Welcome Back to the CISSP Bootcamp

Your instructors:

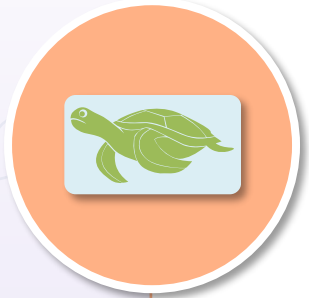
Michael J Shannon

and

David Robichaud

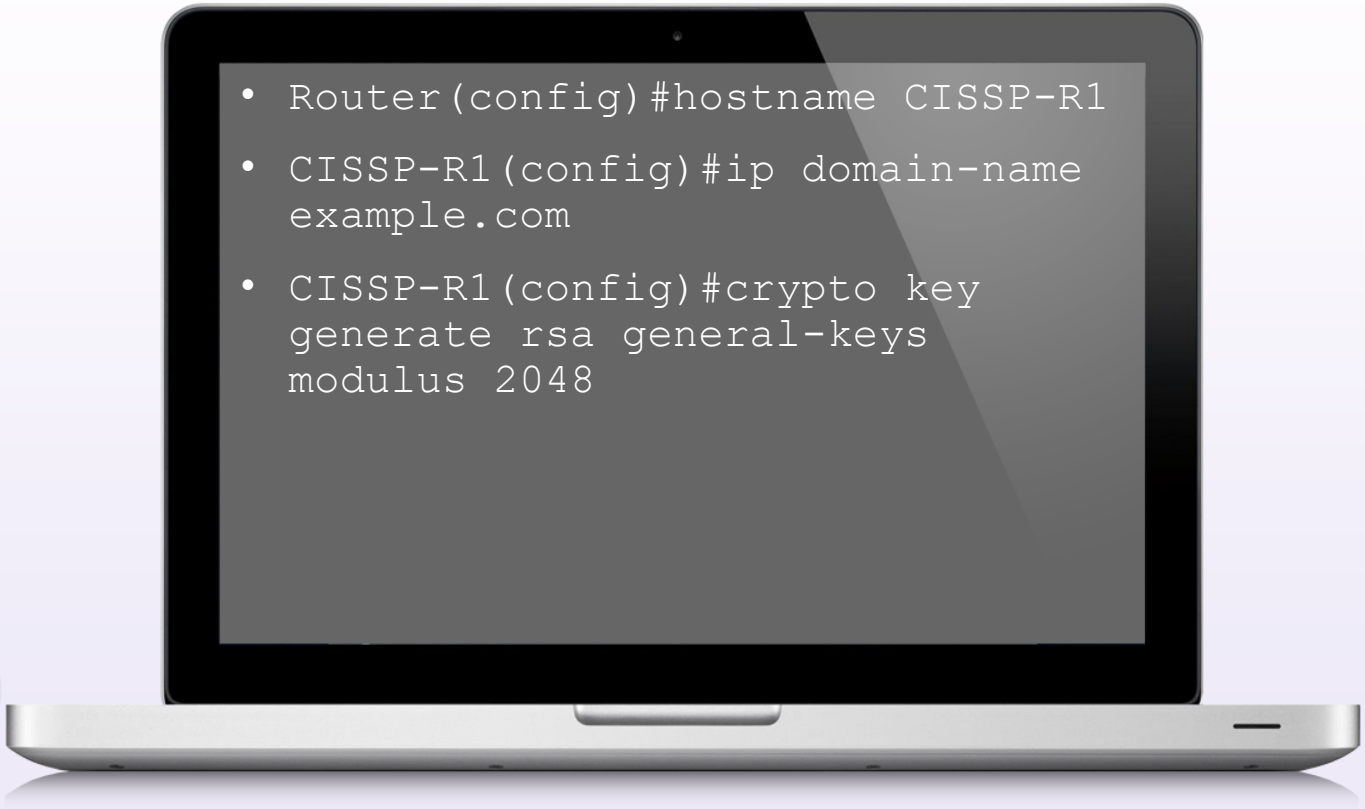
- **Class will begin at 10:00 A.M. Central Standard Time (CST)**

SSH2

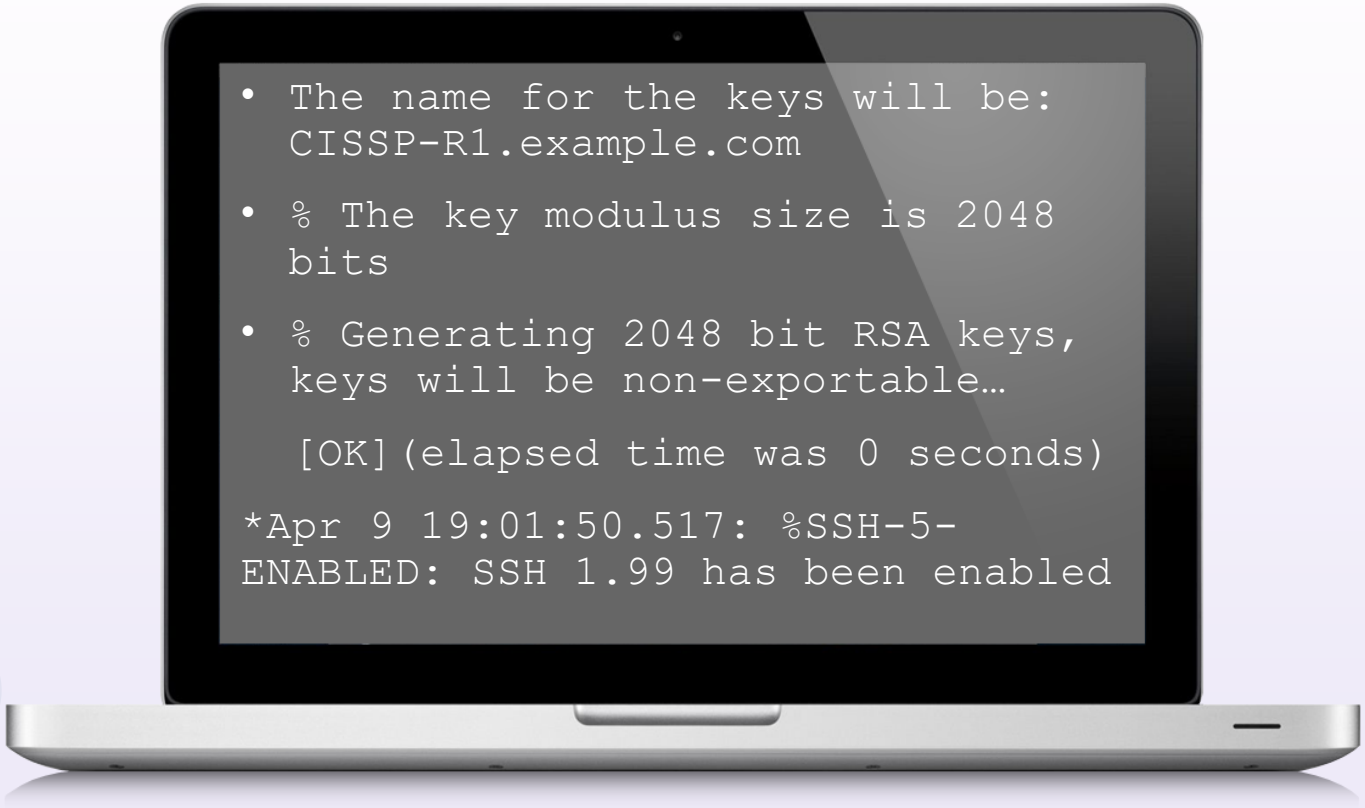


- Management access should be limited to secure protocol alternatives, as in SSH instead of Telnet
- SSH2 is preferable to SSH1 whenever possible
- SSH2 uses symmetric encryption for the bulk data encryption and asymmetric algorithms in their key management processes
- SSH2 uses DH for key exchange

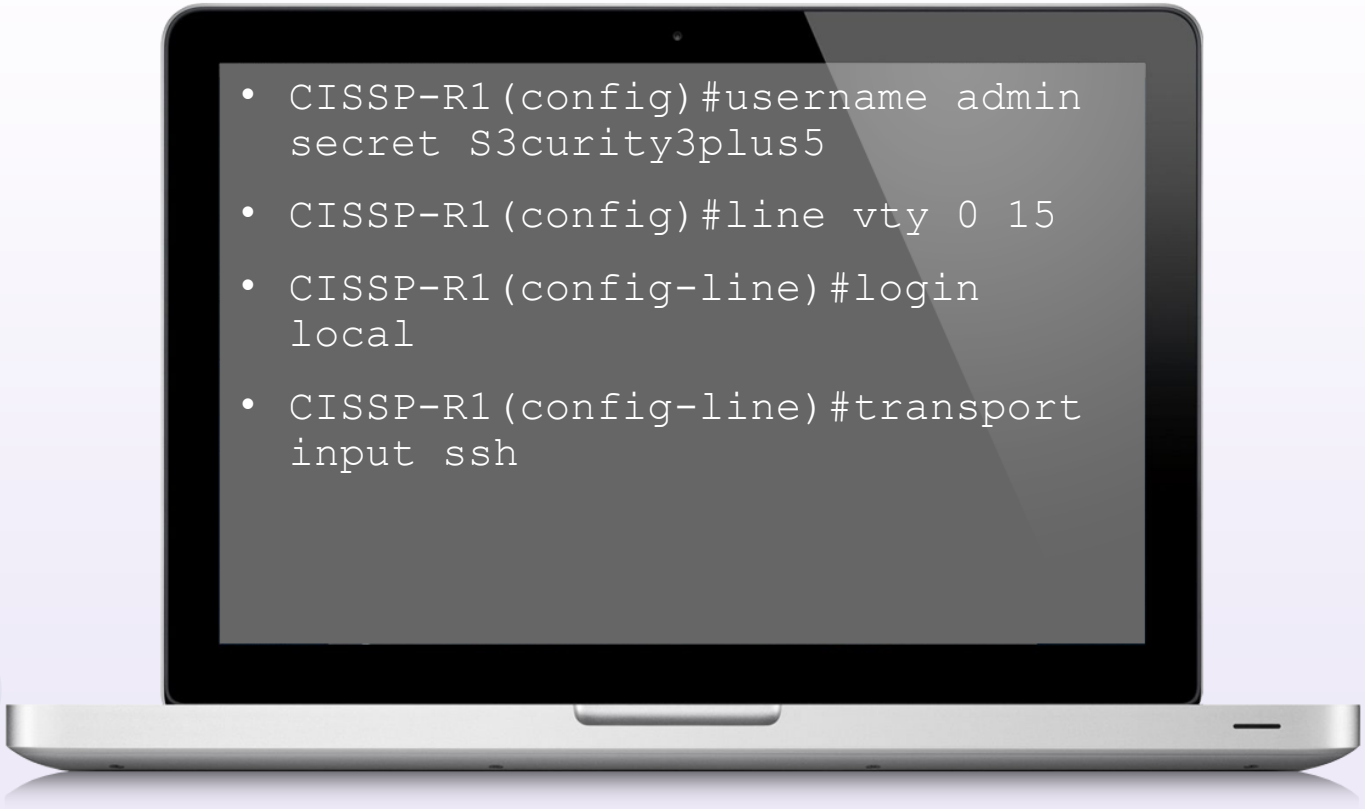
SSH2 on a Cisco Router



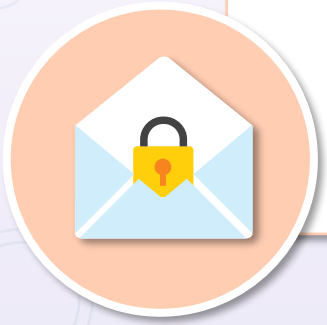
SSH2 on a Cisco Router



SSH2 on a Cisco Router

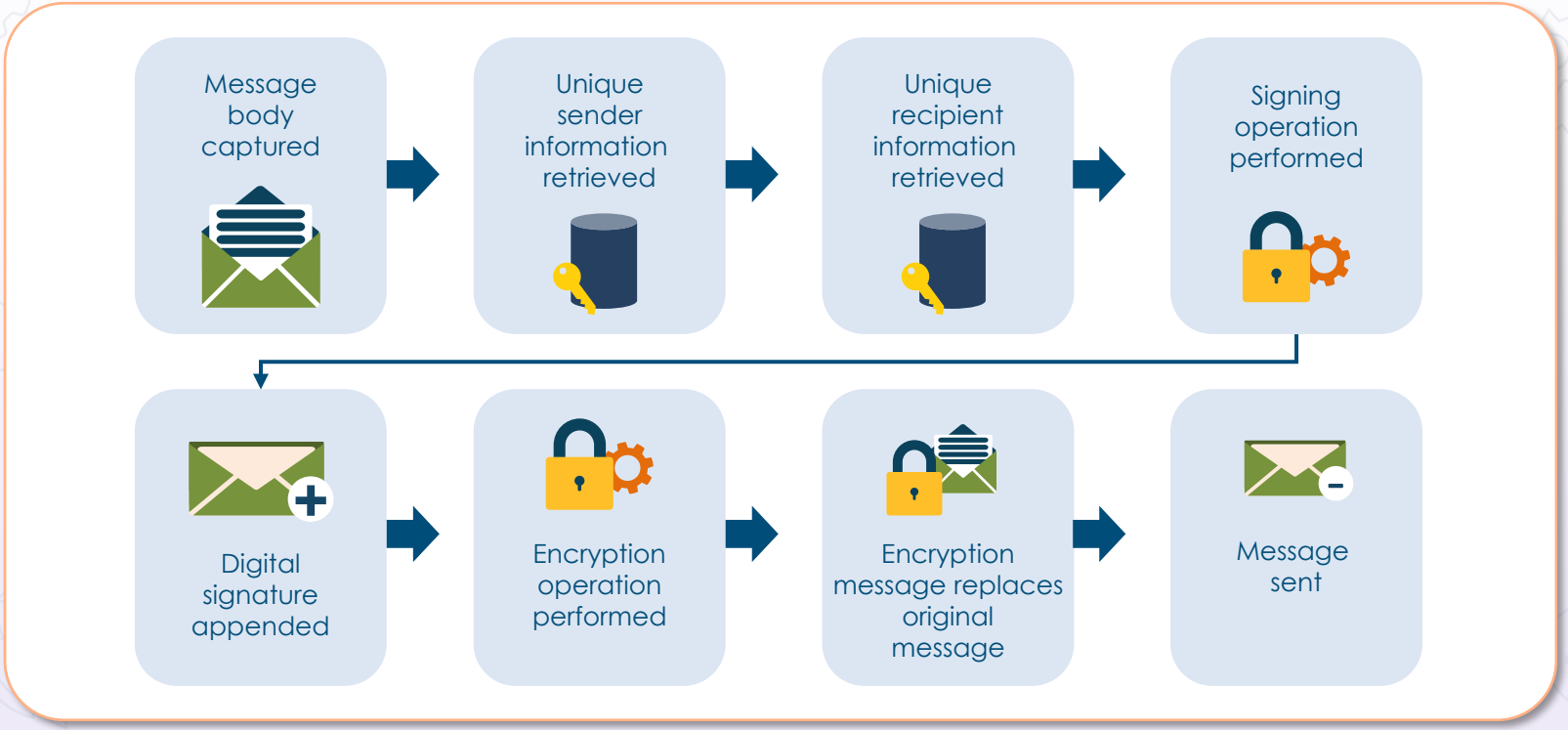


S/MIME



- SMTP is not natively secure, so it needs an extra security layer: Secure/Multipurpose Internet Mail Exchanger
- S/MIME v3 has become the standard for email message security
- Digital signatures are the most common S/MIME service providing authentication, data integrity, and non-repudiation

Sending Email Using S/MIME



FTPS

- Essentially the File Transfer Protocol over TLS
- Also called FTP over TLS and FTP Secure
- Typically used server-to-server
- Uses AES, RSA/DSA, and X509v3 certificates
- Explicit FTPS
  - Selected parts or components for communication are encrypted
- Implicit FTPS
  - All communications are encrypted

SFTP

- IETF-designed version of FTP that provides secure data access and transfer over an SSH2 channel
- It is a function of the SSH Protocol and is also called SSH File Transfer Protocol
- Both the commands and data are encrypted
- Platform-independent
- Slower than SCP

Domain Name System Security Extension (DNSSEC)

- DNSSEC (DNS Security Extensions) protects users from DNS attacks and forces systems to detect DNS attacks
- It adds a layer of trust on top of DNS by providing authentication while the root DNS name servers help verify domains

