WELCOME BACK TO DAY 4

Michael
and
Irfan

Class will begin at 10:00 am
Central Standard Time

VULNERABILITY MANAGEMENT

Objectives

- Explore threat feeds and other resources
- Look at application vulnerability assessment and vulnerability scanning
- Understand penetration testing
- Examine vulnerability response and remediation
- Survey remediation validation and reporting

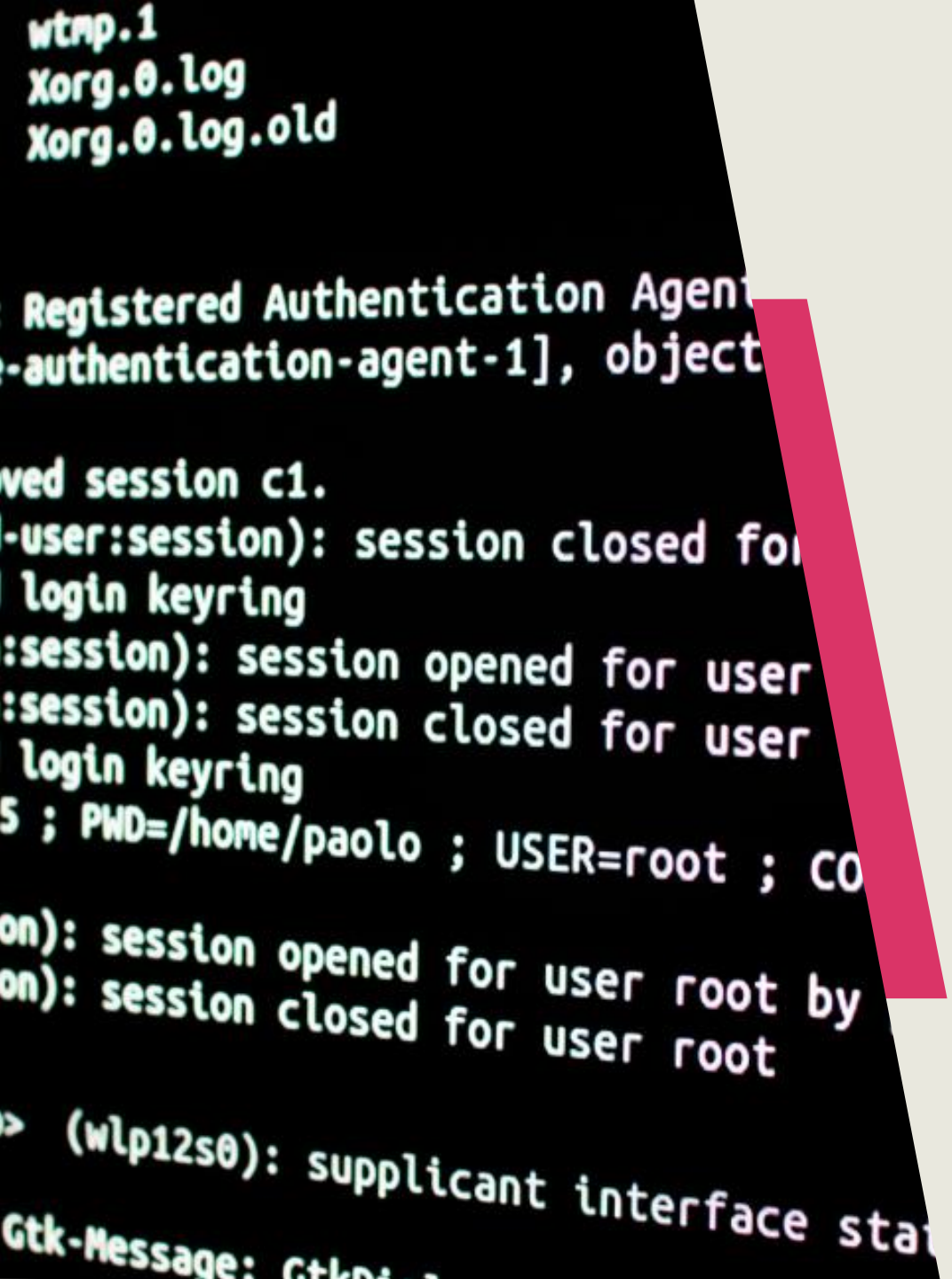
DEMO: EXPLORING THREAT FEEDS AND RESOURCES

In this demo…

We will explore threat feeds and resources

APPLICATION VULNERABILITY ASSESSMENT

- An application vulnerability assessment is a testing methodology used to recognize and assign severity levels to as many security defects as possible in a timeframe
- This process typically involves manual and automated techniques with varying degrees of precision with an emphasis on comprehensive coverage
- It is often part of a larger software assurance initiative such as OWASP Software Assurance Maturity Model (SAMM)



STATIC APPLICATION SECURITY TESTING (SAST)

- SAST tools are also known as code analyzers that conduct a direct white-box analysis of the application source code
- The analysis runs on a static view of code, in that the code is not running at the time of the assessment
- SAST security tools are mainstream and are widely adopted throughout the software industry
- They have broad programming language support and use concepts that are relatively easy to comprehend
- SAST code analyzers have no visibility of the execution flow, can be slow, inaccurate, and outdated, and often need additional customization and/or tuning

DYNAMIC APPLICATION SECURITY TESTING (DAST)

- DAST tools are most often web scanners like OWASP ZAP and Burp Suite (vulnerability scanners)
- They perform know-nothing in that they do not have access to the code or the implementation specifics
- A DAST tool will only inspect the system's responses to a series of tests designed to highlight vulnerabilities
- They function independently of the underlying application platform and offer solid support for manual penetration testing

PACKAGE MONITORING

- Processes and tools that troubleshoot application performance issues in Dev, QA, and production environments with:
  - Code-level insights
  - Distributed transaction tracing
  - Application service maps, and more
- They usually support Java, .NET, .NET core, Node.js, Python, PHP and Ruby applications
- Container monitoring empowers DevOps teams to stay on top of outages and pinpoint server issues with root cause analysis capabilities
  - Proactively monitor and optimize the performance of Docker, Kubernetes and Red Hat OpenShift containers and applications

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
- Vulnerability scanners include Nessus, OpenVAS, Core Impact, Nexpose, GFI LanGuard, QualysGuard, OWASP ZAP, Burp Suite

NETWORK SCANNERS

- 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

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

COMPLIANCE SCANNING

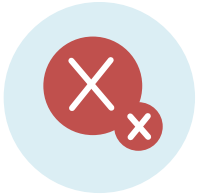
- Different from performing a vulnerability scan, although there can be some overlap
- Compliance audit decides if a system is configured in agreement with a recognized governance policy whereas a vulnerability scan determines if the system is exposed to known vulnerabilities
- Sometimes compliance involves auditing more sensitive data and systems
- 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

ACCURACY CONFIRMATION

True Positive = accurate + action taken

True Negative = accurate + action not taken

False Positive = error + action taken



False Negative = error + action not taken

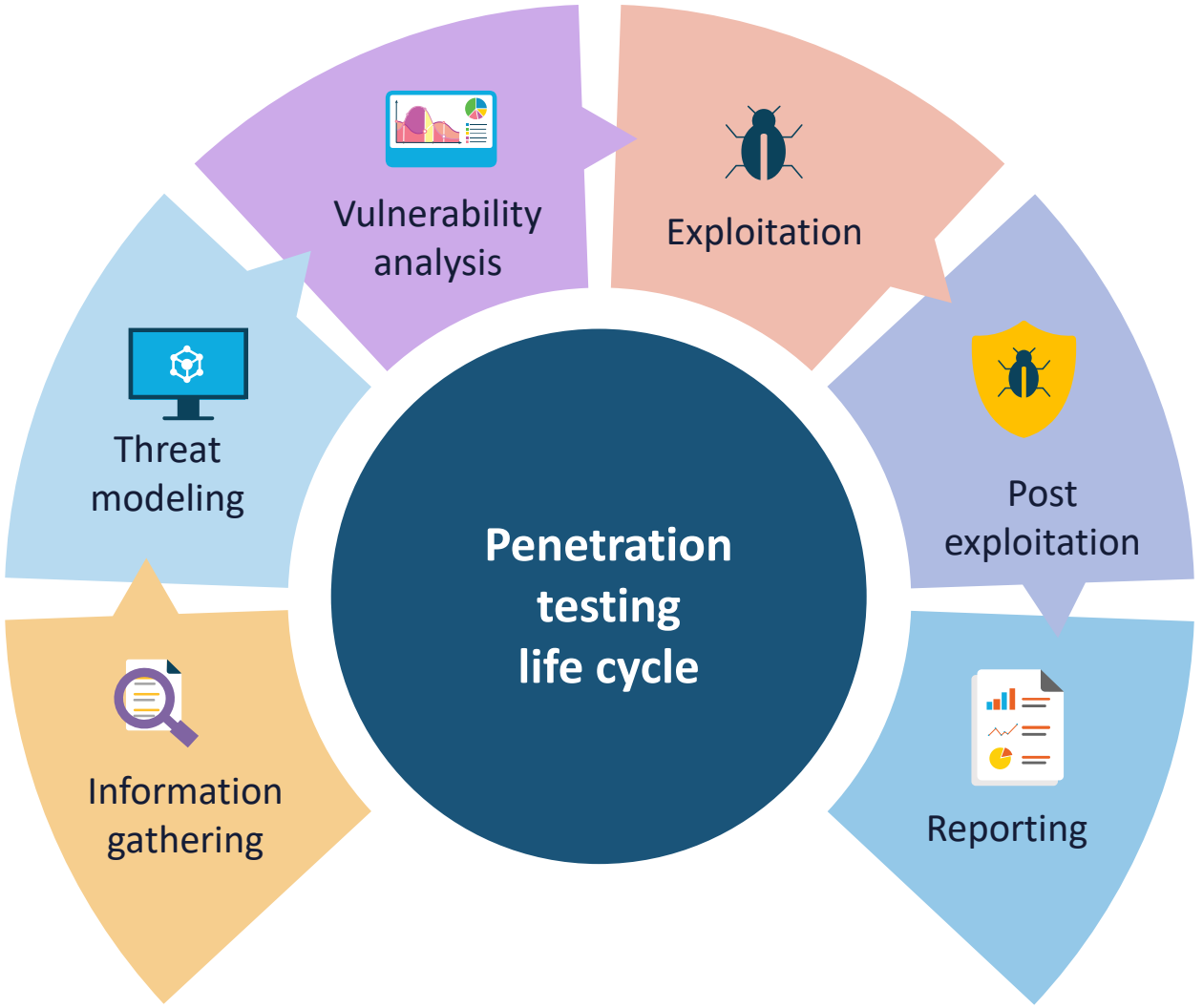
PENETRATION TESTING

- 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 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

PENETRATION TESTING TERMS

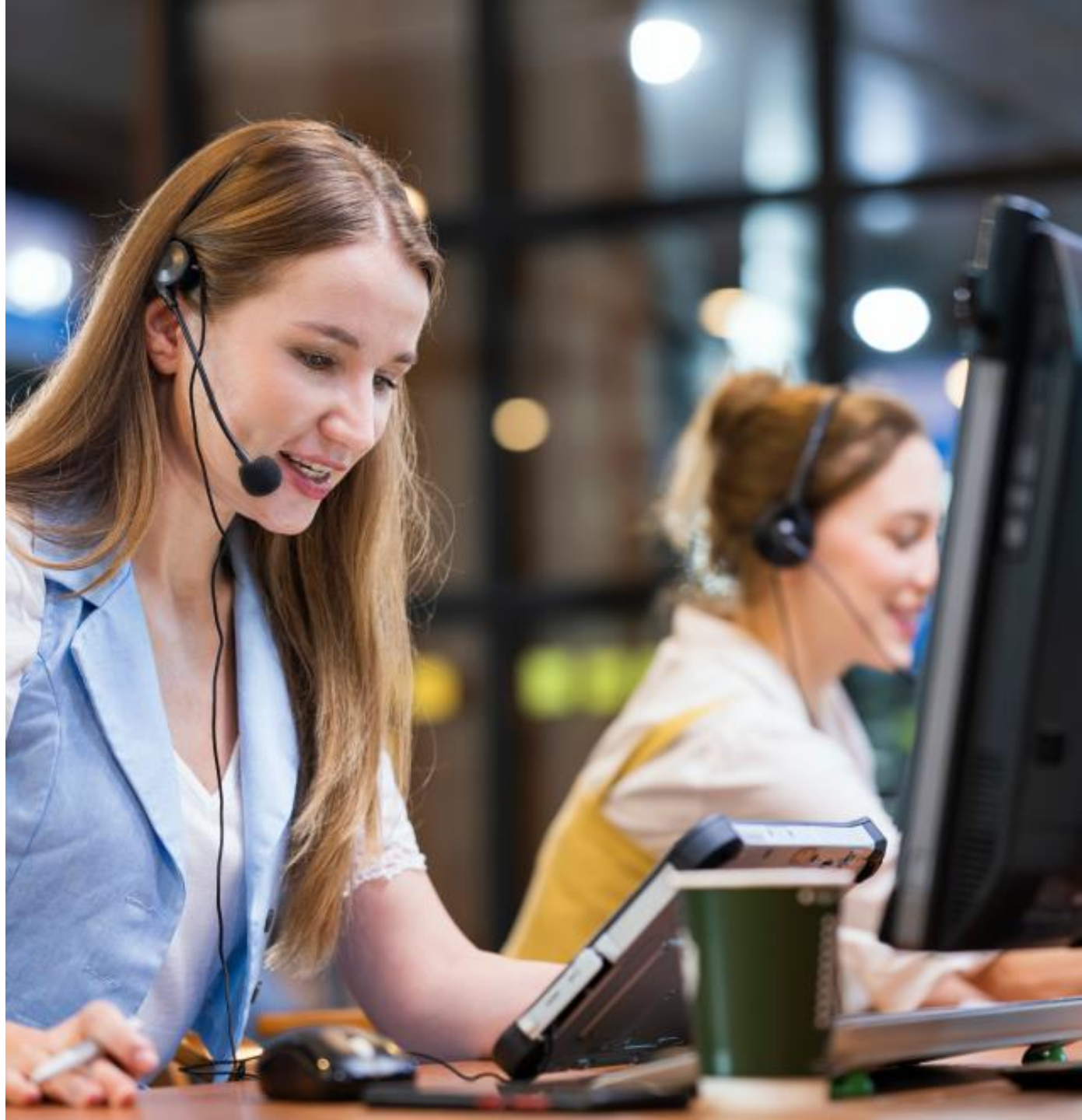
- Pre-engagement meetings determine a variety of elements:
  - Scoping and restrictions
  - Pricing and cost structure
  - Know-all, know-nothing (clear/opaque or viewed/hidden or visible/invisible)
  - Credentialed vs. non-credentialed
  - Bug bounties
  - Intrusive vs. non-intrusive

PENETRATION TESTING LIFE CYCLE



VULNERABILITY RESPONSE AND REMEDIATION

- Additional control implementation
  - Categories (Administrative, Technical, Physical)
  - Types (Detective, Preventative, Deterrent, Compensating, Corrective)
- Patch management (tested)
  - The initiative of applying updates to software, drivers, and firmware to protect against vulnerabilities
  - Effective patch management also assists in choosing the optimal performance and productivity of applications, services, and systems



VULNERABILITY RESPONSE AND REMEDIATION

- Insurance
  - A method for risk sharing treatment
- Segmentation and compartmentalization
  - Partitioning systems, micro-servers, host applications, containers and more to introduce countermeasures
- Compensating controls
  - The security and privacy controls employed in lieu of the controls in the baselines that offer equivalent or comparable protection for a system or organization
- Exceptions and exemptions

REMEDIATION VALIDATION AND REPORTING

- Implementing controls in response to vulnerability scanning and testing must be followed with security control assessment and evaluation
- Next steps involve tuning to address false positives and false negatives
- This will lead to rescanning as well as any new configuration changes or updates/versioning

REMEDIATION VALIDATION AND REPORTING

- Official internal and external audits should follow to assess compliance, maturity, assurance, certification, and accreditation
- The assurance testing process concludes with validation and robust reporting

ROBUST REPORTING

- Reports should have as much information as necessary but not a "data overload"
- May need to express in simpler terms or have different reports for different target audiences
- Dashboards are very effective (R programming)
- Understand components of visual communications
  - Avoid three-dimensional representation
  - Use a palette of sequential colors
  - Avoid pie charts in favor of scatterplots, bars and bubble charts, histograms, density plots, and boxplots

SECURITY MONITORING & ALERTING

Objectives

- Explore computing resource monitoring and activities
- Examine SCAP, SIEM, and SOAR
- Learn about data loss prevention (DLP) systems, Simple Network Management Protocol (SNMP), and NetFlow

MONITORING COMPUTING RESOURCES

- Monitoring and visibility is a critical aspect of hardened security and zero trust initiatives
- The more automated the monitoring solution, the more accurate the results will be as human error is minimized
- All types of systems must be monitored including:
  - Corporate LAN endpoint devices
  - Web, email, productivity, and other application servers (i.e., SharePoint)
  - Voice over Internet Protocol (VoIP), messaging, and conferencing services
  - Databases and storage area networks
  - Infrastructure devices
  - Customer premises edge

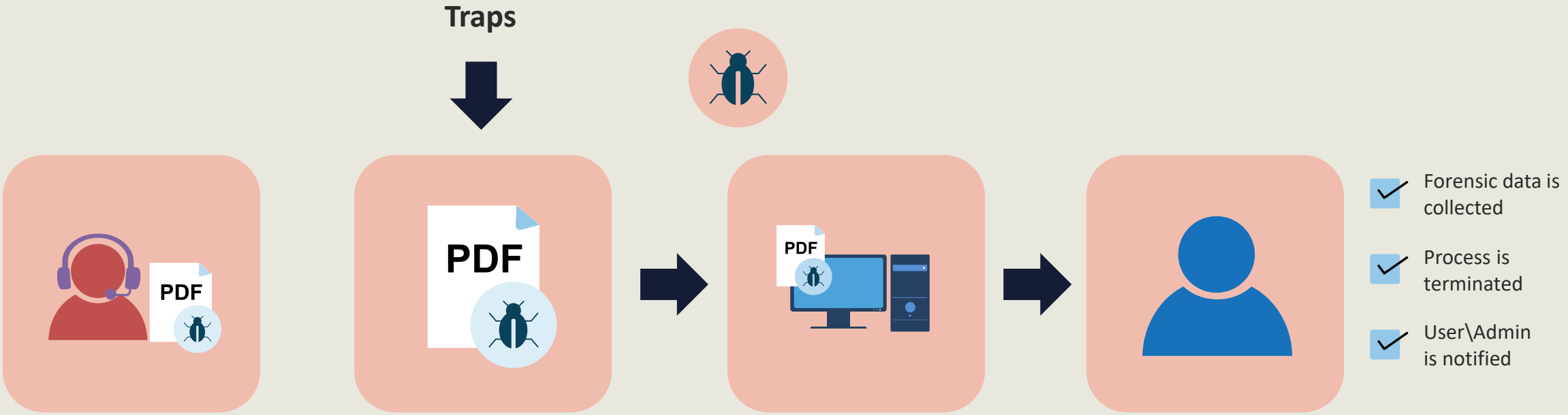
MONITORING AND VISIBILITY

- Network monitoring tools enhance visibility into system health by offering real-time information about various wired, wireless, and cloud-based components
- This suite of tools utilizes two techniques to capture performance metrics from assorted infrastructure and security devices – both physical and virtual:
  - **Agent-based monitoring** leverages lightweight software, known as a monitoring agent, on the devices or virtual machine to track the uptime and performance
  - **Agentless monitoring** uses special application programming interfaces (APIs) or integrated code to track the health of the devices.

AGENT-BASED MONITORING

- A prototypical example of agent-based monitoring is using Simple Network Management Protocol version 2C and 3 agents on infrastructure devices to send traps and informs to SNMP management stations
- In cloud computing environments, special agents can be embedded into virtual machine instances or installed on instantiated virtual servers to perform various system management activities

CASE STUDY: PALO ALTO NETWORKS TRAPS



Infected document opened by unsuspecting user

Traps seamlessly injected into processes

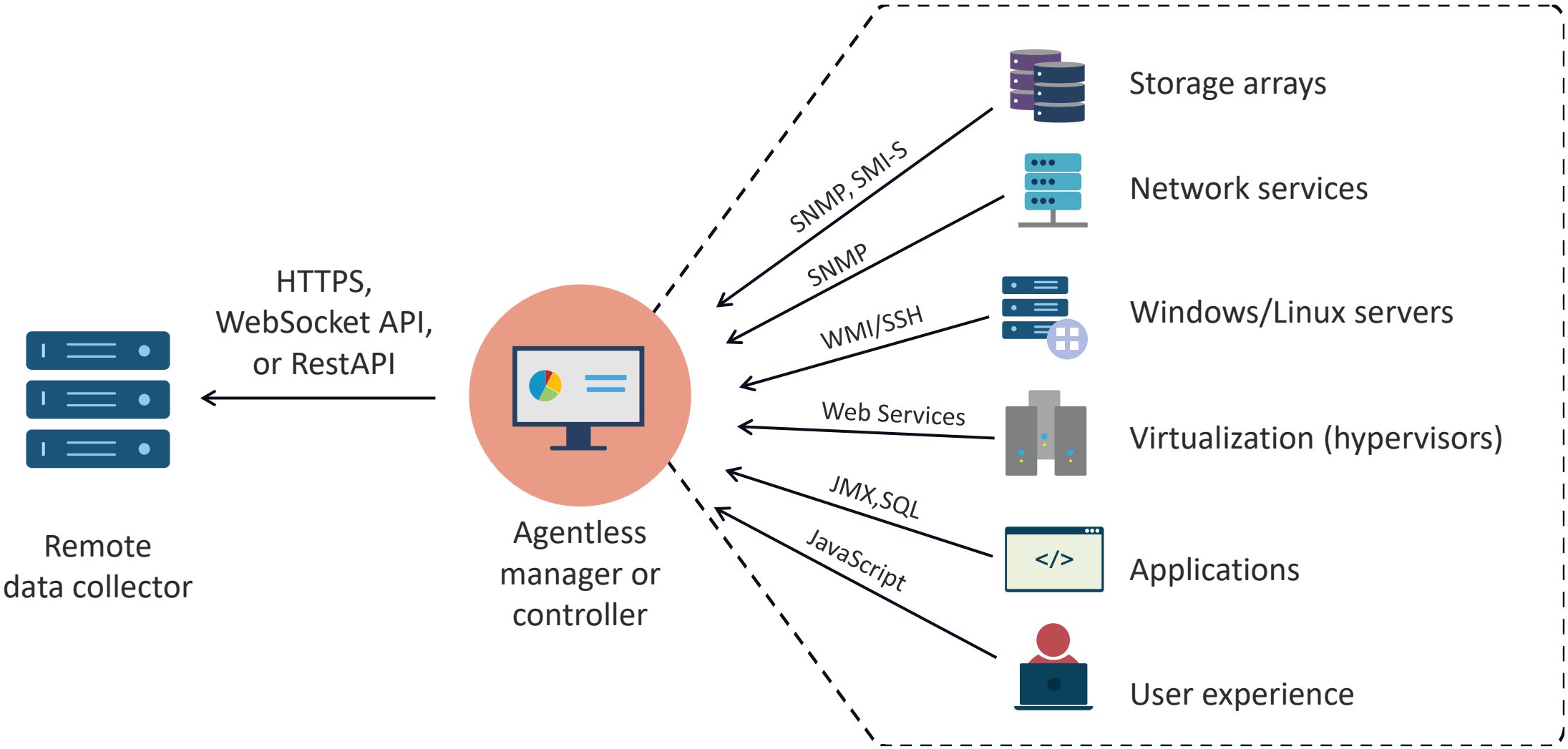
Exploit technique attempted and blocked by Traps before any malicious activity is initiated

