LOGGING, MONITORING, & INVESTIGATIONS

Objectives

- Explore log management, IDS, and IPS
- Examine SIEM and SOAR systems
- Learn about continuous monitoring and tuning
- Review threat intelligence and user and entity behavior analytics
- Explore e-discovery and cyber forensics

LOG MANAGEMENT

- Log management is an IT initiative that continuously collects, stores, processes, and analyzes data from various applications and services
- The goals are to optimize performance, identify logistical problems, manage resources, improve security, and meet compliance
- A log management system (LMS) is a solution that collects, sorts, and stores log data and event logs from a variety of sources in one centralized location
- These systems allow professionals to define a single point from which to access all pertinent data
- Usually, the files are stored in an indexed and searchable format so that the data can be quickly accessed and analyzed

LOG MANAGEMENT GOALS

LOG MANAGEMENT

- Log management systems and tools are used to assist professionals with managing the increasingly high amount of log data generated throughout the enterprise by a myriad of devices, applications, and services to determine:
  - The event, information, and incident data that must be logged
  - The format in which it should be retained
  - Any additional transformation or processing of the data before being sent to other systems or services
  - The time period for which the data should be stored and then archived
  - How the log data should be destroyed

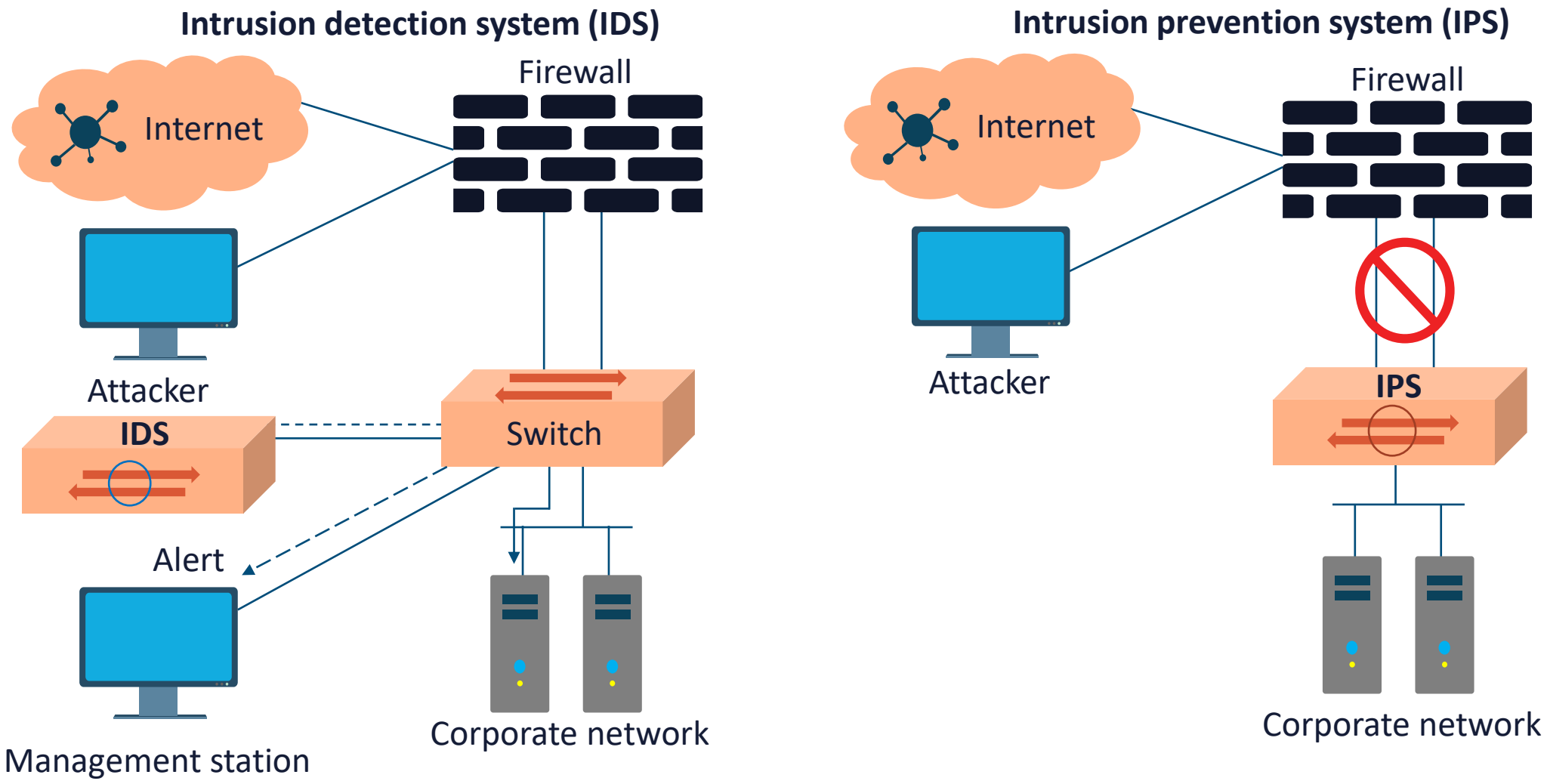
Intrusion Prevention System (IPS)

- An IPS observes network traffic for possible indicators of compromise (IOCs) and threats
- An inline IDS can dynamically stop attacks and send alerts to security operation centers/stations
- A next-generation IPS can even remove malicious content or trigger other security services (for example, machine learning (ML)/artificial intelligence (AI)
  - Although IPS solutions evolved from intrusion detection, they are typically deployed initially in a detection or passive mode for tuning
- An IPS does the same detection and reporting as an IDS, so they are often called **intrusion detection and prevention systems (IDPS)**

IPS/IDPS

- When an IPS directly thwarts malicious traffic, it can reduce the overhead for security teams and security operations centers (SOCs)
- This empowers them to focus on more complex threats, incident handling, and manual SOAR runbooks
- An IPS enhances security policies by blocking unauthorized actions of legitimate users
- They also help support compliance efforts like the PCI-DSS and GDPR

IDS VS. IPS SENSORS



IPS CHARACTERISTICS

Network or host-based

Cloud-based

ML or AI-driven

Signature and anomaly-based

In or out of band

Monitor or passive mode

IPS ACTIONS

- Alerts (logs)
- Alarms
- Verbose dumps
- TCP resets
- Drop packets or addresses inline
- Blocking (shun) on upstream or downstream routers and/or firewalls
- Simple Network Management Protocol (SNMP) traps to managers
- Output to SIEM systems
- Flows to NetFlow collectors
- Data sent to hybrid cloud services

TUNING IPS SENSORS

- **True positive =** true (accurate) + positive (action taken)
- **True negative =** true (accurate) + negative (action not taken)
- **False positive =** false (error) + positive (action taken)
- **False negative =** false (error) + negative (action not taken)

SYSLOG: THE PREDECESSOR TO SIEM

- 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 cluster or a modern 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

