Cyber Security Fundamentals

Brian Olliff

Defensive Engineering Instructor

Topics

Cyber Security Intro
Threats and Vulnerabilities
Firewalls
Intrusion Detection
Advanced Malware Protection
Cisco Security
CIA Triad
Intro to SOCs
Digital Forensics

Learning Objectives

- Understand the basics of what cybersecurity is
- Be able to explain components of threats and vulnerabilities
  - What they are and where they are found
  - How they are scored and prioritized
- Understand different types of firewalls and how they can be used
  - NAT, ACLs, DMZ, etc
- Understand methods for intrusion detection and prevention
- Be able to explain types of malware and how to protect against them
- Understand basics of Cisco security appliances and cloud services
- Be able to explain CIA triad and its importance in cybersecurity

Introduction to Cyber Security

What is Cybersecurity?

- All organizations use electronic/digital systems
- Protect against harm from misuse, compromise, destruction of systems
  - People, businesses, economy, critical infrastructure, etc
- Adequate cybersecurity programs are critical for any organization
- Risks from improper security
  - Data breaches, can result in financial/reputational loss
  - Business interruption from downtime or loss of systems
- Everyone in organization must be involved

Cybersec vs Infosec

- Original information security policies protected data within organization
  - Policies mainly for internal network and employees
- Organizational data extends beyond boundaries of “internal”
  - Multiple interconnected parts - vendors, cloud providers, etc
  - All organizations and all pieces are potential targets
- Cybersecurity - protecting information through prevention, detection, and response to attacks and threats
  - Risk management
  - Threat intelligence and information sharing
  - Threat hunting
  - Vendor, software, and hardware management
  - Incident response and resiliency

NIST (National Institute of Standards and Technology)

- Nonregulatory US federal agency
- Cybersecurity Framework (CSF)
  - Collection of industry standards and best practices
  - Designed to help organizations manage risks
  - Designed for federal agencies, but guidelines useful for all organizations
- Other NIST documentation and guidelines
  - FIPS (Federal Information Processing Standards)
  - Special Publication (SP) 800 series
  - SP 1800 series
  - NISTIR (Internal/Interagency Reports)
  - ITL (Information Technology Laboratory) bulletins

ISO (International Organization for Standardization)

- Combination of national standards institutes from 160+ countries
  - Multiple subjects, not just IT/cybersec related
- ISO/IEC 27000 series - security standards published jointly by ISO & IEC
  - First 6 - recommendations for information security management systems
  - ISO 27001 - specifications for an information security management system
  - 27002 - practice for information security management
  - 27003 - detailed guidance on implementations
  - 27004 - monitoring and measurement of security using metrics
  - 27005 - high-level risk management recommendations
  - 27006 - requirements for certification under ISO 27000
- More than 20 documents

Threats, Vulnerabilities & Exploits

Threats

- Any potential negative impact (or danger) to an asset
  - Asset - any item owned by individual or organization
  - Latent and realized threats
- Malicious actor - entity taking advantage of vulnerability/risk
- Threat vector (or agent) - path used to perform attack
- Types of threats
  - Natural disasters
  - Cyber attacks
  - Virus/malware
  - Data breach
  - Denial of service (DoS)

Vulnerabilities

- Weakness in asset or implementation of asset
  - In system design, implementation, software/code, etc
  - Can potentially be exploited for malicious purposes
- Common in all systems and applications
  - No perfect code, software, hardware exists
- Most can be mitigated using various safeguards and countermeasures
  - Different levels of difficulty and effectiveness depending on vulnerability
- CVE (Common Vulnerabilities and Exposures)
  - Operated by MITRE as an industry standard to identify/classify vulnerabilities
  - IDs assigned to vulnerabilities for public disclosure

Vulnerability Locations

- Applications
  - May prioritize usability over security
  - Errors in coding, may need patches or updates
- Operating systems
  - Present on all computers, constant & continuous updates/patches
- Hardware
  - Firmware coding issues
- Misconfigurations
  - Configuration files/settings in any software or hardware
  - Require careful attention to detail to avoid
- Shrinkwrap software
  - App/executable run on a workstation or server, may contain scripts/code

CVE (Common Vulnerabilities & Exposures)