Traps report the event and collect detailed forensics

AGENTLESS MONITORING

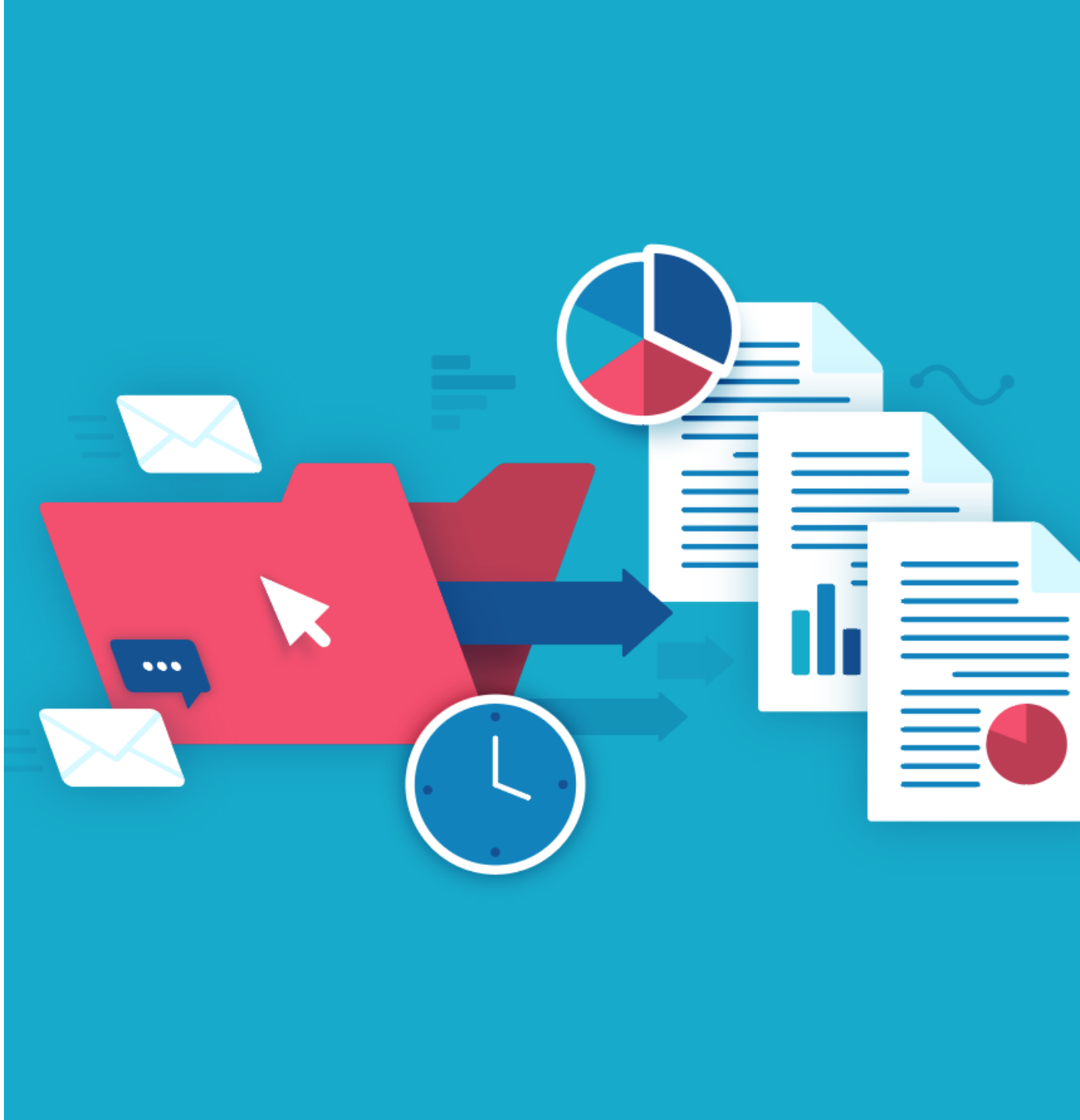
- Agentless monitoring is a less intrusive way to achieve visibility
- It typically utilizes application-specific APIs and different network protocols (such as SNMP and Windows Management Interface -WMI) to discern the overall performance of on-site and cloud-based assets, such as servers and applications
- This monitoring method does not involve the overhead of installing, tuning, and updating dedicated or third-party monitoring agents on every component
- This may be considered easier than the traditional agent-based approach

AGENTLESS MONITORING



LOG AGGREGATION

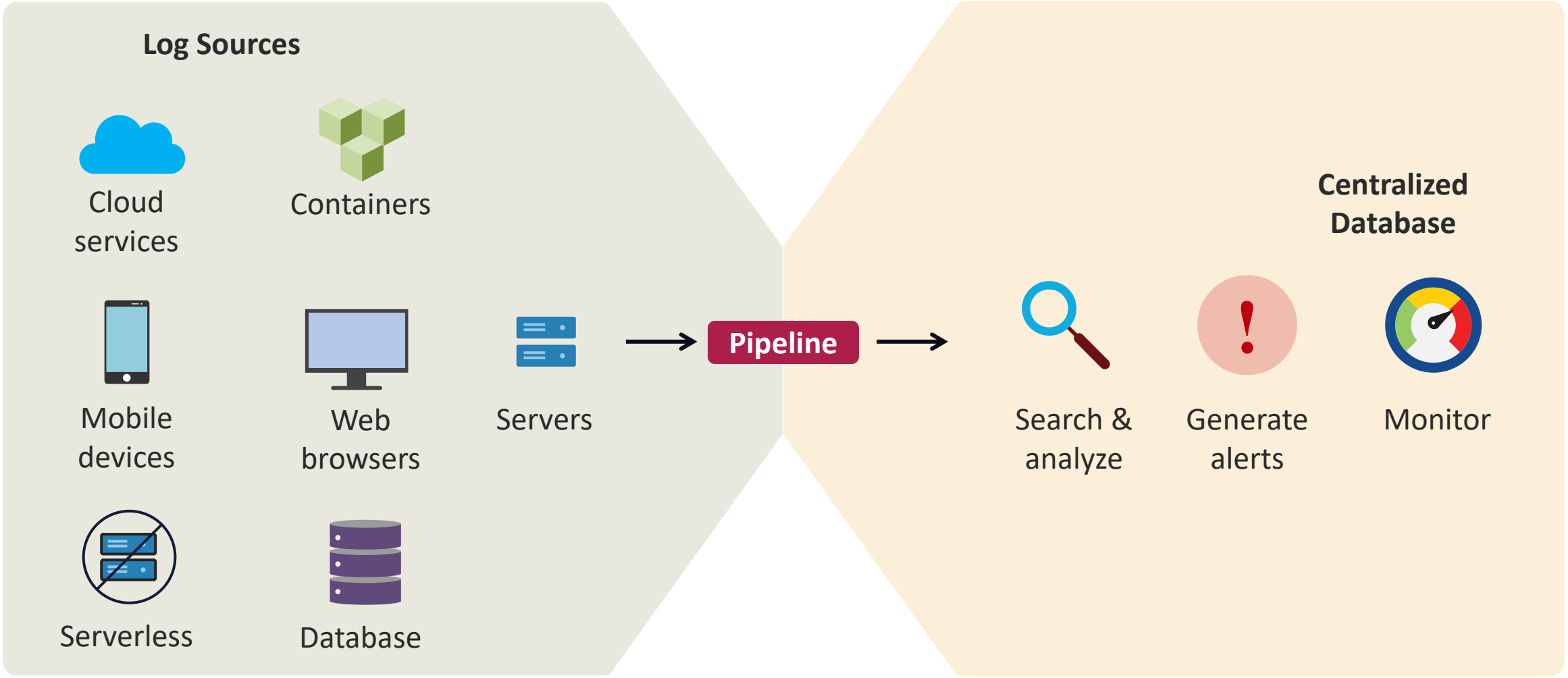
- Log aggregation is the process of accumulating, categorizing, standardizing, and consolidating log data from across an IT infrastructure to enable and enhance streamlined log analysis
- Without log aggregation, administrators and engineers would have to manually organize, deduplicate, and search through log data from various sources to generate meaningful metrics and information



LOG AGGREGATION GOALS

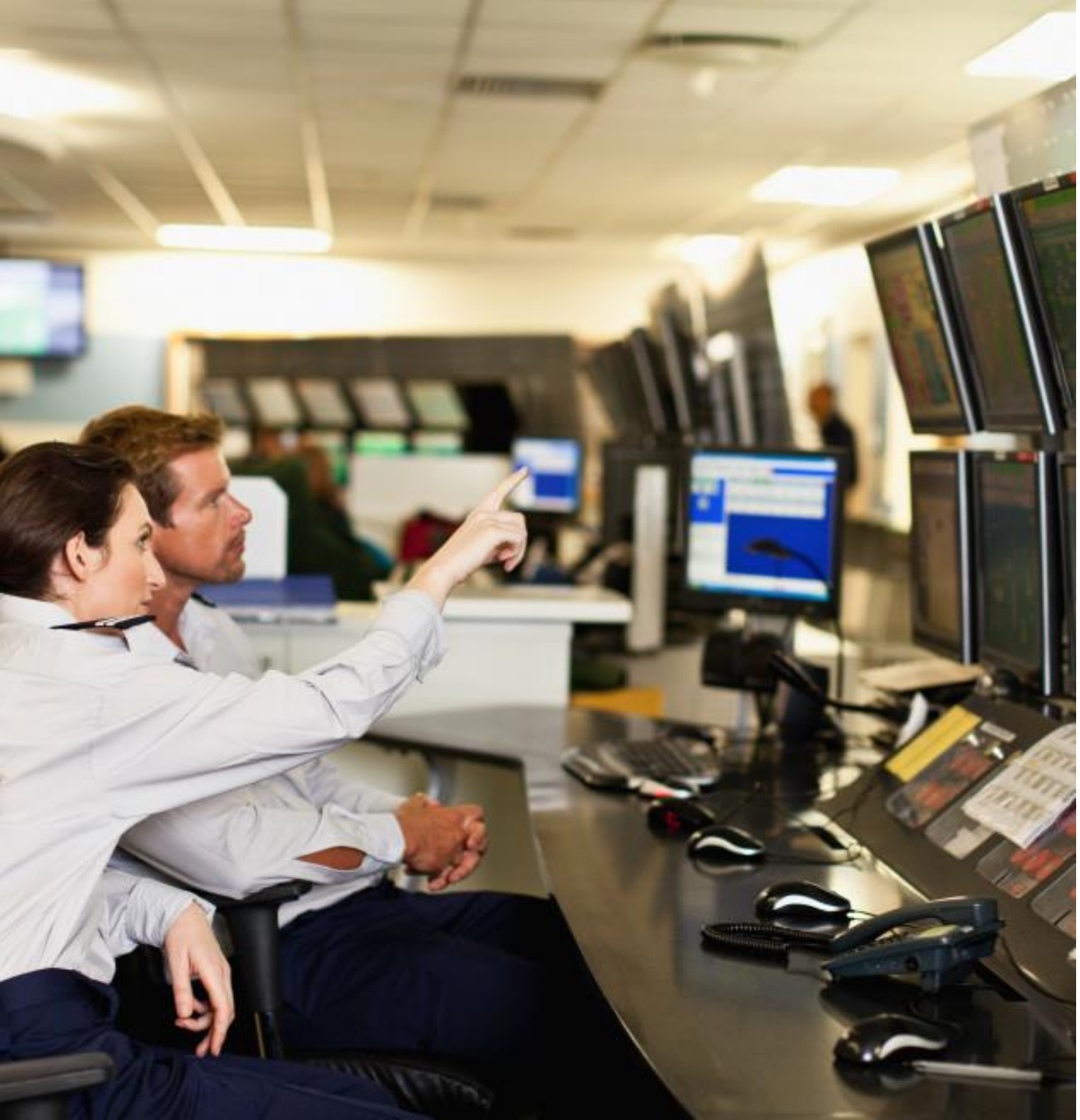
- Replicating log files to a centralized location
- Collecting Syslog, auditd, and other traps
- Supporting automated pipelines and workflows
- Parsing key-value pairs
- Performing more complex transformations such as multiline log aggregation, tokenization, scrubbing, or masking sensitive data

LOG AGGREGATION PIPELINES



ALERTING

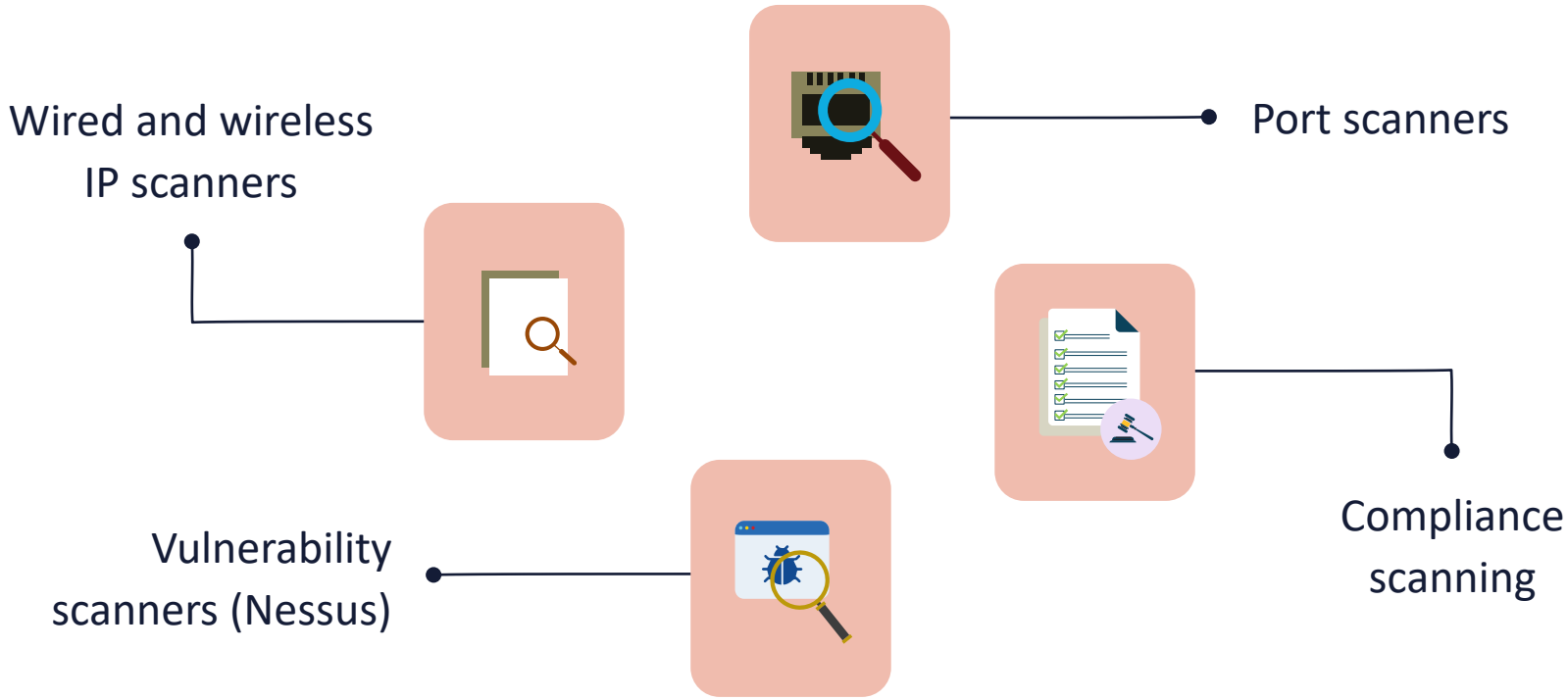
- An alerting system delivers metrics and alarms from various tools and systems to admins and security operators for informational/event notifications, incident management, and optimization of the wider ecosystem
- These platforms help to ensure that event responses are quick and efficient so that the odds of overlooked actions are reduced
- As systems grow larger and more complex, alerting systems are more automated and orchestrated with specialty platforms and services (server-based and serverless)



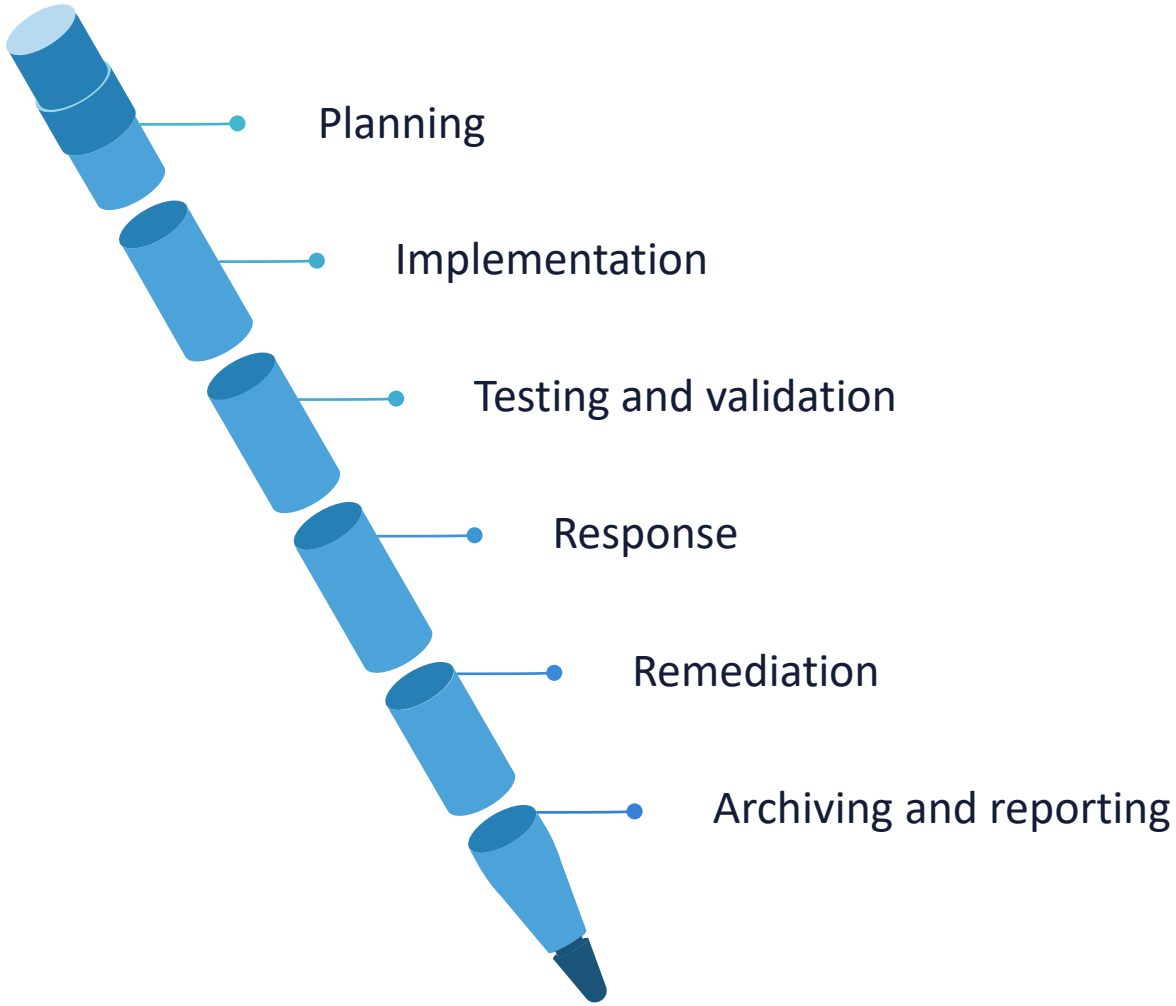
ALERTING BEST PRACTICES

- Choose quality over quantity
- Produce actionable results
- Consider broadcasting for mass notifications
- Have a well-designed service desk and escalation processes
- Prioritize alerts sent by people
- Automate whenever feasible

SCANNING TOOLS



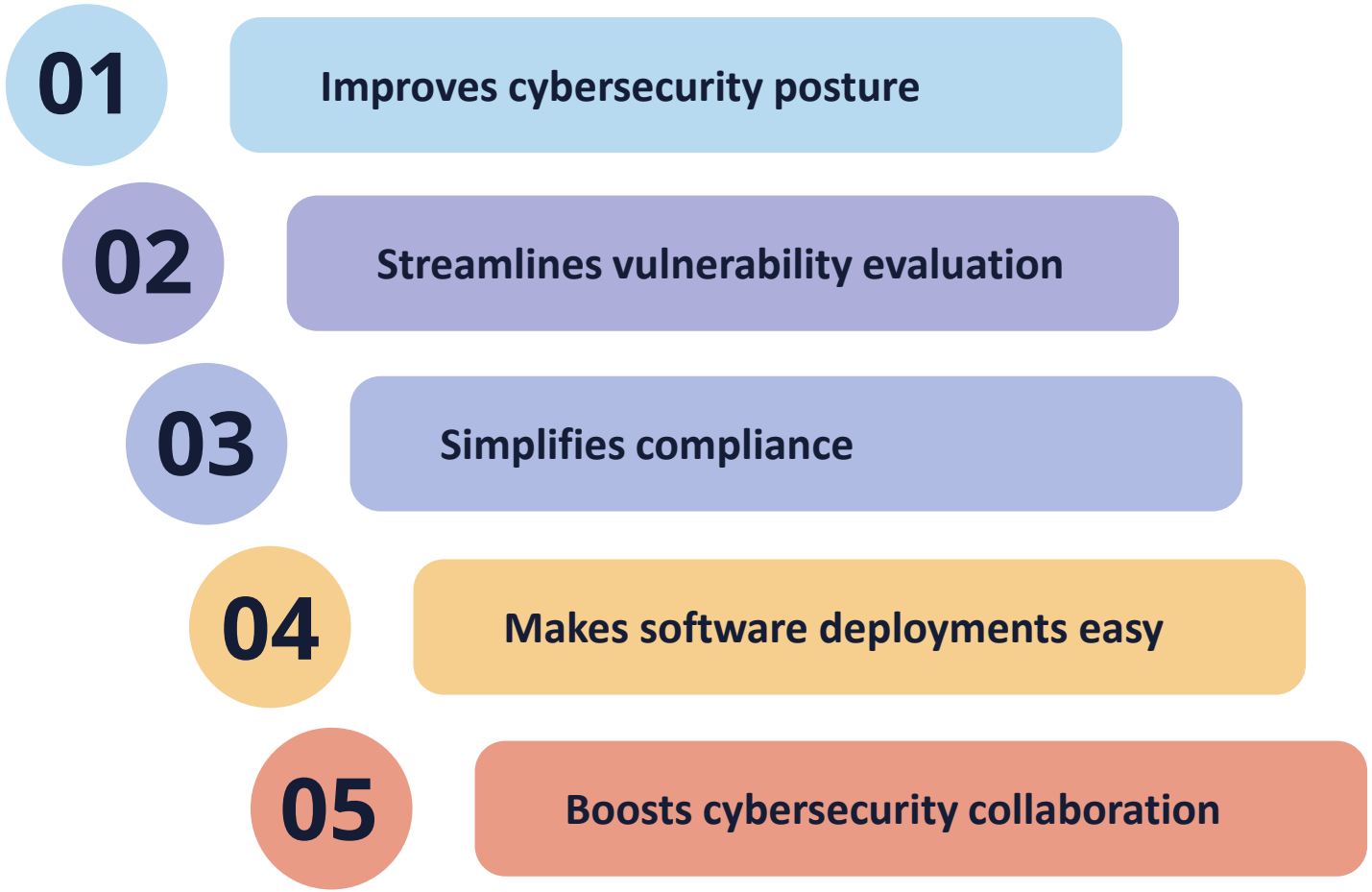
SCANNING AND ALERTING LIFE CYCLE



SECURITY CONTENT AUTOMATION PROTOCOL (SCAP)

According to NIST: "The Security Content Automation Protocol (SCAP) is a synthesis of interoperable specifications derived from community ideas. Community participation is a great strength for SCAP, because the security automation community ensures the broadest possible range of use cases is reflected in SCAP functionality."

