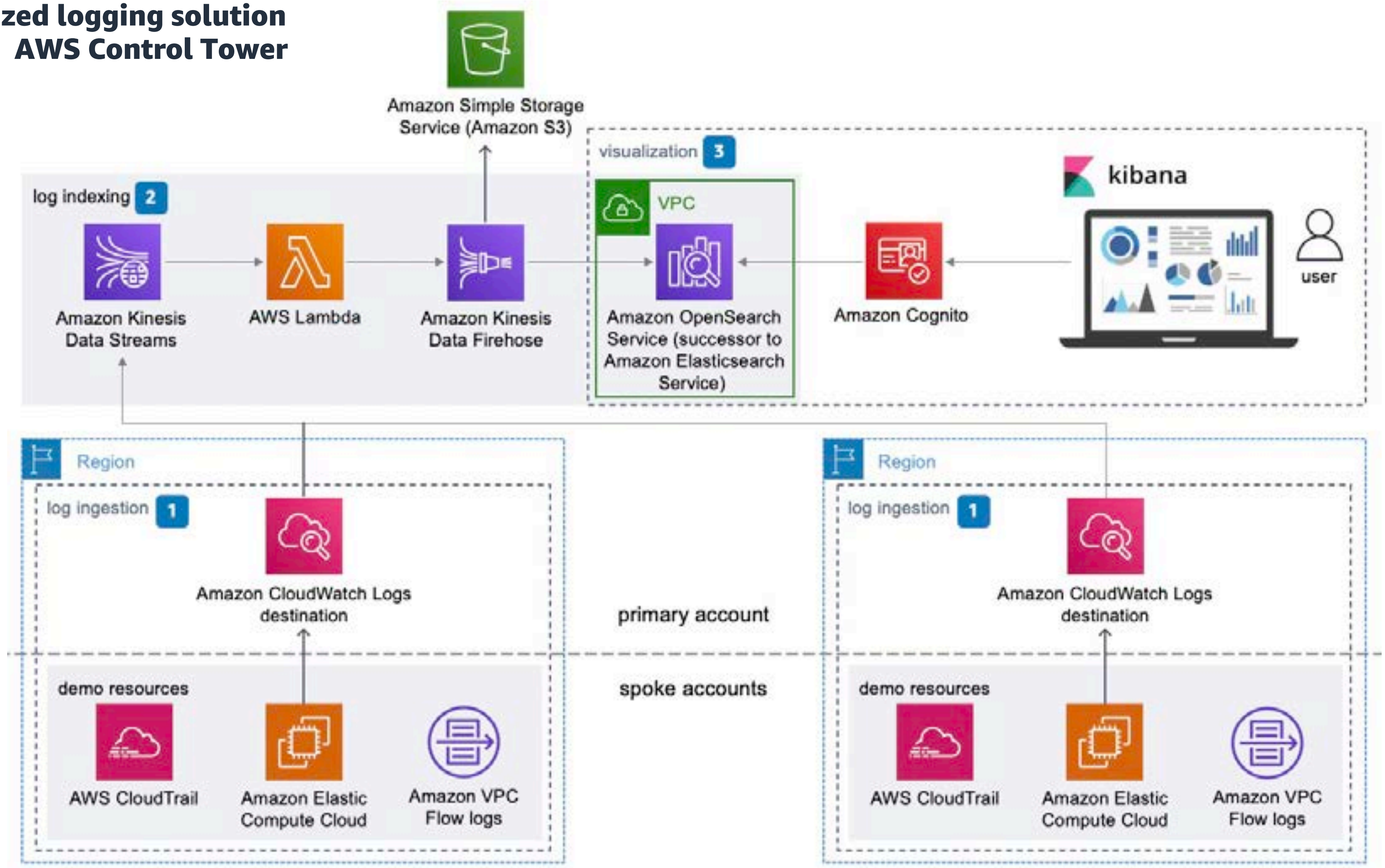
AWS CloudTrail with AWS Organizations

- Turn on CloudTrail for your Organization.
- Update bucket policy.
- Turn on CloudTrail for 222222222222.
- Turn on CloudTrail for 3333333333.



"arn:aws:s3:::mycloudtrailbucket/AWSLogs/o-12345678/*",

Centralized logging solution without AWS Control Tower


Amazon Simple Storage Service (Amazon S3)
visualization 3
log indexing 2
Amazon Kinesis Data Streams
AWS Lambda
Amazon Kinesis Data Firehose
VPC
Amazon OpenSearch Service (successor to Amazon Elasticsearch Service)
Amazon Cognito
kibana
user
Region
log ingestion 1
Amazon CloudWatch Logs destination
primary account
spoke accounts
demo resources
AWS CloudTrail
Amazon Elastic Compute Cloud
Amazon VPC Flow logs
Region
log ingestion 1
Amazon CloudWatch Logs destination
demo resources
AWS CloudTrail
Amazon Elastic Compute Cloud
Amazon VPC Flow logs

Amazon S3 log storage

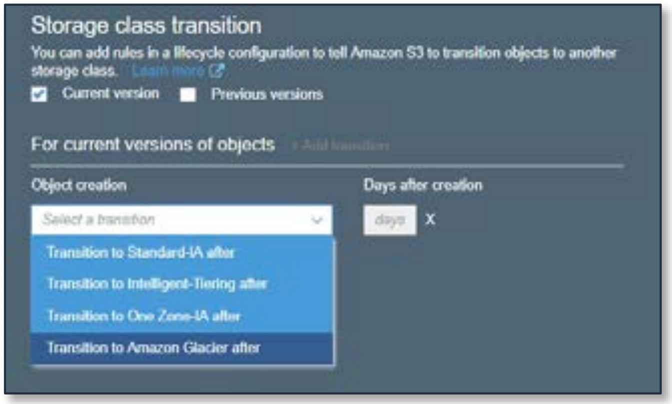
Best practice

- Use a dedicated S3 bucket for CloudTrail logs.
- Implement least-privilege access to buckets where you store log files.
- Enable multi-factor authentication (MFA) Delete on the log storage bucket.
- Limit access to the “AWSCloudTrail_FullAccess” policy.

