CCSP

CCSP EXAM CRAM

EXAM PREPARATION SERIES

2023 EDITION

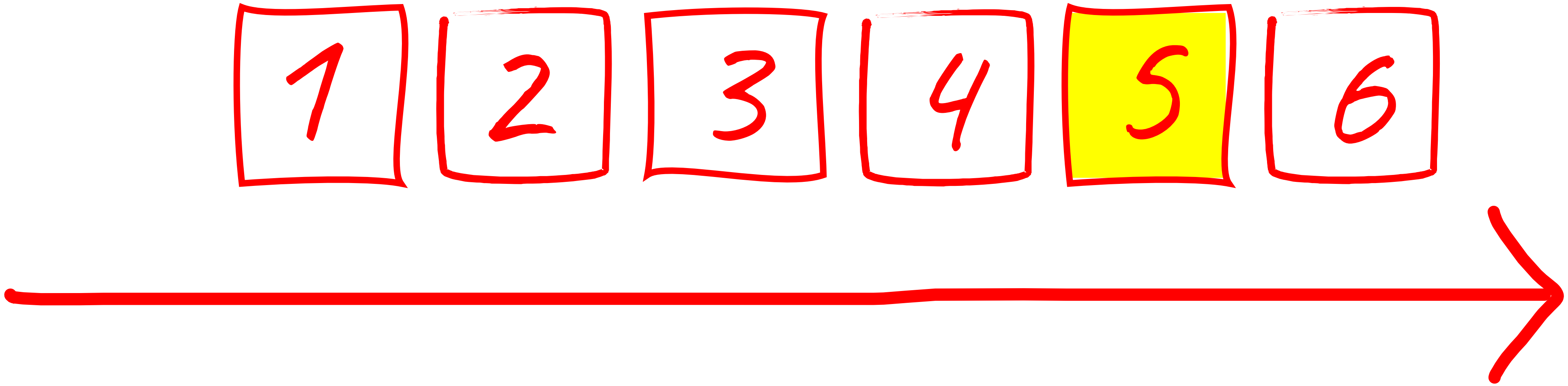
DOMAIN 5

Coverage of every topic in the official exam syllabus!

with **Pete Zerger** vCISO, CISSP, MVP

INTRODUCTION: SERIES OVERVIEW

LESSONS IN THIS SERIES



One lesson for each exam domain

...and a consolidated full course video when the series is complete

EXAM OBJECTIVES (DOMAINS)

DOMAIN	WEIGHT
1. Cloud Concepts, Architecture, and Design	17%
2. Cloud Data Security	20%
3. Cloud Platform and Infrastructure Security	17%
4. Cloud Application Security	17%
5. Cloud Security Operations	**16%**
6. Legal, Risk, and Compliance	13%

Domain 5 is the focus of this video

(ISC)²
CCSP
Certified Cloud Security Professional
Official Study Guide
Third Edition
OFFICIAL
SYBEX

CCSP

CSSP EXAM CRAM

THE COMPLETE COURSE

DOMAIN 5

Cloud Security Operations

INSIDE CLOUD
AND SECURITY

EXAM ESSENTIALS - 5

How to ensure clustered host and guest OS availability

Differences in containerization, serverless, resource schedule, dynamic optimization.

Explain importance of security hygiene practices

Application of security patches, application and maintenance of security baselines.

Standard processes used for IT service management in an org

ITIL, ISO/IEC 20000-1, change management, continuity, incident, problem, availability, etc.

Access control for local and remote system/facility access

Remote access methods (SSH, RDP), jump boxes, bastion hosts, physical access security.

Network security controls as part of a cloud environment

Common security controls like IDS/IPS, honeypots, role of SOC and incident response.

The role of change and configuration management

How these work together, how they differ, how one influences the other.

5. CLOUD SECURITY OPERATIONS

5.1 Implement and Build Physical and Logical Infrastructure for Cloud Environment

Hardware specific security configuration requirements
(e.g., hardware security module (HSM) and Trusted Platform Module (TPM))

Installation and configuration of management tools

Virtual hardware specific security configuration requirements
(e.g., network, storage, memory, central processing unit (CPU), Hypervisor type 1 and 2)

Installation of guest operating system (OS) virtualization toolsets

Trusted Platform Module

"Cryptographic Coprocessor"

A chip that resides on the motherboard of the device.

Multi-purpose, like storage and management of keys used for full disk encryption (FDE) solutions.

Provides the operating system with access to keys, but prevents drive removal and data access

Virtual TPMs are part of the hypervisor and provided to VMs running on a virtualization platform.

HARDWARE SPECIFIC SECURITY

Trusted Platform Module

"Cryptographic Coprocessor"

A chip that resides on the motherboard of the device.

Multi-purpose, like storage and management of keys used for full disk encryption (FDE) solutions.

Provides the operating system with access to keys, but prevents drive removal and data access

Unlike an HSM, it is generally a physical component of the system hardware and cannot be added or removed at a later date.

HARDWARE SPECIFIC SECURITY

Hardware Root of Trust

When certificates are used in FDE, they use a hardware root of trust for key storage.

It verifies that the keys match before the secure boot process takes place

TPM is often used as the basis for a hardware root of trust

Hardware Security Module (HSM)

a physical computing device that safeguards and manages digital keys, performs encryption and decryption functions for digital signatures, strong authentication and other cryptographic functions.

Like a TPM, but are often removable or external devices

Hardware Security Module (HSM)

a physical computing device that safeguards and manages digital keys, performs encryption and decryption functions for digital signatures, strong authentication and other cryptographic functions.

Key Escrow uses an HSM to store and manage private keys

Hardware Security Module (HSM)

Cloud Service Providers all offer a cloud-based HSM solution for customer-managed key scenarios

EXAMPLES: Dedicated HSM (Azure), CloudHSM (AWS), Google KMS (GCP)

SOFTWARE DEFINED NETWORKS

Supports CI/CD and micro-segmentation

SDN

Software Defined Networks

a network architecture approach that enables the network to be intelligently and centrally controlled, or ‘programmed,’ using software

and has capacity to reprogram the data plane at any time

use cases include **SD-LAN** and **SD-WAN**

separating the control plane from the data plane opens up a number of security challenges

SDN vulnerabilities can include man-in-the-middle attack (MITM) and a service denial (DoS) secure with TLS!

CLOUD SECURITY CONTROLS - NETWORK

Segmentation of virtual networks, both public and private subnets, are important elements of cloud network security.

Virtual Private Cloud (VPC)

A virtual network that consists of cloud resources, where the VMs for one company are isolated from the resources of another company.

Separate VPCs can be isolated using public and private networks.

Public and Private Subnets

The environment needs to be segmented public subnets that can access the Internet directly (through a firewall) and protected private networks.

Virtual networks can be connected to other networks with a VPN gateway or network peering.

For VDI/client scenarios, a NAT gateway for Internet access makes sense.

INSTALLATION AND CONFIGURATION OF MANAGEMENT TOOLS

Management tooling considerations on cloud infrastructure:

Redundancy: Any critically important tool can be a single point of failure (SPOF), so adequate planning for redundancy should be performed.

Scheduled downtime and maintenance: Downtime may not be acceptable, so these tools may be patched or taken offline for maintenance on a rotating schedule with migration of live VMs to prevent loss of service.

Isolated network and robust access controls: Access to virtualization management tools should be tightly controlled, with adequate enforcement.

e.g. Need-to-know, least privilege, encryption, and VPN access

Configuration management and change management: Tools and the infrastructure that supports them should be placed under configuration management to ensure that they stay in a known, hardened state.

Logging and monitoring: Audit trail is important, but logging activities can create additional overhead, which may not be appropriate for all systems.

VIRTUAL HARDWARE-SPECIFIC SECURITY CONFIGURATION

a VM shares physical hardware with potentially hundreds of other VMs

The biggest issue related to virtual hardware security is enforcement

For the hypervisor, strict segregation between the guest operating systems running on a single host

There are two main forms of control you should be aware of:

Configuration: Ensure that the hypervisor has been configured correctly to provide the minimum necessary functionality

Disallowing inter-VM network communications if not required and encrypting VM snapshots

Patching: The customer should patch VMs (IaaS) while CSP patches the hypervisor. In PaaS, the CSP owns VM patching

VIRTUAL HARDWARE-SPECIFIC SECURITY CONFIGURATION

Particular concerns for virtual network security controls include:

Virtual Private Cloud (VPC): gives the customer a greater level of control, including managing private non-routable IP addresses and control over inter-VM communication.

Enables granular network segmentation in a ZTNA

Security Groups: a security group is similar to an access control list (ACL) for network access.

They have distinct rules for inbound and outbound traffic.

e.g. security group (AWS), network security group (Azure)

CCSP

CSSP EXAM CRAM

THE COMPLETE COURSE

DEMO

Secure virtual networks with security groups

EXAMPLE FOR CONTEXT:

Features will vary by CSP

INSIDE CLOUD AND SECURITY

GUEST OPERATING SYSTEM VIRTUALIZATION TOOLSETS

Virtualization toolsets installed on the VM

Toolsets exist that can provide extended functionality for various guest operating systems (Linux, Windows, etc.).

For example, Hyper-V integration services enhance VM performance and provide several useful features.

e.g. Guest file copy, time sync, guest shutdown

In a public cloud, these toolsets will typically, be provided by the CSP

5. CLOUD SECURITY OPERATIONS

5.2 Operate Physical and Logical Infrastructure for Cloud Environment

Access controls for local and remote access
(e.g. Remote Desktop Protocol (RDP), secure terminal access, Secure Shell (SSH), console-based access mechanisms, jumpboxes, virtual client)

Secure network configuration
(e.g., virtual local area networks (VLAN), Transport Layer Security (TLS), Dynamic Host Configuration Protocol (DHCP), Domain Name System Security Extensions (DNSSEC), virtual private network (VPN), Chain of Custody and Non-repudiation

5. CLOUD SECURITY OPERATIONS

5.2 Operate Physical and Logical Infrastructure for Cloud Environment

Network security controls
(e.g., firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), honeypots, vulnerability assessments, network security groups, bastion host)

Operating system (OS) hardening through the application of baselines, monitoring and remediation
(e.g., Windows, Linux, VMware)

Patch Management

5. CLOUD SECURITY OPERATIONS

5.2 Operate Physical and Logical Infrastructure for Cloud Environment

Infrastructure as Code (IaC) strategy

Availability of clustered hosts
(e.g. distributed resource scheduling, dynamic optimization, storage clusters, maintenance mode, high availability (HA))

Availability of guest operating system (OS)

Performance and capacity monitoring
(e.g. network, compute, storage, response time)

5. CLOUD SECURITY OPERATIONS

5.2 Operate Physical and Logical Infrastructure for Cloud Environment

Hardware monitoring
(e.g., disk, central processing unit (CPU), fan speed, temperature)

Configuration of host and guest operating system (OS) backup and restore functions

Management plane
(e.g., scheduling, orchestration, maintenance)

5.2 Operate Physical and Logical Infrastructure for Cloud Environment

Access controls for local and remote access
(e.g. Remote Desktop Protocol (RDP), secure terminal access, Secure Shell (SSH), console-based access mechanisms, jumpboxes, virtual client)

Secure network configuration
(e.g., virtual local area networks (VLAN), Transport Layer Security (TLS), Dynamic Host Configuration Protocol (DHCP), Domain Name System Security Extensions (DNSSEC), virtual private network (VPN))Chain of Custody and Non-repudiation

5. CLOUD SECURITY OPERATIONS

5.2 Operate Physical and Logical Infrastructure for Cloud Environment

5.2.1 **Access controls for local and remote access**
(e.g. Remote Desktop Protocol (RDP), secure terminal access, Secure Shell (SSH), console-based access mechanisms, jumpboxes, virtual client)

Secure network configuration
(e.g., virtual local area networks (VLAN), Transport Layer Security (TLS), Dynamic Host Configuration Protocol (DHCP), Domain Name System Security Extensions (DNSSEC), virtual private network (VPN),Chain of Custody and Non-repudiation

ACCESS CONTROLS FOR REMOTE ACCESS

Local and Remote Access Methods

Remote Desktop Protocol (RDP): the native remote access protocol for Windows operating systems.

Secure Shell (SSH): the native remote access protocol for Linux operating systems, and common for remote management of network devices.

RDP and SSH both support encryption and MFA

Secure Terminal/Console-Based Access: a system for secure local access.

A KVM (keyboard video mouse) system with access controls

Jumpboxes: a bastion host at the boundary of lower and higher security zones.

CSPs offer services for this: Azure Bastion, AWS Transit Gateway

Virtual Clients: software tools that allow remote connection to a VM for use as if it is your local machine.

e.g. Virtual Desktop Infrastructure (VDI) for contractors

Access to any of these can be gated with a **privileged access management PAM)** solution on the IAM platform used by the CSP

VIRTUAL PRIVATE NETWORK (VPN)

Extends a private network across a public network, enabling users and devices to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.

Split tunnel vs full tunnel

Full tunnel means using VPN for all traffic, both to the Internet and corporate network.

Split tunnel uses VPN for traffic destined for the corporate network only, and Internet traffic direct through its normal route.

Remote access vs site-to-site

In site-to-site, IPSec site-to-site VPN uses an always on mode where both packet header and payload are encrypted. IPSec tunnel mode

In a remote access scenario, a connection is initiated from a users PC or laptop for a connection of shorter duration. IPSec transport mode

Local and Remote Access Controls

Session Encryption: Data transmitted in remote access sessions must be encrypted using strong protocols such as TLS 1.3 and session keys.