IMPORTANCE OF SCAP



SCAP SPECIFICATIONS

- **Asset Identification** plays an important role in an organization's ability to quickly correlate different sets of information about assets
- The **Asset Reporting Format (ARF)** is a data model to express the transport format of information about assets, and the relationships between assets and reports

SCAP

SCAP SPECIFICATIONS

- **Common Platform Enumeration (CPE)** is a standardized method of describing and identifying classes of applications, operating systems, and hardware devices present among an enterprise's computing assets
- **Open Vulnerability Assessment Language (OVAL)** is an information security community effort to standardize how to assess and report upon the machine state of computer systems
- The **Open Checklist Interactive Language (OCIL)** defines a framework for expressing a set of questions to be presented to a user and corresponding procedures to interpret responses to these questions

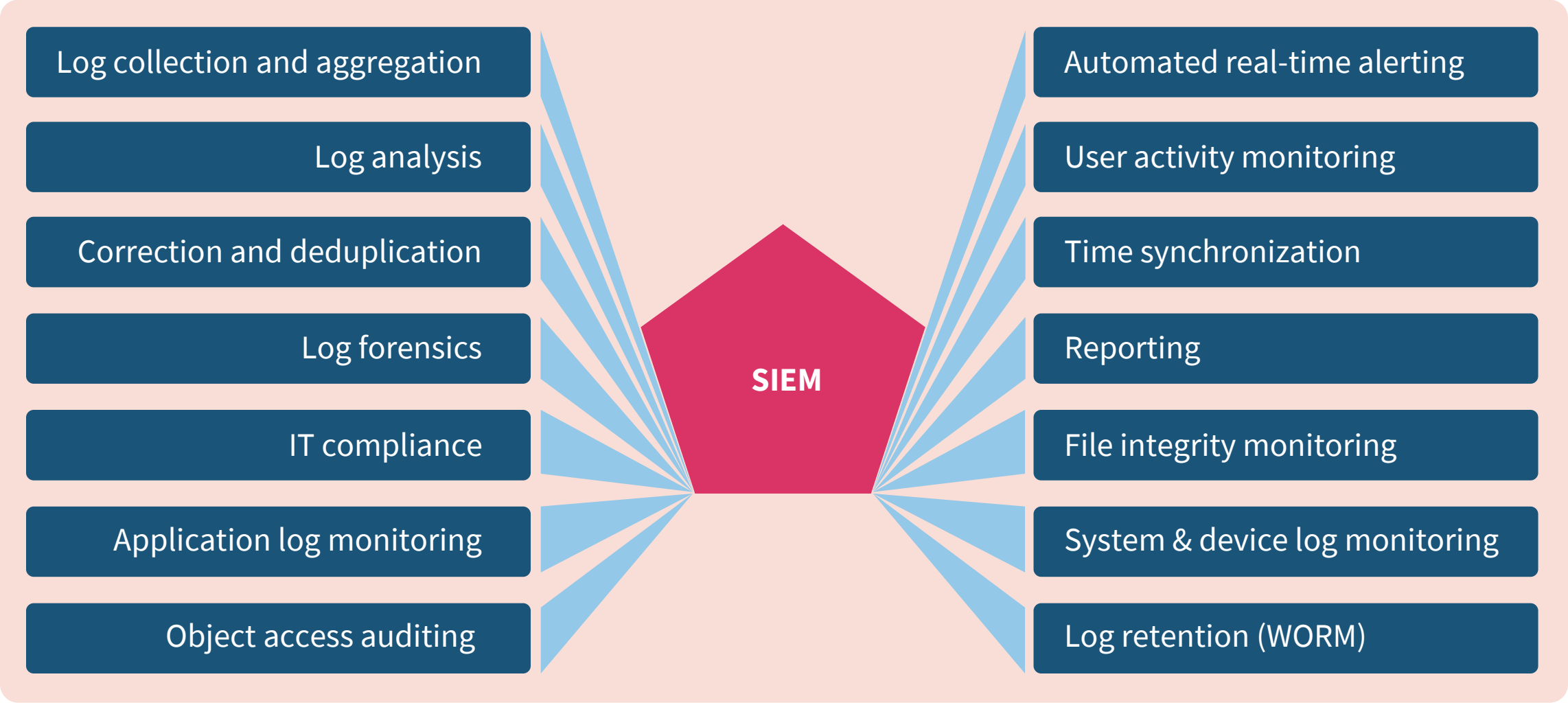
SCAP SPECIFICATIONS

- **Trust Model for Security Automation Data (TMSAD)** describes a common trust model that can be applied to specifications within the security automation domain, such as SCAP
- The **Extensible Configuration Checklist Description Format (XCCDF)** is a specification language for writing security checklists, benchmarks, and related kinds of documents
- **Software Identification (SWID) Tagging** allows for the proper management of software inventories of managed devices in support of higher-level business, information technology, and cybersecurity functions

SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

- Security information and event management is a solution that helps enterprises detect, analyze, and respond to security threats before they affect business operations
- SIEM is a combination of security information management (SIM) and security event management (SEM) into a unified security management system
- SIEM technology gathers event log data from a range of sources and recognizes activity that diverges from the norm in real-time

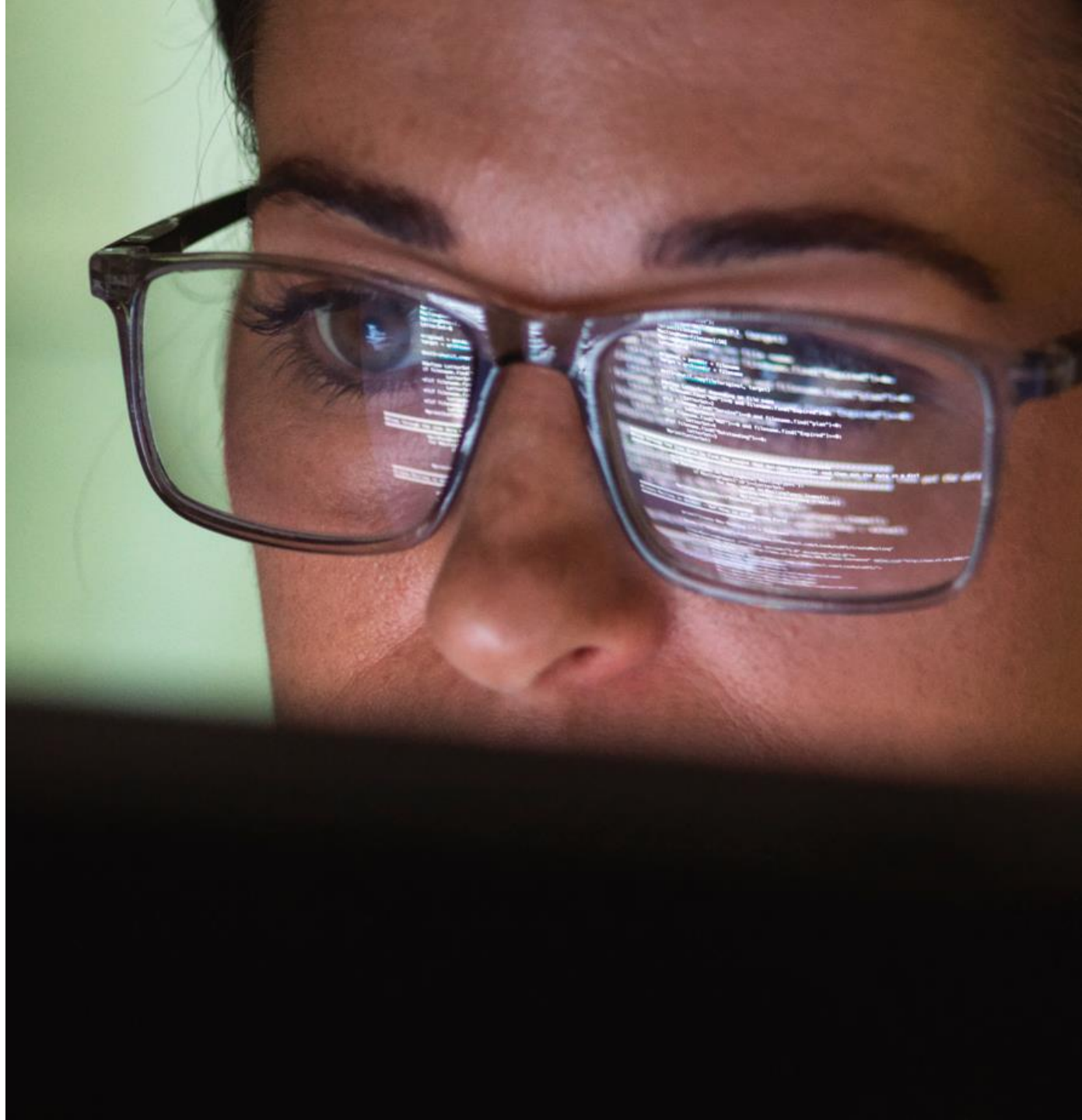
SIEM

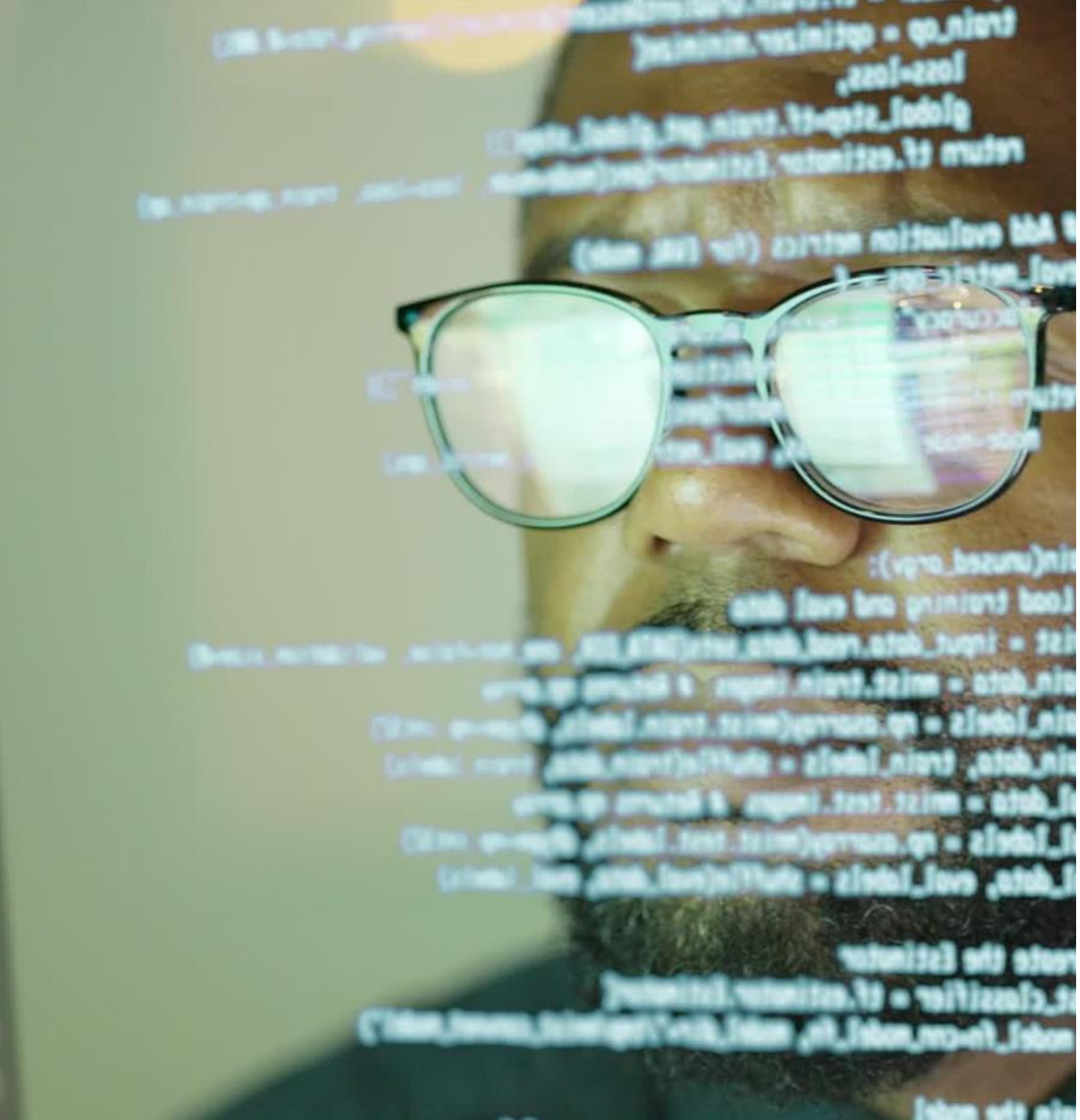

Log collection and aggregation
Log analysis
Correction and deduplication
Log forensics
IT compliance
Application log monitoring
Object access auditing
SIEM
Automated real-time alerting
User activity monitoring
Time synchronization
Reporting
File integrity monitoring
System & device log monitoring
Log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

BENEFITS OF SIEM SYSTEMS

SECURITY ORCHESTRATION AND AUTOMATION AND RESPONSE (SOAR)

- Security orchestration, automation, and response is an assortment of software services and tools that allow organizations to simplify and aggregate security operations in three core areas
  - Threat and vulnerability management
  - Incident response
  - Security operations automation

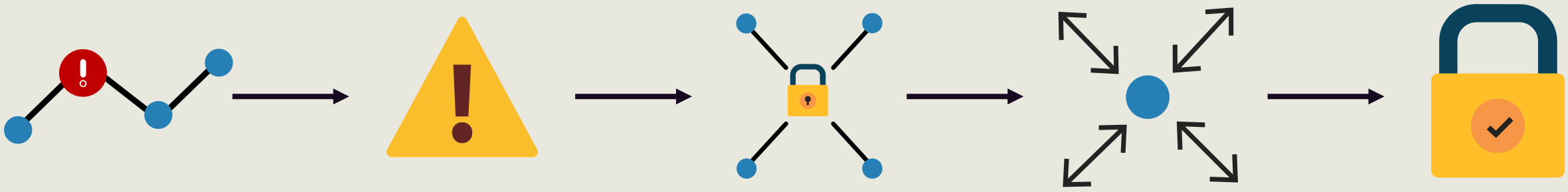




SECURITY ORCHESTRATION AND AUTOMATION AND RESPONSE

- 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



Threat detection

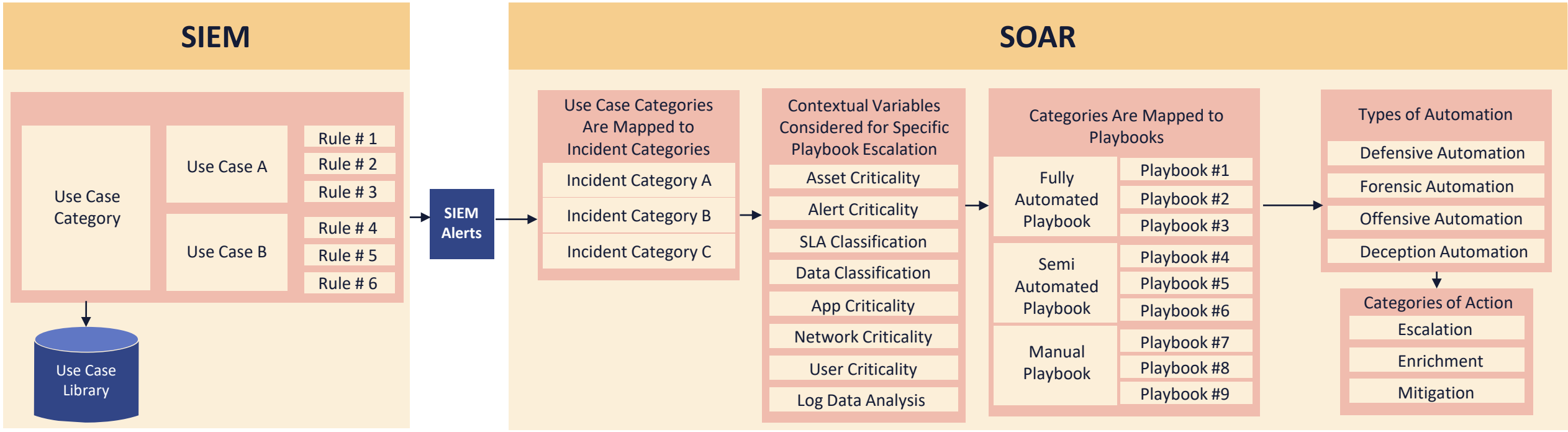
Notification

Investigation

Response

Resolution

SIEM + SOAR


SIEM
Use Case Category
Use Case A
Use Case B
Rule # 1
Rule # 2
Rule # 3
Rule # 4
Rule # 5
Rule # 6
Use Case Library
SIEM Alerts
SOAR
Use Case Categories Are Mapped to Incident Categories
Incident Category A
Incident Category B
Incident Category C
Contextual Variables Considered for Specific Playbook Escalation
Asset Criticality
Alert Criticality
SLA Classification
Data Classification
App Criticality
Network Criticality
User Criticality
Log Data Analysis
Categories Are Mapped to Playbooks
Fully Automated Playbook
Semi Automated Playbook
Manual Playbook
Playbook #1
Playbook #2
Playbook #3
Playbook #4
Playbook #5
Playbook #6
Playbook #7
Playbook #8
Playbook #9
Types of Automation
Defensive Automation
Forensic Automation
Offensive Automation
Deception Automation
Categories of Action
Escalation
Enrichment
Mitigation

ANTIVIRUS SYSTEMS

- Antivirus software is intended to protect computers and mobile devices from exploits, malware, crackers, and cybercriminals
- The systems examine data on hard drives, memory, and incoming packets from the Internet (websites, email messages, attachments, and applications) to recognize, block, and offer ongoing protection against malicious software, infected links, and other threats and suspicious activity

ANTIVIRUS SYSTEMS

- Antivirus software functions by regularly scanning all devices to discover and block known worms and viruses as well as new and emerging malware variants
- If a device gets infected, antivirus software will also quarantine and eradicate it
- Many systems employ a heuristic detection method to examine code for suspicious architecture and behavior rather than a specific static signature

ANTIVIRUS SYSTEMS

- To offer the best possible protection, these systems use several forms of detection:
  - Signature detection
  - Heuristic detection of files
  - Multicriteria analysis (MCA) – uses the data from other detection methods to flag a file as possibly dangerous
  - Sandbox and cloud analysis
  - Intrusion prevention via host intrusion prevention system (HIPS)
  - Anti-spam
  - Ransomware protection

ANTIVIRUS SYSTEMS FEATURES

Signature detection to look for specific code from known viruses

Heuristic detection to find suspicious architecture and behavior in code

Cloud and sandbox analysis to run suspicious programs inside a contained and secure system to see what they do

HIPS to bridge firewalls and other security systems for added protection

DATA LOSS PREVENTION (DLP)

- Data loss prevention is a security initiative that recognizes and mitigates unsafe or unauthorized sharing, transfer, or use of sensitive data such as personally identifiable information (PII) and protected health information (PHI)
- DLP engines and services can help organizations with monitoring and protection of sensitive information across on-premises systems, cloud-based locations, and endpoint devices
- It also assists with compliance for regulations such as the Health Insurance Portability and Accountability Act (HIPAA) and General Data Protection Regulation (GDPR)

DATA LOSS PREVENTION

Data

- Trade secrets
- Account numbers
- Social security numbers
- Intellectual property
- Personal health records

Can leak

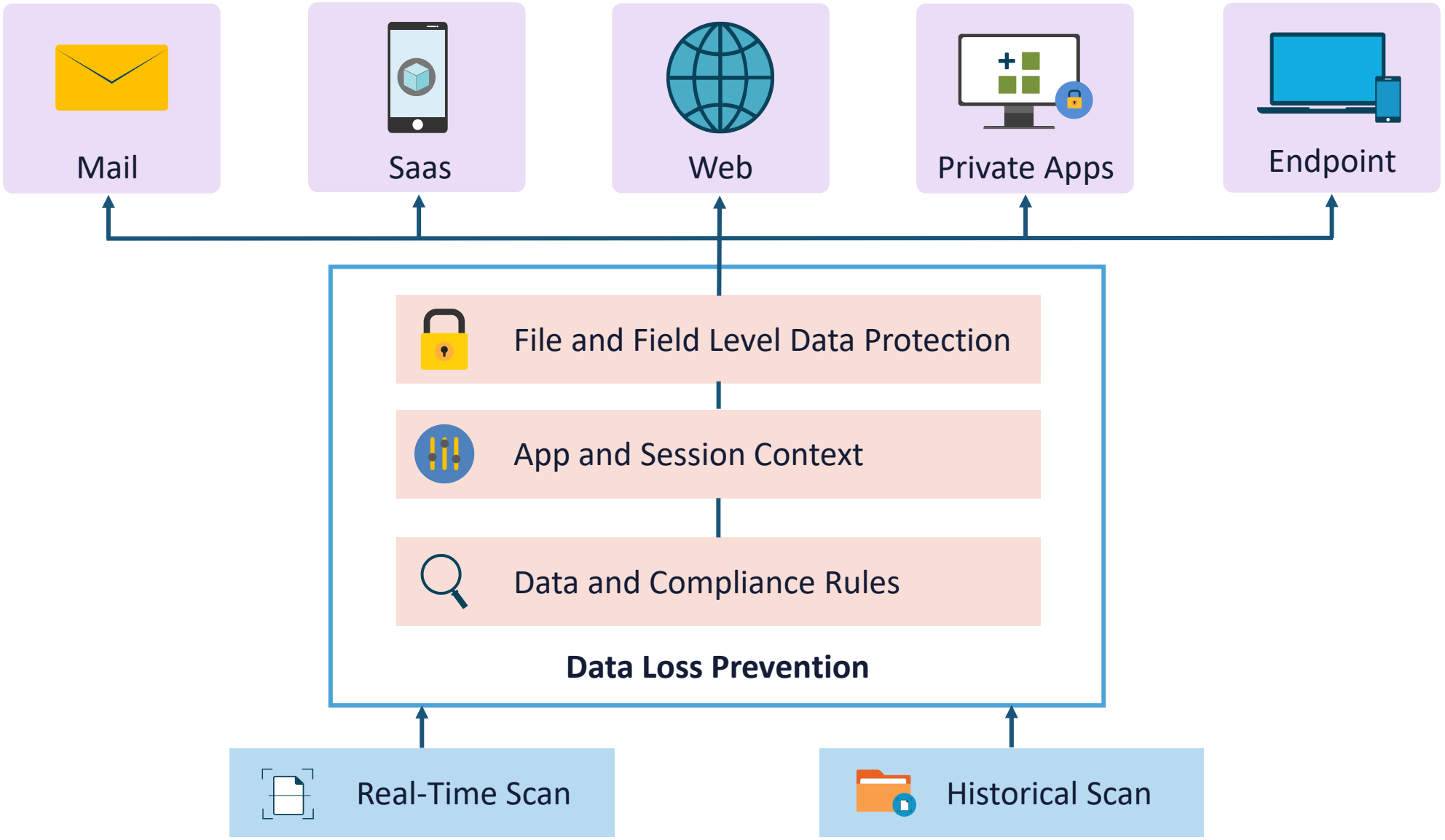
- Stored on network or shared drives
- Copied on external removable media devices
- Transmitted electronically: email, instant message, online, etc.

To an outsider

- Competitors
- Regulators
- Unauthorized internal users
- Press or media

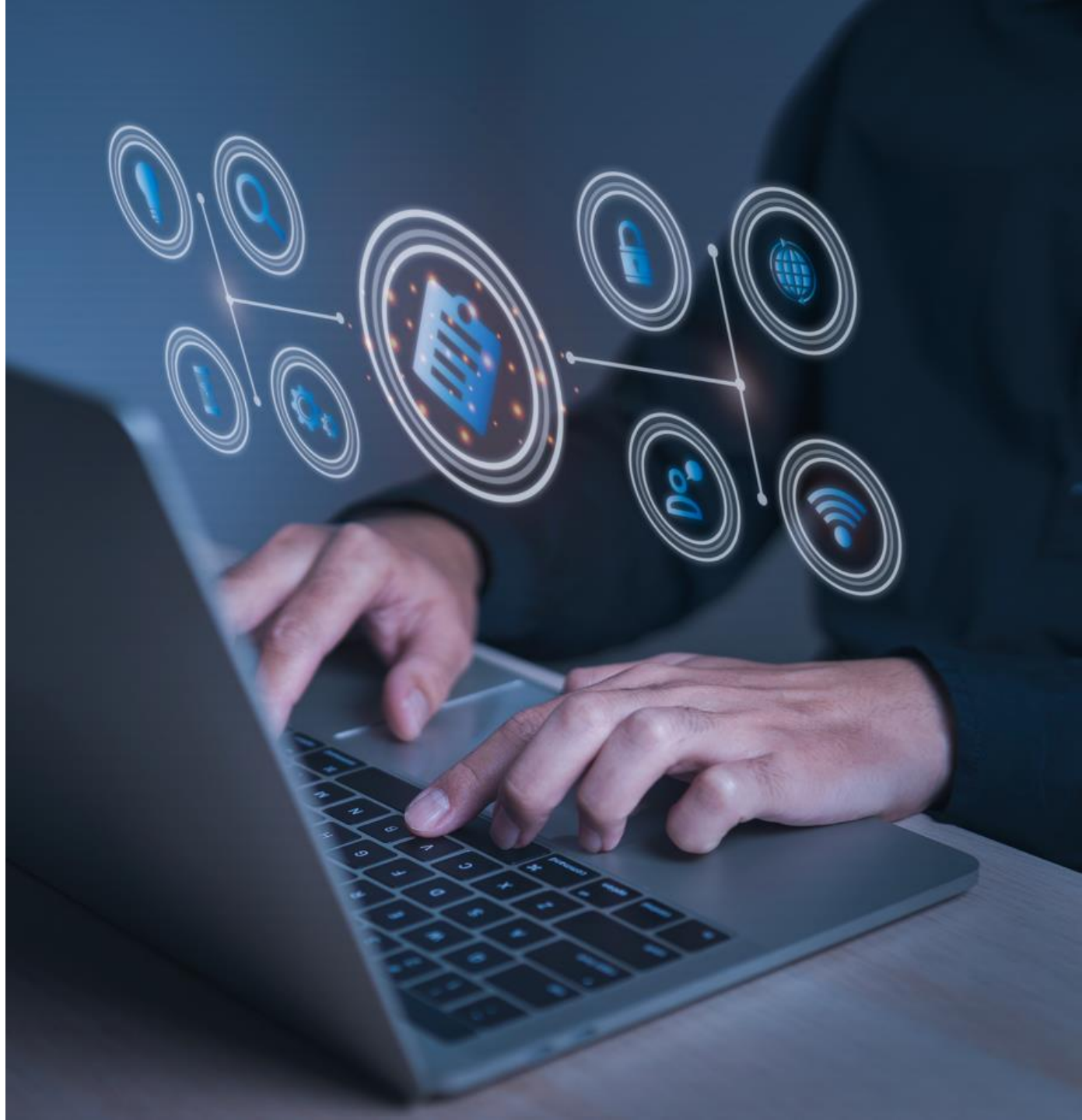
Resulting in a breach

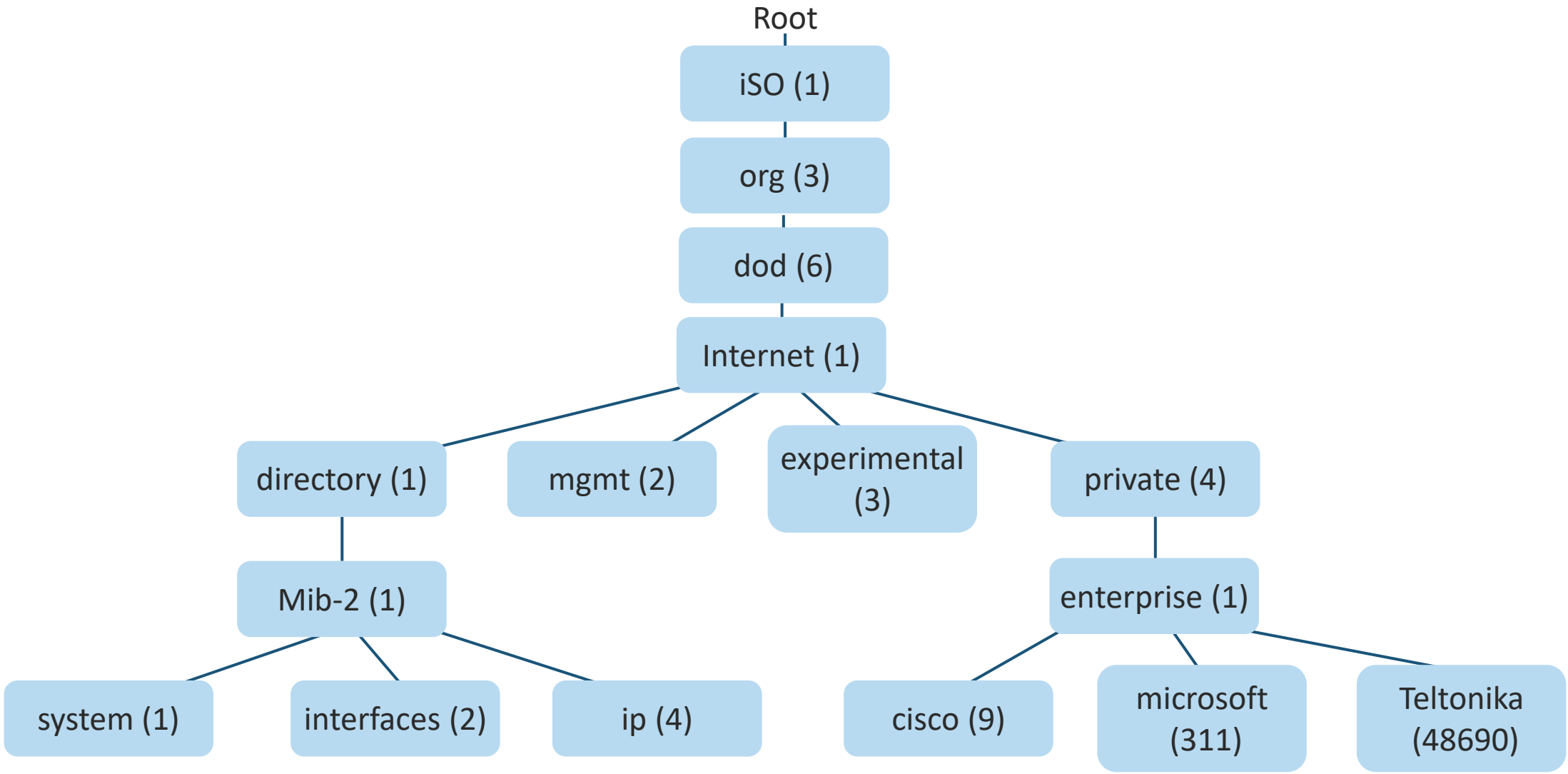
- Company defamation
- Monetary expense for each record lost
- Legal liabilities
- Loss of assets
- Breach of customer trust
- Close of the business