CloudTrail: Lifecycle management

Best practices

- Configured through Amazon S3
- Available actions:
  - Transition to different storage tier
  - Expire (delete) object
  - Transition and expire



Storage class transition

You can add rules in a lifecycle configuration to tell Amazon S3 to transition objects to another storage class. Learn more

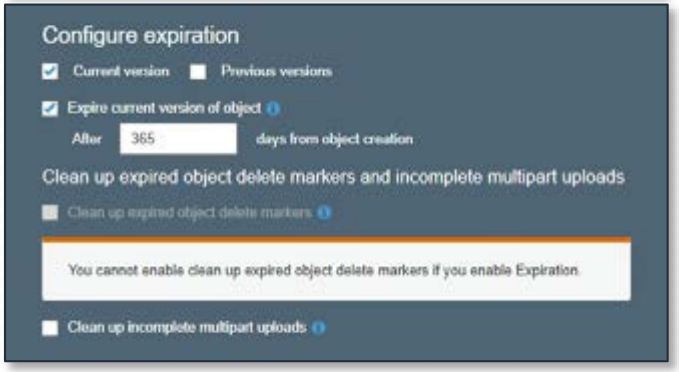
☑ Current version □ Previous versions

For current versions of objects + Add transition

Object creation: Select a transition

- Transition to Standard-IA after
- Transition to Intelligent-Tiering after
- Transition to One Zone-IA after
- Transition to Amazon Glacier after

Days after creation: days X



Configure expiration

☑ Current version □ Previous versions

☑ Expire current version of object

After 365 days from object creation

Clean up expired object delete markers and incomplete multipart uploads

□ Clean up expired object delete markers

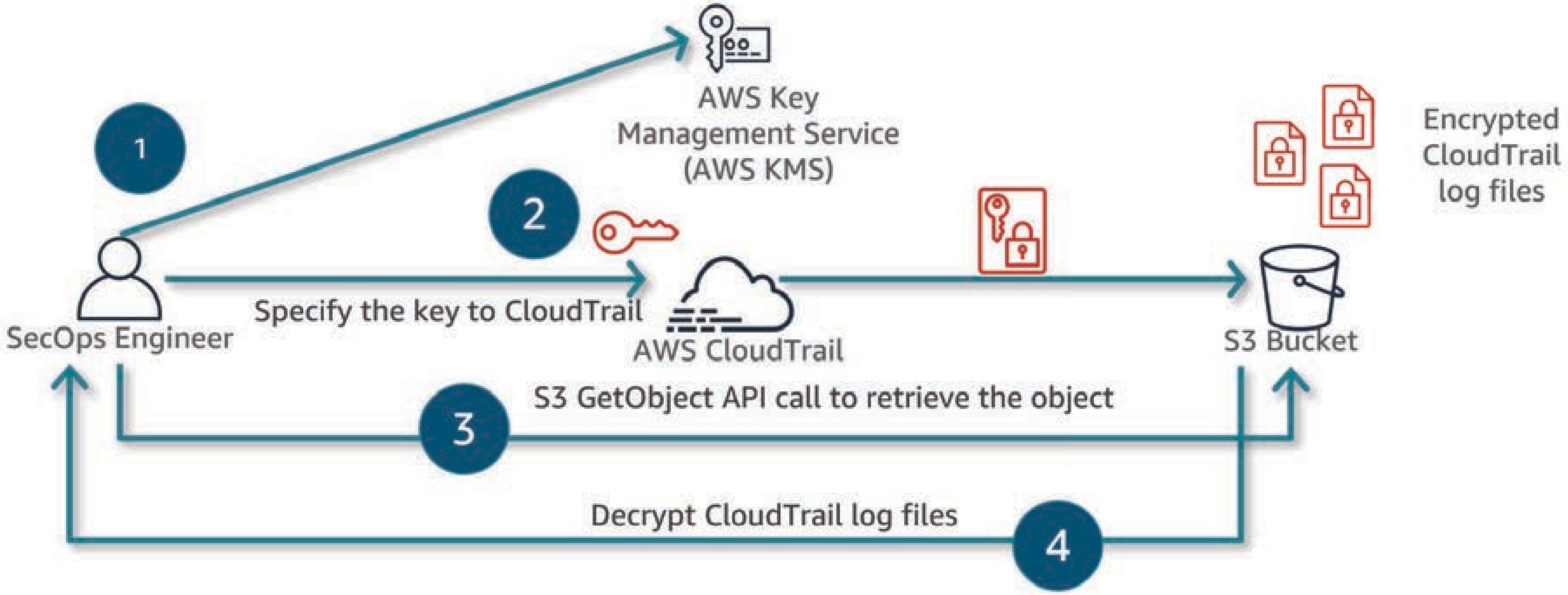
You cannot enable clean up expired object delete markers if you enable Expiration.

□ Clean up incomplete multipart uploads

CloudTrail confidentiality: AWS KMS encryption

Best practice

- Create or use an existing AWS Key Management Service (KMS) key and apply key policy to allow CloudTrail to encrypt and SecOps engineers to decrypt.


1
AWS Key Management Service (AWS KMS)
2
Specify the key to CloudTrail
SecOps Engineer
AWS CloudTrail
S3 Bucket
Encrypted CloudTrail log files
3
S3 GetObject API call to retrieve the object
Decrypt CloudTrail log files
4

Enable log integrity validation

Best practice

Once you turn on log file integrity validation, CloudTrail will start delivering digest files on an hourly basis to the same S3 bucket where you receive your CloudTrail log files, but with a different prefix.

- CloudTrail log files are delivered to: /optional_prefix/AWSLogs/AccountID/CloudTrail/*
- CloudTrail digest files are delivered to: /optional_prefix/AWSLogs/AccountID/CloudTrail-Digest/*

Integrate with CloudWatch Logs

Best practices

- Monitor and alert on specific events.
- Simple searching is provided.
- Use AWS Config to ensure CloudTrail is sending events to CloudWatch Logs.

Visibility with Amazon CloudWatch

Section 3 of 5

Indicators of compromise

- Abnormal CPU utilization
- Significant or sudden increases in database reads
- HTML response sizes
- Mismatched port-application traffic
- Unusual DNS requests
- Unusual outbound network traffic
- Anomalies in privileged user account activity
- Geographical irregularities (source of traffic)
- Unusually high traffic at irregular hours
- Multiple, repeated, or irregular login attempts

CloudWatch Alarms best practices

These are just a few examples of areas that should be monitored with CloudWatch Alarms:

- AWS Console sign-In requests without MFA
- IAM policy configuration changes
- Root account usage
- Authorization failures; unauthorized API calls made within your AWS account
- AWS KMS key configuration changes
- AWS CloudTrail configuration changes
- AWS EC2 instance and S3 changes
- AWS VPC, Route table, Internet Gateway, ACLs or security group configuration changes

Metric alarms

A metric alarm has the following possible states:

- OK – The metric or expression is within the defined threshold.
- ALARM – The metric or expression is outside the defined threshold.
- INSUFFICIENT_DATA – The alarm has just started, the metric is not available, or not enough data is available for the metric to determine the alarm state.

