CompTIA Security+ Study

Sunday, January 22, 2023 2:21 PM

Things to Know More

XSS vs XSRF vs SSRF

Sideloading
Refactoring (Changing code keeping performance the same)
Shimming for APIs (Intercepting and changing calls to make compatible)

VBA Visual Basic Application (Enables macros)
.vbs Virtual Basic Script (Based on Visual Basic)
.vb Visual Basic code
.ps1 (Power Shell script file)
.py (Python. Cross platform and general purpose)

DOM (Document Object Model)

NVD (National Vulnerability Database)
CVE (Common Vulnerabilities and Exposures)
CVSS (Common Vulnerability Scoring System)
AIS (Automated Indicator Sharing)

- Government initiative
- CISA capability

CISA (Cybersecurity and Infrastructure security Agency)
TAXII (Trusted Automated Exchange of Intelligent Information)
STIX (Structured Threat Information Expression)

- Language
- Serialized Format
- Exchange CTI

CTI (Cyber Threat Intelligence)

RFC (Request for Comments)

- Formal Document
- Describes specs for a certain technology

TTP's (Tactics, Techniques and Procedures)

- Threat intelligence
- Identify patters and behaviors
- Defend against threat vectors and strategies

SOAR (Security Orchestration, Automation and Response)

- Automated response to security incidents

SIEM (System Information and Event Management)

- Detect anomalies in logging of events
- Collected from multiple devices

Syslog Server

- Collecting diagnostic and monitoring data from networked devices

ICS Server (Internet Connection Sharing)
- Windows service
- One internet connected computer
- Passes internet connection to other computers on LAN

SNMP (Simple Network Management Protocol)
- Collect and organize info about managed devices on IP networks

SSL (Secure Socket Layer)
- Depreciated
- Encryption Protocol

Penetration testing
- Actively testing security controls

Vulnerability scanning
- Passively testing security controls

Active Reconnaissance
- Engaging with target

Passive Reconnaissance
- Not engaging with target

Warchalking
- Marking outside of building where Wi-Fi is open and available
- Multiple markings to designate specific details

Wardriving
- In a moving vehicle
- Scanning for Wi-Fi networks
- Software to do so is available online
- Place antennas to avoid this

3 states of digital data
- At rest (Can be encrypted)
- In motion (Can be encrypted)
- In processing (Not encrypted)

MSP (Managed Service Provider)
MSSP (Managed Security Service Provider)
MSA (Master Service Agreement)
- Between MSP/MSSP and Client

Fog computing
- Network surrounding IoT devices and edge devices to increase processing time

Edge Computing
- Bringing resources closer to sources of data to increase response time

Edge devices
- Devices on the edge of the organization usually public facing.

Thin Client computing
- Networked computer
- Uses server resources for computing
- Runs with minimum amount of hardware and software components

Containerization
- Virtualization on an application level

Microservice

- Self-contained code
- Components
- Combined to make an application function

SDN (Software Defined Networking)
- Software based controllers
- Network Virtualization
- Uses underlying hardware infrastructure

SDP (Software Defined Perimeter)
- Black cloud
- Way to hide internet connected infrastructures
- Works for on premise or cloud

SDV (Software Defined Visibility)

VPC (Virtual Private Cloud)
- Connect via Transit Gateway
- From on-premise
- Cloud Computing

VM Sprawl
- Many VM's
- Not managed properly
- Mitigate by:
    - Usage audit
    - Asset documentation

VM Escape
- Processes break out of the VM and onto the Host machine
- Mitigate by:
    - Sandboxing
    - Patch management

Dead code
- Unused results

Code bloat
- Long or resource intensive code
- Not necessary

Duplicate code
- Juist that
- Double the code
- Not needed

SDK (Software Development Kit)
- Collection of tools
- Used to develop apps for specific platform

CERT (Computer Emergency Response Team)
CSIRT (Computer Security Incident Response Team)
IETF (Internet Engineering Task Force)
OWASP (Open Web Application Security Project)

TOTP (Time-based One Time Password)
- One time password
- Generated using current time

