Welcome back to the Security+ Bootcamp

Your instructors:

Michael J Shannon

and

Carl Mullin

Class will begin at 10:00 A.M. Central Standard Time (CST)

Defining Risk

- Inherent (total) risk
  - Risk the organization faces if safeguard is not implemented
- Residual risk
  - Risk that remains once safeguard is in place
- Residual = inherent risk - safeguards (controls)

Structured vs. Unstructured Threats

Structured threats

- Planned
- Organized
- Persistent
- Multi-phased
- Can be internal or external
- Exploit kits, zero-days, modules, and ransomware

Unstructured threats

- Accidental
- Non-malicious
- Drive-by web surfing
- No AUP
- Poor awareness
- E-mail and webmail
- USBs and personal electronics

Risk and Threat Matrix

	Event type								
	Accidental Leak	**Espionage**	**Financial fraud**	**Misuse**	**Opportunistic data theft**	**Physical theft**	**Product alteration**	**Sabotage**	**Violence**
Nonhostile									
Reckless insider	X			X			X		
Untrained/distracted insider	X			X			X		
Outward sympathizer	X			X					
Unknown (nonhostile or hostile)									
Supplier	X	X	X	X	X		X		
Partner	X	X	X	X	X		X		
Hostile									
Irrational individual	X			X		X		X	X
Thief		X	X		X	X			
Disgruntled insider	X	X	X	X	X	X	X	X	X
Activist		X		X	X	X	X	X	
Terrorist						X		X	X
Organized crime		X	X		X	X	X		
Competitor		X			X		X	X	
Nation state		X			X		X	X	

Tim Casey et al., "A Field Guide To Insider Threat," PDF file, https://www.nationalinsiderthreatsig.org (IT@Intel, Intel Corporation, October 2015), https://www.nationalinsiderthreatsig.org/itrmresources/Intel%20Insider%20Threat%20Field%20Guide.pdf.

Multiparty Risk

- Organizations that operate with outsourcing, suppliers, licensees, agents, and the like
- The frequency and scale of third-party use has grown substantially over the last two decades
- There is greater regulatory emphasis on how organizations manage third parties to address the inherent risks

Risk Treatment

Also called risk handling or appetite

- Risk acceptance
  - Do not implement any safeguards
  - Justification in writing is often required
- Risk avoidance
  - Choose not to undertake actions that introduce risk
- Risk transference/sharing
  - Pass the risk to a third-party, such as an insurance company or a cloud service provider
- Risk mitigation
  - Implement safeguards that will eliminate or reduce risk exposure - risk may exist, but impact is reduced

Assessing Risk

- What are your assets at risk?
  - Risk assessment is about information gathering
  - Asset Inventory and categorization
  - Both tangible and intangible assets
- Identify risks to most valuable assets first
  - Vulnerability, threats, and attacks
  - Who, Why, and How?
- Only focus on risks that are most likely to occur
  - Maximizes available resources
  - Focus on most likely to least likely

Creating a Risk Register

- Risk Register is also called ledger or log
- Often represented as a scatter plot/table from a database
- Fulfills regulatory compliance
- Repository of identified risks, impact, scenarios, and potential responses

Identified Risks	Root Causes	Probability and Impact	Ranking	Categories	Priorities	Time and Cost Objectives	Potential Responses	Risk Owners	Assumptions

Qualitative Risk Analysis

The most common method used in risk and security

- Descriptive approach using subjective opinions, history, and scenarios to determine risk levels
  - Expert judgement
  - Best practices
  - Experience
  - Intuition
- Often involves interviewing people (Delphi) regarding assets, known risks, known vulnerabilities, common threats, and historical impacts

Qualitative Heat Map

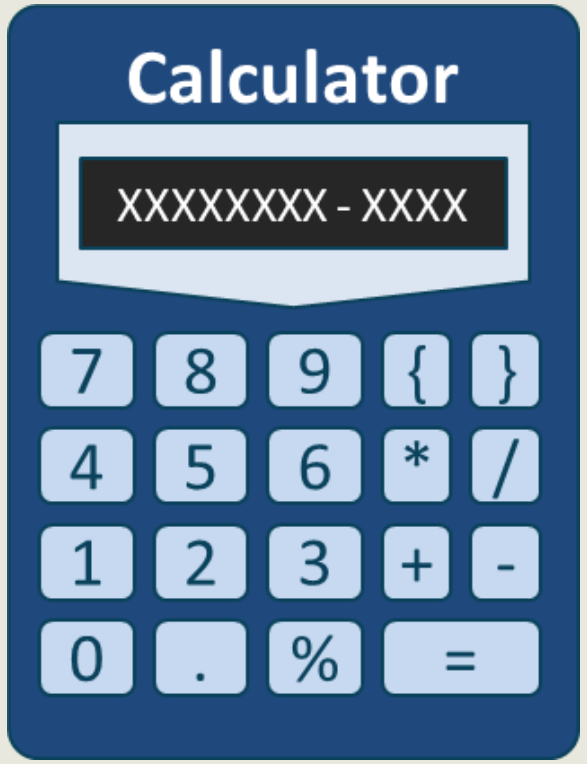
Likelihood			Impact				
			Negligible	Minor	Moderate	Critical	Disastrous
			1	2	3	4	5
	Frequent	5	Medium	Medium	High	High	High
	Likely	4	Medium	Medium	Medium	High	High
	Occasional	3	Low	Medium	Medium	Medium	High
	Seldom	2	Low	Low	Medium	Medium	Medium
	Improbable	1	Low	Low	Low	Medium	Medium

Quantitative Risk Analysis

Rapidly gaining popularity due to FAIR analysis

- Scientific/mathematical approach to getting monetary and numeric results based on the following:
  - Asset values
  - Impact and magnitude
    - Severity of incident
  - Probability and likelihood of occurrence
    - Threat frequency
  - Costs and effectiveness of safeguards
  - Probabilities based on percentages and calibrated estimation

Classic Quantitative Analysis (Whitman)



- AV (asset value)
  - Value of the asset according to the organization
- EF (exposure factor)
  - Percentage of asset loss caused by identified threat
- SLE (single loss expectancy)
  - Potential loss if attack occurs
  - (Asset value * exposure factor)
- ARO (annualized rate of occurrence)
  - Estimated frequency the threat will occur within a single year
- ALE (annualized loss expectancy) = (SLE * ARO)

Classic Quantitative Analysis (Whitman)

Risk analysis						
Asset	**Threat**	**Asset value**	**Exposure factor**	**Single loss expectancy**	**Annualized rate of occurrence**	**Annualized loss expectancy**
SRV_1	Fire	$15000	100%	$15000	0.1	$1500
SRV_2	Fire	$20000	100%	$20000	0.1	$2000
SRV_1	Flood	$15000	100%	$15000	0.0001	$1.5
SRV_2	Flood	$20000	100%	$20000	0.0001	$2.0
SRV_1	Virus (no AV software)	$15000	10%	$1500	365	$547,500
SRV_1	Virus (with AV software)	$15000	10%	$1500	1	$1500

Disasters

Environmental	Man-made intentional	Man-made unintentional
• Earthquakes • Wildfires • Flooding • Snow • Tsunamis • Hurricanes • Tornadoes • Landslides • Asteroids	• Arson • Terrorist • Political • Break-ins • Theft • Damage • File destruction • Information disclosure	• Mistakes • Power outage • Illness • Epidemics • Information disclosure • Damage • File destruction • Coding errors

Privacy and Data Breach Consequences

Primary and secondary loss

- Productivity
- Response
- Replacement
- Fines and judgments
- Competitive advantage
- Reputation

Main Causes of Data Breaches

- Cyber attacks
- Device loss or theft
- Employee leakage or theft
- Human errors

Data and Asset Classification

Military Classifications

- Top secret
- Secret
- Sensitive but unclassified (SBU)
- Confidential
- Unclassified

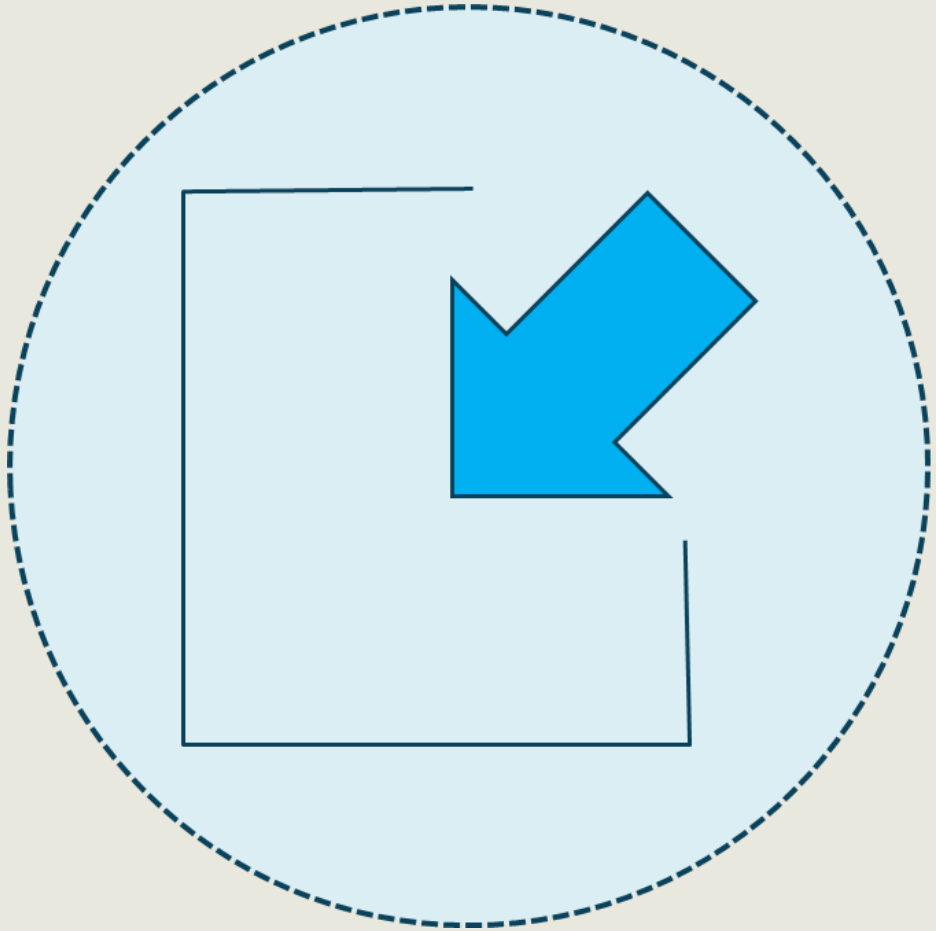
Commercial Classifications

- Corporate confidential
- Personal confidential
- Trade secret/proprietary
- Private
- Public

Roles and Responsibilities

- Chief privacy officer
  - Ensures privacy of all data in the entire organization
- Owner
  - Owner of the information
  - Determines classification level
- Steward
  - Manager of the data and metadata
  - Ensures compliance (standards/controls) and data quality
- Custodian
  - Keeper of the information
  - Ensures C.I.A. is maintained
- Processors
  - Handles data entry and input

Data Minimization for Privacy



- A directive that states that collected and processed data should not be kept or used unless it is critical
- The details should be determined early in the lifecycle to support data privacy standards, such as GDPR

Tokenization for Privacy Enhancement

- Data tokenization is a technique used to remove directly identifying elements
- The process replaces the raw data with randomly generated tokens (or pseudonyms)
- It is most often deployed with structured data, like payment cards or Social Security numbers
- The original data does not leave the enterprise in order to meet regulatory requirements
- Tokenization and encryption can be used together to further achieve data defense in depth

Additional Privacy Concepts

Information life cycle

Impact assessment

Terms of agreement

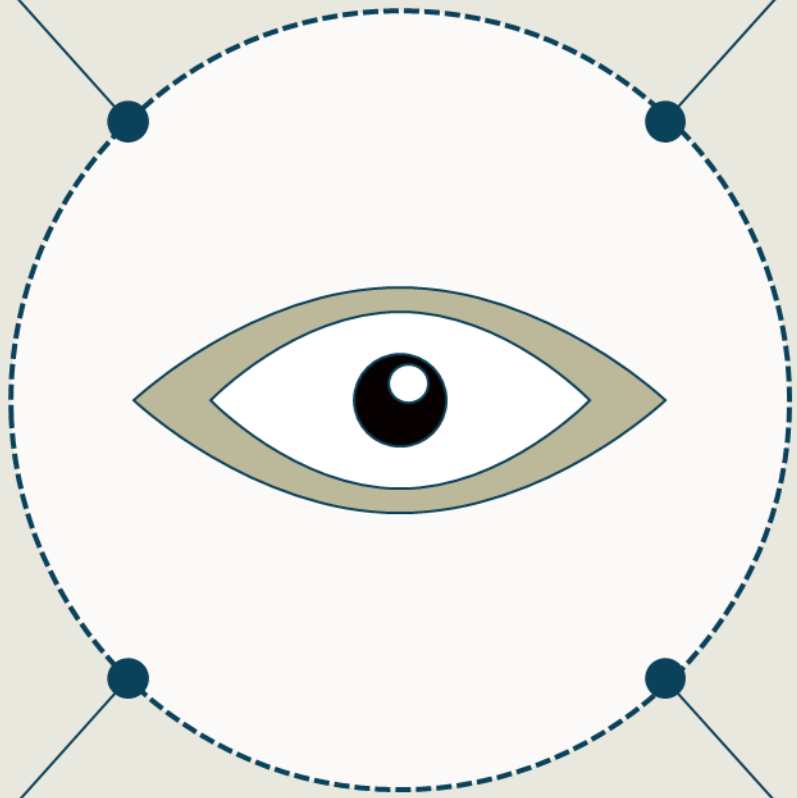
Privacy notices

Open-Source Intelligence (OSINT)

- OSINT is any data or information that can collected legally from free, public sources concerning an individual or organization
- It is usually information found on the Internet, but can be sourced from books or reports in a public library, articles in a newspaper/magazine, statements in a press release, and FOIA reports
- Can be gathered using tools like Maltego, sharing centers, and code repositories like GitHub, among others

Other Vulnerability Intelligence Sources

- Automated Indicator Sharing (AIS)
- Structured Threat Information Exchange (STIX)



- Predictive analysis and threat maps
- Trusted Automated eXchange of Indicator Information (TAXII)

Research Sources

- Vendor web sites
- Vulnerability feeds
- Conferences
- Academic journals
- Request for Comments (RFC)
- Local industry groups

Research Sources

Social media

Threat feeds

Adversary tactics, techniques, and procedures (TTP)

OSINT tools

Emerging social media tools

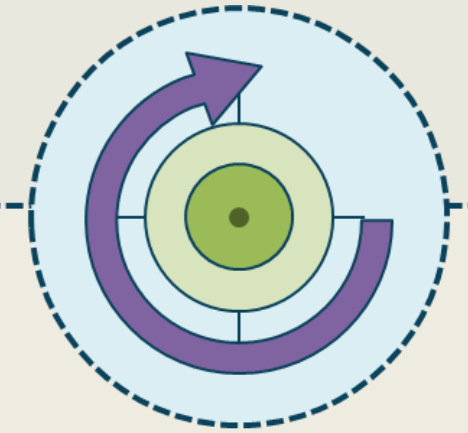
Word of mouth

Threat Hunting

Also called Hunt Teams

- Threat hunting involves groups of cyber investigators aggressively seeking out threats on a network or system
- They are often compliance or regulatory auditors
- They attempt to quickly recognize anomalies and discover historic patterns in data and Indicators of Compromise (IoCs) to counter cybercriminals and mitigate threats

Threat Hunting



Intelligence fusion:
Proactively seeking out threats before they occur

Threat feeds:
Information gathering from real-time sources

Advisories and bulletins:
Alerts from various vendors and organizations like @RISK from SANS.ORG

Vulnerability Scanning

- Vulnerability scanning is the process of identifying known and unknown weaknesses in systems, applications, services, and policies using tools
- Vulnerability scanning is an easier and often more focused process looking for unpatched systems, misconfigurations, and open ports
- It is typically automated and done on a routine basis (weekly, quarterly), taking at most a few hours

Scanning and Testing Results

True Positive = accurate + action taken

True Negative = accurate + action not taken

False Positive = error + action taken

False Negative = error + action not taken

Sources of Vulnerability Scans

Involves tools and techniques

- Various logs (system, application, firewall, etc.)
- Simple Network Management Protocol (SNMP) traps and informs
- NetFlow v5 and v9 collections
- Security information and event management (SIEM) systems
- Security Orchestration, Automation, and Response (SOAR)
- Next-Generation Intrusion Prevention System (NGIPS) alerts and logs
- Cloud-based ML and AI visibility/analysis

Vulnerability Databases

Common Vulnerabilities and Exposures (CVE)

- A list of entities from MITRE.org that represent publicly known cybersecurity vulnerabilities
- Consists of an ID number, description, and public references
- Used by the National Vulnerability Database (NVD)

Common Vulnerability Scoring System (CVSS)

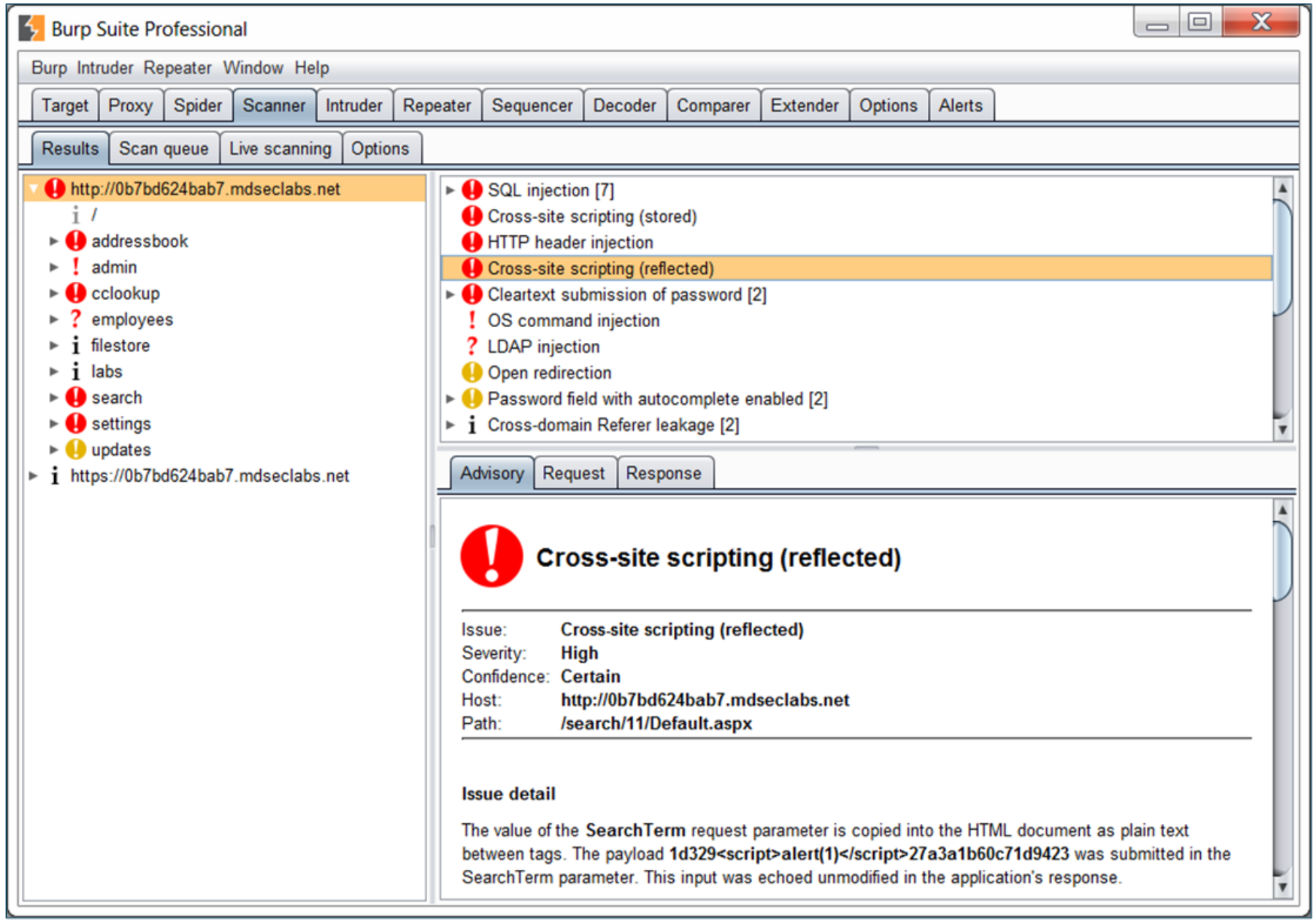
- Open standard for weighing the severity of computer system vulnerabilities
- Uses a uniform and consistent scoring method ranging from 0 to 10, with 10 being the highest severity