Strong Authentication: May be combined with cryptographic controls such as a shared secret key for SSH and/or MFA

Strong MFA factors, device state, and other conditions of access

Enhanced logging and reviews: All admin accounts should be subject to additional logging and review of activity, and frequent access reviews.

Privileged access solutions in IDaaS often include access reviews

Use of identity and access management tool: Many CSPs offer Identity-as-a-Service (IDaaS) that enables strong authentication and access controls schemes

Examples include Azure Active Directory, Google Identity Services

Single Sign-On (SSO): IDaaS solutions enable users to log into other services using their company accounts. Many IDaaS solutions function as an SSO provider.

Local and Remote Access Controls

Separate privileged and nonprivileged accounts:

A general best practice for administrative users is the use of a dedicated admin account for sensitive functions and a standard account for day-to-day use.

While listed in the CBK for the CCSP, this is NOT always true

Increasingly, IDaaS solutions offer a Privileged Identity Management (PIM) or Privileged Access Management (PAM) for just-in-time privilege elevation.

Solution features

These solutions typically offer:

-Temporary elevation of privilege

-Approval gates

-An audit trail when privilege is activated

-An access review process (to avoid permissions sprawl)

CCSP

CSSP EXAM CRAM

THE COMPLETE COURSE

DEMO

Privileged Access Management (PAM)

EXAMPLE FOR CONTEXT:
Features will vary by CSP

INSIDE CLOUD
AND SECURITY

5. CLOUD SECURITY OPERATIONS

5.2 Operate Physical and Logical Infrastructure for Cloud Environment

Access controls for local and remote access
(e.g. Remote Desktop Protocol (RDP), secure terminal access, Secure Shell (SSH), console-based access mechanisms, jumpboxes, virtual client)

Secure network configuration

5.2.2 (e.g., virtual local area networks (VLAN), Transport Layer Security (TLS), Dynamic Host Configuration Protocol (DHCP), Domain Name System Security Extensions (DNSSEC), virtual private network (VPN),Chain of Custody and Non-repudiation

Zero Trust Security

no entity is trusted by default!

Addresses the limitations of the legacy network perimeter-based security model.

Treats user identity as the control plane

Assumes compromise / breach in verifying every request.

ZERO TRUST NETWORK ARCHITECTURE

-Network Security Group (NSG)

-Network **Firewalls**

-Inbound and outbound **traffic filtering**

-Inbound and outbound **traffic inspection**

-Centralized **security policy** management and enforcement

NETWORK SECURITY

Network security groups provide an additional layer of security for cloud resources

Act as a virtual firewall for virtual networks and resource instances. (e.g. VMs, databases, subnets)

Carries a list of security rules (IP and port ranges) that allow or deny network traffic to resource instances.

Provides a virtual firewall for a collection of cloud resources with the same security posture.

Exists in multiple CSPs. Details may vary slightly with each.

CLOUD SECURITY CONTROLS - NETWORK

Segmentation

Restricting services that are permitted to access or be accessible from other zones using rules to control inbound/outbound traffic.

Rules are enforced by the IP address ranges of each subnet.

Within a virtual network, segmentation can be used to achieve isolation. Port filtering through a network security group

CLOUD SECURITY CONTROLS - NETWORK

Private Subnets

Not for public services (like websites)

Our VPC contains private subnets. Each of these subnets has its own CIDR IP address range and cannot connect directly to the internet.

They could be configured go through the NAT gateway if outbound internet connectivity is desired.

Client VMs and database servers will often be hosted in a private subnet.

The private subnet will use one of the following IP address ranges:

10.0.0.0
172.16.x.x – 172.31.x.x
192.168.0.0

Private IP ranges are defined in RFC 1918

All other IP address ranges, except the APIPA 169.254.x.x, are public addresses.

SECURE NETWORK DESIGN

East-West Traffic

where traffic moves laterally between servers within a data center.

north-south traffic moves outside of the data center.

VLAN

Virtual Local Area Network

a collection of devices that communicate with one another as if they made up a single physical LAN.

Creates a distinct broadcast domain

Screened Subnet

aka "DMZ":

a subnet is placed between two routers or firewalls.

bastion host(s) are located within that subnet.

VLAN

VLAN

Many public clouds offer a **virtual private cloud (VPC)** which is essentially a sandboxed area within the larger public cloud dedicated to a specific customer.

VPCs take the form of a dedicated VLAN for a specific user organization, which means other cloud tenants are blocked from accessing resources in the VPC.

VPC Connectivity

To create a secure connection to your VPC, you can connect a VPN using L2TP/IPsec using a VPN gateway (aka transit gateway).

Network peering is another method for connecting virtual networks in the cloud.

Peering is the more common option between cloud networks

Site-to-site VPN common for on-premises to cloud connectivity

DNS SECURITY

DNSSEC

DNS Security Extensions

A set of specifications primarily aimed at reinforcing the integrity of DNS

Achieves this by providing for cryptographic authentication of DNS data using digital signatures

Provides proof of origin and makes cache poisoning and spoofing attacks more difficult

Does not provide for confidentiality, since digital signatures rely on publicly decryptable information

PROTECTING DATA IN MOTION

How can we encrypt different types of data **in motion**?

> Data in motion is most often encrypted using **TLS** or **HTTPS**
>
> This is typically how a session is encrypted before a user enters the credit card details.

TLS uses an x.509 certificate with a public/private key pair

DYNAMIC HOST CONFIGURATION PROTOCOL

DHCP

Dynamic Host Configuration Protocol

The IP address associated with a system event can be used when identifying a user or system

With proper DHCP logs, a SIEM can leverage this data to track an IP address to a specific endpoint

Some hypervisors offer a feature to limit which network cards are eligible to perform DHCP offer

This prevents rogue DHCP servers from issuing IPs to clients and servers

METHODS TO PROVIDE NON-REPUDIATION

Non-repudiation is **the guarantee that no one can deny a transaction.**

Digital Signatures prove that a digital message or document was not modified—intentionally or unintentionally—from the time it was signed.

based on asymmetric cryptography (a public/private key pair)

the digital equivalent of a handwritten signature or stamped seal.

message authentication code (MAC). the two parties that are communicating can verify non-repudiation using a session key

Electronic financial transfers (EFTs) frequently use MACs to preserve data integrity.

Hash-based message authentication code (HMAC) is a special type of MAC with a cryptographic hash function AND a secret cryptographic key

HTTPS, SFTP, FTPS, and other transfer protocols use HMAC

METHODS TO PROVIDE NON-REPUDIATION

Cryptographic Key Establishment and Management

Cryptography provides a number of security functions including confidentiality, integrity, and nonrepudiation.

Encryption tools like TLS or a VPN can be used to provide confidentiality.

Hashing can be implemented to detect unintentional data modifications. integrity

Additional security measures like **digital signatures** or hash-based message authentication code (HMAC) can be used to detect intentional tampering.

HMAC can simultaneously verify both data integrity and message authenticity

5. CLOUD SECURITY OPERATIONS

5.2 Operate Physical and Logical Infrastructure for Cloud Environment

5.2.3 **Network security controls**
(e.g., firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), honeypots, vulnerability assessments, network security groups, bastion host)

Operating system (OS) hardening through the application of baselines, monitoring and remediation
(e.g., Windows, Linux, VMware)

Patch Management

BASTION HOST

A dedicated host for secure admin access

Bastion Host

A host used to allow administrators to access a private network from a lower security zone

Will have a network interface in both the lower and higher security zones

Will be secured at the same level as the higher security zone it's connected to.

"Jumpbox" or "jump server" two common names for bastion hosts

CSPs offer services for this: Azure Bastion, AWS Transit Gateway

NETWORK SECURITY CONTROLS

Basic familiarity with functionality and stengths of each

Firewalls

-Stateless and stateful
-Application, host, and virtual
-Web application (WAF)
-Next generation (NGFW)

Intrusion Detection and Prevention Systems (IDS, IPS)

-Host-based (HIDS and HIPS)
-Network (NIDS and NIPS)
-Hardware vs Software

Other Security Controls

-Honeypot
-Vulnerability assessments

We'll cover all these in detail in section 5.6

5. CLOUD SECURITY OPERATIONS

5.2 Operate Physical and Logical Infrastructure for Cloud Environment

Network security controls
(e.g., firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), honeypots, vulnerability assessments, network security groups, bastion host)

5.2.4 **Operating system (OS) hardening through the application of baselines, monitoring and remediation**
(e.g., Windows, Linux, VMware)

Patch Management

OS Hardening

Hardening is the configuration of a machine into a secure state through application of a configuration baseline.

Baselines can be applied to a single VM image, or to a VM template created that is then used to deploy all VMs.

A hardened VM image may be customer-defined, CPS-defined, or from a third party, often available through a cloud marketplace.

The Center for Internet Security (CIS) offers hardened VM images in CSP marketplaces

BASELINES, BENCHMARKS, AND CONTROLS

Control

a high-level description of a feature or activity that needs to be addressed and is not specific to a technology or implementation.

Is expressed as

Benchmark

contains security recommendations for a specific technology, such as an IaaS VM.

and implemented through a

Baseline

is the implementation of the benchmark on the individual service.

BENCHMARKS/SECURE CONFIGURATION GUIDES

Benchmarks describe configuration baselines and best practices for securely configuring a system.

Platform-/Vendor-Specific Guides: released with new products so that they can be set up as securely as possible, making them less vulnerable to attack.

Web Servers: the two main web servers used by commercial companies are Microsoft's **Internet Information Server (IIS)**, and the Linux-based **Apache**.

Because they are public-facing, they are prime targets for hackers.

To help reduce the risk, both Microsoft and Apache provide security guides to help security teams reduce the attack surface, making them more secure.

These guides advise updates being in place, unneeded services are disabled, and the operating system is hardened to minimize risk of security breach.

BENCHMARKS/SECURE CONFIGURATION GUIDES

Benchmarks describe configuration baselines and best practices for securely configuring a system.

Operating Systems: Most vendors, such as Microsoft, have guides that detail the best practices for installing their operating systems.

OS benchmarks are also available from CIS and others

Application Server: Vendors produce guides on how to configure application servers, such as email servers or database servers, to make them less vulnerable to attack.

Network Infrastructure Devices: companies like Cisco produce network devices and offer benchmarks for secure configuration.

Benchmarks aim to ease process of securing a component, reduce attack footprint, and minimize risk of security breach.

OS HARDENING

Open ports and services

listening ports should be restricted to those necessary, filtered to restrict traffic, and disabling some ports entirely if unneeded.

Block through firewalls, disable by disabling underlying service.

Registry

access should be restricted, and updates controlled through policy where possible.

always take a backup of the registry before you start making changes.

Disk encryption

drive encryption can prevent unwanted access to data in a variety of circumstances. Using full disk encryption (Bitlocker or dm-crypt)

OS (Operating System)

OS hardening can often be implemented through security baselines

Can be applied through group policies or management tools (like MDM)

Baselines can implement all the above

BASELINE OPTIONS

for operating system hardening

Vendor-supplied baselines. Microsoft, VMware, and some Linux creators offer configuration guidelines for their products that point out specific security options and recommended settings.

DISA STIGs. The U.S. Defense Information Systems Agency (DISA) produces baseline documents known as Security Technical Implementation Guides (STIGs).

WARNING: DISA STIGs may include configurations that are too restrictive for many organizations.

NIST checklists. The National Institute of Technology and Standards maintains a repository of configuration checklists for various OS and application software.

CIS benchmarks. The Center for Internet Security (CIS) publishes baseline guides for a variety of operating systems, applications, and devices, which incorporate many security best practices.

CIS benchmark scripts are priced based on environment size

5. CLOUD SECURITY OPERATIONS

5.2 Operate Physical and Logical Infrastructure for Cloud Environment

Network security controls
(e.g., firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), honeypots, vulnerability assessments, network security groups, bastion host)

Operating system (OS) hardening through the application of baselines, monitoring and remediation
(e.g., Windows, Linux, VMware)

5.2.5 **Patch Management**

PATCH MANAGEMENT

Patch Management

aka "update management"

ensures that systems are kept up-to-date with current patches.

process will evaluate, test, approve, and deploy patches.

system audits verify the deployment of approved patches to system

patch both native OS and 3rd party apps

apply out-of-band updates promptly.

Cloud service providers (CSP) generally provide a patch management feature tailored to their IaaS offering.

5. CLOUD SECURITY OPERATIONS

5.2 Operate Physical and Logical Infrastructure for Cloud Environment

5.2.6 Infrastructure as Code (IaC) strategy

Availability of clustered hosts
(e.g. distributed resource scheduling, dynamic optimization, storage clusters, maintenance mode, high availability (HA))

Availability of guest operating system (OS)

Performance and capacity monitoring
(e.g. network, compute, storage, response time)

INFRASTRUCTURE AS CODE

IaC

Infrastructure as Code

is the management of infrastructure (networks, VMs, load balancers, and connection topology) described in code

just as the same source code generates the same binary, code in the IaC model results in the same environment every time it is applied.

IaC is a key DevOps practice and is used in conjunction with continuous integration and continuous delivery (CI/CD).

IaC is very common (the standard) in the cloud

INFRASTRUCTURE AS CODE

Cloud-Native Controls

Platforms like Microsoft Azure and Amazon Web Services (AWS) have their own tools, such as **Azure Resource Manager (ARM)** and **AWS Cloud Formation**.

These tools make managing Microsoft and AWS cloud resources easier, supporting Infrastructure-as-Code.

Separate tools, for separate platforms, platform-specific

Third-Party Solutions

Third-party tools adds more flexibility, functionality, and multi-platform support.

Organizations will typically move to third-party IaC solutions when the native cloud solutions do not meet their functionality needs.