- For uniqueness
- No replay attacks

HOTP (HMAC-based One Time Password)

- Same as TOTP
- Except uses a counter
- Increments by one after each authentication
- No replay attacks

Hard Token

- User in physical possession of device
- Hardware authentication device
- Examples
    - USB
    - Keycards
    - RFID
    - Keyfobs
    - Tradition keys

Soft Token

- Digital authentication
- Based on software
- Flexible usage

Static Authentication

- Reuses static identifier
- Such as a password
- Or a PIN

Certificate-based Authentication (CBA)

- Authentication for anything other than humans
- Such as IoT
- Servers
- e-passports
- uses a digital certificate derived from cryptography
- SMART CARD

Biometrics

- FAR (False Acceptance Rate)
    - Percentage
- FRR (False Rejection Rate)
    - Percentage
- CER (Crossover Error Rate)
    - Overall accuracy of a biometrics system
    - EER (Equal Error Rate)

Note:

Authentication process can be based on various categories of authentication factors and attributes. Authentication factors include unique physical traits of each individual such as fingerprints ("something you are"), physical tokens such as smart cards ("something you have"), or usernames and passwords ("something you know"). The categories of authentication attributes include geolocation ("somewhere you are"), user-specific activity patterns, such as keyboard typing style ("something you can do"), revealing something about an individual, e.g. wearing an ID badge ("something you exhibit"), or proving the relation with a trusted third party ("someone you know"). Multifactor authentication systems require implementation of authentication factors from two or more distinct categories.

From <https://www.examcompass.com/comptia-security-plus-practice-test-9-exam-sy0-601>

RAID

- 1
  - Mirroring
  - Slow
  - Fault tolerance to 1 drive
  - Minimum of 2 drives to work
- 0
  - Striping
  - Fast
  - No fault tolerance
  - Minimum of 2 drives to work
- 5
  - Block level striping with distributed parody
  - 3 drives needed
  - Can lose 1 with no data loss
- 6
  - Block level striping
  - 2 parody blocks
  - 4 drives needed
  - Can lose 2 with no data loss
- 10
  - 1+0
  - Striped Mirrors
  - 4 drives needed
  - Can lose 1 drive from either mirror

NAS (Network Attached Storage)
SAN (Storage Area Network)

Backups

- Full
  - Full and complete backup independent of last full backup
  - Longest
- Differential
  - Data backed up of changed files since last Full Backup
  - Quick
- Incremental
  - Data backed up of changed files since last incremental backup
  - Fastest
  - Can be hourly
  - Longer to restore due to reconstruction

https://www.acronis.com/en-us/blog/posts/incremental-differential-backups/

Restoring from:

- Full
  - Copy of full backup
- Differential
  - Copy of full
  - Copy of last differential
- Incremental
  - Copy of Full

    - All incremental

SCADA (Supervisory Control and Data Acquisition)
- Category of software applications for controlling industrial processes
- Real time processing

ICS (Industrial Control Systems)
PLC (Programmable Logic Controller)
FPGA (Field Programmable Gate Array)

PBX (Private Branch Exchange)
- Internal telephone exchange or switching system
- Handles internal communications

PSTN (Public Switched Telephone Network)
- Paid service
- Also known as POTS (Plain Old Telephone Service)

VoIP (Voice over IP)
- Internet calling
- VoIP PBX is common inter-organization
- Endpoints
    - Special hardware devices
    - Or application programs
    - Enables calls from computing devices
- Gateways
    - Network devices
    - Convert voice and fax in real time
    - Between IP network and PSTN//POTS

MFP (Multi-Function Printer)
- Usually smaller organization
- can print, scan, copy, and fax

MFD (Multi-Function Device)
- Usually larger organization
- can print, scan, copy, and fax
- High document management
- Advanced scanning functionality
- Advanced solutions capability
- High-speed printing
- Production-quality printing options

MPS (Managed Print Service)
MDS (Managed Document Service)

PED (Portable Electronic Device)
MFA (Multi-Factor Authentication)
IoT (Internet of Things)
RTOS (Real Time Operating System)
SoC (System on Chip)
Zigbee
- IoT devices
- Communication
- Home network