Web Vulnerability Scanning

- The most common vulnerability scanners will test web applications and services to look for:
  - Cross-site scripting and request forgery
  - SQL and other command injection
  - Broken authentication and session management
  - Insecure direct object references
  - Insecure server configuration (XML, PHP, etc.)
  - Exposing sensitive data

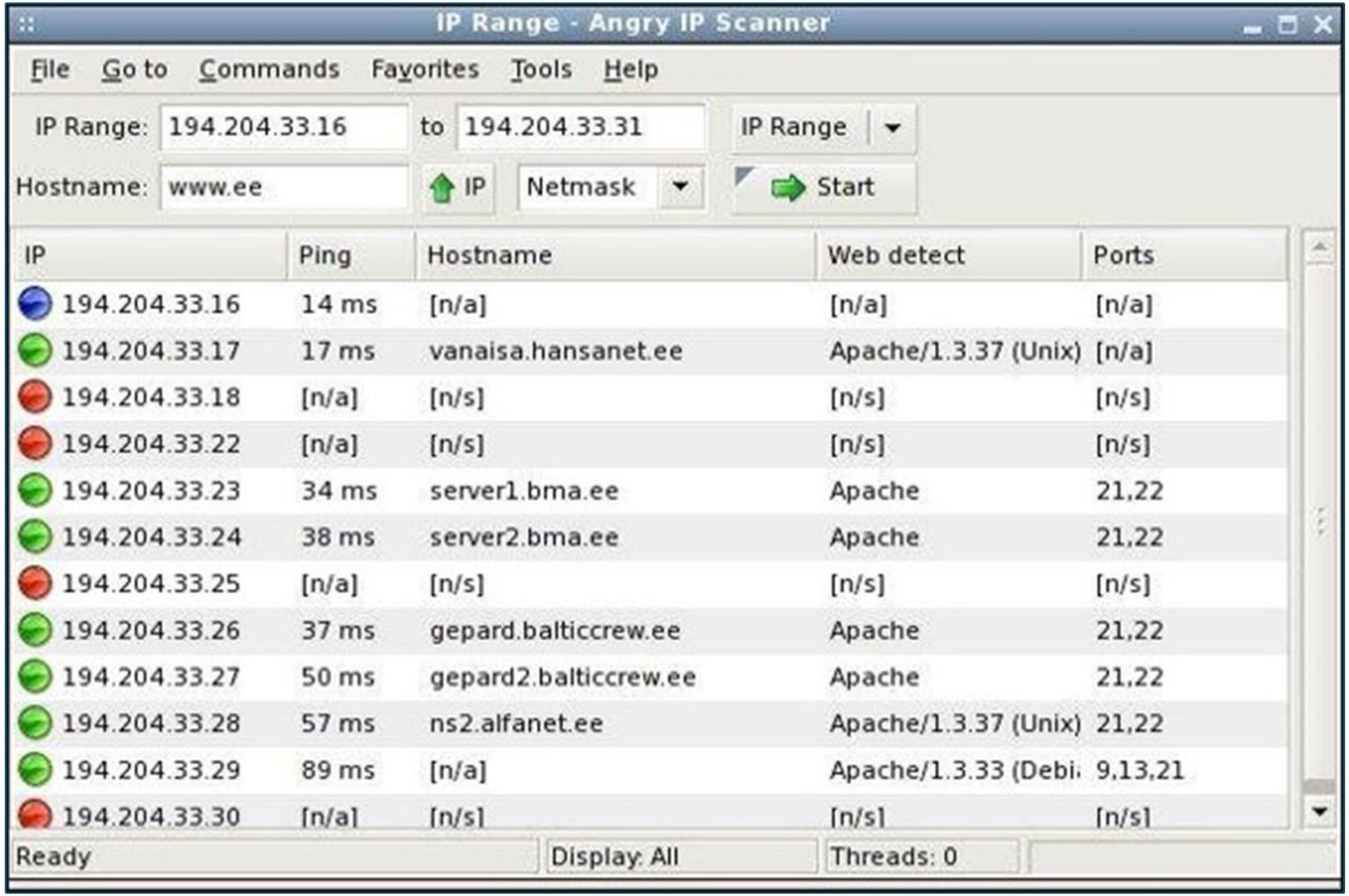
Vulnerability Scanning Toolkits

- Nessus
- OpenVAS
- Core Impact
- Nexpose
- GFI LanGuard
- QualysGuard
- OWASP ZAP
- Burp Suite


Burp Suite Professional
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Results Scan queue Live scanning Options
http://0b7bd624bab7.mdseclabs.net
/
addressbook
admin
cclookup
employees
filestore
labs
search
settings
updates
https://0b7bd624bab7.mdseclabs.net
SQL injection [7]
Cross-site scripting (stored)
HTTP header injection
Cross-site scripting (reflected)
Cleartext submission of password [2]
OS command injection
LDAP injection
Open redirection
Password field with autocomplete enabled [2]
Cross-domain Referer leakage [2]
Advisory Request Response
Cross-site scripting (reflected)
Issue: Cross-site scripting (reflected)
Severity: High
Confidence: Certain
Host: http://0b7bd624bab7.mdseclabs.net
Path: /search/11/Default.aspx
Issue detail
The value of the SearchTerm request parameter is copied into the HTML document as plain text between tags. The payload 1d329<script>alert(1)</script>27a3a1b60c71d9423 was submitted in the SearchTerm parameter. This input was echoed unmodified in the application's response.

Network Scanning Tools

- Network scanners can be used to scan IP addresses, ports, and device locations presented in a customized graphical XML view
- Most provide network monitoring and management capabilities to detect, diagnose, and resolve network issues and outages
- Active malware worms are also considered network scanners


IP Range - Angry IP Scanner
File Go to Commands Favorites Tools Help
IP Range: 194.204.33.16 to 194.204.33.31 IP Range
Hostname: www.ee IP Netmask Start
IP Ping Hostname Web detect Ports
194.204.33.16 14 ms [n/a] [n/a] [n/a]
194.204.33.17 17 ms vanaisa.hansanet.ee Apache/1.3.37 (Unix) [n/a]
194.204.33.18 [n/a] [n/s] [n/s] [n/s]
194.204.33.22 [n/a] [n/s] [n/s] [n/s]
194.204.33.23 34 ms server1.bma.ee Apache 21,22
194.204.33.24 38 ms server2.bma.ee Apache 21,22
194.204.33.25 [n/a] [n/s] [n/s] [n/s]
194.204.33.26 37 ms gepard.balticcrew.ee Apache 21,22
194.204.33.27 50 ms gepard2.balticcrew.ee Apache 21,22
194.204.33.28 57 ms ns2.alfanet.ee Apache/1.3.37 (Unix) 21,22
194.204.33.29 89 ms [n/a] Apache/1.3.33 (Debi 9,13,21
194.204.33.30 [n/a] [n/s] [n/s] [n/s]
Ready Display: All Threads: 0

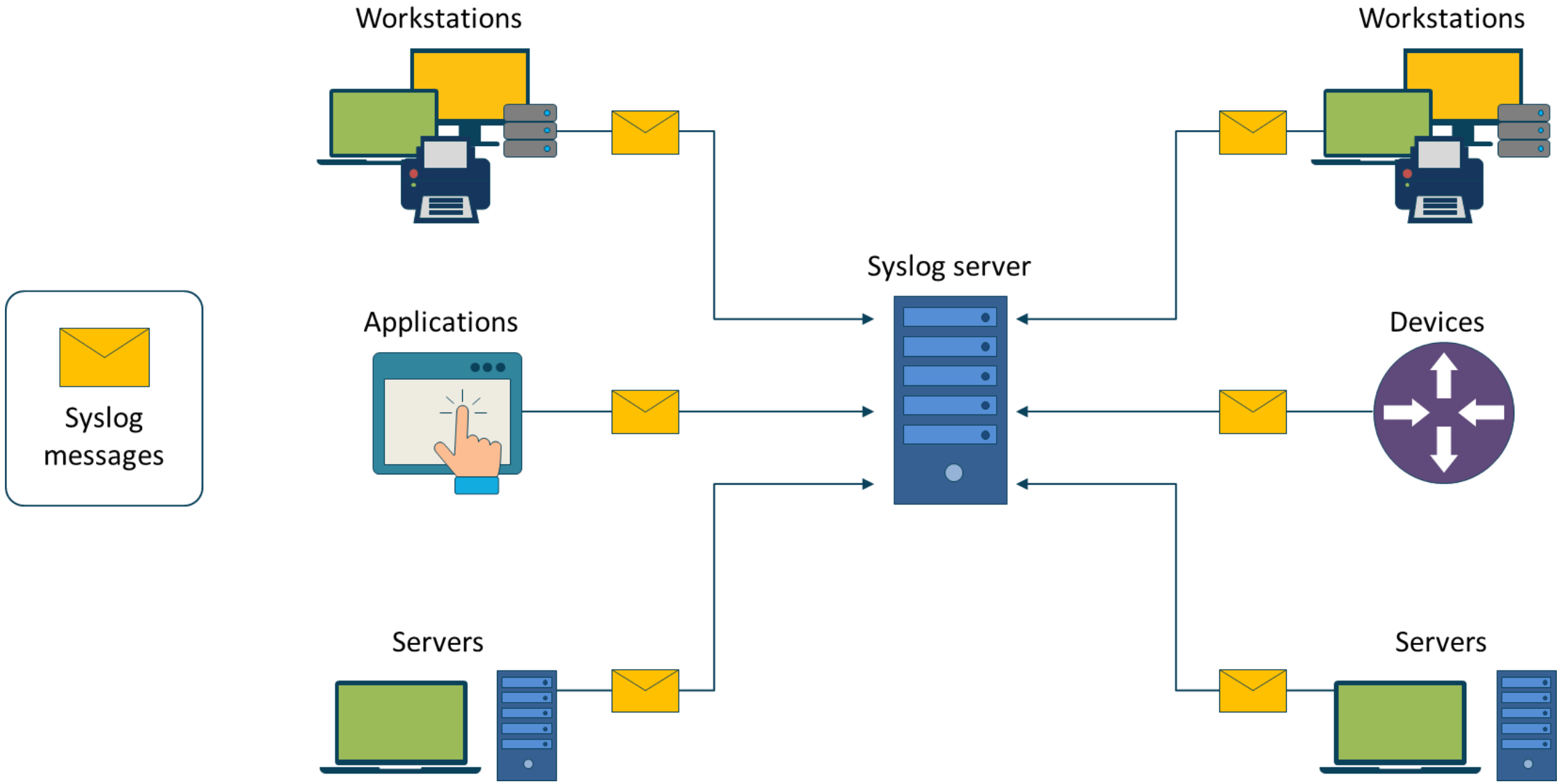
Compliance Scanning

- Different from performing a vulnerability scan, although there can be some overlap
- Compliance audit decides if a system is configured in agreement with a recognized governance policy whereas a vulnerability scan determines if the system is exposed to known vulnerabilities
- Sometimes compliance involves auditing more sensitive data and systems
- There are many diverse forms of financial and government compliance requirements
- Typically, the compliance requirements are minimal baselines that can be taken differently depending on the goals of the organization
- Compliance requirements must be in line with the business goals to ensure that risks are correctly recognized and alleviated

System Logging (syslog)

- Syslog is a standard and well-established system logging protocol defined in RFC 5424
- It typically sends system informational or event messages to a designated syslog server or SIEM system
- It is predominantly used to gather various device logs from different systems in a centralized fashion for monitoring, visibility, and analysis
- It traditionally uses UDP 514 or TCP 1468

Syslog


Workstations
Workstations
Syslog server
Applications
Devices
Syslog
messages
Servers
Servers

Syslog Severity Levels

Code	Severity	Description
0	Emergency	System is unusable
1	Alert	Action must be taken immediately
2	Critical	Critical conditions
3	Error	Error conditions
4	Warning	Warning conditions
5	Notice	Normal but significant condition
6	Information	Informational messages
7	Debug	Debug-level messages

SIEM

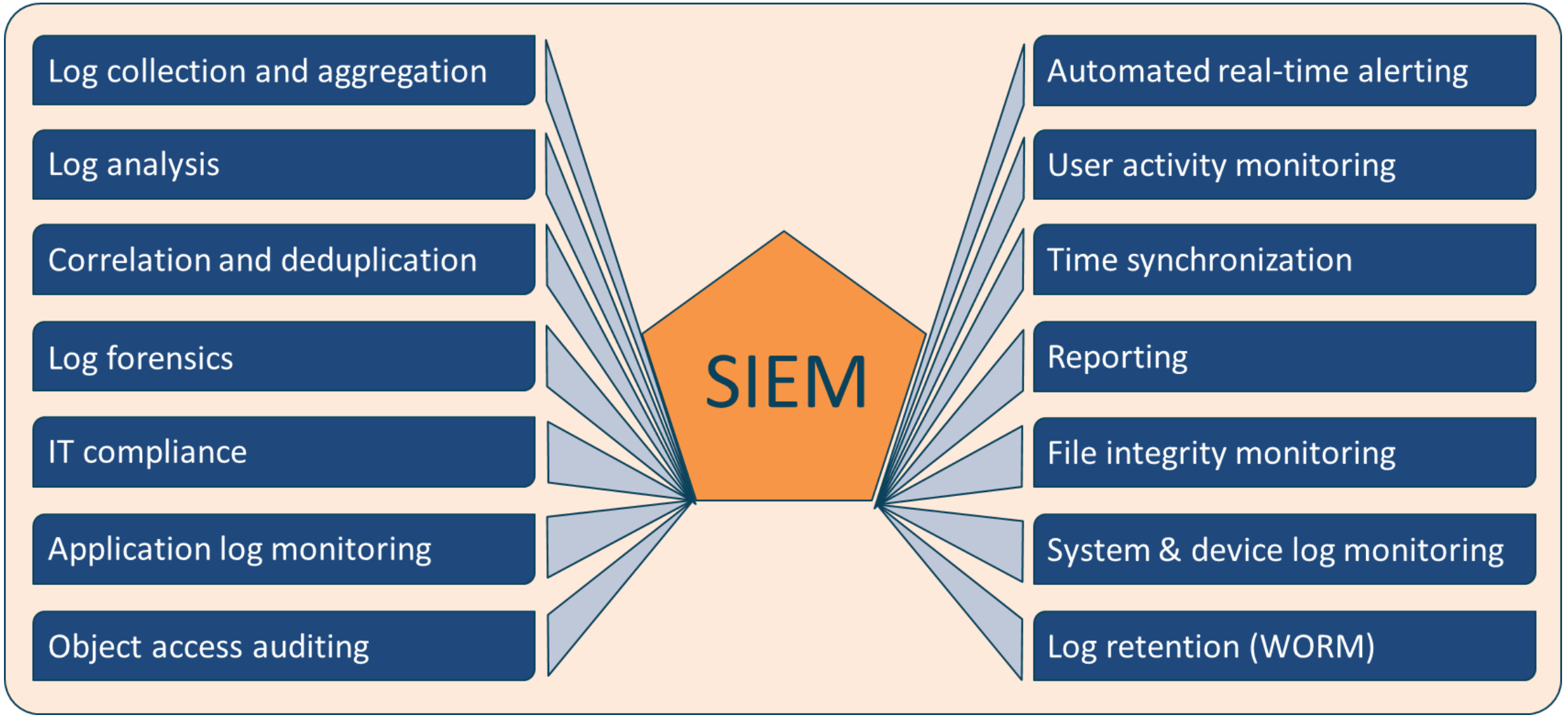
The term SIEM is a combination of security event management (SEM) and security information management (SIM)

Centralize the storage and analysis of logs and other security-related documentation to perform near real-time analysis

Can send filtered data to mining, big query, and data warehousing servers in a data center or at a cloud service provider

Allow security and network professionals to take countermeasures, perform rapid defensive actions, and handle incidents

SIEM


Log collection and aggregation
Log analysis
Correlation and deduplication
Log forensics
IT compliance
Application log monitoring
Object access auditing
SIEM
Automated real-time alerting
User activity monitoring
Time synchronization
Reporting
File integrity monitoring
System & device log monitoring
Log retention (WORM)

Common SIEM Data Sources

Automation and Orchestration

Automation

- IT automation involves generating a single task to run automatically without any human intervention
- Automation could involve sending alerts to a SIEM system, dynamically triggering a serverless function at a cloud provider, or adding a record to a database when a batch job is run
- Enterprises often automate both cloud-based and on-premise tasks

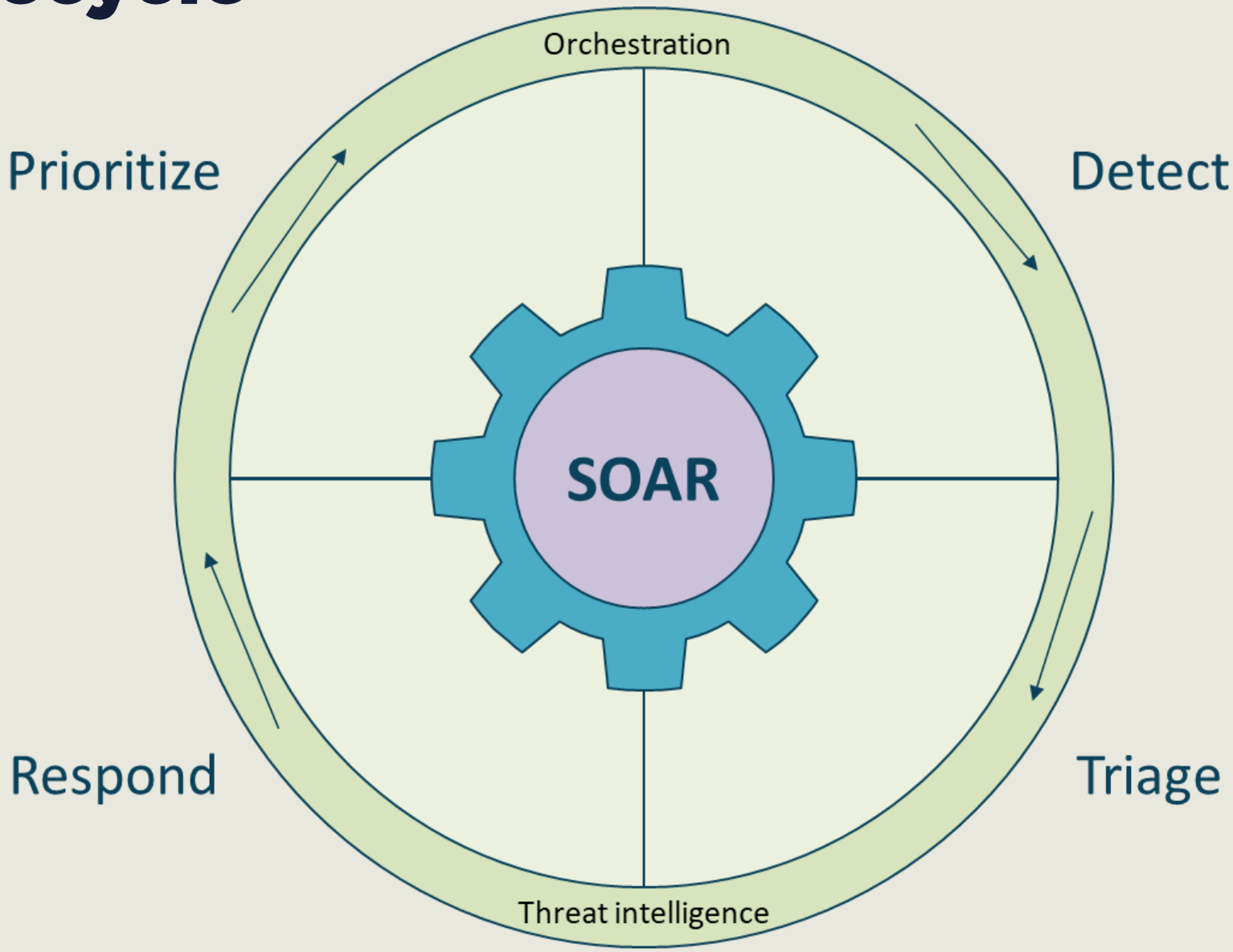
Orchestration

- Orchestration involves managing several or many automated tasks or processes
- As opposed to focusing on one task, orchestration combines all the individual tasks
- Orchestration occurs with various technologies, applications, containers, datasets, middleware, systems, and more