Composite alarms

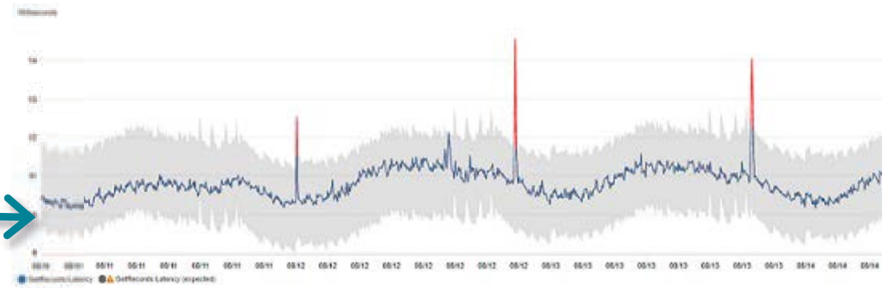
Alarms can be combined and grouped.

- They are hierarchical.
- They use Boolean logic **AND**, **OR**, and **NOT**.
- They can help to alleviate or avoid alarm fatigue by reducing noise.

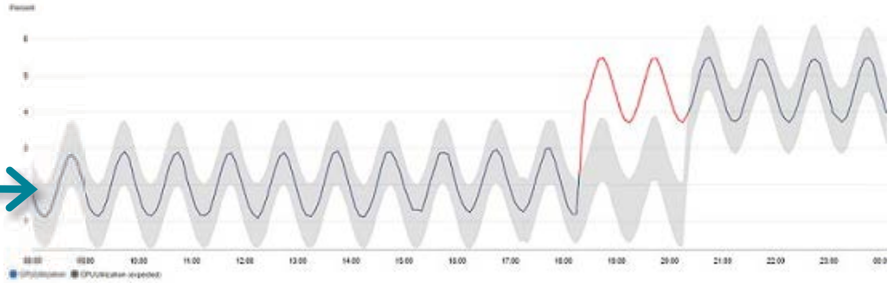
Using CloudWatch anomaly detection

- The expected range of values is shown as a wide gray band.

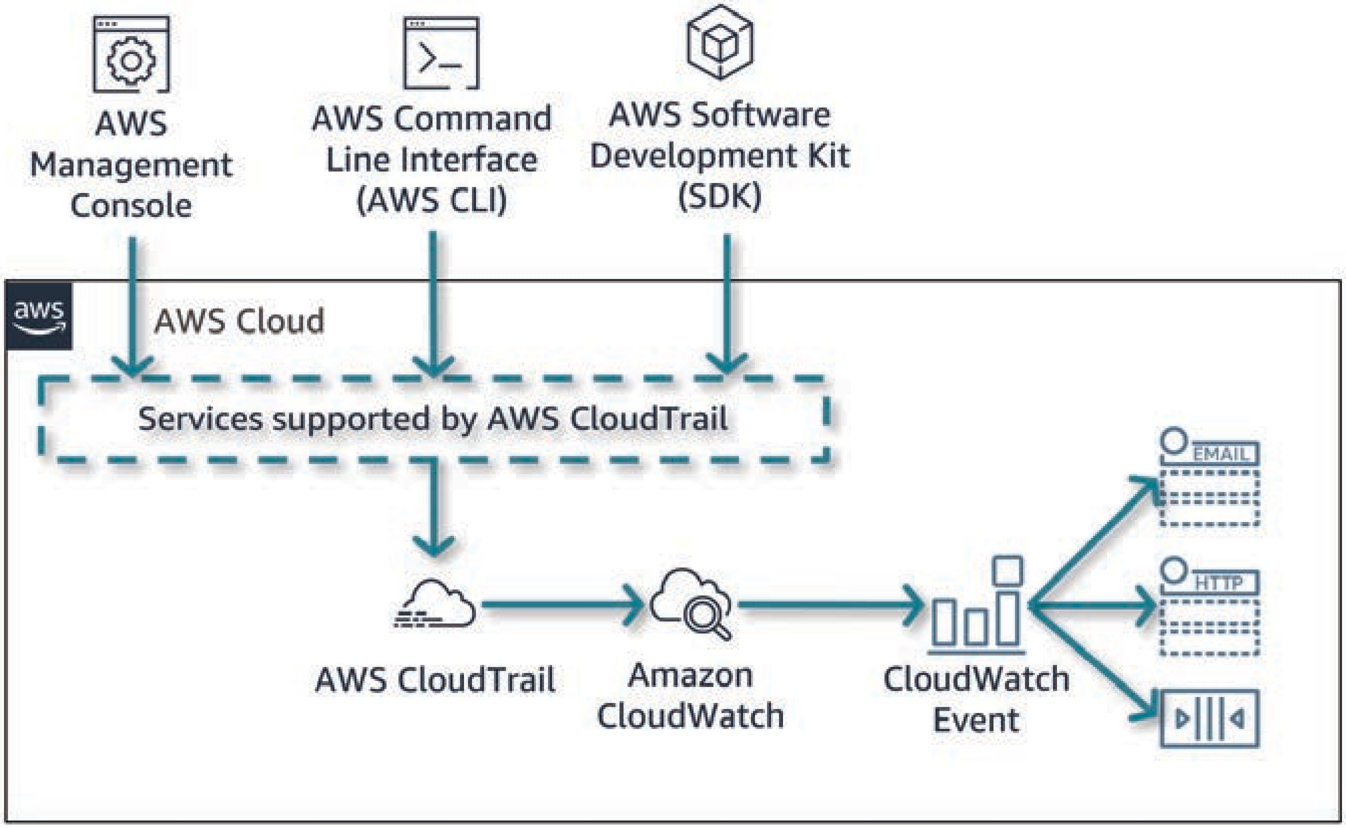
- Actual values outside this band are shown as red (the points extending above the wide band).



- Anomaly detection algorithms account for the seasonality and trend changes of metrics.



Alerting: Notifications of API activity


AWS Management Console
AWS Command Line Interface (AWS CLI)
AWS Software Development Kit (SDK)
aws
AWS Cloud
Services supported by AWS CloudTrail
AWS CloudTrail
Amazon CloudWatch
CloudWatch Event
EMAIL
HTTP

Follow-up actions:

- Create a ticket.
- Send an email.
- Automatically remediate.
- Message somebody on Slack.

Enhancing monitoring and alerting

Section 4 of 5

Detect with: Amazon GuardDuty

- One-click activation without architectural or performance impact
- Continuous monitoring of AWS accounts and resources
- Instant On provides findings in minutes
- No agents, no sensors, no network appliances
- Global coverage, regional results
- Built-in anomaly detection with machine learning
- Partner integrations for additional protections

GuardDuty data sources

Flow Logs

- Flow logs for VPCs *do not need to be turned on* to generate findings.
- Data is consumed through independent, duplicate stream.
- Turn on VPC Flow Logs to augment data analysis *(charges apply)*.