For example, some organizations move to **Terraform** for infrastructure-as-Code because it supports the major CSPs using a single language .

CSPs offer a marketplace where third-parties can publish offers

INFRASTRUCTURE AS CODE

These characteristics help reduce errors and configuration drift

There are two distinct characteristics of infrastructure-as-code (IaC) that improve resiliency in IaaS and PaaS service models:

Declarative | IaC must know the current state; it must know whether the infrastructure already exists to know whether to create it or not.

Imperative deployment methodologies are unaware of current state

Idempotent | Deployment of an IaC template can be applied multiple times without changing the results.

If the IaC template says, "deploy 4 VMs"" and 3 exist, 1 more is deployed

5. CLOUD SECURITY OPERATIONS

5.2 Operate Physical and Logical Infrastructure for Cloud Environment

Infrastructure as Code (IaC) strategy

5.2.7 **Availability of clustered hosts**
(e.g. distributed resource scheduling, dynamic optimization, storage clusters, maintenance mode, high availability (HA))

Availability of guest operating system (OS)

Performance and capacity monitoring
(e.g. network, compute, storage, response time)

AVAILABILITY OF CLUSTERED HOSTS

Cluster advantages include high availability via redundancy, optimized performance via distributed workloads, and the ability to scale resources

Cluster management agent

Often part of hypervisor or load balancer software, is responsible for mediating access to shared resources in a cluster.

Reservations are guarantees for a certain minimum level of resources available to a specified virtual machine.

A **limit** is a maximum allocation.

A **share** is a weighting given to a particular VM

Share value is used to calculate percentage-based access pooled resources when there is contention.

AVAILABILITY OF CLUSTERED HOSTS

Cluster advantages include high availability via redundancy, optimized performance via distributed workloads, and the ability to scale resources

Distributed Resource Scheduling (DRS) is the coordination element in a cluster of VMware ESXi hosts

DRS mediates access to the physical resources.

Handles resources available to a cluster, reservations and limits for the VMs running on the cluster, and maintenance features.

Dynamic Optimization is Microsoft's DRS equivalent delivered through their cluster management software.

Storage clusters pool storage, providing reliability, increased performance, or possibly additional capacity.

CSP owned in public cloud, org owned in a private cloud

5. CLOUD SECURITY OPERATIONS

5.2 Operate Physical and Logical Infrastructure for Cloud Environment

Infrastructure as Code (IaC) strategy

Availability of clustered hosts
(e.g. distributed resource scheduling, dynamic optimization, storage clusters, maintenance mode, high availability (HA))

5.2.8 **Availability of guest operating system (OS)**

Performance and capacity monitoring
(e.g. network, compute, storage, response time)

AVAILABILITY OF GUEST OPERATING SYSTEM

Guest OS availability in the cloud (IaaS VMs)

Guest OS availability

Once a VM is created in IaaS, the CSP no longer has direct control over the OS.

Customer can use baselines, backups, and cloud storage features to provide resiliency of the guest OS.

e.g. vendor supplied OS baseline templates, cloud storage redundancy (zone or geo-redundancy) features

Backup and recovery

In virtualized cloud infrastructure, this might involve the use of snapshots.

CSPs offer backup features for VMs in the IaaS model

AVAILABILITY OF GUEST OPERATING SYSTEM

Guest OS availability in the context of the cloud (IaaS)

Resiliency

Resiliency is achieved by architecting systems to handle failures from the outset rather than needing to be recovered.

For example, virtualization host clusters with live migration provide resiliency

Resiliency of the physical hypervisor cluster, networks, and storage are responsibility of the CSP

5. CLOUD SECURITY OPERATIONS

5.2 Operate Physical and Logical Infrastructure for Cloud Environment

Infrastructure as Code (IaC) strategy

Availability of clustered hosts
(e.g. distributed resource scheduling, dynamic optimization, storage clusters, maintenance mode, high availability (HA))

Availability of guest operating system (OS)

5.2.9 **Performance and capacity monitoring**
(e.g. network, compute, storage, response time)

PERFORMANCE AND CAPACITY MONITORING

CSP should implement monitoring to ensure that they are able to meet customer demands and promised capacity.

Consumer should monitor to ensure CSP is meeting their obligations

Most monitoring tasks will be in support of the availability objective.

Alerts should be generated based on established thresholds and appropriate response plans initiated.

"CORE 4": Monitoring should include utilization, performance, and availability of 1) CPU, 2) memory, 3) storage and 4) network.

If it's not used, it's wasted and increasing costs!

💡 Just as reviews make log files impactful, appropriate use of performance data is also essential.

5.2 Operate Physical and Logical Infrastructure for Cloud Environment

5.2.10 **Hardware monitoring**
(e.g., disk, central processing unit (CPU), fan speed, temperature)

Configuration of host and guest operating system (OS) backup and restore functions

Management plane
(e.g., scheduling, orchestration, maintenance)

HARDWARE MONITORING

Physical hardware is necessary to provide all the services that enable the virtualization that enables cloud computing.

Hardware monitoring should monitor: CPU, RAM, fans, disk drives, and network components

Environmental: Computing components are not designed for use in very hot, humid, or wet environments.

HVAC, temperature, and humidity monitoring are important.

In public cloud, hardware monitoring will be the responsibility of the CSP and not the consumer.

5. CLOUD SECURITY OPERATIONS

5.2 Operate Physical and Logical Infrastructure for Cloud Environment

Hardware monitoring
(e.g., disk, central processing unit (CPU), fan speed, temperature)

5.2.11 **Configuration of host and guest operating system (OS) backup and restore functions**

Management plane
(e.g., scheduling, orchestration, maintenance)

Responsibility by category

SaaS. CSP retains full control over backup and restore and will often have SLA restore commitments.

Customer typically has shared responsibility for their data

PaaS. Shared responsibility: CSP owns infrastructure backups, consumer owns backups of their data.

IaaS. Consumer owns backup/recovery of VMs.

Consumer backups may include full backups, snapshots, or definition files used for infrastructure as code deployments

Considerations

Sensitive data may be stored in backups.

Access controls and need-to-know principles to limit exposure

Physical separation: backups should be stored on different hardware or availability zones.

Zone redundant or geo-redundant cloud storage

Integrity of all backups should be verified routinely to ensure that they are usable.

5.2 Operate Physical and Logical Infrastructure for Cloud Environment

Hardware monitoring
(e.g., disk, central processing unit (CPU), fan speed, temperature)

Configuration of host and guest operating system (OS) backup and restore functions

5.2.12 **Management plane**
(e.g., scheduling, orchestration, maintenance)

MANAGEMENT PLANE

Management
PLANE

Provides virtual management options analogous to physical admin options of a legacy datacenter

e.g. powering VMs on and off, provisioning virtual infrastructure for VMs like RAM and storage

Orchestration is the automated configuration and management of resources in bulk

Patch management and VM reboots are commonly orchestrated tasks

The **management console** is the web-based consumer interface for managing resources

CSP must ensure management portal calls to the management plane only allow customer access to their own resources.

5. CLOUD SECURITY OPERATIONS

5.3 Implement Operational Controls and Standards (e.g., ITIL, ISO/IEC 20000-1)

Change management

Continuity management

Information security management

Continual service improvement mgmt

Incident management

Problem management

Release management

Deployment management

5. CLOUD SECURITY OPERATIONS

5.3 Implement Operational Controls and Standards (e.g., ITIL, ISO/IEC 20000-1)

Configuration management

Service level management

Availability management

Capacity management

OPERATIONAL CONTROLS AND STANDARDS

ISO/IEC 20000-1

Specifies requirements for "establishing, implementing, maintaining and continually improving a service management system(SMS)”

Supports management of the service lifecycle, including planning, design, transition, delivery and service improvement

Configuration, Change & Asset Management

Change Control

refers to the process of evaluating a change request within an organization and deciding if it should go ahead.

requests are sent to the **Change Advisory Board (CAB)** to ensure that it is beneficial to the company.

requires changes to be requested, approved, tested, and documented.

Change Management

policy that details how changes will be processed in an organization

Guidance on the process

Change Control

process of evaluating a change request to decide if it should be implemented

The process in action

Configuration, Change & Asset Management

Change Control

refers to the process of evaluating a change request within an organization and deciding if it should go ahead.

requests are sent to the **Change Advisory Board (CAB)** to ensure that it is beneficial to the company.

Automating change management

In an environment that leverages CI/CD and infrastructure-as-code, change reviews may be partially automated when new code is ready for deployment.

This reduces operational overhead and human error, reduces security risk, and enables more frequent releases while maintaining a strong security posture.

CONFIGURATION & CHANGE MANAGEMENT

Configuration Management

Ensures that systems are configured similarly, configurations are known and documented.

Baselining ensures that systems are deployed with a common baseline or starting point, and imaging is a common baselining method.

Baseline is composed of individual settings called **configuration items (CI)**

Change Management

Helps reduce outages or weakened security from unauthorized changes.

Versioning uses a labeling or numbering system to track changes in updated versions of software.

Together, can prevent incidents and outages

CONTINUITY MANAGEMENT

Relevant for both customer and CSP

Continuity is concerned with the **availability** aspect of the CIA triad

There are a variety of standards related to continuity management.

NIST Risk Management Framework and ISO 27000

Both deal with business continuity and disaster recovery (BCDR), terms that fall under the larger category of continuity management.

Health Insurance Portability and Accountability Act (HIPAA)

Healthcare data in the United States is governed by this standard.

Mandates adequate data backups, disaster recovery planning, and emergency access to healthcare data in the event of a system interruption.

ISO 22301:2019 Security and resilience — BC management systems

This specifies the requirements needed for an organization to plan, implement and operate, and continually improve the continuity capability.

For the exam, remember these are associated with BCDR and availability

INFORMATION SECURITY MANAGEMENT

The goal of information security management is to ensure a consistent organizational approach to **managing security risks**

It is the approach an organization takes to preserving confidentiality, integrity, and availability (the CIA triad) for systems and data.

Standards that provide guidance for implementing and managing security controls in a cloud environment include:

-ISO 27001

-ISO 27017

-ISO 27018

-ISO 27701

-NIST RMF

-SP 800-53

-NIST CSF

-AICPA SOC 2

High-level familiarity with these will be good insurance on exam day...

and useful throughout your cybersecurity career

INFORMATION SECURITY MANAGEMENT

There are standards to guide CSPs and organizations in their development of information security management standards.

ISO/IEC 27001

A global standard for information security management that helps organizations protect their data from threats.

ISO/IEC 27017

Covered in depth in Domain 1 (section 1.5)

A security standard developed for cloud service providers and users to make a safer cloud-based environment and reduce the risk of security problems.

ISO/IEC 27018

Will be covered in depth in Doman 6 (section 6.2)

The first international standard about the privacy in cloud computing services

Is a "Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors".

INFORMATION SECURITY MANAGEMENT

ISO/IEC 27701

Extends the ISMS guidance in 27001 to manage risks related to privacy, by implementing and managing a privacy information management system (PIMS)

NIST RMF & CSF

RMF is MANDATORY, CMF is VOLUNTARY

RMF's audience is the entire federal government and **CSF** is aimed at private (commercial) business, though both address cybersecurity risk management.

NIST SP 800-53

Gov't-focused, guidance follows FIPS 200

Provides a catalog of security and privacy controls for all U.S. federal information systems except those related to national security.

AICPA SOC 2

Will be covered in depth in Doman 6 (section 6.2)

Service Organization Controls (SOC 2) framework has seen wide adoption among CSPs as well as the use of a third party to perform audits.

This also provides increased assurance for business partners and customers who cannot audit the CSP directly.

Continual Service Improvement

One critical element of continual service improvement includes areas of monitoring and measurement

These often take the form of security metrics.

Metrics need to be tailored to the audience they will be presented to, which often means "executive friendly".

Business leaders will be less interested in technical topics.

The metrics should be used to aggregate information and present it in an easily understood, actionable format.

Incident Management

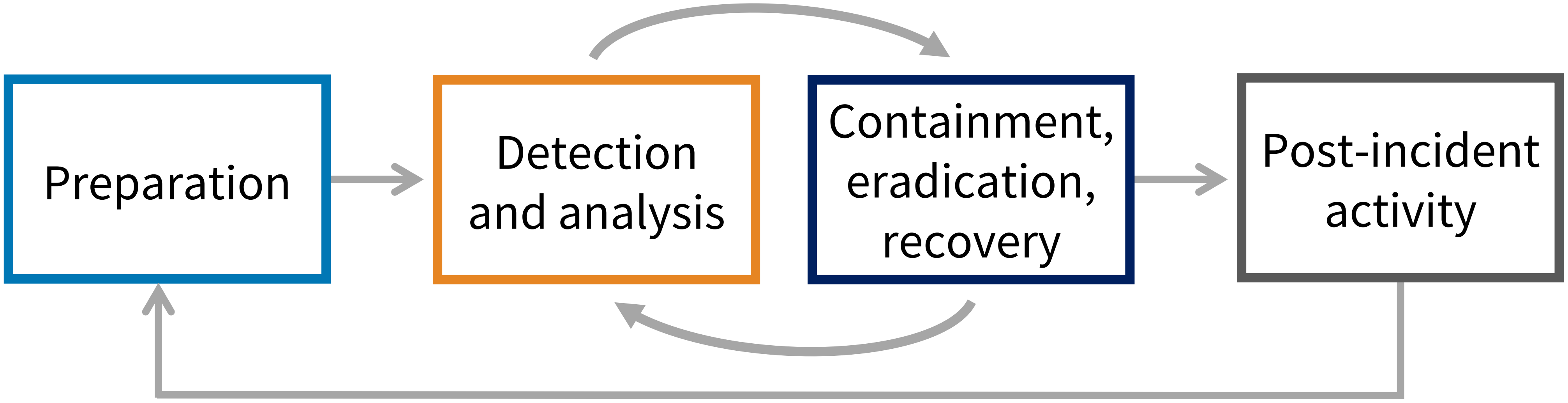
Events are any observable item, including routine actions such as a user successfully logging into a system.