Security Orchestration, Automation, and Response (SOAR)

- SOAR is an assortment of software services and tools
- It allows organizations to simplify and aggregate security operations in three core areas
  - Threat and vulnerability management
  - Incident response
  - Security operations automation
- Security automation involves performing security related tasks without the need for human intervention
- Can be defensive detection, response, and remediation, or offensive vulnerability assessment and penetration testing
- You should automate if the process is routine, monotonous, and time-intensive

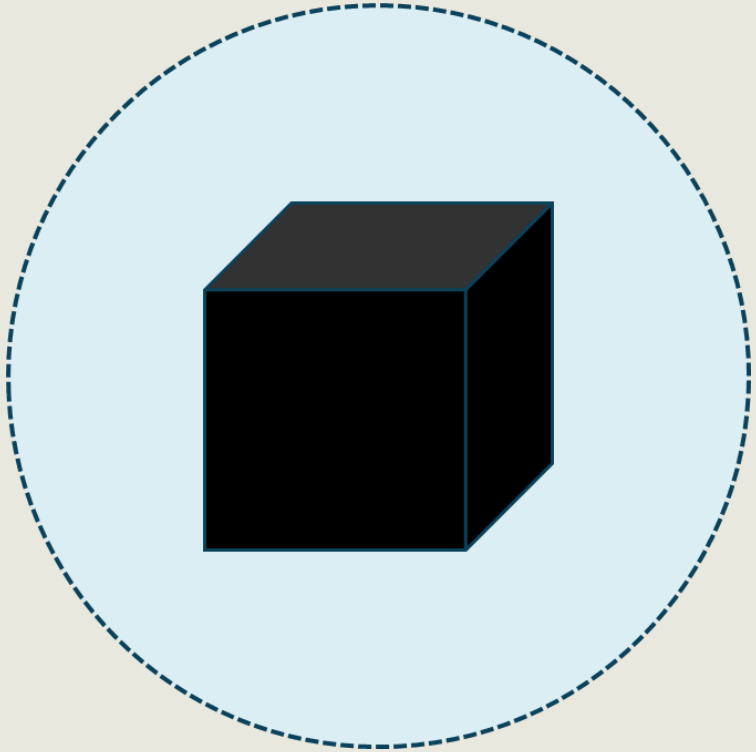
SOAR Lifecycle



Penetration Testing

- Penetration testing is security testing in which assessors simulate real-world attacks to identify methods for evading the security features of an application, system, or network
- Often involves launching real attacks on real systems and data that use tools and techniques commonly used by attackers
- Penetration testing can also be useful for determining:
  - How well the system tolerates real world-style attack patterns
  - The likely level of sophistication an attacker needs to successfully compromise the system
  - Additional countermeasures that could mitigate threats against the system
  - The defenders' ability to detect attacks and respond appropriately

Black Box Testing



- Black box is a technique of testing without having any knowledge of the internal working of the application
- It only examines the fundamental aspects of the system and has no or little relevance with the internal logical structure of the system
- Black box testing is also software testing method in which the internal structure, design, or implementation of the component being tested is NOT known to the tester

White Box Testing

- White box testing techniques involve the detailed investigation of internal logic, structure, and configuration of the application or system
- It is often desirable or necessary for a pentester to have full knowledge of target application or system
- The internal structure, design, and implementation of the component being tested is fully known to the tester
- A gray box testing technique is having some limited knowledge of the internal workings of the target

Other Pentesting Terms

- Credentialed vs. non-credentialed testing involves the decision to use an existing directory user account
  - Credentialed tests would be considered a white box or gray box approach
- Intrusive vs. non-intrusive
  - (also passive vs. active)
- Promiscuous vs. inline
- Spamming or flooding vs. packet sniffing

Passive Reconnaissance

- Less-intrusive process to daily operations and employee productivity used in early stages
- Passive reconnaissance and testing involves using wired and wireless packet sniffers, passive scanners, or network taps
- Goal is to gather metadata and copies of frames or packets to observe the contents with no remaining footprint
- Firewalls and other appliances have CLI-based and GUI packet tracer capabilities

Passive Reconnaissance

- Less-intrusive process to daily operations and employee productivity used in early stages
- Passive reconnaissance and testing involve using wired and wireless packet sniffers, passive scanners, or network taps
- Goal is to gather metadata and copies of frames or packets to observe the contents with no remaining footprint
- Firewalls and other appliances have CLI-based and GUI packet tracer capabilities

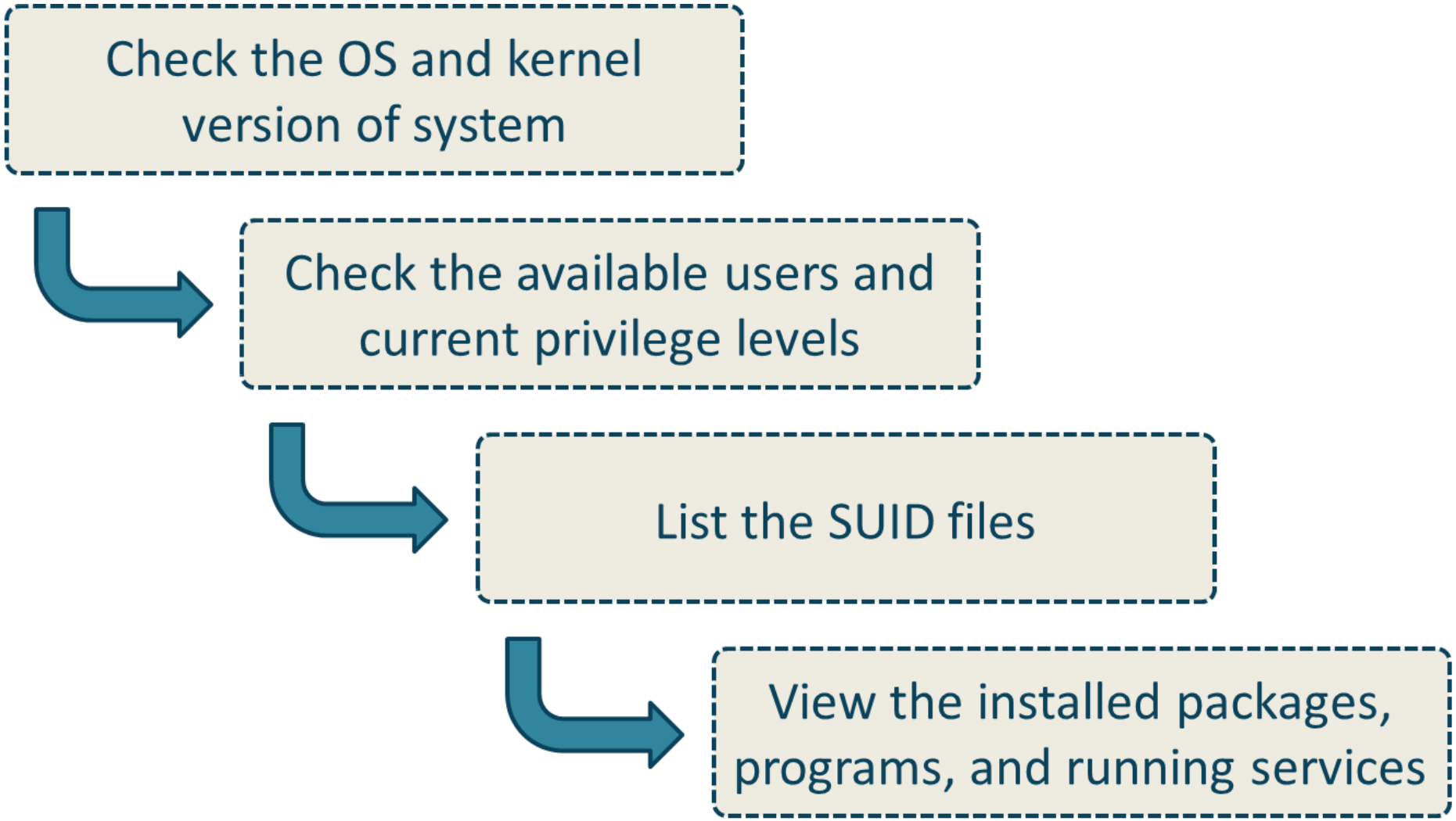
Active Reconnaissance

- Active reconnaissance and testing typically involves an action on a target endpoint or network that could be traced back to the attacker
- Examples include:
  - Running a web application scanner like OWASP ZAP
  - Conducting Nessus port and address scanning
  - Using vulnerability scanning tools in active modes
  - Banner grabbing
  - Active fingerprinting

Penetration Testing Methodology

- **Step 1: Rules of engagement agreement** (bug bounty?)
- **Step 2: Reconnaissance and initial engagement**
  - Before performing penetration testing you will conduct planning and preparation, information gathering (packet sniffing) and analysis, and passive and active vulnerability assessment
  - May also involve OSINT and social engineering
- **Step 3: Privilege escalation**
  - Attempting to get root or administrative credentials to as many systems as possible
  - CSP access keys and SSO credentials are very valuable

Examples of Linux Escalation of Privilege



Penetration Testing Methodology

- **Step 4: Lateral movement and pivoting**
  - Pivoting allows you to jump from one segment, domain, or system to another as in VLAN hopping, port forwarding, and trust exploits
- **Step 5: Persistence**
  - The code or script attempts to be persistent if there is a logoff, reboot, or network disconnect
  - Reverse telnet session bypasses firewalls and AV modules and remains connected persistently
- **Step 6: Cleanup**
  - Cover tracks and remove indicators of compromise

Exercise Teams

Red team

Offense

- Vulnerability assessments
- Penetration tests
- Social engineering

Purple team

Common goal

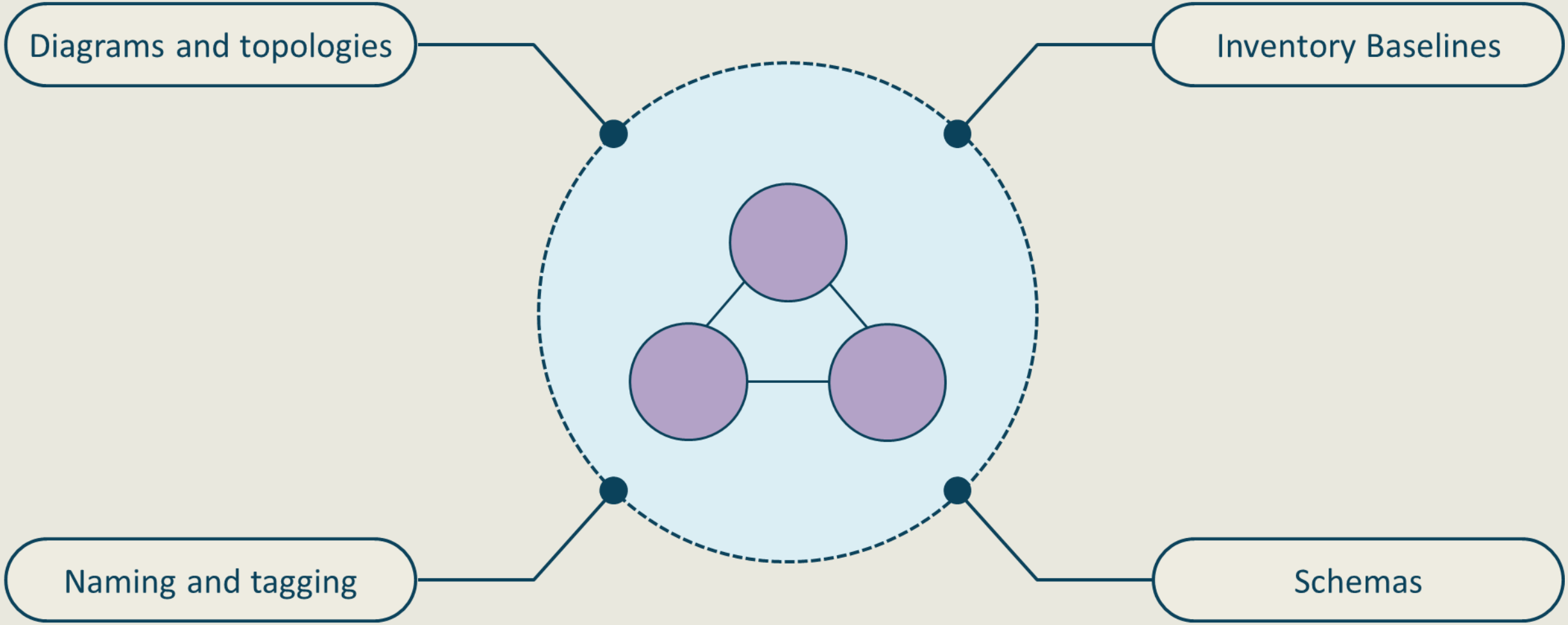
- Improving organization
- Security posture

Blue team

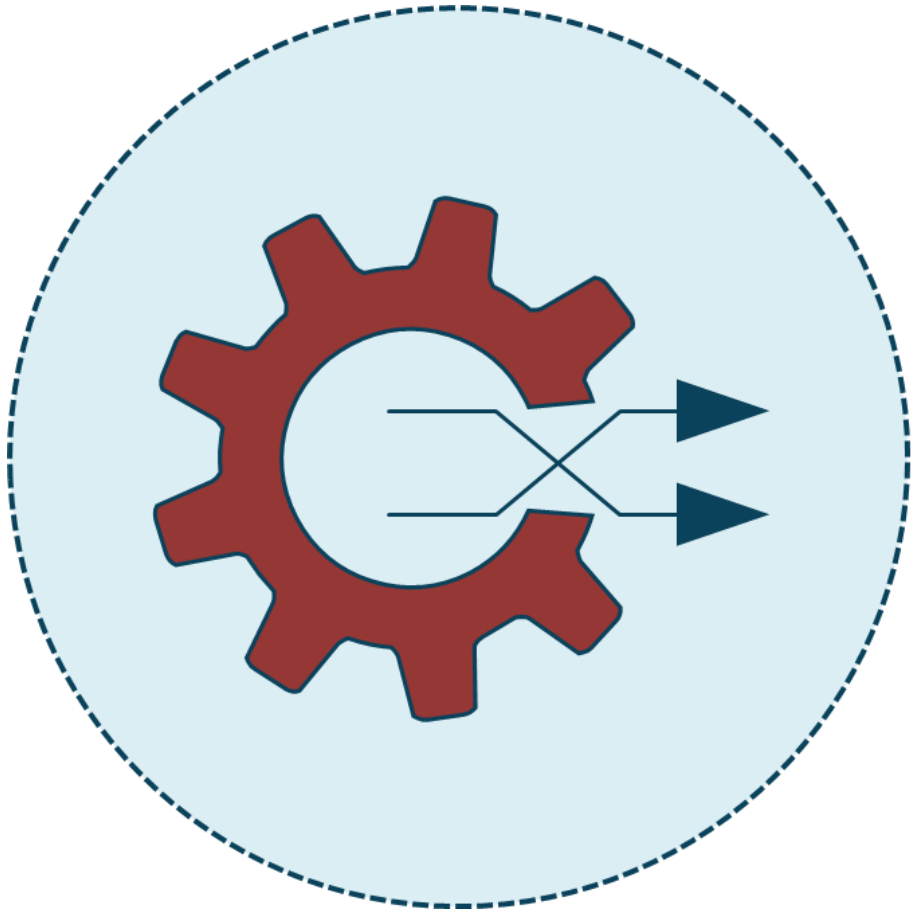
Defense

- Implementing controls
- Security monitoring
- Incident response

Configuration Management



Change Management

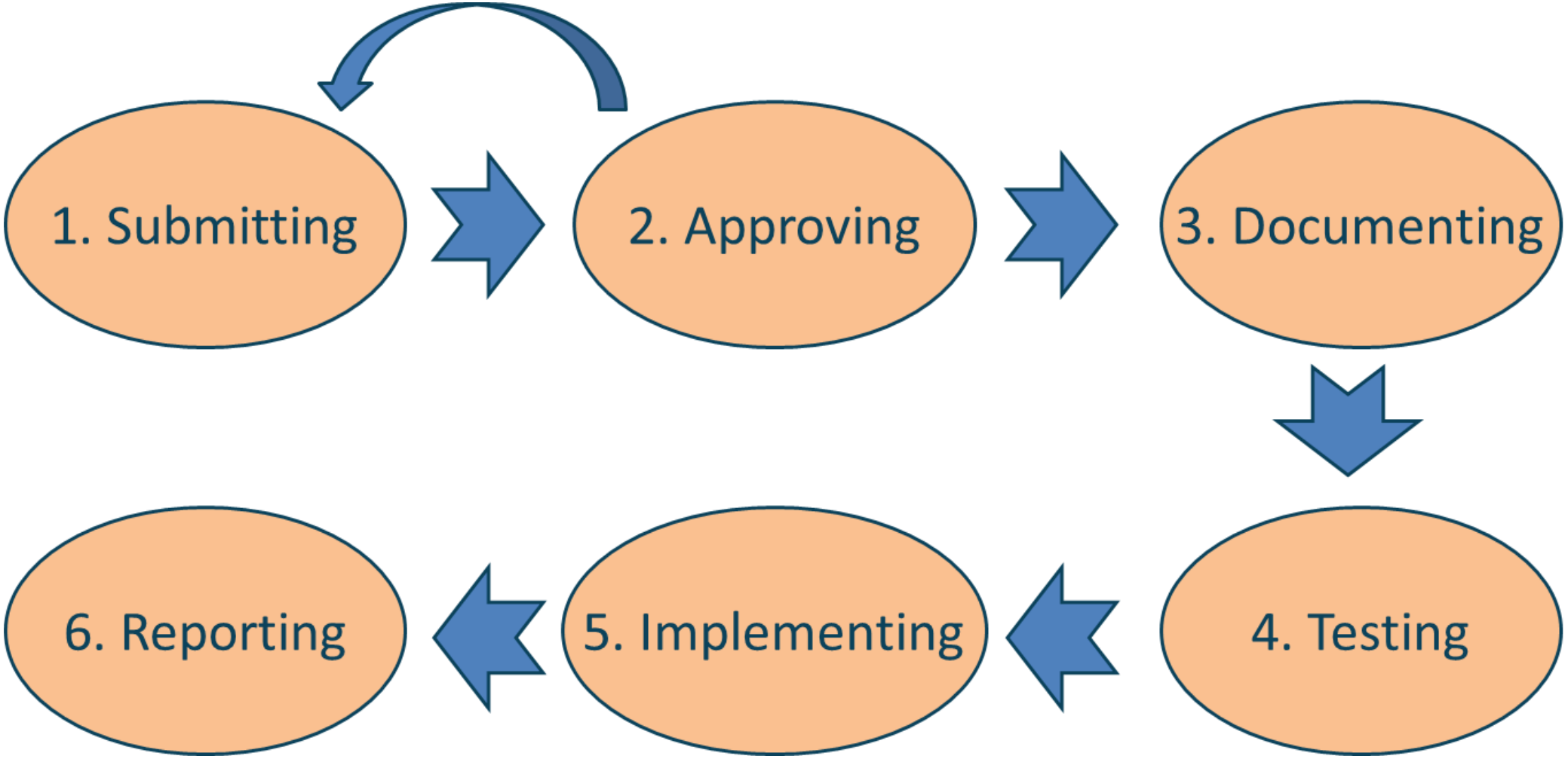


- Change management is also called a change control practice
- The goal is to maximize the amount of successful service and product changes
- Should make certain that risks have been adequately assessed, authorized, and managed with a change schedule
- Should involve a change log