- Developed and operated by MITRE
- Identify, define, and catalog publicly disclosed vulnerabilities
- CVE Record - CVE-YYYY-####
  - YYYY: Year the vulnerability was identified
  - ####: At least 4 digits to identify vulnerability (in order discovered)
  - Description of vulnerability
  - Reference URLs
  - Date entry was created
- Feeds into NVD (National Vulnerability Database, run by NIST)
  - CVSS score - numerical indication of severity

MITRE CVE Entry

CVE-ID	
CVE-2021-44228	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

Apache Log4j2 2.0-beta9 through 2.15.0 (excluding security releases 2.12.2, 2.12.3, and 2.3.1) JNDI features used in configuration, log messages, and parameters do not protect against attacker controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled. From log4j 2.15.0, this behavior has been disabled by default. From version 2.16.0 (along with 2.12.2, 2.12.3, and 2.3.1), this functionality has been completely removed. Note that this vulnerability is specific to log4j-core and does not affect log4net, log4cxx, or other Apache Logging Services projects.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- CERT-VN:VU#930724
- URL:https://www.kb.cert.org/vuls/id/930724
- CISCO:20211210 A Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021
- URL:https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apache-log4j-qRuKNEbd
- CISCO:20211210 Vulnerabilities in Apache Log4j Library Affecting Cisco Products: December 2021
- URL:https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apache-log4j-qRuKNEbd
- CISCO:20211210 Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021
- URL:https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apache-log4j-qRuKNEbd
- CONFIRM:https://cert-portal.siemens.com/productcert/pdf/ssa-397453.pdf
- URL:https://cert-portal.siemens.com/productcert/pdf/ssa-397453.pdf
- CONFIRM:https://cert-portal.siemens.com/productcert/pdf/ssa-479842.pdf
- URL:https://cert-portal.siemens.com/productcert/pdf/ssa-479842.pdf
- CONFIRM:https://cert-portal.siemens.com/productcert/pdf/ssa-661247.pdf
- URL:https://cert-portal.siemens.com/productcert/pdf/ssa-661247.pdf

NVD CVE Entry

CVE-2021-44228 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Description

Apache Log4j2 2.0-beta9 through 2.15.0 (excluding security releases 2.12.2, 2.12.3, and 2.3.1) JNDI features used in configuration, log messages, and parameters do not protect against attacker controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled. From log4j 2.15.0, this behavior has been disabled by default. From version 2.16.0 (along with 2.12.2, 2.12.3, and 2.3.1), this functionality has been completely removed. Note that this vulnerability is specific to log4j-core and does not affect log4net, log4cxx, or other Apache Logging Services projects.

Severity

CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** 10.0 CRITICAL **Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.

QUICK INFO

CVE Dictionary Entry:
CVE-2021-44228
NVD Published Date:
12/10/2021
NVD Last Modified:
11/06/2023
Source:
Apache Software Foundation

Exploits

- Something that takes advantage of a vulnerability
  - Software, tools, techniques, or processes
  - Leads to access, privilege escalation, denial of service, etc
- All systems/software have vulnerabilities
  - Time between discovery and patching can make exploits dangerous
- Zero-day - exploited vulnerability before vulnerability is known
- Commonly shared/traded on dark web
  - “Hidden” area of internet, requires specific software to access
  - Component of deep web - areas of internet not indexed by search engines
- Not all exploits are developed/shared with malicious intent
  - Proof-of-concept (POC) to demonstrate vulnerabilities
  - Security researchers often develop

Risk

- Probability/likelihood that a threat is realized or occurs
- Managed using risk management frameworks (RMF)
- Three basic components of risk - assets, threats, and vulnerabilities
- Assets
  - Physical or virtual assets - routers/servers or software/confidential data
  - Loss, damage, or compromise of asset leads to financial loss
- Threats can affect confidentiality, integrity, or availability of assets
- Risk can never be eliminated completely
  - Residual risk - amount of risk still remaining after safeguards and controls