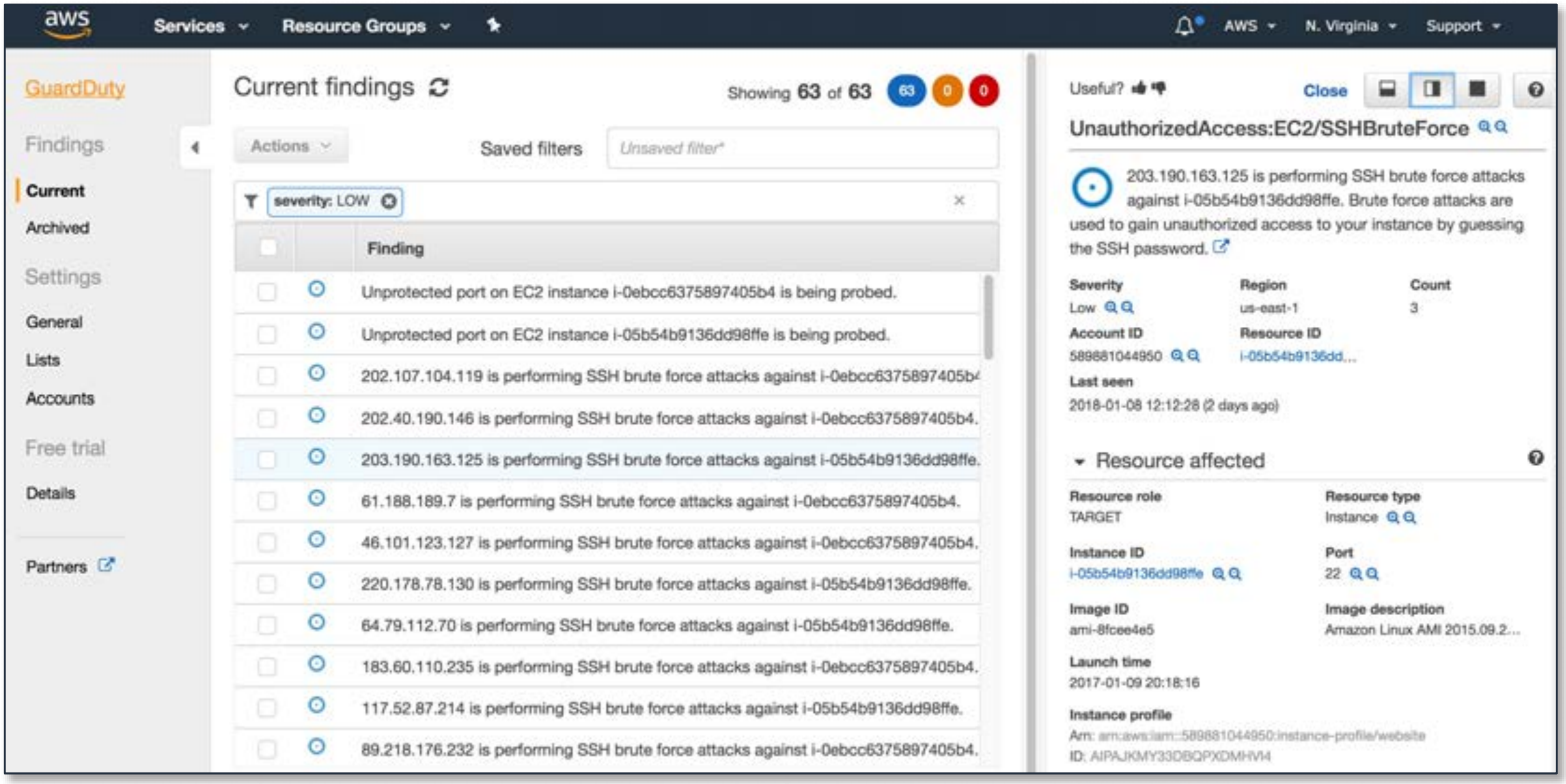
DNS events

- DNS logs are based on queries made from EC2 instances to known questionable domains.
- DNS logs are in addition to Route 53 query logs.
- Amazon Route 53 is not required for GuardDuty to generate DNS based findings.

CloudTrail events

- CloudTrail history of AWS API calls used to access the console, SDKs , AWS Command Line Interface or AWS CLI, and so on, parsed by GuardDuty.
- Identification of user and account activity including source IP address is used to make the calls.

GuardDuty: Findings



Current findings

Showing 63 of 63 (63) (0) (0)

severity: LOW

□		Finding
□	⊙	Unprotected port on EC2 instance i-0ebcc6375897405b4 is being probed.
□	⊙	Unprotected port on EC2 instance i-05b54b9136dd98ffe is being probed.
□	⊙	202.107.104.119 is performing SSH brute force attacks against i-0ebcc6375897405b4
□	⊙	202.40.190.146 is performing SSH brute force attacks against i-0ebcc6375897405b4.
□	⊙	203.190.163.125 is performing SSH brute force attacks against i-05b54b9136dd98ffe.
□	⊙	61.188.189.7 is performing SSH brute force attacks against i-0ebcc6375897405b4.
□	⊙	46.101.123.127 is performing SSH brute force attacks against i-0ebcc6375897405b4.
□	⊙	220.178.78.130 is performing SSH brute force attacks against i-05b54b9136dd98ffe.
□	⊙	64.79.112.70 is performing SSH brute force attacks against i-05b54b9136dd98ffe.
□	⊙	183.60.110.235 is performing SSH brute force attacks against i-0ebcc6375897405b4.
□	⊙	117.52.87.214 is performing SSH brute force attacks against i-05b54b9136dd98ffe.
□	⊙	89.218.176.232 is performing SSH brute force attacks against i-0ebcc6375897405b4.

UnauthorizedAccess:EC2/SSHBruteForce

203.190.163.125 is performing SSH brute force attacks against i-05b54b9136dd98ffe. Brute force attacks are used to gain unauthorized access to your instance by guessing the SSH password.

Severity: Low
Region: us-east-1
Count: 3
Account ID: 589881044950
Resource ID: i-05b54b9136dd...
Last seen: 2018-01-08 12:12:28 (2 days ago)

Resource affected

Resource role: TARGET
Resource type: Instance
Instance ID: i-05b54b9136dd98ffe
Port: 22
Image ID: ami-8fcee4e5
Image description: Amazon Linux AMI 2015.09.2...
Launch time: 2017-01-09 20:18:16
Instance profile
Arn: arn:aws:iam::589881044950:instance-profile/website
ID: AIPAJKMY33DBQPXDMHVI4

Manage and remediate with: AWS Security Hub

- Managed AWS service
- Consolidates and aggregates findings.
- Provides controls for the following standards:
  - Center for Internet Security (CIS) AWS Foundations
  - Payment Card Industry Data Security Standard (PCI DSS)
  - AWS Foundational Security Best Practices
- Integrates with ticketing, chat, incident management, investigation, GRC, SOAR, and SIEM tools.