Types of Changes

- **Standard** changes are low-risk, pre-authorized and well-documented - often service requests that don't need additional authorization
- **Normal** changes follow a specific process for scheduling, assessment, and authorization - low risk, but do go through an approval process
- **Emergency** changes must be implemented immediately and may involve an advisory board

Change Management Lifecycle



Change Management Lifecycle

1. Submitting

The proposed change is analyzed and validated. If necessary, the submitter may be required to provide more information before it is approved or escalate the change to a higher authority

Change Management Lifecycle

2. Approving

The proposed change request should first be delivered to the individual or group responsible for change management in the organization

Change Management Lifecycle

3. Documenting

After approval, the change needs to be inputted into a change log or configuration management database (CMDB). This log or database must be updated regularly as each change progresses through the various phases

Change Management Lifecycle

4. Testing

Before implementing the change, there may need to be a formal testing and verification process. This allows for modifications to be made if any issues arise. There can also be a determination if any other processes are affected by the change

Change Management Lifecycle

5. Implementing

After the change is tested and approved it can be deployed based on a schedule that has been determined. The schedule needs to document the projected phases of the change and define the milestones for the change process

Change Management Lifecycle

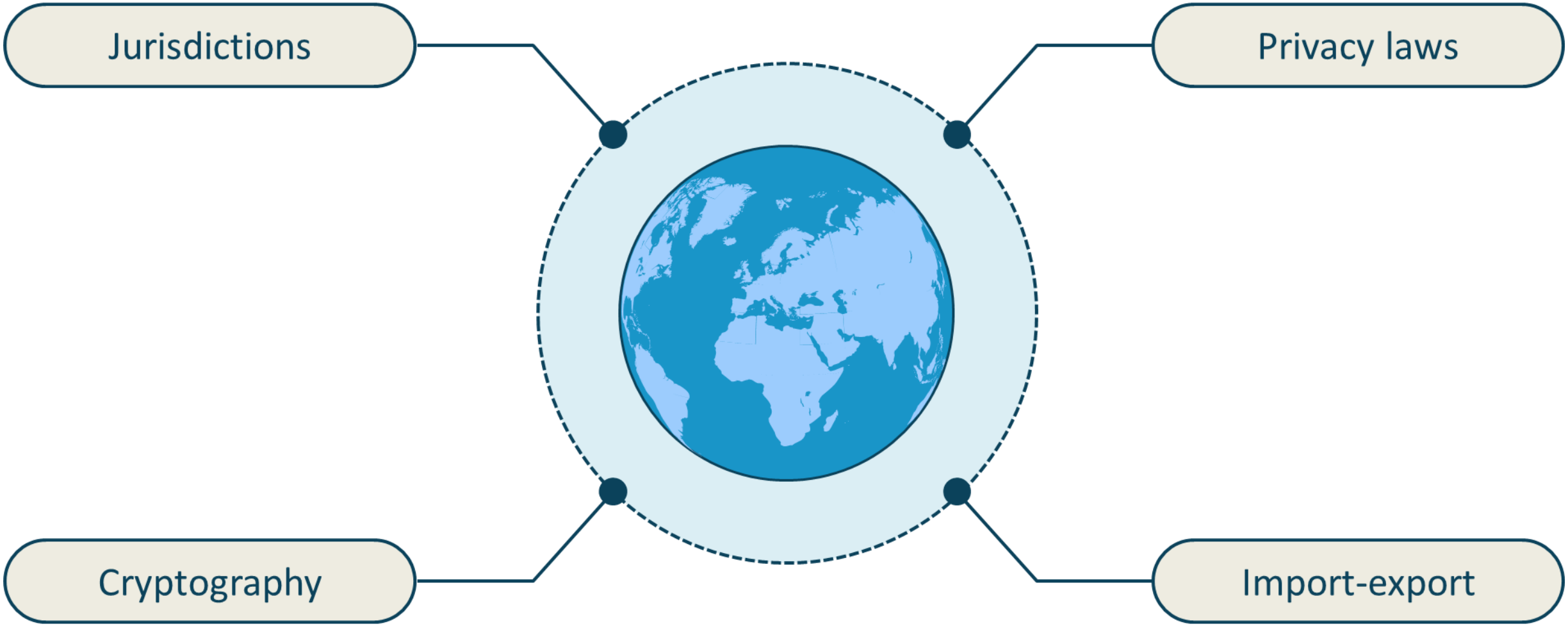
6. Reporting

After the change has been implemented a full report should be submitted to management. If there are any negative consequences to implementing the change, this should trigger an iterative move to an earlier phase of the lifecycle

Geographical Considerations for Data

- Where to store offsite data and backups
  - Distance - city, state, country, cloud
  - Location selection - can we operate or store there?
  - Security standards and practices
  - Legal implications and laws in that area
  - Data sovereignty
- Local geographic restrictions on mobile devices and corporate auto fleets can be enforced with geofencing

Geographical Considerations for Data



Data Sovereignty

- Data sovereignty issues can arise especially when sending or storing sensitive data in other jurisdictions or in different global regions
- The data ownership, custodianship, stewardship, and usage must be well-established and agreed-upon based on all legal and governmental directives
- There will also be variances in cultural norms, customs, sensitivity, behavior (e.g., Asian vs. European customs)
- Mandates began during the cold war to control transborder flow for example:
  - The International Traffic in Arms Regulations (ITAR)
    - Items covered under ITAR appear on a list called the United States Munitions List (USML)
  - Export Administration Regulations (EAR)

Cloud Computing Geolocation

Issues vary depending on governing regulations

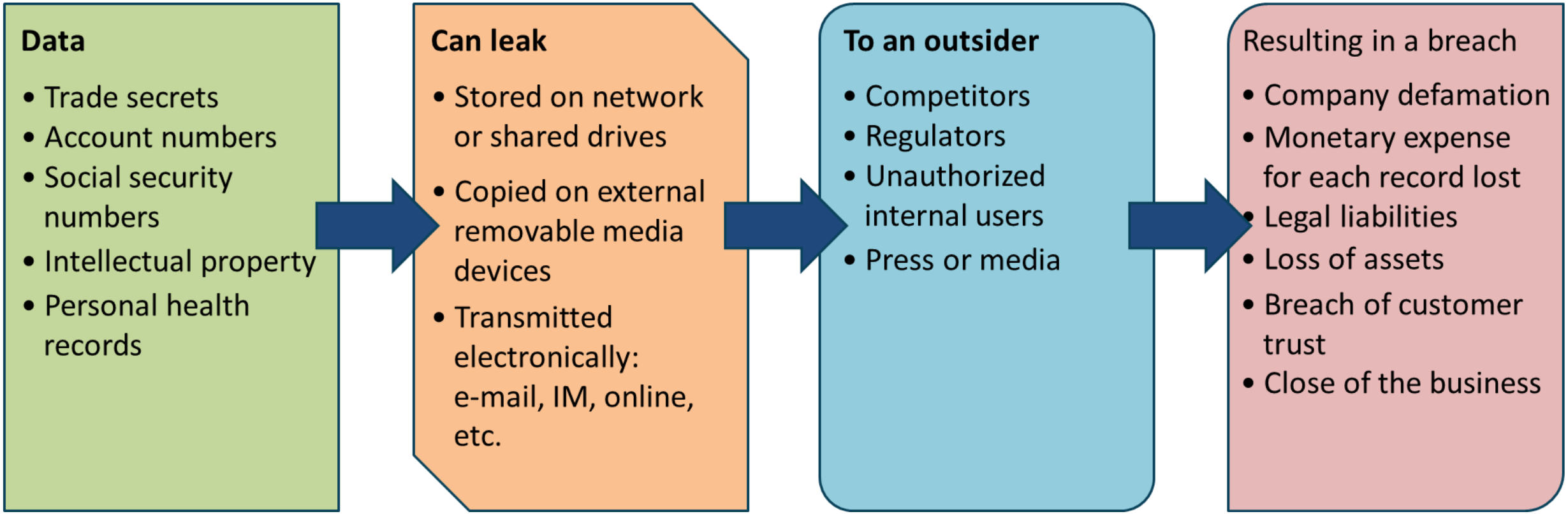
- According to NIST: "Shared cloud computing workloads can move from cloud servers located in one country to servers located in another country. Each country has its own laws for data security, privacy, and other aspects of information technology.“
- "Because the requirements of these laws may conflict with an organization's policies or mandates, an organization may decide that it needs to restrict which cloud servers it uses based on their location."

Cloud Computing Geolocation (cont.)

Issues vary depending on the countries involved

- "A common desire is to only use cloud servers physically located within the same country as the organization, or physically located in the same country as the origin of the information. Geolocation can be accomplished in many ways, with varying degrees of accuracy.“
- "But traditional geolocation methods are not secured and are enforced through management and operational controls that cannot be automated and scaled. Therefore, traditional geolocation methods cannot be trusted to meet cloud security needs."

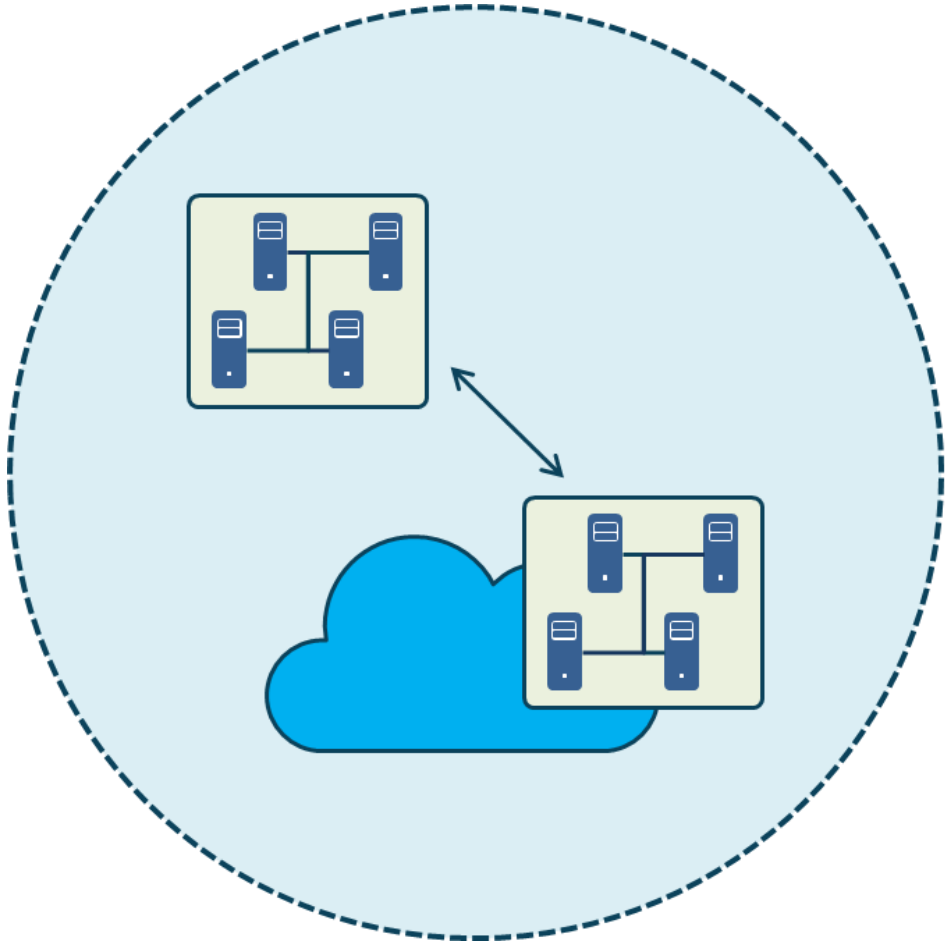
Data Loss Prevention (DLP)



Digital Rights Management (DRM)

- Digital rights management (DRM) mechanisms are varied access control technologies used to control usage of proprietary hardware and copyrighted works
- Organizations will often need to deploy systems within devices to enforce DRM policies
- DRM technologies attempt to manage the use, modification, and distribution of copyrighted software and multimedia content

Cloud Access Security Brokers (CASB)



- Software service implemented between cloud customer and Software as a Service provider
- Could be on-premise or in-service provider cloud
- Acts as a gatekeeper to help enforce enterprise security policies while cloud resources are being accessed

Response and Recovery Controls

- Security guards are a critical response control
  - Typically, 24x7, but varies per organization
  - Can be a deterrent, detective, and preventative control
  - Provides rapid security response if an intrusion or incident occurs
- Computer Security Incident Response Teams (CSIRT)
  - Can be an internal (swarm) team or third-party
  - Provides 24x7 incident response services to users, companies, government agencies, and organizations
  - Should deliver a reliable and trusted single point of contact for reporting computer security incidents
  - Should provide the means for reporting incidents and for disseminating important incident-related information
  - CSIRT will be the first responders in many scenarios and can also be involved in cyber forensics

Common Recovery Control Activities

Recovering data from backups and snapshots

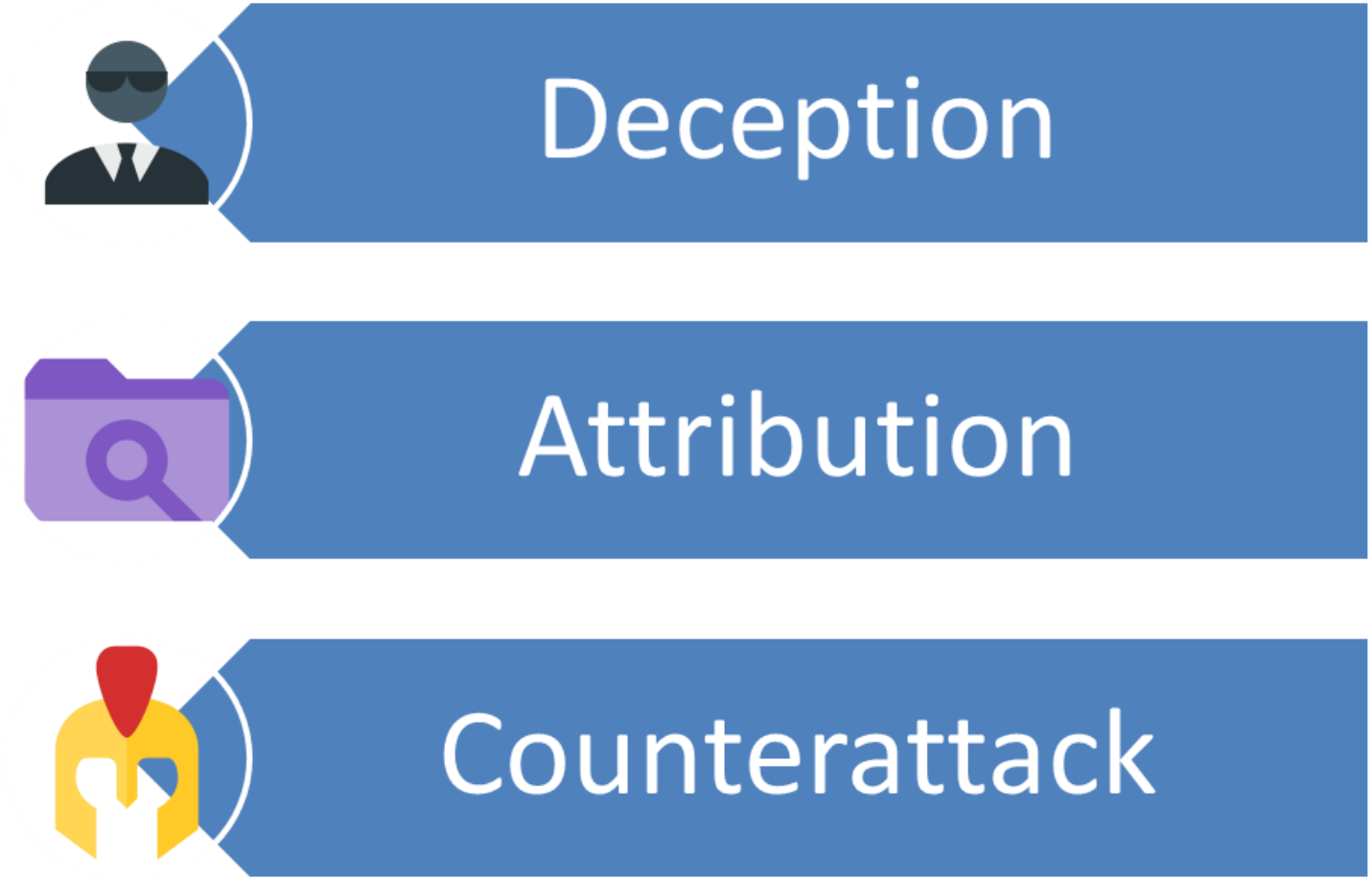
Conducting mobile device location and remote wiping

Developing and testing business continuity recovery plans

Determining RTO and RPO metrics for business impact analysis

Finding best disaster recovery sites

Active Defense



Active Defense: Deception and Disruption

Honeypots and evil twins are used in wireless networks to trap potential attackers and as a man-in-the-middle attack

Honeynets are entire physical and virtual subnets used to entice attackers for gathering intel and counterattacks

Honeyfiles or honey tokens are most often used to catch a privileged insider during a structured attack