Firewalls

Firewalls

- Traditional firewall placement
  - Outside network (untrusted) -> Firewall -> Inside network (trusted)
  - Internet edge firewall
- Often placed in other locations around network
- Multiple features available depending on type of firewall
  - NAT, access control lists, application inspection
  - Primary feature is to block or allow traffic based on rules
- Several methods/processes for blocking or allowing traffic
  - Packet filtering techniques
  - Application proxies
  - NAT
  - Stateful inspection
  - Next generation firewalls (NGFW)

Packet Filtering

- Method of controlling traffic using definitions of what is allowed/denied
- Packet filters operate at transport layer of OSI model
  - Analyze TCP/UDP packets and compare against access control lists (ACLs)
- ACLs can inspect several parts of a packet
  - Source & destination addresses and ports
  - Protocol
- Each entry of ACL is an access control entry (ACE)
  - Can inspect Layer 2 - 4
- Do not inspect more advanced information
  - Sequence numbers, TCP control flags, ACK fields, etc
- Packet filtering can be deceived by spoofing

Stateful Inspection

- Additional benefits compared to packet-filtering firewalls
- Every packet flowing through interfaces are tracked
  - Ensure they are part of valid connections (state)
- App layer information can be inspected, in addition to packet headers
- Allows for additional rules based on payload
- State table
  - Database containing information about state of connections
  - If established, closed, reset, negotiating
- Provide additional attack protections and filtering options

Deep Packet Inspection

- Some applications require data packets to be handled differently
  - Apps/protocols that embed IP information in payload
  - Secondary channels on dynamically assigned ports
- More sophisticated firewalls & appliances can inspect to handle
  - Cisco ASAs, Cisco FTD, IOS zone-based firewalls, etc
- Ability to identify dynamic port information and allow data flow on them
- DPI firewalls inspect Layer 7 to protect against additional threats
- Can also be configured to deny application-specific
  - Certain FTP commands
  - HTTP content types
  - Other types of application protocols

Next Generation Firewalls (NGFW)

- Provide more advanced features using context-aware security
  - Application information and granular control
  - User identification and location-based controls
  - Time of day filtering
- Cisco Firepower Threat Defense (FTD)
  - Provide standard firewall features (packet filtering, etc)
  - Application inspection and awareness
    - Allows interception of conversation to inspect application layer info
- Often combine additional features
  - NAT, DHCP server, VPN functionality (IPsec and SSL), IPS, etc

Application Proxies

- Intermediate security devices on private/protected networks
  - Also called proxy servers
  - Can also provide caching to improve throughput
- Client requests routed through proxy to unprotected network
  - Web proxy is common example
  - Proxy then routes request on behalf of internal client
- Majority operate at application layer
- Can also be used in reverse proxy function
  - Web application firewall (WAF)
  - Designed to protect against certain types of attacks
  - Typically do not provide protection against web server

Network Address Translation

Network Address Translation (NAT)

- Layer 3 devices can translate internal IP to public IPs
  - Internal: *real*, public: *mapped*
  - Ex: 192.168.1.10 -> NAT -> 123.45.67.89
- Frequently used by firewalls (other devices support)
- Hides private internal address from unprotected network(s)
  - Only exposes public address or range
- Allows usage of any IP address space for internal networks
  - A best practice is to use space reserved for private usage (RFC 1918)
  - Traditional Class A, B, or C

Port Address Translation (PAT)

- Allows many devices on internal network to share one public IP address
  - Typically firewall's public IP
- Performed by inspecting Layer 4 headers
- PAT example:
  - Internal network uses 192.168.10.0/24 subnet
  - Client accesses website on Internet from 192.168.10.42 (source port 1234)
  - Firewall uses PAT to translate request
    - New source IP - 123.4.56.78 (firewall public IP)
    - New source port - 6392 (randomly selected)

Static Translation

- Used primarily when access needed from unprotected to protected
  - Ex: web server on protected network with private IP
- Also called one-to-one mapping
- Uses NAT to accomplish
  - Web server IP: 192.168.100.80
  - Firewall public IP: 123.45.67.89
  - Static mapping allows connections directed to public IP to be routed to web
- Many types of devices support
  - Cisco ASA, FTD, IOS zone-based firewalls, etc
  - Home wireless routers