Mail
Saas
Web
Private Apps
Endpoint
File and Field Level Data Protection
App and Session Context
Data and Compliance Rules
Data Loss Prevention
Real-Time Scan
Historical Scan

SIMPLE NETWORK MANAGEMENT PROTOCOL

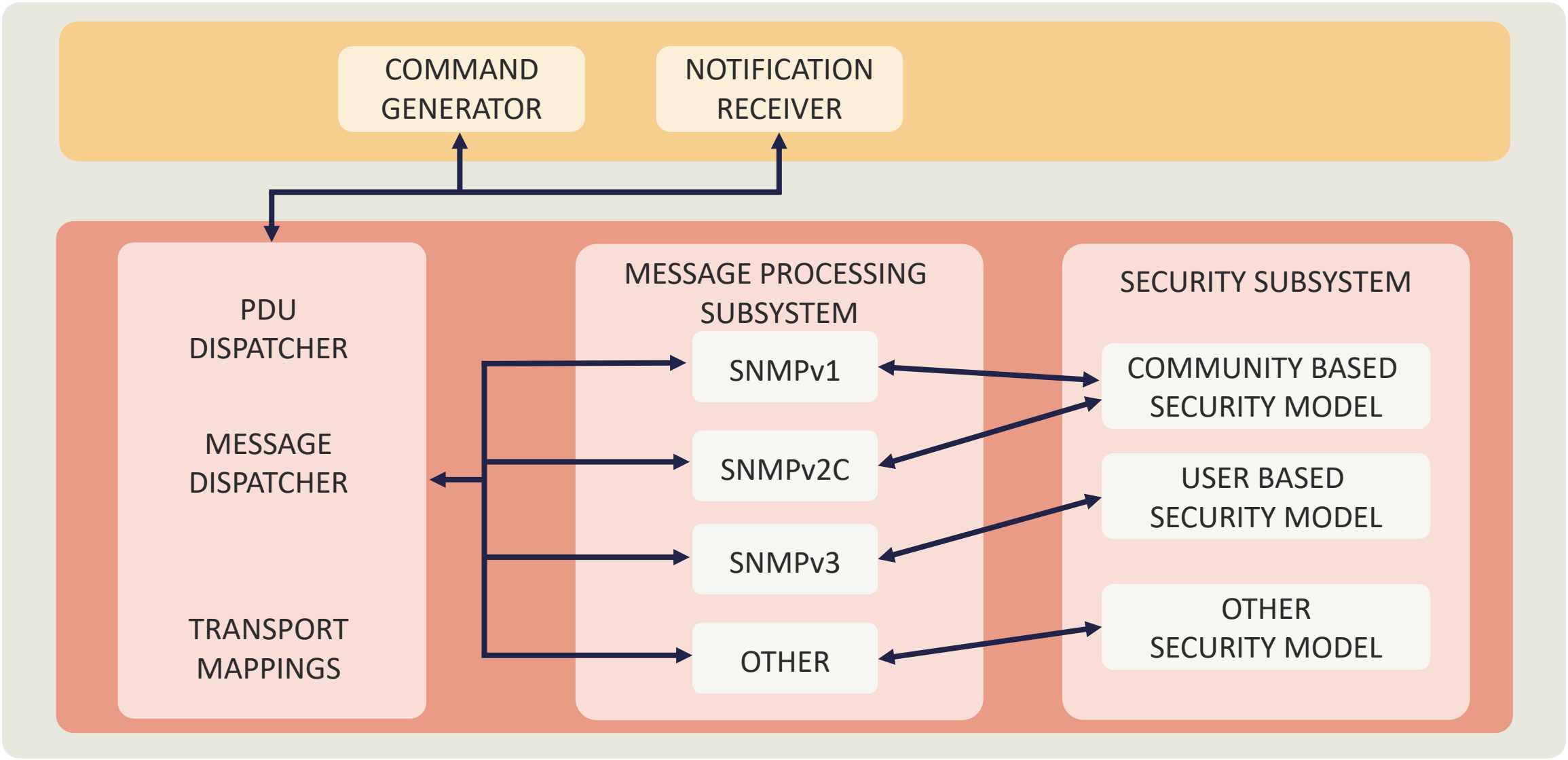
- Simple Network Management Protocol is a powerful protocol and toolset that facilitates the sharing of information among various devices on a network, regardless of their hardware or software
- Although there are many emerging replacements for SNMP, it is still widely deployed in enterprises globally
- SNMP uses a basic client-server architecture using:
  - **Managers** collect and process information about devices on the network
  - Clients, called **agents**, are any type of device or device component connected to the network





OID Tree Example

SNMP V3 ARCHITECTURE



SNMP VERSION 2C VS. SNMP VERSION 3

	SNMPv2	SNMPv3
Primary standards	RFC- 1901	RFC- 3412, RFC- 3414, RFC- 3415, RFC- 3417,
Allowed operations	Get, GetNext, Set, Trap, GetBulk, Inform, Response	Get, GetNext, Set, Trap, GetBulk, Inform, Response with PDU message format
Authentication	Community based	User and group based
Plain text community strings	Yes	No
Data encryption	None	DES/SHA/MDS/AES
Device identification	Request/response protocol	EngineID uniquely identifies each SNMP entity
MIB	Defines general framework for definition and construction of MIB	Configures permissions based on user for differing levels of MIB access
Default/known passwords	Yes	No
Data tampering protection	No	Yes
Eavesdropping protection	No	Yes
Unauthorized access protection	Limited based on locally defined ACLs	Yes

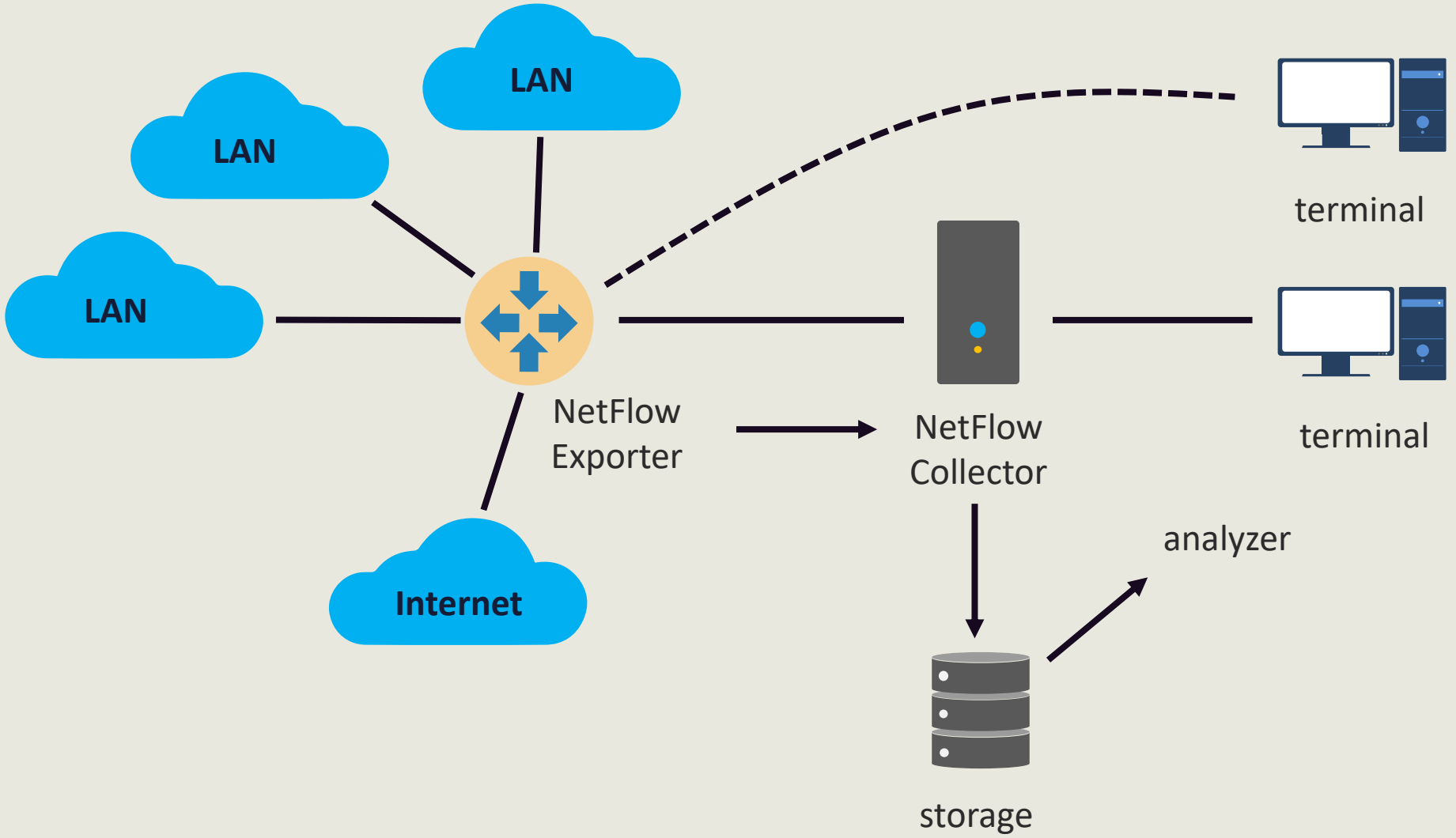
NETFLOW

- NetFlow is a network monitoring protocol, developed by Cisco, invented to capture metrics about the volume and types of traffic traversing a network device
- Technically, a flow is defined by its 5-tuple, a collection of five data points:
  - The source and destination IP addresses exchange information
  - The source and destination ports, if any (ICMP, for example, doesn't use ports)
  - The protocol

NETFLOW 9

- By collecting and analyzing this flow data, engineers can learn details about how the network is being used for troubleshooting network issues, identifying bandwidth hogs, and tracking which external IPs or countries one is exchanging data with
- NetFlow was first implemented in Cisco devices in 1995
- It has followed a curious evolution over the years, starting as a static protocol with a fixed set of statistics collected for all flows
- In version 9, the latest version from 2021, network professionals can choose which statistics to enable, and vendors can implement extensions (extensible) to attach proprietary metadata to flow entries

NETFLOW


LAN
LAN
LAN
LAN
Internet
NetFlow
Exporter
NetFlow
Collector
terminal
terminal
analyzer
storage

ENTERPRISE SECURITY CAPABILITIES

Objectives

- Explore firewalls, IDS, IPS, and web filters
- Examine operating system security and secure protocols
- Learn about DNS filtering, email security, and file integrity monitoring
- DLP solutions, network access control, and endpoint detection and response

DEMO: EXPLORING FIREWALL IMPLEMENTATIONS

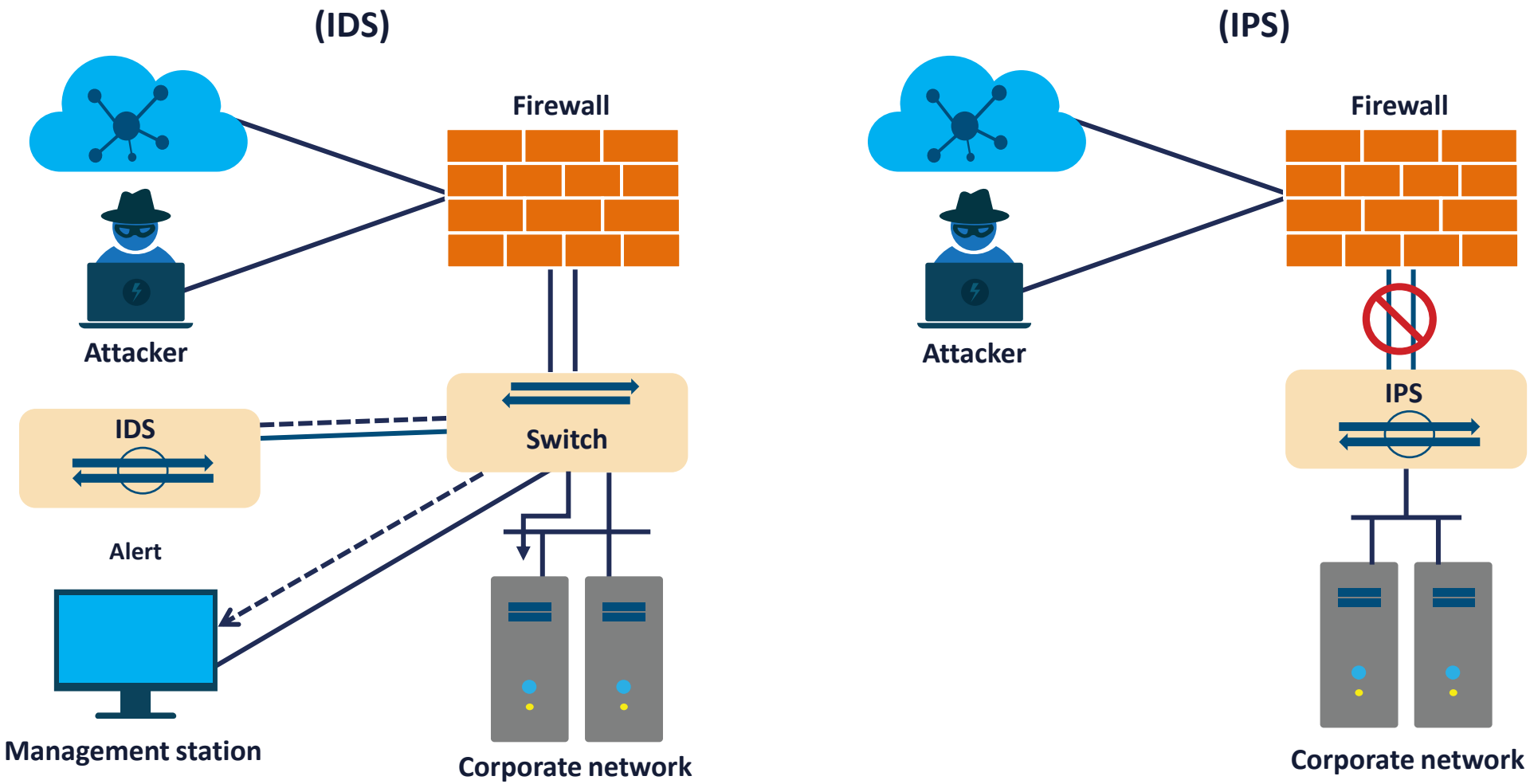
In this demo…

We will explore various firewall implementations like rule-based, access lists, ports and protocols, and screened subnets

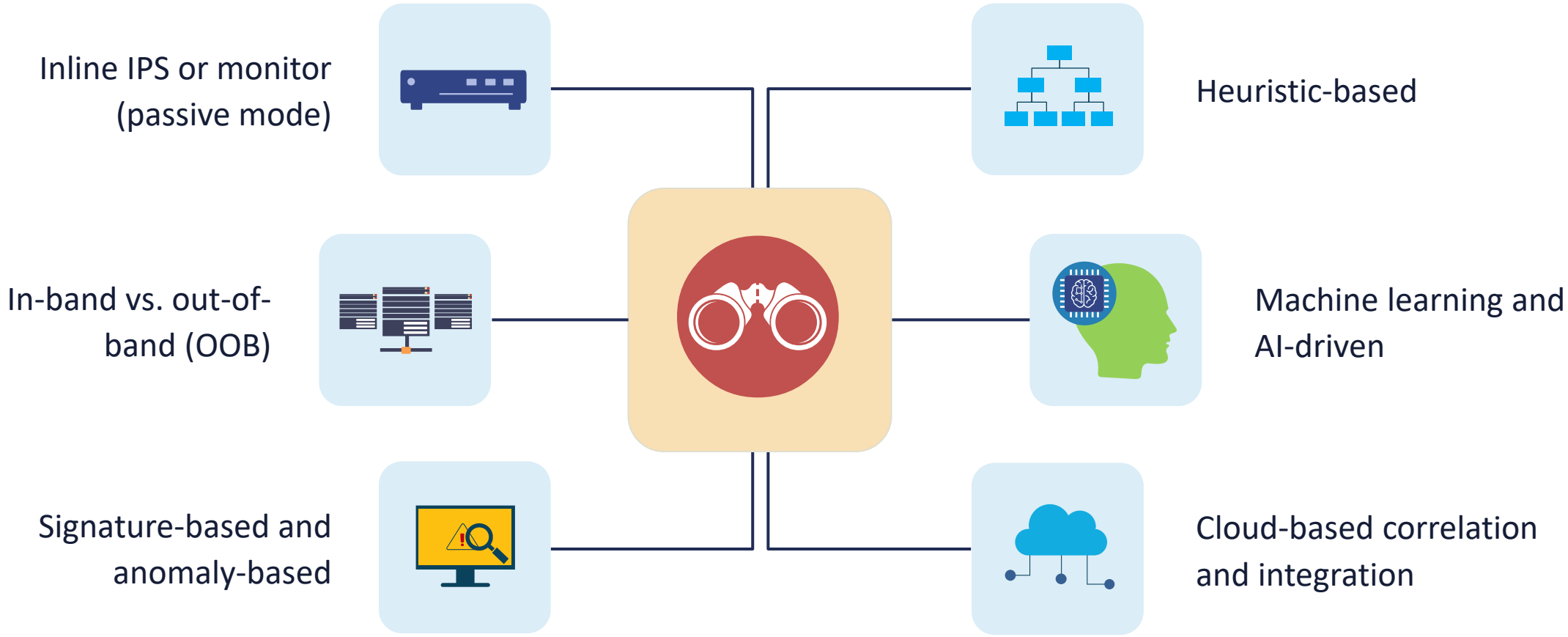
INTRUSION DETECTION AND PREVENTION SYSTEMS (IDS AND IPS)

- IDS and IPS is a combination of hardware and/or software to allow visibility and mitigation of existing exploits and malware on the network or individual hosts
- Snort IDS running on Unix machines was the original intrusion detection daemon
- Original services were highly static signature-based solutions with anomaly detection introduced in later models
- These have evolved into advanced next-generation artificial intelligence (AI)/machine learning (ML) solutions

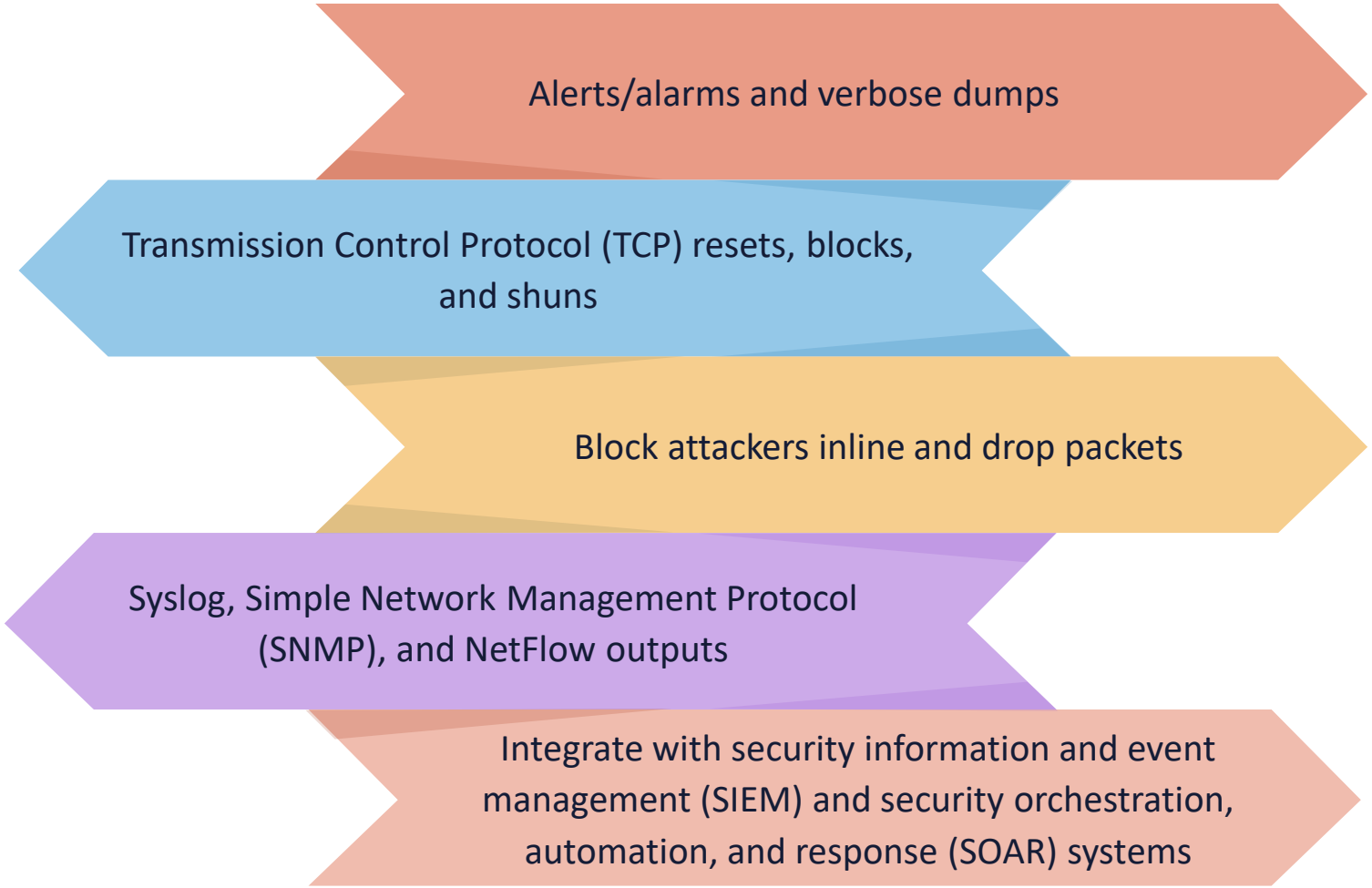
IDS VS. IPS


(IDS)
Firewall
Attacker
IDS
Switch
Alert
Management station
Corporate network
(IPS)
Firewall
Attacker
IPS
Corporate network

IPS CHARACTERISTICS



IPS ACTIONS


Alerts/alarms and verbose dumps
Transmission Control Protocol (TCP) resets, blocks, and shuns
Block attackers inline and drop packets
Syslog, Simple Network Management Protocol (SNMP), and NetFlow outputs
Integrate with security information and event management (SIEM) and security orchestration, automation, and response (SOAR) systems

IPS TUNING

True positive

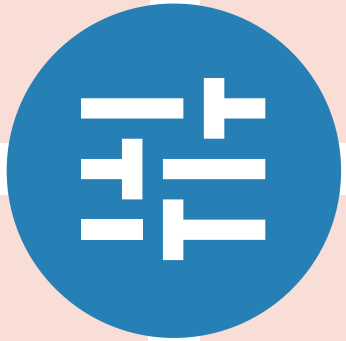
True (accurate) + positive

(action taken)

False positive

False (error) + positive

(action taken)