Remediation with Security Hub

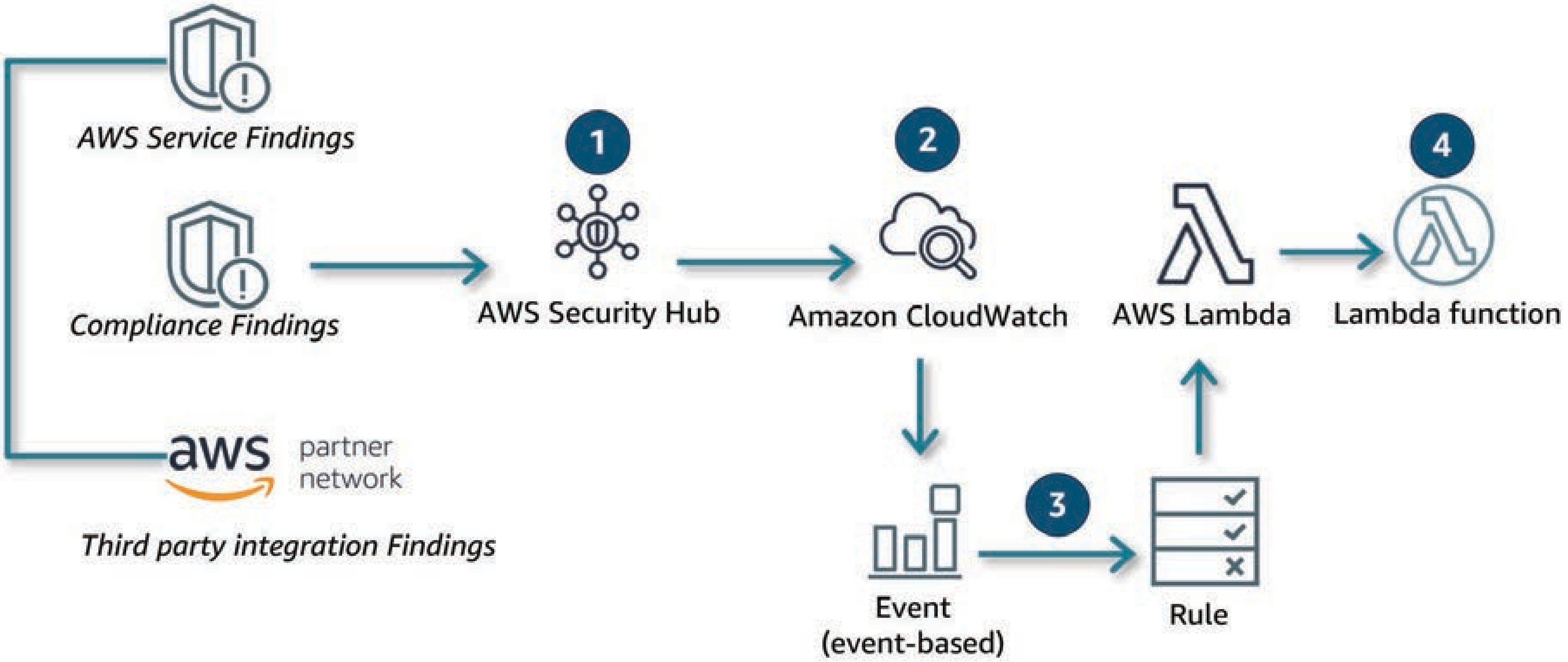
Manual remediation

- This is best for anything that has the potential to impact business objectives. This type of intervention is slower, but notifications can help expedite response.
- This option should also be used to test newly created automatic remediations before they are put into a production environment.

Automatic remediation

- This is best when there is a low risk of a negative impact to the workloads in the account.
- For example, you would not use an automatic remediation that stops an EC2 instance responsible for a business-critical function.

Auto remediation example



Auditing your AWS environment

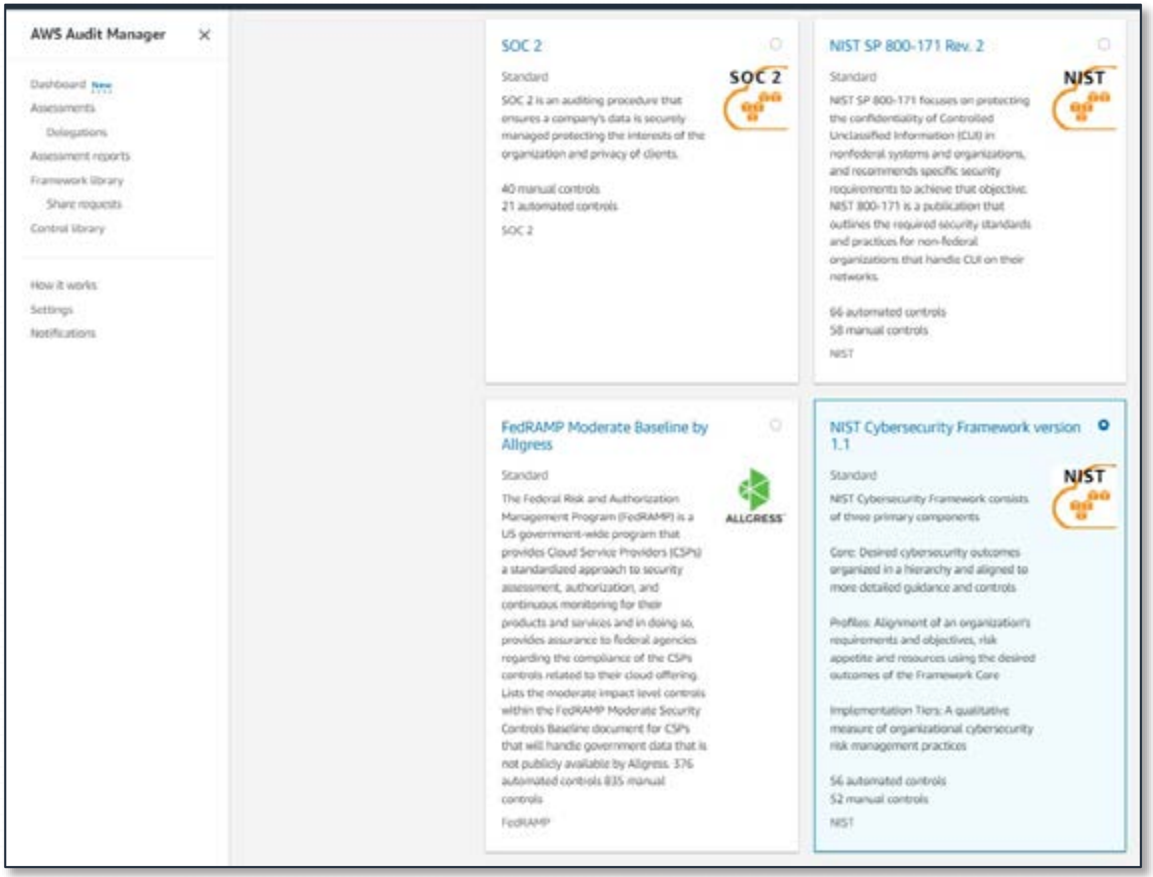
Section 5 of 5

AWS Audit Manager

AWS Audit Manager provides an automated and continuous process for the following:

- Collects evidence of security controls
- Assesses whether controls are operating effectively
- Provides assessment reports to streamline audit preparation

Choose a framework



SOC 2 ○

Standard

SOC 2 is an auditing procedure that ensures a company's data is securely managed protecting the interests of the organization and privacy of clients.