Access Control Lists

ACLs

- ACLs found on firewalls, routers, switches, wireless controllers, etc
- Each entry in ACL is an *access control entry* (ACE)
  - Can classify, filter packets based on multiple packet characteristics
    - Layer 2 & 3 protocol information (EtherTypes, TCP, UDP, etc)
    - Layer 3 header info (source & destination IPs)
    - Layer 4 header info (source & destination ports)
- ACLs applied to interfaces for filtering (inbound or outbound)
  - Inbound filters first, then firewall processes
  - Outbound filters **after** firewall processes packets
- Differences in filtering based on type of device
  - Router will check all packets
  - Stateful firewall checks first packet of flow

Cisco Firewall ACLs

- Order is important
  - ACEs are appended to end of ACL when added
  - ACEs are evaluated & matched from top to bottom
  - “Implicit deny” at end of all ACLs
- Interfaces are assigned security levels (higher = more secure)
  - By default, inside interface is 100, outside interface is 0
  - Higher level to lower level traffic does not need ACE
  - Lower level to higher level requires ACL to permit traffic
- ACLs can control traffic **through** or **to** a security appliance
  - When filtering to appliance, ACLs applied using access control groups
- TCP/UDP return traffic is automatically allowed to pass
  - Other protocols (ICMP) require ACLs for both directions

ACL Types

- Standard ACLs
  - Can identify packets based on destination IP address only
  - Can not be applied to an interface for filtering purposes
  - Can only be used if security appliance is running in routed mode
- Extended ACLs
  - Most commonly used type of ACL (for security purposes)
  - Can classify packets based on source/destination IP and port
    - Also Layer 3 protocols and destination ICMP type
  - Multiple different uses
    - Interface filtering
    - QoS packet classification
    - Identification for NAT, VPN encryption

ACL Types

- EtherType ACLs
  - Can filter IP and non-IP traffic by checking Ethernet type code field in L2
  - Can only be used if appliance running in transparent mode
  - Includes implicit deny, but does **not** affect IP traffic
    - Both EtherType and extended ACLs can be applied to interface
- Webtype ACLs
  - Can be used to restrict traffic through SSL VPN tunnel
  - Contains implicit deny if ACL configured
  - If ACL not defined, traffic will pass

Firewall Usage

Segmentation

- DMZ (demilitarized zone)
  - Separated network segment for additional security
  - Typically used for hosting public resources
    - Can also be used for connections to business partners
  - Minimize exposure of internal network
    - Connections from DMZ to internal are heavily restricted
- Can also be used to segment internally
  - Separation for different departments, security zones, etc
  - Used to isolate network portions
  - Can allow specific, more restricted traffic as needed between segments

Micro-Segmentation

- Used for segmenting between applications or individual devices
- Requires careful consideration of what communication is needed
  - Relationship between systems and data interaction
- Cisco Application Centric Infrastructure (ACI)
  - Ability to assign endpoints to endpoint groups (EPGs)
    - Typically used for grouping VMs to apply filtering & forwarding policies
  - Micro-segment in ACI is *µSeg EPG*
  - Endpoints and application EPGs can be grouped into new µSeg EPGs
    - Apply policies as needed
- Ex: segment of web servers, but contains both prod and dev
  - Can segment further to apply more granular policies to restrict

High Availability (HA)

- Active-standby failover
  - Primary device (firewall) always active
  - If fails, secondary device will take over
  - Configuration and state tables synchronized to ensure functionality
- Active-active failover
  - Both devices active and passing traffic at same time
  - If one fails, other will continue to function normally
- Clustering
  - Devices work together for larger and more scalable environments
  - Can increase throughput and make scaling more efficient

Data Center Usage

- Placement and usage will of firewall will vary depending on needs
- East-to-west traffic
  - Traffic flowing from one segment/app to another
  - Also known as lateral traffic
- North-to-south traffic
  - Traffic flowing in or out of a datacenter
  - Commonly between datacenter and internal corporate network
- Software-defined networking (SDN)
  - With Cisco ACI, can introduce advanced segmentation (and micro)
  - Policy-based automation with physical and virtual environments
  - Allows limiting traffic on same network, unless policies configured to allow