True negative

True (accurate) + negative

(action not taken)

False negative

False (error) + negative

(action not taken)

WEB FILTERS

- A web filter is an application layer gateway server or service (physical or virtual dedicated to analysis and control of HTTP and HTTPS traffic
- Agent-based web filters require the deployment of lightweight software packages on network devices, whereas agentless filters can be instantly deployed in Random Access Memory (RAM) or persistently without any manual configuration
- Many filtering solutions are deployed on the customer premises equipment as a centralized proxy to process all web traffic from layer 3 through layer 7

WEB FILTERING

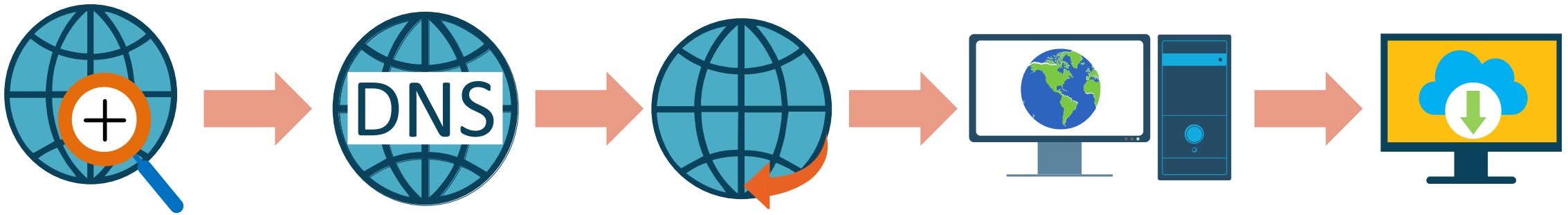
Search or go directly to a website

Domain name resolution

URL request

Web page returned

Upload or download files



Safe search

DNS filtering

URL filtering

Content categorization

File filtering

REPUTATION FILTERING

- Web reputation services accuracy is typically determined by the breadth, depth, and variety of the data being used
- The algorithms used to analyze the relationships between Internet objects and web reputations must be persistently trained by experienced human analysts and artificial intelligence tools
- With an accurate web reputation source fueling associated URL filters, firewall solutions, or other specialty appliances, one can produce a resilient, proactive cybersecurity posture

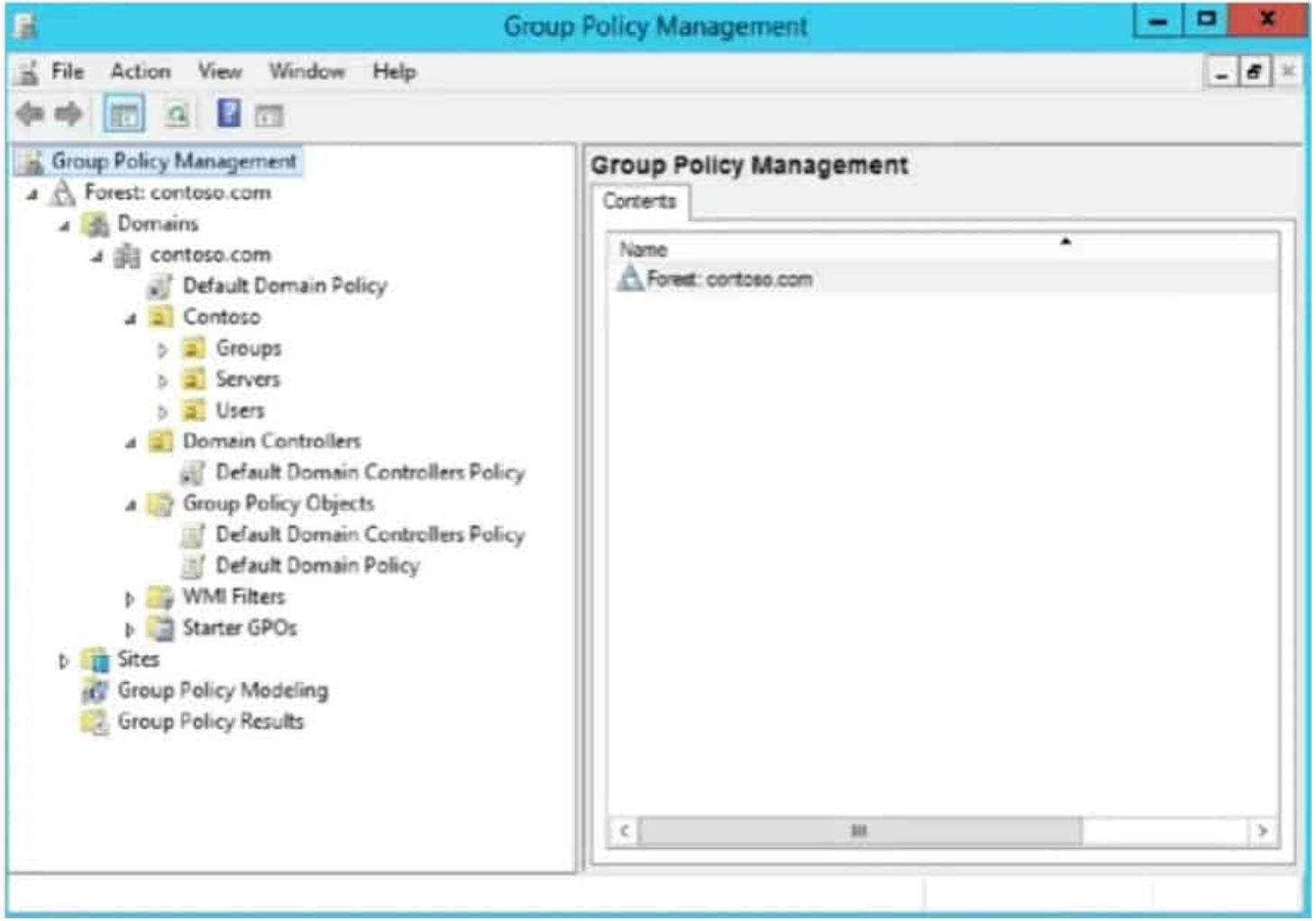
O/S SECURITY: GROUP POLICY

- Group Policy (GP) is a Microsoft Windows service that enabled IT administrators to centrally manage and configure the settings on Windows operating systems
- Group Policy can manage operating system settings, applications, browsers, and user settings
- GP is used in Active Directory (AD) environments with domain-joined computers as well as Microsoft Azure hybrid joined devices

O/S SECURITY: GROUP POLICY

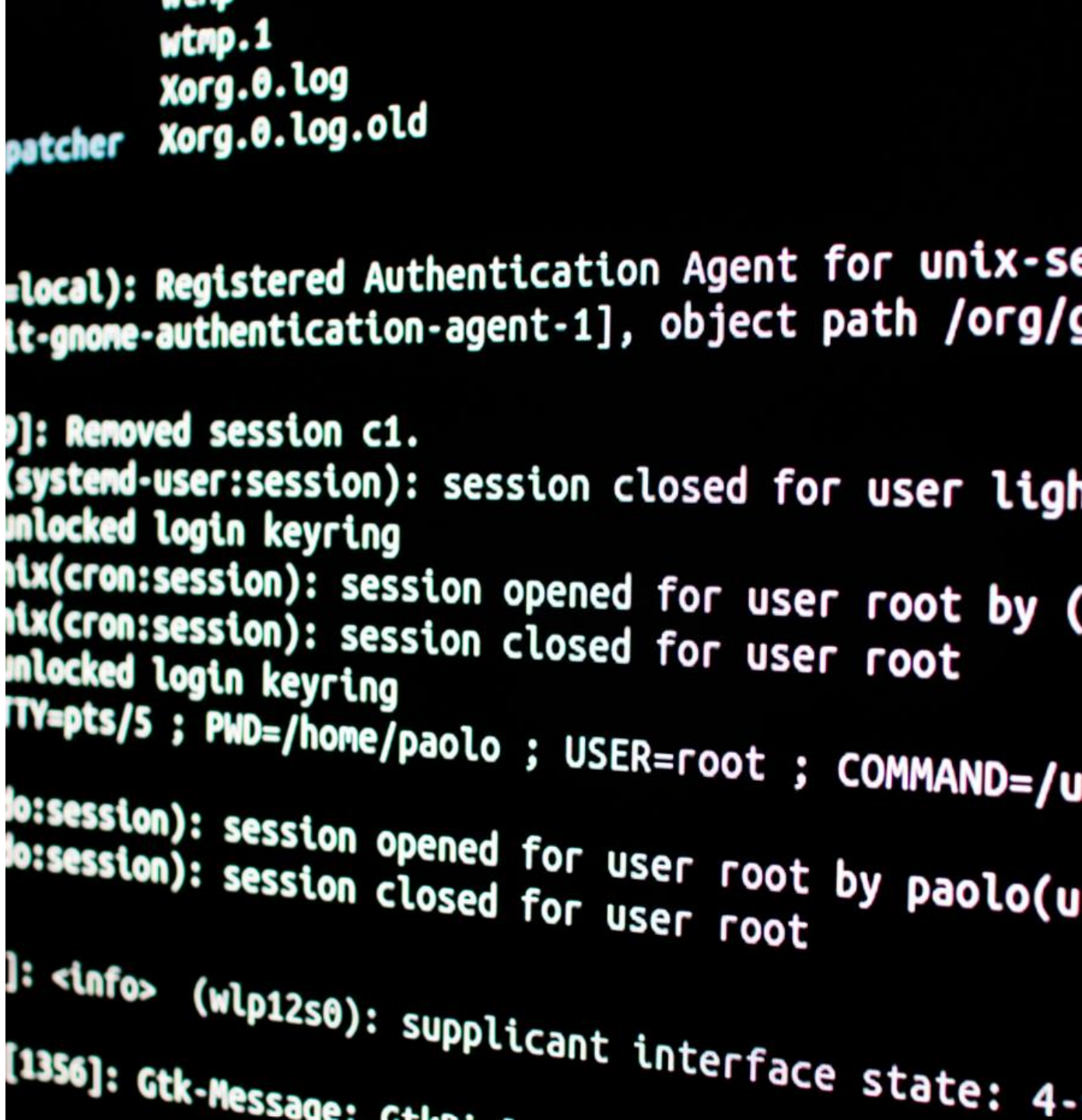
- Some Group Policy examples include:
  - Password Policy
  - Screen Lock
  - Power Settings
  - Map Network Drives
  - Install printers, software, desktop shortcuts, etc.
  - Software restrictions (blocking access to programs)
- Group Policy Objects (GPOs) are collections of policy settings that apply to the domain (or OU) to manage users, computers, or the entire domain

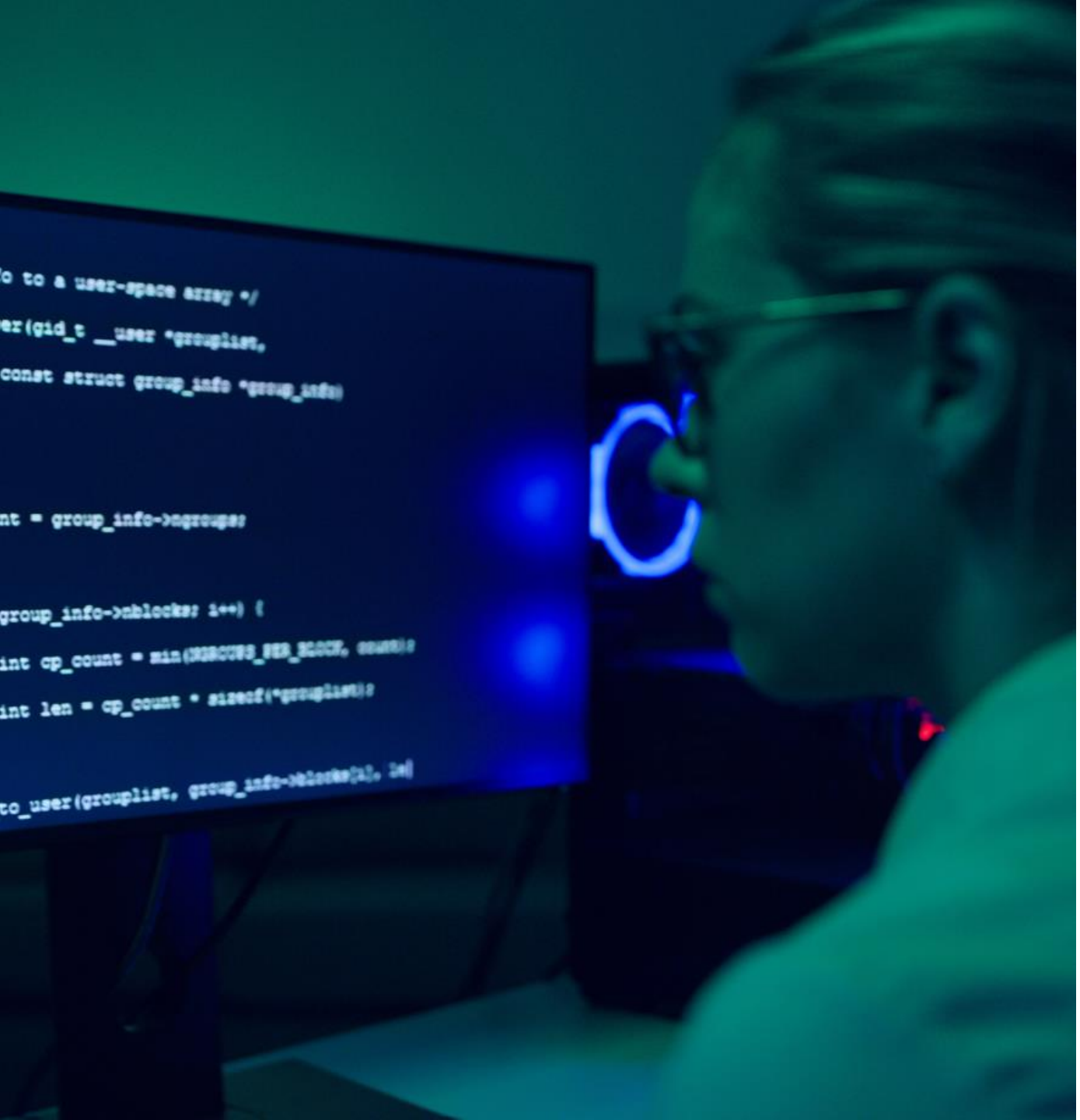
GROUP POLICY MANAGEMENT CONSOLE (GPMC)



O/S SECURITY: SECURITY ENHANCED LINUX

- Security Enhanced Linux (SELinux) is an access control system built into the Linux kernel
- It is used to enforce the resource policies that define what level of access users, programs, and services have on a system
- In its default enforcement mode, SELinux will deny and log any unauthorized attempts to access any resource
- This enforces the principle of least privilege, in that explicit permission must be given to a user or program to access files, directories, sockets, and other services

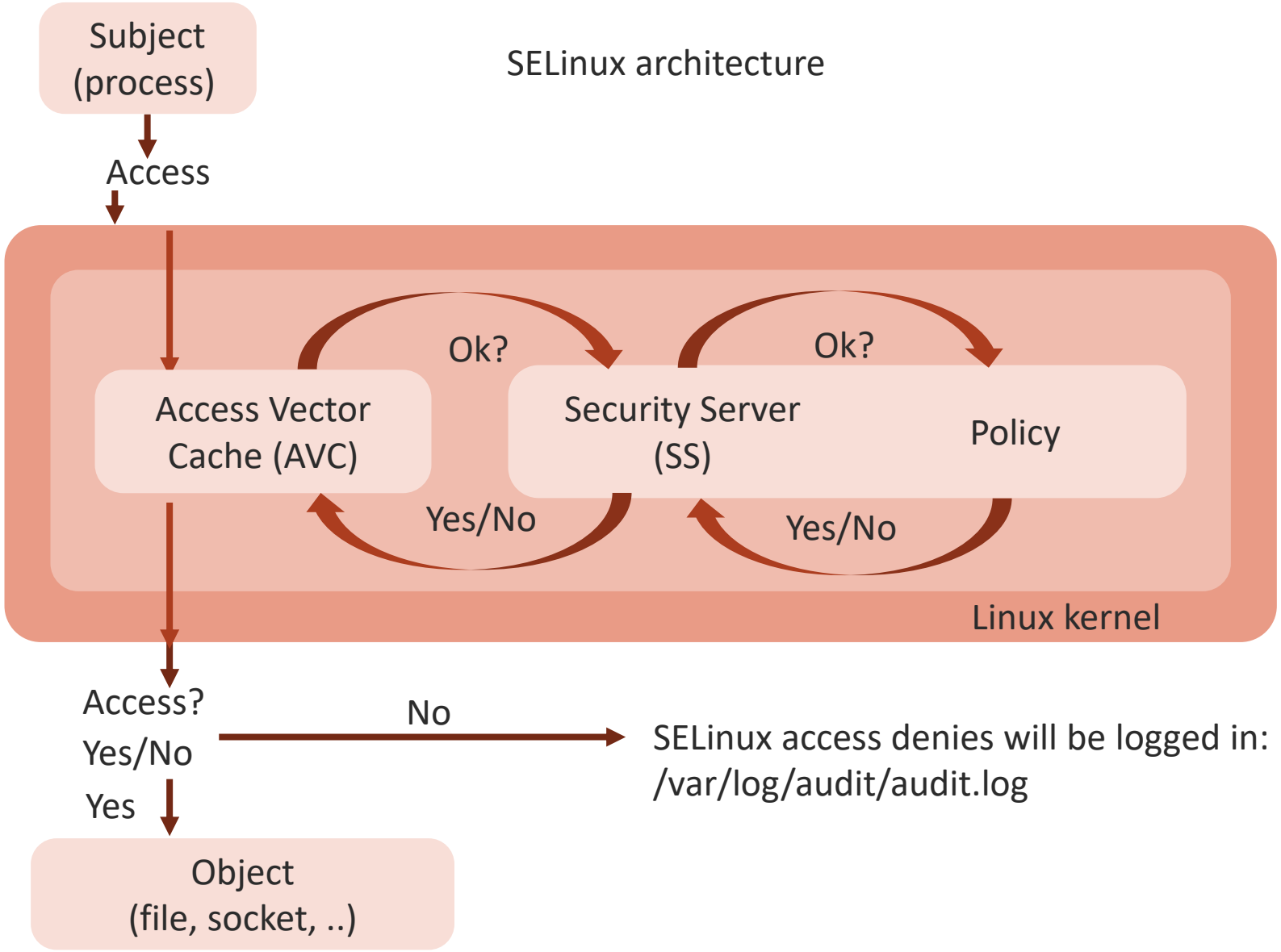




SELINUX

- There are several ways to configure SELinux to protect a system
- The most common are targeted policy or multi-level security (MLS)
  - Targeted policy is the default option and covers a range of processes, tasks, and services
  - MLS can be very complicated and is typically only used by government organizations
- The /etc/sysconfig/selinux file has a section that shows you whether SELinux is in permissive mode, enforcing mode, or disabled, and which policy is supposed to be loaded

SELINUX


Subject
(process)
SELinux architecture
Access
Ok?
Ok?
Access Vector
Cache (AVC)
Security Server
(SS)
Policy
Yes/No
Yes/No
Linux kernel
Access?
Yes/No
No
SELinux access denies will be logged in:
/var/log/audit/audit.log
Yes
Object
(file, socket, ..)

INTERNET PROTOCOLS ARE UNSECURE BY DESIGN

Number	Name	Description
7	Application	HTTP, FTP, SMTP, DNS, TELNET, LDAP, POP, IMAP
6	Presentation	ASCII, PNG, MPEG, AVI, MIDI
5	Session	SSL/TLS, SQL, RPC, NFS
4	Transport	TCP, UDP, SPX, AppleTalk
3	Network (or Internetwork)	IP, IPX, ICMP, ARP, BGP, OSPF
2	Link	PPP/SLIP, Ethernet, Frame Relay, ATM
1	Physical	Binary transmission, encoding, bit rates, voltages

SECURITY+ PORTS AND PROTOCOLS

Layer 7 Application	Port Number	Use
File Transfer Protocol (FTP)	20/21	Port 21 is the control, while port 20 is used to transfer files
Secure Shell (SSH)	22	Designed to transmit data through a remote connection
SSH File Transfer Protocol	22	A separate protocol from FTP (it is not compliant with FTP servers) that uses SSH to encrypt file transfers
TACACS+	49	Cisco proprietary protocol used for authentication, authorization, and accounting (AAA) services
Domain Name System (DNS)	53	Used to associate IP addresses with domain names
Dynamic Host Configuration Protocol (DHCP)	67/68	This network management protocol is used to assign local IP addresses to devices on a network. It is used to create multiple private IP addresses from one IPv4 address
Hypertext Transfer Protocol (HTTP)	80	Protocol used for websites and most Internet traffic

SECURITY+ PORTS AND PROTOCOLS

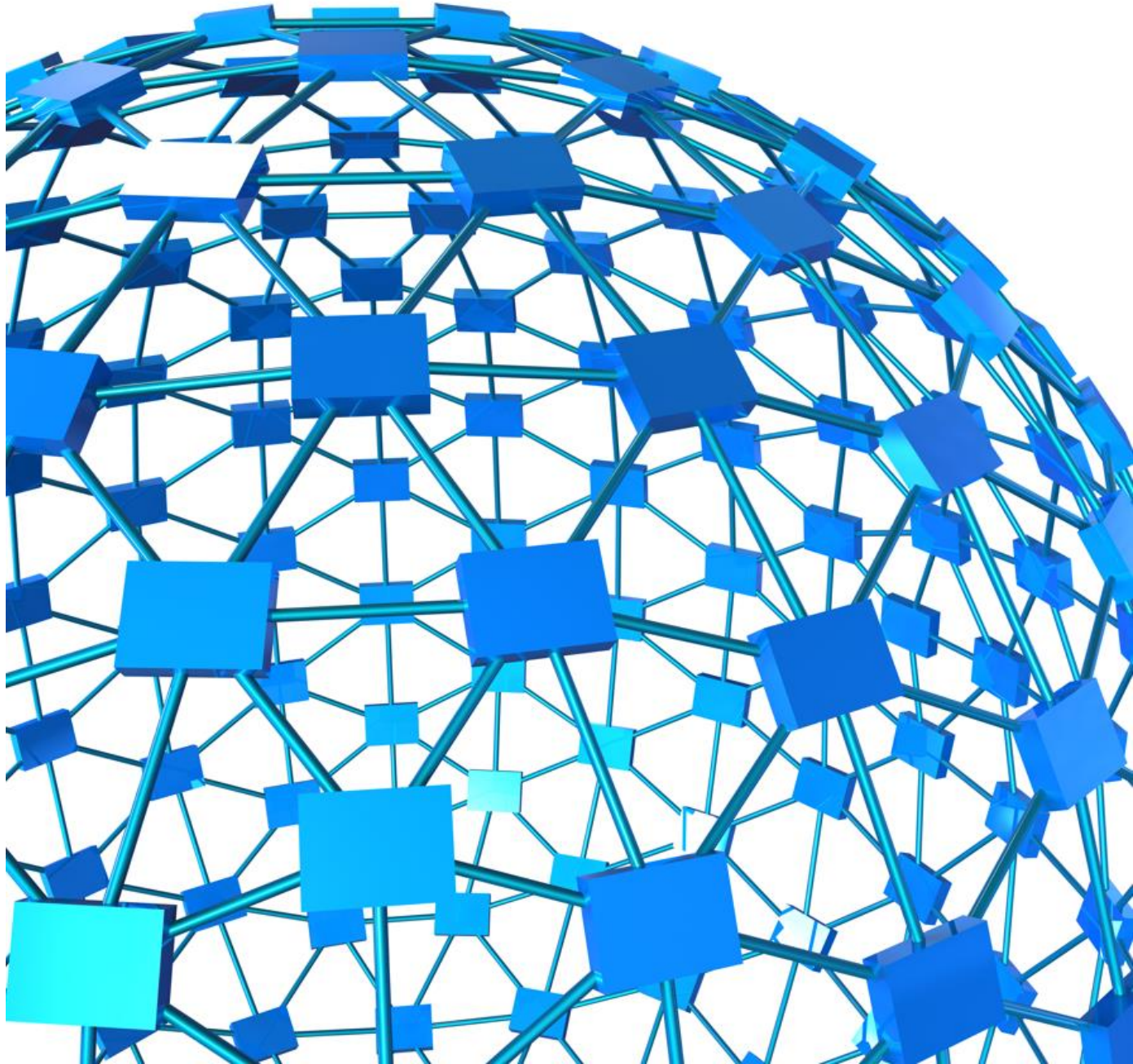
Kerberos	88	Network authentication protocol that allows for communication over a non-secure network
Post Office Protocol (POP)	110	Email protocol that allows email clients to communicate with email servers; POP providers only one-way communication
Internet Message Access Protocol (IMAP)	143, 993	Email protocol used by email clients to communicate with email servers; provides two-way communication unlike POP
Simple Network Management Protocol (SNMP)	161/162	Protocol used to monitor and manage network devices on IP networks
Lightweight Directory Access Protocol (LDAP)	389	Used to manage and communicate with directories
Hypertext Transfer Protocol Secure (HTTPS)	443	Secure version of HTTP that used TLS for encryption; most websites use HTTPS instead of HTTP
Lightweight Directory Access Protocol Secure (LDAPS)	636	Secure version of LDAP that uses TLS for encryption