Incidents, by contrast, are events that are unplanned and have an adverse impact on the organization

Not all incidents will require the security team, but exam focus is security

All incidents should be investigated and remediated to restore the organization’s normal operations and to minimize adverse impact

INCIDENT MANAGEMENT



A popular security incident management methodology is the **NIST SP 800-61 rev2** "Computer Security Incident Handling Guide"

Covered in depth in section "5.6 - Manage Security Operations"

MANAGING INCIDENT RESPONSE

6 phases of incident response

SANS 504-B

1	**Preparation**	Where incident response plans are written, and configurations documented.
2	**Identification**	Determining whether or not an organization has been breached. Is it really an incident?
3	**Containment**	Limiting damage (scope) of the incident.
4	**Eradication**	Once affected systems are identified, coordinated isolation or shutdown, rebuild, and notifications.
5	**Recovery**	Root cause is addressed and time to return to normal operations is estimated and executed.
6	**Lessons Learned**	Helps prevent recurrence, improve IR process.

Problem Management

In the ITIL framework, problems are the causes of incidents or adverse events that impact the CIA triad.

Problems are, in essence, the root cause of incidents

problem management utilizes root-cause analysis to identify the underlying problem(s) that lead to an incident.

It also aims to minimize the likelihood of future recurrence

An unsolved problem will be documented and tracked in a known issues or known errors database.

A temporary fix is called a "workaround"

RELEASE MANAGEMENT

Agile and CI/CD are the norm for the cloud

Today, traditional release management practices have largely been replaced with release practices in Agile development methodologies

The primary change is the frequency of releases due to the increased speed of development activities in continuous integration/continuous delivery (CI/CD).

Release scheduling may require coordination with customers and CSP.

Release manager is responsible for a number of checks, including ensuring change requests and approvals are complete, before approving final release gate.

Changes that impact data exposure may require Security team

Some of the release process is often automated, but manual processes may be involved, such as updating documentation and writing release notes.

The increased automation and pace of release in Agile and CI/CD typical to the cloud necessitates **automated security testing and policy controls**.

DEPLOYMENT MANAGEMENT

In more mature organizations, the CD in CI/CD stands for **continuous deployment**, which further/fully automates the release process.

Once a developer has written their code and checked it in, automated testing is triggered, and if all tests pass, code is integrated and deployed automatically

Less manual effort means lower cost, fewer mistakes, faster releases.

Even organizations with continuous deployment may require some deployment management processes to deal with deployments that cannot be automated

Processes for new software and infrastructure should be documented

Containerization (managed Kubernetes) is common in mature organizations supporting more frequent deployment in public cloud environments

DevSecOps

Fully automated deployment requires greater coordination with and integration of information security throughout the development process

SERVICE LEVEL MANAGEMENT

Service level management focuses on the organization's requirements for a service, as defined in a **service level agreement (SLA)**.

SLAs are like a contract focused on measurable outcomes of the service being provided

Should include clear metrics that define 'availability' for a service

SLAs require routine monitoring for enforcement, and this typically relies on metrics designed to indicate whether the service level is being met

Cloud infrastructure decisions should be made with the SLA in mind

Defining the levels of service is usually up to the cloud service provider (CSP) in public cloud environments.

Customer should monitor their CSPs compliance with the SLAs promised with various services, including ensuring credits for SLA failures are received.

AVAILABILITY MANAGEMENT

A service may be "up", that is to say the service is reachable but not available - meaning it cannot be used.

Availability and uptime are often used synonymously, but there is an important distinction: Availability means the specific service is up AND usable.

AuthN and AuthZ must work, and requests must be fulfilled

Many of the same concerns that an organization would consider in business continuity and disaster recovery apply in availability management

BCDR plans aim to quickly restore service availability in adverse events

Other concerns and requirements, such as data residency or the use of encryption, can complicate availability.

Customer must configure services to meet their requirements

Cloud consumers have a role to play in availability management as well; how much depends on the cloud service category (IaaS, PaaS, or SaaS)

CAPACITY MANAGEMENT

Responsibility will vary by cloud service category (IaaS, PaaS, SaaS)

One of the core concerns of availability is the amount of service capacity available compared with the amount being subscribed to.

For example, if a service has 100 active users but only 50 licenses available, that means the service is over capacity and 50 users will be denied service.

Capacity issues can be physical (infrastructure) or logical (e.g. licenses)

Measured service is one of the core elements of cloud computing, so metrics that illustrate demand for the service are relatively easy to identify

Responsibility for capacity management belongs to CSP at the platform level, but belongs to customer for deployed apps and services

Customer must choose appropriate service tiers, design app to scale

The cloud provides the "perception of unlimited capacity", but in reality, is oversubscribed by design, and CSP must monitor how much is too much.

5. CLOUD SECURITY OPERATIONS

5.4 Support Digital Forensics

Forensic data collection methodologies

Evidence management

Collect, acquire, and preserve digital evidence

eDiscovery

or “electronic discovery”, is the identification, collection, preservation, analysis, and review of electronic information.

Usually associated with collection of electronic information for legal purposes or security breach

FORENSIC INVESTIGATION STANDARDS

Forensic Investigation Standards

- -ISO/IEC 27037:2012
- -ISO/IEC 27041:2015
- -ISO/IEC 27042:2015
- -ISO/IEC 27043:2015
- -ISO/IEC 27050-1:2016
- -CSA Domain 3: Contracts & eDiscovery

ISO/IEC 27037:2012

Guide for collecting, identifying, and preserving electronic evidence

ISO/IEC 27041:2015

Guide for incident investigation

ISO/IEC 27042:2015

Guide for digital evidence analysis.

ISO/IEC 27043:2015

Guide for incident investigation principles and processes

GUIDANCE ON FORENSIC DATA COLLECTION

ISO/IEC 27050

A four-part standard within the ISO/IEC 27000 family of information security standards

Offers a framework, governance, and best practices for forensics, eDiscovery, and evidence management

Hiring an outside forensic expert is the best path for most organizations

CSA Security Guidance

Free guidance in **Domain 3: Legal Issues: Contracts and Electronic Discovery**

Offers guidance on legal concerns related to security, privacy, and contractual obligations

Covers topics like data residency, liability of data processor role

FORENSIC DATA COLLECTION METHODOLOGIES

Evidence Collection Process

Logs are essential

All activities should be logged including time, person performing the activity, tools used, system or data inspected, and results.

Document everything

including physical or logical system states, apps running, and any physical configurations of hardware as appropriate.

Consider volatility

Volatile data (data not on a durable storage) requires special handling and priority. Collect data from volatile sources first!

Evidence Collection Best Practices

Utilize original physical media

utilize original physical media whenever possible, as copies may have unintended loss of integrity.

Verify data integrity

at multiple steps by using hashing, especially when performing operations such as copying files.

Follow documented procedures

dedicated evidence custodian, logging all activities, leave systems powered on to preserve volatile data.

Evidence Collection Best Practices

Establish and maintain communications

with relevant parties such as the CSP, internal legal counsel, and law enforcement for guidance and requirements.

Communication with relevant parties and communication plans covered in section 5.5

EVIDENCE MANAGEMENT

RECAP from DOMAIN 2

Legal Hold

protecting any documents that can be used in evidence from being altered or destroyed.

sometimes called litigation hold

Chain of Custody

tracks the movement of evidence through its collection, safeguarding, and analysis lifecycle

documents each person who handled the evidence, the date/time it was collected or transferred, and the purpose for the transfer.

Confirms appropriate collection, storage, and handling

EVIDENCE MANAGEMENT

SCOPE of evidence

describes what is relevant when collecting data

in a multitenant cloud environment, this may be particularly important

collection from shared resources may expose other customers data

Scope of data collection is more challenging in the cloud

If the CSP does not adequately manage scope, they may expose sensitive data of an unrelated company!

ON PREMISES VS CLOUD

The cloud comes with additional challenges when it comes to forensic investigation

Data location:

Do you know where the data is hosted? And laws of countries it's hosted in?

Many cloud services store copies of data in multiple locations

Rights and responsibilities:

What rights for forensic data collection are listed in your CSP contract?

If it requires CSP cooperation, what is their response SLA?

Tools:

Are your forensic tools suitable for a multi-tenant environment?

What is your organizations liability if you unintentionally capture another customer's data on a shared resource?

e.g. remnants of a previous customer's data on physical storage

ON PREMISES VS CLOUD

Laws and regulations impact a consumer's ability to perform forensic data collection in the cloud

Regulatory and Jurisdiction

Cloud data should be stored and have data sovereignty in region stored.

Many countries have laws requiring businesses to store data within their borders.

The US introduced the **Clarifying Lawful Overseas Use of Data (CLOUD) Act** in 2018 due to the problems that FBI faced in forcing Microsoft to hand over data stored in Ireland.

Aids in evidence collection in investigation of serious crimes

In 2019, the US and the UK signed a data-sharing agreement to give law enforcement agencies in each country faster access to evidence held by cloud service providers.

Verifying audit and forensic data collection rights with your CSP to ensure you understand your rights and their legal obligations before you sign contracts is critical.

ON PREMISES VS CLOUD

Data residency and data sovereignty more challenging in the cloud

Cloud considerations (cont)

Forensic investigators should know their legal rights in every jurisdiction (region or country) where the organization hosts data in the cloud.

Some countries will not allow eDiscovery from outside their borders

Chain of custody

In traditional forensic procedures, it is "easy" to maintain an accurate history of time, location, and handling.

In the cloud, physical location is somewhat obscure. However, investigators can acquire a VM image from any workstation connected to the internet.

Time stamps and offsets can be more challenging due to location.

Maintaining a proper chain of custody is more challenging in the cloud.

Breach notification laws

Varies by country and regulations. For example, GDPR requires notification within 72 hours. Applies to all with EU customers, even if it's a 3rd party breach!

EVIDENCE UTILITY

Evidence should possess these **five attributes to be useful.**

Authentic: The information should be genuine and clearly correlated to the incident or crime.

Accurate: The truthfulness and integrity of the evidence should not be questionable.

Complete: All evidence should be presented in its entirety, even if it might negatively impact the case being made.

It is illegal in most jurisdictions to hide evidence that disproves a case.

EVIDENCE UTILITY

Evidence should possess these **five attributes to be useful.**

Convincing: The evidence should be understandable and clearly support an assertion being made.

e.g. chain of events presented from audit logs should be clear

Admissible: Evidence must meet the rules of the body judging it, such as a court.

Hearsay (indirect knowledge of an action) or evidence that has been tampered with may be thrown out by a court

Courts typically set a higher standard than regulators

EVIDENCE ADMISSIBILITY

Requirements for evidence to be **admissible in a court of law:**

Evidence must be relevant to a fact at issue in the case.

Makes a fact more or less probable

The fact must be material to the case.

The evidence must be competent (reliable).

Must be obtained by legal means.

Evidence obtains by illegal means will be thrown out

To prevail in court, evidence must be **sufficient**, which means “convincing without question, leaving no doubt”

ACQUISITION OF EVIDENCE

Importance of collecting

EVIDENCE

As soon you discover an incident...

You must begin to collect evidence and as much information about the incident as possible.

Evidence can be used in a subsequent legal action or in finding attacker identity.

Evidence can also assist you in determining the extent of damage.

DATA COLLECTION CHALLENGES IN THE CLOUD

Control

Most customer control in IaaS, least in SaaS

Using a cloud service involves loss of some control, and different service models offer varying levels of access.

Multitenancy and shared resources

Evidence collected while investigating a security incident may unintentionally include data from another customer.

Most likely if CSP or delegate were performing forensic recovery from shared physical resource, such as a storage array.

Data volatility and dispersion

Cloud environments support high availability techniques for data, like data **sharding**.

Sharding breaks data into smaller pieces, storing multiple copies of each piece across different data centers.

ORDER OF VOLATILITY

To determine what happened on a system, you need a copy of the data. **What evidence should you collect first?**

If it disappears in system reboot, power loss, passage of time, it is volatile

MOST

VOLATILITY

LEAST

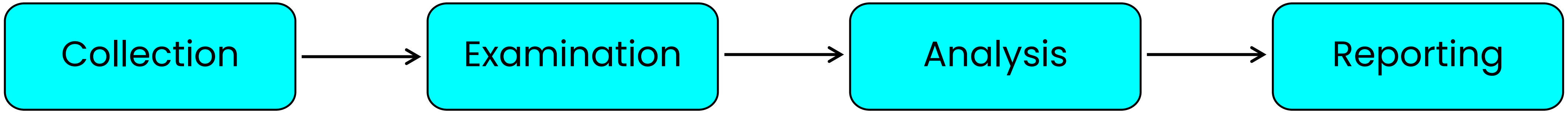
Volatility, in approximate order:

1. CPU, cache, and register contents
2. Routing tables, ARP cache, process tables, kernel statistics
3. Live network connections and data flows
4. Memory (RAM)
5. Temporary file system and swap/pagefile
6. Data on hard disk
7. Remotely logged data
8. Data stored on archival media and backups

FOR THE EXAM: Remember that volatile (perishable) information should be collected first.