Intrusion Detection & Prevention

IDS/IPS

- Intrusion detection systems (IDS)
  - Designed to detect and alert on malicious activity
- Intrusion prevention systems (IPS)
  - Same as IDS, but with blocking capabilities
  - Can be configured in promiscuous mode (monitoring) or inline for blocking
- Network-based and host-based
  - Traditional network based
  - Next-generation IPS
  - Host-based IPS
- Can be combined with firewalls for enhanced protection (Cisco FTD)

Pattern Matching

- IPS searches for a fixed sequence of bytes
  - Typically correlated with specific service or source/destination ports
- Reduces inspection overhead on each packet
  - Limited to protocols that are associated with well-defined ports
- Uses signatures for detection
  - Set of predefined conditions that match specific intrusions
  - Ex: port number 5432, contents contain “ff06b5”
- Can result in high number of false positives and false negatives
- Stateful pattern-matching recognition
  - Detection that considers chronological order of packets in TCP stream
  - Can directly correlate pattern with exploit
  - Still has possibilities of false positives/negatives

Protocol Analysis

- Can also be called protocol-decode analysis
- Extends capabilities of stateful pattern recognition
- Network IDS decodes all protocol or client-server traffic
  - Based on definition of specific protocol, analyzes elements for issues
- Can look at specific protocol fields within packet
  - May also examine length of field or number of arguments
- IPS looks at specific commands and fields depending on protocol
- False positives reduced if protocol in question is properly defined
  - Can be increased if not well defined, or protocol implementation is flexible

Heuristic & Anomaly-based Analysis

- Heuristic scanning uses behavioral information of traffic
  - Statistical analysis and logic
  - Can be resource intensive
  - Requires fine-tuning and testing for specific networks
- Anomaly-based analysis identifies traffic that differs from “normal”
  - Requires baselines established of normal traffic patterns
  - Can be difficult to maintain depending on complexity and frequency of change in network
- Protocol-based detection (type of anomaly-based)
  - Depends on well-defined protocols

Threat Correlation

- Cisco IPS devices include correlation abilities
- Uses data from Cisco Talos
  - Security researchers, analyze threats and provide threat intelligence
- Data is gathered from global sources, analyzed, and provided
- Includes reputation of source IPs, domains, etc
  - Based on past behavior and actions
  - Used to predict how trustworthy future actions from IP will be

Advanced Malware Protection

Malicious Software (Malware)

- Virus
  - Infects hosts to create an undesirable outcome
  - Data deletion, theft, corruption
- Worm
  - Self-replicating virus
  - Can execute malicious code without user interaction
- Mass-mailer
  - Worm sent via multiple email messages
  - Often uses local directories/address books to automatically spam
- Logic Bomb
  - Malicious code set to execute when certain criteria are met
  - Date, time of day, disk free space, etc

Malware

- Trojan horse
  - Malicious code hidden inside another application
  - Runs when application is run, often without user knowledge
  - Typically use social engineering to trick users into downloading or running
- Backdoor
  - Allows attacker to access victim machine remotely
  - Can open port to allow communication, or establish “reverse shell”
- Exploit
  - Designed to take advantage of specific vulnerability (or multiple)
- Downloader
  - Downloads and installs other malicious software

Malware

- Spammer
  - Sends unsolicited mass emails (or instant messages, group postings, etc)
  - Usually with goal of tricking users into clicking link, opening attachment
  - May also request reply to message with sensitive information
- Keylogger
  - Software (or hardware) designed to record keyboard presses
  - Can store locally or send to remote attacker
- Rootkit
  - Set of tools used for privilege escalation and persistence
  - Can allow complete control of system
- Ransomware
  - Compromises system and holds data hostage, demanding payment

AMP for Endpoints

- (Now called Cisco Secure Endpoint)
- Improvement over traditional HIPS and personal firewalls
- Provides more granular visibility into threats
  - Uses Cisco threat intelligence and continuous analysis of threats
  - Device and file trajectory
    - Origin of attack on network
    - How malware progressed through environment and individual host
- Offers retrospective analysis and protection
  - Threat may not have been detected immediately
  - After analysis by Cisco, actions can be taken after initial discover
    - Deletion, quarantine, etc