POSIX (Portable Operation System Interface)
RTOS (Real Time Operating System)

Key stretching
- Salting (Pseudo-random data) added before hashing
- Hash the resulting value to add time
- Common algorithms
    - Bcrypt
    - PBKDF2 (Password-based Key Derivation Function2)

Screened subnet
- Lightly protected subnet
- DMZ

Extranet
- Secure network for remote access
- Used by trusted 3rd parties for internal access
- Physically not at same location

Intranet
- Internal network for employee
- For internal working of an organization

Internet
- THE internet. DUH

Server room fact
- Hot and cold isles helps efficiently manage airflow

Digital signatures
- Integrity
- Authentication
- Non-repudiation

ECC (Elliptic Curve Cryptology)
- Symmetric keys
- Simple
- Good for low power devices with lesser processing ability

RSA (Rivest-Shamir-Adleman)
- Asymmetric keys
- Generates 2 key pair
- Private key is used for decrypting
- Public key in used for encrypting

Out of band key exchange
- Not sending a symmetric key over the net
- Deliver the key in person or via telephone

In band key exchange
- Additional encryption to send key
- Common to use asymmetric keys to transfer

Session keys
- Ephemeral keys
- Change each time
- Symmetric

PFS (Perfect Forward Secrecy)
- Encryption system

- Changes keys frequently and automatically
- If most recent key is hacked is only for a short time

EFS (Encrypting File System)
- Windows
- First in NTFS 3.0
- Filesystem level encryption
- Protects physical access hacks

Stream cipher
- Encrypting individual bits

Block cipher
- Symmetric Keys
- Encrypting blocks of data
- ECB (Electronic Code Book)
    - Used mostly with symmetric encryption
    - Fast and simple
    - Direct relationship between plain text and ciphertext
- CBC (Cipher Block Chaining)
    - Made from ECB
    - Previous block output is input for the next
- CTR (Counter)
    - A counter is used as input to the algorithm
    - Downside is you need a synchronous counter at both ends
- GCM (Galois/Counter)
    - Essentially a stream cipher
    - Very complex but fast
    - Provides data integrity and confidentiality

Symmetric keys
- Same key to encrypt/decrypt
- Secret key encryption
- Session key encryption

Asymmetric keys
- 2 keys
- One private
- One public
- Public key encryption

Security through obscurity
- Code obfuscation
- Steganography
- SSID Broadcast Suppression

Homomorphic Encryption
- Enable processing encrypted data
- For sensitive data
- Can be used to remove barriers inhibiting data sharing
- Add security to existing systems

Hashing
- One-way function

- Used to validate integrity
- Same outputs before and after transit indicate no tampering

Encryption
- Two-way function
- Using algorithms and keys

Encoding
- Two-way function
- Using algorithms
- No keys

DNSSEC (Domain Name Service Security Extensions)
- Using key pairs to increase security
- Digitally signed data by the owner

EDNS (Extension mechanisms for DNS)
- Expanding the size limitations of the protocol
- Send in larger packets over UDP

Split DNS
- Configuration
- Two DNS servers (Sub-Domains) are created for the same domain
- One for internal network and another for external
- Used to tighten security

DDNS (Dynamic DNS)
- Automatic refreshing
- Auto updates new IP addresses

STP (Spanning Tree Protocol)
- Protection against broadcast storms and switching loops
- Network protocol
- Loop-free logical topology for ethernet networks
- RSTP (Rapid Spanning Tree Protocol)
    - Adds advancements

RTP (Real-time Transport Protocol)
- SRTP (Secure)
- Transmission of video streams
- Lives inside SIP

SIP (Session Initiation Protocol)
- Private IP systems
- Signaling protocol
- Initiating
- Maintaining
- Terminating
- Voice, Video and messaging
- Mobile such as LTE(VoLTE)

S/MIME(Secure Multipurpose Internet Mail Extensions)
- Sending digitally signed and encrypted email messaged
- Authentication
- Nonrepudiation
- Data Integrity