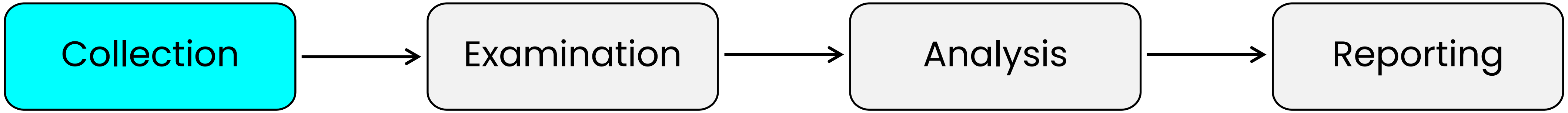
EVIDENCE COLLECTION AND HANDLING

There are four general phases of digital evidence handling:



EVIDENCE COLLECTION AND HANDLING

There are four general phases of digital evidence handling:

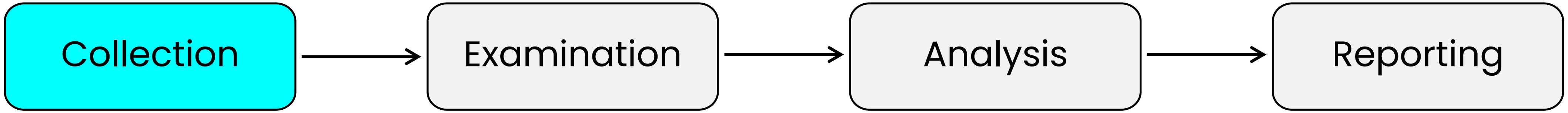


Collection → Examination → Analysis → Reporting

There are a number of concerns in the Collection phase relevant to the CCSP exam

EVIDENCE COLLECTION AND HANDLING

There are four general phases of digital evidence handling:



Proper evidence handling and decision making should be a part of the incident response procedures and training for team members performing response activities.

EVIDENCE PRESERVATION

Collect originals, work from copies!

Understand the concerns for **evidence preservation**

How to retain logs, drive images, VM snapshots, and other datasets for recovery, internal and forensic investigations.

Protections for evidence storage include:

- locked cabinets or safes
- dedicated/isolated storage facilities
- environment maintenance (temp, humidity)
- access restrictions and document/track activity
- blocking interference (shield from wireless) Faraday cage

ACQUISITION Applies to Iaas

Areas and considerations in evidence acquisition.

Disk aka hard drive. Was the storage media itself damaged?

Random-access memory (RAM). Volatile memory used to run applications.

Swap/Pagefile. used for running applications when RAM is exhausted.

OS (operating system). Was there corruption of data associated with the OS or the applications?

Device. When the police are taking evidence from laptops, desktops, and mobile devices, they take a complete system image.

The original image is kept intact, installed on another computer, hashed, then analyzed to find evidence of any criminal activity.

ACQUISITION

Applies to Iaas

Firmware. embedded code, could be reversed engineered by an attacker, so original source code must be compared to code in use.

a coding expert to compare both lots of source code in a technique called regression testing. rootkits and backdoors are concerns

Snapshot. if the evidence is from a virtual machine, a snapshot of the virtual machine can be exported for investigation.

Cache. special high-speed storage that can be either a reserved section of main memory or an independent high-speed storage device.

memory cache AND disk cache, both are volatile

Network. OS includes command-line tools (like netstat) that provide information that could disappear if you reboot the computer.

Like RAM, connections are volatile and lost on reboot.

Artifacts. any piece of evidence, including log files, registry hives, DNA, fingerprints, or fibers of clothing normally invisible to the naked eye.

INTEGRITY

Hashes

Most likely of these to appear on the exam

When either the forensic copy or the system image is being analyzed, the data and applications are **hashed** at collection.

It can be used as a **checksum** to ensure integrity later.

File can be hashed before and after collection to ensure a match on the original hash value to prove data integrity.

Provenance

Data provenance effectively provides a historical record of data and its origin and forensic activities performed on it.

Similar to **data lineage**, but also includes the inputs, entities, systems and processes that influenced the data.

Data lineage is the process of tracking flow of data over time, showing where the data originated, how it has changed, and its ultimate destination.

PRESERVATION

Preservation

Data needs to be preserved in its original state so that it can be produced as evidence in court.

original data must remain unaltered and pristine.

What is a “forensic copy” of evidence?

an image or exact, sector by sector, copy of a hard disk or other storage device, taken using specialized software, preserving an exact copy of the original disk.

Deleted files, slack space, system files and executables (and documents renamed to mimic system files and executables) are all part of a forensic image.

Putting a copy of the most vital evidence in a WORM drive will prevent any tampering with the evidence (you cannot delete data from a WORM drive.)

You could also write-protect/put a legal hold on some types of cloud storage.

CSSP EXAM CRAM

THE COMPLETE COURSE

CCSP

DEMO Log collection and retention in the cloud to preserve evidence

EXAMPLE FOR CONTEXT:

Features will vary by CSP

INSIDE CLOUD AND SECURITY

5. CLOUD SECURITY OPERATIONS

5.5 Manage Communication with Relevant Parties

Vendors

Customers

Partners

Regulators

Other stakeholders

Both company security policies (transparency)
AND regulatory compliance (law) shape communication

Communication Plan

Communication Plan

The plan that details how relevant stakeholders will be informed in event of an incident. (like a security breach)

Would include plan to maintain confidentiality, such as encryption to ensure that the event does not become public knowledge.

Contact list should be maintained that includes stakeholders from the government, police, customers, suppliers, and internal staff.

Compliance regulations, like GDPR, include notification requirements, relevant parties, and timelines

Confidentiality amongst internal stakeholders is desirable so external stakeholders can be informed in accordance with the plan.

Stakeholder Management

When we have an incident, there are multiple groups of relevant stakeholders that we need to inform and manage, and may include:

-Vendors

-Customers

-Partners

-Regulators

-Other Stakeholders

A **stakeholder** is a party with an interest in an enterprise;

corporate stakeholders include investors, employees, customers, and suppliers.

Regulated industries, such as banking and healthcare will have requirements driven by the regulations governing their industries.

Communication Plan

Vendors: The first step in establishing communication with vendors is an inventory of critical third parties on which the organization depends.

This inventory will drive vendor risk management activities in two ways:

1) Some vendors may be critical to the company's ongoing function, like the CSP

2) Others may provide critical inputs to a company's revenue generation

Vendor communications may be governed by contract and SLA

Customers: As cloud consumers, most company's will be the recipients of communications from their chosen CSPs.

Consumers should define (or at least monitor) communication SLA

Partners: Often have a level of access to a company's systems similar to that of the company's own employees but are not under company control.

Communication needs will evolve through partner onboarding, maintenance, and offboarding

Communication Plan

Regulators: Most regulators have developed cloud-specific guidance for compliant use of cloud services.

GDPR, HIPAA, and PCI DSS have communication requirements

Other Stakeholders: The company may need to communicate with the public, investors, and the company's cyber insurance company in a crisis.

Procedures for order and timing of contact should be created

Some cyber insurance providers require that they are the first point of contact in the event of a security incident.

Who is responsible for communication?

If customer data is impacted, the company is always responsible timely communication

This is true regardless of the cloud service model in use, even if the CSP is at fault

SHARED RESPONSIBILITY FOR SECURITY

Responsibility	IaaS	PaaS	SaaS
✓ Application Security	C	C/P	C/P
Network Security	C/P	P	P
Host Infrastructure	C/P	P	P
Physical Security	P	P	P
✓ Data Classification	C	C	C
✓ Identity & Access Management	C	C/P	C/P

C = Customer, **P** = Provider (CSP)

Customer always plays a role in access control and data security

5. CLOUD SECURITY OPERATIONS

5.6 Manage Security Operations

Security operations center (SOC)

Intelligent monitoring of security controls
(e.g. firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), honeypots, network security groups, artificial intelligence (AI))

Log capture and analysis
(e.g. security information and event management (SIEM), log management)

5. CLOUD SECURITY OPERATIONS

5.6 Manage Security Operations

Incident management

Vulnerability assessments

Security Operations Center (SOC)

A support unit designed to centralize a variety of security tasks and personnel at the tactical (mid-term) and operational (day-to-day) levels.

Both the CSP and consumer should have a SOC function

Key functions of the SOC include:

-Threat Prevention

-Threat Detection

-Incident Management

-Continuous Monitoring & Reporting

-Alert Prioritization

-Compliance Management

CSP Dashboards: Azure Status, AWS Service Health Dashboard, Google Cloud Status Dashboard

CCSP

CSSP EXAM CRAM

THE COMPLETE COURSE

DEMO

CSP Cloud Health and Service Status Dashboards

EXAMPLE FOR CONTEXT:

Features will vary by CSP

INSIDE CLOUD AND SECURITY

MONITORING

a **form of auditing** that focuses on active review of the log file data.

used to hold subjects accountable for their actions

also used to monitor system performance.

tools such as IDSs or SIEMs automate monitoring and provide real-time analysis of events.

MONITORING SECURITY CONTROLS

Monitoring security controls used to be an activity closely related to formal audits that occur relatively infrequently, often annually or less.

A newer concept is known as continuous monitoring, is described in the **NIST SP 800-37: Risk Management Framework (RMF)**

The RMF specifies the creation of a continuous monitoring strategy for getting near real-time risk information.

Network firewalls, web app firewalls (WAF), and IDS/IPS provide a critical source of information for NOC or SOC teams.

These devices should be continuously monitored to ensure they are functional

Monitoring for functionality should include monitoring log generation, centralized log aggregation, and analysis.

HARDWARE vs SOFTWARE

Hardware

A piece of purpose-built network hardware.

May offer more configurable support for LAN and WAN connections.

Often has superior throughput versus software because it is hardware designed for the speeds and connections common to an enterprise network.

In the cloud, it's virtual - a network virtual appliance (NVA)

Software

Software based firewalls that you might install on your own hardware.

Provide flexibility to place firewalls anywhere you'd like in your organization.

On servers and workstations, you can run a host-based firewall.

Host-based (software) are more vulnerable
to being disabled by attackers

APPLICATION vs HOST-BASED vs VIRTUAL

Application

Typically caters specifically to application communications.

Often that is HTTPS or Web traffic.

An example is called a web application firewall (WAF)

Host-based

An application installed on a host OS, such as Windows or Linux, both client and server operating systems.

Virtual

In the cloud, firewalls are implemented as virtual network appliances (VNA).

Available from both the CSP directly and third-party partners (commercial firewall vendors)

FIREWALL AND STATE

Stateless

Watch network traffic and restrict or block packets based on source and destination addresses or other static values.

Not 'aware' of traffic patterns or data flows.

Typically, faster and perform better under heavier traffic loads.

Stateful

Can watch traffic streams from end to end.

Are aware of communication paths and can implement various IP security functions such as tunnels and encryption.

Better at identifying unauthorized and forged communications.

MODERN FIREWALLS

Firewall

Web Application

aka "WAF"

Protect web applications by filtering and monitoring HTTPS traffic between a web application and the Internet.

Typically protects web applications from common attacks like XSS, CSRF, and SQL injection.

Some come pre-configured with OWASP rulesets

Firewall

Next Generation

aka "NGFW"

a deep-packet inspection firewall that moves beyond port/protocol inspection and blocking.

adds application-level inspection, intrusion prevention, and brings intelligence from outside the firewall.

IDS VS IPS RESPONSE

IDS

Intrusion Detection System

generally responds passively by logging and sending notifications

IPS

Intrusion Prevention System

is placed in line with the traffic and includes the ability to block malicious traffic before it reaches the target

FLAVORS OF INTRUSION DETECTION SYSTEMS

HIDS

host-based IDS

can monitor activity on a single system only. A drawback is that attackers can discover and disable them.

NIDS

network-based IDS

can monitor activity on a network, and a NIDS isn't as visible to attackers.

FLAVORS OF INTRUSION DETECTION SYSTEMS

HIPS

host-based IPS

can monitor activity on a single system only. A drawback is that attackers can discover and disable them.

NIPS

network-based IPS

can monitor activity on a network, and a NIPS isn't as visible to attackers.

Honeypot

a system that often has **pseudo flaws** and **fake data** to lure intruders

as long as attackers are in the honeypot, they are not in the live network.

DECEPTION AND DISRUPTION

Honeypot

A group of honeypots is called a honeynet.

Lure bad people into doing bad things. Lets you watch them.

Only ENTICE, not ENTRAP. You are not allowed to let them download items with “Enticement”.

For example, allowing download of a fake payroll file would be entrapment.

Goal is to **distract** from real assets and **isolate** in a padded cell until you can track them down.

ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

Monitoring tools, like a SIEM, use AI and ML to automate investigation and response

Artificial Intelligence

Focuses on accomplishing "smart" tasks combining machine learning and deep learning to emulate human intelligence

Machine Learning

A subset of AI, computer algorithms that improve automatically through experience and the use of data.

Deep Learning

a subfield of machine learning concerned with algorithms inspired by the structure and function of the brain called **artificial neural networks**.

SYSLOG/SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

User Entity Behavior Analysis (UEBA)

This is based on the interaction of a user that focuses on their identity and the data that they would normally access on a normal day.

It tracks the devices that the user normally uses and the servers that they normally visit.