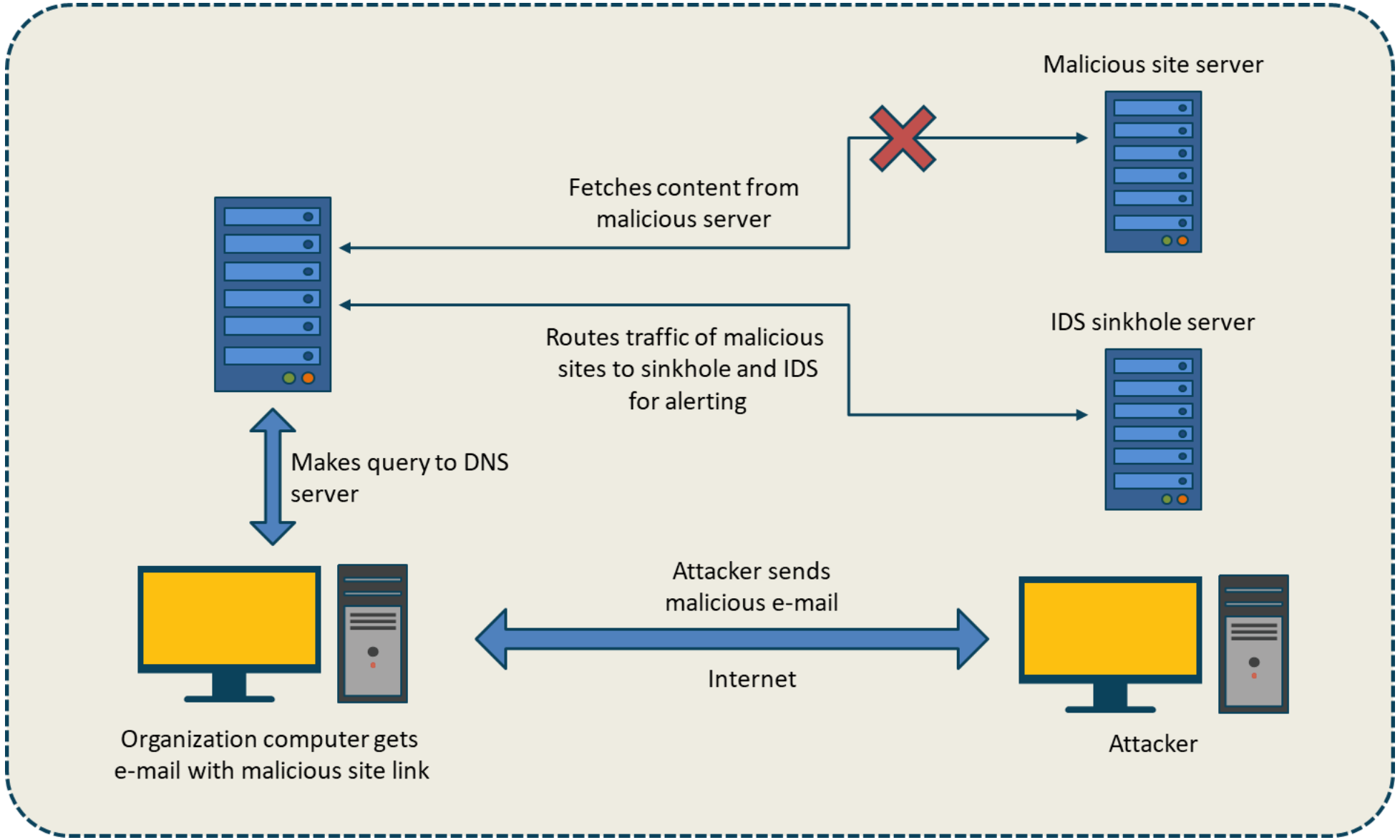
Active Defense: Fake Telemetry

- Deception has become a strategic tool used by many large organizations from several sectors
- Fake telemetry involves augmenting existing tools in the enterprise to offer critical threat intelligence for early breach detection and high-fidelity alerting

Active Defense: DNS Sinkhole

- Using DNS sinkholes, threat analysts can look at the malicious traffic in real time, monitor and analyze, then generate better prevention controls in the future
- Example: Botnet Filtering on a Cisco Adaptive Security Appliance

DNS Sinkhole

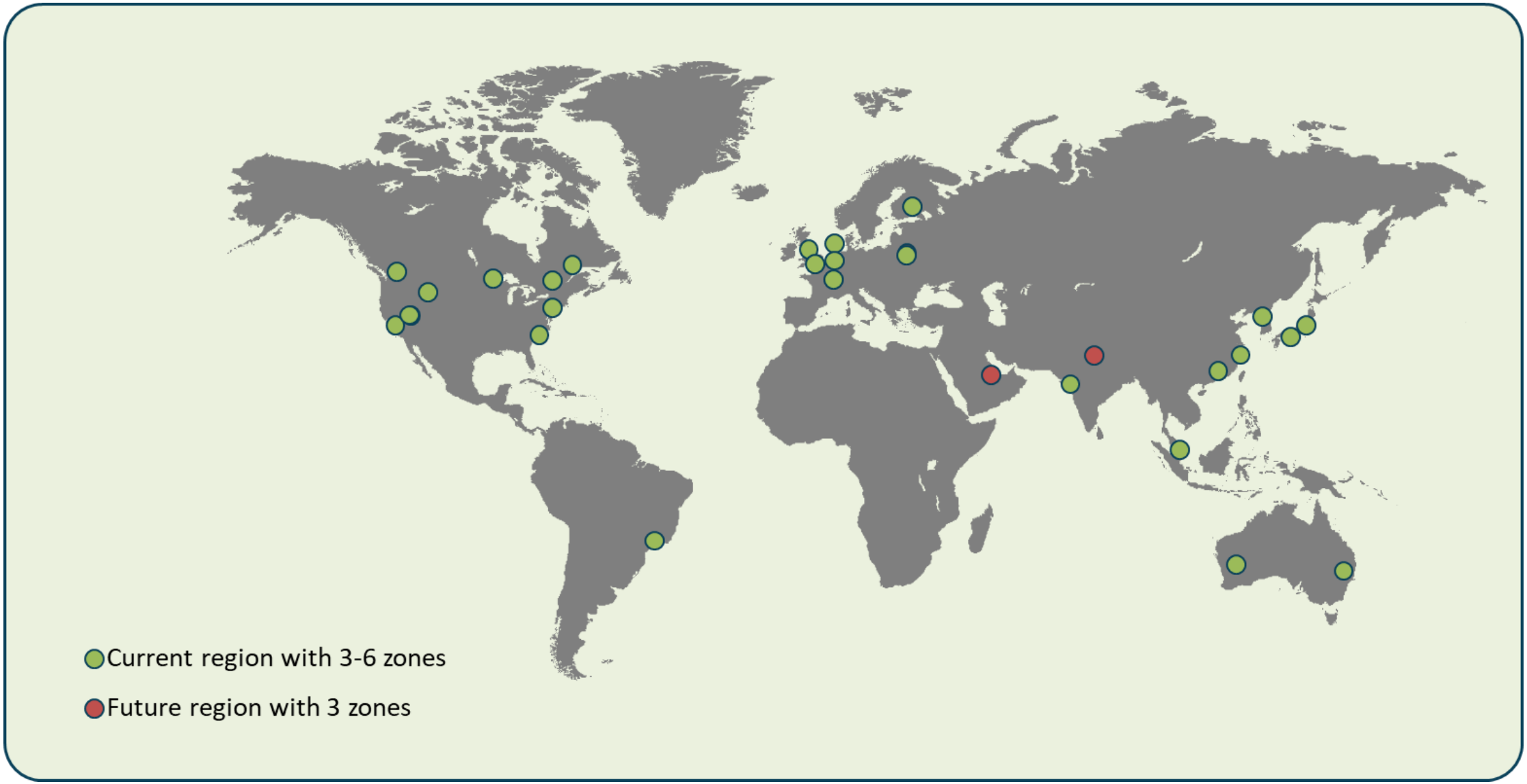


Redundancy Concepts

Duplication and geographical dispersal and to achieve high availability

- Proper dispersal of data and system backups are key aspects of a business continuity plan
- Eliminating single points of failure by duplicating systems and components either physically or virtually
- Redundancy includes storing spare physical components off site as well

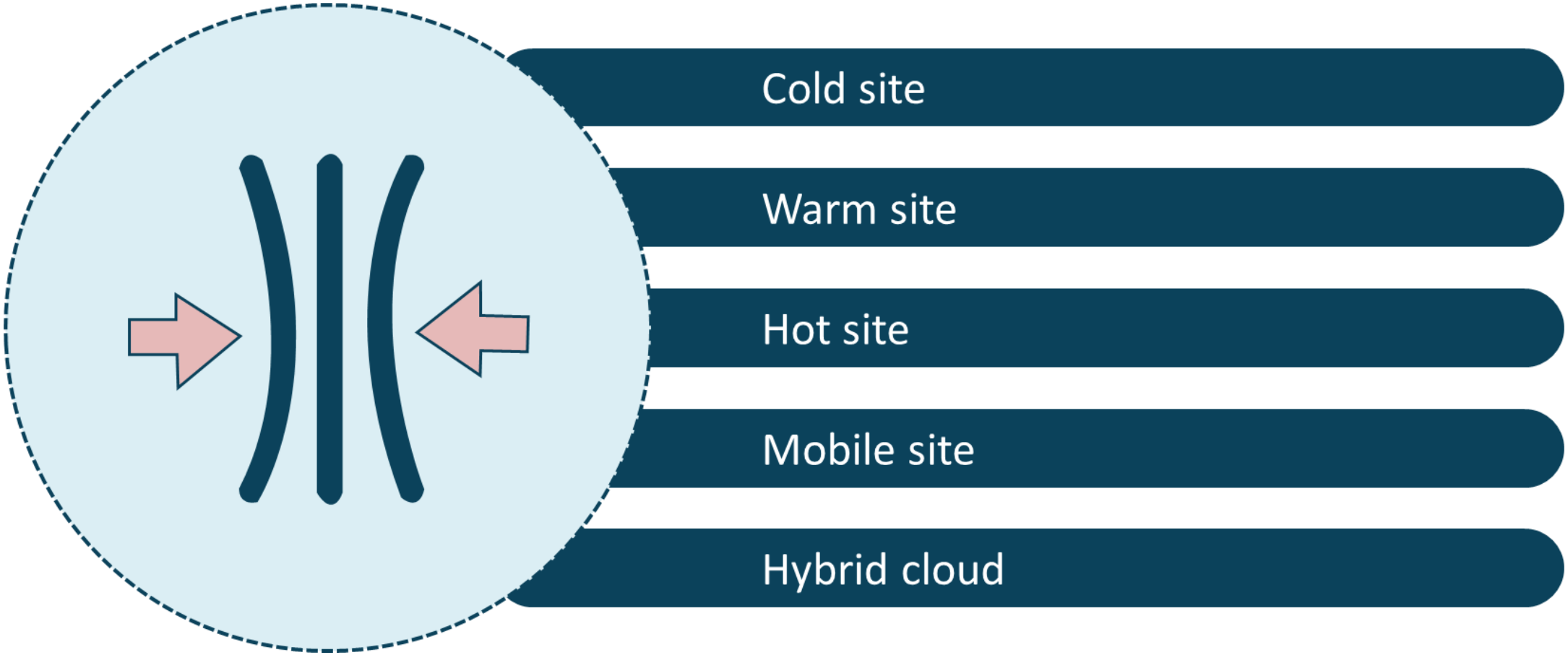
Amazon Web Services Regional Availability



Site Resiliency

- Resiliency is the capacity of a server, network, database, or storage system to rapidly recover and continue operations when a hardware failure, power outage, or other disruption occurs
- The more common term is "site resilience" and it refers to maintaining the durability and high-availability of mission critical services and data

Site Resiliency



Redundant Array of Independent Disks (RAID)

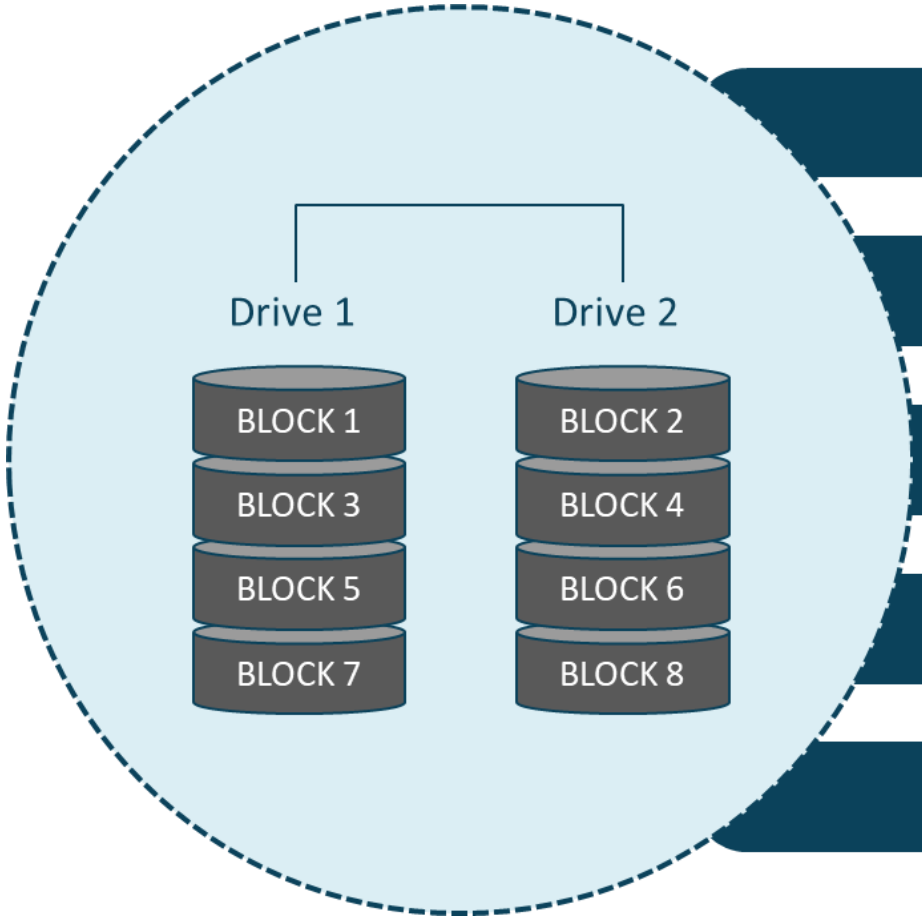
RAID 0

RAID 1 and 10

RAID 6

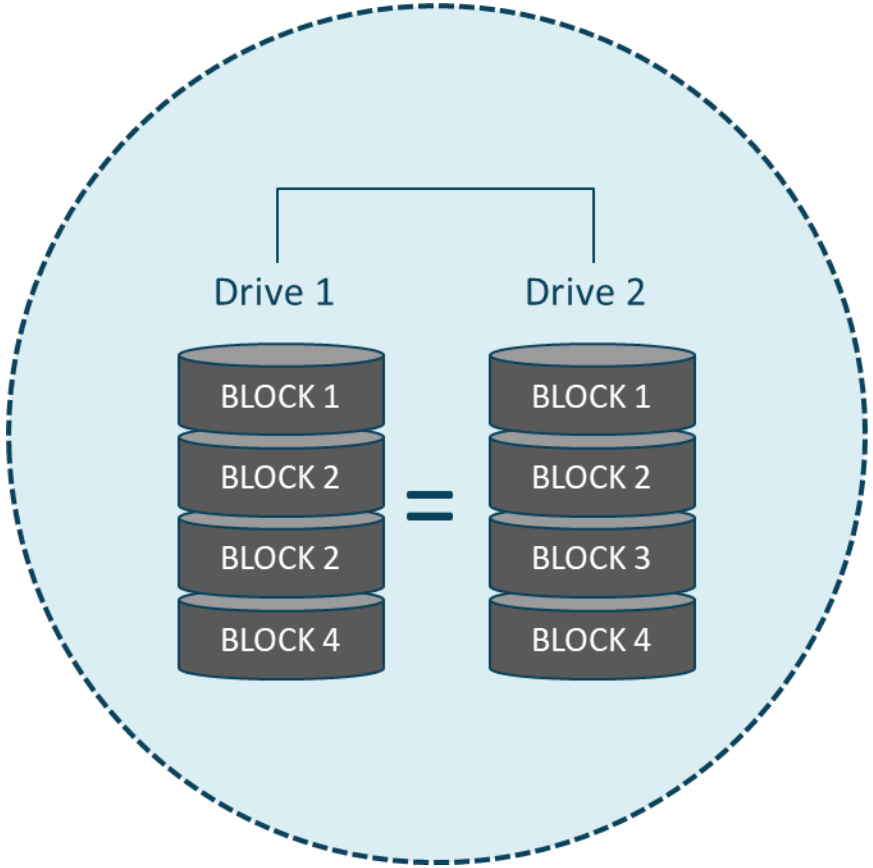
RAID 5

RAID Level 0



- Data is split up into blocks
- Blocks are written across all array drives
- Uses at least two disks at a time
- Offers fast read and write speeds
- Not redundant = no fault tolerance

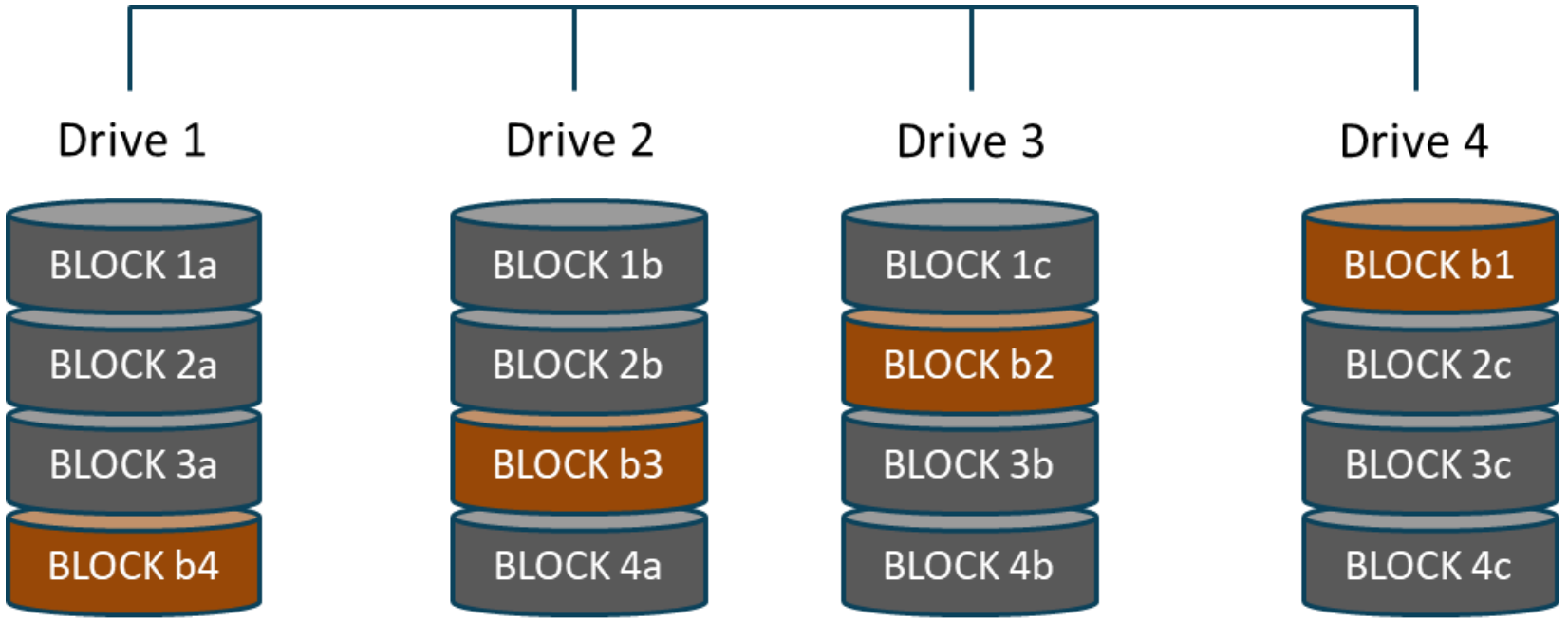
RAID Level 1 (Mirroring)



- Configuration of least two drives that contain the exact same data
- If one drive fails, the others will still function
- RAID 1 offers high read performance, as data can be read off any of the drives in the array
- Since data needs to be written to all the drives in the array, the write speed is slower than a RAID 0 array