AMP for Networks

- Similar functionality to AMP for Endpoints, but on network
  - Continuous tracking and analysis
  - Retrospective analysis and alerts
  - File trajectory to track files across network
- Provides file capture capabilities to gather and analysis files
- Can be standalone device, or installed on Firepower appliances
- Works with AMP for Endpoints and AMP for Security Appliances
  - Ability to detect/analyze threats regardless of location
- Cloud analysis of files (either SHA256 hash, or file itself)
  - With FMC, files can be analyzed locally, unless never seen by FMC
    - Then sent to cloud for analysis

Cisco Security Appliances

Web Security Appliance (WSA)

- Designed to protect against web-based threats and attacks
  - Provides content filtering capabilities to align with org policies
- Uses cloud-based intelligence from Cisco
  - URL reputation, file reputation, sandboxing, retrospective analysis
- Can be used in transparent or explicit proxy mode
  - Explicit - client configured to route web requests directly to WSA
    - Client -> WSA -> firewall -> website
  - Transparent - clients not aware of proxy server, uses WCCP
    - Client -> router -> redirect to WSA -> firewall -> website
    - WCCP registration
      - WSA sends registration announcement every 10 seconds
      - Router accepts request and sends acknowledgement

WSA Features (AsyncOS)

- Real-time antimalware adaptive scanning
  - Can dynamically select scanning engine
    - Based on URL reputation, content type, scanner effectiveness
  - Helps with detection of malware embedded in other files
- Layer 4 traffic monitoring
- Third-party DLP integration
  - Can redirect traffic to DLP appliance to inspect web content/traffic
- File reputation, sandboxing, and retrospective actions
  - Uses data from Cisco Talos to update file reputation intelligence
  - Can inspect malware (or suspected) behavior
- Application visibility & control
  - Inspect and block disallowed applications

Email Security Appliance (ESA)

- Mail gateway for organization (SMTP gateway/mail exchanger(MX) /etc)
  - Accept and relay messages as needed (inbound and outbound)
- Uses listeners to handle SMTP traffic
  - Public listeners for inbound email from Internet
  - Private listeners for email from internal network (usually from mail server)
- Listener configuration requires specific information
  - Interface on ESA and TCP port being used
  - Public or private
  - Hosts allowed to connect
  - Domains that public listeners will accept mail

ESA Features (AsyncOS)

- Access control
  - Can restrict inbound senders based on IP, IP range, or domain name
- Antispam
  - Multiple layers of filtering based on Cisco SenderBase, and Cisco Talos
- Network antivirus and AMP
  - AV includes Sophos & McAfee. AMP for continuous and retrospective
- DLP
- Encryption
  - Outbound email encryption using local key server or hosted service
- Email authentication
  - Inbound checks for SPF, DKIM, DMARC
  - Outbound DKIM signing
- Outbreak filters

Security Management Appliance (SMA)

- Centralized management and reporting of WSAs and ESAs
  - Policy configuration and deployment
  - Status and log reporting from all appliances
- Like WSAs and ESAs, can be deployed as physical or virtual appliance
- Most policies configuration performed on SMA
  - Published to appropriate appliances as needed
  - Eliminates need to individually manage multiple WSAs or ESAs
  - Some config still needed on individual appliances

Cisco Identity Services Engine (ISE)

- "Security identity management solution"
  - Allows admins to collect information about network, users, devices
  - Policy management point for authentication, authorization, accounting
  - Network profiling and posturing
- Network Access Control (NAC) to enforce device config/policies
  - Helps ensure devices have up-to-date security settings and applications
  - NAC Web Agent - temporary agent
  - NAC Agent - permanently installed agent
  - AnyConnect Secure Mobility Client - permanently installed, multi-purpose
- Features to assist with securing mobile device access
  - Integrations with MDM solutions to help enforce policies
  - Automatic redirection to MDM onboarding portals
  - Internet-only access for non-compliant devices

Cisco ISE

- ISE supports Cisco Platform Exchange Grid (pxGrid)
  - Provides methods to interconnect different parts of IT infrastructure
    - Security monitoring and detection systems
    - Network policy systems
    - Asset, configuration, identity and access management platforms
  - Uses API to share information from ISE to other policy network devices
- ISE can be used as a CA for certificate managements on endpoints
  - Standalone or subordinate