Sentiment Analysis

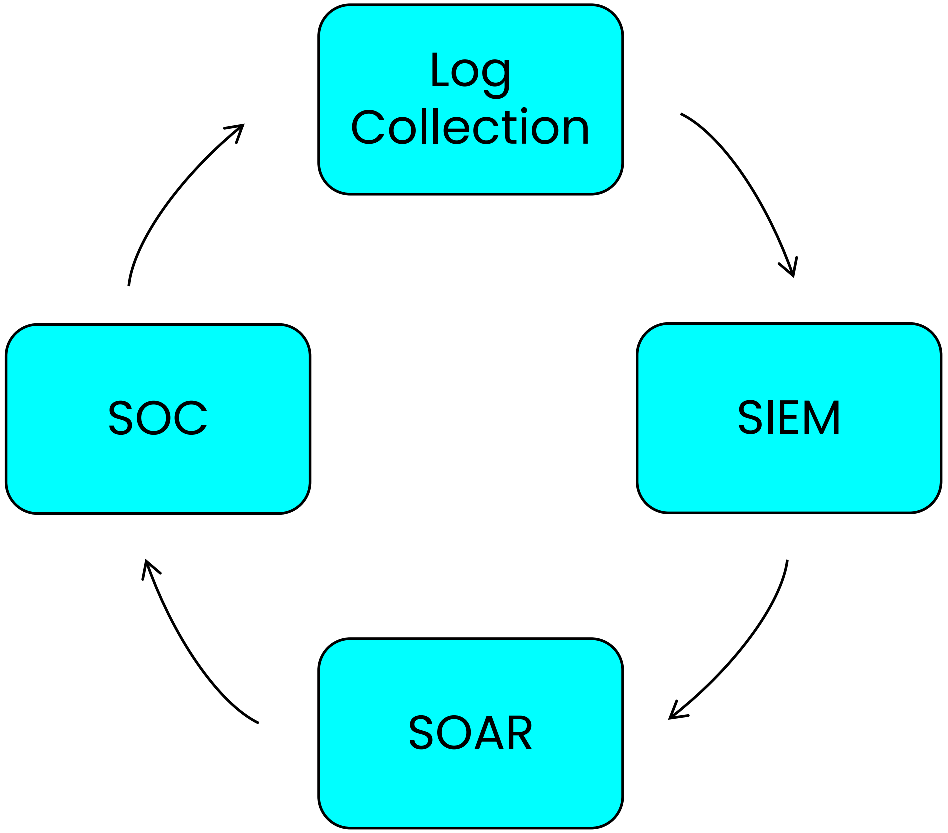
Artificial intelligence and machine learning to identify attacks.

Cybersecurity sentiment analysis can monitor articles on social media, look at the text and analyze the sentiment behind the articles.

Over time, can identify a users' attitudes to different aspects of cybersecurity.

LOG CAPTURE AND ANALYSIS

Tooling that allows an organization to define incident analysis and response procedures in a digital workflow format.



Integrates your security processes and tooling in a central location (SOC).

Response automation, using machine learning and artificial intelligence

These make it faster than humans in identifying and responding to true incidents.

Reduces MTTD and accelerates response

Uses **playbooks** that define an incident and the action taken. Capabilities vary by situation & vendor

Over time, should produce faster alerting and response for the SOC team.

SIEM AND SOAR

uses AI, ML, and threat intelligence

SIEM

Security Information Event Management

system that collects data from many other sources within the network.

provides real-time monitoring, analysis, correlation & notification of potential attacks.

SOAR

Security Orchestration Automation, & Response

centralized alert and response automation with threat-specific playbooks.

response may be fully automated or single-click.

Many providers deliver these capabilities together

LOGGING, STORAGE, AND ANALYSIS OF DATA EVENTS

Logs are worthless if you do nothing with the log data. They are made valuable only by **review**.

That is, they are valuable only if the organization makes use of them to identify activity that is unauthorized or compromising.

SIEM (Security Information Event Monitoring) tools can help to solve some of these problems by offering these key features:

- Log centralization and aggregation
- Data integrity
- Normalization
- Automated or continuous monitoring
- Alerting
- Investigative monitoring

RECAP from DOMAIN 2

LOGGING, STORAGE, AND ANALYSIS OF DATA EVENTS

Key **SIEM features** necessary to optimize event detection and visibility and scale security operations:

Log centralization and aggregation

Rather than leaving log data scattered around the environment on various hosts, the SIEM platform can gather logs from a variety of sources, including:

operating systems, applications, network appliances, user devices, providing a single location to support investigations.

Data integrity

The SIEM should be on a separate host with its own access control, preventing any single user from tampering.

A cloud SIEM solves this issue

RECAP from DOMAIN 2

LOGGING, STORAGE, AND ANALYSIS OF DATA EVENTS

Key **SIEM features** necessary to optimize event detection and visibility and scale security operations:

Normalization

SIEMs can normalize incoming data to ensure that the data from a variety of sources is presented consistently.

Automated or continuous monitoring

Sometimes referred to as correlation, SIEMs use algorithms to evaluate data and identify potential attacks or compromises.

Alerting

SIEMs can automatically generate alerts such as emails or tickets when action is required based on analysis of incoming log data

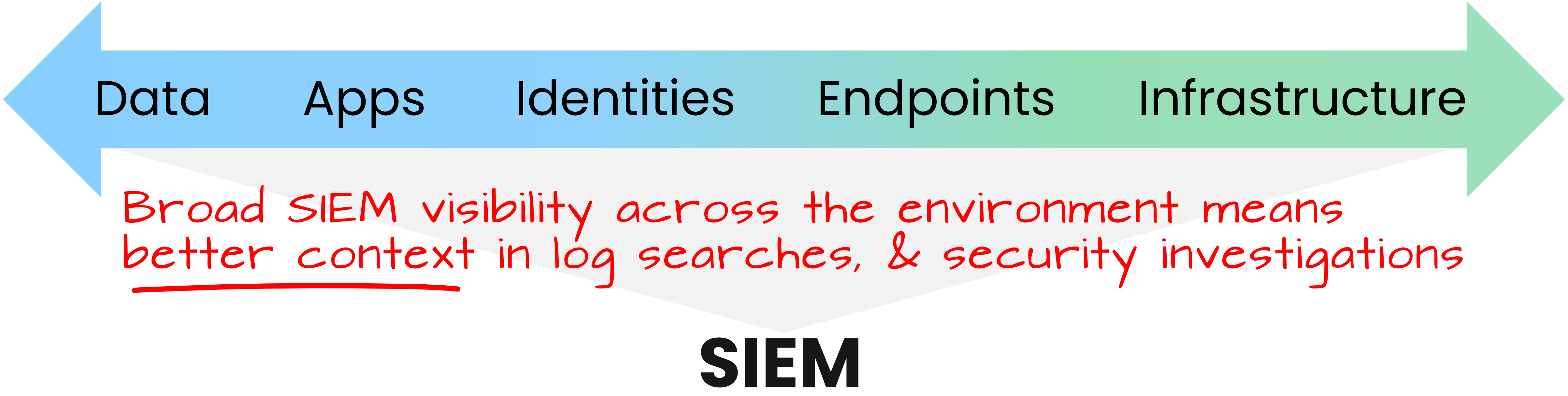
RECAP from DOMAIN 2

LOGGING, STORAGE, AND ANALYSIS OF DATA EVENTS

Key **SIEM features** necessary to optimize event detection and visibility and scale security operations:

Investigative monitoring

When manual investigation is required, the SIEM should provide support capabilities such as querying log files, generating reports.



Data

Apps

Identities

Endpoints

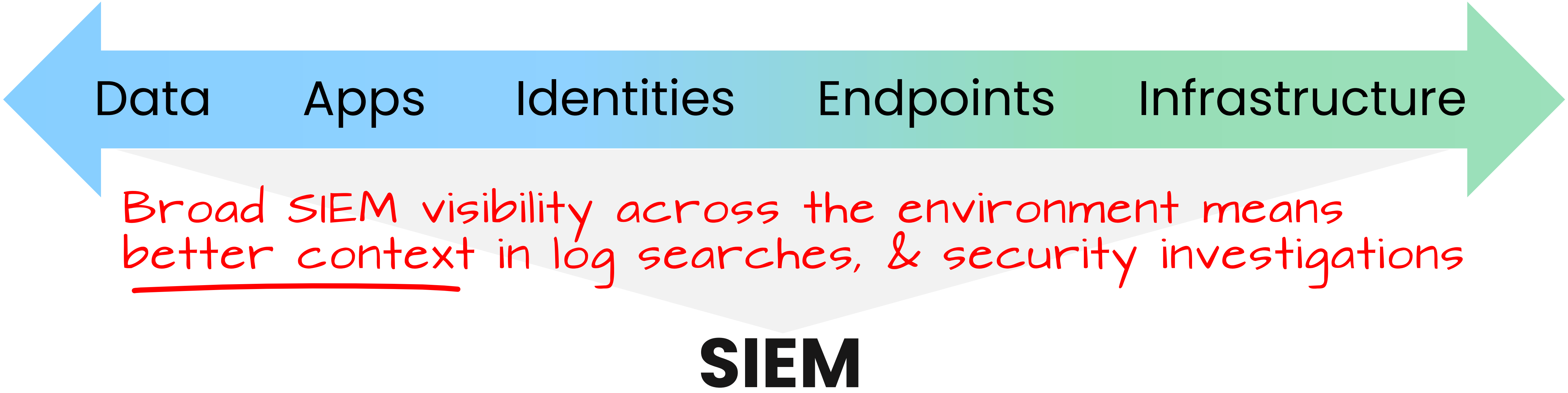
Infrastructure

Broad SIEM visibility across the environment means better context in log searches, & security investigations

SIEM

LOGGING, STORAGE, AND ANALYSIS OF DATA EVENTS

The key to that visibility is log collection



Data Apps Identities Endpoints Infrastructure

Broad SIEM visibility across the environment means better context in log searches, & security investigations

SIEM

LOG COLLECTION AND ANALYSIS WITH A SIEM

Log Collectors

SIEM has built-in log collector tooling that can collect information from both the syslog server and multiple other servers. An agent is placed on the device that can collect log information, parse and restructure data, and pass to SIEM for aggregation.

Ingestion may be with via an agent, syslog, or API

Log Aggregation

Can correlate and aggregate events so that duplicates are filtered and a better understanding network events is achieved to help identify potential attacks.

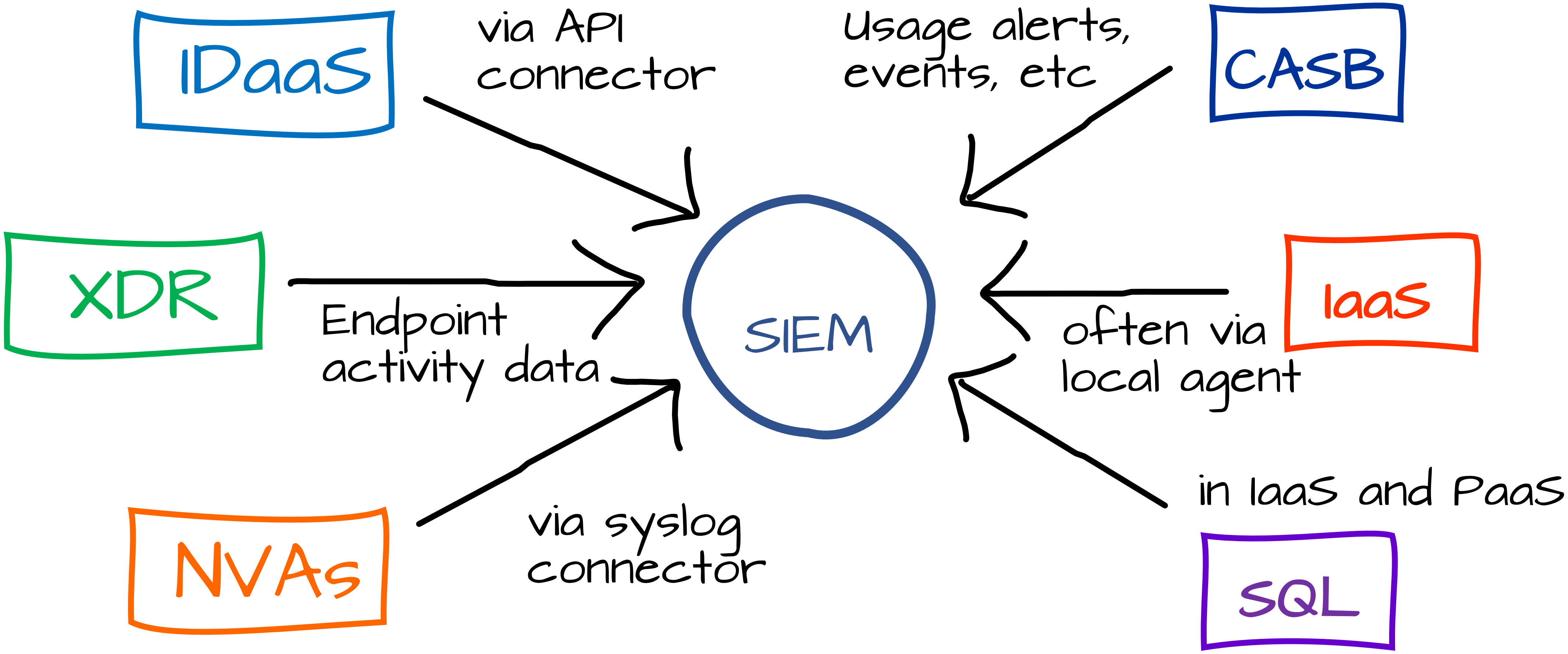
Packet Capture

Can capture packets and analyze them to identify threats as soon as they reach your network, providing immediate alert to security team if desired.

Data Inputs

The SIEM system collects a massive amount of data from various sources.

May include network devices, IDM, MDM, CASB, XDR, and more



Log Ingestion with a SIEM

EXAMPLE

LOG CAPTURE AND ANALYSIS

Logs are worthless if you do nothing with the log data. They are made valuable only by **review**.

That is, they are valuable only if the organization makes use of them to identify activity that is unauthorized or compromising.