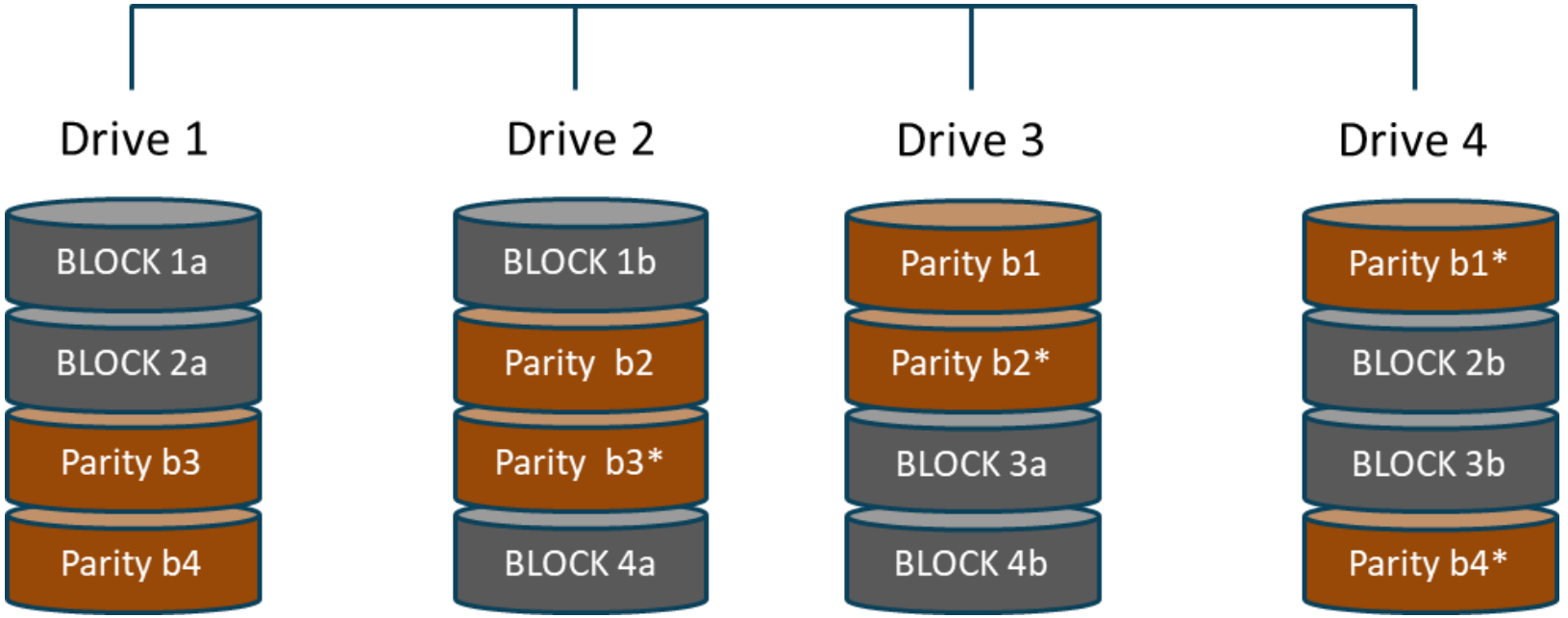
RAID Level 5

- RAID 5 requires at least three drives
- Data is striped across multiple drives, but also has "parity" data distributed across the drives
- Data is restored by using the parity information stored across the other drives
- Read times are very fast but the write speed is slower due to the parity that must be calculated
- The most popular RAID 5 configurations use four drives, which lowers the lost storage space to 25 percent (works with up to 16 drives)

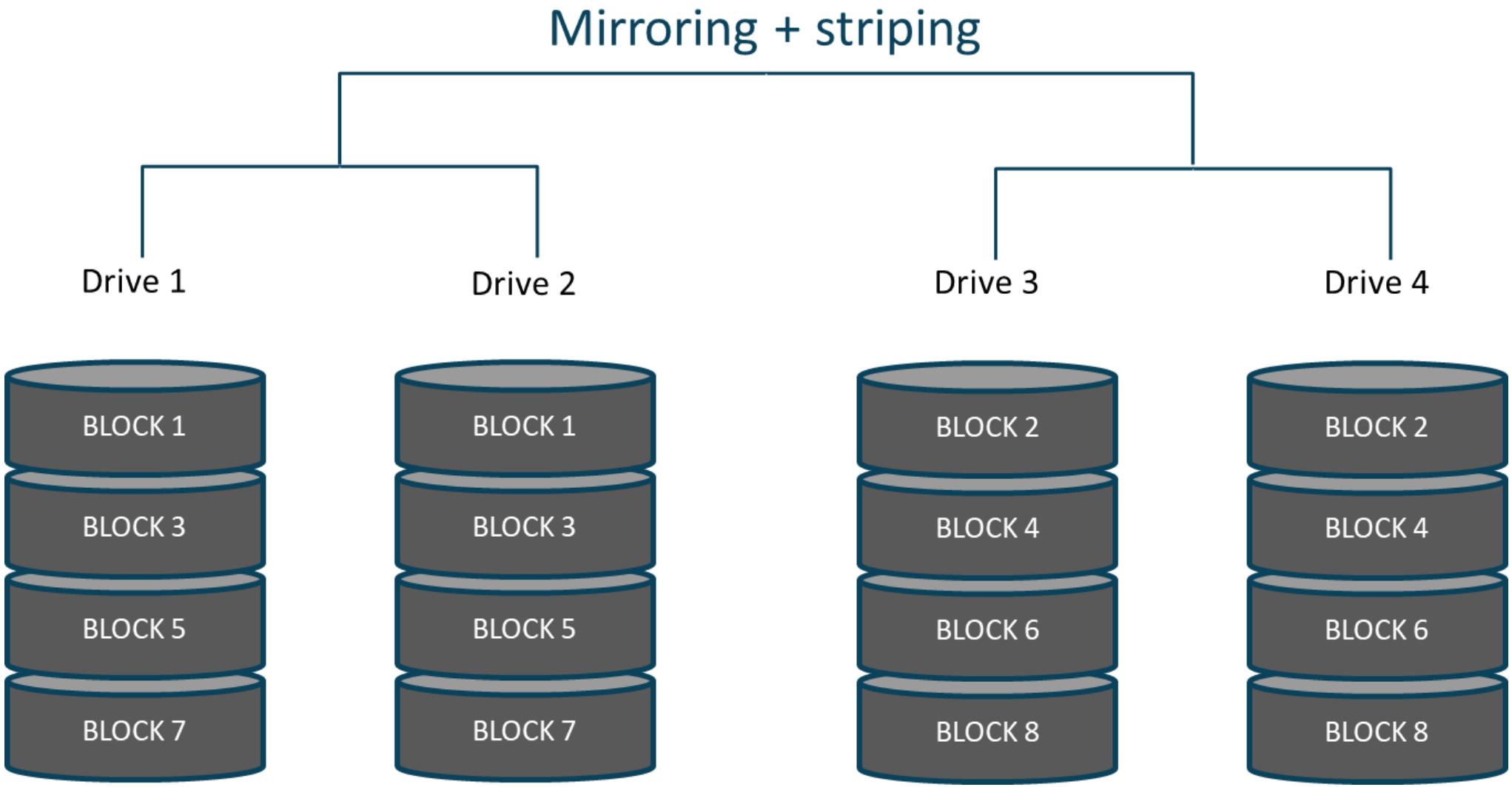


RAID Level 6

- RAID 6 is like RAID 5, but the parity data is written to two drives, so it requires at least four drives
- This solution can survive two drives failing simultaneously
- Read speeds are as fast as RAID 5, but the write speeds are slower than RAID 5 due to the additional parity data that must be calculated



RAID Level 10

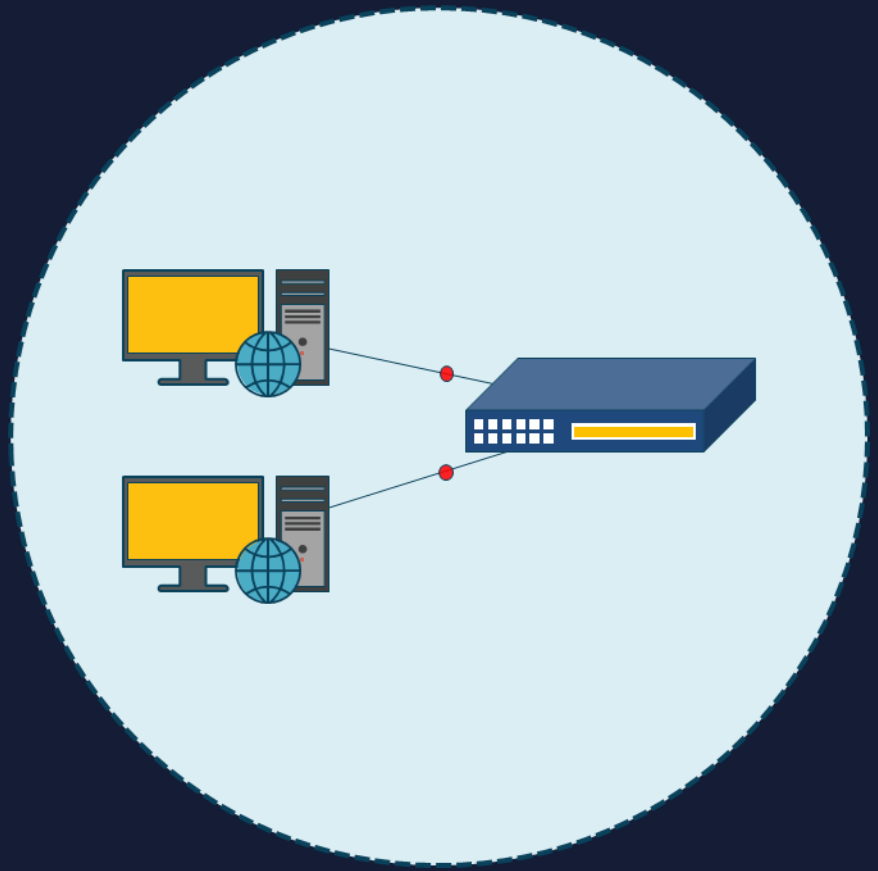


RAID Comparisons

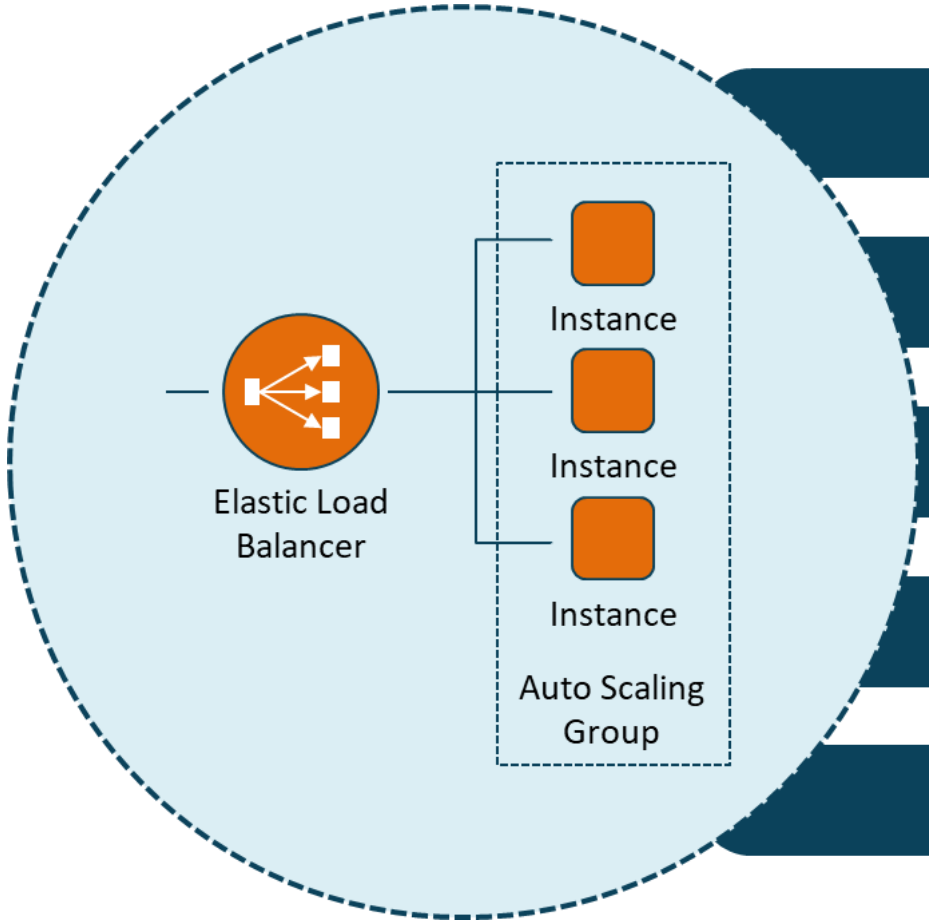
Features	RAID 0	RAID 1	RAID 5	RAID 6	RAID 10
Minimum number of drives	2	2	3	4	4
Fault tolerance	None	Single-drive failure	Single-drive failure	Two-drive failure	Up to one disk failure in each sub-array
Read performance	High	Medium	Low	Low	High
Write performance	High	Medium	Low	Low	Medium
Capacity Utilization	100%	50%	67% - 94%	50% - 88%	50%

Network Load Balancers

- Popular due to the usage of intensive applications and services
- Optimize application availability and performance (TCP, UDP, TLS)
- Distribute traffic across multiple servers in order to efficiently allocate resources and offer failover solutions



Load Balancing at Cloud Providers

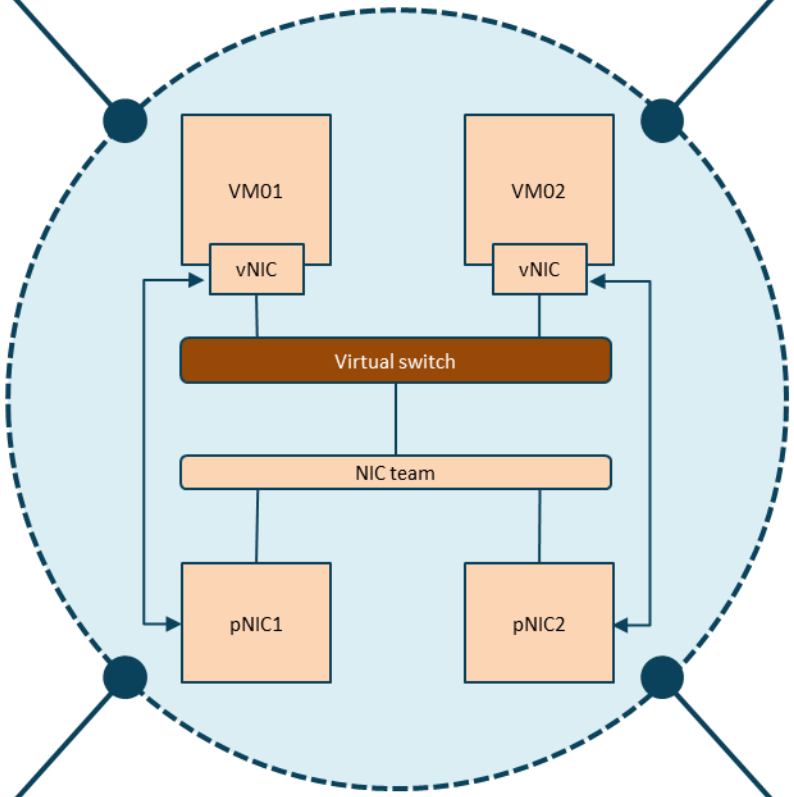


- Network or application load balancing (HTTP/HTTPS)
- Performs health checks on virtual instances
- Produces flow logs for visibility reports
- Runs the SSL/TLS listener
- Can have various firewalls applied

NIC Teaming

Group up NICs

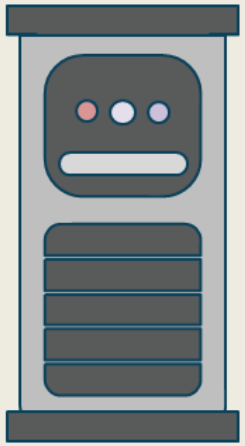
Physical and/or virtual



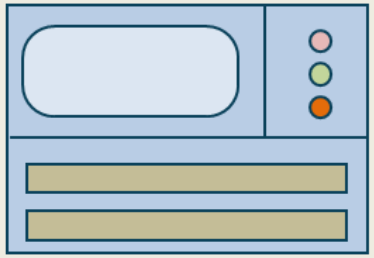
Fault tolerance

From 1 to 32 adapters

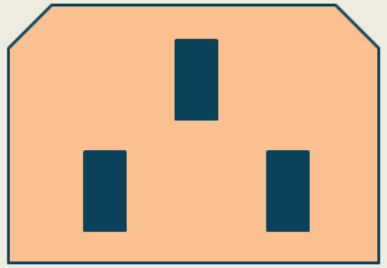
Redundant Power



Uninterruptible power supplies (UPS)

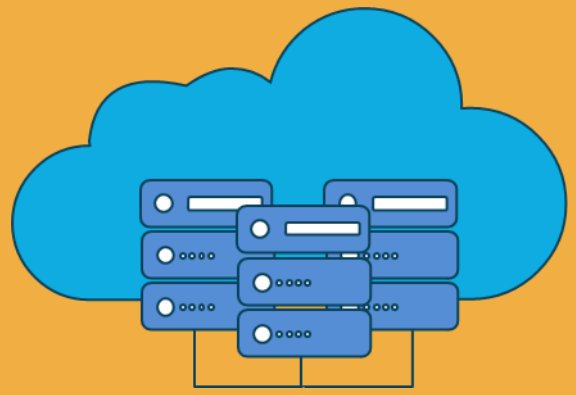


Generators



Managed power distribution units (PDUs)

Replication with SAN

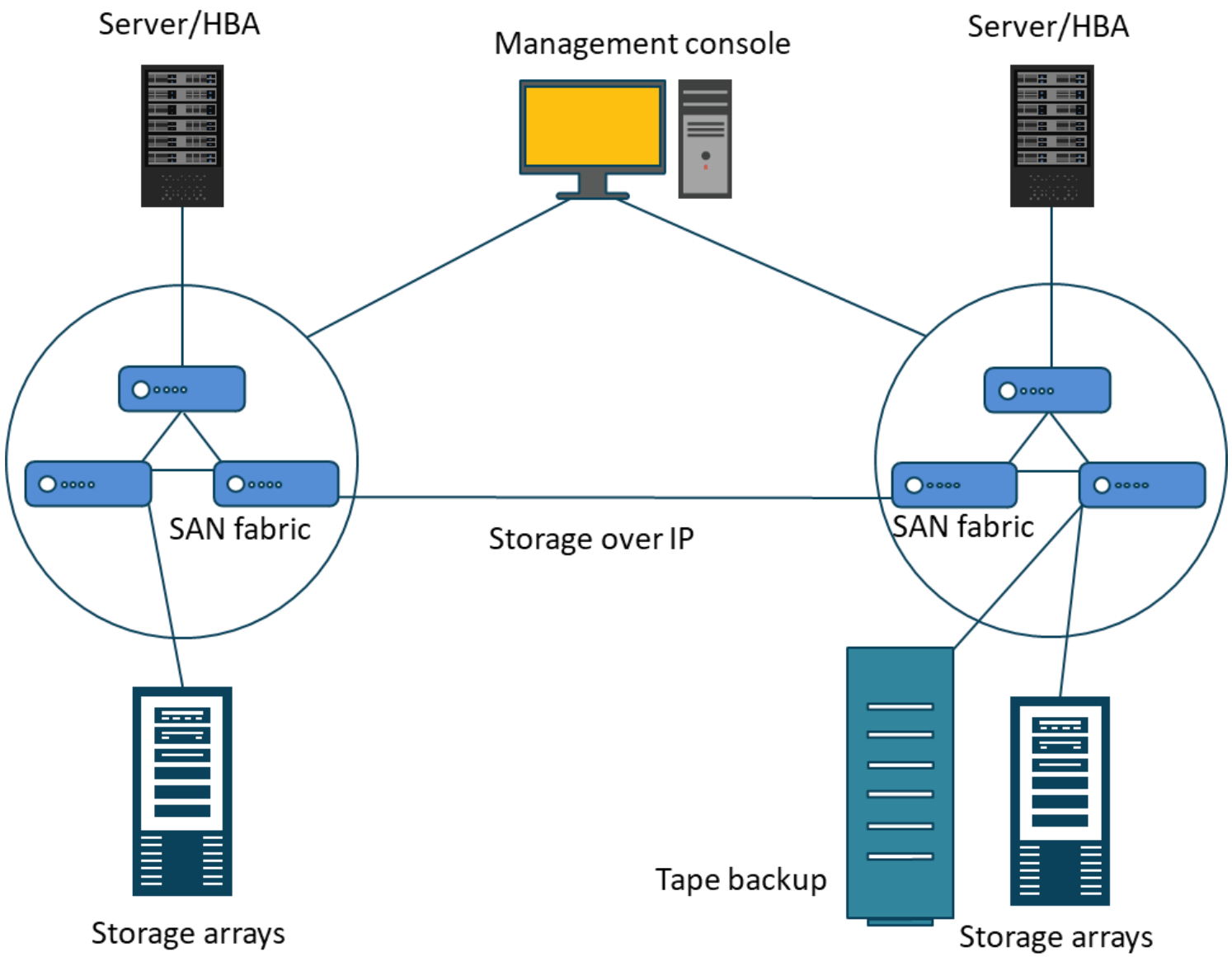


Storage Area Networking

- A storage area network (SAN) is a dedicated, independent, high-performance 10/100 GB network that interconnects shared fabrics of storage devices to multiple servers
- SAN moves storage resources off the main user LAN so that each server can access shared storage as if it is a directly attached drive (usually SSD)
- A host will send out a block-based access request for the storage device
- Uses Ethernet or fiber cabling, host bus adapters, SAN switches, storage arrays