40 manual controls
21 automated controls

SOC 2

NIST SP 800-171 Rev. 2 ○

Standard

NIST SP 800-171 focuses on protecting the confidentiality of Controlled Unclassified Information (CUI) in nonfederal systems and organizations, and recommends specific security requirements to achieve that objective. NIST 800-171 is a publication that outlines the required security standards and practices for non-federal organizations that handle CUI on their networks.

66 automated controls
58 manual controls

NIST

FedRAMP Moderate Baseline by Allgress ○

Standard

The Federal Risk and Authorization Management Program (FedRAMP) is a US government-wide program that provides Cloud Service Providers (CSPs) a standardized approach to security assessment, authorization, and continuous monitoring for their products and services and in doing so, provides assurance to federal agencies regarding the compliance of the CSPs controls related to their cloud offering. Lists the moderate impact level controls within the FedRAMP Moderate Security Controls Baseline document for CSPs that will handle government data that is not publicly available by Allgress. 376 automated controls 835 manual controls

FedRAMP

NIST Cybersecurity Framework version 1.1 ●

Standard

NIST Cybersecurity Framework consists of three primary components

Core: Desired cybersecurity outcomes organized in a hierarchy and aligned to more detailed guidance and controls

Profiles: Alignment of an organization's requirements and objectives, risk appetite and resources using the desired outcomes of the Framework Core

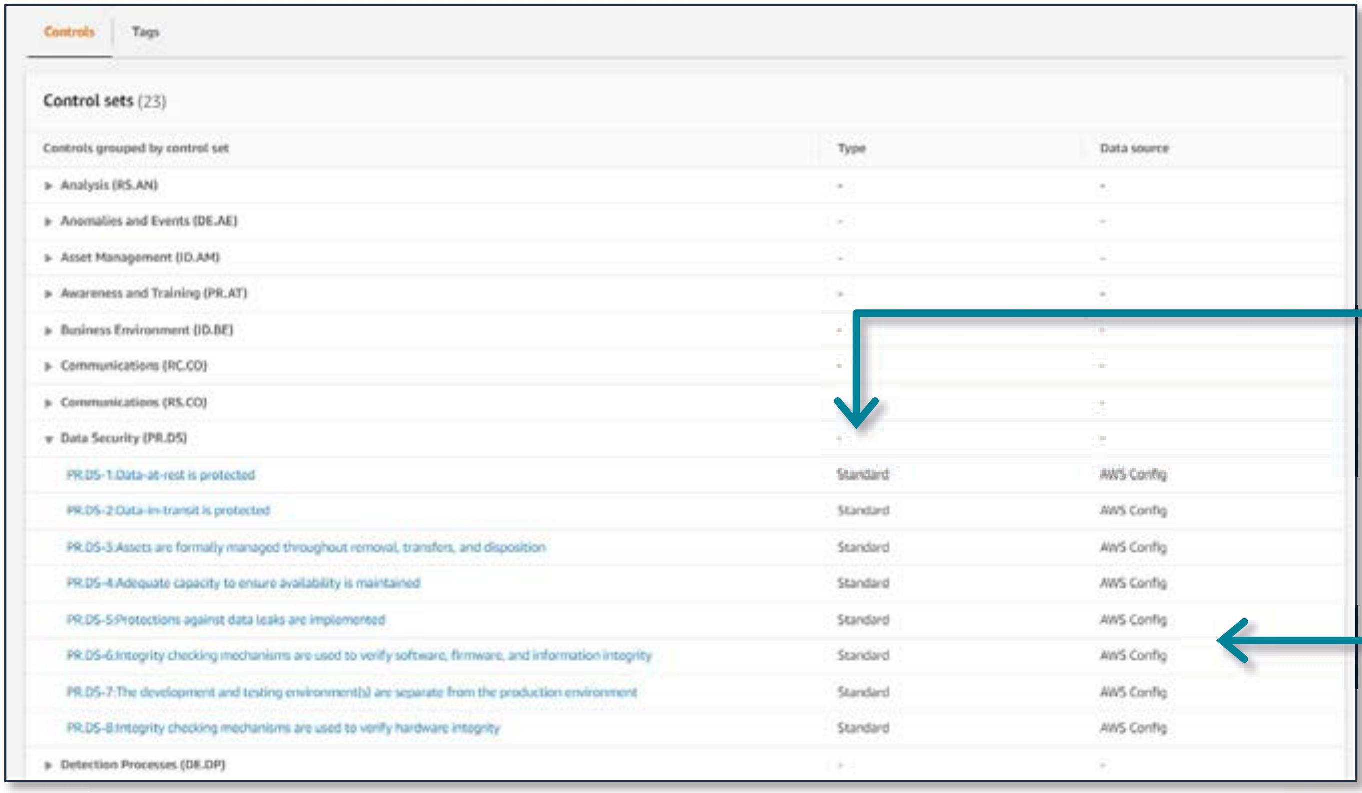
Implementation Tiers: A qualitative measure of organizational cybersecurity risk management practices

56 automated controls
52 manual controls

NIST

- Numerous frameworks are available specific to industry, location-based regulatory guidance, and international standards.
- Here, you can see the NIST Cybersecurity Framework is selected.