Cisco Cloud-based Security

Cisco Cloud Email Security (CES)

- Email Security Appliance (ESA) in the cloud
- All typical cloud benefits combined with ESA functionality
  - High availability and redundancy from multiple data centers
- Typically used as hybrid model
  - On-premise ESAs combined with cloud based (CES)
- “Outsource” portion of email security, still maintaining control on-prem
  - On-premise allows for regulation compliance (when needed)
  - Use cloud as “first line of defense”

Cisco AMP Threat Grid

- Now called **Cisco Secure Malware Analytics**
- Crowdsourced malware from closed community
- Analyzed using Cisco-proprietary techniques
  - Both static and dynamic analysis
  - Different than standard sandboxing methods
  - Analysis is outside of virtual environment, allowing vm-evading analysis
- Provides detailed look into attack campaigns and distribution
  - Detailed reports for security admins with IOCs and threat scores
- Glovebox
  - Allows interaction with malware in safe environment
  - Test how malware behaves & how reacts to user interaction

Umbrella

- Formerly OpenDNS
- DNS services, threat intelligence, threat protection at DNS layer
- OpenDNS available as free service: individuals, students, small business
  - Change DNS to point to Umbrella servers
- Premium services
  - Cisco Umbrella
    - Advanced protection for enterprise networks (and roaming)
    - Blocks known malicious sites from being resolved
  - Investigate
    - Detailed information on attacks
    - Provides searching and API integration
    - Predictive threat intelligence

Stealthwatch Cloud

- Now called **Secure Cloud Analytics**
- SaaS solution (Software as a Service)
- Monitors various public cloud environments
  - AWS, Azure, GCP
- In AWS, uses VPC Flow Logs (Amazon equivalent of NetFlow)
- GCP supports VPC Flow Logs (or Google GPC Flow Logs)
- Azure, traffic collected in Network Security Group (NSG) flow logs
  - Feature of Network Watcher

CloudLock

- Protects against cloud data breaches using DLP (data loss prevention)
  - Assists with data protection and compliance
- Pre-configured policies and policy-driven responses
  - File-level encryption
  - Quarantine
  - End-user notifications
- Can monitor data at rest using API
- Visibility of user activity with data
  - Protection against account compromises using UEBA
    - User and Entity Behavior Analytics

Confidentiality, Integrity, & Availability

CIA Triad

- Confidentiality
  - Private data remains private
  - Information not disclosed to unauthorized entities or processes
  - Commonly enforced with encryption and access control restrictions
- Integrity
  - Ensuring that systems/data not modified without authorization
  - Typically verified using cryptographic methods (hashing, digital signatures)
- Availability
  - Systems/applications remain accessible to authorized users
  - High availability, redundancy, & effective security controls
- All three should be guaranteed in any secure system

Risk

- Possibility or likelihood of a security incident occurring
- FFIEC Cybersecurity Assessment Tool
  - Inherent risk profile and cybersecurity maturity
  - ISO 27001 assessment
- Assessment is a continual process
  - Establish risk management context (scope, approach, method, etc)
  - Quantitative or qualitative assessment
  - Response to identified risks
  - Stakeholder communication
  - Monitor and review risks and actions

Risk Scoring

- Designed to assist with severity and prioritization
- CVSS (Common Vulnerability Scoring System)
  - Most commonly used for vulnerabilities by IR teams
- CWSS (Common Weakness Scoring System)
  - Used for scoring software weaknesses
- CMSS (Common Misuse Scoring System)
  - Standardized measurement of software feature misuse vulnerabilities
- CCSS (Common Configuration Scoring System)

Protected Information

- Regulations and laws often require identification of PII/PHI
- Personally Identifiable Information (PII)
  - Information that could be used to identify an individual
    - Name, SSN, place/date of birth, DL #, etc
- Protected Health Information (PHI)
  - Required to be protected by various regulations (HIPAA in US)
    - Patient's name
    - Any data directly linked to individual (DoB, death, discharge, etc)
    - Medical record numbers
    - Photos of face or recognizable features
    - Past, present, future mental health condition

Data Loss Prevention (DLP)