SECURITY+ PORTS AND PROTOCOLS

File Transfer Protocol Secure (FTPS)	989/990	FTPS uses TLS for encryption; it can run on ports 20/21 but is sometimes allocated to ports 989/990
Internet Message Access Protocol Secure (IMAPS)	993	Secure version of IMAP that uses TLS for encryption
Post Office Protocol 3 Secure (POP3S)	995	Secure version of POP that uses TLS for encryption
Remote Authentication Dial-In User Service (RADIUS)	1812, 1813	Used to provide AAA for network services
Diameter	3868	Developed as an upgrade to Radius
Secure Real Time Protocol (SRTP)	5004	SRTP replaced RTP and is a protocol used to stream audio and video communication using UDP

DNS FILTERING

- DNS filtering is the technique of using DNS to block malicious websites and filter out damaging or unsuitable content
- This ensures that organizational data stays secure and private
- It allows the enterprise to have control over what their employees can access on company-managed networks and endpoints
- DNS filtering is often part of a wider access control strategy



DNS FILTERING

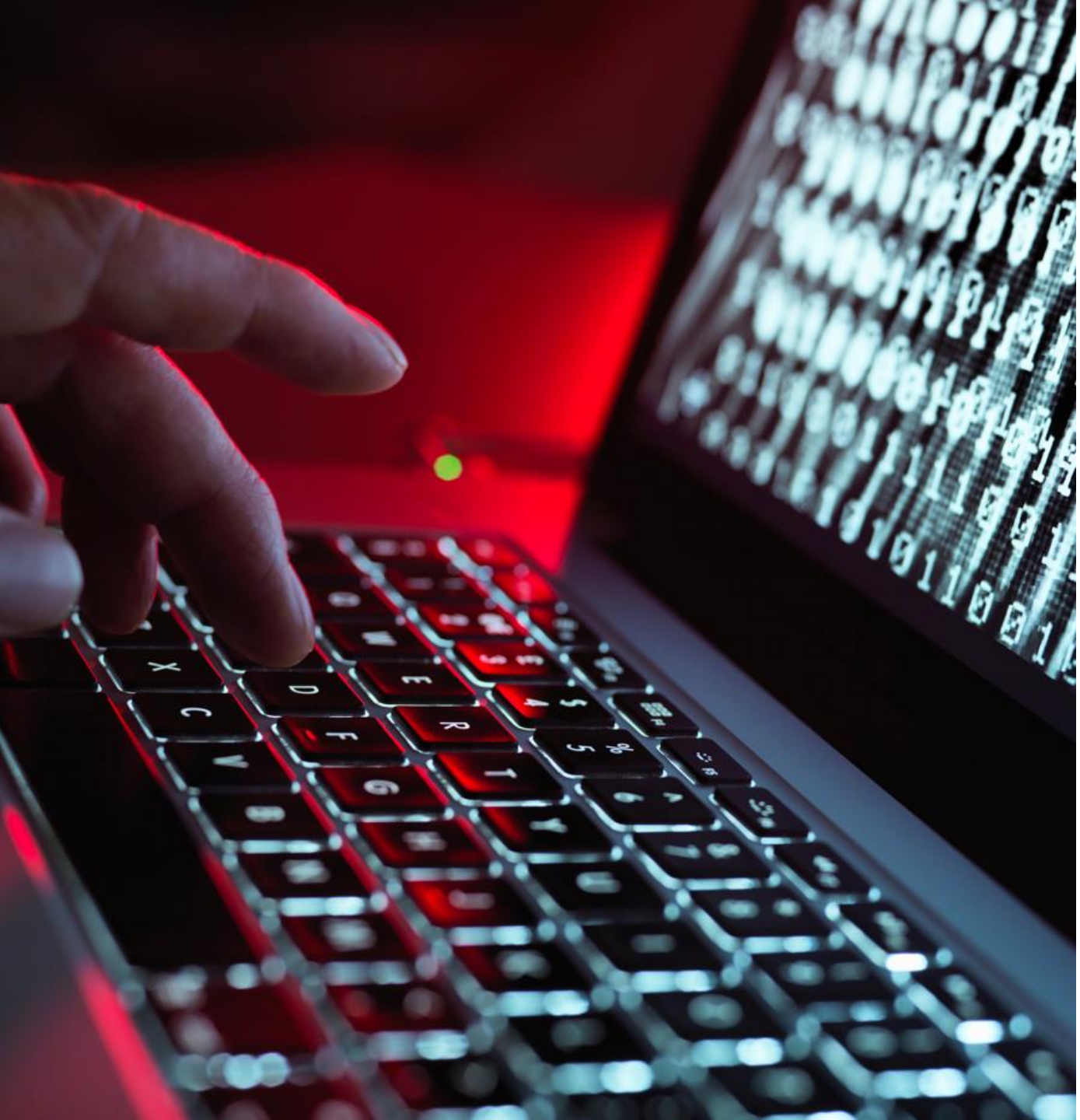
- All DNS queries are delivered to a DNS resolver
- Specifically configured DNS resolvers often function as filters by refusing to resolve queries for certain domains that are tracked in a blocklist or reputation list, therefore blocking users from accessing those domains servers
- DNS filtering services can also use an allowlist instead of a blocklist

DNS FILTERING

- DNS filtering can blocklist web attributes based on domain name or IPv4/v6 address:
  - **By domain**: The DNS resolver does not resolve (or look up) the IP addresses for certain domains at all
  - **By IP address**: The DNS resolver attempts to resolve all domains, but if the IP address is on the blocklist, the resolver will not send it back to the requestor

DNS SECURITY EXTENSIONS (DNSSEC)

- DNSSEC adds a layer of trust on top of DNS by providing authentication
  - This extension does not provide confidentiality
- When a DNS resolver is looking for www.skillsoft.com, the ".com" name servers help the resolver verify the records returned for "Skillsoft," and this security extension service helps verify the records returned for site
- The root DNS name servers help verify .com, and information published by the root is vetted by a thorough security procedure, including the Root Signing Ceremony



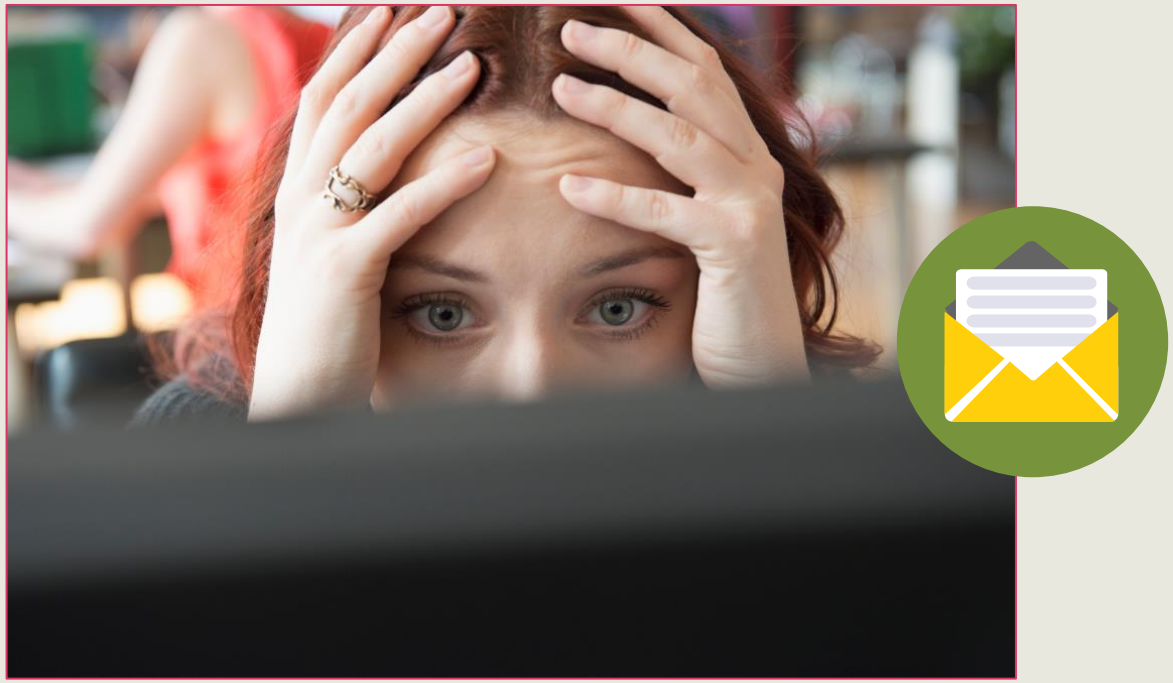
DNSSEC

- DNSSEC allows you to sign your company's DNS records so that any system that has an authenticating DNS resolver will automatically verify if the records are valid or have been compromised by a man-in-the-middle (MITM) attack
- To facilitate signature validation, DNSSEC adds a few new DNS record types:
  - RRSIG – contains a cryptographic signature
  - DNSKEY – contains a public signing key
  - DS – contains the hash of a DNSKEY record
  - NSEC and NSEC3 – for explicit denial-of-existence of a DNS record
  - CDNSKEY and CDS – for a child zone requesting updates to DS record(s) in the parent zone

OPENDNS

- OpenDNS is a company that offers DNS resolution services and a suite of consumer solutions with the goal of making the Internet faster, safer, and more reliable
- It is also a cloud-delivered enterprise security service that protects against threats on the Internet; OpenDNS's consumer products include parental and content filtering, web performance, and web security
- They offer businesses the Umbrella (as in Cisco Umbrella) service, which is designed to protect against malware, botnets, phishing, and targeted online attacks

SENDER POLICY FRAMEWORK (SPF)



- Practically all abusive email messages carry fake sender addresses today
- The victims whose addresses are being spoofed often suffer consequences such as:
  - Reputational damage
  - Need to repudiate the abuse
  - Time lost sorting out misdirected bounce messages
- Sender address forgery is a threat to both users and companies as it undermines the email medium and erodes people's confidence
  - This is why a bank never sends direct information about an account by email and keeps making a point of that fact

SENDER POLICY FRAMEWORK

- The Sender Policy Framework is an open standard that introduces a method to prevent sender address forgery
- More precisely, the current version of SPF — called SPFv1 or SPF Classic — protects the envelope sender address, which is used for messages delivery
- SPFv1 permits domain owners to designate their mail sending policy (e.g., which mail servers they use to send mail from their domain)

SENDER POLICY FRAMEWORK

- The SPF solution requires two sides to work together:
  1. The domain owner publishes this information in an SPF record in the domain's DNS zone, and when someone else's mail server receives a message claiming to come from that domain…
  2. The receiving server can check whether the message complies with the domain's stated policy
- For example, if the message comes from an unknown server, it will be marked as a fake

DOMAINKEYS IDENTIFIED MAIL (DKIM)

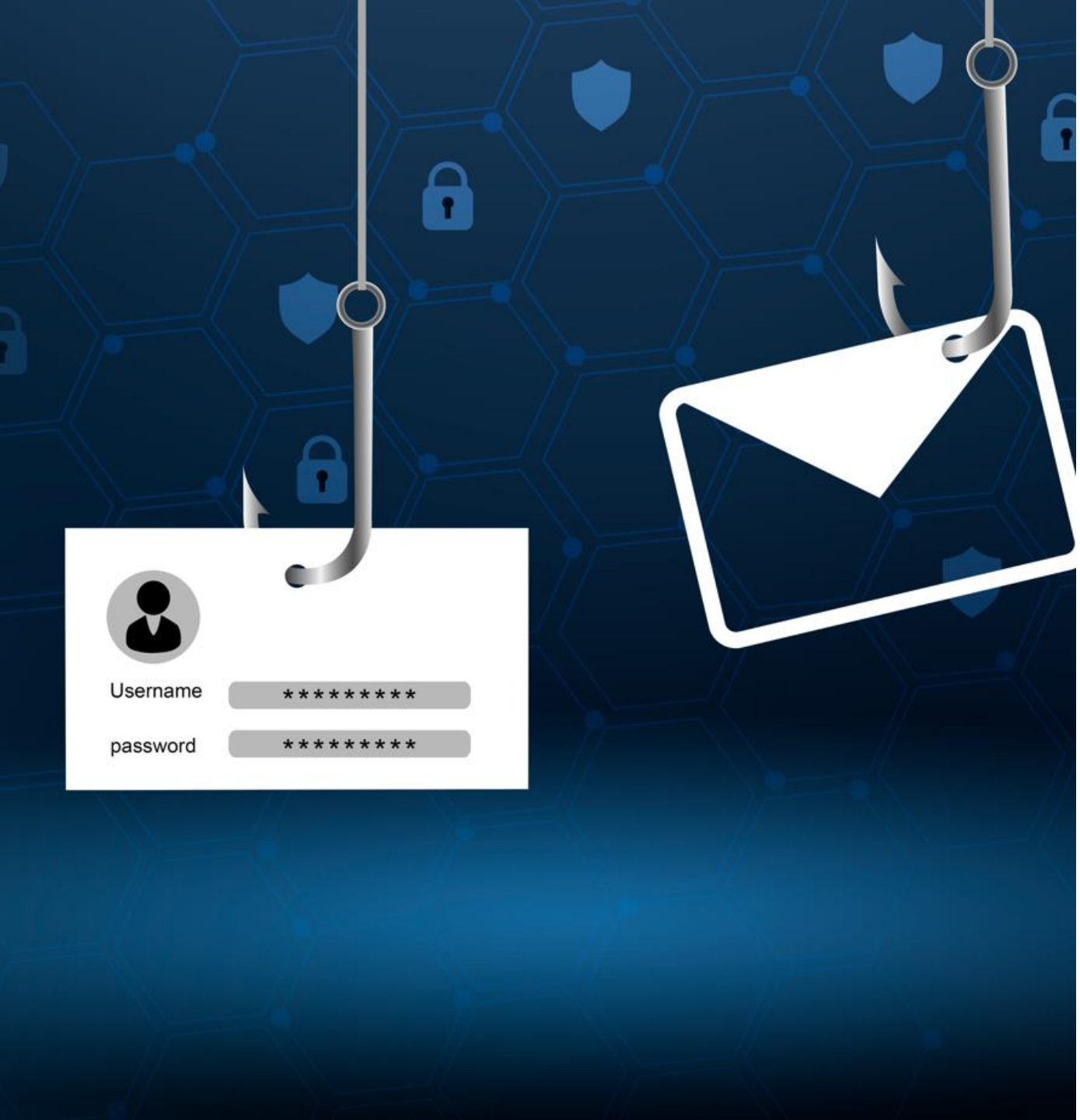
- DKIM is an email authentication method conducted between the outbound and inbound mail server or Message Transfer Agents (MTAs)
- The authentication process happens transparently to the end user
- With DKIM, the outbound mail server appends a digital signature to the email then the inbound server verifies the signature by looking up the public key and then comparing it with the signature from the specified outgoing mail server

DOMAINKEYS IDENTIFIED MAIL (DKIM)

- With DKIM, If the public key does not match the signature, it may be because:
  - The email was not sent from the mail server designated in the email header but was sent from another (spoofed) server instead
  - The email was modified in transit to the recipient
  - For instance, an attacker could intercept an email that was sent from a valid mail server, change it and then resend it

DOMAIN-BASED MESSAGE AUTHENTICATION REPORTING AND CONFORMANCE (DMARC)

- Organizations and end users undergo a high volume of spam and phishing from the Internet
- Many modern solutions work in isolation from each other
- Each receiver makes exclusive decisions about how to evaluate the reporting results
- Legitimate domain owners rarely get any meaningful feedback
- **DMARC** attempts to address this by providing coordinated, tested methods for domain owners and email receivers



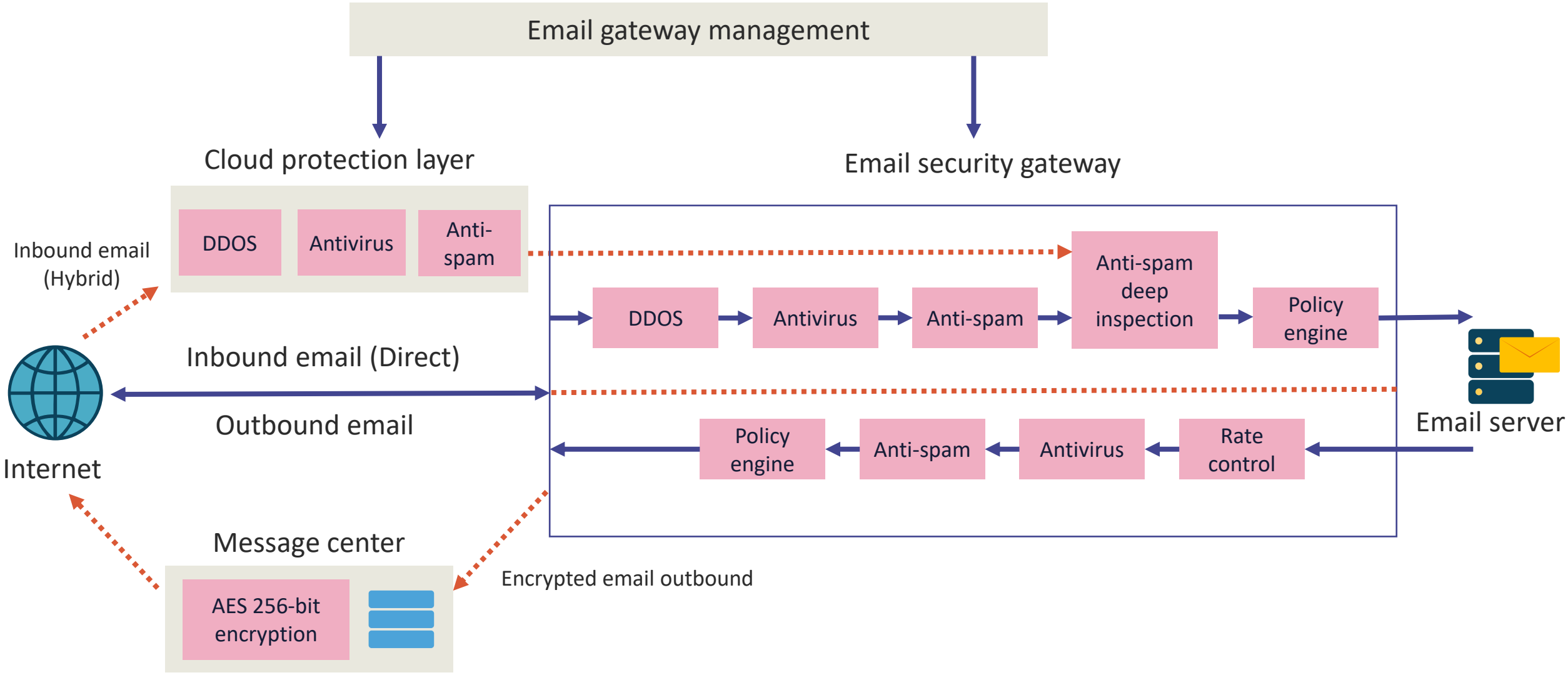
DOMAIN-BASED MESSAGE AUTHENTICATION REPORTING AND CONFORMANCE

- DMARC is an email authentication, policy, and reporting protocol
- **It builds on the widely deployed SPF and DKIM protocols**, offering:
  - Linkage to the sender ("From:") domain name
  - Published policies for recipient handling of authentication failures
  - Reporting from receivers to senders, to enhance and monitor protection of the domain from fraudulent email

EMAIL SECURITY GATEWAYS

- These special gateway appliances are dedicated email security services that work in or with MTAs to protect electronic mail
- They are also called secure email gateways (SEGs)
- This is a suite of tools that filter emails as they enter or leave the email server
- Emails are routed through the gateway service and typically require the DNS MX-records to be changed, regardless of email platform
- Many email providers today also offer a cloud-native email security solution called an Integrated Cloud Email Security (ICES), either in parallel or as a replacement for the legacy SEG

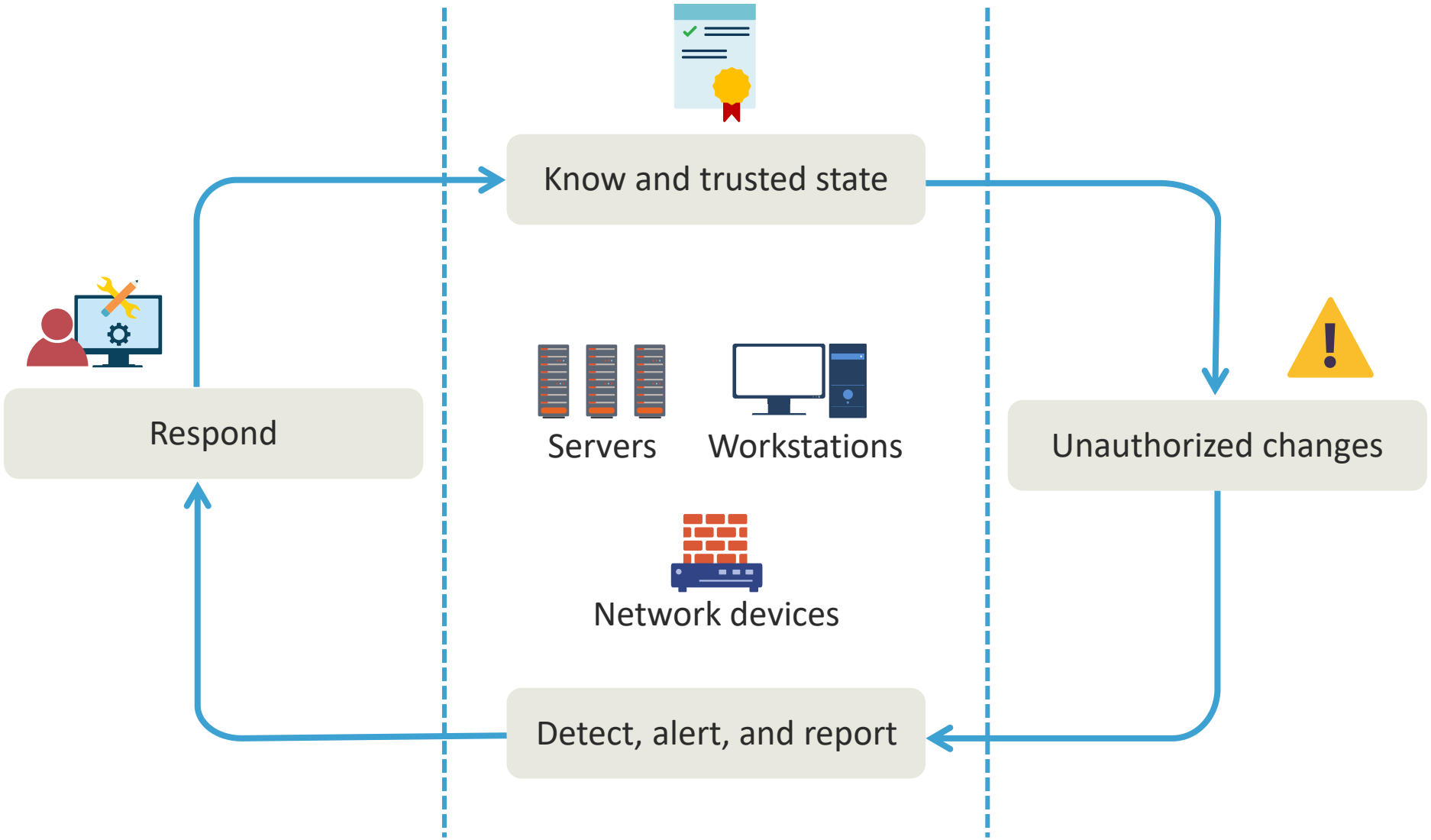
EMAIL SECURITY GATEWAYS



FILE INTEGRITY MONITORING (FIM)

- File Integrity Monitoring examines operating system files, configuration files, registries, application software, and Linux system files for changes and indicators of compromise
- Windows FIM provides alerts about suspicious activity such as:
  - File and registry key creation or removal
  - File modifications (changes in file size, access control lists, and hash of the content)
  - Registry modifications (changes in size, access control lists, type, and content)

FIM


Know and trusted state
Unauthorized changes
Detect, alert, and report
Respond
Servers
Workstations
Network devices

DATA LOSS PREVENTION (DLP)

Data

- Trade secrets
- Account numbers
- Social security numbers
- Intellectual property
- Personal health records

Can leak

- Stored on network or shared drives
- Copied on external removable media devices
- Transmitted electronically: email, instant messaging, online, etc.