DNSSEC

- 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

Secure RTP

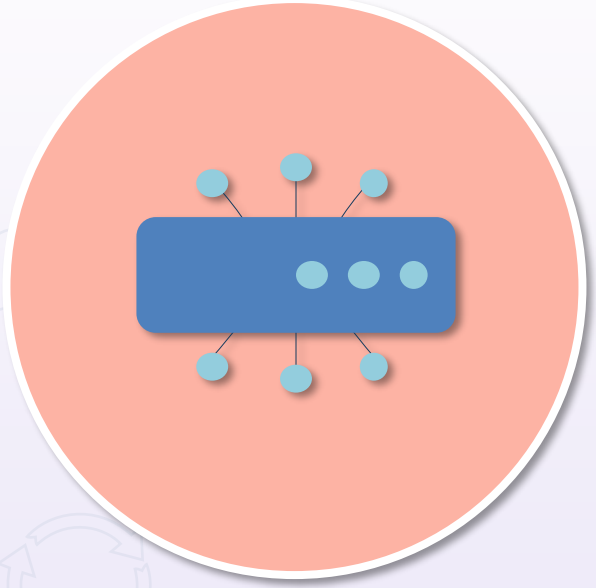
VoIP security

- Secure Real-Time Transport Protocol (SRTP) extends the RTP protocol by providing enhanced security techniques
- Provides encryption, integrity, and authentication verification of data and messages transported by RTP
- Released in 2004 by Cisco Systems and Ericsson
- Uses AES as its default encryption cipher in Segmented Integer Counter Mode and f8-mode to allow the AES block cipher to be used as a stream cipher for the RTP data stream

LDAPS

- LDAP was based on X.500 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 SSL/TLS
- SASL (Simple Authentication and Security Layer) BIND also offers authentication services using mechanisms like Kerberos, or a client certificate sent with TLS

SNMPv3



- SNMPv3 can be configured in three modes:
  - noAuthNoPriv – no cryptographic hash or encryption (passwords)
  - AuthNoPriv – cryptographic HMAC (SHA1 or SHA2) to secure authentication credentials and provide integrity, but no data encryption
  - AuthPriv – HMAC for integrity and secure authentication credentials, and encryption (AES) of data

QUIC

- QUIC is a "newish" transport protocol that was originally designed by Jim Roskind at Google
- It reduces latency compared to using TCP
  - Since TCP is implemented in operating system kernels, and middlebox firmware, making significant changes to TCP is next to impossible
  - QUIC is built on top of UDP – it has no such limitations
- QUIC is like TCP+TLS+HTTP/2 implemented over UDP and provides for
  - dramatically reduced connection establishment time
  - improved congestion control
  - multiplexing without head of line blocking, and
  - connection migration

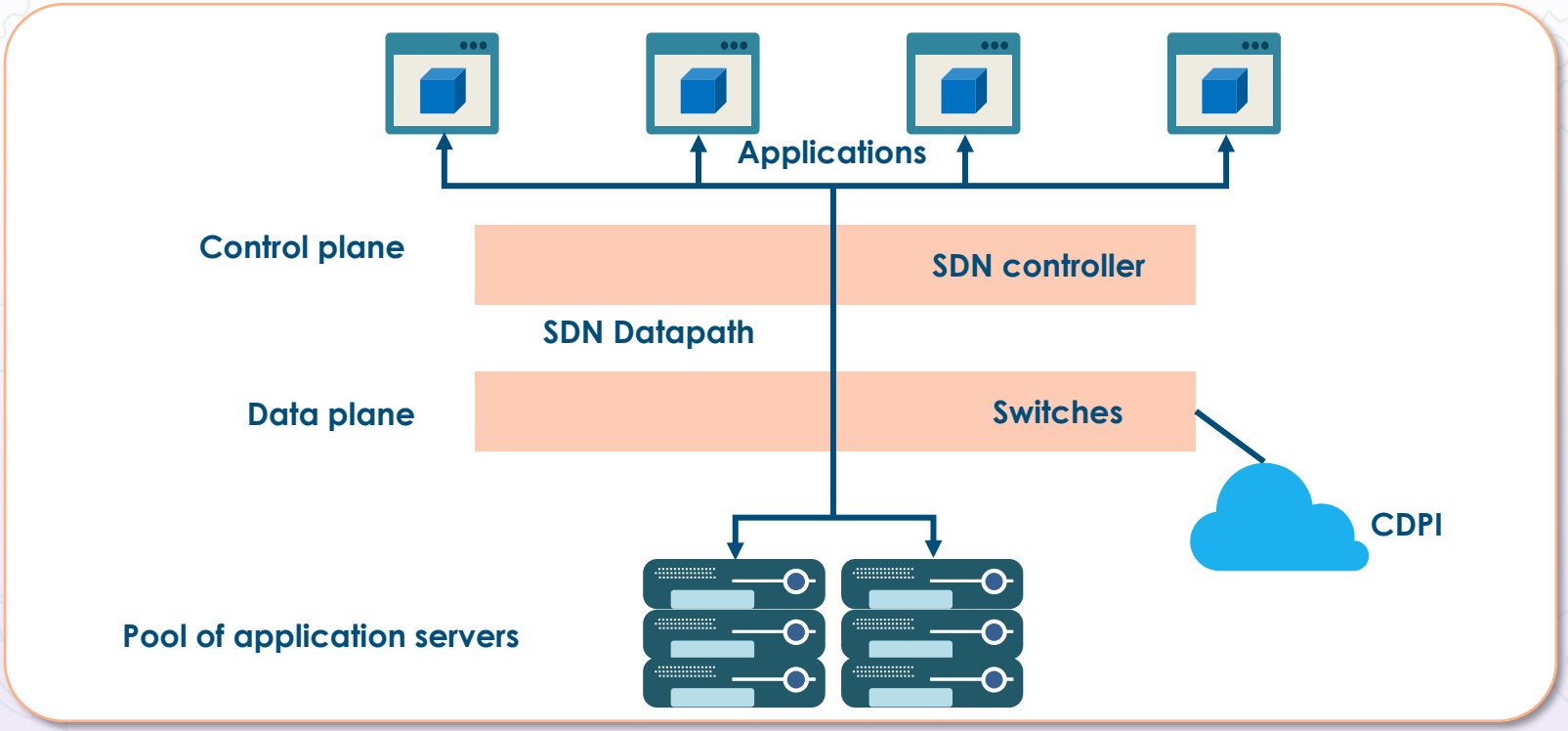
HTTP Strict-Transport-Security (HSTS)

- If a web site accepts an HTTP connection and redirects it to HTTPS, users may initially access the non-encrypted version of the site before being redirected
- This creates a vulnerability to man-in-the-middle attacks, as the redirect can be exploited to direct users to a malicious site instead of the secure version of the original site
- HTTP Strict-Transport-Security (HSTS) allows a TLS web site to instruct browsers that it should only be accessed using HTTPS, instead of using HTTP
- The web server employs the HTTP **`Strict-Transport-Security`** header

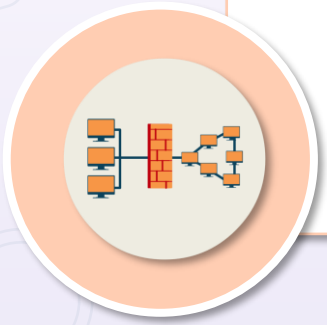
Micro-segmentation for SDN

- Software-defined networking (SDN) virtualizes network functionality by separating the control and data planes and implementing the network intelligence in software – typically hypervisor or proprietary server solutions
- Micro-segmentation is a method of creating zones in data centers and cloud environments to insulate workloads from one another and secure them independently

Software-defined Networking (SDN)

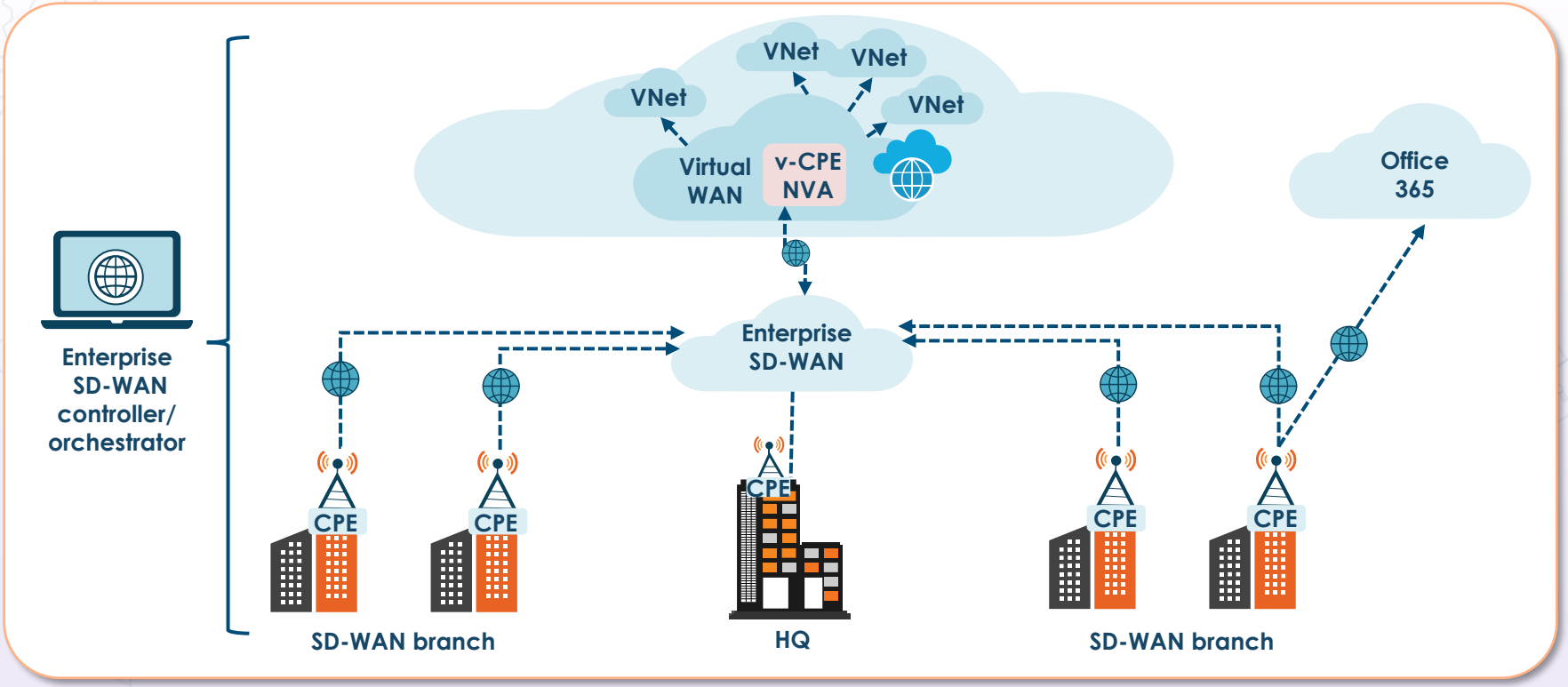


SD-WAN

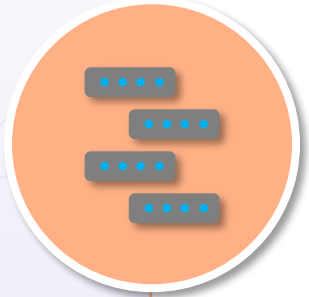


- Software Defined Wide Area Network is an SDN approach that raises network traffic management away from the hardware and premises to next-generation software in the cloud for superior agility, control, and visibility
- Incorporates a centralized control function with user-defined application and routing policies to deliver highly secure, robust, application-aware network traffic management

Microsoft SD-WAN Solution

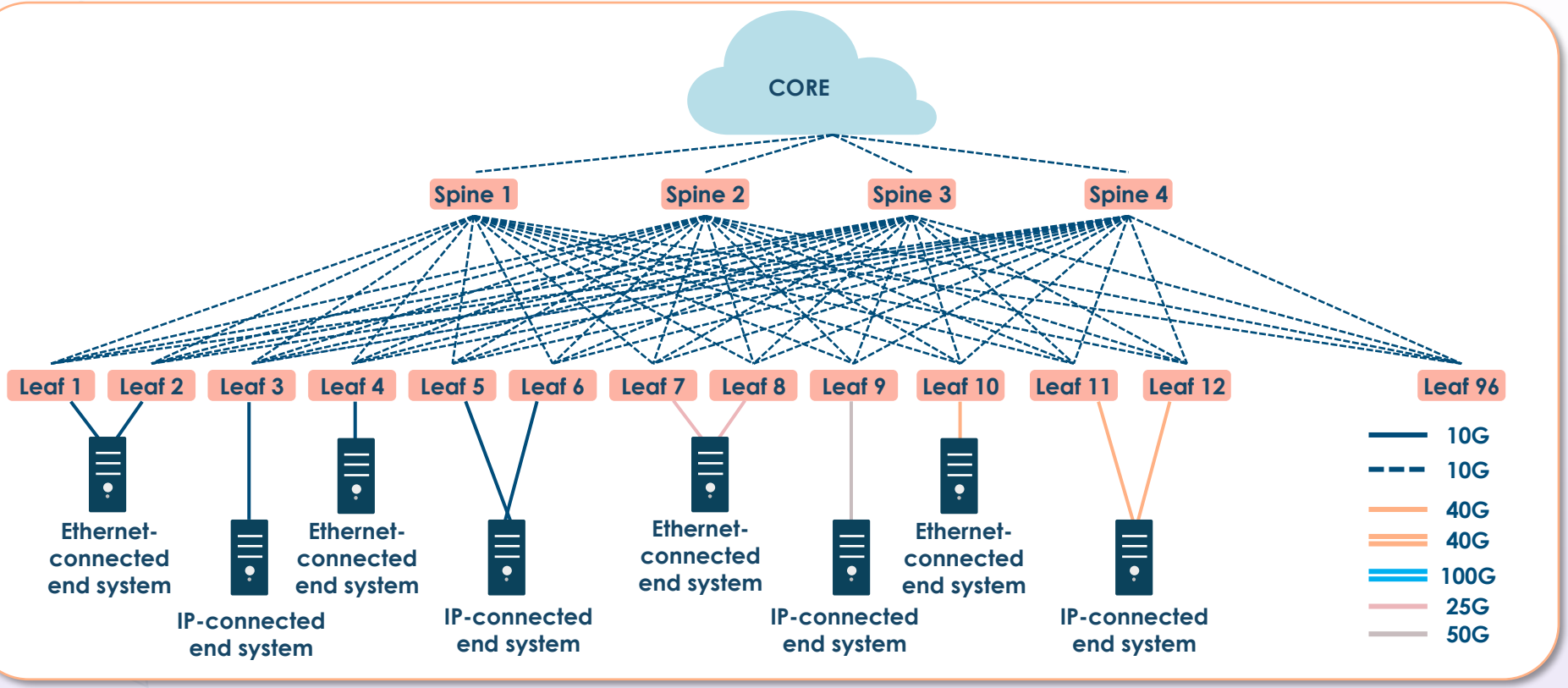


VXLAN

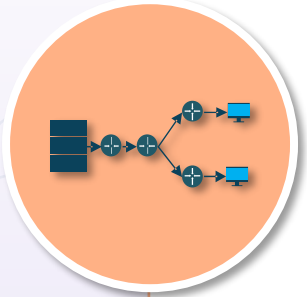


- VXLAN solutions from a variety of vendors decouple the physical hardware from the network map in order to support virtualization
- This uncoupling allows the data center network to be deployed programmatically
- It allows both Layer 2 and Layer 3 transport between VMs and bare-metal servers
- Has a much larger scale than traditional VLANs

VXLAN Architecture

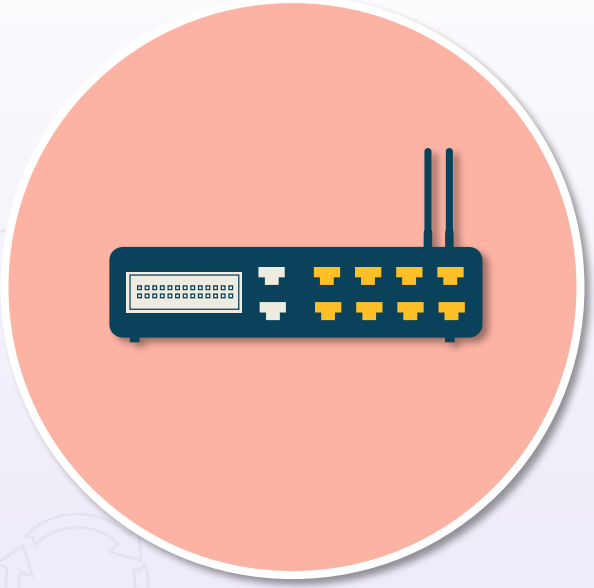


Switch and Layer 2 Security



- Switch port security as a base configuration on all layer 2 devices
  - Hard code access and trunk ports
  - Mitigate MAC flooding attacks
  - Enable PortFast and auto-recovery
  - Loop prevention and flood guard techniques
- Deploy VLANs and PVLANs to enforce a Layer 2 trust model and compartmentalization
- DHCP snooping, DAI, IP SourceGuard
- Protect any dynamic trunking protocol, like VTP
- IEEE 802.1X PNAC and 802.11AE MACsec are critical features
  - MACsec uses AES-GCM-128/256 with GMAC – this is an AEAD