- Detection (and hopefully prevention) of sensitive data leaving org
  - Sensitive emails, documents, etc
  - Malicious (external or internal actor) or accidental
- Multiple Cisco products integrate with third-party DLP
  - ESA integrates with RSA email DLP
    - Can block, quarantine, auto-encrypt, etc
  - WSA can redirect outbound traffic through DLP appliance
    - Prevent data storage in Dropbox, Google Drive, etc
- Allow for analysts to discover, block, remediate

Defense in Depth

Defense in Depth

- Layers of various security controls to protect assets & organization
  - Cross-boundary
  - If one layer fails to detect or stop threat, other controls can protect
- Multiple types of controls in different layers
  - Non-technical
  - Physical security
  - Network & host security
  - Application & data security
- Starts with identifying assets, risks, and threats
- Proactive and reactive security

Network Defense in Depth

- Multiple planes of network
  - Management
  - Control
  - User/data
  - Services
  - Policy
- Software-defined networking (SDN) introduces centralized controller
  - Global view of network
  - Manages and controls network devices

Limited Access

- Least privilege
  - Only grant the minimum access needed to perform job role
  - Applies to **ALL** users
  - Can apply to application requirements
    - Minimum access to function (no root/admin access)
- Separation of duties
  - One individual should not perform all critical (or privileged) duties
  - Duties must be separated/divided between multiple individuals
  - Can prevent on malicious insider from causing severe damage to org
  - Ex: auditors should not have access to modify

Introduction to Security Operations Centers

SOC

- Monitoring and protection of organization's assets
  - Applications, databases, servers, workstations, network, etc
- Creation requires careful planning and implementation
  - What are objectives?
  - What assets require monitoring?
  - How large is organization?
- Incident response teams typically work in SOC
  - Computer Security Incident Response Team (CSIRT)
- Aggregated logging and monitoring systems
  - Security Information and Event Manager (SIEM)
  - Security Orchestration, Automation, and Response (SOAR)

Building a SOC

- How can threats and compromises be detected quickly?
- How are incidents triaged to determine scope and severity?
- What sort of impact would a compromise have on organization?
- Who is responsible for monitoring and detecting incidents?
- Who needs to be informed about suspected (and confirmed) incidents?
- What criteria exist for external notifications?
  - Who and when?

Effective Operations

- Support from senior leadership
- Operation as a program instead of project
  - Clear strategies for operations
- Governance structure(s)
  - Established metrics to provide visibility
- Effective teamwork
- Access to needed systems/data for proper logging & analysis
- Established and documented processes and procedures
- Appropriate budget for requirements

Playbooks and Runbooks

- Collection of procedures and operations
  - System monitoring and logging
  - Incident response
  - Communication
- Assists with defining, building, managing, and monitoring operations
- Often use runbook automation (RBA)
- Metrics used to measure effectiveness
  - Mean time to repair (MTTR)
  - Mean time between failures (MTBF)
  - Mean time to discover incidents
  - Mean time to mitigate incident

Introduction to Digital Forensics

Digital Forensics

- Collecting/recovering, analyzing, and presenting evidence
  - Primarily for court/legal purposes
- Find out what happened and collect data
- Evidence can come from any device that stores data
  - Any type of computer
  - Smartphone/tablet
  - Network infrastructure devices & management systems
  - Printers
  - IoT devices
- DFIR - Digital Forensics and Incident Response

Chain of Custody

- Documenting and preserving evidence
  - From very start of investigation until evidence is finally presented
- Often required to introduce or use in court
- Integrity of all evidence must be protected (evidence preservation)
  - Disk imaging, memory dumps - hash verification
- Information to document
  - Method of evidence collection
  - When evidence was collected
  - How evidence was transported, tracked, and stored
  - Who could access evidence, when & how it was accessed

Evidence Preservation

- Work with copy of evidence only, never with original data
- Use tools specifically for forensic evidence
- Use write-protection devices
  - Physical devices that prevent original hardware from being modified
- Protection from static discharge (ESD)
  - Faraday cage can be used for additional protection
- Careful transportation methods
  - Lockable (and locked) containers
  - Evidence never left unattended during transport

EXPERTS AT MAKING YOU AN EXPERT