HSTS (HTTP Strict Transport Security)
- For websites with a valid SSL (HTTPS)

- The response header can be HSTS
- Forcing communication only via HTTPS
- Block all HTTP communication

FTP (File transfer Protocol)
- Open and not secure
- Simple login required
- Can auth as anonymous if configured as such

SFTP (SSH File Transfer Protocol)
- Uses SSH
- Secure tunnel
- Uses one port
- Better usability to firewalls

FTPS (File Transfer Protocol extension)
- Adds a layer to existing FTP
- Adds support for TLS and even SSL
- Uses multiple port numbers
- Secure client and server and tunnel

TFTP (Trivial File Transfer Protocol)
- Uses UDP not secure
- Different protocol than FTP

SNMP (Simple Network Management Protocol)
- Application layer protocol
- Port 161/162
- Higher the version, the more secure
- V1
    - Uses community strings for auth in unencrypted form
    - UDP only
- V2
    - Community strings for auth in unencrypted form
    - UDP
    - TCP via configuration
- V3
    - Hash-based MAC with MD5 or SHA for auth
    - DES-56 for privacy
    - TCP
    - Validation of data integrity

IPsec
- AH (Authentication Header)
    - Authentication
    - Data integrity
    - Data origin authentication
    - Optional replay protection service
- ESP (Encapsulating Security Payload)
    - ADDS CONFIDENTIALITY
    - Data Authentication and confidentiality
    - Data integrity
    - Data origin authentication
    - Replay protection
    - Same algorithms as AH
    - Coverage is different

- Transport mode
    - Host-to-host communications
    - Data portion of packet in encrypted
    - Light bandwidth savings
    - Can expose original IP header to 3rd party elements in packet path
- Tunnel Mode
    - Network-to-Network
    - Host-to-Network
    - Host-to-host over internet
    - Entire packet is encrypted
        - Must encapsulate into new IP packet in order to work.
    - Meant to be used by routers and gateways

POP3 (Post Office Protocol 3)
- Retrieve Email
- Application Layer protocol
- Common use
- One way email synchronization
- POP3S
    - Port 995

IMAP (Internet Messaging Access Protocol)
- Serves the same function
- Replaced POP3
- Supports multiple logins
- Multidirectional Synchronization
- IMAPS
    - Uses TLS/SSL
    - Port 993

STARTTLS
- Used over IMAP and POP3
- Used after initializing the connection in cleartext
- Used on standard port 143
- Like a patch or a band-aid

SMTP(Simple Main Transfer Protocol)
- SMTPS
    - Uses TLS
    - Depreciated

NTP (Setwork Time Protocol)
- NTPsec
    - Secured

DHCP scope
- Pool of IP addresses on a DHCP server
- Typically a range
- Also defines lease duration

DHCP Reservation
- Permanent IP address assignment
- Specific IP within a DHCP scope that's reserved
- Reserved to be leased to a specific DHCP client

DHCP snooping
- Layer 2 security technology
- Built in the OS on capable network switches

- During a DHCP connection the switch creates a DHCP binding table
- Table contains info about the host
- If a packet from rouge host fails to match it will be dropped
- Protects against
    - DHCP spoofing attack
    - DHCP starvation attack

DHCP relay agent

- A host or router
- Forwards DHCP packets between clients and servers
- Relay agent receives DHCP messages
- Generates new ones to send out on another interface
- Useful for a SD-WAN (Software Defined - Wide Area Network)

Endpoint security

- EDR (Endpoint Detection and Response)
    - Detection
    - Analysis
    - Response
    - Real-time monitoring
- SWG (Secure Web Gateway)
    - Can serve as a DLP
    - Like a proxy to the outside internet
    - Holds responsibility to enforce policy
- CASB (Cloud Security Access Broker)
    - On premise or cloud based point
    - Like the sheriff to enforce laws set by cloud service admins
    - 4 pillars of CASB
        - Visibility
        - Compliance
        - Data Security
        - Threat Protection
    - Top 3 uses
        - Govern usage
        - Secure data
        - Protect against threats
- NGFW (Next-Generation Firewall)
    - Integrated intrusion prevention
    - Application awareness (Application level inspection)
    - Ability to see and block risky apps
    - Cloud delivered threat intelligence