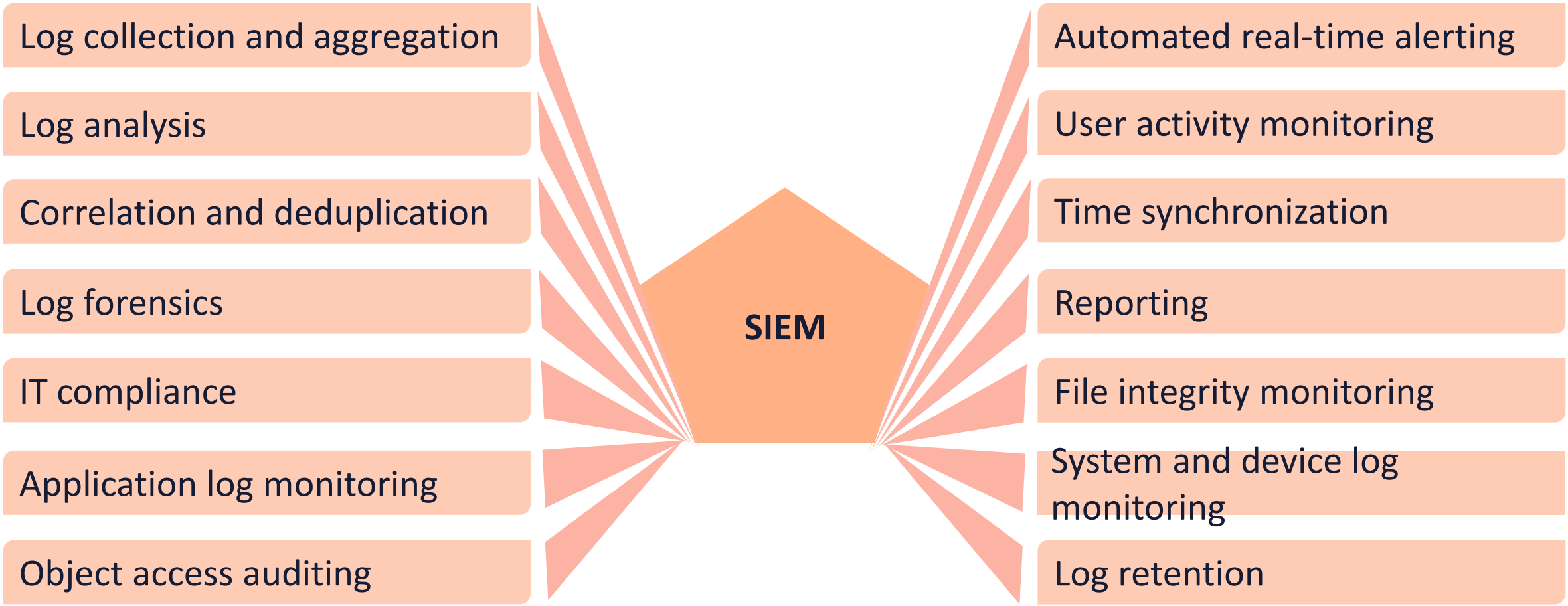
SYSLOG LEVELS

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

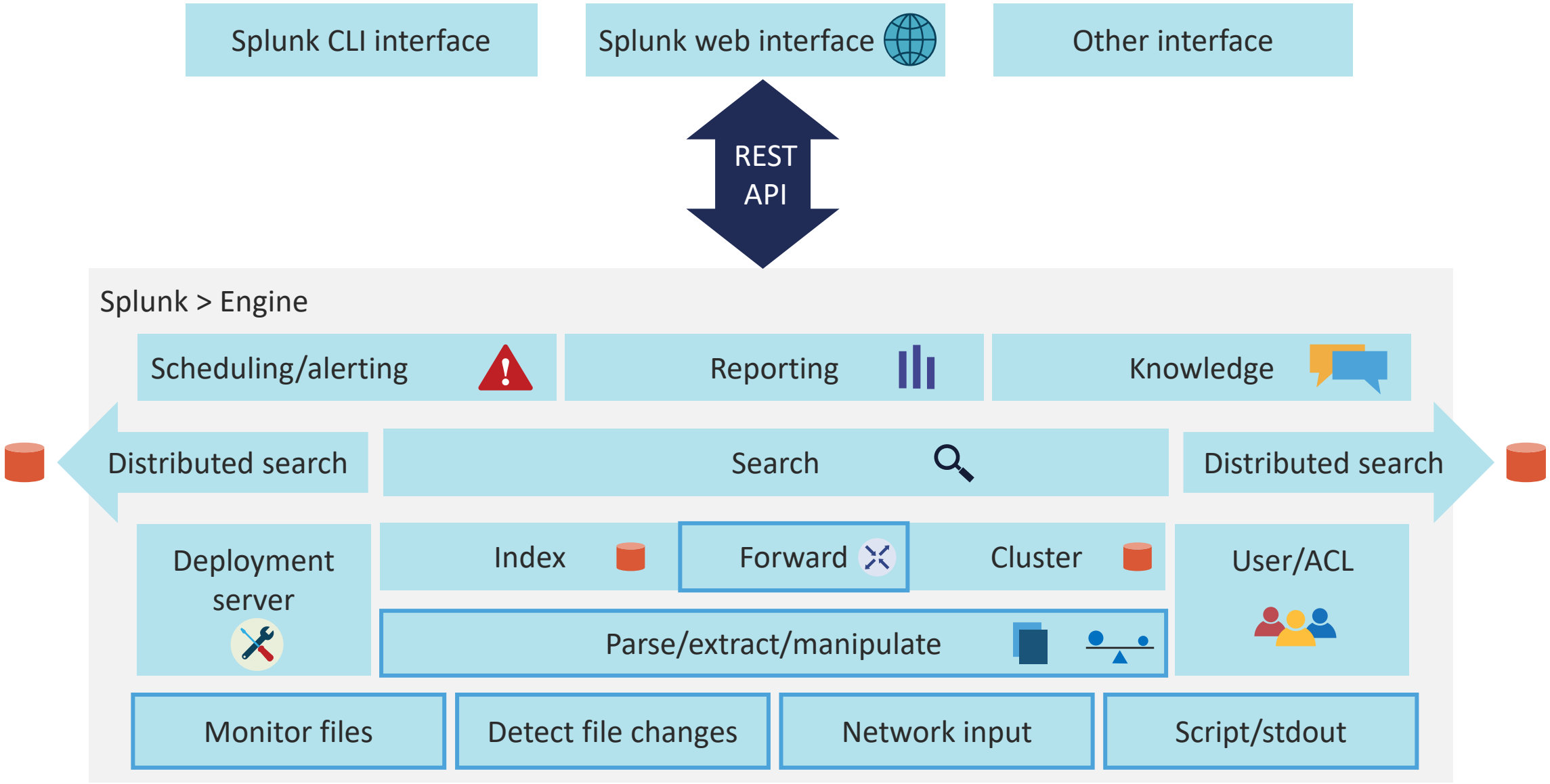
SIEM

- The term SIEM is a combination of security information management (SIM) and security event management (SEM)
- SIEM centralizes the collection, storage, and analysis of logs and other security-related data to perform near-real-time analysis
- It often sends filtered and "massaged" data to mining, big query, and data warehousing servers in a data center or at a cloud service provider
- This critical combination of software enables network and security teams to take better 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 and device log monitoring
Log retention

CISCO SPLUNK SIEM ARCHITECTURE EXAMPLE



SOAR

- SOAR is a mixture of software services and tools that enable organizations to simplify, automate, aggregate, and organize security operations in three core areas:
  - Threat and vulnerability management
  - Incident response
  - Security operations automation

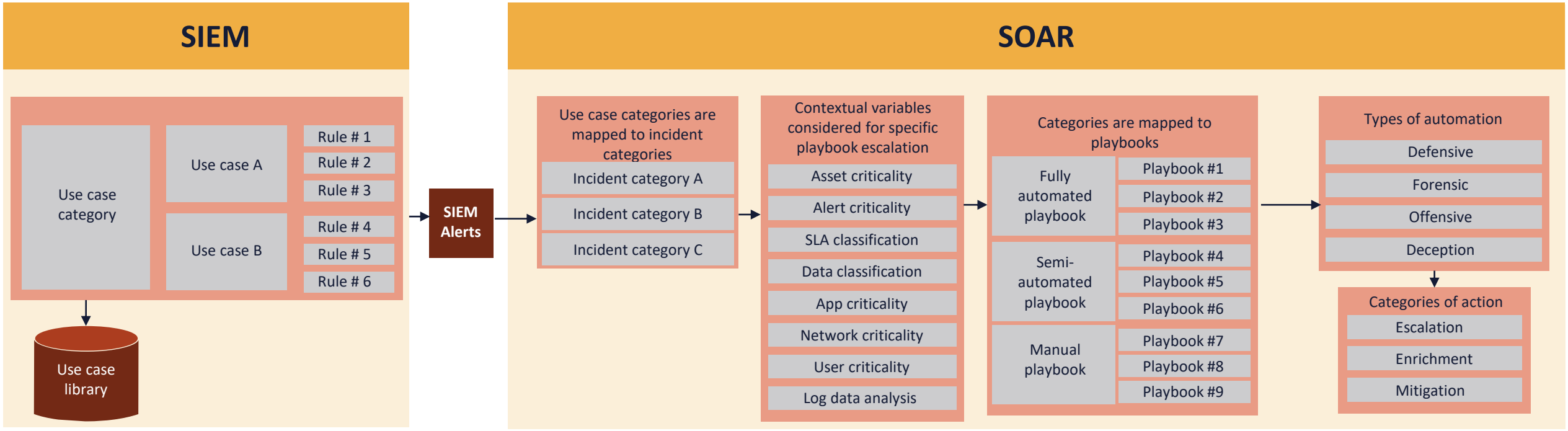
SOAR ELEMENTS

- Commonly, SIEM use cases, categories, and rules are mapped to incident categories, and these categories are then mapped to SOAR playbooks
- SOAR typically supports three types of playbooks:
  - Manual (a series of manual tasks)
  - Semi-automated (a hybrid of automated and manual subtasks)
  - Fully-automated (completely automated)

SOAR ELEMENTS

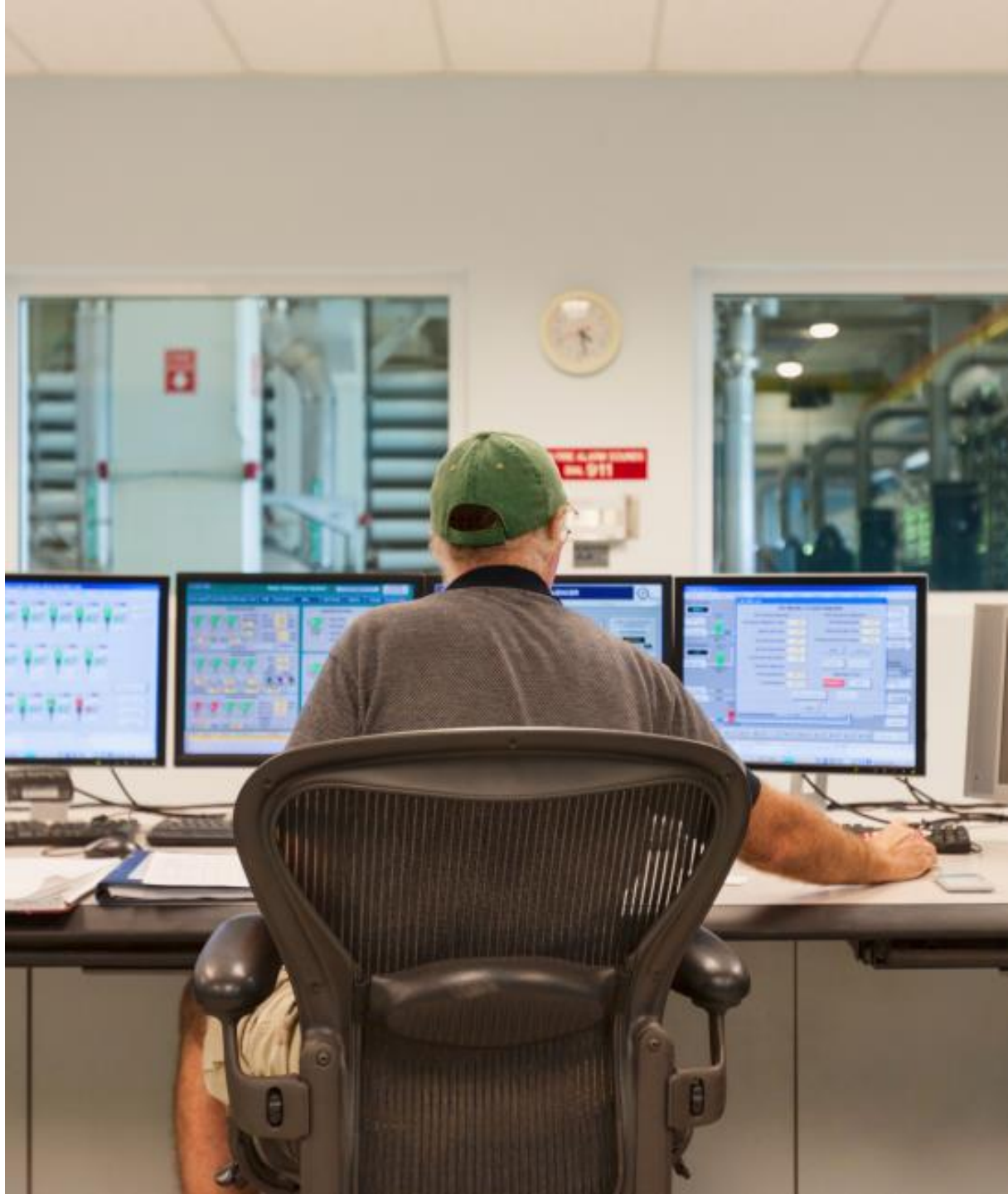
- SOAR supports four types of automation:
  - Defensive – anything that tries to prevent the threat or risk
  - Forensic – anything that tries to retrieve additional evidence
  - Offensive – anything proactive that tries to investigate an asset
  - Deception – anything that retrieves or adjusts honeynets
- SOAR delivers three action categories:
  - Enrichment – adding additional configuration management database (CMDB) or environment data
  - Escalation – email, ticket escalation, Simple Notification Service (SNS), chat/messaging communication
  - Mitigation – the modification of device configuration