Explore framework controls



Control sets (23)

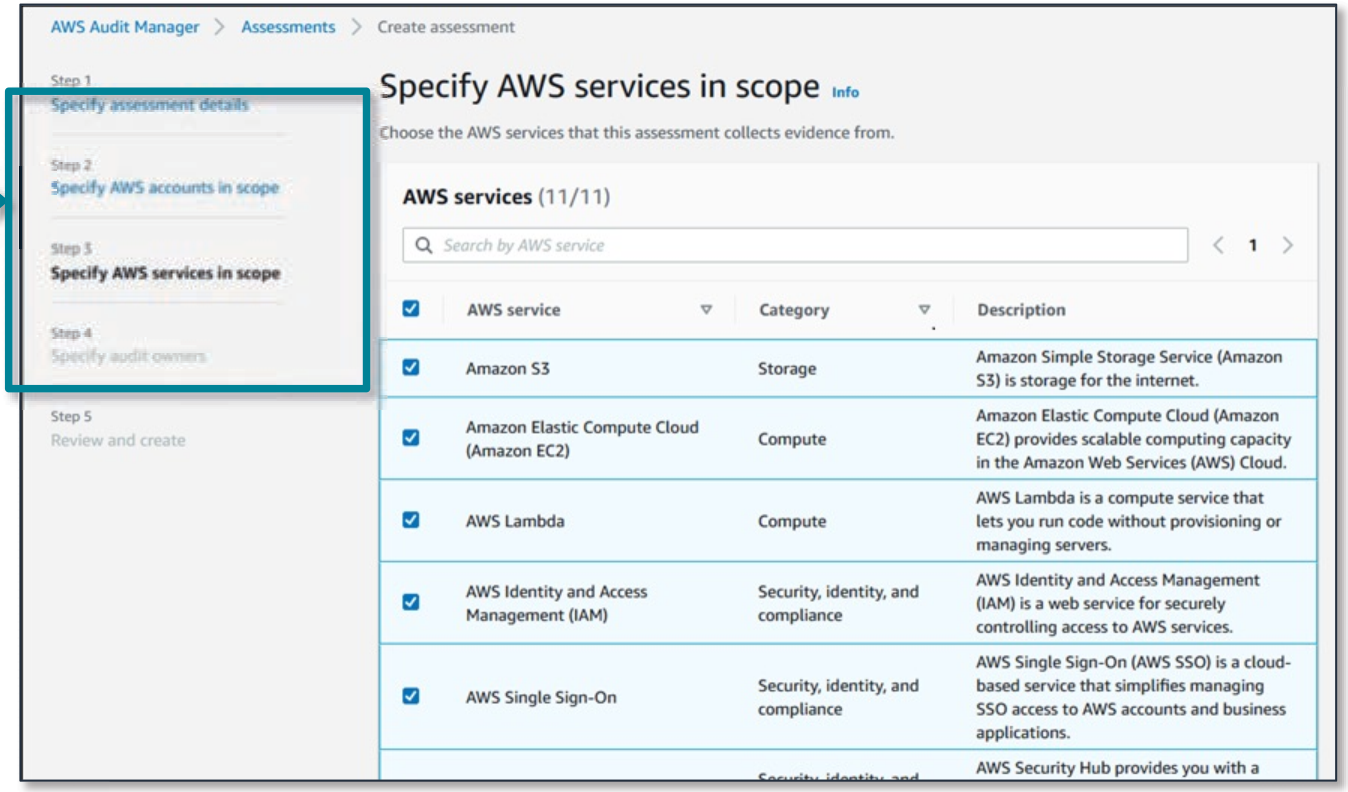
Controls grouped by control set	Type	Data source
▸ Analysis (RS.AN)	-	-
▸ Anomalies and Events (DE.AE)	-	-
▸ Asset Management (ID.AM)	-	-
▸ Awareness and Training (PR.AT)	-	-
▸ Business Environment (ID.BE)	-	-
▸ Communications (RC.CO)	-	-
▸ Communications (RS.CO)	-	-
▾ Data Security (PR.DS)	-	-
PR.DS-1:Data-at-rest is protected	Standard	AWS Config
PR.DS-2:Data-in-transit is protected	Standard	AWS Config
PR.DS-3:Assets are formally managed throughout removal, transfers, and disposition	Standard	AWS Config
PR.DS-4:Adequate capacity to ensure availability is maintained	Standard	AWS Config
PR.DS-5:Protections against data leaks are implemented	Standard	AWS Config
PR.DS-6:Integrity checking mechanisms are used to verify software, firmware, and information integrity	Standard	AWS Config
PR.DS-7:The development and testing environment(s) are separate from the production environment	Standard	AWS Config
PR.DS-8:Integrity checking mechanisms are used to verify hardware integrity	Standard	AWS Config
▸ Detection Processes (DE.DP)	-	-

- Controls are categorized as standard or custom.
- Data source is the service or artifact from which the evidence is derived.

Define audit scope

Select:

- Accounts
- Services
- Audit owners



AWS Audit Manager > Assessments > Create assessment

Step 1
Specify assessment details

Step 2
Specify AWS accounts in scope

Step 3
Specify AWS services in scope

Step 4
Specify audit owners

Step 5
Review and create

Specify AWS services in scope Info

Choose the AWS services that this assessment collects evidence from.

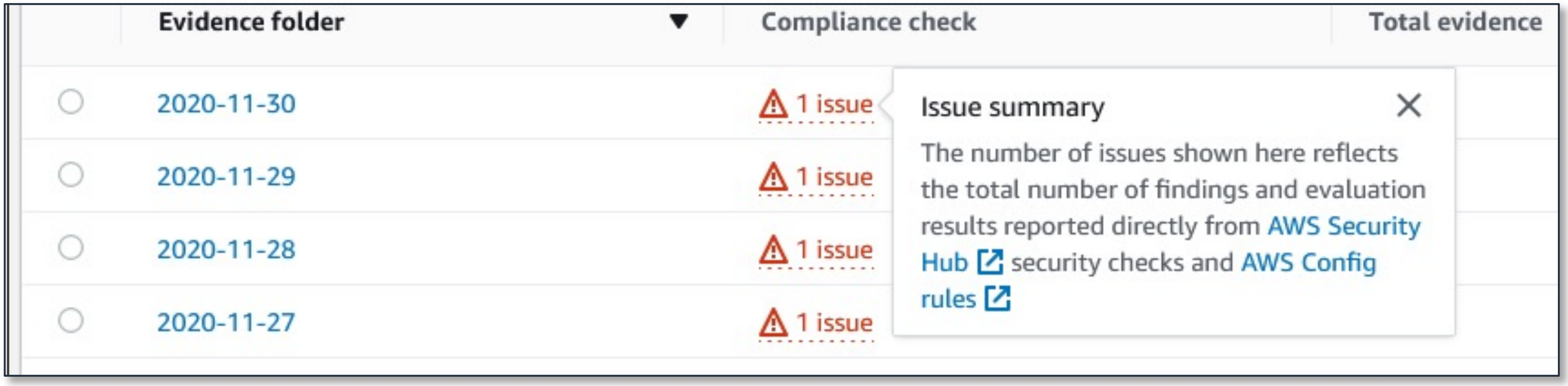
AWS services (11/11)

Search by AWS service

☑	AWS service	Category	Description
☑	Amazon S3	Storage	Amazon Simple Storage Service (Amazon S3) is storage for the internet.
☑	Amazon Elastic Compute Cloud (Amazon EC2)	Compute	Amazon Elastic Compute Cloud (Amazon EC2) provides scalable computing capacity in the Amazon Web Services (AWS) Cloud.
☑	AWS Lambda	Compute	AWS Lambda is a compute service that lets you run code without provisioning or managing servers.
☑	AWS Identity and Access Management (IAM)	Security, identity, and compliance	AWS Identity and Access Management (IAM) is a web service for securely controlling access to AWS services.
☑	AWS Single Sign-On	Security, identity, and compliance	AWS Single Sign-On (AWS SSO) is a cloud-based service that simplifies managing SSO access to AWS accounts and business applications.
		Security, identity, and	AWS Security Hub provides you with a

Gather evidence

- Evidence is automatically collected and stored in folders with a default name of the date it was collected.
- You can also manually upload evidence (this is required by some control types).