Securing the SAN

- For securing data in transit, consider IPsec AH for integrity and origin authentication
- 802.1AE (MACsec) can provide encryption and more on the SAN frames
- Use secure management protocols on console
- Harden all switches and servers
- Encrypt data at rest with AES-256-GCM

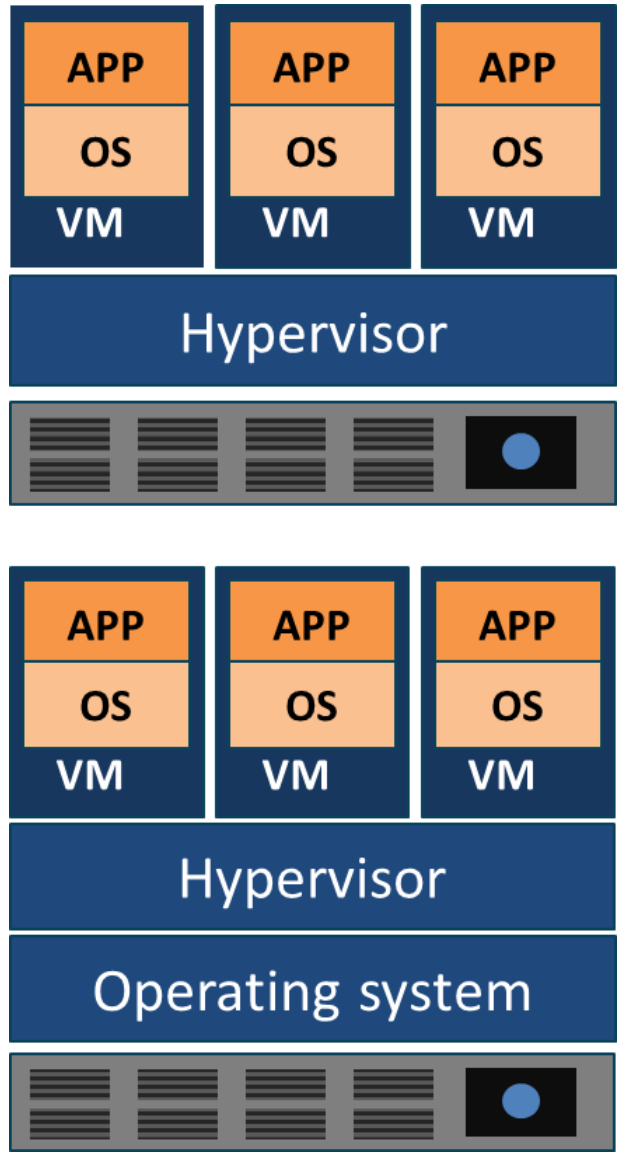


Virtualization (VMs)

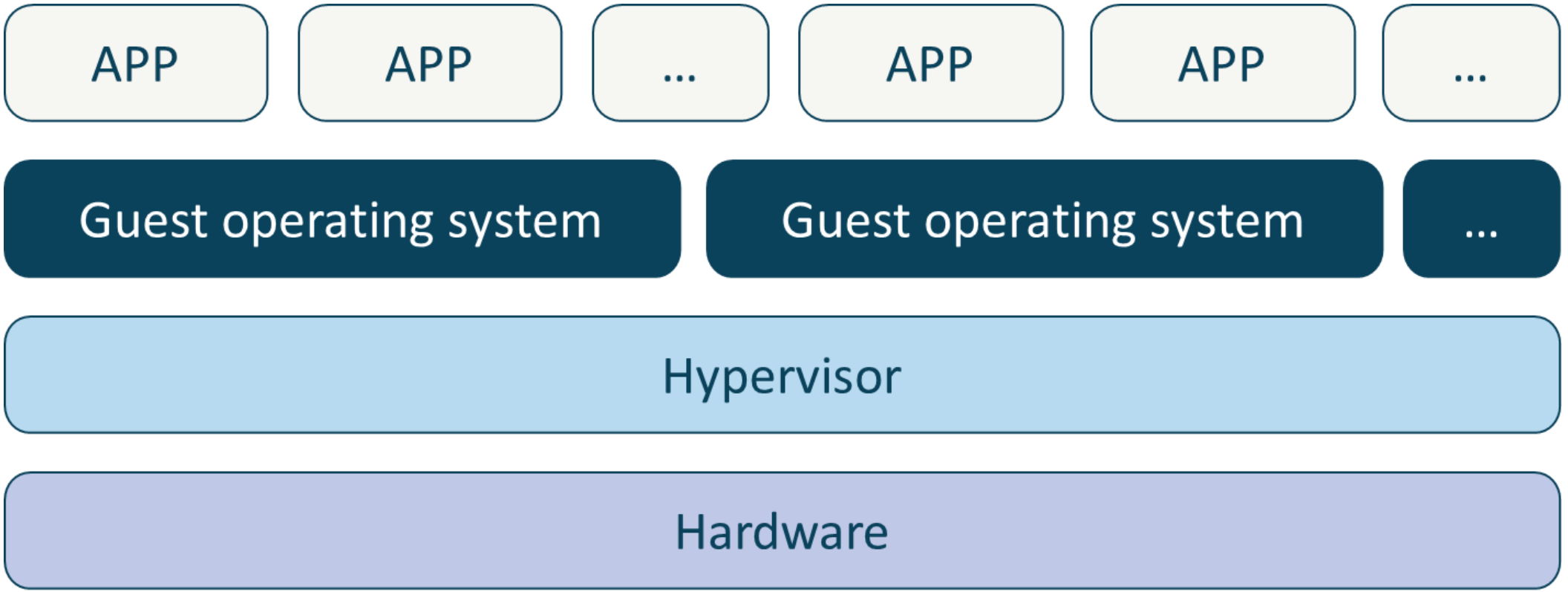
- Virtualization is the process of running a virtual instance of a computer system in a layer abstracted from the underlying hardware server
- It most often refers to running multiple operating systems on a computer system simultaneously
- To the applications running on top of the virtualized machine, it can seem as if they are on their own dedicated operating system with libraries, DLLs, and associated programs

Hypervisors

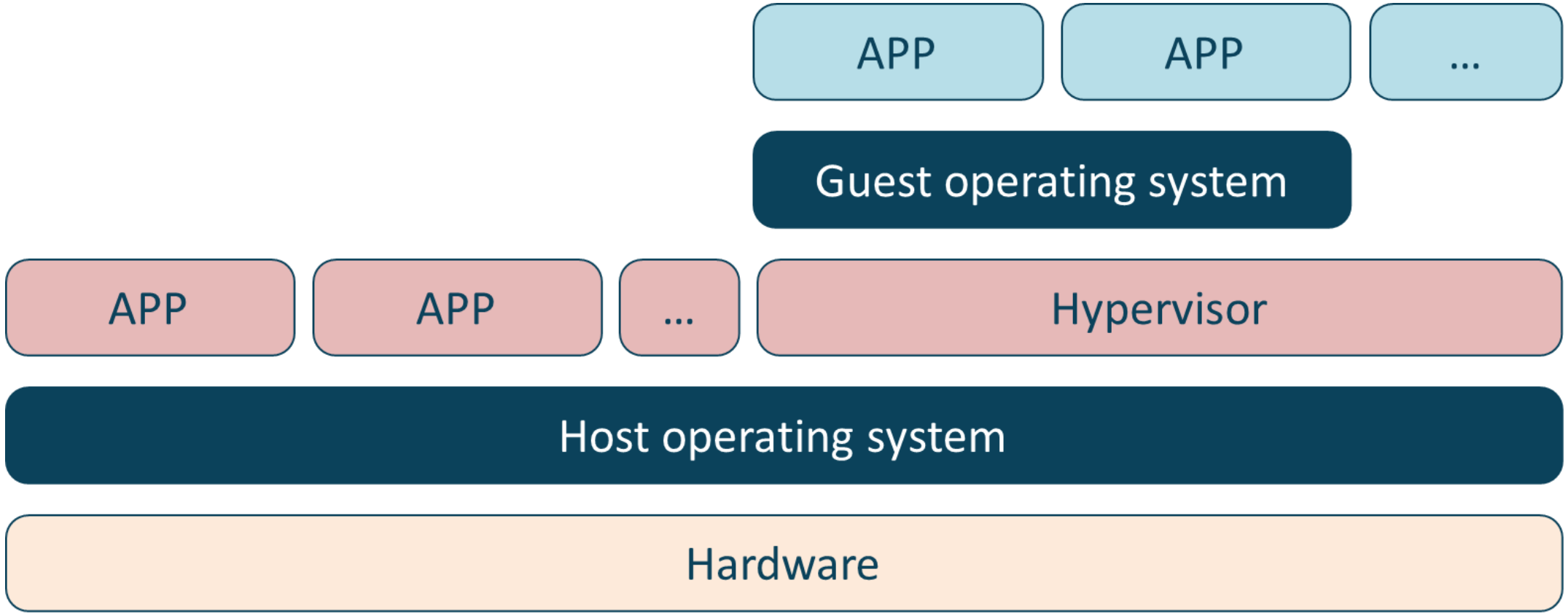
- Software that runs virtual machines
- Controls interaction between the VMs and the hardware
- Type I - bare metal or native
  - Runs directly on the underlying hardware
  - XenServer, KVM, Hyper-V, ESXi
- Type II - hosted
  - Runs on the OS installed on the hardware
  - Oracle VirtualBox 6, VMWare Player/Workstation



Type 1 Hypervisors



Type 2 Hypervisors



Virtualization Vulnerabilities

- **VM sprawl**
  - When the number of VMs overtakes the administrator's ability to manage them and the available resources
- VM sprawl avoidance
  - Enforce a strict process for deploying VMs
  - Have a library of standard VM images
  - Archive or recycle under-utilized VMs
  - Use a Virtual Machine lifecycle management tool or a cloud service provider-managed service
- **VM escape**
  - A serious threat where a process running in the guest VM interacts directly with the host OS
- VM escape protection
  - Patch VMs and VM software regularly
  - Only install what you need on the host and the VMs
  - Install verified and trusted applications only
  - Strong access control policies and passwords

Snapshot Backups

- Easier and faster backups and restores
- Immediate point-in-time virtual copy of source typically to on-premise or cloud object storage
- Should be replicated to another media to be considered a backup
- Time to back up does not increase with amount of data
- Improved RTO and RPO
- Restores are faster and less data is lost with an outage

Non-persistence Concepts

Many administrators need to roll a system back to a prior state of existence

Revert to Known State

Last Known Good Configuration

Live Boot Media

Non-Persistence VDIs

- Persistent VDI desktops are a type of desktop virtualization where users can preserve their personalized configurations, personal data, and instance settings so that their desktop is retrievable at log in
- Non-persistent desktops are thin, stateless systems where the user cannot retain data or configure a desktop instance as it is deleted at the end of the session
- CSPs are commonly making these services available as bastion servers or jump hosts for management

Availability vs. Durability

Availability

- Availability refers to system uptime
- Specifically, the client's ability to access the service
- The storage system is operational and can deliver data upon request
- Usually measured as 99.0 to 99.999 per year of uptime

Durability

- Durability is related to long-term data protection
- The data-at-rest does not suffer from bit rot, degradation, or other corruption
- CSPs offer from 11 to 16 "9s" of durability

Scalability vs. Elasticity

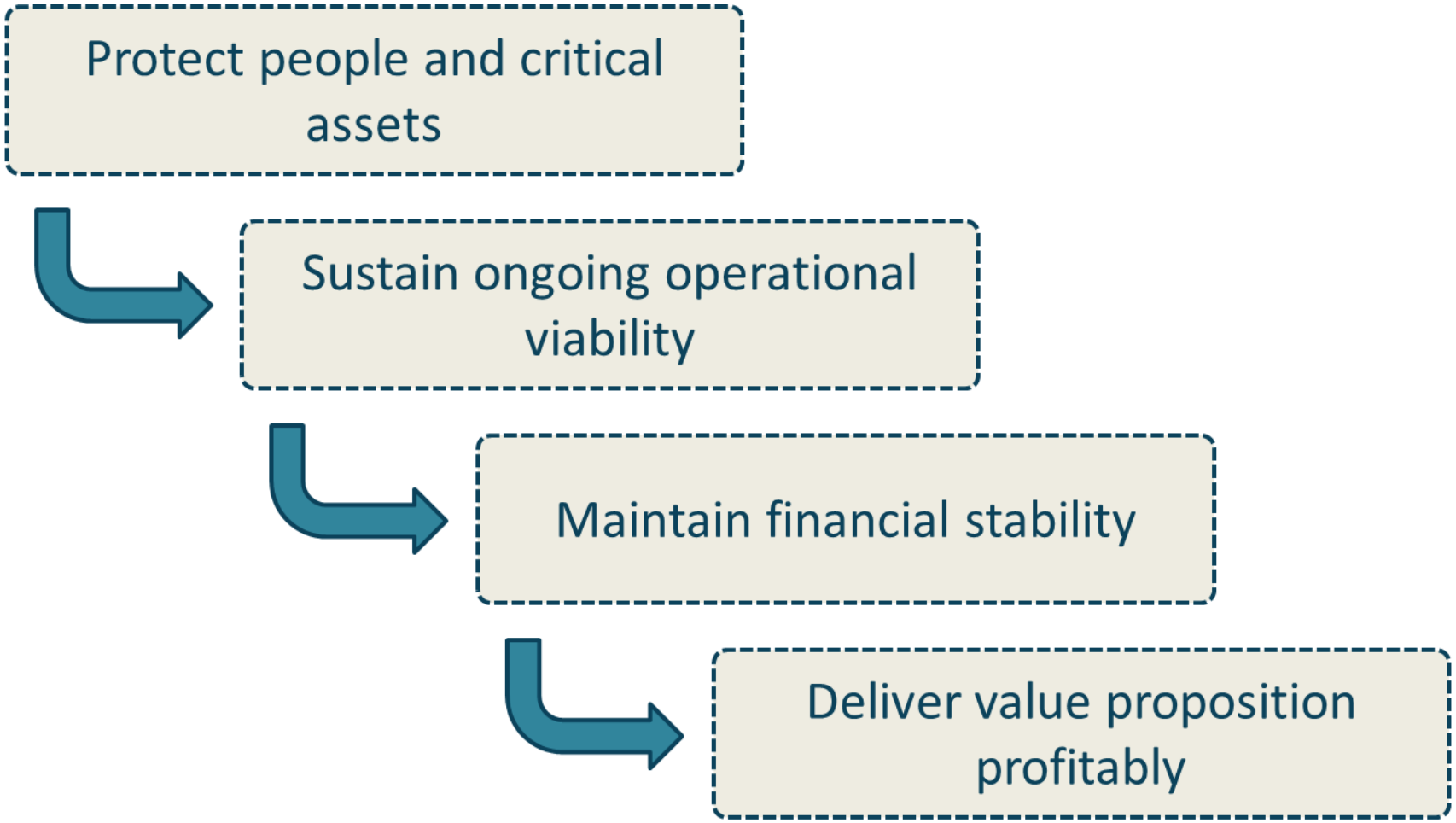
The ability of a system to increase the workload on its current hardware resources (scale up)

The ability of a system to increase the workload on its current and additional dynamically added, on demand hardware resources (scale out)

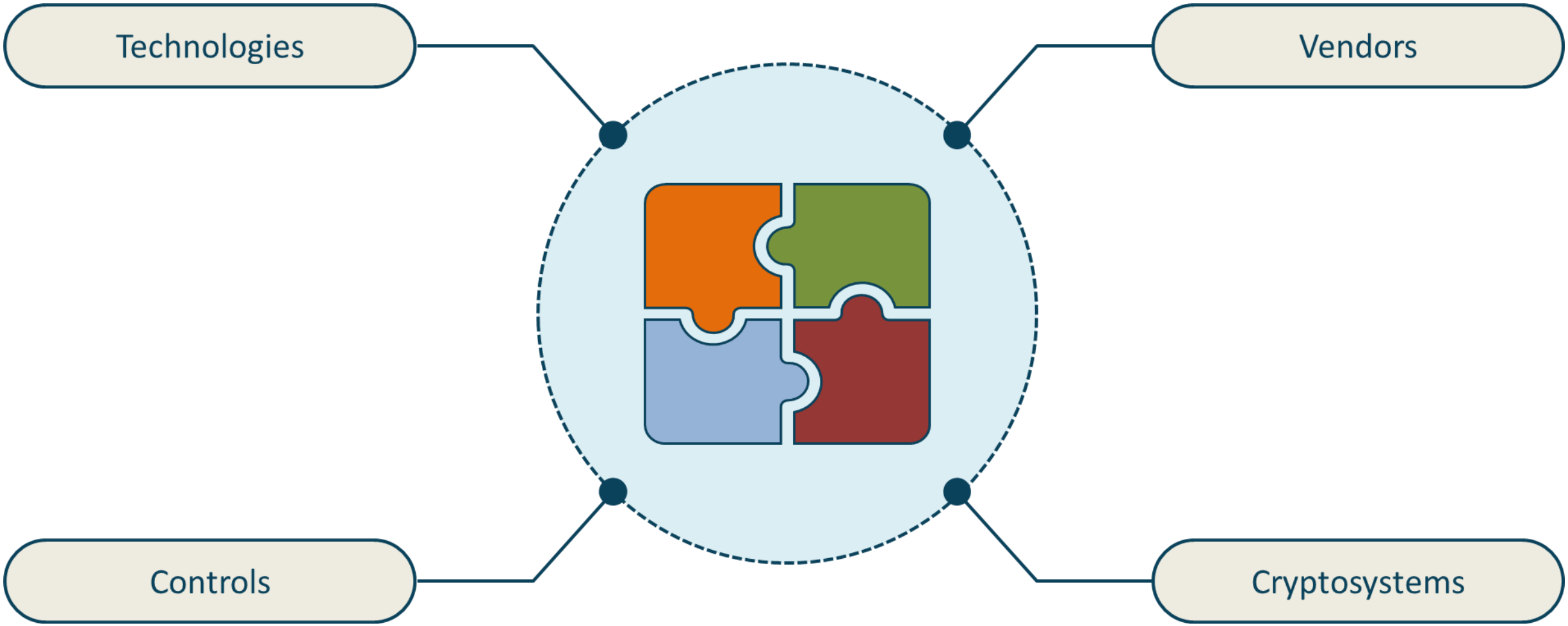
Data Recovery and Restoration

1. Repair the hard disk drive
2. Image the drive to new drive or disk image file
3. Logical recovery of files, partition, MBR, and file system
4. Repair damaged files that were restored

DRP Order of Restoration



Diversity Concepts



NIST SP 800-53 Controls

- Managerial
- Operational
- Technical

Managerial Controls

- Also referred to as "administrative controls"
- Should be published or printed definition of policies
  - Risk assessment and management
  - Best practices and guidelines
  - Password policies
  - Screening, hiring, and termination procedures
  - Mandatory vacations
  - Training and awareness