Wireless LAN Controller Security



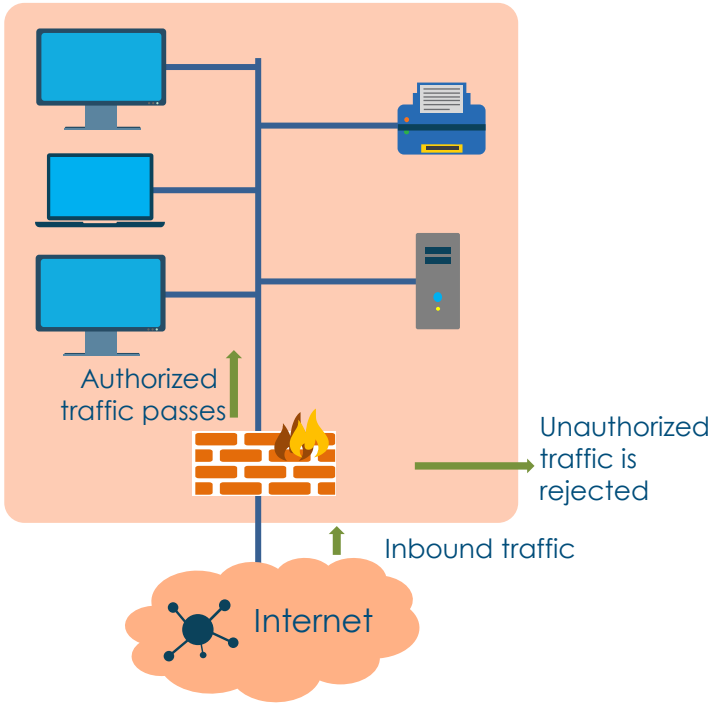
- WLCs have a "session level" access control for management protocols and MFP features
  - All interactive management traffic to the controller will be done through HTTPS/SSH (encrypted)
- Control Plane Policing and CPU ACLs control the control plane and which devices can talk to the main controller processor
- Network IDS/IPS solutions
- SIEM and log event correlation
- Locate rogue radios and access points

Secure Routers

- Network Address Translation
- Infrastructure Access Control Lists (ACLs)
- Unicast and Multicast Reverse Path Forwarding
- Integrated and modular L2-7 next-generation firewall and intrusion prevention services (IDS/IPS)
- VPN gateways for TLS and IPsec
- URL filtering and caching
- Integration with various cloud security services (web, email, DLP, anti-malware)
- Coordinate with Managed Security Service Providers (MSSP)

Firewalls

- A firewall is a metaphor representing software and/or hardware controls that can limit the damage spreading from one subnet, VLAN, zone, or domain to another
- It is typically deployed as a barrier (zone interface point) between an internal (trusted) network and an external (untrusted) network
- They are integrated systems of threat defense functioning at layers 2-7 and can be categorized as network or application firewalls



Next-generation Firewalls

Layer 5-7 policies

Also called DPI and AVC

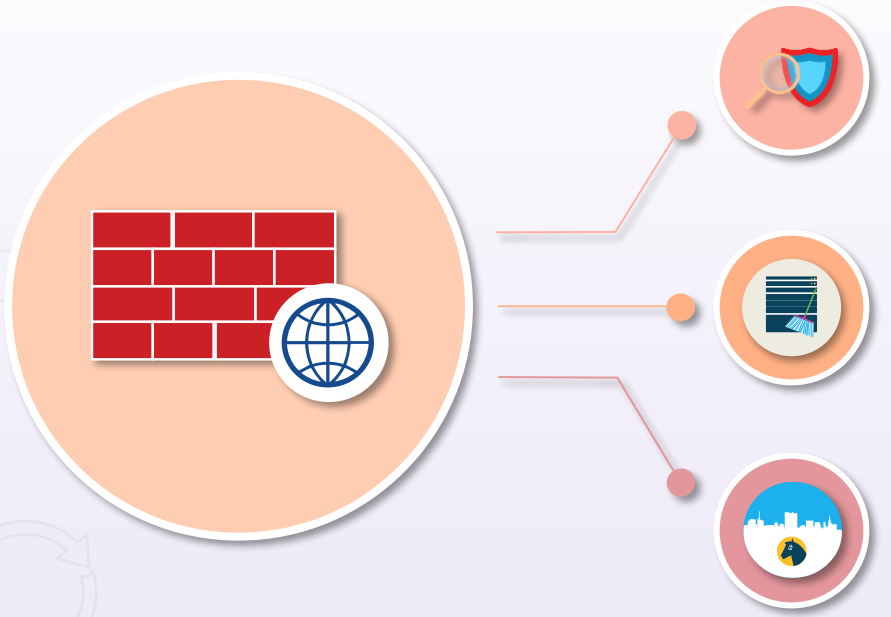
Authentication proxies

Interactive and transparent

Identity services

For ABAC engines and IdM

Next-generation Firewalls



Integrated IDS/IPS

Modular and cloud-based IPS

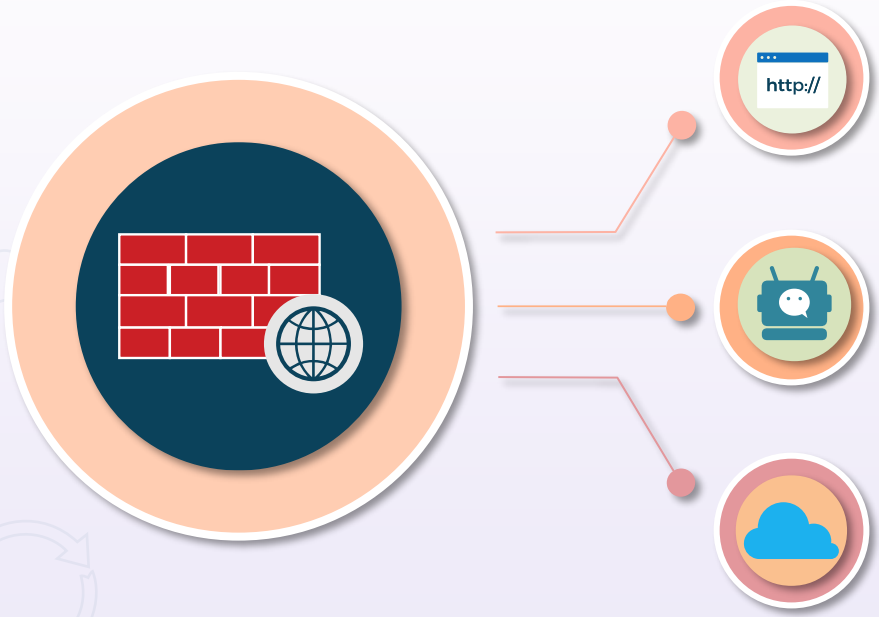
Content security

With data loss prevention (DLP)

Advanced malware protection

Cloud-based solutions

Next-generation Firewalls



URL filtering

To enforce AUPs

Botnet filtering

DNS-based Anti-DDoS protection

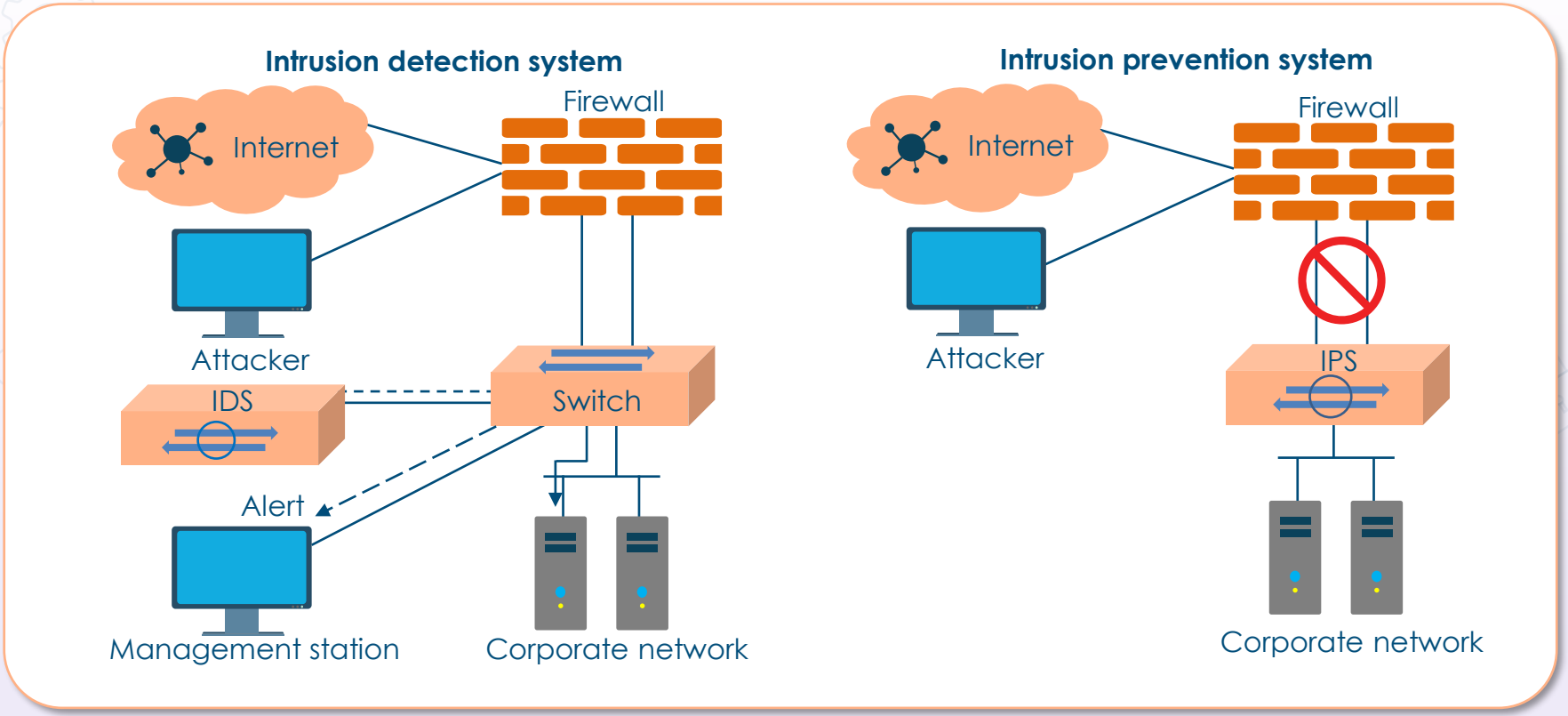
Cloud correlation and participation

Sec-as-a-service (MSSP) integration

Web Application Firewall (WAF)

- An appliance (physical or virtual), server plugin, or filter that applies a set of rules to an HTTP or HTTPS conversation
- Typically, these rules cover common web attacks, such as cross-site scripting (XSS) and SQL injection
- Typically deployed as dynamically configured WebACLs and Anti-DDoS engines with other threat management services
- The AWS WAF can be deployed on an elastic application load balancer, CDN distribution, or API gateway

IDS vs. IPS


Intrusion detection system
Internet
Firewall
Attacker
IDS
Switch
Alert
Management station
Corporate network
Intrusion prevention system
Internet
Firewall
Attacker
IPS
Corporate network

Intrusion Prevention Services (IPS)

- Inline IPS or monitor (passive mode)
- In-band vs. OOB
- Signature-based
- Anomaly-based
- Heuristic/behavioral-based (ML)
- Cloud-based (NGIPS)
- Network or Host-Based

IPS Actions

- Alerts and alarms
- Verbose dumps
- TCP resets
- Drop packets or addresses
- Blocking (shun) on firewalls and routers
- SNMP traps
- Logging to Syslog and SIEM systems
- Flows to NetFlow collectors

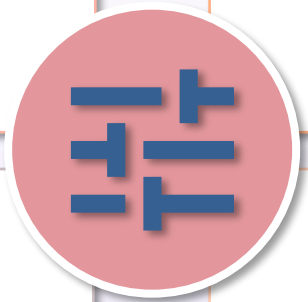
IPS Tuning

True positive

True (accurate) + positive (action taken)

False positive

False (error) + positive (action taken)



True negative

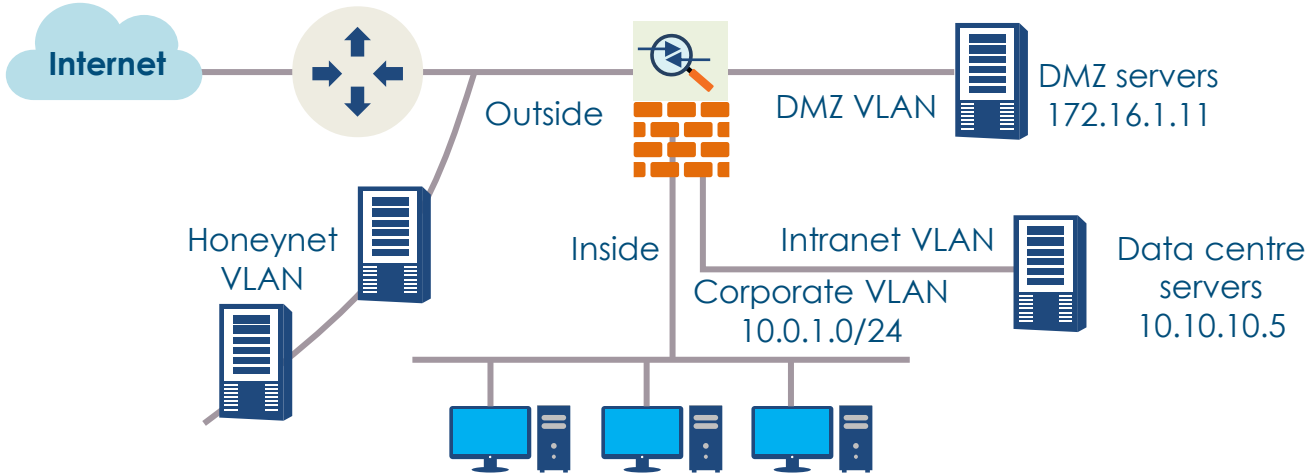
True (accurate) + negative (action not taken)

False negative

False (error) + negative (action not taken

Honeypots and Honeynets

- Honeypots and honeynets are isolated systems, sites, and services with data that appear to be valuable to an attacker
  - Entice potential malicious users to connect (internal or external)
  - Track and log all traffic to and from the honeypot
  - Run IDS services and other next-generation cloud-based analysis
  - Perform active defense procedures



Active Defense

- DECEPTION
- ATTRIBUTION
- COUNTERATTACK

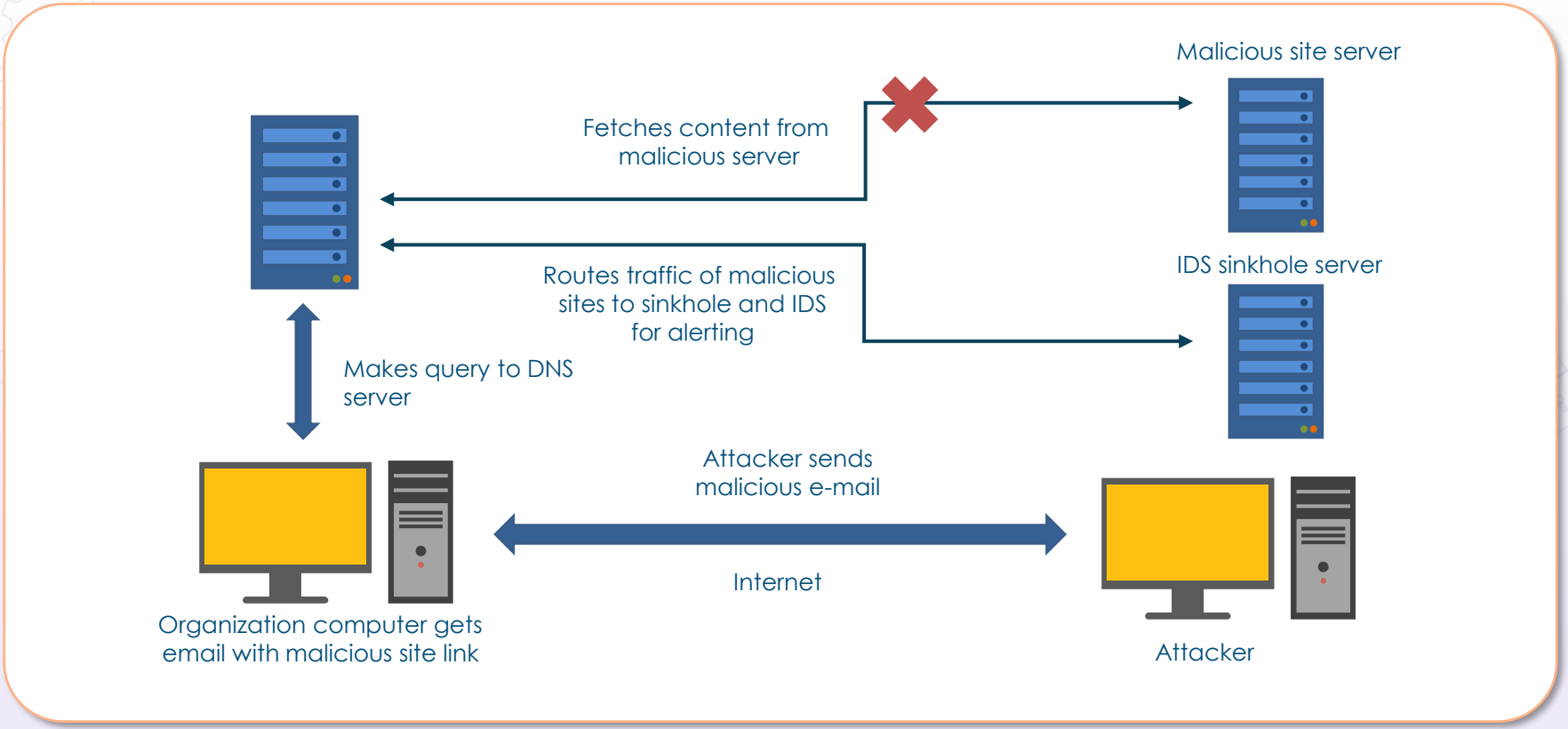
Deception: Fake Telemetry

- Deception is the first and most common phase of active defense used by many organizations
- Fake telemetry involves augmenting existing enterprise tools to offer critical threat intelligence for early breach detection and high-fidelity alerting
- Making tools available on honeypots and honeynets for attackers to use in order to attribute and attack back