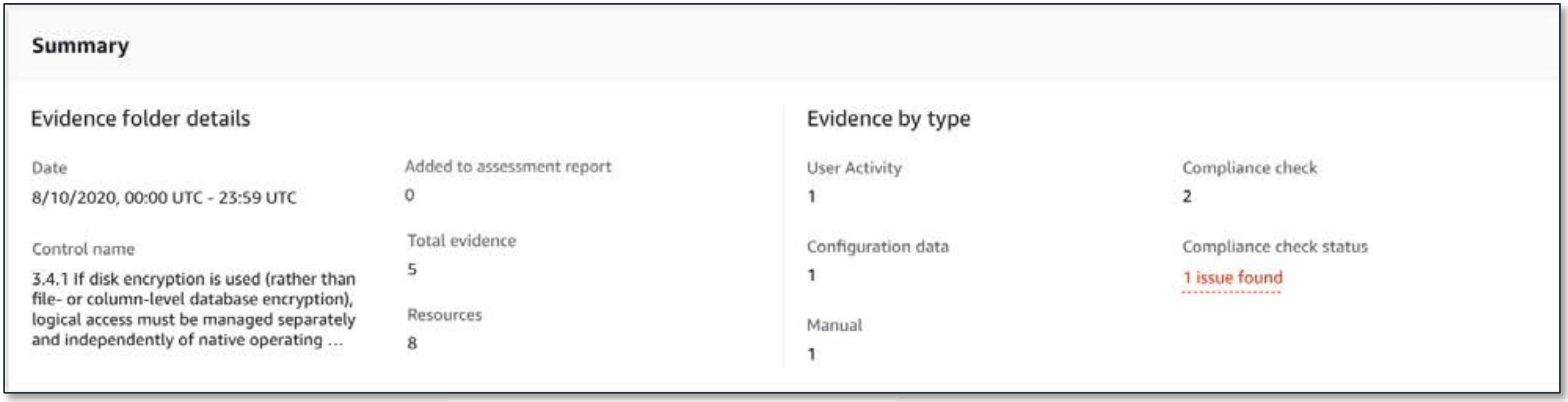
	Evidence folder ▼	Compliance check	Total evidence
○	2020-11-30	⚠ 1 issue	
○	2020-11-29	⚠ 1 issue	
○	2020-11-28	⚠ 1 issue	
○	2020-11-27	⚠ 1 issue	

Issue summary ✕

The number of issues shown here reflects the total number of findings and evaluation results reported directly from AWS Security Hub security checks and AWS Config rules

Evidence summary

- The summary section provides a high-level overview of the items in the evidence folder.



Summary

Evidence folder details

Date
8/10/2020, 00:00 UTC - 23:59 UTC

Control name
3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating ...

Added to assessment report
0

Total evidence
5

Resources
8

Evidence by type

User Activity
1

Configuration data
1

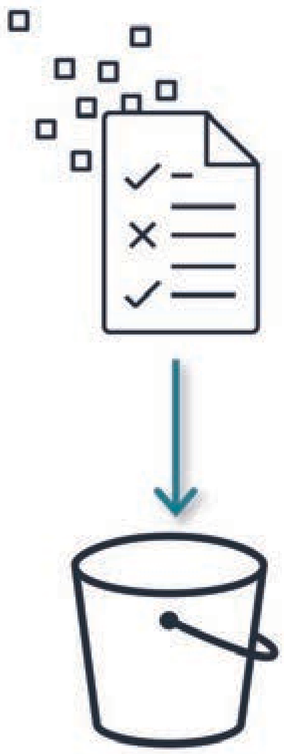
Manual
1

Compliance check
2

Compliance check status
1 issue found

Compile a report

- After you select the evidence to include in your assessment report, you can generate the final assessment report to share with auditors.
- When you generate an assessment report, it is placed into the S3 bucket that you designated as your assessment report destination.



Module 4: Monitoring and Alerting

Remember…

- Use service and application logging.
  - AWS CloudTrail
  - VPC Flow Logs
- Automate response to events as much as possible.
- Some key services and features include the following:
  - CloudWatch Alarms
  - Amazon GuardDuty
  - Security Hub
  - AWS Audit Manager

Let’s check our knowledge with a few questions.

Question 1

Which services can VPC Flow Logs records be published to? (Select TWO)

A. Amazon S3

B. Amazon RDS

C. Amazon DynamoDB

D. Amazon CloudWatch Logs

E. AWS CloudTrail

Answer 1

Which services can VPC Flow Logs records be published to? (Select TWO)

A. (Correct) Amazon S3

B. Amazon RDS

C. Amazon DynamoDB

D. (Correct) Amazon CloudWatch Logs

E. AWS CloudTrail

Question 2

AWS CloudTrail log file integrity validation is invaluable in security and forensic investigations. Which industry standard algorithm is used for validation hashing?

A. MD5

B. SHA-256

C. AES-256

D. DES

Answer 2

AWS CloudTrail log file integrity validation is invaluable in security and forensic investigations. Which industry standard algorithm is used for validation hashing?

A. MD5

B. (Correct) SHA-256

C. AES-256

D. DES

Lab 3: Security Monitoring

By the end of this lab, you will be able to do do the following:

- Configure an Amazon Linux 2 instance to send log files to Amazon CloudWatch
- Create Amazon CloudWatch alarms and notifications to monitor for failed login attempts
- Create Amazon CloudWatch alarms to monitor network traffic through a Network Address Translation (NAT) gateway

Lab duration: 45 minutes

AWS Security Best Practices

Course conclusion

AWS Security Best Practices

Course objectives

Congratulations on completing this course! You have successfully learned and applied your skills to meet the following objectives:

- Design and implement a secure network infrastructure.
- Design and implement compute security.
- Design and implement a logging solution.

Next Steps

Security Engineering on AWS

- Protect your infrastructure against common security threats
- Protect data at rest and in transit with encryption
- Apply security assessments in an automated and reproducible manner
- Configure authentication for resources and applications in the AWS Cloud
- Gain insight into events by monitoring and analyzing logs

One more thing...

- Login to http://aws.training.
- Click My Transcript, then select the Archived tab.
- Find the training completed “AWS Security Best Practices” and click “Evaluate”.

Thank you

All trademarks are the property of their owners.