SIEM (Security Information Event Monitoring) tools can help to solve some of these problems by offering these key features:

- Log centralization and aggregation
- Data integrity
- Normalization
- Correlation and detection
- Alerting
- Investigative monitoring

SIEM is a core tool of the Security Operations Center

LOG FILES

data is recorded in databases and different types of log files.

common log files include security logs, system logs, application logs, firewall logs, proxy logs.

should be protected by centrally storing them and using permissions to restrict access.

archived logs should be set to read-only to prevent modifications.

LOG FILES

Log files play a core role in providing evidence for investigations. You'll want to be familiar with the many different types of log files a typical SIEM might ingest.

Network: This log file can identify the IP and MAC addresses of devices that are attached to your network. Usually sent to a central syslog server

NIDS/NIPS can be important in identifying threats and anomalies from these.

log files from a proxy server can reveal who's visiting malicious sites.

The collective insight may be useful in stopping DDoS attack

Web: web servers log many types of information about the web requests, so evidence of potential threats and attacks will be visible here.

information collected about each web session: IP address request, Date and time, HTTP method, such as GET/POST, Browser used, and HTTP Status code.

400 series HTTP response codes are client-side errors

500 series HTTP response codes are server-side errors

These logs must be fed to a SIEM, IDS/IPS or other system to analysis this data

LOG FILES

These files exist on client and server systems. Sending these to a SIEM can help establish a central audit trail and visibility into the scope of an attack.

System: contains information about hardware changes, updates to devices, and time synchronization, group policy application, etc.

Application: contains information about software applications, when launched, success or failure, and warnings about potential problems or errors.

Security: contains information about a successful login, as well as unauthorized attempts to access the system and resources.

can identify attackers trying to log in to your computer systems.

captures information on file access and can determine who has downloaded certain data.

You will find log files with these names in the Event Viewer on any Windows client or server

LOG FILES

Log files play a core role in providing evidence for investigations. You'll want go be familiar with the many different types of log files for the Security+ exam.

DNS: contains virtually all DNS server-level activity, such as zone transfer, DNS server errors, DNS caching, and DNSSEC.

DNS query logging often disabled by default due to volume.

Authentication: information about login events, logging success or failure.

multiple sources authenticating log files in a domain environment, including RADIUS, Active Directory, and cloud providers Azure Active Directory.

LOG FILES

VoIP phones are embedded systems that must be secured

Log files related to voice applications can be valuable in identifying anomalous activity, unauthorized users, and even potential attacks

VoIP and Call Managers: These systems provide information on the calls being made and the devices that they originate from.

may also capture call quality by logging the Mean Optical Score (MOS), jitter, and loss of signal. Significant loss in quality may indicate attack

each call is logged (inbound and outbound calls), the person making the call, and the person receiving the call. Including long-distance calls

Session Initiation Protocol (SIP) Traffic: SIP is used for internet-based calls and the log files generally show:

the 100 events, known as the INVITE, the initiation of a connection, that relates to ringing.

the 200 OK is followed by an acknowledgement.

Large number of calls not connecting may indicate attack

SYSLOG/SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

Event Reporting (Review Reports)

A SIEM typically includes dashboard and collects reports that can be reviewed regularly to ensure that the policies have been enforced and that the environment is compliant.

Also highlight whether the SIEM system is effective and working properly. Are incidents raised true positives?

False positives may arise because the wrong input filters are being used or the wrong hosts monitored.

SIEM dashboards will typically provide a views into status of log ingestion and security concerns identified through correlation.

CCSP

CSSP EXAM CRAM

THE COMPLETE COURSE

DEMO Service logging and SIEM ingestion of cloud logs

EXAMPLE FOR CONTEXT:

Features will vary by SIEM & CSP

INSIDE CLOUD AND SECURITY

INCIDENT RESPONSE LIFECYCLE

> The incident response lifecycle in the CBK is from **NIST SP 800-61 rev2**, the "Computer Security Incident Handling Guide"

1st party incidents are internal to the organization
3rd party incidents affect an external entity, like the CSP

INCIDENT RESPONSE LIFECYCLE

Preparation

Refers to the organization’s **preparation** necessary to ensure they can respond to a security incident, including tools, processes, competencies, and readiness.

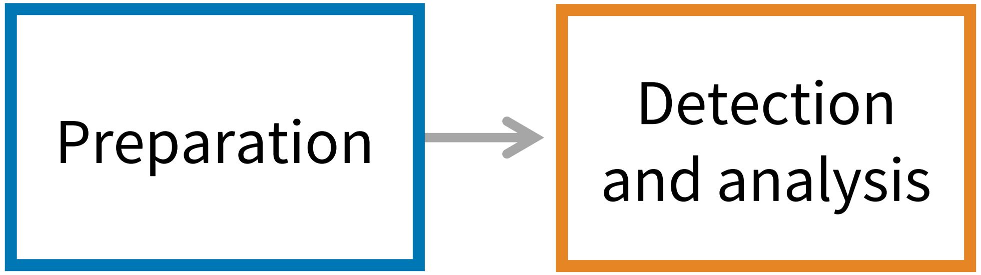
INCIDENT RESPONSE LIFECYCLE

Preparation

Plan review multiple times per year in a walkthrough, aka 'tabletop exercise'

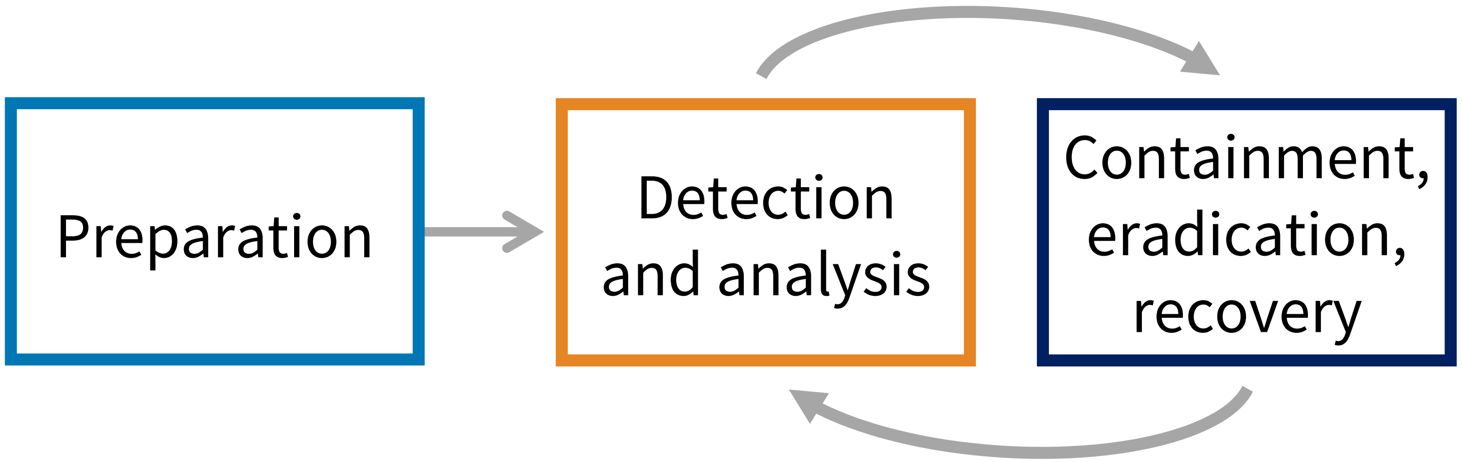
These details should be documented in a **security incident response plan** that is regularly reviewed and updated.

INCIDENT RESPONSE LIFECYCLE



The activity to **detect** a security incident in a production environment and to **analyze** all events to confirm the authenticity of the security incident.

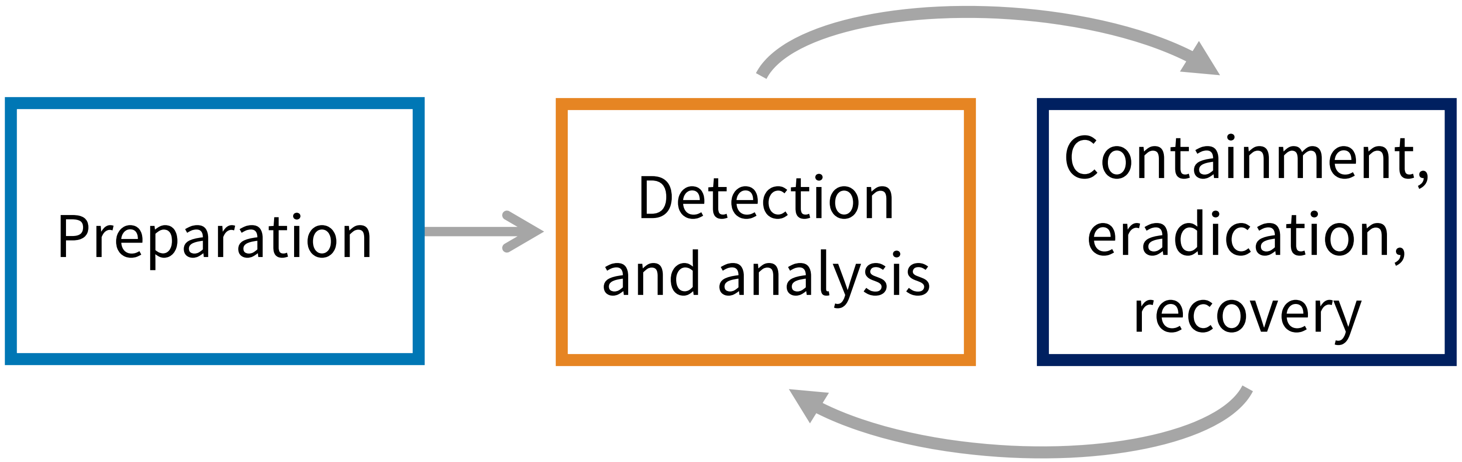
INCIDENT RESPONSE LIFECYCLE



Limits the damage (scope) of the incident

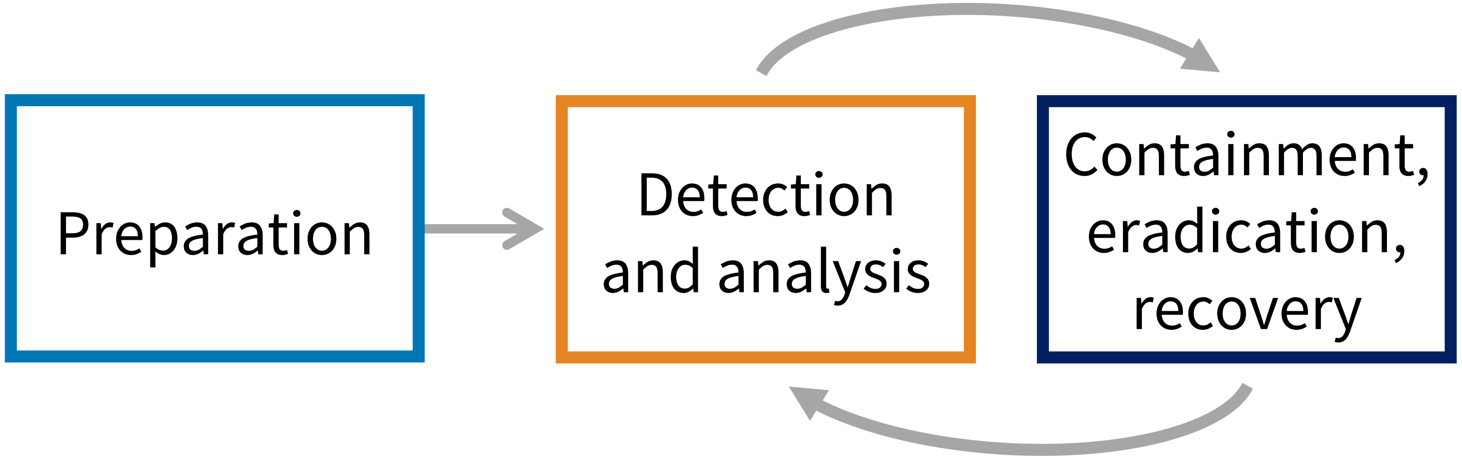
In **containment**, the required and appropriate actions taken to contain the security incident based on the analysis done in the previous phase.

INCIDENT RESPONSE LIFECYCLE



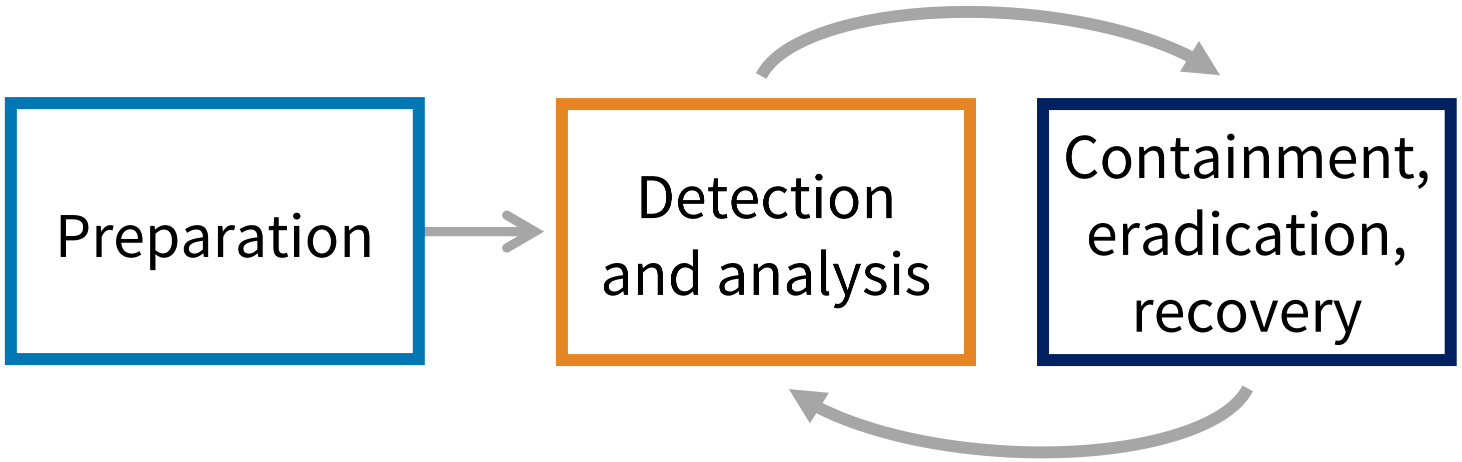
Eradication is the process of eliminating the root cause of the security incident with a high degree of confidence.