SIEM AND SOAR WORKING TOGETHER



CONTINUOUS MONITORING & TUNING

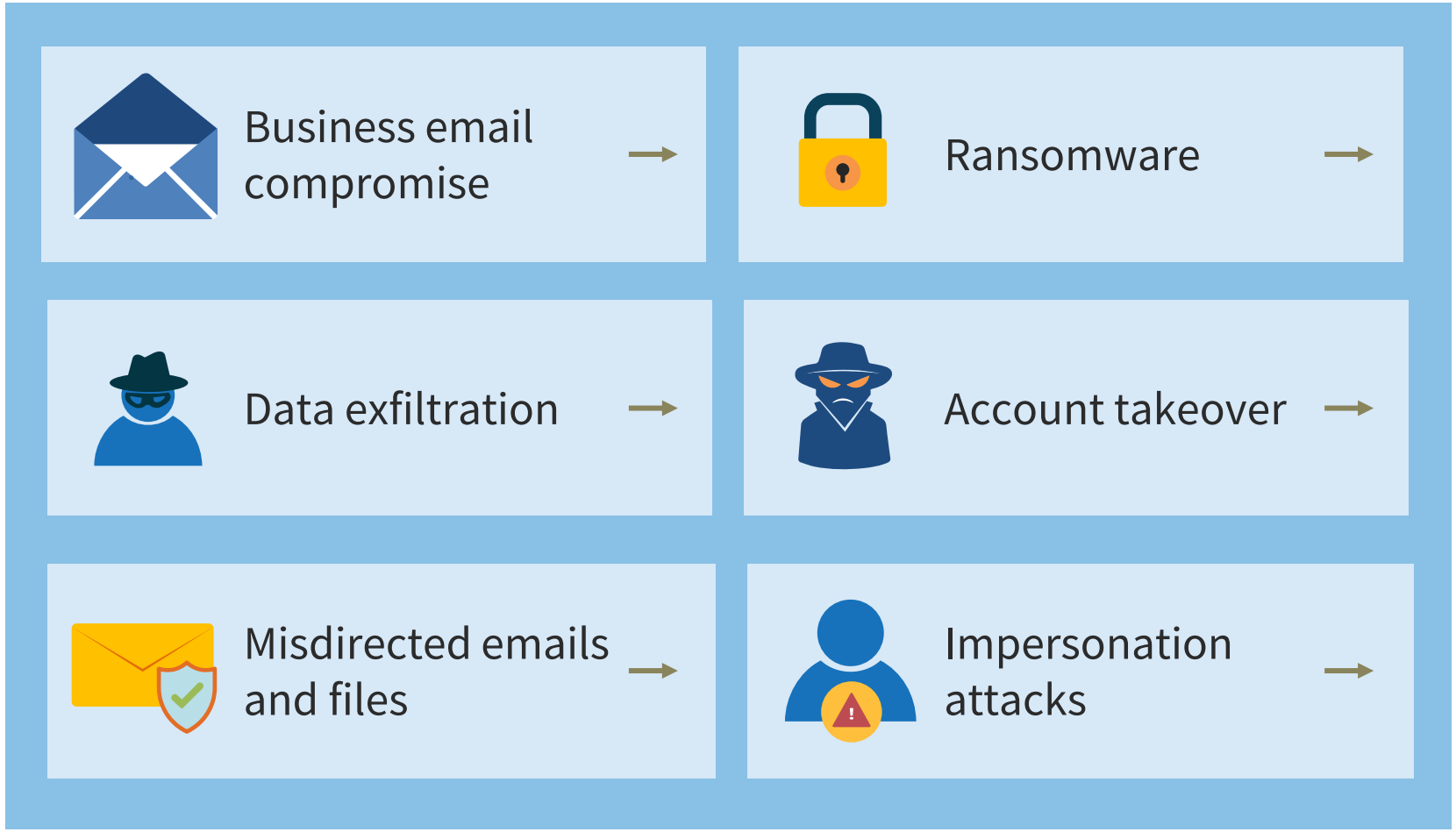
- Continuous security monitoring (CSM) is an official initiative for threat intelligence that automates the monitoring of security controls, gaps/weaknesses, and other cyber threats
- It is a modern centralized SOC solution that offers real-time visibility into the organization's security maturity and posture
- It continually investigates cyber threats, security misconfigurations, or other vulnerabilities
- SIEM and SOAR are common real-world implementations



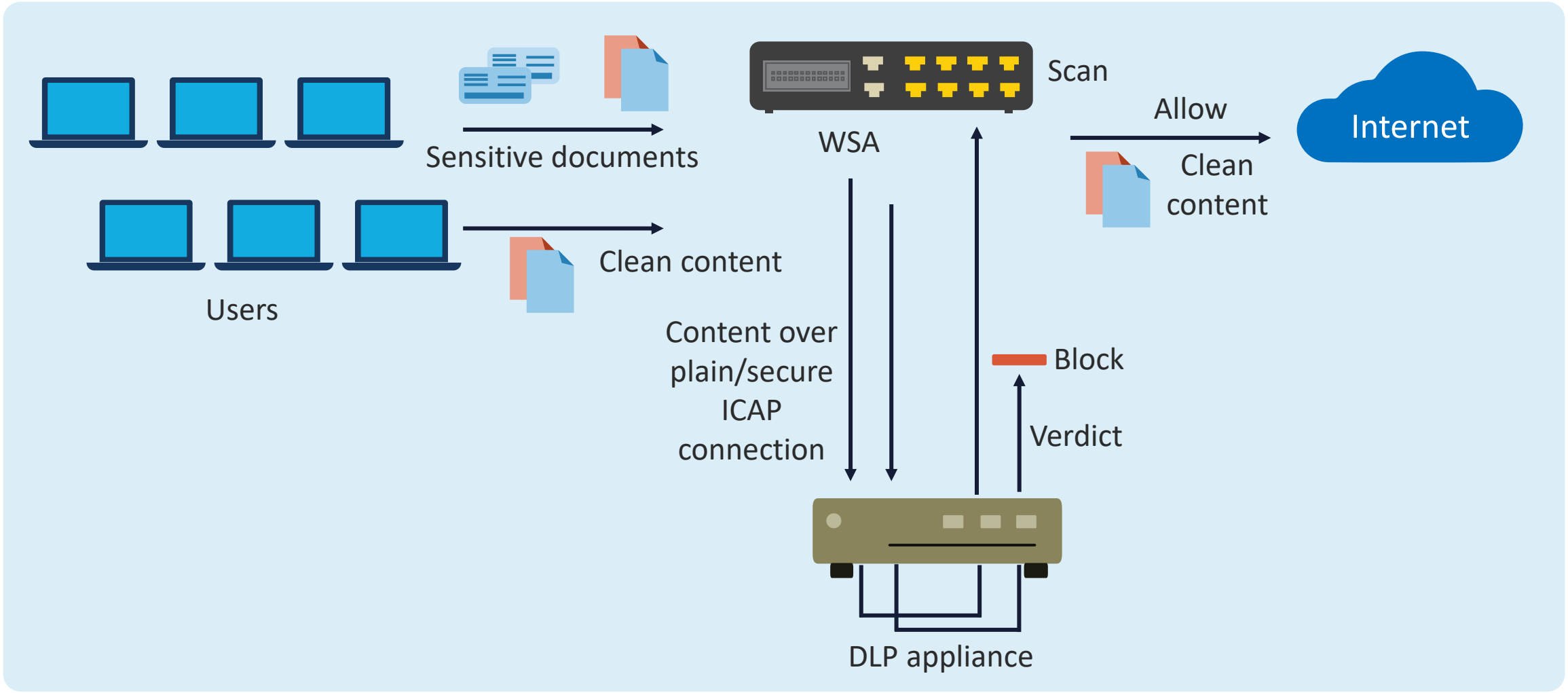
COMMON CONTINUOUS MONITORING & TUNING TARGETS

- Patch management
- Big data volumes
- Third-party library debugging
- Security misconfiguration remediation
- Overall website and web application security
- Real-time website spoofing protection
- Deploying Internet of Things (IoT) devices
- Industrial IoT (embedded) remote monitoring

EGRESS MONITORING SERVICES

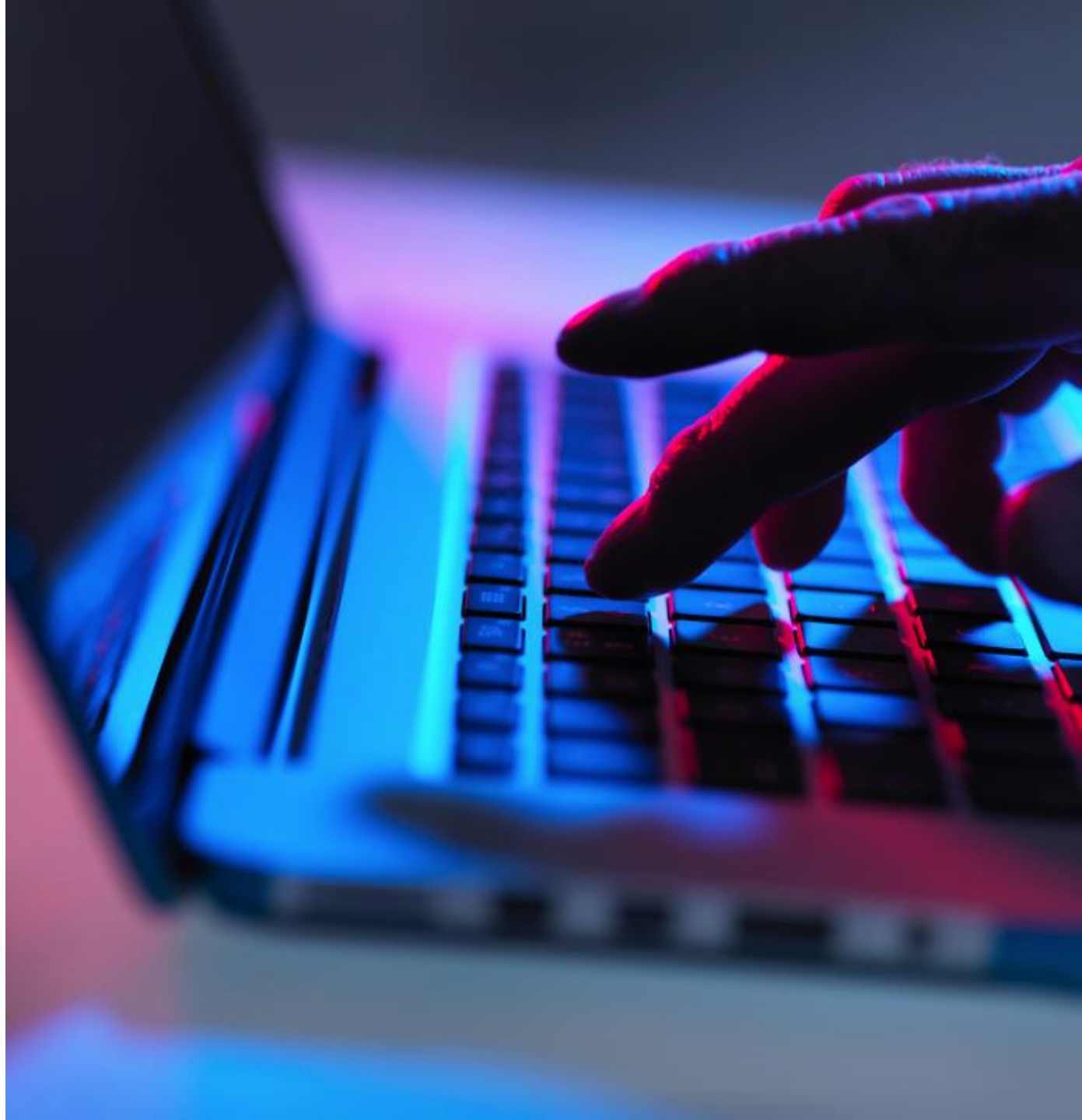


EGRESS MONITORING FOR DATA LOSS PREVENTION



THREAT INTELLIGENCE

- Threat intelligence is information and metrics that are received, processed, and analyzed to understand a threat actor’s motives, targets, and attack behaviors
- This initiative helps organizations to take proactive actions that can prevent, or at least mitigate cyber attacks
- Threat intelligence also provides contextual information about potential attackers, their intents, motivations, capabilities, and possible indicators of compromise (IOCs)
- Intelligence is often driven by real-time threat feeds delivered through various channels directly to dashboards