Deception: DNS Sinkhole

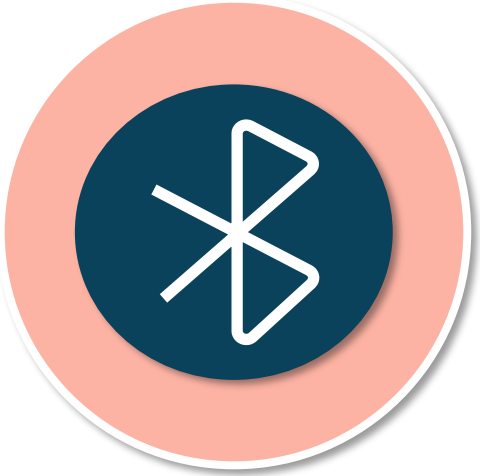
- DNS sinkhole (or black hole DNS) is used to spoof DNS servers to prevent resolving hostnames of specified URLs
  - This can be accomplished by configuring the DNS forwarder to return a false IP address to a specific URL
- It can be used against attackers to slow them down in a honeynet deployment and then possibly perform active defense attribution techniques
- Can also be used to prevent access to malicious URLs at an enterprise level for internal users

DNS Sinkhole



Wi-Fi Protected Access 2 (WPA2)

The de facto standard

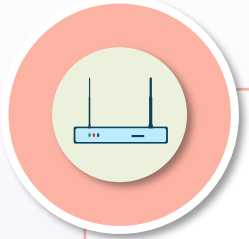


- The replacement for the temporary WPA (2004)
- Devices require testing and certification from Wi-Fi Alliance (2006)
- Supports Personal (PSK) and Enterprise modes
- Uses Counter Mode Cipher Block Chaining Message Authentication Code Protocol

WPA2 Modes

WPA2 Personal

- Shared secret key is a static key used to add challenge and response during AP and client association
- Manually configured on devices and AP
- Local access controls
- AES used for encryption (replaced WPA TKIP)



WPA2 Enterprise

- Centralized authentication server is required
- AES used for encryption (replaced WPA TKIP)
- RADIUS used for authentication and key distribution
    - EAP-TLS/EAP-TTLS
    - EAP-FAST
    - PEAP

CCMP Encryption

- Used with WPA2 as part of IEEE 802.11i standard
- Designed as the replacement for WEP and any interim solution (TKIP) using AES
- Provides strong message encryption with CCM
- Uses 48-bit initialization vectors and 128/256-bit keys
- Provides authenticity and integrity checking with CBC-MAC

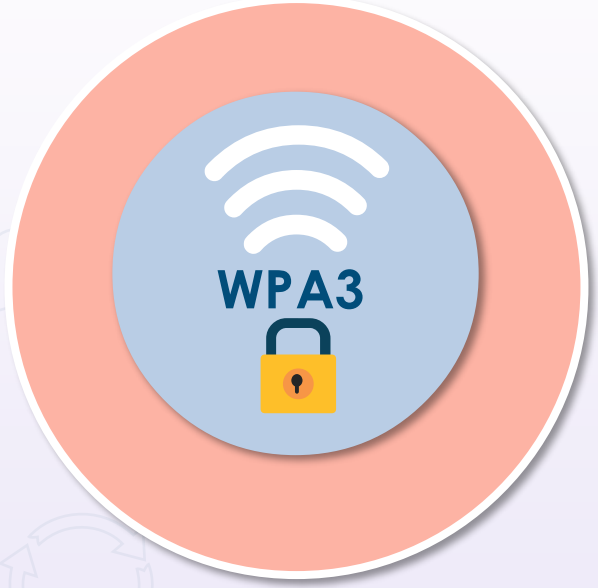
802.11 EAP Variants

802.1x EAP types feature/benefit	MDS … Message digest 5	TLS … Transport-level security	TTLS … Tunneled transport-level security	PEAP … Protected transport-level security	FAST … Flexible authentication via secure tunneling
Client-side certificate required	No	Yes	No	No	No (PAC)
Server-side certificate required	No	Yes	No	Yes	No (PAC)
WEP key management	No	Yes	Yes	Yes	Yes
Rogue AP detection	No	No	No	No	Yes
Provider	MS	MS	Funk	MS	Cisco
Authentication attributes	One way	Mutual	Mutual	Mutual	Mutual
Deployment difficulty	Easy	Difficult (due to client certificate deployment)	Moderate	Moderate	Moderate
Wi-Fi security	Poor	Very high	High	High	High

WPA3

- All WPA3 networks use the latest security methods, disallow outdated legacy protocols, and require the use of Protected Management Frames (PMF)
  - PMF enhances privacy protections already in place for data frames with mechanisms to improve the resiliency of mission-critical networks
- Authenticated encryption: GCMP-256
- Key derivation and confirmation: 384-bit HMAC with Secure Hash Algorithm (HMAC-SHA384)
- Key establishment and authentication: ECDH and ECDSA (384-bit)
- Robust management frame protection: 256-bit Broadcast/Multicast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256)

WPA3 Personal



- Natural password selection – lets users choose passwords that are easier to remember with SAE
- Ease of use – provides enhanced protections with no change to the way users connect to a network
- Forward secrecy – protects data traffic even if a password is compromised after the data was transmitted

Simultaneous Authentication of Equals (SAE)

- Originally implemented as 802.11s
- Password-based authentication
- Password-authenticated key agreement
- WPA3 replaces PSK with SAE
- More secure initial key exchange

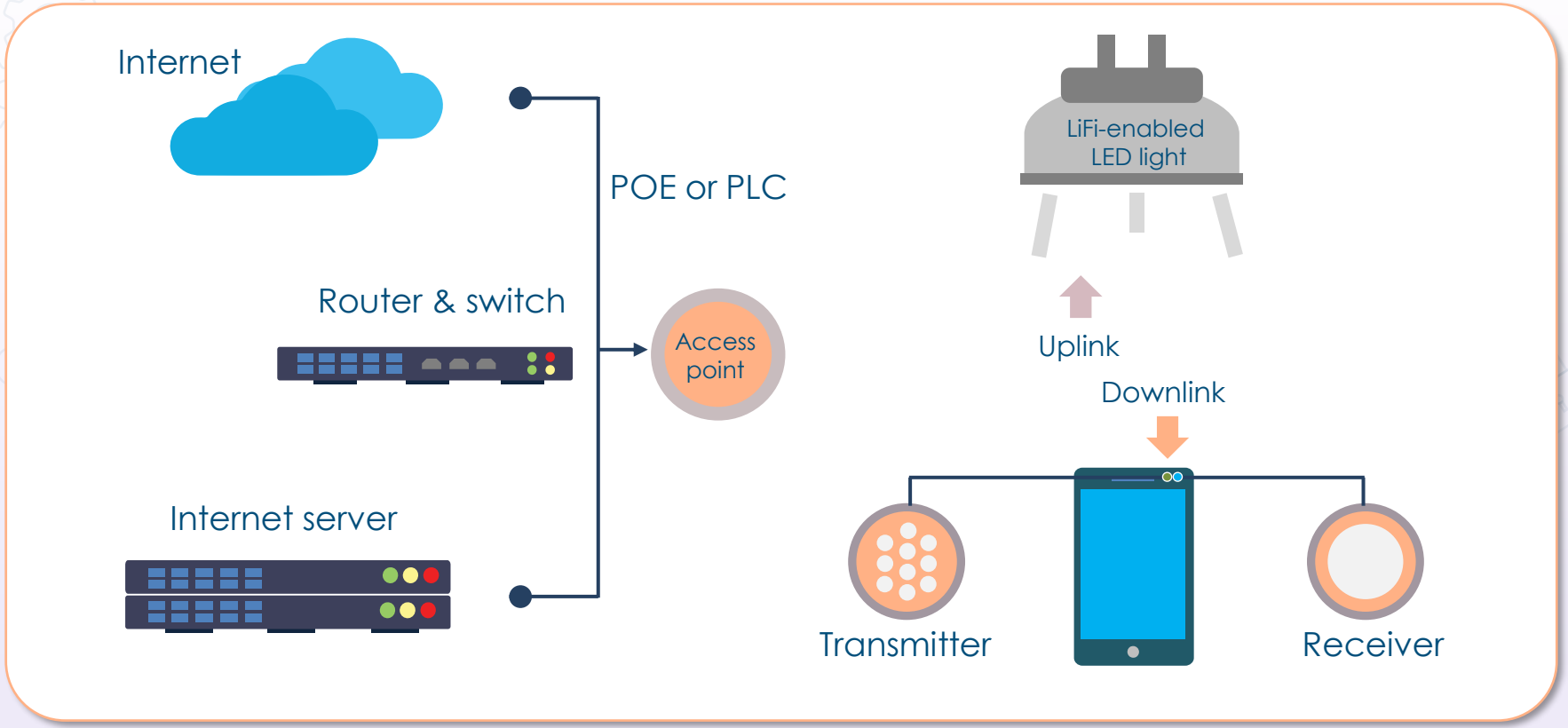
Dragonblood Attack

- Vulnerability in WPA3 discovered by the same researcher who discovered the KRACK attack on WPA2
- Exploit of the Dragonfly handshake protocol of WPA3
- If successful, an attacker within the range of a victim's network could recover the Wi-Fi password and infiltrate the target network
- Is in fact a collective of 5 attacks: 1 DoS, 2 downgrade attacks, and 2 side-channel information leaks

LiFi (802.11 bb)

- LiFi is a mobile wireless technology that uses light instead of the RF spectrum to transmit data
- Supported by a global consortium of companies driving a next generation of wireless to integrate into the 5G core
- LiFi is simpler than wireless and uses direct modulation methods akin to those used in low-cost infrared devices like remote control components
- LED light bulbs have high intensities and therefore can achieve very large data rates

LiFi (802.11 bb)



Zigbee (IEEE 802.15.4-2011)

PAN Technology

- Zigbee components can connect and communicate using the same IoT language
- Millions of Zigbee products are already deployed in smart homes and commercial buildings
- The network topology is a self-forming and self-healing mesh
- Ranges are up to 300+ meters (line of sight) and up to 75-100 meter indoors
- Supports AES-128 at Network Layer and the Application Layer

Cellular Networks

- Used in hotels, airports, and other commercial scenarios to gather credentials or registration profiles before users can access a public Wi-Fi
- 5G is the next generation of global networking
  - All 5G devices in a cell are linked to the Internet and telephone network by radio waves through a local antenna in the cell
  - The goal is to deliver bandwidths up to 10 Gbps by using higher-frequency radio waves than current cellular networks
- Cell phone and other devices should be part of enterprise mobility management
  - Works with vendors, carriers, and end-users for policy adherence

Satellite

- Mobility solutions, GPS, unnumbered IoT devices, and even electrical grids and other power suppliers commonly rely on satellites for operational continuity
- Uplinks and downlinks are often sent through open telecom network security protocols that are effortlessly accessed by attackers
- Satellite ground stations are principally vulnerable to threat actors
- All military-grade satellite communications are subject to all Commercial Solutions for Classified (CSfC) requirements, including dual tunnel encryption and other packages

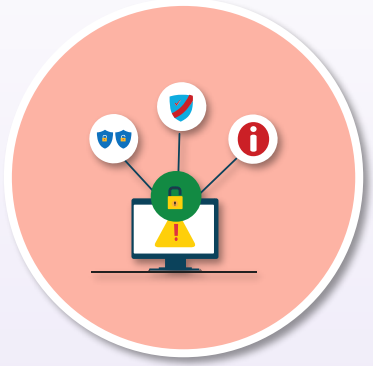
Satellite

- Network security infrastructure authenticates communications at every phase of data transmission that gets sent to the earth-bound devices before it goes to the satellite
- Trusted computing technology can ensure trustworthiness of devices, device identity and security validity, using cryptographic keys
- Geofencing and geotagging are facilitated by satellite technology

Acceptable Use Policies

- The most important aspect of the written security policy from the customer perspective is the Acceptable Use Policy (AUP)
- Endpoint security must begin with security awareness of the employee and contractor responsibility
- An AUP is a document specifying constraints and practices that a user must agree to for access to a corporate network or the Internet
- It is often divided into different sections based on various categories of access
- There should always be an enforcement mechanism in place to support the policy

Endpoint Physical Security



- Lock computers and laptop docking stations
- Screen savers with strong passwords
- Disable unused ports and peripherals
- Enforce removable device AUP
- Use MFA with biometrics if feasible

Endpoint Physical Security

- Implement a clean desk policy
- Provide locking cabinets and closets
- Remove/disconnect devices at end of day
- Protect printers, fax, and multi-function devices
- No piggybacking/tailgating policy

End User Participation

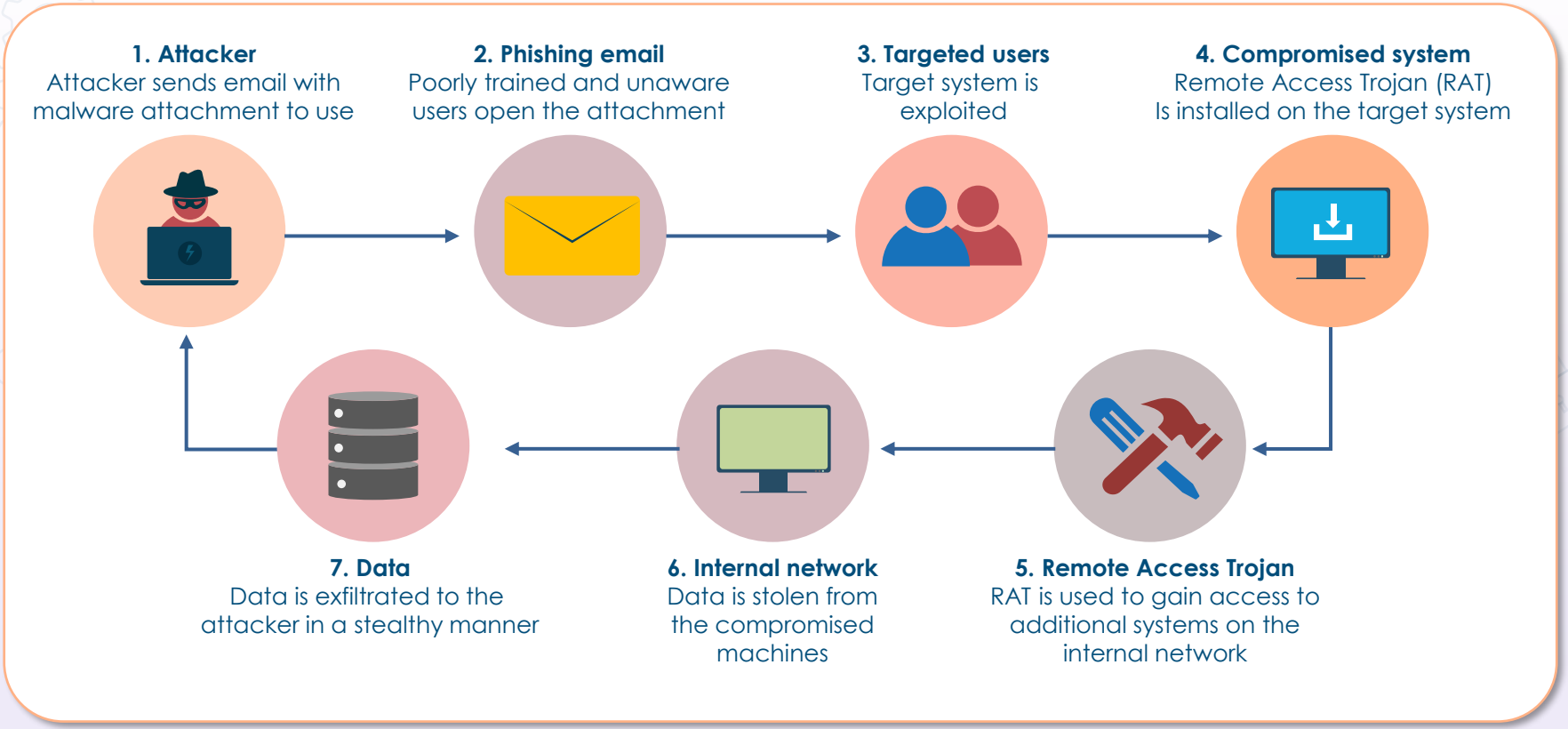
- End users will have varying degrees of participation in hardware, firmware, and software updates and upgrades
- If fully automated, the user may only be able to postpone (snooze) the process for a maximum amount of time
  - OS updates, WSUS, Silverlight, KACE, etc.