INCIDENT RESPONSE LIFECYCLE



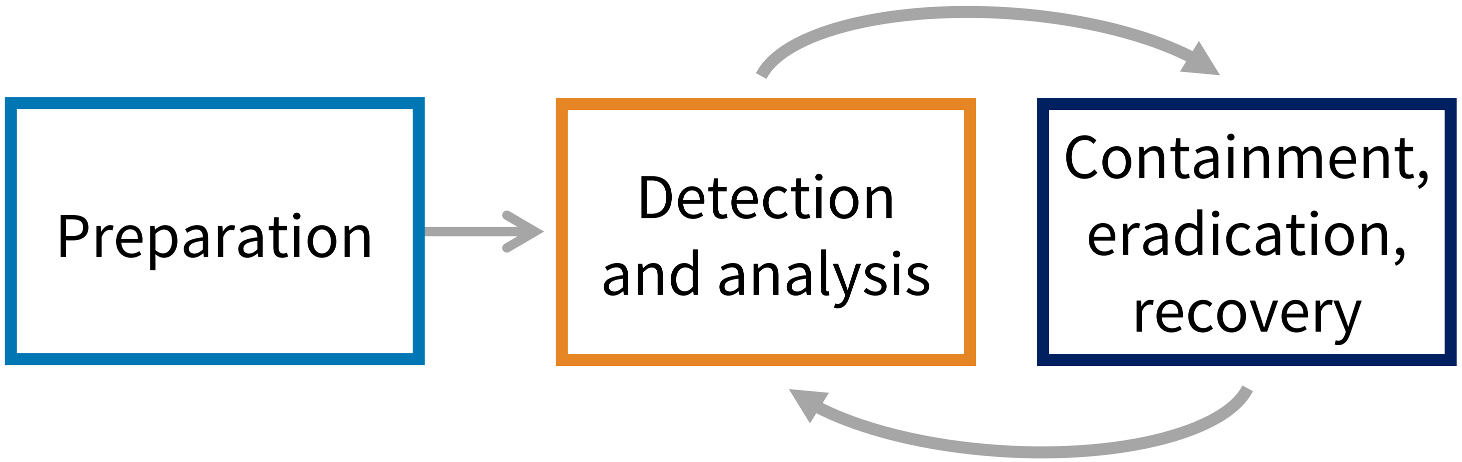
During the incident, our focus is on protecting and restoring business-critical processes.

INCIDENT RESPONSE LIFECYCLE



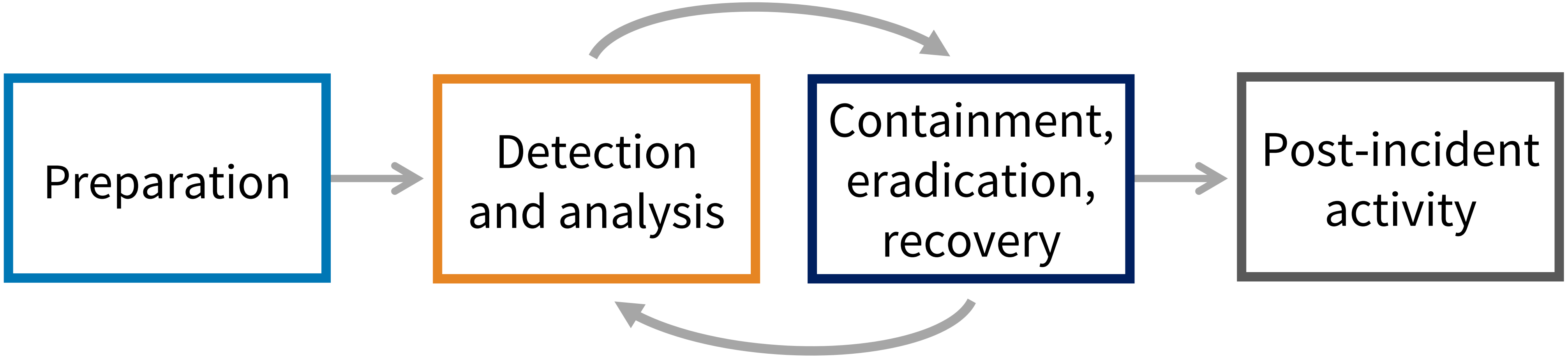
Recovery should happen after the adversary has been evicted from the environment and known vulnerabilities have been remediated.

INCIDENT RESPONSE LIFECYCLE



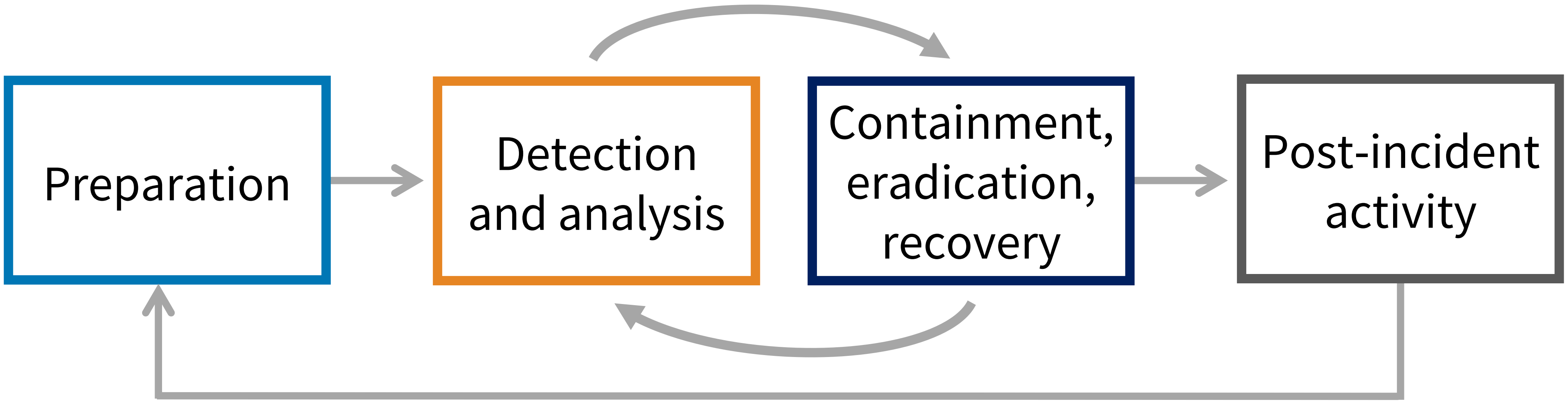
Recovery returns the environment to its normal, fully functional, original state prior to the incident.

INCIDENT RESPONSE LIFECYCLE



The **post-mortem analysis** is performed after the recovery of a security incident.

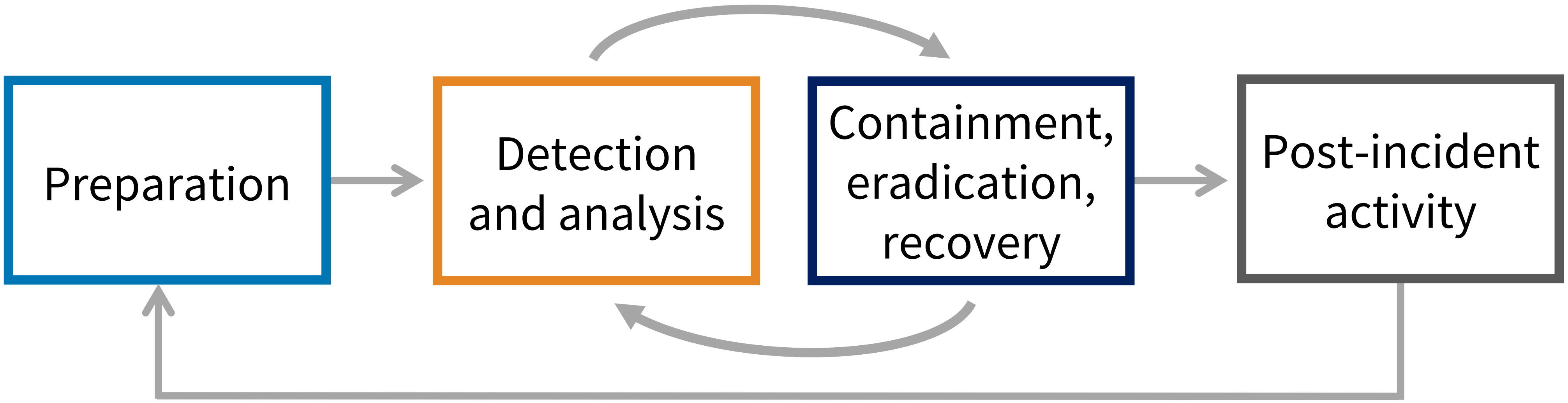
INCIDENT RESPONSE LIFECYCLE



Actions performed during the process are reviewed to determine if any changes need to be made in the preparation or detection and analysis phases.

How can we improve the IR process?

INCIDENT RESPONSE LIFECYCLE



The **lessons learned** drive **continuous improvement** ensuring effective and efficient incident response.

RIGHT TO AUDIT IN THE CLOUD

> Use of vulnerability scanners and pen testers may be limited by your CSP’s terms of service.
>
> A CCSP should understand the type and frequency of testing the CSP allows.

CSPs typically have penetration testing and scanning "rules of engagement"

VULNERABILITY MANAGEMENT

Vulnerability Management | includes routine vulnerability scans and periodic vulnerability assessments.

Vulnerability Scanners | can detect known security vulnerabilities and weaknesses, absence of patches or weak passwords.

Are used to conduct:

Vulnerability Assessments | extend beyond just technical scans and can include reviews and audits to detect vulnerabilities.

VULNERABILITY SCANS

A vulnerability scan assesses possible security vulnerabilities in computers, networks, and equipment that can be exploited.

Credentialed Scan: A credentialed scan is a much more powerful version of the vulnerability scanner. It has higher privileges than a non-credentialed scan.

Spot vulnerabilities that require privilege, like non-expiring PWs

Non-Credentialed Scan: A non-credentialed scan has lower privileges than a credentialed scan. It will identify vulnerabilities that an attacker would easily find.

Scans can find missing patches, some protocol vulnerabilities

VULNERABILITY SCANS

A vulnerability scan assesses possible security vulnerabilities in computers, networks, and equipment that can be exploited.

Non-Intrusive Scans: These are passive and merely report vulnerabilities. They do not cause damage to your system.

Intrusive Scans: Can cause damage as they try to exploit the vulnerability and should be used in a sandbox and not on your live production system.

Configuration Review: Configuration compliance scanners and desired state configuration in PowerShell ensure that no deviations are made to the security configuration of a system.

The combination of techniques can reveal which vulnerabilities are most easily exploitable in a live environment.

VULNERABILITY SCANS

Network Scans: These scans look at computers and devices on your network and help identify weaknesses in their security.

Application Scans: Before applications are released, coding experts perform regression testing that will check code for deficiencies.

Web Application Scans:
Crawl through a website as if they are a search engine looking for vulnerabilities.

Perform an automated check for site/app vulnerabilities, such as cross-site scripting and SQL injection.

Also know difference between SAST and DAST for the exam

There are many sophisticated web application scanners available, due in part due to mass adoption of cloud computing.

VULNERABILITY SCANS

Common Vulnerabilities and Exposures (CVE) and Common Vulnerability Scoring System (CVSS)

CVSS is the overall score assigned to a vulnerability. It indicates severity and is used by many vulnerability scanning tools.

CVE is simply a list of all publicly disclosed vulnerabilities that includes the CVE ID, a description, dates, and comments.

The CVSS score is not reported in the CVE listing – you must use the **National Vulnerability Database (NVD)** to find assigned CVSS scores.

The CVE list feeds into the NVD

The National Vulnerability Database (NVD) is a database, maintained by NIST, that is synchronized with the MITRE CVE list.

VULNERABILITY SCAN OUTPUT

A **vulnerability scanner** can identify and report various vulnerabilities before they are exploited, such as:

Examples include:
-software flaws
-missing patches
-open ports
-services that should not be running
-weak passwords

will help companies avoid known attacks such as SQL injection, buffer overflows, denial of service, and other type of malicious attacks.

A **credentialed vulnerability scan** is the most effective as it provides more information than any other vulnerability scan.

VULNERABILITY SCANS

A vulnerability scan assesses possible security vulnerabilities in computers, networks, and equipment that can be exploited.

False Positive: where the scan believes that there is a vulnerability but when physically checked, it is not there.

False Negative: When there is a vulnerability, but the scanner does not detect it.

True Positive: This is where the results of the system scan agree with the manual inspection.

Log Reviews: Following a vulnerability scan, it is important to review the log files/reports that list any potential vulnerabilities.

INSIDE CLOUD AND SECURITY

THANKS

FOR WATCHING!