THREAT INTELLIGENCE

Strategic

Understanding the high-level motives and trends of attackers, then using the data to engage in due diligence of security and business decisions

Stakeholders:

- CISO
- CIO
- CTO
- Executive board
- Strategic intel

Operational

Knowing about the capabilities and threat vectors of adversaries, then leveraging the knowledge to perform more granular and directed cybersecurity

Stakeholders:

- Threat hunter
- SOC analyst
- Vulnerability mgmt.
- Incident response
- Insider threat

Tactical

Conducting malware analysis and enhancement, including getting atomic, stateless, and behavioral IOCs for active defense initiatives

Stakeholders:

- SOC analyst
- SIEM
- Firewall
- Endpoints
- IDS/IPS

EXAMPLE: AMAZON GUARDDUTY

- GuardDuty is a managed threat intelligence service that constantly monitors for malevolent and unauthorized behavior
- It looks out for unusual application programming interface (API) calls or potentially unauthorized deployments that indicate a possible account compromise (zero day)
- It detects potentially compromised instances or reconnaissance by advanced persistent threat actors
- It performs pre-crime AI activities on domains and IP
- It utilizes proprietary ML and AI along with strategic partners like CrowdStrike, Trend Micro, Trustwave, and Rapid7

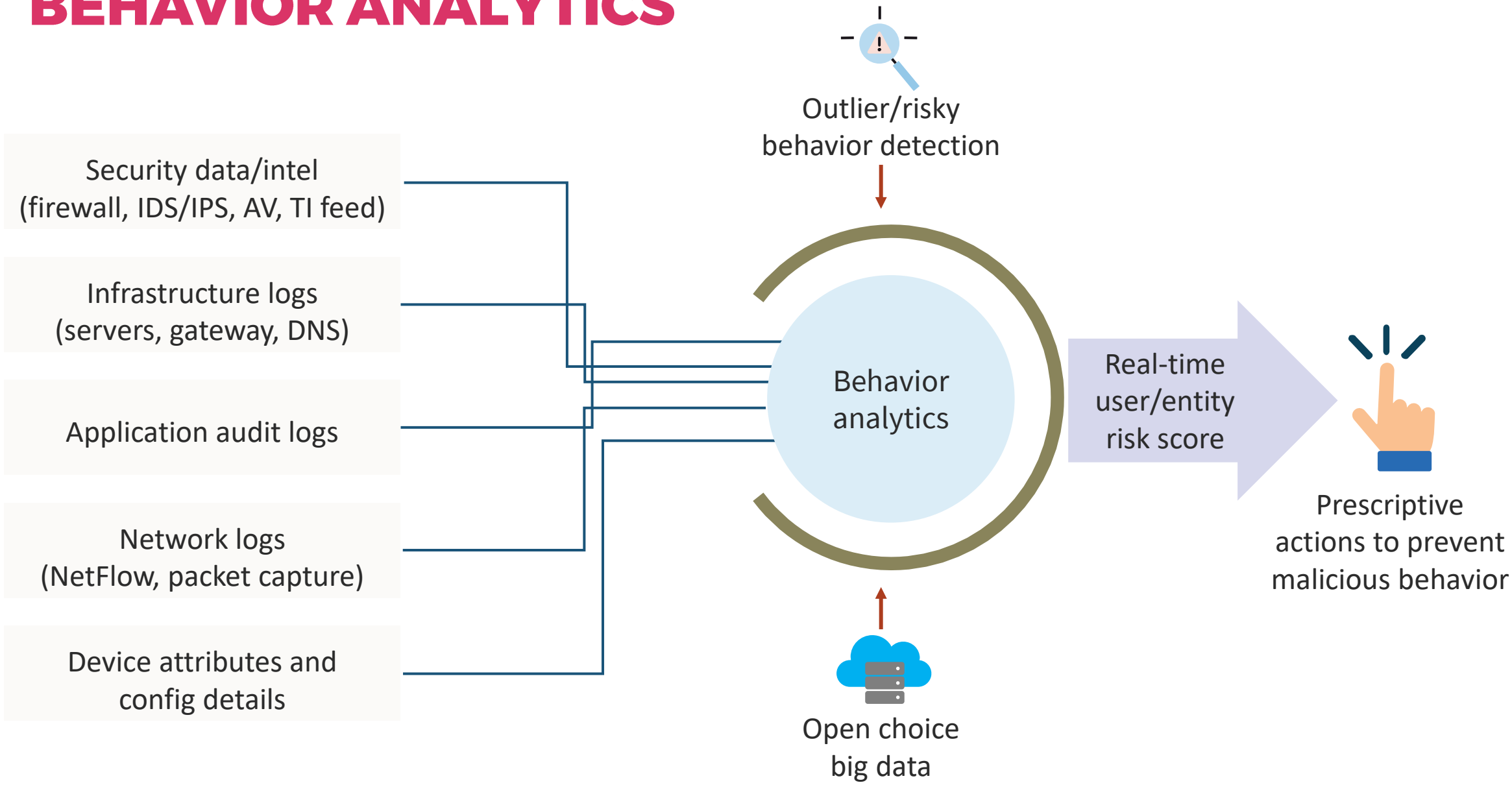
USER AND ENTITY BEHAVIOR ANALYTICS

- Behavior analytics (BA) collects and analyzes data from principal actions conducted on a digital product such as an app or a website
- Organizations can dynamically determine exactly how subjects interact with a digital experience
- Decisions can then be made for enhanced security and continual improvement
- Behavior analytics is a relatively new technique for analyzing quantitative and qualitative user and non-person entity (NPE) data to learn how subjects behave when using and interacting with devices, applications, and services
- Next-generation endpoint detection tools such as Palo Alto Cortex XDR leverage BA

BEHAVIORAL ANALYTICS

- Behavioral analytics often leverages machine (deep) learning engines and AI tools to answer questions such as:
  - What are subjects doing that may violate an acceptable use policy (AUP) or introduce risk?
  - What are subjects interested in and what are they completely ignoring?
  - Where on your corporate site or app do subjects get stuck and have issues?
  - What do users do right before they exit the Intranet site or corporate app?

BEHAVIOR ANALYTICS



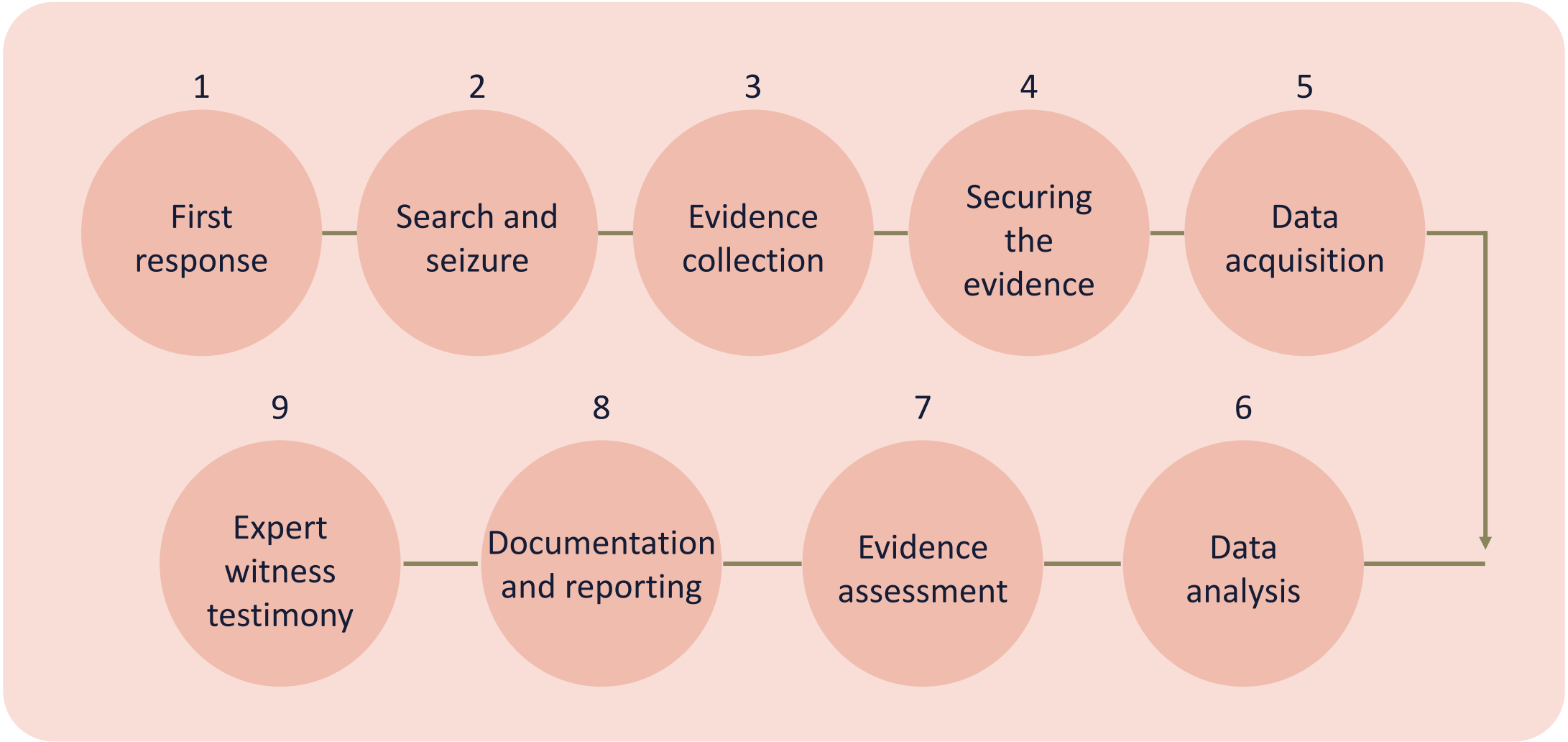
WHY PERFORM FORENSIC INVESTIGATION?