Personal Security Suites

Security suites

- These are all-in-one, full-scale security packages that offer a single, integrated solution
- There is only one vendor to get the upgrades and updates from
- Depending on the security vendor, the suite may also include a two-way firewall, parental control system, a local spam filter, VPN to protect your data in transit, online backup, and dedicated ransomware protection
- Best practice is to install two products from different vendors (e.g., Sophos + Malwarebytes)

Email Is the Prime Target



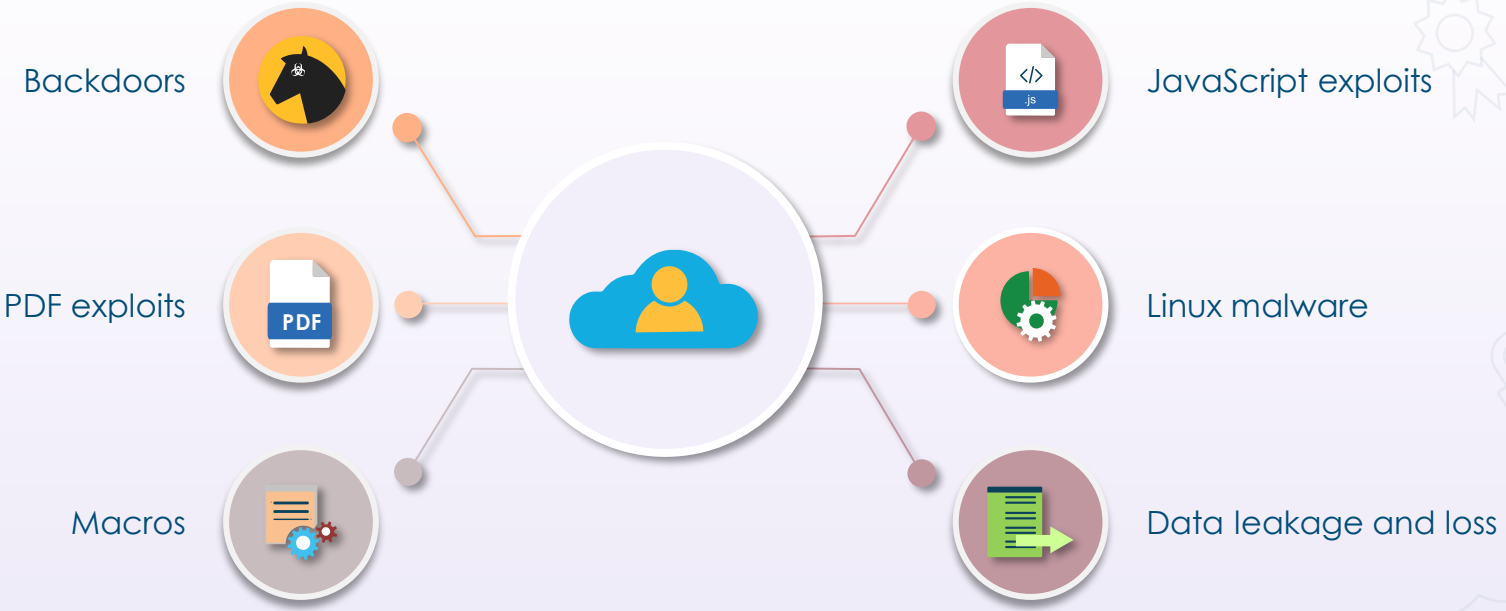
Securing Email and Webmail

- Use rotating passwords that involve four random words separated by "-" or "."
  - For example, texmex-world-glove-listen
- Implement strong malware scanners and spam filters
- Never reply to spam or click any "unsubscribe" links, as this will only confirm to the spammer that your email address is real
- Gain expertise in recognizing phishing emails
- Corporate and business email compromise (BEC) is on the rise
- Conduct awareness programs
- Use "two-tier" or multi-factor authentication when logging on to your email and webmail, if available

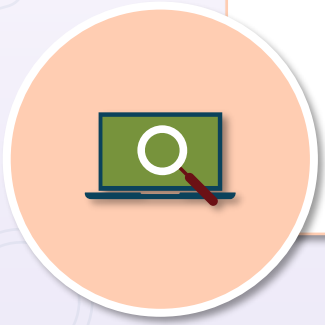
Securing Email and Webmail

- Before opening an attachment, make certain that you know who it's from and that you are expecting it
- Consider a confirming SMS text or phone call
- Only send personal information over email when necessary
- Use encrypted email where possible
- Avoid using email over free Wi-Fi

Personal Cloud Storage Vulnerabilities



Endpoint Detection and Response (EDR)



- Evolved from early HIDS solutions
- A "lighter" software agent installed on the host system often provides the basis for event monitoring and reporting
- EDR tools primarily focus on detecting and investigating suspicious activities and are indicators of compromise (IoCs) on hosts/endpoints
- EDR tools monitor endpoint and network events and send information to a SEIM system or centralized database so further analysis, investigation, and reporting can take place

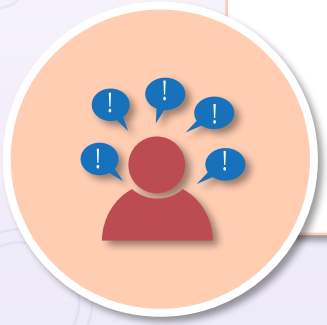
Key EDR Features

- Filtering – reduces alert fatigue and lowers the possibility for real threats to slip through unnoticed
- Advanced Threat Blocking – prevents threats the moment they are detected and throughout the lifecycle of the attack
- Incident Response Capabilities - threat hunting and incident response can help prevent full-blown data breaches (DLP)
- Multiple Threat Protection – cloud-based visibility into many finding categories

Next-generation Endpoint Protection

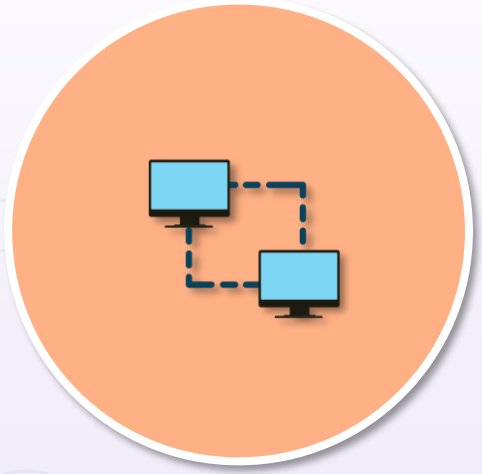
- Partner with an MSSP or CASB
- Advanced anti-virus with ML and AI
- Managed threat hunting (honey tokens)
- Cloud-based threat intelligence and User Behavioral Analytics (UBA)
- IT hygiene

Heuristics and Behavioral Analytics



- Most NGIPS and anti-virus systems use heuristic and ML mechanisms to achieve better results than traditional signature-based and anomaly-based solutions
- Heuristic engine used by an anti-malware/IPS program might include proactive rules and behavioral analytics to look for
  - a program that tries to copy itself into other programs (in other words, a classic computer virus), or
  - a program that tries to remain resident in memory after it has finished executing

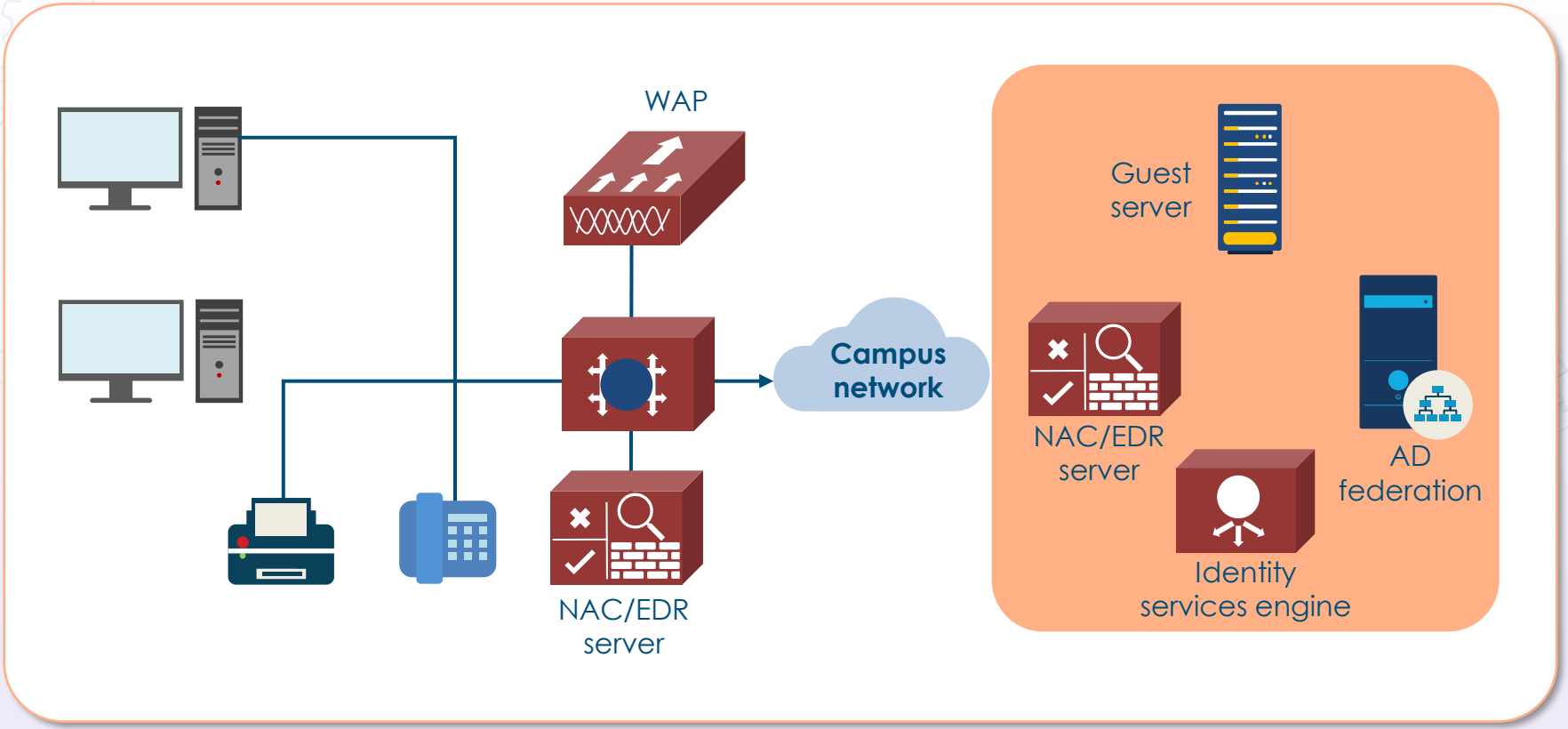
NAC and Endpoint Protection



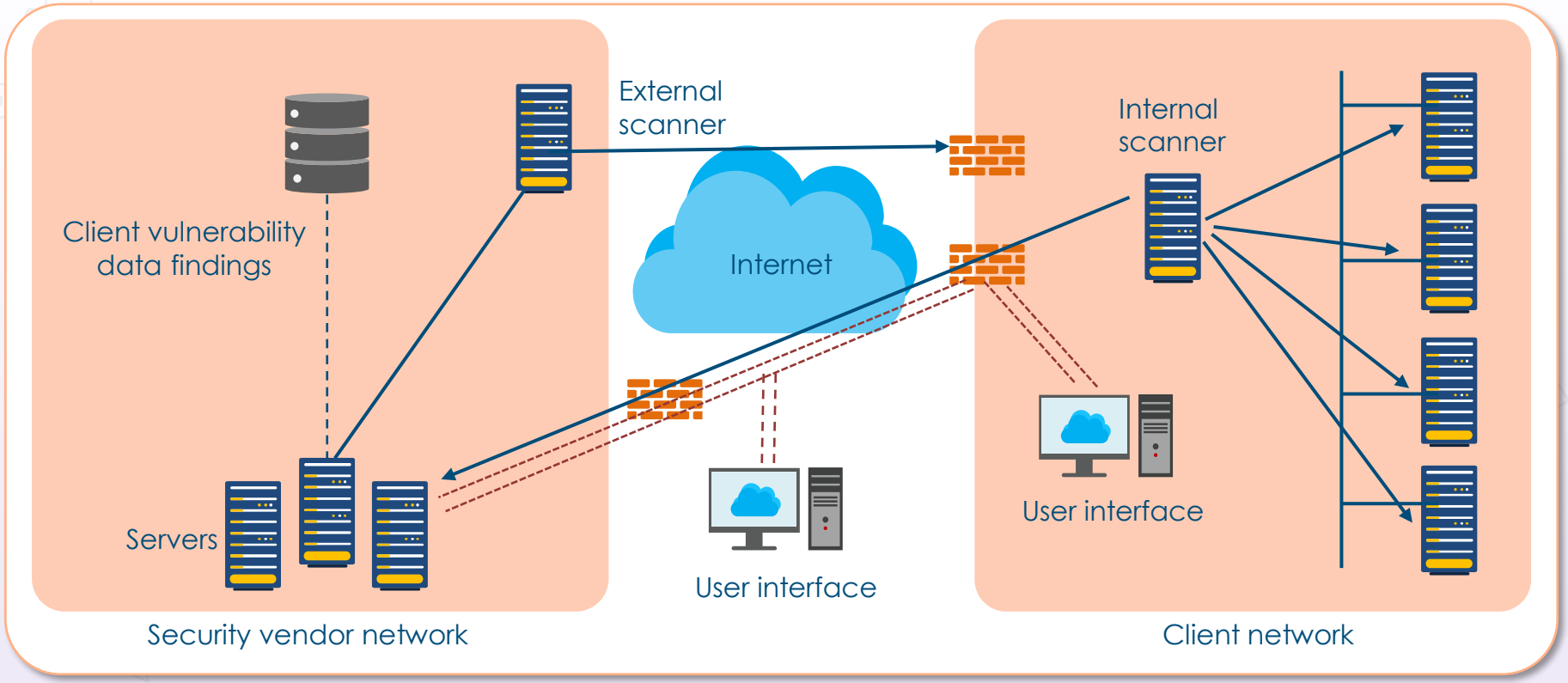
Network Admission Control (NAC) was an industry initiative sponsored by Cisco

- Cisco NAC and similar technologies are officially on the exam but have been replaced by newer solutions, such as TrustSec and Zero Trust Security
- It was part of the Cisco Self-Defending Network initiative and is the foundation for enabling NAC on Layer 2 and Layer 3 networks
- Do not trust anything inside or outside the perimeter without stringent authentication and verification
- Helps secure access from users and their devices, API calls, IoT, microservices, containers (Dockers, Kubernetes,) and more

Traditional NAC Solution



Cloud-based EDR

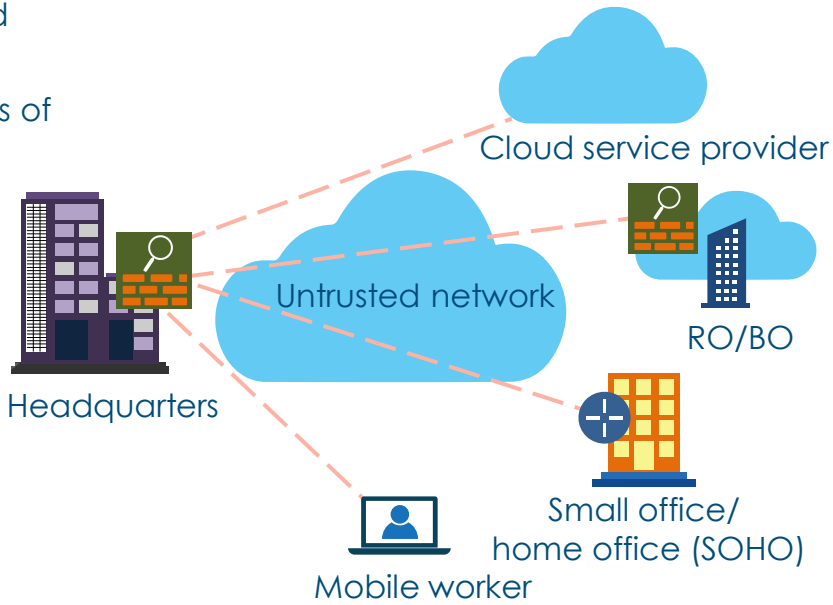


IPsec

- IP Security (IPsec) offers security services to traffic crossing untrusted networks, like the Internet, between two or more trusted devices or networks
- IPsec VPNs can also be used to protect management traffic as it crosses an organization's intranet and between front-end and back-end services
- IPsec is also popular when connecting to cloud service providers using managed site-to-site and peer-to-site VPN solutions
- IPsec is native to the IPv6 stack through the AH and ESP extension headers