UEFI (Unified Extensible Firmware Interface)

- Replacement to BIOS
- Includes a GUI, mouse support, secure boot functionality
- Prevents loading of malware and unauthorized OS during startup process

Measured Boot

- Windows thing
- Checks system startup components
- Stores resulting config log in TPM
- Later the log is sent to trusted server for remote attestation
- Used to verify integrity of the windows startup process
- Neutralizes hard-to-detect malware and rootkits that run before OS

Code signing
- Confirm the author
- Verify that it's not been altered or corrupted
- Uses a cryptographic hash
    - Validate authenticity and integrity

SED (Self Encrypting Devices)
- Opal storage specification
- Outlines and defines

FDE (Full Disk Encryption)
- Software technology

SDN (Software Defined Networking)
SSP (System Security Plan)
SHE (Structured Exception Handler)
HSM (Hardware Security Module)
EFS (Encrypting File System)
AES (Advanced Encryption Standard)

High availability server clustering (H/A)
- Active/Active mode
    - Distributes traffic to all servers
    - 2 or more load balancers working in tandem
    - Aggregate the load
    - Save user info for return requests
    - Disadvantage is running at near full capacity
        - No overhead or room for failure
- Active/Passive mode
    - Not all load balancers are active
    - Passive ones monitor the active
    - When it goes down a passive steps in
    - Failover
    - Distributes traffic to servers marked as active

Load balancing
- Round Robin
    - Request allocated to the next sequential server
    - Weighted round robin introduces variance for server processing power.
- Session affinity
    - Feature on load balancers
    - Allows subsequent request from user to pass through to original server.
    - Disregards balancing rules
    - AKA
        - Server Sticky
        - Session Persistence
        - Server affinity
        - Server persistence

Data Center traffic
- East-West
    - Traffic within data center
    - Server-to-server
- North-South
    - Traffic that exits the data center
    - Server-to-client

VPN's

- VPN Concentrator
    - Dedicated device
    - Single point for VPN connections from outside organization
    - Responsible for security of encrypted connections
- Split Tunnel
    - Uses VPN private connection and open connection
    - Alleviates bottlenecks
    - Can specify applications to use either or
- Full Tunnel
    - Using the VPN for all traffic
    - More secure than split tunneling
    - Uses more bandwidth
- Tethering
    - VPN on mobile device
    - Tether to computer or other device
- VPN Type
    - Remote Access
        - Allows remote user to remote in the organization
    - Intranet-Based
        - Provide site-to-site internal connectivity
        - Within a company
        - Different physical locations
    - Client-to-Site
        - Connect and individual device to the internal organization
    - Site-to-Site
        - Connection between 2 or more networks
        - Such as corporate network and a branch of the company
    - Extranet-Based
        - Extend resources to outside the company
        - Suppliers
        - Customers
        - Partners
- Common Tunnel Protocols
    - OpenVPN
    - IKEv2/IPsec
    - WireGaurd
    - SSTP
    - L2TP/IPsec
    - TLS
- Depreciated protocols
    - GRE (Generic Routing Encapsulation)
    - PPTP (Point-to-Point Tunneling Protocol)

STP frame (Spanning Tree Protocol)

- Use of BPDU (Bridge Protocol Data Units)
- Used to establish a spanning tree
- Types
    - Configuration BPDU
        - Determine port roles
        - Elect root bridge
    - Topology change notification (TCN) BDPU

EAP (Extensible Authentication Protocol)