- Laws have been violated
- Organizational policies have been violated
- Systems have been attacked
- Data and identity have been breached
- Intellectual property has been exfiltrated
- Privileged insiders are suspected of crimes
- Next phase of incident response

FORENSIC E-DISCOVERY

- Cyber forensics is an aspect of e-discovery
- Innovative technologies have emerged to lower the risks and costs associated with big data, especially in litigation and internal corporate/government investigations
- The e-discovery process includes four phases:
  - Identifying and collecting documents
  - Sorting through data by relevance
  - Creating production sets
  - Data management

THE NINE-PHASE CYBER FORENSIC LIFECYCLE



INVESTIGATIVE TECHNIQUES

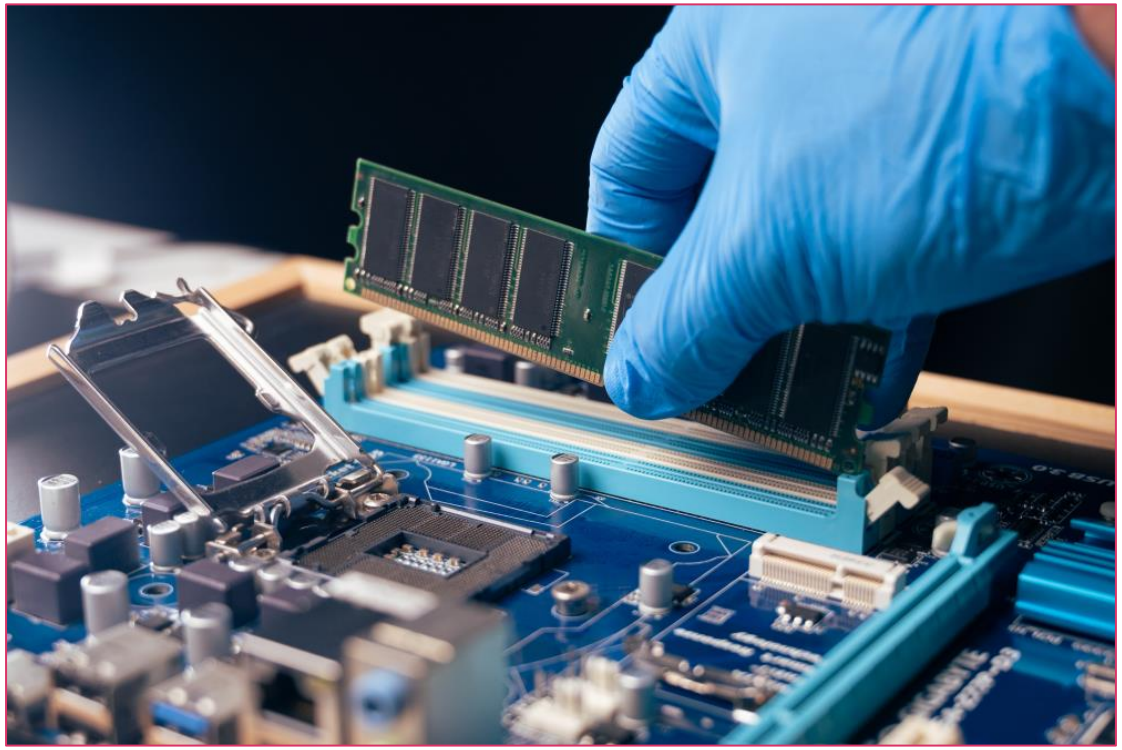
- Forensic teams will use some case software, such as EnCase from Guidance Software running on powerful Linux laptops
- These systems connect with USB/FireWire to write blocking imagers [for example, Forensic Toolkit or (FTK)]
- Forensic kits will bundle tools and utilities such as
  - Decryption and cracking tools
  - dd
  - Tcpdump, nbtstat, netstat, and netcat
  - memcpy
  - TShark or Wireshark

INVESTIGATIVE TECHNIQUES

- Filter for Security Identifiers (SIDs) and leverage regular expressions and searches
- Generate memory dumps and disk images using write blockers:
  - Hard disk drive (HDD) bit-level copy, sector-by-sector
  - Deleted files, slack spaces, and unallocated clusters
  - Compressed and encrypted volumes and files, then hashes
- Take digital pictures and conduct interviews and interrogations
- Bring in law enforcement agencies and other third-party investigators

ORDER OF VOLATILITY

1. CPU, cache, and register content
2. Routing table, Address Resolution Protocol (ARP) cache, process table, and kernel statistics
3. Memory
4. Temporary file system/swap space
5. Data on local hard disks
6. Directly attached or RAID data
7. Remotely logged data
8. Data on backup media
9. Data in cloud storage or archive



CHAIN OF CUSTODY

Chain of custody				
Registered/ certified mail	Date/time	Released by	Received by	Reason
	Date	Name/agency/organization	Name/agency/organization	
	Time	Signature	Signature	
	Date	Name/agency/organization	Name/agency/organization	
	Time	Signature	Signature	
	Date	Name/agency/organization	Name/agency/organization	
	Time	Signature	Signature	
	Date	Name/agency/organization	Name/agency/organization	
	Time	Signature	Signature	

FORENSIC ANALYSIS

- Forensic analysis is the process of determining who had motive, opportunity, and method (MOM) to commit the breach or crime:
  - Who, what, where, when, why, and how?
- These experienced and skilled team members may not get involved until the other preliminary activities are conducted
  - This is a combination of an art and a science
- This may include law enforcement, or other agencies as opposed to members of an internal incident response team or CSIRT

FORENSIC INVESTIGATION ACTIVITIES

- Tracking the attacker kill chain
- Using pattern matching and tracing tools
- Discovering hidden data (slack space)
- Extracting data remanence from incomplete wiping techniques (recovering deleted files)
- Reverse engineering of malware
- Disposing cloud-based or hypervisor-based files and artifacts
- Examining honey tokens and honey files
- Mapping logins using geolocation
- Conducting interrogations

FORENSIC REPORTING AND DOCUMENTATION

- Cyber forensic investigators must be prepared to present evidence in a manner that the legal system and courts consider admissible
- If the goal is to deliver justice, constructing a lucid and comprehensive digital forensics report is critical to the process
- Every claim must be supported by verifiable and substantiated, concrete evidence

FORENSIC REPORTING BEST PRACTICES

- Do not violate laws when collecting, handling, processing, or analyzing evidence
- Only include the pertinent data and information
- Avoid using complex or convoluted terminology:
  - Consider including a glossary in reports
- Focus on concrete and indisputable facts:
  - Exclude your personal opinions
- Make use of any forensics notes taken during the investigation
- Automate the process if possible

ELEMENTS OF A BASIC FORENSIC REPORT

a) Title of report
b) Table of contents
c) Case summary
d) Evidence summary
e) Objectives and hypothesis
f) Steps taken during an investigation (for example, forensic analysis)
g) Digital forensic tools that were utilized
h) Relevant findings
i) Recommended next steps (for example, criminal charges)
j) Appendices and exhibits (optional)
k) Formatting – numbering, headers, footers, etc. (optional)
l) Figures (optional)
m) Glossary (optional)

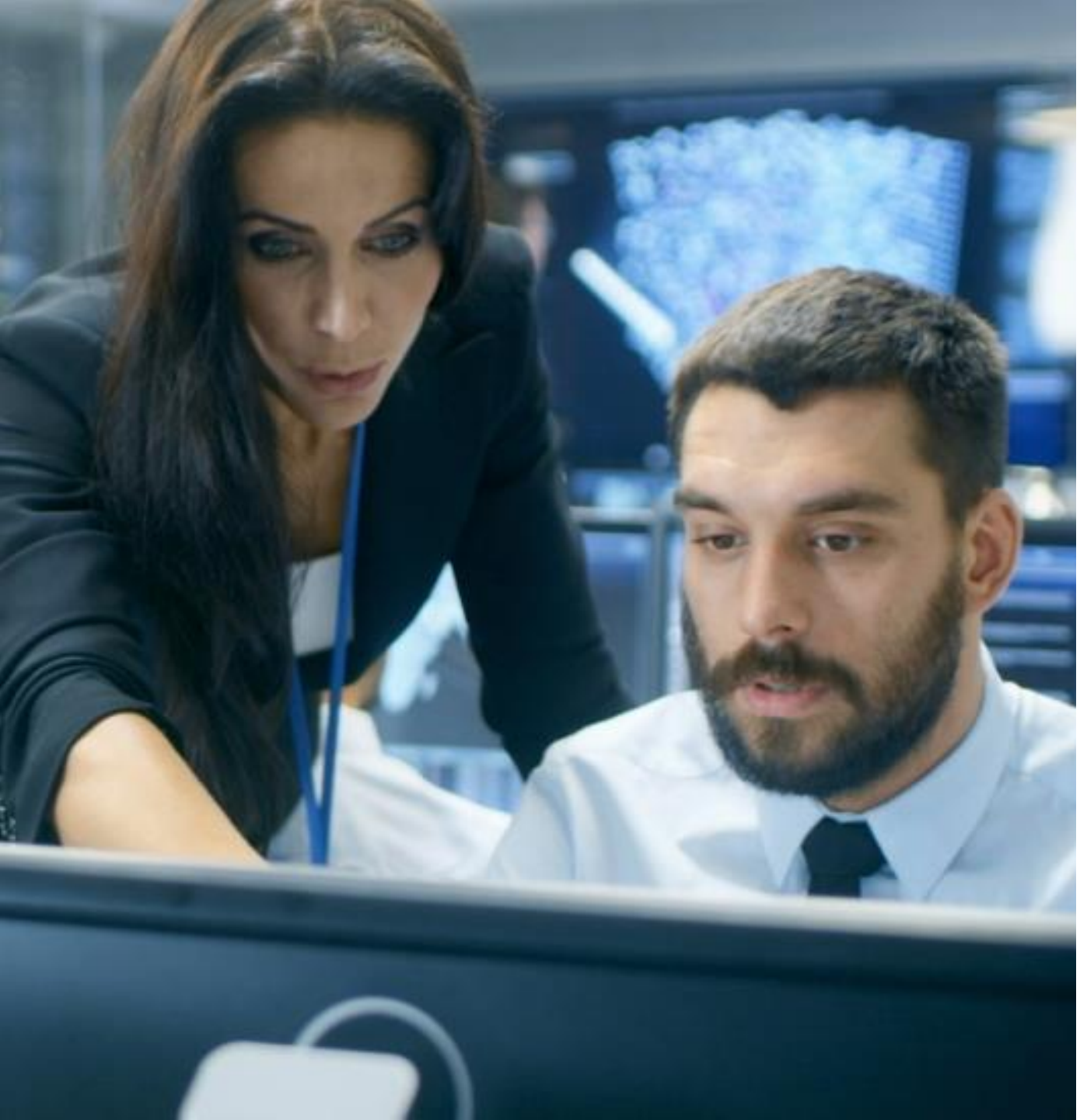
FOUNDATIONAL SECURITY OPERATIONS AND RESOURCE PROTECTION

Objectives

- Explore configuration management operations and change management practice
- Examine security operations like need-to-know/least privilege, segregation of duties, privileged account management, and job rotation
- Describe service-level agreements
- Know about resource protection
- Learn the incident management life cycle (detection, response, mitigation, reporting, recovery, remediation, and lessons learned)

CONFIGURATION MANAGEMENT OPERATIONS

- The goal of configuration management is to ensure that accurate and meaningful information is readily available regarding the configuration of applications and services along with the configuration items (CI) that support them
- Operations include all relationships and dependencies between the CIs
- Resource objects include hardware, software, networks, sites, vendors, suppliers, and people
- Operational activities include provisioning, baselining, and automation



CONFIGURATION MANAGEMENT

- Configuration management (CM) is a governance and systems life cycle process for ensuring consistency among all assets (CIs) in an operational environment:
  - Classifies and tracks individual CIs
  - Documents functional capabilities and interdependencies
  - Verifies the effect a change to one configuration item has on other systems

CONFIGURATION MANAGEMENT

- CM practices offer the required data about assets and their configurations, including their interactions with other assets, which assists administrators and managers with
  - Problem resolution
  - Incident response
  - Network component deployment
  - Strategy formulation
  - Budgetary forecasting
  - Global decision-making