IPsec

- IPsec and SSL VPNs are both cryptography-based VPNs
- In terms of deployment, there are two basic types of VPNs: site-to-site VPNs and remote-access VPNs
  - Remote access can be full-tunnel or clientless
- Operates in tunnel or transport modes
- Two main protocols are AH and ESP
- IPsec provides five essential security functions:
  - confidentiality (3DES, AES-128/256)
  - data integrity (SHA1, SHA2/3)
  - origin authentication using pre-shared keys or RSA/ECDSA signatures
  - anti-replay protection, and
  - key management (IKEv1/2, DHKE, ECDHE)



IPsec Security Suites

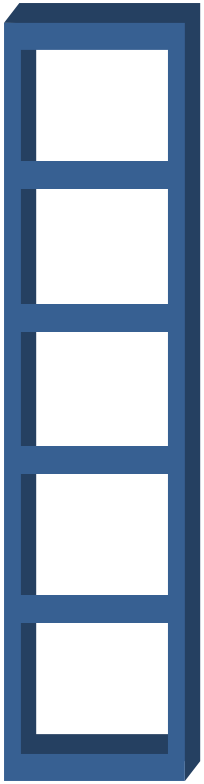
IPsec protocol

Confidentiality

Data integrity

Origin authentication

Key management



ESP | ESP +AH | AH

DES | 3DES | AES

MD5 | SHA-1 | SHA-2

PSK | RSA | ECDSA

DH | ECDH | IKE | IKEv2

SSL/TLS

SSL/TLS is the most ubiquitous certificate-based peer authentication in use on the Internet (HTTPS)

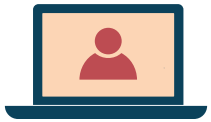
Transport Layer Security (TLS) is standardized by IETF

TLS 1.3 is the most recent published version

It is also used with SMTP, LDAP, and POP3

The only mandatory cipher suite includes RSA for authentication, AES for confidentiality, and SHA for integrity and digital signatures

Transport Layer Security (TLS)



TLS VPN tunnel

1 User makes a connection to TCP port 443

2 The server response contains server's public key

3 User software verifies signature on identity certificate, validating authenticity of public key

4 User software create a shared-secret key

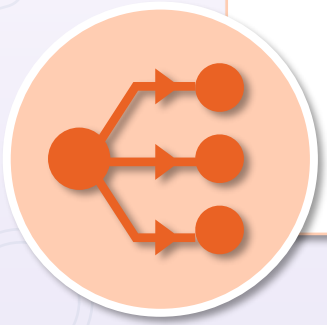
5 Shared-secret key, encrypted with public key of the server, is sent to the server

6 Bulk encryption occurs using the shared-secret key with a symmetric encryption algorithm

TLS Best Practices

- Prevent downgrade attacks from web clients
- Use HTTP Strict Transport Security (HSTS)
- Use the most recent security suites (no RC4 or DES/3DES)
- Do not let vendor-installed code intercept traffic
- Verify encryption
- Perform OCSP stapling from browsers to enforce certificate expirations
- Implement Certificate Pinning to trusted CAs

CSP Elastic Load Balancers

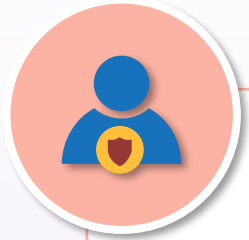


- Network or application load balancing
- Represents virtual network to the public
- Performs health checks on instances
- Produces flow logs
- Runs the TLS listener
- Can also have layer 3/4 and web application firewall (WebACL)

Need-to-know vs. Least Privilege

Need-to-know

- Originated in military and intelligence operations and pertains to data access and information flow
- Can be implemented using different access control models although MAC is the most secure
    - Lattice models are effective
    - Bell-LaPadula for confidentiality
    - Biba or Clark-Wilson for integrity

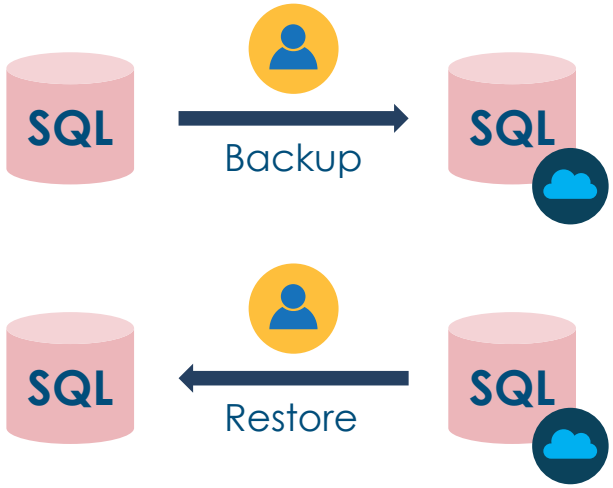


Least privilege

- Subjects are only given access to the objects they need and nothing else unless they go through/pass a strict approval process"
- Can be implemented using different access control models although MAC is the most secure
- Can use network operating system controls or ABAC for different scenarios

Separation of Duties

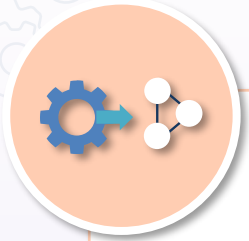
- Processes where more than one entity is required to complete a particular task
- Often involves dual operator principles as well where two subjects are needed to modify a particular object
- Automation and orchestration can help enforce this principle
- Rotation of duties is also a related principle
    - Example: forced (mandatory) vacations



Mediated Access

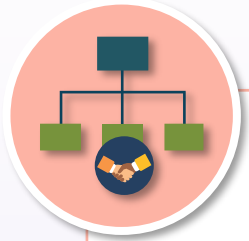
- This principle involves avoiding direct client-to-server access whenever feasible
- Uses various proxies for
  - authentication (interactive or transparent)
  - translation services (NAT)
  - bastion (jump) hosts and CSP services
  - web proxies for content and URL filtering, and
  - using managed security service providers (MSSP) and cloud access security brokers (CASB)

SLA vs. OLA



Service-level agreement

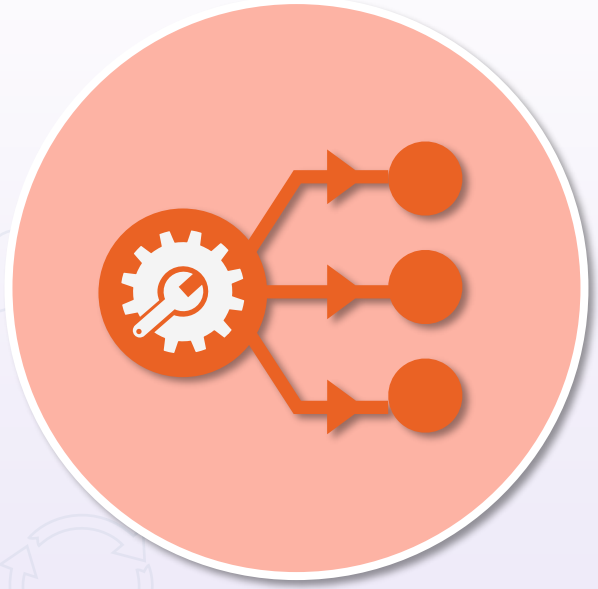
- Defines the precise responsibilities of the service provider and sets customer expectations
- Also clarifies the support system (service desk) response to problems or outages for an agreed level of service
- Should be used with new third-party vendors or cloud providers (SaaS, IaaS, PaaS) for 24-hour support



Organizational-level agreement

- Documents the pertinent information for regulating the relationship between internal service recipients and an internal IT area (service provider)
- Difference is what the service provider is promising the customer (SLA) vs. what the functional IT groups promise each other (OLA)
- An OLA often corresponds to the structure of an SLA, with a few specific differences based on the enterprise

Configuration Management



- 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
- Includes all relationships and dependencies between the CIs
- Objects include hardware, software, networks, sites, vendors, suppliers, and people

Configuration Management

- CM is a governance and systems life cycle process for ensuring consistency among all assets (configuration items, or 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

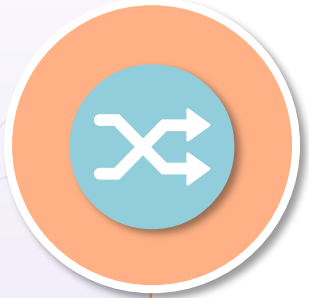
Configuration Management

- Directory Services tools
- Diagrams and topologies
- Inventory baselines
- Naming and tagging schemas

Configuration Management Database (CMDB)

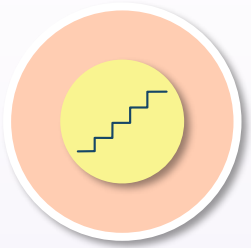
- A configuration management system (CMS) is a set of data, tools, utilities, and processes used to support configuration management
- All information should be tagged and labeled with a common unified schema, preferably using key-value pairs
- This data will populate a database system known as a CMDB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

Change Management



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

Types of Changes

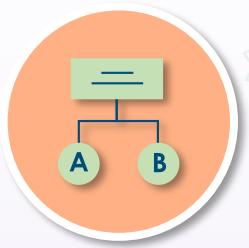


Standard

- Low-risk changes
- Pre-authorized and well-documented
- Can be automated
- Service requests that don't need additional authorization
- Example: changing directory password

Normal

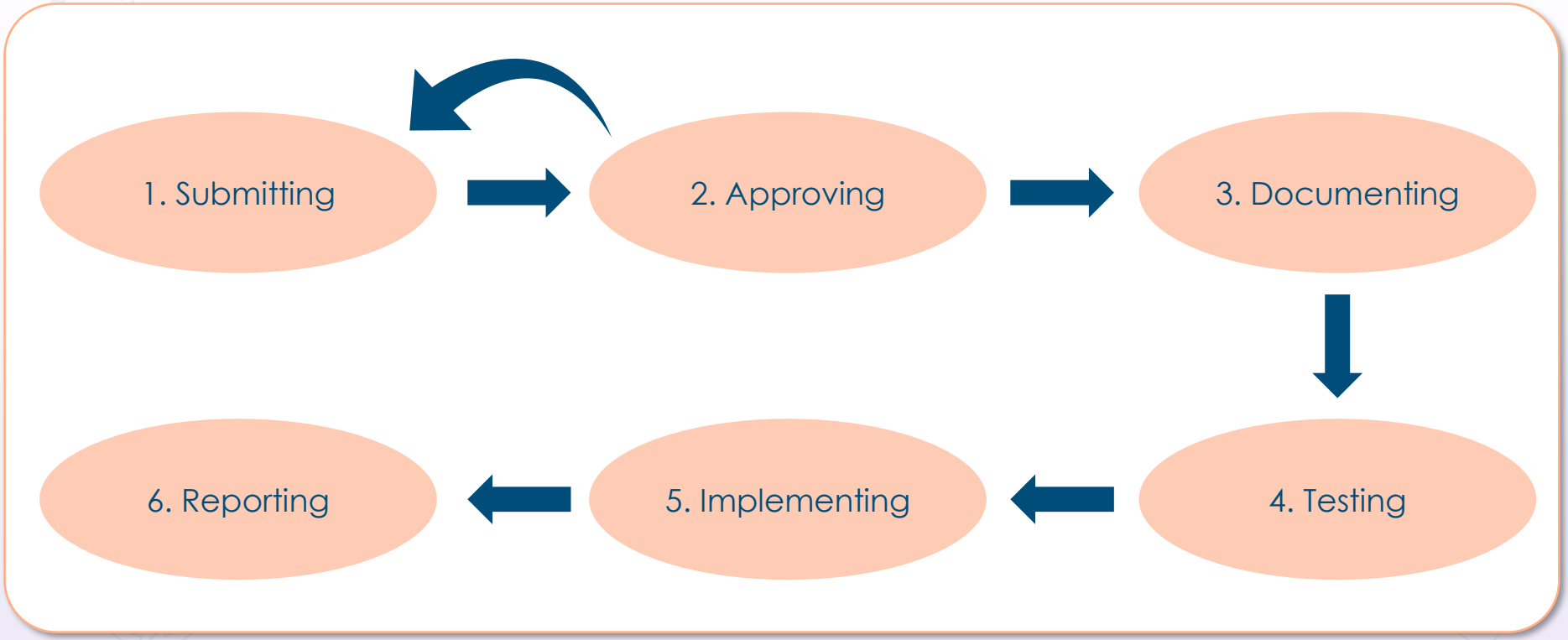
- Changes follow a specific process for scheduling, assessment, and authorization
- They are lower risk, but they do go through an approval process
- Example: onboarding a new phone or laptop; installing an application



Emergency

- Changes that must be implemented immediately
- Often a result of problem management or after-action reporting
- May involve escalation or an emergency advisory board if the amount of resources or disruption is significant

Change Management Lifecycle



1. Submitting

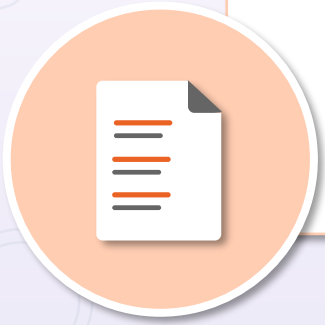
The proposed change is analyzed and validated. If necessary, the submitter may be required to provide more information before it is approved or escalate the change to a higher authority

2. Approving

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

3. Documenting

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

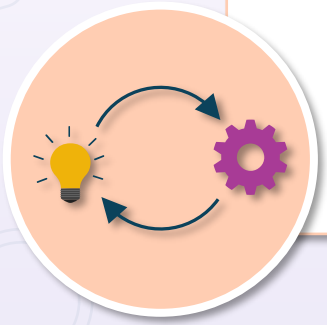


4. Testing

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

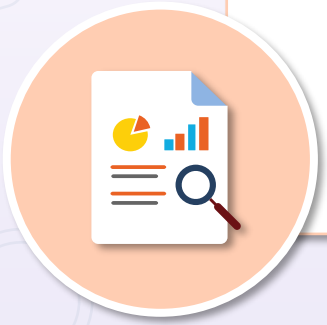
5. Implementing

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



6. Reporting

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

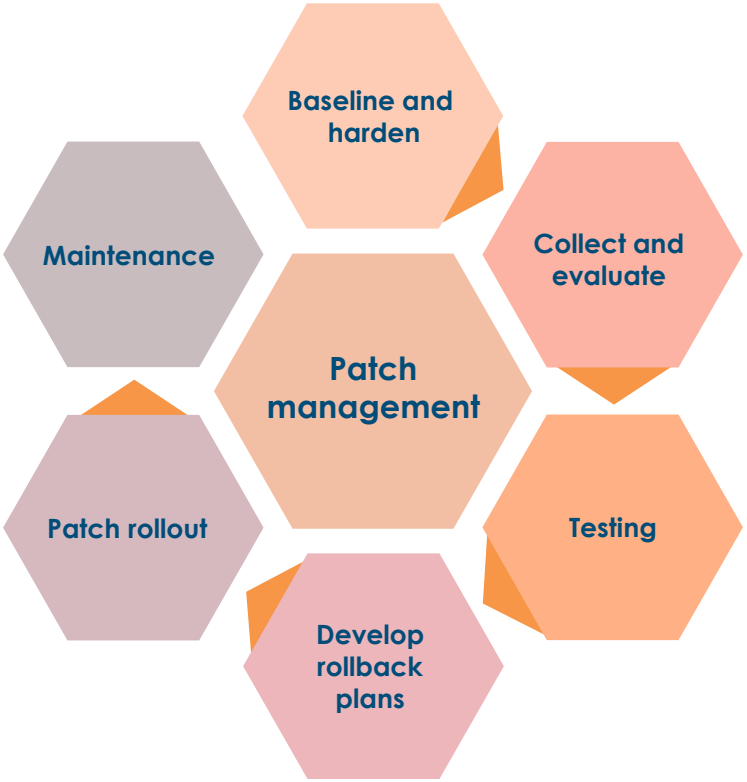


Patch Management

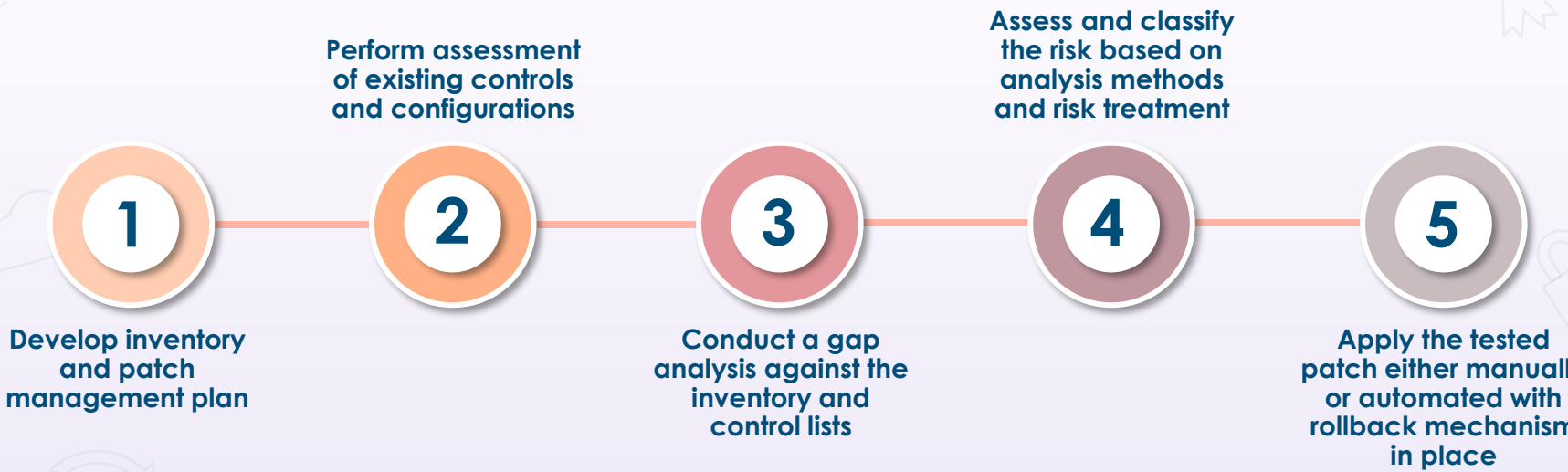
A critical control

- Many organizations do not consider or continually improve their patch management plan
- Vulnerability/exposure reviews and gap analysis are not performed or done properly
- A configuration management database (CMDB) of all configuration items (CIs) should be maintained
- 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