To an outsider

- Competitors
- Regulators
- Unauthorized internal users
- Press or media

Resulting in a breach

- Company defamation
- Monetary expense for each record lost
- Legal liabilities
- Loss of assets
- Breach of customer trust
- Close of the business

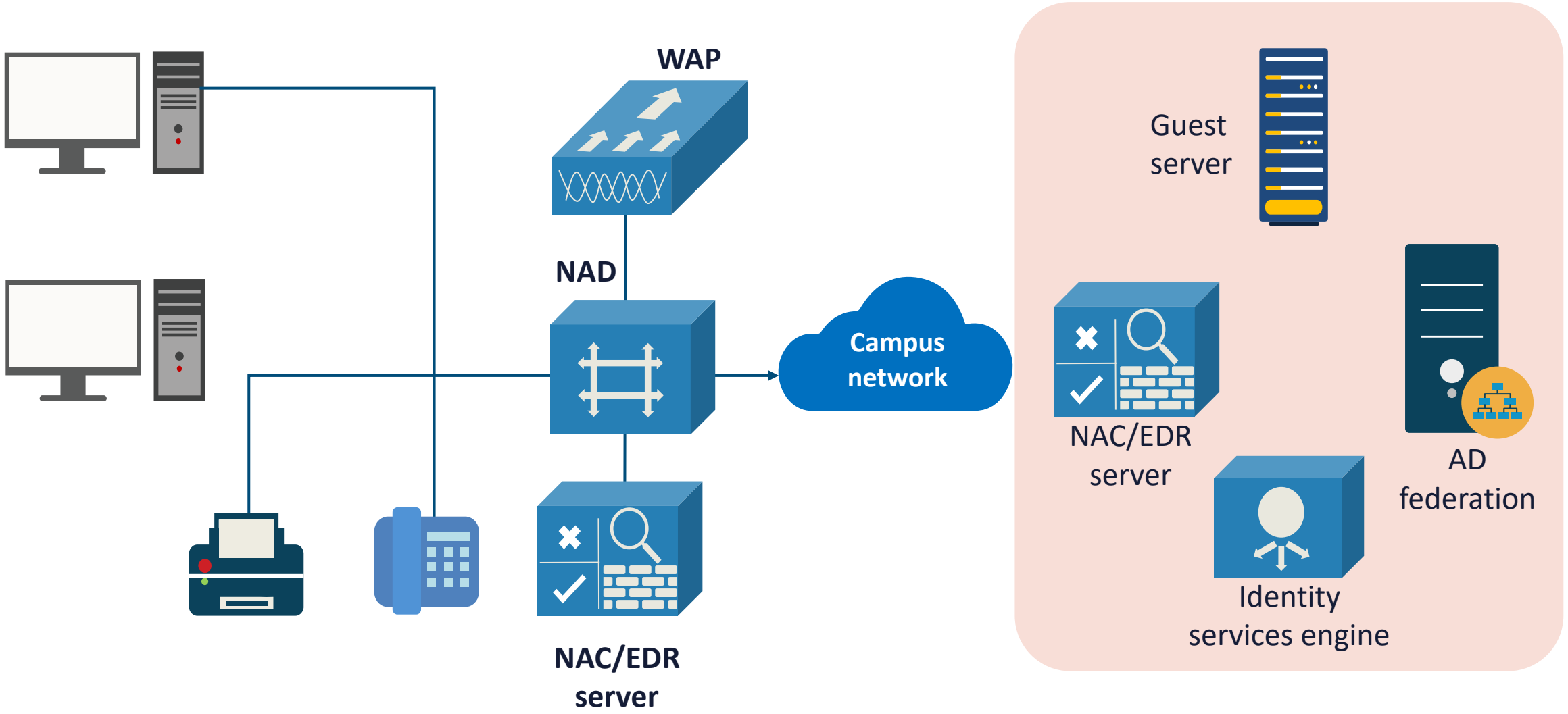
DATA LOSS PREVENTION SOLUTIONS

- There are a variety of hardware/software solutions that cam mitigate data leakage and data loss:
  - Secure email gateways
  - Cloud-based email security
  - Cloud access security brokers (CASB)
  - Endpoint detection and response (EDR)
  - Database activity monitoring (DAM)

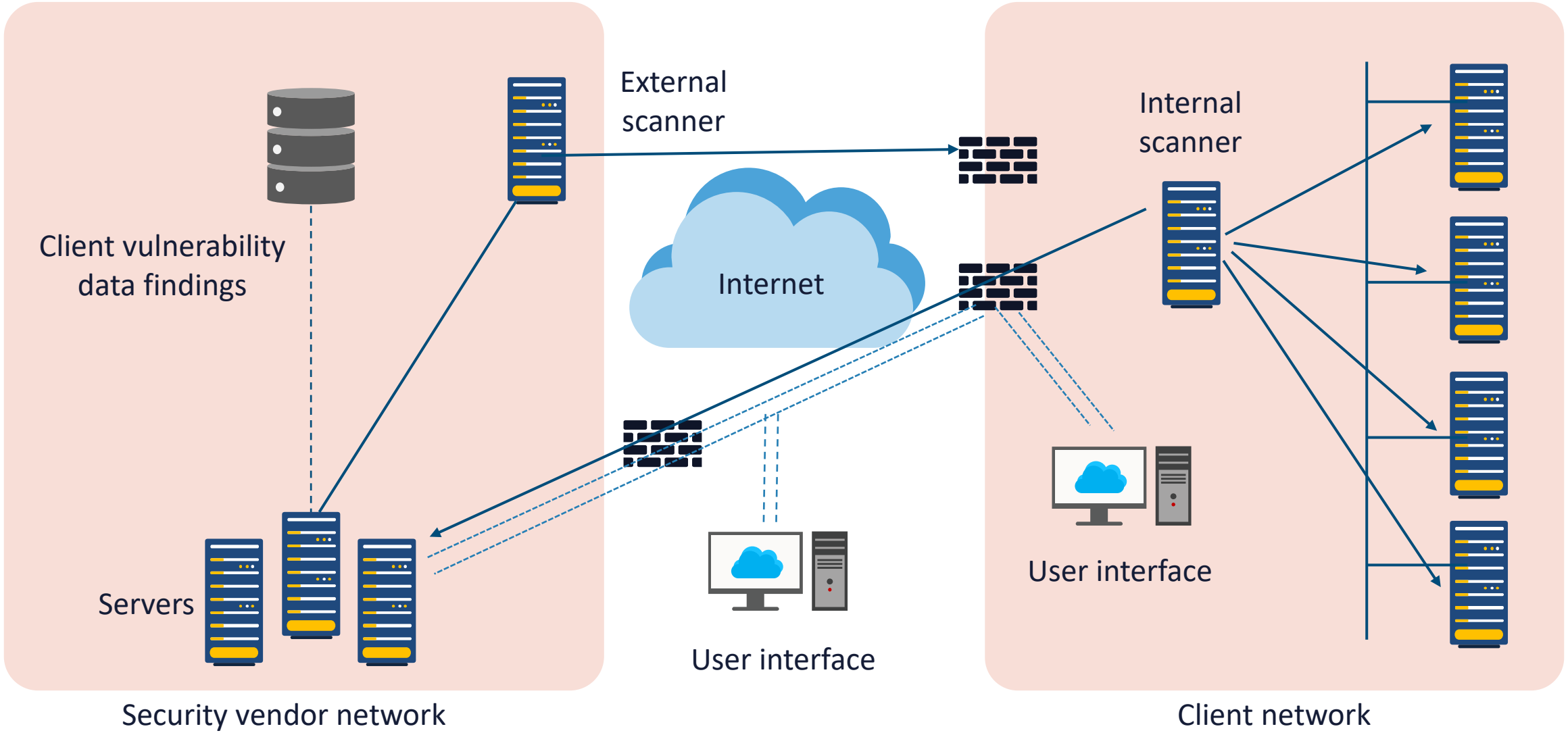
NETWORK ACCESS (ADMISSION) CONTROL (NAC)

- Network admission control (NAC) was an industry initiative sponsored by Cisco
- It typically enables 802.1X port-based network access control (PNAC) on Layer 2 and Layer 3 networks
- Does not trust anything inside or outside the perimeter without stringent authentication and verification
- Helps secure access from users and their devices, application programming interface (API) calls, Internet of Things (IoT), microservices, containers (Dockers, Kubernetes), and more

NETWORK ADMISSION CONTROL



CLOUD-BASED NAC/EDR



ENDPOINT DETECTION AND RESPONSE SOLUTIONS

- EDR has evolved from early HIDS solutions and involves a "lighter" software agent (i.e., Palo Alto Traps) installed on the host system; this often provides the basis for event monitoring and reporting
- EDR tools focus on detecting and investigating suspicious activities and are indicators of compromise (IoCs) on hosts/endpoints
- EDR monitors endpoint and network events and send information to a SEIM system or centralized database so further analysis, investigation, and reporting can take place
- Modern solutions are Extended Detection and Response (XDR) and user behavior analytics (UBA)

EXTENDED DETECTION AND RESPONSE

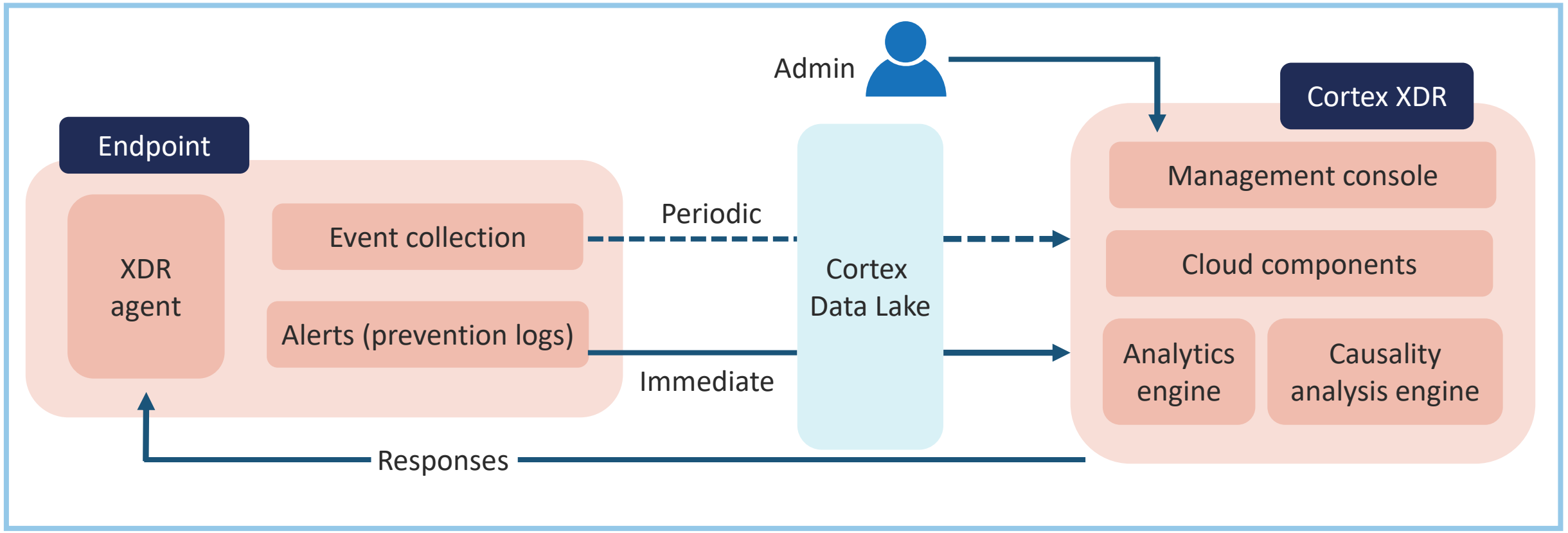
Threat protection driving by machine learning

Incident management

Automated root cause analysis

EXTENDED DETECTION AND RESPONSE

EXAMPLE: PALO ALTO CORTEX XDR



IDENTITY AND ACCESS MANAGEMENT

Objectives

- Learn about provisioning and deprovisioning user accounts
- Understand password concepts
- Know federation, single sign-on (SSO), and access control models
- Examine multi-factor and biometric authentication
- Define privileged access management (PAM) tools

DEMO: PROVISIONING AND DEPROVISIONING USER ACCOUNTS

In this demo…

We will examine provisioning and deprovisioning user accounts including permission assignments and implications, and identity proofing

DEMO: EXPLORING PASSWORD CONCEPTS

In this demo…

We will explore password concepts like best practices, length, complexity, reuse, expiration, age, password managers, and passwordless solutions

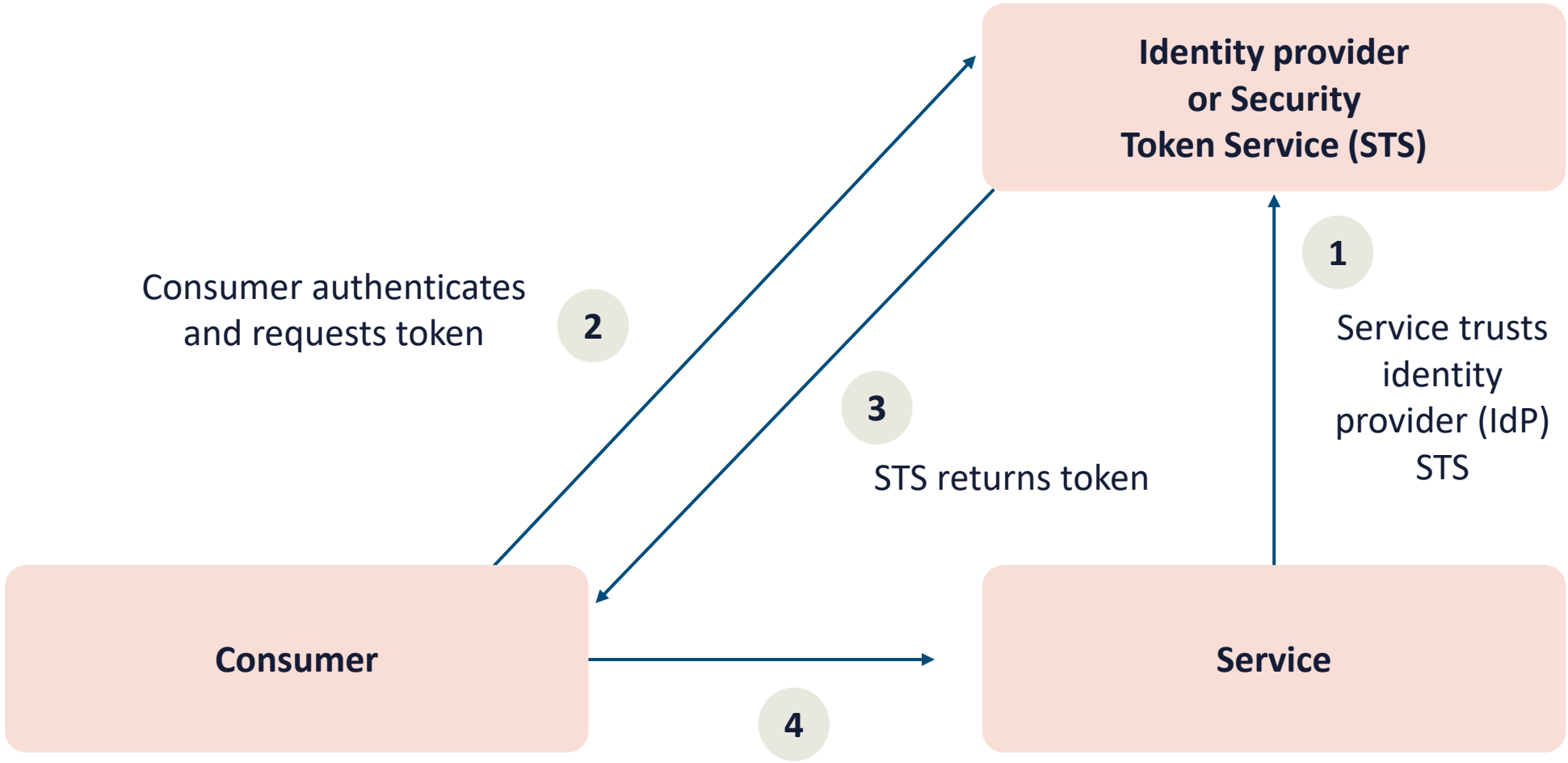
FEDERATION AND SINGLE SIGN-ON (SSO)

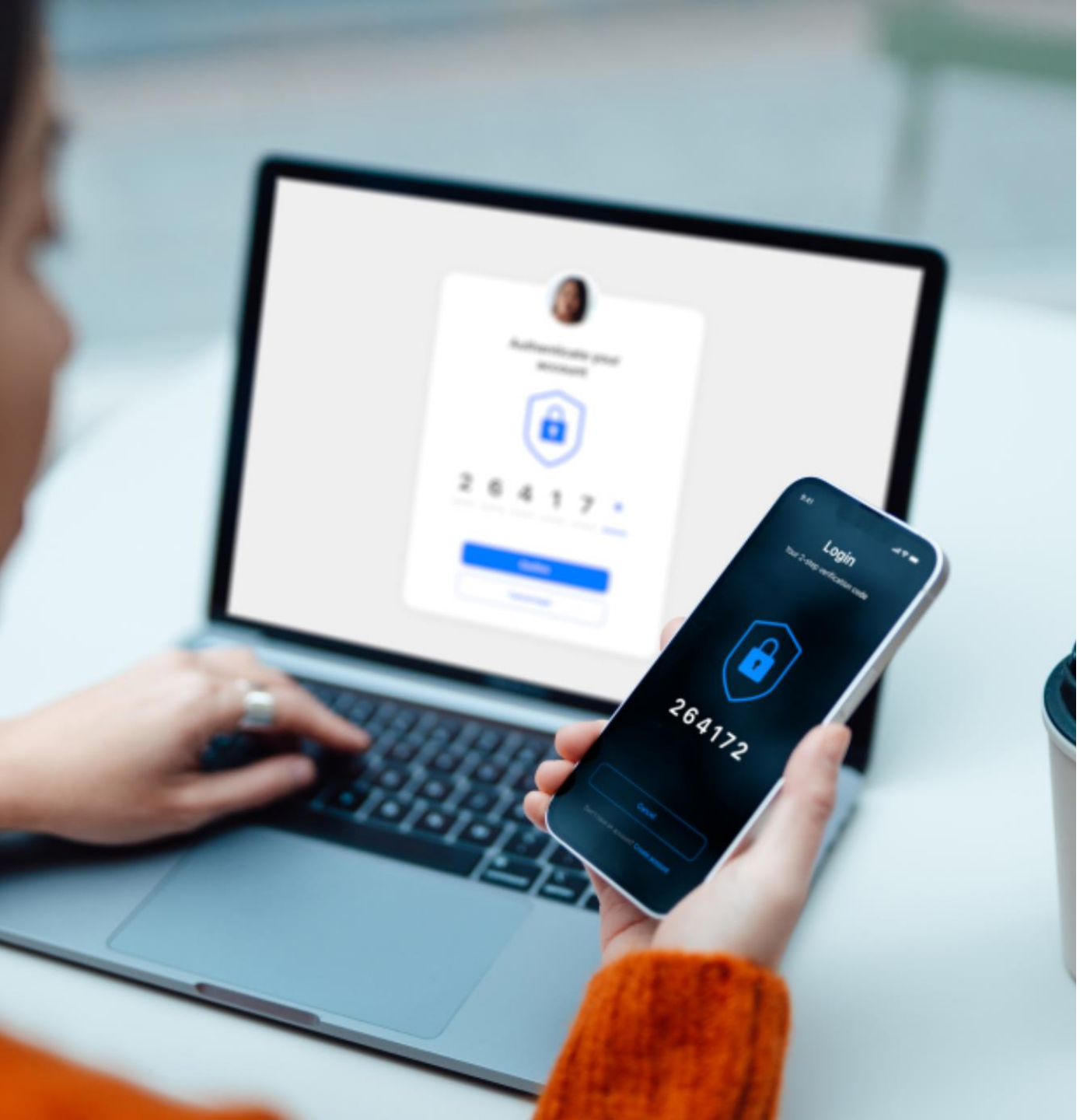
- Federated identity management, also known as federated single sign-on, refers to the formation of a trusted relationship between separate entities and third parties, such as cloud/application vendors or partners, enabling them to share identities and authenticate users across domains and realms
- When two domains are federated, a principal can authenticate to one domain and then access resources in the other domain without needing to perform an additional login procedure

FEDERATION AND SINGLE SIGN-ON

- SSO allows a user to access multiple applications using a single set of credentials
- This feature can be applied to employees, contractors, and customers to simplify the login experience
- To perform their duties, employees often sign on to multiple business applications including messaging, email, productivity apps, various accounts, HR functions, intranet sites, financial records, etc.

FEDERATED ACCESS

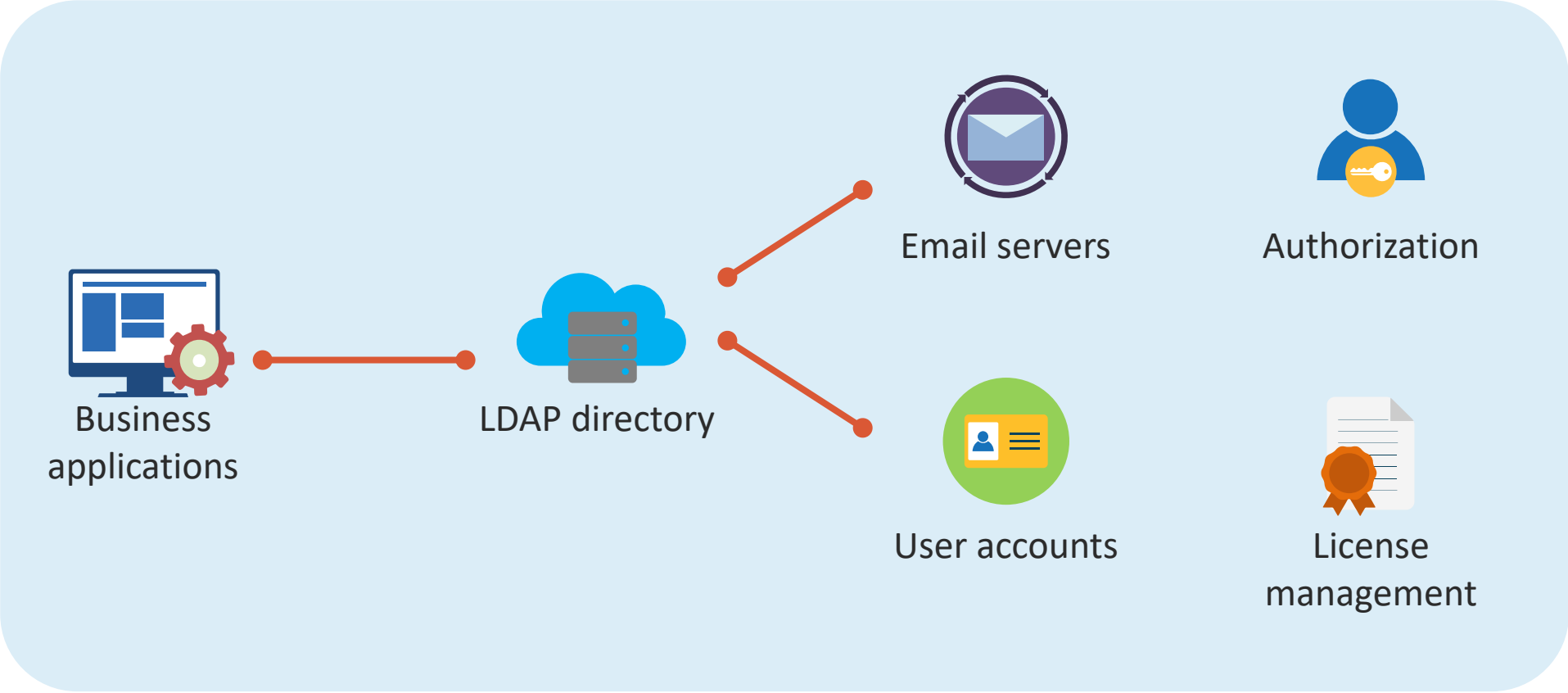




LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL (LDAP)

- LDAP was based on the X.500 directory but is a lighter, cross-platform, and standards-based solution
- LDAP servers are easy to install, maintain, and optimize, but they are without solid security of the queries, updates, and valuable information in the LDAP directory
- LDAPS (TCP 636) is LDAP over Transport Layer Security (TLS)
- Simple Authentication and Security Layer (SASL) BIND also offers authentication services using mechanisms like Kerberos, or a client certificate sent with TLS

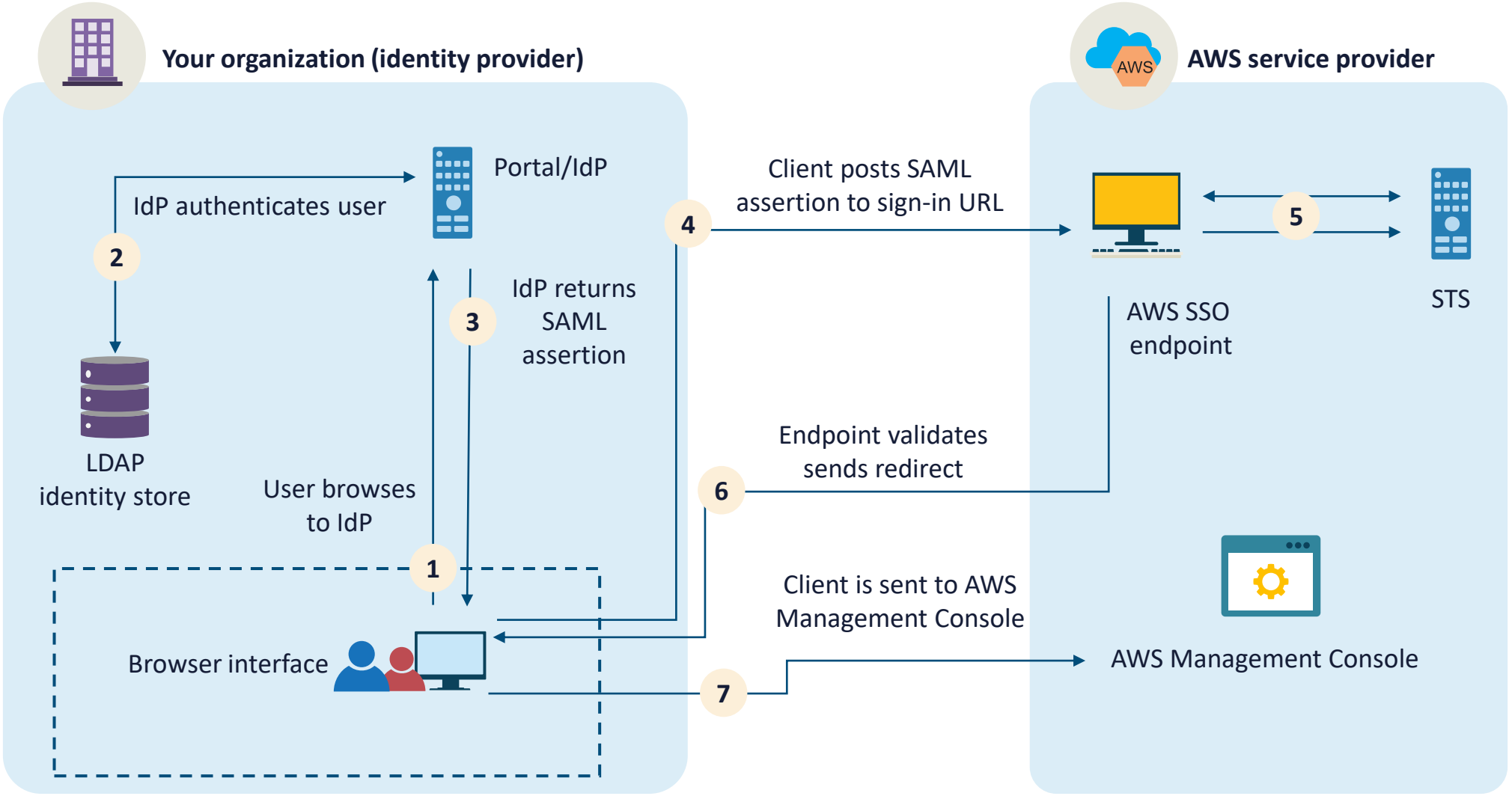
LDAP


Business applications
LDAP directory
Email servers
Authorization
User accounts
License management