CONFIGURATION MANAGEMENT RESOURCES

Directory services tools and utilities

Centralized inventory engines and baselines

Infrastructure as Code (IaC) diagrams and topologies

Configuration management databases (CMDBs)

CONFIGURATION MANAGEMENT DATABASE

- A configuration management system (CMS) is a set of data, tools, utilities, and processes used to support configuration management
- All information should be tagged and labeled with a common unified schema, preferably using key-value pairs
- **This data will often populate a data warehouse system known as a CMDB:**
  - Relational databases have been used historically
  - NoSQL/document databases are emerging as a common solution
- Companies often leverage a cloud service provider, such as AWS DynamoDB or Google BigQuery

CMDB

- A CMDB is not a typical data warehouse
- It plays a critical role in several IT management initiatives, like IT service management (ITSM) and IT asset management (ITAM)
- The CMDB assists various IT services to better align with business needs by providing current and accurate data to
  - Change and patch management
  - Incident and problem management
  - Availability management
  - Release and deployment management

CHANGE MANAGEMENT PRACTICE

- Is also called the "change control practice"
- Maximizes the amount of successful service and product changes
- Should make certain that risks have been adequately assessed, authorized, and managed with a change schedule
- Operates with the configuration database to track all possible dependencies and repercussions of changes
- Involves a change log or change database

TYPES OF CHANGES

Standard

- Are low-risk changes
- Are pre-authorized and well-documented
- Can be automated
- Do not need additional authorization
- Example: changing directory password

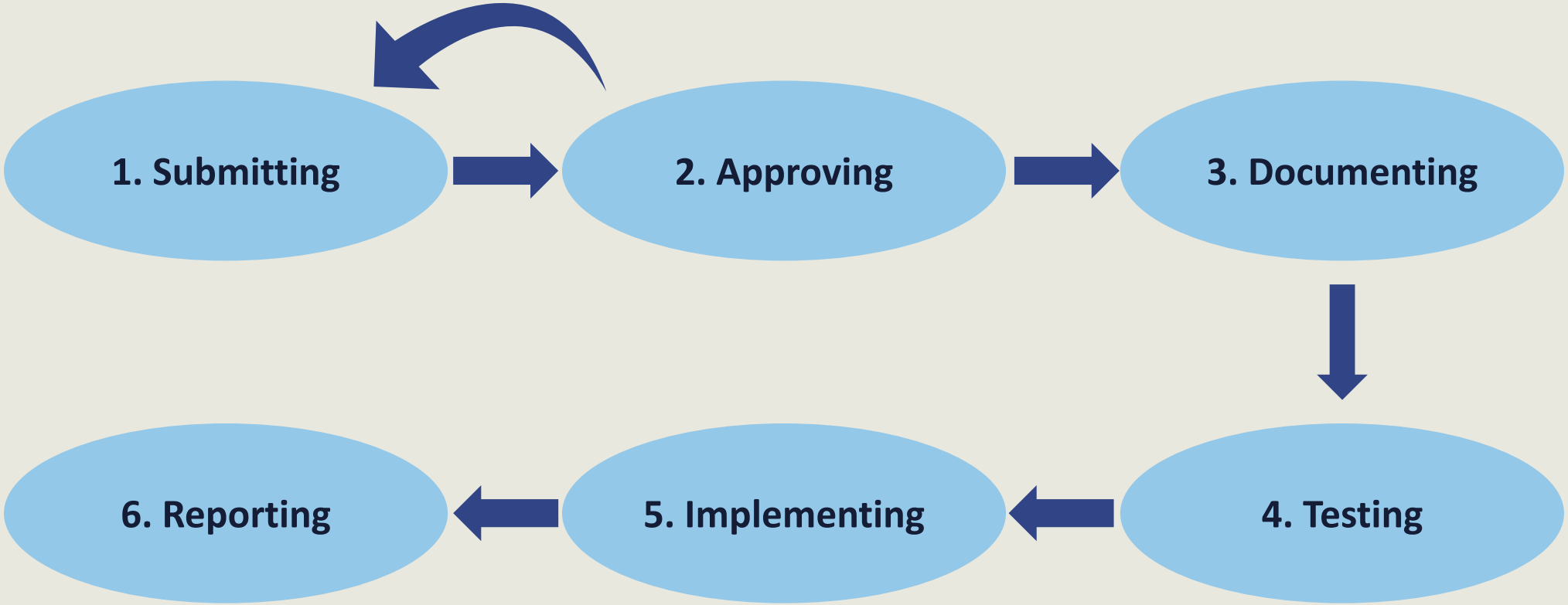
Normal

- Follow a specific process for scheduling, assessment, and authorization
- Are lower risk, but they do go through an approval process
- Example: onboarding a new phone or laptop, installing an application

Emergency

- Must be implemented immediately
- Are often a result of problem management or after-action reporting
- May involve escalation or an emergency advisory board if the number of resources or disruption is significant

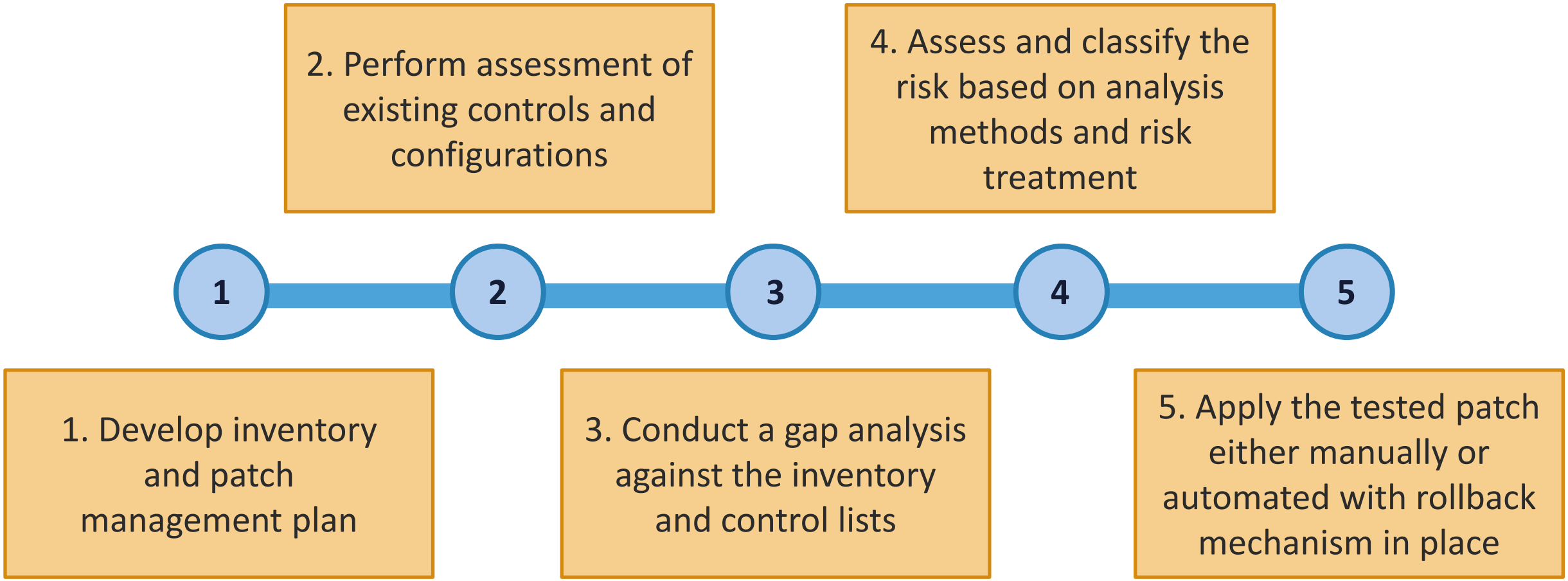
CHANGE MANAGEMENT LIFE CYCLE



PATCH MANAGEMENT

- Patch management is a critical aspect of configuration and change management
- Vulnerability/exposure reviews and gap analysis are not performed or done properly regarding patches and updates
- Only certain personnel should have the authority to test, apply, and determine the urgency of patching activities
- Agreements with any applicable vendors should also be made to address any potential issues before patch deployment

PATCH MANAGEMENT LIFE CYCLE



LEAST PRIVILEGE AND ZERO TRUST

- Although both Zero Trust and least privilege control the levels of access to resources such as data, networks, and other assets, each takes a different approach
- Zero trust is a more all-encompassing approach, whereas least privilege is more granular
- The principle of least privilege (PoLP) states that users, systems, and processes should have only the minimum levels of permissions necessary to perform their tasks
- The goal is to reduce the attack surface so that if compromised, the possible damage and lateral movement on the network are reduced

LEAST PRIVILEGE AND ZERO TRUST

- Zero Trust is a wide-ranging architecture that integrates several principles and technologies, **including least privilege**, to protect resource objects
- Least privilege is an explicit principle that is used within a Zero Trust framework or similar security model
- Zero Trust is focused on continuous verification and never implicitly trusts, while least privilege deals with limiting specific access rights for users to an absolute minimum

SEGREGATION OF DUTIES (SoD)

- Segregation of duties (SoD) is a critical internal administrative, physical, and technical control
- It is an important aspect of an effective risk management strategy
- SoD focuses on dividing up responsibilities of key organizational processes by distributing the discrete functions of to multiple people, groups, teams, or departments
- This can be helpful in reducing the risk of potential errors and fraud

SEGREGATION OF DUTIES (SoD)

- SoD is intended to thwart unilateral actions in an organization’s workflow, which often lead to incidents that exceed the organization’s risk tolerance
- In a nutshell, no single person or group should be granted control over a task or asset where they have the unrestrained ability to overlook errors, fabricate information, exfiltrate data, or attempt theft
- **A common example is to have a separate data backup group and a separate data recovery or restoration team**

PRIVILEGED ACCOUNT MANAGEMENT (PAM)

- Is a security initiative that enables organizations to counter cyberthreats through visibility, detection, and hindrance of all unauthorized privileged access to critical resource objects
- Is also called privileged identity management (PIM) or simply privilege management

PAM

- PAM operates by implementing security processes that control and monitor all privileged account access
- It emphasizes monitoring and management of the use of privileged accounts:
  - This includes local and domain administrative accounts, emergency accounts, specialty management, and service accounts
- Two main use cases for PAM are averting credential theft and attaining compliance - payment card industry (PCI), Sarbanes-Oxley Act (SOX)