Patch Management Lifecycle



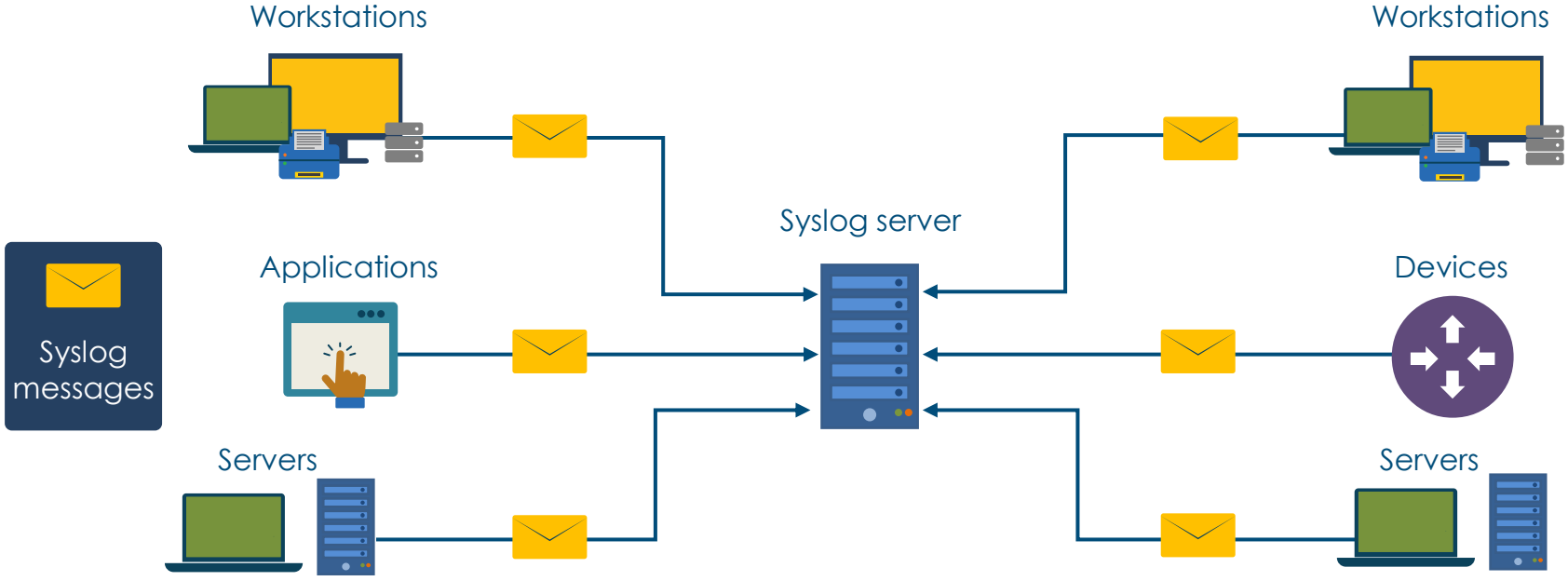
System Logging with Syslog

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

System Logging with Syslog

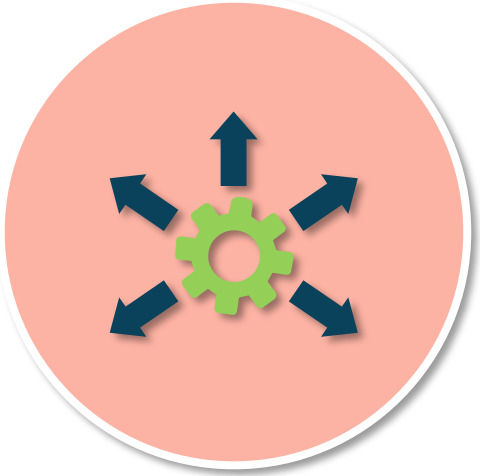
Code	Severity	Description
0	Emergency	System is unusable
1	Alert	Action must be taken immediately
2	Critical	Critical conditions
3	Error	Error conditions
4	Warning	Warning conditions
5	Notice	Normal but significant condition
6	Information	Informational messages
7	Debug	Debug-level messages

System Logging with Syslog



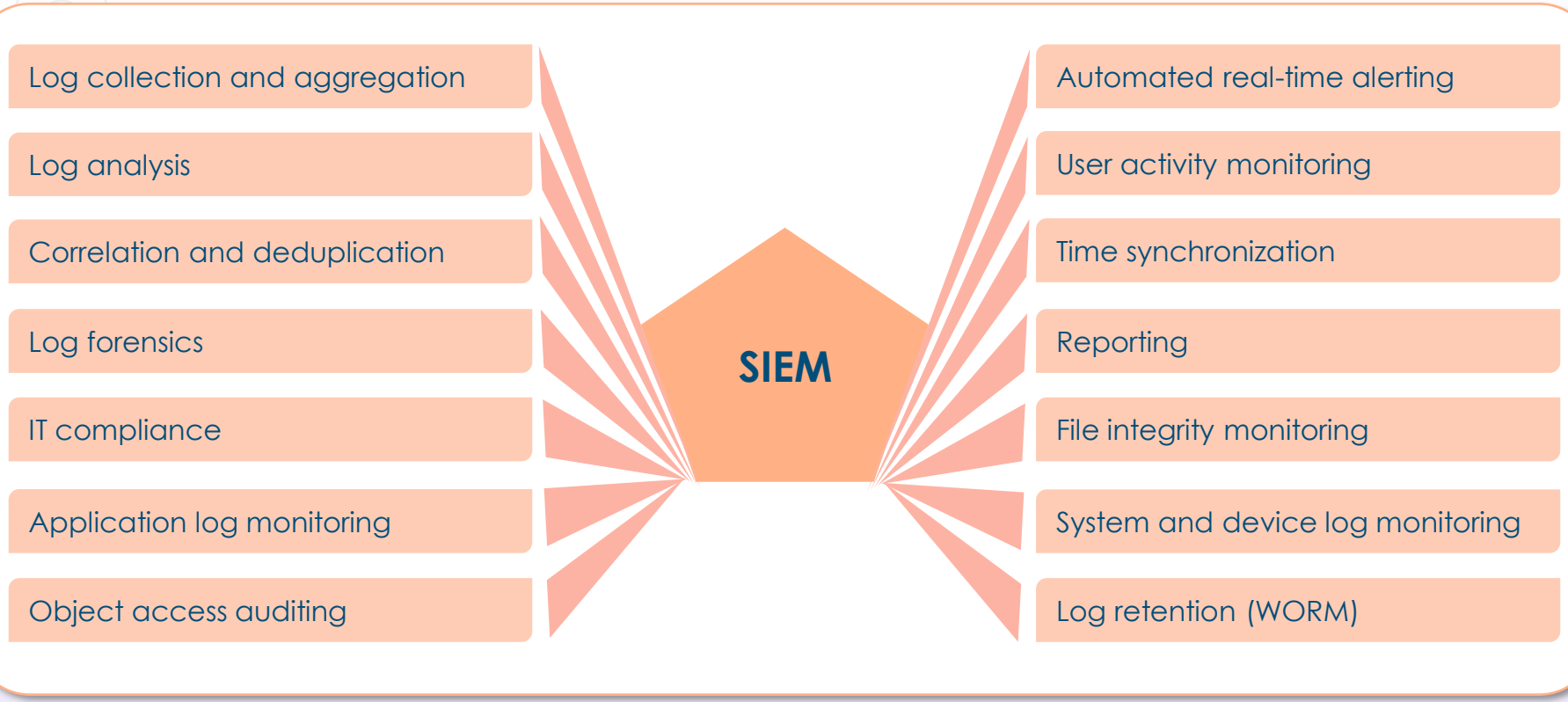
Security Information & Security Event Management

SIEM



- The term SIEM is a combination of security information management (SIM) and security event management (SEM)
- Centralize the storage and analysis of logs and other security-related documentation to perform near real-time analysis
- Can send filtered data to mining, big query, and data warehousing servers in a data center or at a cloud service provider
- Allow security and network professionals to take countermeasures, perform rapid defensive actions, and handle incidents

SIEM


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

Security Orchestration, Automation, and Response (SOAR)

- SOAR is an assortment of software services and tools
- It allows organizations to simplify and aggregate security operations in three core areas:
  - Threat and vulnerability management
  - Incident response
  - Security operations automation

4 Key SOAR Elements

1. SIEM use cases, categories, and SIEM Rules are mapped to incident categories and these categories are then mapped to playbooks

2. Three types of playbooks: Manual playbooks (a series of manual tasks); Semi-Automated playbooks (a hybrid of automated and manual subtasks); and Fully-Automated playbooks (completely automated)

3. Four types of Automation

a. Defensive Automation (anything that tries to prevent the threat or risk)

b. Forensic Automation (anything that tries to retrieve additional evidence)

c. Offensive Automation (anything pro-active that tries to investigate an asset)

d. Deception Automation (anything that retrieves or adjusts deception tools)

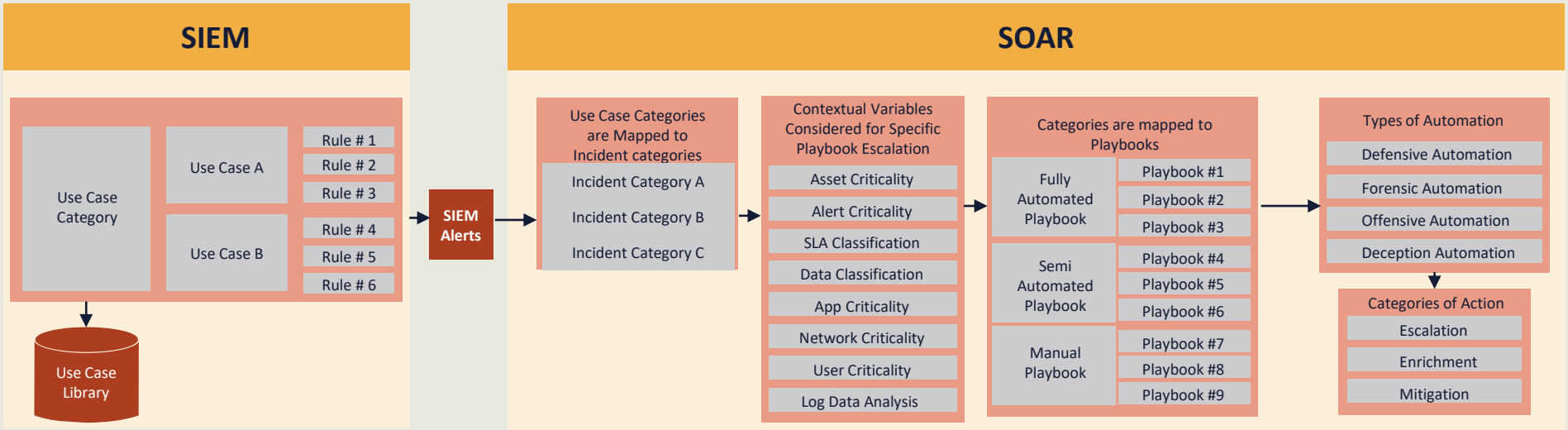
4. Three different categories of action

a. Enrichment (adding additional CMDB or environment data)

b. Escalation (e-mail, ticket escalation, SNS, chat/messaging communication)

c. Mitigation (the modification of device configuration)

SIEM AND SOAR



Vulnerability Assessment and Management

Define first!

- It should be quantified as a percentage of probability and not just a vague list of "scary things"
- The likelihood that a threat agent's actions will result in a loss (frequency and magnitude)
- It can be a derived value from threat capability of actors combined with the resistance of existing security controls

Vulnerability Assessment and Management

- All assets and asset classes must first be valued, prioritized, categorized, classified, and labeled accurately
- Recognize who has the role of Asset Manager (digital as well)
- Use all available tools and proven methodologies:
  - Inventory systems and various logs (system, application, firewall, etc.)
  - Simple Network Management Protocol (SNMP) traps
  - NetFlow collection
  - Security information and event management (SIEM) systems
  - Next-Generation Intrusion Prevention System (NGIPS) alerts and logs
  - Cloud-based visibility tools
  - Machine learning and artificial intelligence data analysis

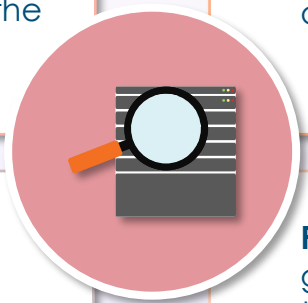
Expert Judgment

- Internal subject matter experts
- Risk register and lessons learned (LL) database
- Historical documentation
- Compliance experts
- External expert judgment
- Third-party consultants
- Cyber insurance providers
- Legal expertise

Vulnerability Intelligence Sources

Automated Indicator Sharing (AIS) is a DHS system for data sharing about cyber observables with the goal to maximize the near-real-time distribution of all relevant and actionable cyber threat indicators among the private sector and federal agencies for network defense

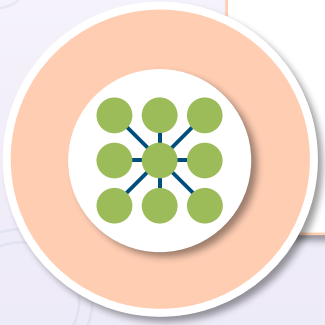
Structured Threat Information eXpression (STIX) is a structured language developed by MITRE for a collaborative way to represent cyber threat intelligence and observable data



Trusted Automated exchange of Indicator Information (TAXII) is a free and open transport mechanism that standardizes the automated exchange of cyber threat information. Push and pull messages are supported – supporting both subscription feeds and on-demand queries. TAXII leverages existing protocols when possible – with native support for HTTP and HTTPS

Predictive analysis and threat maps are generated by AI-driven and ML analysis tools, often working with cloud service provider managed services or MSSPs

Open-source Intelligence (OSINT)



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

Research Sources

- Vendor web sites
- Vulnerability feeds
- Conferences
- Academic journals
- Request for Comments (RFC)
- Local industry groups
- Social media
- Threat feeds
- Adversary tactics, techniques, and procedures (TTP)
- OSINT tools
- Emerging social media tools
- Word of mouth

Vulnerability Databases

Common Vulnerabilities and Exposures (CVE)

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

Common Vulnerability Scoring System (CVSS)

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

Vulnerability Scanning

- Vulnerability scanning is the process of using tools to identify known and unknown weaknesses in systems, applications, services, and policies
- Vulnerability scanning is an easier and often more focused process of 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
- HTTP/S is the most common traffic by far, and web application vulnerability scanners like Burp Suite and OWASP ZAP are popular
  - Cross-site scripting; cross-site request forgery; SQL, LDAP, and command injection; path traversal; insecure server configuration

Protocol Analyzers

- Devices that capture and analyze network traffic between two or more systems
- Traffic can be filtered and decoded to visualize what processes are occurring
- Can be used to find network bottlenecks, troubleshoot, and analyze malware behavior
- Advanced analyzers also generate statistics for trend analysis and network optimization
- Crackers can use them to gather information or even clear-text usernames and passwords, among other things

Exploitation Frameworks (EKs)

- Exploitation kits used by penetration testers and crackers to find vulnerabilities and attack vectors
- Often specialize in certain components, like routers, browsers, embedded devices, PowerShell, etc.
- Often open-source initiatives with broad cooperation from white, gray, and black hat hackers
- Can be used to prioritize vulnerabilities and threats in the enterprise
  - RIG EK and RIG-v EK
  - GrandSoft EK
  - GreenFlash Sundown