- Authentication Framework
- Networking and Internet connections
- Defined in RFC 3748
- Updated by RFC 5247
- Not a wire protocol
- LEAP
    - Lightweight Extensible Authentication Framework
    - User credentials easily compromised
    - Cisco recommends to not use this
- EAP-TLS (MOST SECURE)
    - Transport Layer Security
    - Client side and server side certificates for authentication
    - RFC 5216
    - Open standard
    - Very popular
- EAP-MD5
    - MD5 hash function
    - Minimal security
- EAP-POTP
    - Protected One-Time Password
    - OTP tokens
    - Provides 2FA
- EAP-PSK
    - Pre Shared Key
- EAP-PWD
    - Password
- EAP-TTLS
    - Tunneled Transport Layer Security
    - Extends TLS
    - Does not require a CA-signed PKI certificate to server
- EAP-IKEv2
    - Internet Key Exchange v2
    - Mutual authentication and session key establishment
    - Supports
        - Asymmetric key pairs
        - Passwords
        - Symmetric keys
- EAP-FAST
    - Flexible Authentication via Secure Tunneling
    - Replacement for LEAP by Cisco
    - More secure but still lightweight
    - Uses a PAC (Protected Access Tunnel) to establish a TLS tunnel in which credentials are verified.
- TEAP
    - Tunnel Extensible Authentication Protocol
    - Tunnel-based EAP method
    - Uses TLS
- EAP-SIM
    - Subscriber Identity Module
    - Uses SIM card ang GSM network

    - GSM (Global System for Mobile Communication)
- EAP-AKA
    - Authentication and Key Agreement
    - For UMTS (Universal Mobile Telecommunications System)
- EAP-GTC
    - Generic Token Card
- EAP-EKE
    - Encrypted Key Exchange
- EAP-NOOB
    - Nimble Out-Of-Band

WPA3
- Enterprise
    - Large networks
    - IEEE 802.1X
    - Requires RADIUS server
    - AES-GCMP
    - AES-CCMP (also)
- Personal
    - SAE
    - No server

WPA2
- AES-CCMP
    - Encryption scheme
- Personal
    - Home networks
    - Not as secure
    - PSK (Pre Shared Key)(Client Authentication method)
    - No server required
- Enterprise
    - SAE (Simultaneous Authentication of Equals)(Client authentication method)
    - Uses a server for authentication

WEP (Wired Equivalent Privacy)
- Old
- Depreciated
- Not secure

WPA
- Wi-Fi Protected Access
- Replaced WEP
- Depreciated
- Vulnerable to Brute Force attacks
- Used TKIP (Replaced by AES)

WPS (Wi-Fi Protected Setup)
- Easily allows non-technical users to setup and add devices to network

IEEE
- 802.1x
    - PNAC (Port-based Network Access Control)
    - Authenticated by a central authority
    - Ethernet switch authenticates

    - For devices connecting to network via its ports
    - Used in enterprise modes
- 802.3
    - LAN
    - Physical link layer
    - Data Transmission layer
- 802.11
    - Wireless standard
    - Wi-Fi
    - 2.4/5 GHz
- 802.15
    - Zigbee
    - 2.4GHz

RADIUS (Remote Authentication Dial-in User Service)
- Primarily used for network access
- Combines authentication and authorization
- Encrypts only the password in the access-request packet

TACASA+ (Terminal Access Controller Access Control System plus)
- Primarily used for device management
- Separates Authentication and authorization
- Encrypts the entire payload of the access-request packet

MAC - Mandatory
DAC - Discretionary
Role-BAC - Roles
Rule-BAC - Rules
ABAC - Attribute
FACL - File Access Control List
- Rule-BAC

FIM - File Integrity Monitoring
- Detect unauthorized changes to files

EFM - Encrypting File System
- Windows mechanism

PAM - Pluggable Authentication Modules
- Modular authentication system
- Provides flexibility
- Enforces policies such as passwords
- Account lockouts
- 2FA
- Widely used in Unix/Linux systems

CRL - Certificate Revocation List
OCSP - Online Certificate Status Protocol
- Interactive
- Using an OCSP responder

CSR - Certificate Signing Request
CN - Common Name
- Device
- Individual
- Organization
- Other identity the cert is issued for

FQDN - Fully Quantified Domain Name

- In a SSL the CN must match the FQDN (It refers to it)
- e.g. www.example.com
- That is = hostname.SLD.TLD