SECURITY ASSERTION MARKUP LANGUAGE (SAML)

- SAML is an XML-based open-source SSO standard
- SAML is used by many cloud SSO connections for thousands of large enterprises, government agencies, and service providers that communicate on the Internet
- A key advantage of SAML is open-source interoperability
- Some large companies now require SAML for Internet SSO with Software as a Service (SaaS) applications and other external Internet Service Providers (ISPs)
- It is a common federated solution with cloud service providers

SAML 2.0 AT AMAZON WEB SERVICES



OAUTH/OIDC

- OAuth 2.0 is an open authorization framework that allows a third-party application to get limited access to an HTTP service
- Developers use OAuth to publish and interact with protected data in a safe and secure manner
- Service provider developers can use OAuth to store protected data and give users secure delegated access
- OAuth is designed to work with HTTP and basically allows access tokens to be issued to third-party clients by an authorization server with the approval of the resource owner
- The third party then uses the access token to access the protected resources offered by the resource server

OAUTH/OIDC

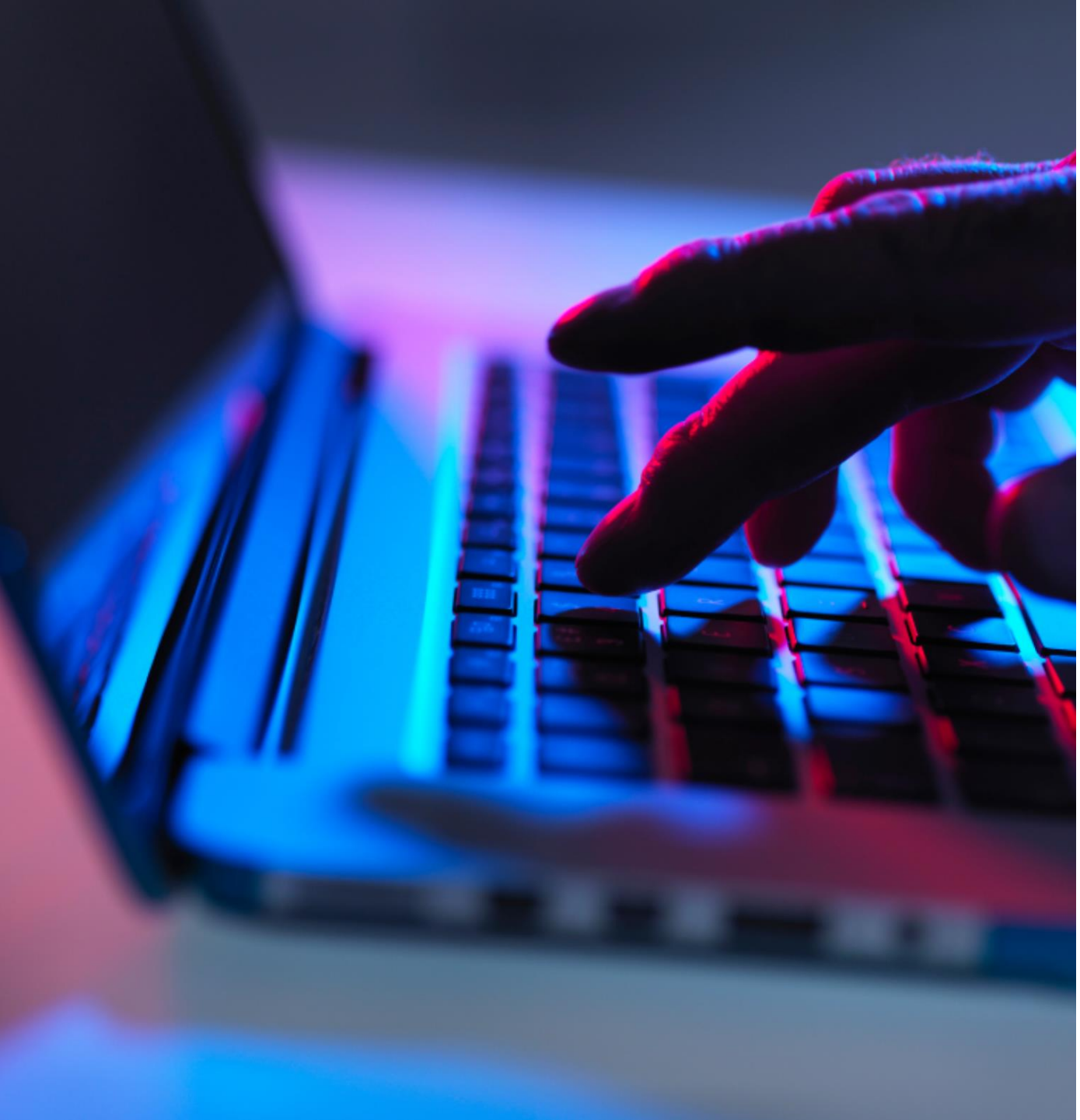
- OpenID Connect 1.0 is a basic identity layer on top of the OAuth 2.0 protocol
- It verifies the end-user identity using an authorization server
- It can get basic profile information about the user with an interoperable REST-like methodology
- Supports web-based, mobile, and JavaScript clients
- OpenID is extensible, as functionality can be added

MANDATORY ACCESS CONTROL (MAC)

"MAC is an access control policy that is uniformly enforced across all subjects and objects within the boundary of an information system. A subject that has been granted access to information is constrained from doing any of the following:

- Passing the information to unauthorized subjects or objects
- Granting its privileges to other subjects
- Changing one or more security attributes on subjects, objects, the information system, or system components
- Choosing the security attributes to be associated with newly-created or modified objects
- Changing the rules governing access control"

CSRC Content Editor, "Mandatory Access Control (MAC) - Glossary," CSRC, accessed Sept 6, 2021, https://csrc.nist.gov/glossary/term/mandatory_access_control.



MAC

- A mandatory access control model uses a strict set of established sensitivity levels and access controls for integrity and confidentiality based on classifications
- These are mathematical models used in high-security environments, like military, government agencies, and enterprises involved with sensitive data and activities
- Typically, state machine and information flow models are designed by a security team or steering committee as opposed to an administrator or asset owner

DISCRETIONARY ACCESS CONTROL (DAC)

- The DAC policy is enforced over all entities so that a subject being granted access can:
  - Pass the information to other subjects or objects
  - Grant its privileges to other subjects
  - Change security attributes on subjects, objects, information systems, or system components
  - Choose the security attributes to be associated with newly-created or revised objects; or
  - Change the rules governing access control

DISCRETIONARY ACCESS CONTROL

- DAC models involve control and management by the owner/creator of the object
- DAC leaves a certain amount of access control to the discretion of the object's owner – or anyone else who is authorized to control the object's access
- The opposite of a MAC model in that the owner can determine who should have access rights to an object and what those rights should be

ROLE-BASED ACCESS CONTROL (RBAC) MODELS

- NIST: "Access control based on user roles (i.e., a collection of access authorizations a user receives based on an explicit or implicit assumption of a given role).
- Role permissions may be inherited through a role hierarchy and typically reflect the permissions needed to perform defined functions within an organization. A given role may apply to a single individual or to several individuals."

CSRC Content Editor, "RBAC - Glossary," CSRC, accessed Sept 6, 2021, https://csrc.nist.gov/glossary/term//rbac.

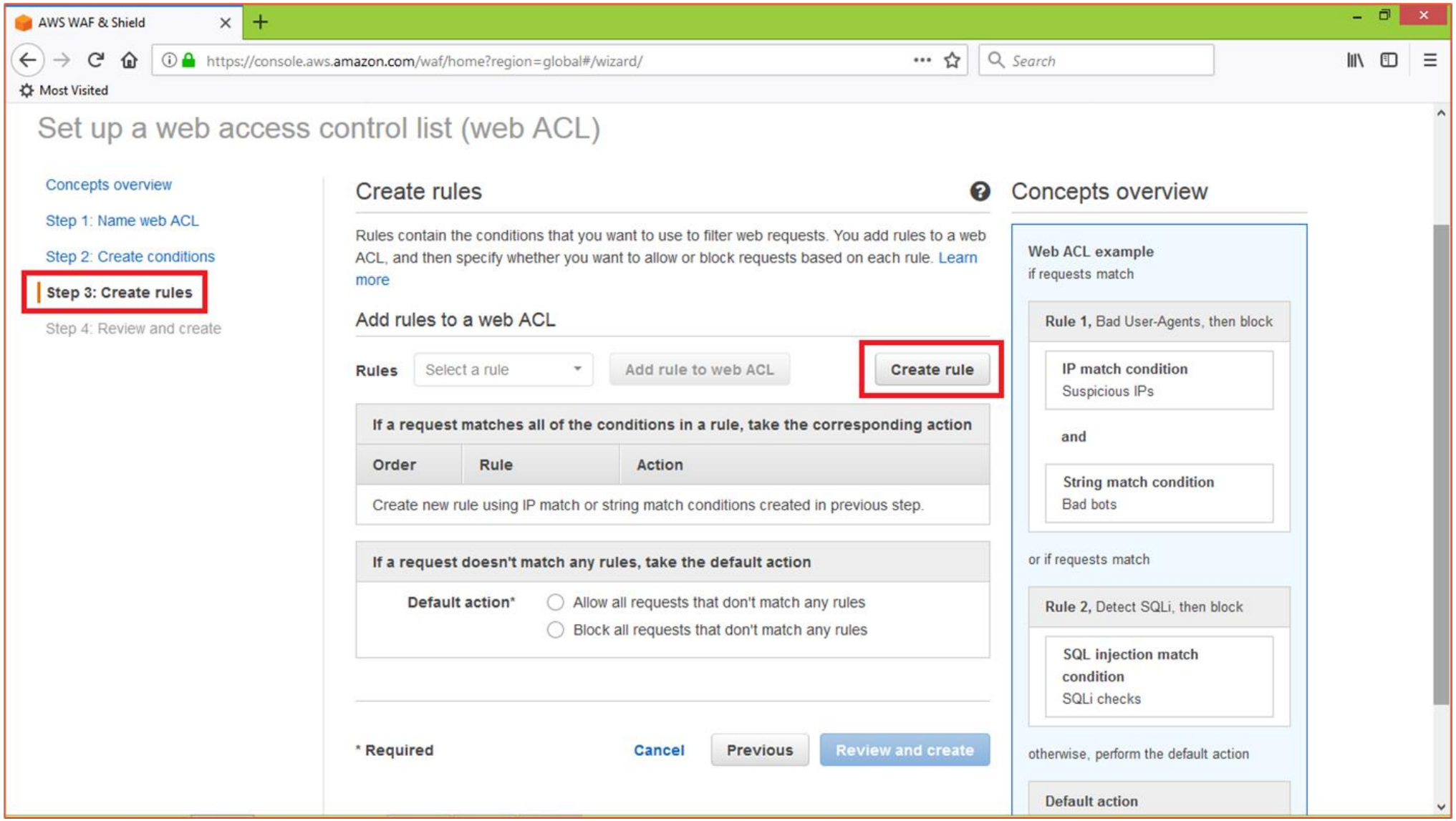
RULE-BASED ACCESS CONTROLS

- With Rule-based (or Rules-based) Access Control, access is permitted or denied to resource objects based on a set of rules defined by a system or network administrator
- As with DAC, access properties are stored in access control lists (ACLs) associated with each resource object
- When a certain group or user account attempts to access a resource, the operating system checks the rules contained in the ACL for that object
- Examples of Rules-based Access Controls are time-based ACLs, router infrastructure ACLs, static (stateless) firewalls, and AWS network ACLs

SAMPLE INBOUND ACCESS RULE

Protocol	Port	Source	Destination	Name	Action
UDP	53	Any	192.16.10.200	Allow DNS queries	Allow
TCP	80, 443	Any	192.168.10.201	Allow HTTP and HTTPS	Allow
TCP	3, 389	IT_Admin_IP_Range	Any	Allow RDP	Allow
Any	Any	Any	Any	Default	Deny

SAMPLE INBOUND ACCESS RULE



MULTI-FACTOR AUTHENTICATION (MFA)

- Multi-factor authentication typically involves adding an additional authentication mechanism to the initial origin authentication or credential presentation
  - Something you know
  - Something you have
  - Something you are
  - Somewhere you are

SOMETHING YOU KNOW

- Password
- Personal identification number (PIN)
- Passphrase
- Secret word or phrase

SOMETHING YOU HAVE

- Hard/soft authentication tokens (YubiKey/Authy)
- Badge or smart card
- X509v3 certificates
- Security keys

SOMETHING YOU ARE

- Fingerprint
- Ocular biometrics
- Facial recognition
- Speech patterns

SOMEWHERE YOU ARE

- Remote client-based and clientless VPN
- Remote Software Defined Perimeter (SDP)
- 802.1x wired or wireless network
- Cloud IdM managed network

FINGERPRINT BIOMETRICS

- This is one of the oldest and most common biometrics since they vary from person to person and do not change over time
- Integrated into mobile devices and laptop computers using hardware and/or software
- A fingerprint scanner system has two functions
- Gets an image of the finger
- Determines whether the outline of ridges and valleys in the image matches the patterns in pre-scanned images

FACIAL RECOGNITION

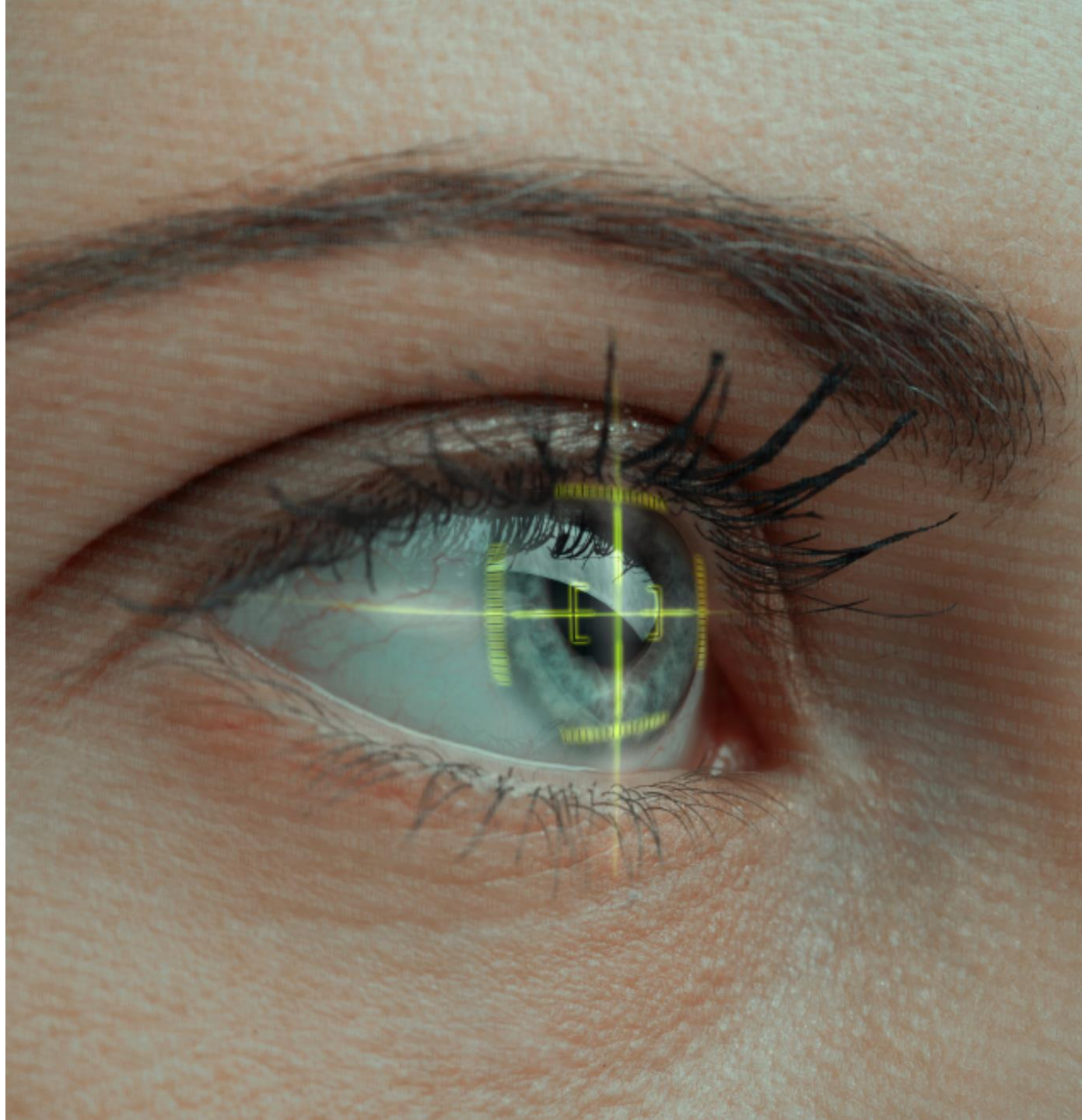
- One of the fastest growing mechanisms pre-pandemic
- Commonly used to identify or verify an individual in still or video images
- The main applications of face recognition are in areas of security biometrics and human-to-computer interaction (including robotics)
- The primary method for modeling facial images is Principal Component Analysis (PCA)
    - This is simpler, has a high learning capability, and possesses vigorous sensitivity to small changes in the face image

IRIS SCAN BIOMETRICS

- The iris is the thin, circular structure "color" part of the eye and controls the diameter and size of the pupils and therefore the amount of light reaching the retina
- Muscles attached to the iris expand or contract the pupil so the larger the pupil, the more light that can enter
- Iris scanners use camera technology to get images of the intricate and detailed structures of the iris using delicate infrared illumination

RETINA SCAN BIOMETRICS

- The retina is a thin tissue composed of neural cells located in the back portion of the eye
- Due to the complex make-up of the capillaries, every person's retina is distinctive
- Scanner sends a beam of low-energy infrared light into an eye when user looks through the scanner's eyepiece



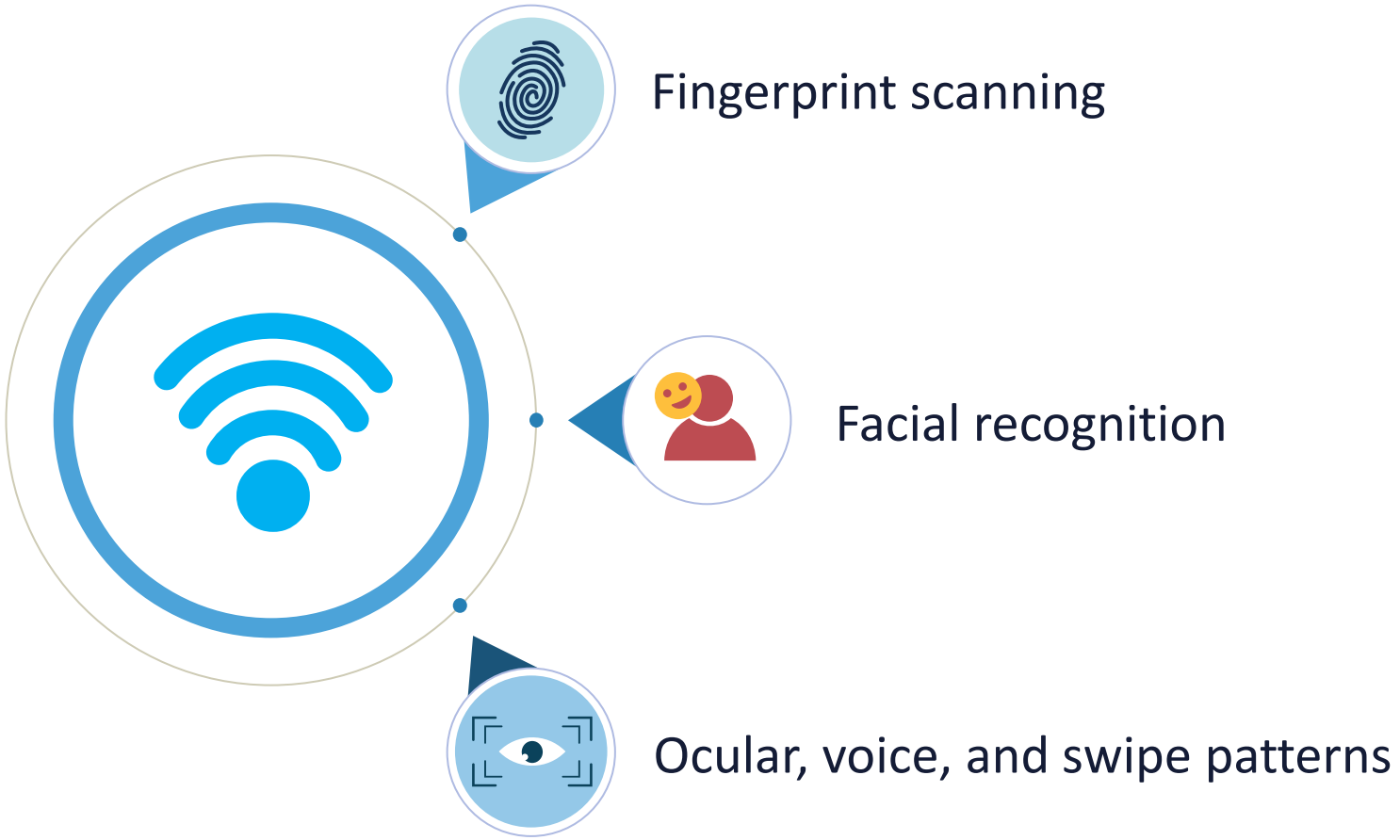
RETINA SCAN BIOMETRICS

- A beam of light traces a standardized path on the retina and the pattern of variations are converted to code and stored in a database
- Retinal scanning is categorized as invasive since the eye must be very close to the eyepiece

VOICE RECOGNITION

- There is a difference between speaker recognition and speech recognition
- "Voice recognition" can be used for both terms
- Speaker recognition leverages the aural aspects of speech that diverge among people
- Traits include human physical structure learned social communication patterns
- Voice recognition is classified as a "behavioral biometric" which is non-invasive

MOBILE BIOMETRICS



BIOMETRIC MEASUREMENTS

- **False acceptance rate (FAR)** measures the probability that the biometric system will incorrectly accept an access effort by an unauthorized user
  - A system's FAR is often specified as the ratio of the number of false acceptances divided by the amount of authentication attempts
- The **False rejection rate (FRR)** is the probability that the system incorrectly rejects access to an authorized person, due to failing to match the biometric input with a template
- The **Crossover error rate (CER)** is the value of FAR and FRR when the sensitivity is setup so that FAR and FRR are the same
  - This is an excellent metric for quantitative comparison of differing biometrics

PRIVILEGED ACCESS MANAGEMENT

- Privileged access management (PAM) is an identity security initiative that helps organizations counter cyberthreats by monitoring, detecting, and stopping unauthorized access to critical resources
- PAM works as a collaboration of people, processes, and technology to provide visibility into subjects using privileged accounts and what they are doing
- System security is enhanced by limiting the number of subjects that have access to administrative functions
- Additional layers of protection mitigate data breaches by threat actors

PAM COMPONENTS

Just-in-time permissions

A practice where the privilege granted to applications or systems is limited to predetermined periods of time, on an as-needed basis

Minimizes the risk of standing privileges that attackers can easily exploit

Password vaulting

A program that securely stores credentials for multiple applications and in an encrypted format

Users can access the vault via a single "master" password and the vault then presents it for the account they need to access

Ephemeral credentials

Dynamically generated credentials that are created when needed, then discarded afterward

Like persistent credentials, these credentials offer the subject a temporary token needed to gain access

PRIVILEGED ACCESS MANAGEMENT