Operational Controls

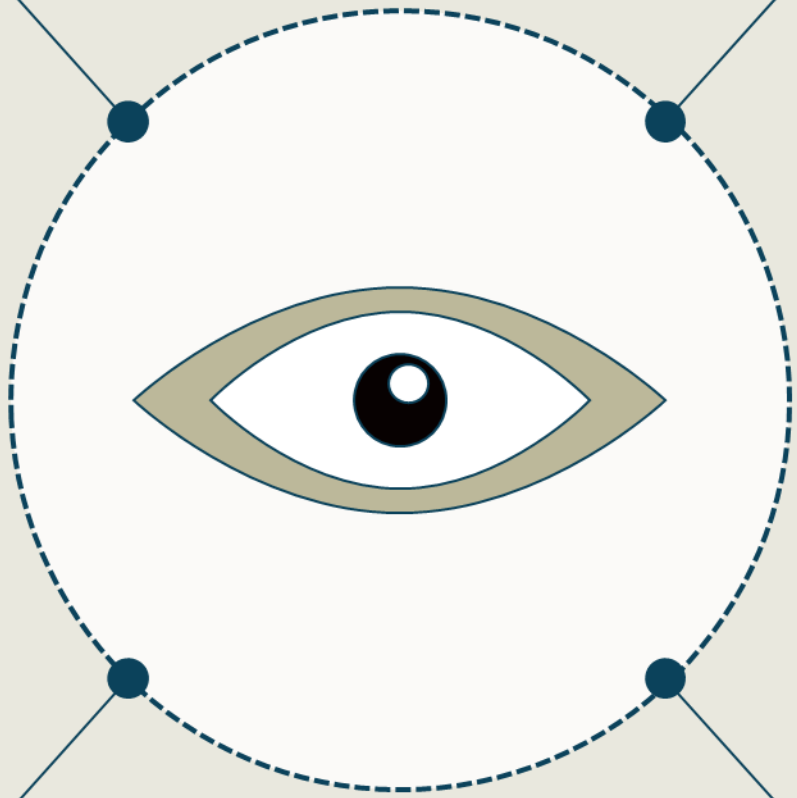
- Change and configuration management database
- Conducting awareness and training
- Implementing physical and environmental controls
- Contingency planning
- Incident response testing and drills
- System and data integrity mechanisms
- Mobile device and application management
- Disaster recovery plan testing and drills

Technical Controls

- Technical controls are security mechanisms that the specific systems run - either manually or more often automated and orchestrated
- These controls deliver confidentiality, integrity, authenticity, and availability protections
- They defend against unauthorized access or misuse
- They also facilitate detection of security violations and support security requirements for applications and data

Other Vulnerability Intelligence Sources

- Automated Indicator Sharing (AIS)
- Structured Threat Information Exchange (STIX)



- Predictive analysis and threat maps
- Trusted Automated eXchange of Indicator Information (TAXII)

Technical Controls

Infrastructure security and device hardening

Identity and Access Management

Cryptographic key management and HSM

Web application firewalls and threat modeling tools

Next-generation endpoint detection and response

Classic Control Categories

Administrative	Technical	Physical
Effective hiring practices	Controlled user interfaces	Guards
Effective termination practices	Password, tokens, OTPs	Fences
Classification of data based on levels of sensitivity	Firewalls	Motion detectors
Supervision of employees	Routers that filter traffic	Locks
Tracking employee activity	Anti-virus software	Cable conduits
Separation of duties	Access control lists	Swipe cards
Rotation of duties	Intrusion detection/prevention systems	Badges
	Smart cards	Dogs
	Biometrics	Cameras
		Alarms

Types of Controls

- Preventative
- Detective
- Corrective
- Deterrent
- Compensating

Secure Application Development

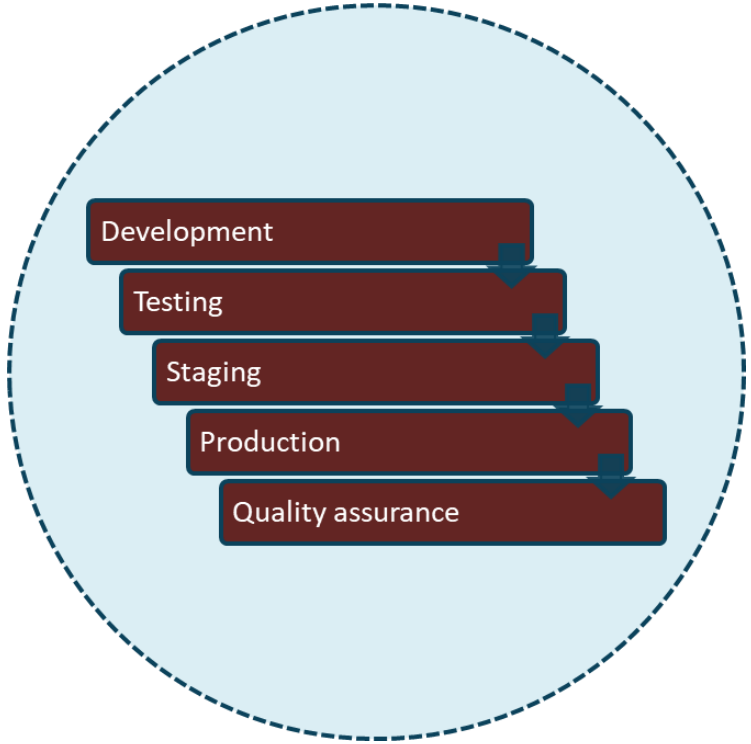
Secure by design

- The custom or outsourced application is developed with security integrated into the entire SDLC
- Attackers cannot simply overcome the security controls, even if they have white or gray box familiarity with the application design
- Example: using a virtual private cloud solution at AWS, GCP, or Azure

Secure Application Development

Secure by deployment

- The application was not developed with security integrated, but is deployed into an environment where security was considered in the network and system design
- Example: an application is deployed with air-gapped separation from any untrusted networks (private or on-premise cloud)

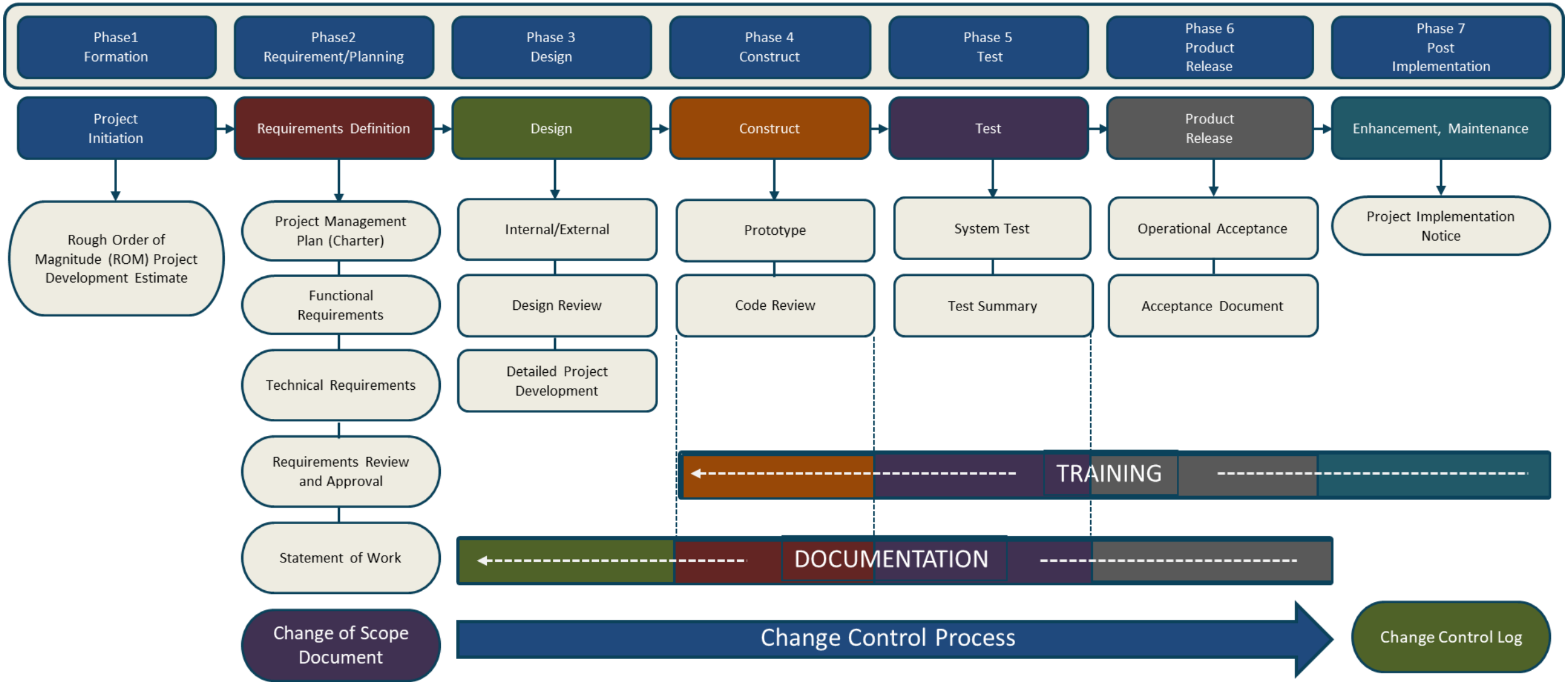


Secure Application Development

Secure by default

- This design consideration assumes that the application is natively secure without any modifications or additional controls
- Example: a server application has certain possible unsecure functions, but they are disabled by default at deployment based on Infrastructure as Code

Secure Application Environments



Provisioning and Deprovisioning

- Provisioning and deprovisioning can involve providing or removing software access to employees, customers, partners, and contractors on an as needed basis
- In modern environments it also involves using autoscaling services at cloud service providers to take advantage of cloud elasticity

Provisioning and Deprovisioning Enablers

Infrastructure as code and automation

Auto scaling technologies

Virtual machines and containers

Rapid deployment using Agile, Spiral, and CI/CD

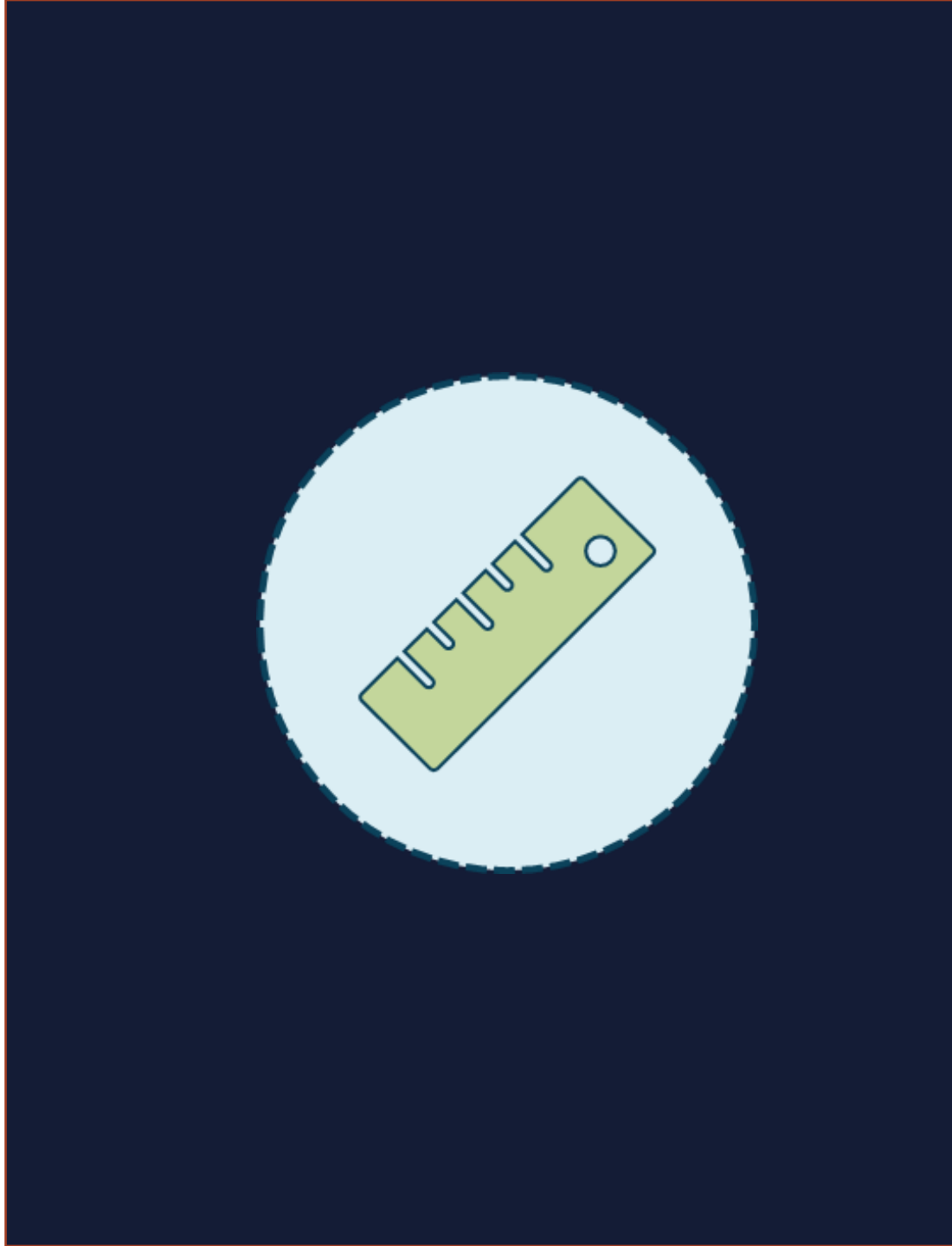
“Hybrid as a cloud” solutions

Integrity Measurement

- NIST SP 800-155 - BIOS Integrity Measurement Guidelines
- Checking for digitally signed code and programs
- Using Linux IMA subsystem
- Implementing Trusted Computing Base solutions (TPM)
- Server-side vs. client-side execution validation

Another Integrity Measurement Example

- WS-Security (WSS) is a SOAP extension used to enforce web confidentiality and integrity security
- It is a member of the Web service specifications and was published by OASIS
- The protocol specifies how integrity and confidentiality can be enforced on messages and allows the communication of various security token formats, such as SAML, Kerberos, and X.509



Secure Coding Techniques

- Normalization
  - Ensuring there is no redundancy in data and making sure that similar components are stored together
  - Also referred to a deduplication
- Using stored procedures
  - Subroutine available to applications that access a relational database management systems (RDBMS)
- Camouflage and obfuscation
- Removing dead code
- Employing memory management
- Control data exposure

API Considerations

Digitally sign all API calls

Do not embed any credentials in an API call

Only connect to trusted sources

Protect secret keys used for APIs

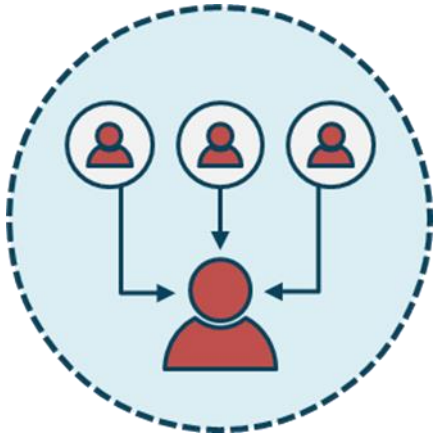
Deploy secure coding practices

Software Diversity

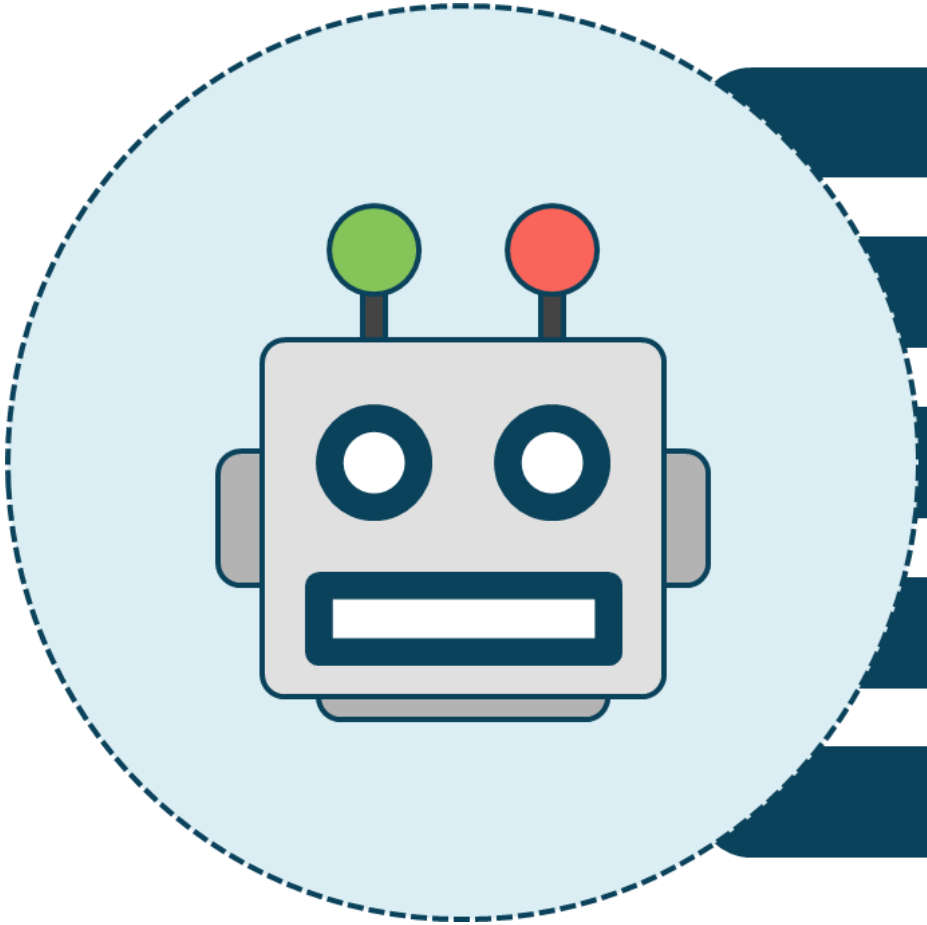
- An application development methodology where two or more functionally duplicate versions of the app are developed from the same specification
- Uses different developers or programming teams
- The goal is better error detection, improved consistency, and fewer programming errors
- End-user applications are often written in modern programming languages like Java and others
- The operating systems, firmware/middleware, support libraries, and virtual machines are still written in low-level languages that place flexibility and performance over security

Software Diversity

- Programming errors in low-level code are often exploitable and can sometimes give attackers unrestricted access to compromised host systems
- Automated software diversity techniques use randomization to significantly increase the difficulty of exploiting the huge amounts of low-level code in existence
- Diversity-based defenses are motivated by the assumption that a single attack will fail against multiple targets with unique attack surfaces



Automation and Scripting



- Continuous monitoring
- Continuous validation
- Continuous integration
- Continuous delivery
- Continuous deployment

SSL/TLS Inspection

- SSL/TLS inspection involves hardening all of your web services that are responding to HTTPS clients on the Internet and in private networks
- It also comprises the deployment of Web Application Firewalls (WAF) and deep packet inspection at site perimeters and on cloud computing components like elastic load balancers, CDN gateways, and API gateways to decrypt and inspect TLS traffic
- Managed Security Service Providers (MSSP) offer cloud-based inspection and analysis

TLS Best Practices

- Have up-to-date security software and settings
- Make sure browsers are updated
- Don't let vendor-installed code intercept traffic
- Ensure that client computers are malware-free
- Perform certificate revocation checks

TLS Best Practices

- Verify that encryption is being done
- Check certificate expiration dates
- Get TLS certificates from trusted authorities
- Employ pinning and OCSP stapling
- Deploy HSTS protocols