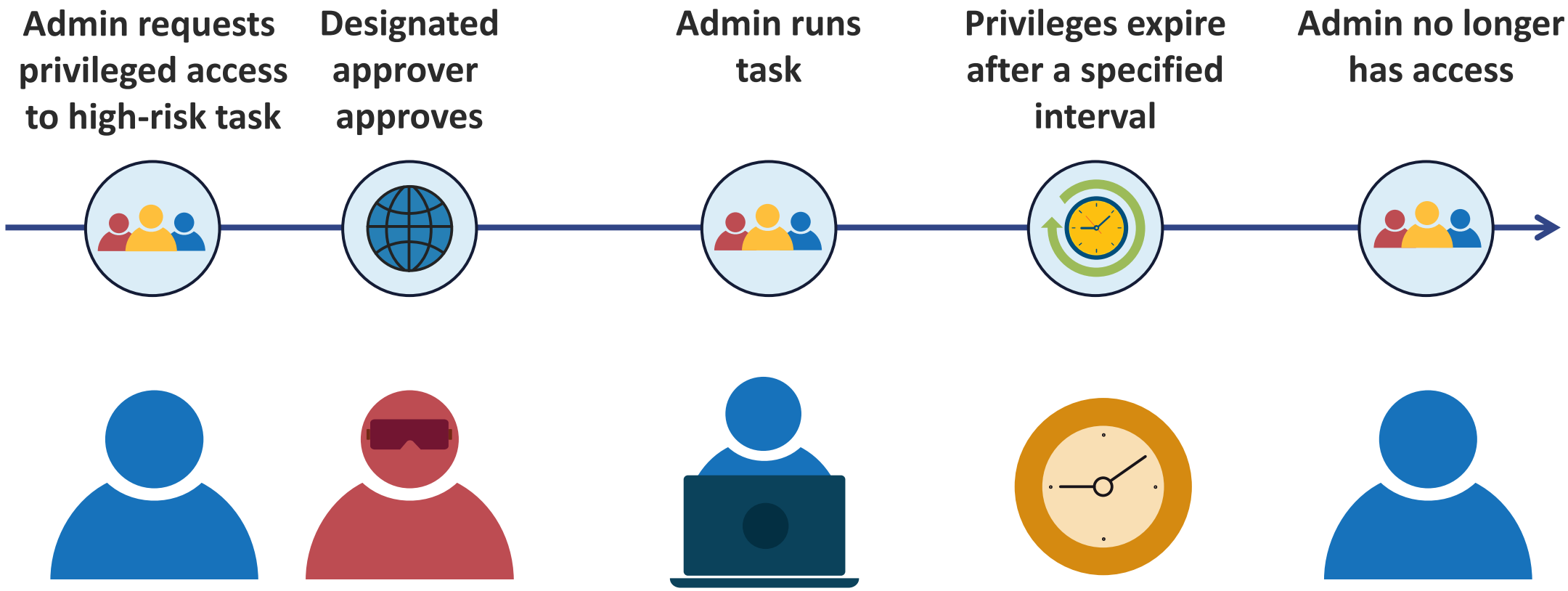
PAM

- A PAM initiative identifies the users, processes, and mechanisms that demand privileged access and designates the policies that apply to them
- It must support established security policies such as automated password management and multi-factor authentication
- Realm and domain administrators must also be able to automate the process of generating, modifying, and deleting accounts
- PAM should also continuously monitor sessions to facilitate report generation for security teams to recognize and scrutinize anomalies

BENEFITS OF PAM

- Deliver just-in-time access to critical resources
- Support DevSecOps with unified password security
- Permit secure passwordless remote access with encrypted gateways
- Monitor privileged sessions to back exploratory audits
- Analyze anomalous privileged actions that can harm the organization
- Trap privileged account events and incidents for compliance audits
- Generate reports on all privileged user access and activity

MICROSOFT PAM



JOB ROTATION

- Job rotation is an administrative control that is often part of SoD or Zero Trust initiatives
- It is also called rotation of duties
- Job rotation is based on the security principles of need-to-know, privilege, and access, and is considered an access control method
- Rotation of duties initiatives help organizations enhance the skill sets of their employees and be resilient to single points of personnel-based failure

JOB ROTATION

- Job rotation is also an excellent way to discover and mitigate insider security threats like collusion and the committing of fraudulent activities and acceptable use policy (AUP) violations
- Typically, there is a predefined timeframe for the standard rotation of a role within a particular business process
- Privileged users should be the highest priority for job rotation policies
- **Job rotation can also include policies such as mandatory time off or forced vacations**

SERVICE-LEVEL AGREEMENTS (SLA)

- An SLA will define the precise responsibilities of the service provider (vendor) and customer expectations
- SLAs help clarify the support system (service desk) response to problems or outages for an agreed level of service
- They can be internal between business units or departments (these are often called operational-level agreements [OLA])
- They should be used with new vendors or cloud providers for 24-hour support

SERVICE-LEVEL AGREEMENTS (SLA)

- The provider must realize that the use of contractual agreements such as hosting/connection agreements and SLAs are used to allocate shared responsibility and risk among both providers and consumers
- The SLA will also establish liability for the failure of one or more services and control
- The realization of risk is appropriately documented and understood by all involved parties

MASTER SERVICE AGREEMENT (MSA)

- An MSA is a contract two parties enter into during a service transaction
- As part of due diligence in your business continuity plan (BCP), any/all expectations with the candidate service provider must be confirmed
- This agreement details the expectations of both parties
- The goal of a master service agreement is to make the contract process faster
- It also should make future contract agreements simpler

ELEMENTS OF AN MSA OR SLA

- Confidentiality
- Delivery requirements
- Limitations of liability and dispute resolution
- Geographic locations
- Intellectual property rights
- Payment terms and cost structure
- Venue of law
- Warranties
- Work standards

RECIPROCAL AGREEMENTS

- A reciprocal agreement is between two organizations with similar infrastructure and technology – often difficult to legally enforce
- The most common goal is that one can be a recovery site for the other in case of a disaster or lengthy outage
- Reciprocal agreements are also seen with data backup and escrow services whereby two departments or organizations agree to store each other's backup data on their computers

RESOURCE PROTECTION

- Resource security and protection are two similar terms that represent ways to safeguard computer resources, data at rest, and data in transit
- Protection controls the access to all system resources
- It is explicitly the action of external and physical security
- Resource protection offers discrete and tangible feedback from controls that secure access to all the systems and resources

EXAMPLE: PROTECTION WITH INFORMATION RIGHTS MANAGEMENT (IRM)

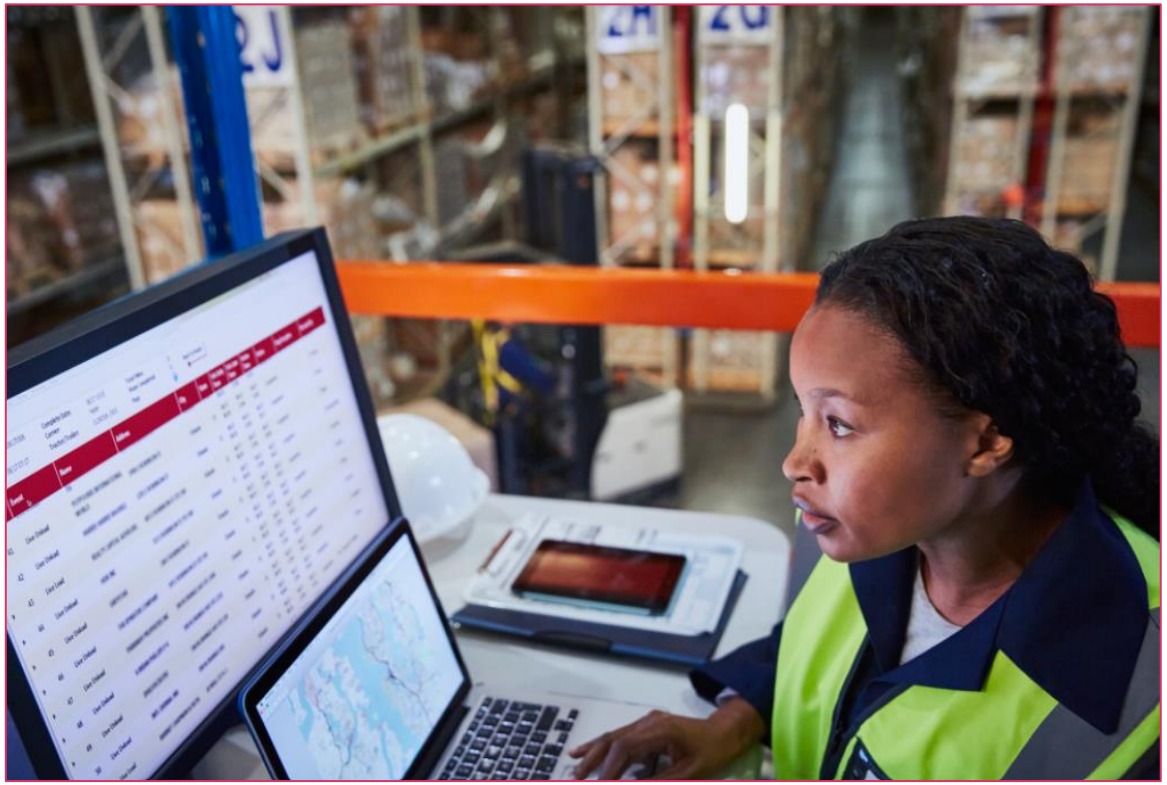
- The objectives of information rights management (IRM) are to employ controls that work with, or in addition to, access control security to protect data and file-level assets
- An example is to control copying, deleting, and modifying certain PDF documents to protect intellectual property (IP) and copyrights
- Content creators must protect and enforce all access and usage of digital assets
- Since digital signing and certificates are often used, an enterprise public key infrastructure (PKI) may be part of the policy

EXAMPLE: WINDOWS RESOURCE PROTECTION (WRP)

- Windows Resource Protection (WRP) averts the replacement of critical system files, folders, and registry keys installed with the operating system
  - It was first introduced in Windows Server 2008 and Windows Vista
- Permission for full access to change WRP-protected resources is restricted to the "TrustedInstaller" service
- Resources protected with WRP can only be modified using the Supported Resource Replacement Mechanisms with the Windows Modules Installer service
- This protection helps to avoid application and operating system failures

INCIDENT MANAGEMENT LIFE CYCLE: PREPARATION

- Incident response refers to the steps taken when a negative event disrupts normal operations
- The primary goal is to reduce the immediate impact
- Incident management documents incident types and category definitions based on risk assessments, risk registers, and the business impact analysis (BIA)



INCIDENT MANAGEMENT LIFE CYCLE: PREPARATION

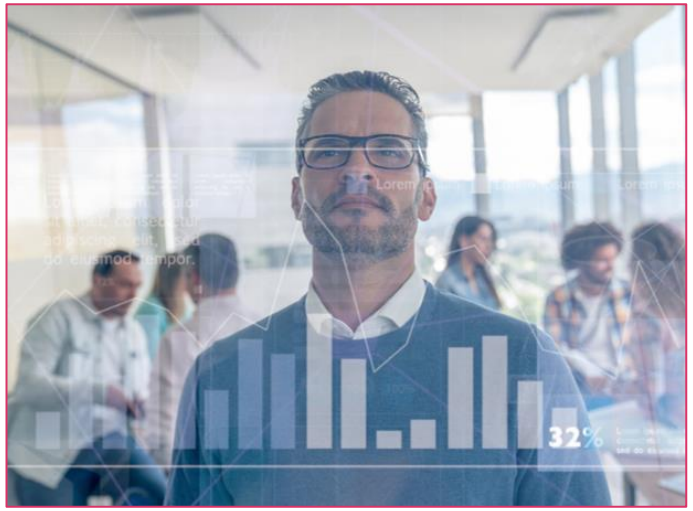
- Preparation involves all information gathering, missions, charters, and project initiation tasks
- Managers must get buy-in and funding from executive management and know the scope of the response plan
- This involves establishing incident response teams:
  - Will the organization use a swarm team?
- Determine the roles and responsibilities of internal employees on incident response teams