Wildcard certificate

- Allows registration for one root domain
- Such as a SLD
- Allows all subdomains to be covered under it
- Example.com
- Mail.example.com
- Cars.example.com
- Etc…

SAN (Subject Alternative Name) certificate

- AKA Multi-Domain
- For one organization to secure multiple domains

EV (Extended Validation) Certificate

- Highest Level of security

Root Certificate

- Self-signed by a RCA (Root Certificate Authority)

Code-Signing Certificates

- For software
- Validate integrity

Self-signed

- Lower security

Computer certificates

- Prove identity of a device

S/MIME Certificates

- For encrypting and digitally signing email messages

x.509 Certificates

- PEM - Privacy Enhanced Mail
    - Most common format
    - Text file
    - Base64 ASCII
    - Apache server or similar
    - Plain text headers and footer
    - Filename extensions
        - .crt
        - .pem
        - .cer
        - .key

- PB7 (PKCS#7)
    - Base64 ASCII
    - Microsoft windows and Java Tomcat server
    - .p7b

- PFX (PKCS#12 or PKCS12) (Personal Information Exchange)
    - Binary
    - Windows servers
    - Store certificate chain and private key in single encrypt-able file
    - .p12
    - .pfx

- DER (Distinguished Encoding Rules)
    - Binary encoding for x.509 certificates and private keys
    - Mostly seen in JAVA contexts
    - No plaintext components
    - .der
    - .cer

Key Escrow
- Third-party trusted
- Copy of encryption keys
- Can be used for malicious purposes
- Recovery agent
    - Individual or organization
    - Access to key database
    - Permission level to allow extraction
    - Responsible for maintaining key integrity

Logging
- NXLog
    - Cross platform
    - Log-managing tool
- Journalctl
    - Linux
    - Querying and displaying log files
    - Binary
- NetFlow
    - Cisco
    - IP Traffic collection
    - No packet sampling
- sFlow
    - Packet sampling
    - Cross platform
    - Collection method
- IPFIX
    - IETF standard
    - Defines IP flow information for formatting and transfer from exporter to collector

SOAR Playbook - checklist of actions performed in response to security incident
SOAR Runbook - Exact steps to enable an automated response to a security incident

ISO/IEC (International Organization for Standardization/International Electrotechnical Commission)
- 27001
    - Globally recognized InfoSec standard
    - Requirements for ISMS (Information Security Management System)
    - Systematic approach
    - Manage and protect sensitive information
    - Specifies security controls and procedures to protect information assets
- 27002
    - Code of practice for information security management
    - Guidelines and principles

        - Initiating
        - Implementing
        - Maintaining
        - Improving
        - Infosec management in an organization
    - InfoSec risks and management guidelines
        - Security management
        - Asset management
        - Human resource security
        - Physical and environmental security
        - Communications and operations management
        - Information security incident management
- 27701
    - Extension to 27001/27002
    - Additional privacy information management requirements and controls
    - Focus on privacy data management
- 31000
    - Risk management standard
    - Framework
        - Identify
        - Assess
        - Manage risks
    - Guidelines
        - Risk assessment
        - Risk treatment
        - Risk management process
    - Applicable to all types of organizations

CCM - Cloud Controls Matrix
CSA - Cloud Security Alliance
CSF - NIST Cyber Security Framework
CIS - Center for Internet Security
AUP - Acceptable Use Policy
SLA - Service Level agreement
EULA - End User Level Agreement
BPA - Business Partnership Agreement
MOU - Memorandum Of Understanding
MOA - Memorandum of Agreement
NDA - Non Disclosure Agreement
ISA - Interconnection Security Agreement (For Extranet)
SOW - Statement of Work
MSA - Master Service Agreement (Service provider and client. Responsibilities and expectations)
ALE - Annual Loss Expectancy
EOL - End of Life
EOSL - End of Service Life
ETL - Extract, Transform, Load
SDLC - Software Development Life-Cycle
EOF - End of File
ERP - Enterprise Recourse Planning
SLE - Single Loss Expectancy
ALE - Annual Loss Expectancy
ARO - Annual Rate of Occurrence