Compliance Scanners

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

Security Audits

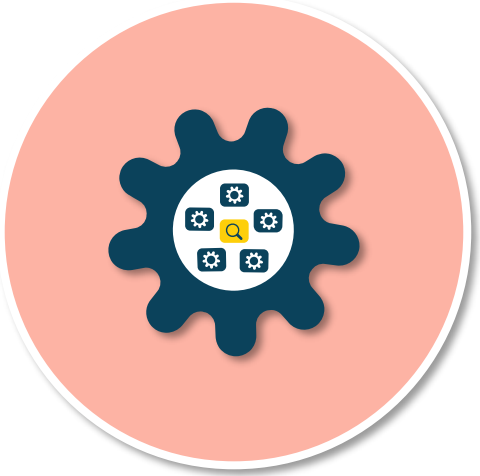
May be for compliance or to measure maturity against a model like CMM

- Internal vs. external
- In-house vs. third-party
- Vulnerability assessment
- Penetration testing
- Log reviews
- Synthetic transactions
- Code review and testing
- Misuse case testing
- Test coverage analysis

- Interface testing
- Account management
- Management review and approval
- Key performance and risk indicators
- Backup verification data
- Training and awareness
- Disaster recovery (DR) and business continuity (BC)

Penetration Testing

Will involve vulnerability assessments



- A more elaborate test in which assessors simulate real-world attacks to identify methods for evading the security features of an application, system, or network
- Often involves launching real attacks on real systems and data using attack tools and techniques
- Also be useful for determining the following:
  - 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' abilities to detect attacks and respond

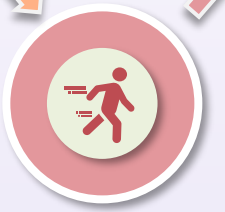
Penetration Testing

1: Rules of engagement agreement

2: Reconnaissance and initial engagement

3: Privilege escalation

4: Lateral movement and pivoting



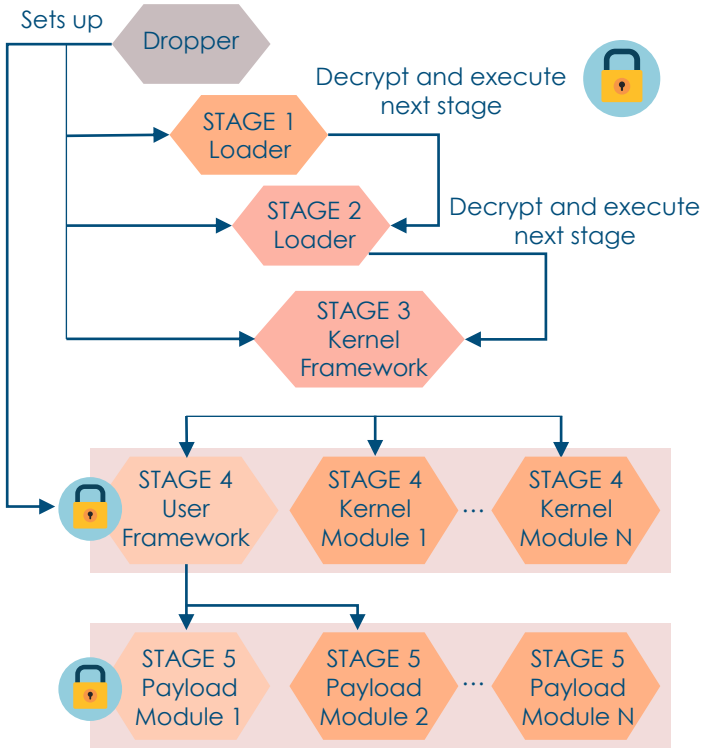
5: Persistence

Threat Hunting

- Also called "Hunt Teams"
- Threat hunting involves groups of cyber investigators aggressively seeking out threats on a network or system
- They are often compliance or regulatory auditors
- They attempt to quickly recognize anomalies and discover historic patterns in data and Indicators of Compromise (IoCs) to counter cybercriminals and mitigate threats
- **Can also be Red Team vs. Blue Team exercises**

Threat Modeling

- Involves creating an abstraction of a system to identify risk and probable threats (private cloud/sandboxing)
- When cyberthreat modeling is applied to systems being developed, it can lower vulnerabilities and risk
- With the widespread adoption of threat intelligence technologies, most enterprises are trying to adopt a threat-focused approach to risk management
- Provides visibility, increased security awareness and prioritization, and understanding of posture



Generating Reports

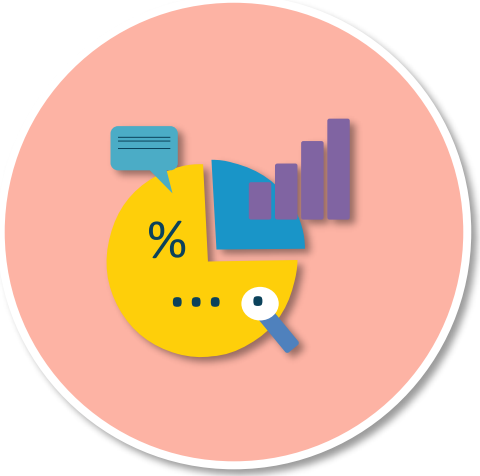
- Reports should have as much information as necessary but not a "data overload"
- May need to express in simpler terms or have different reports for different target audiences
- Dashboards are very effective (R programming)
- Understand components of visual communications
  - Avoid three-dimensional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

Incident Response

- Steps taken when a negative event disrupts normal operations
- Primary goal is to reduce the immediate impact
- Should have documented incident types/category definitions based on risk assessments, risk registers, and business impact analysis (BIA)
- Know roles and responsibilities of the first responders, including reporting requirements and escalation processes
- Collect contact lists, public relations people, and legal teams
- Best practice is to have pre-performed exercises, drills, and simulations

Incident Response Lifecycle

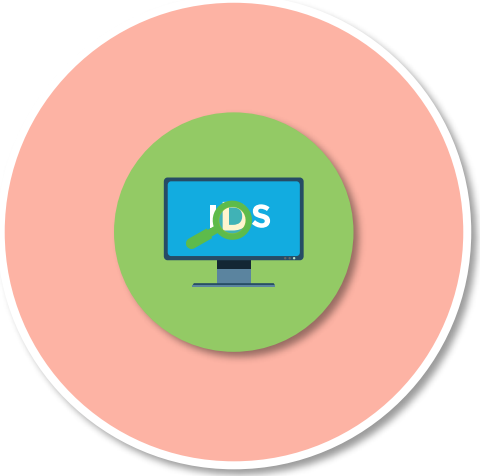
Preparation



- Involves all information gathering, missions, charters, and project initiation tasks
- Get buy-in and funding from executive management in order to know the scope of the response plan
- Establish incident response teams
  - Determine the roles and responsibilities of internal employees on incident response teams
- Establish first responders and processes for communication to relevant stakeholders
- Conduct IR exercises and drills based on budget

Incident Response Lifecycle

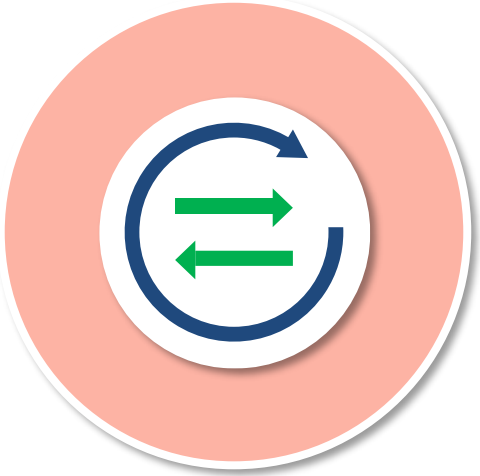
Detection



- Also referred to as "Identification"
- Separate an event from an incident or breach immediately, using pre-defined metrics and experience
- Categorize and prioritize the incident based on an established risk register or risk ledger
    - 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?
    - **Can you quickly identify the root cause?**

Incident Response Lifecycle

Response



- Main goal is containment of the outbreak or malware exploit
- Implement short-term processes, such as disconnecting devices from the network
- Use firewalls, NG-IPS, ML algorithms, and other forensic tools to maintain separation, containment, and segregation
- Evaluate backups and snapshots for future recovery

Incident Response Lifecycle

Mitigation

- This step is also called "eradication" and is often integrated with the previous phase, Containment/Response, as opposed to being a separate action
- Involves determining the root cause of the incident and applying immediate remedies if available
- Involves removing all indicators of compromise and any action, artifacts, remnants, or fingerprints associated with the attack

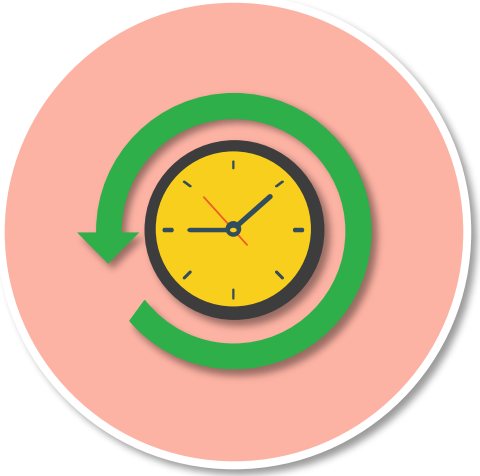
Incident Response Lifecycle

Recovery

- 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
- Will often involve business impact analysis (BIA) metrics and indicators like RTO, RPO, and MTTR

Incident Response Lifecycle

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 Response Lifecycle

Reporting

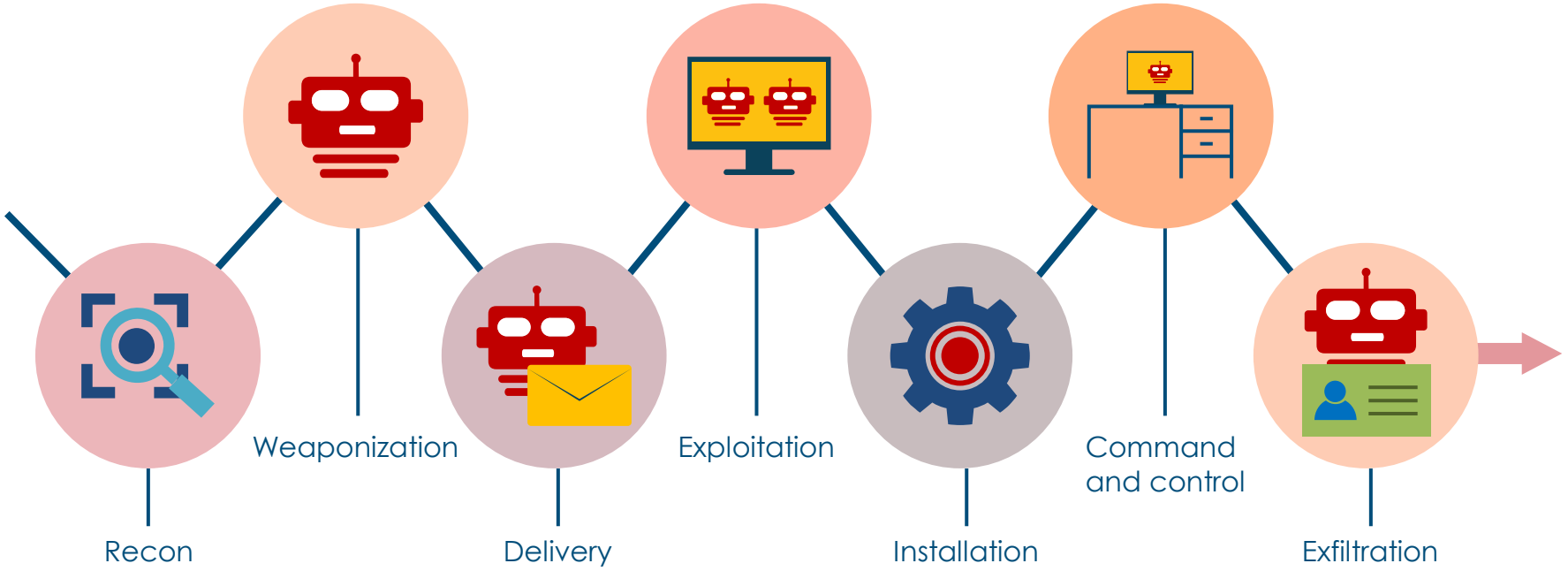
- Reports should be generated from physical, digital, and/or audio notes taken throughout the entire process
- Final reports should meet these requirements:
  - Be concise and comprehensive
  - Generate with different audiences in mind
  - Use newer graphical representation with Python and R programming tools
  - Include recommendations to prevent future incidents
  - Take problem management into consideration

Incident Response Lifecycle

Lessons learned

- Knowledge gained from the process of conducting the program
- Sessions usually held at the response close-out
- To 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

7-Step Cyber Kill Chain



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

E-discovery

- **The focus of this certification is on cyber forensics**
- 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, and
  - data management

Forensic Lifecycle

1. Identification

Detecting the incident

- Once you have determined this is not an event but rather an incident that needs forensics, you will need to identify and classify
- Forensics may not occur until later in the incident response lifecycle (remediation or reporting)
- The notification can come from
  - personal complaint by phone or text
  - monitoring system alarm or alert
  - audit result
  - IDS/IPS/EDR sensor alarm, or
  - notification from trusted or anonymous source

2. Collection

Order of volatility sets the priority

1. CPU, cache, and register content
2. Routing table, ARP cache, process table, and kernel statistics
3. Memory
4. Temporary file system/swap space
5. Data on hard disk
6. Remotely logged data
7. Data on archival media

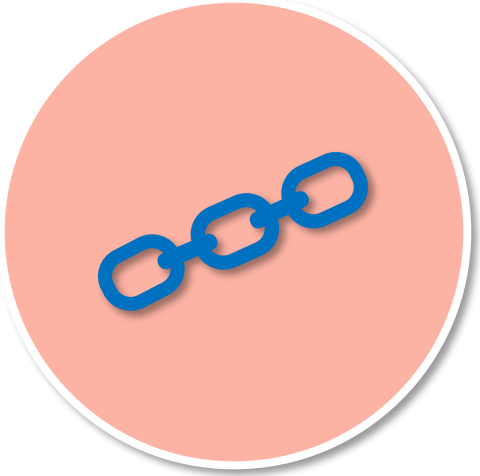
- Forensic toolkits (EnCase from Guidance) and write-blockers

Common utilities include:

- Tcpdump and dd
- nbtstat and netstat
- nc (Netcat)
- memcopy
- tshark
- foremost

2. Collection

Maintain the chain of custody



- Imaging technologies (create copies)
  - Memory dumps from write blockers
  - HDD bit-level copy, sector-by-sector
  - Include deleted files, slack spaces, and unallocated clusters
  - Look for encrypted volumes and files
- Digital pictures and interviews
- Provide a history of the handling of the evidence to maintain integrity, provide accountability, prohibit tampering, and provide assurance through the entire life cycle

Chain of Custody Documentation

Chain of custody				
Registered 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	

2. Collection

Media management

- Should have a software inventory system for configuration items and a category for components removed for investigative and forensic purposes
- Collected media (all types) must be classified and labelled
- Secure storage facilities with dual operators include
    - locked rooms
    - locked cabinets
    - safes, and
    - offsite storage facilities

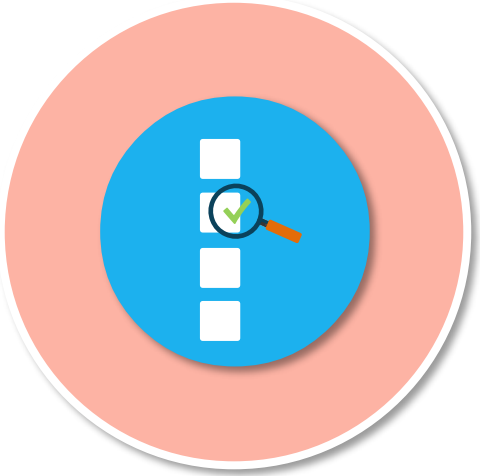
3. Examination

Where data becomes information

- Examination involves finding the relevant data in order to have the proper information to analyze in the next step
- Use tested techniques for
  - validation
  - filtering (i.e., user SIDs)
  - pattern matching
  - tracing
  - hidden data discovery, and
  - data extraction

4. Analysis

Building a solid forensic case



- Operating on the relevant data, facts, and artifacts from collection and examination phases
- May determine that more work should be done in earlier steps
    - If more information is needed, then iterate back to collection and examination
- Answer the 'who, what, where, when, why, and how?'
- Infer motive, opportunity, means
- Is a combination of an art and science that can take years to master
- Use expert judgment of others

5. Reporting

Communicate results effectively

- Track people hours and expenses in case software
- Provide electronic and physical documents of all findings
- Meet with proper authorities and possibly prepare to offer expert testimony
- Provide any needed clarification
- Identify overall impact on business and recommend any countermeasures
- Who, what, when, and how – important for court and other proceedings