INCIDENT MANAGEMENT LIFE CYCLE: PREPARATION

- Incident management preparation also involves knowing the roles and responsibilities of the first responders, including reporting requirements and escalation processes
- Security managers collect contact lists, public relations people, and legal teams
- Best practices involve exercises, drills, and simulations

INCIDENT MANAGEMENT LIFE CYCLE: DETECTION AND RESPONSE (TOOLS AND SERVICES)

- Various logs and SNMPv3 traps
- NetFlow and SIEM collection
- Next generation intrusion prevention system (NGIPS) and endpoint detection and response (EDR) alerts and logs
- Hybrid cloud-based visibility tools using machine learning and artificial intelligence data analysis
- Vulnerability databases - Common Vulnerabilities and Exposures (CVE), MITRE, National Vulnerability Database (NVD)
- Tool kits such as Kali Linux, or Parrot
- Web application vulnerability scanners like Burp Suite and Zed Attack Proxy (ZAP)



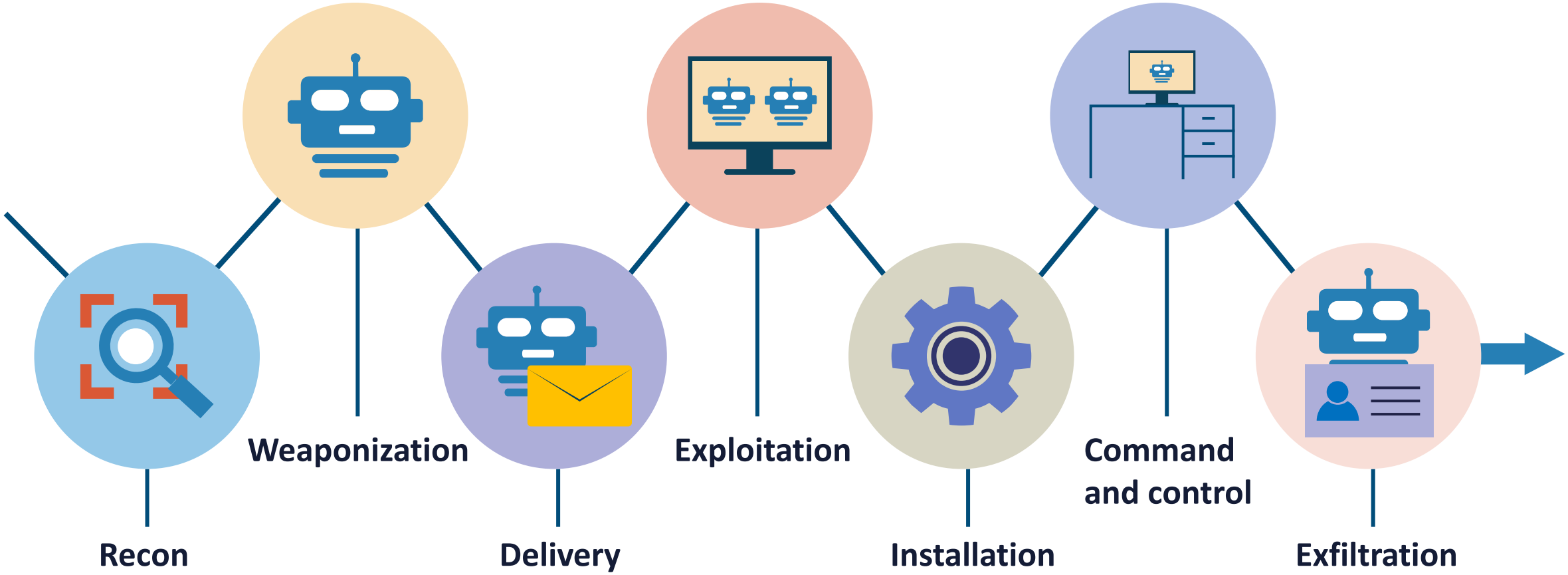
INCIDENT MANAGEMENT LIFE CYCLE: DETECTION

- Responders (manual or automated) separate an event from an incident immediately, using predefined metrics and experience
- In this early stage, categorization and prioritization of the incident is based on an established risk register or risk database:
  - When did it occur?
  - How were you alerted?
  - Who made the discovery?
  - What is the scope of impact?
  - Does it qualify for escalation or disaster recovery?

INCIDENT MANAGEMENT LIFE CYCLE: RESPONSE

- The main goal is containment of the outbreak or malware exploit
- Responders implement short-term processes, such as disconnecting devices from the network
- Utilize firewalls, NGIPS, machine learning algorithms, and other forensic tools to maintain separation, containment, and segregation
- Evaluate backups and snapshots for future recovery
- **If the root cause can be determined here, that is a bonus but not necessarily the goal**

RESPONSE INVOLVES UNDERSTANDING THE KILL CHAIN

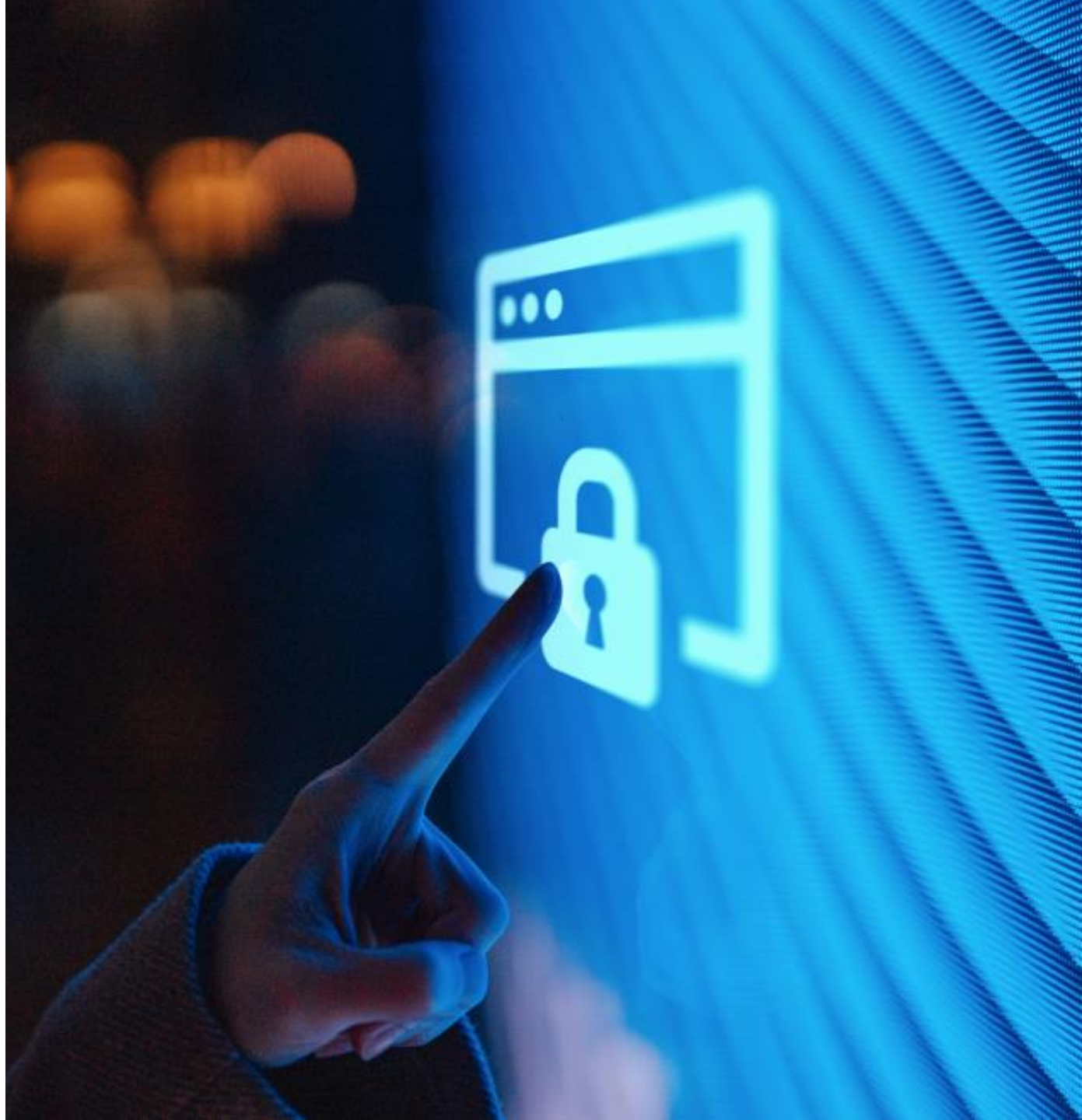


INCIDENT MANAGEMENT LIFE CYCLE: MITIGATION

- This step is also called eradication and is often integrated with the previous phase as opposed to being a separate activity
- Mitigation involves quarantine and applying immediate remedies, if available
- It also consists of removing all indicators of compromise and any action, artifacts, remnants, or fingerprints associated with the attack
- **Mitigation tools include antivirus programs; next generation EDR; SOAR runbooks; and cloud-based threat management services**

INCIDENT MANAGEMENT LIFE CYCLE: REPORTING

- Reporting and documentation is rarely a separate step but rather ongoing persistent activities throughout the entire life cycle
- This phase does not include the After-Action Report (AAR) and lessons learned
- Reports should be generated from physical, digital, and/or audio notes taken throughout the entire process



INCIDENT MANAGEMENT LIFE CYCLE: REPORTING

- Final reports should
  - Be concise and comprehensive
  - Be generated with different audiences in mind
  - Use newer graphical representation with Python and R programming tools
  - Include recommendations to prevent future incidents
  - Take problem management into consideration

RECOVERY AND REMEDIATION

- The process of restoring negatively affected data, applications, systems, and devices to an established baseline performance level or, if possible, the original state
- This often involves only remediation to a certain operational point and not total recovery
- During this process, it is vital to establish that you are not in danger of another incident or breach
- This will often involve BIA metrics and indicators like RTO, RPO, and MTTR

RECOVERY AND REMEDIATION

- This is more elaborate than recovery, as it involves a remedy that puts the application or system into a state before the incident occurred
- Remediation may take hours or weeks depending on the fact that the incident may rise to the state of a disaster or catastrophe and business continuity is occurring
- Recovery and remediation are often combined into the same phase or stage of incident response

INCIDENT MANAGEMENT LIFE CYCLE: LESSONS LEARNED

- AARs should be produced after incident response testing/drills AND the actual real-world events
- This data should populate a lessons learned ledger or database
- This is the bulk of the information and knowledge gained from the process of conducting the program
- Data > Information > Knowledge > Wisdom

INCIDENT MANAGEMENT LIFE CYCLE: LESSONS LEARNED

- Hold sessions at the response close-out
- Share and use knowledge derived from an experience
- Endorse the recurrence of positive outcomes
- Prevent the recurrence of negative outcomes
- Try to avoid "blamestorming," although someone may be ultimately held accountable if expected due care and diligence were not performed