|  |  |  |
| --- | --- | --- |
| 21 TCP | FTP | File Transfer Protocol is used to transfer files from host to host |
| 22 TCP/UDP | SSH, SCP, SFTP | Secure Shell is used to remotely administer network devices and systems. SCP is used for secure copy and SFTP for secure FTP. |
| 23 TCP/UDP | Telnet | Unencrypted method to remotely administer network devices (should not be used) |
| 25 TCP | SMTP | Simple Mail Transfer Protocol is used to send email over the Internet |
| 53 TCP/UDP | DNS | Domain Name Service is used to resolve hostnames to IPs and IPs to hostnames |
| 69 UDP | TFTP | Trivial FTP is used as a simplified version of FTP to put a file on a remote host, or get a file from a remote host |
| 80 TCP | HTTP | Hyper Text Transfer Protocol is used to transmit web page data to a client for unsecured web browsing |
| 88 TCP/UDP | Kerberos | Used for network authentication using a system of tickets within a Windows domain |
| 110 TCP | POP3 | Post Office Protocol v3 is used to receive email from a mail server |
| 119 TCP | NNTP | Network News Transfer Protocol is used to transport Usenet articles |
| 123 UDP | NTP | NTP Provides time synch between computers and network systems |
| 135 TCP/UDP | RPC/DCOM-sc m | Remote Procedure Call is used to located DCOM ports request a service from a program on another computer on the network |
| 137-139 TCP/UDP | NetBIOS | NetBIOS is used to conduct name querying, sending of data, and other functions over a NetBIOS connection |
| 143 TCP | IMAP | Internet Message Access Protocol is used to receive email from a mail server with more features than POP3 |
| 161 UDP | SNMP | Simple Network Management Protocol is used to remotely monitor network devices |
| 162 TCP/UDP | SNMPTRAP | Used to send Trap and InformRequests to the SNMP Manager on a network |
| 389 TCP/UDP | LDAP | Lightweight Directory Access Protocol is used to maintain directories of users and other objects |
| 443 TCP | HTTPS | Hyper Text Transfer Protocol Secure is used to transmit web page data to a client over an SSL/TLS-encrypted connection |
| 445 TCP | SMB | Server Message Block is used to provide shared access to files and other resources on a network |
| 465/587 TCP | SMTP with SSL/TLS | Simple Mail Transfer Protocol used to send email over the Internet with an SSL and TLS secured connection |
| 514 UDP | Syslog | Syslog is used to conduct computer message logging, especially for routers and firewall logs |
| 636 TCP/UDP | LDAP SSL/TLS | LDAP is used to maintain directories of users and other objects over an encrypted SSL/TLS connection |
| 860 TCP | iSCSI | iSCSI is used for linking data storage facilities over IP |
| 989/990 TCP | FTPS | File Transfer Protocol Secure is used to transfer files from host to host over an encrypted connection |
| 993 TCP | IMAP4 with SSL/TLS | Internet Message Access Protocol is used to receive email from a mail server over an SSL/TLS-encrypted connection |
| 995 TCP | POP3 (SSL/TLS) | Post Office Protocol v3 is used to receive email from a mail server using an SSL/TLS-encrypted connection |
| 1433 TCP | Ms-sql-s | Microsoft SQL server is used to receive SQL database queries from clients |
| 1645/1646 UDP | RADIUS (alternative) | Remote Authentication Dial-In User Service is used for authentication and authorization (1645) and accounting (1646) |
| 1701 UDP | L2TP | Layer 2 Tunnel Protocol is used as an underlying VPN protocol but has no inherent security |
| 1723 TCP/UDP | PPTP | Point-to-Point Tunneling Protocol is an underlying VPN protocol with built-in security |
| 1812/1813 UDP | RADIUS | Remote Authentication Dial-In User Service is used for authentication and authorization (1812) and accounting (1813) |
| 3225 TCP/UDP | FCIP | Fibre Channel IP is used to encapsulate Fibre Channel frames within TCP/IP packets |
| 3260 TCP | iSCSI Target | iSCSI Target is as the listening port for iSCSI-targeted devices when linking data storage facilities over IP |
| 3389 TCP/UDP | RDP | Remote Desktop Protocol is used to remotely view and control other Windows systems via a Graphical User Interface |
| 3868 TCP | Diameter | A more advanced AAA protocol that is a replacement for RADIUS |
| 6514 TCP | Syslog over TLS | It is used to conduct computer message logging, especially for routers and firewall logs, over a TLS-encrypted connection |

Ports can be any number between 0 and 65,535 = private IP addresses are either 10.x.x.x, 172.16-31.x.x, or 192.168.x.x.

**Hping is a handy little utility that assembles and sends custom ICMP, UDP, or TCP packets and then displays any replies. It was inspired by the ping command but offered far more control over the probes sent.**

**IPsec is the most secure protocol that works with VPNs.**

**Banner grabbing is conducted by actively connecting to the server using telnet or netcat and collecting the web server's response. This banner usually contains the server's operating system and the version number of the service (SSH) being run.**

**Open ID Connect (OIDC) is an authentication protocol that can be implemented as special types of OAuth flows with precisely defined token fields.**

**OpenID: an open standard, providing decentralized authentication, allowing users to log into multiple unrelated websites with one set of credentials maintained by a third-party service referred to as an OpenID provider**

**OAuth2.0: is an open standard for authorization, commonly used as a way for internet users to log into third-party websites using their Microsoft, google, fb, twitter, etc, accounts without exposing their password (Azure AD)**

**Security Assertion Markup Language (SAML): is an XML-based, open-standard data format for exchanging authentication and authorization data between parties, in particular, between and IdP(identity provider) and a SP(service provider) – common in on-prem federation scenarios**

**Kerberos – authorized protocol in MF Azures AD (NTLM) stronger encryption, interpretability, and mutual authentication (Client and server verified), tuns as a 3rd party trusted server known as the key dist provider KDC, includes an auth server, ticket granting service, and a database of secret keys for users and services, helps prevent replay attacks through timestamps**

***Heuristic analysis* is a method employed by many computer anti-virus programs designed to detect previously unknown computer viruses and new variants of viruses already in the wild.**

**The Federal Information Security Management Act (FISMA) is a United States federal law that defines a comprehensive framework to protect government information, operations, and assets against natural or human-made threats. FISMA requires that government agencies and other organizations that operate systems on behalf of government agencies comply with security standards.**

**In what order should the digital evidence be collected based on the order of volatility?** **Processor Cache, Random Access Memory, Swap File, and then the Hard Drive or USB Drive**

**o Well-Known Ports**

▪ Ports 0 to 1023 are considered well-known and are assigned by the Internet Assigned Numbers Authority (IANA)



**o Registered Ports**

▪ Ports 1024 to 49,151 are considered registered and are usually assigned to proprietary protocols

**o Dynamic or Private Ports**

▪ Ports 49,152 to 65,535 can be used by any application without being registered with IANA

**o Software as a Service (SaaS)**

▪ Provides all the hardware, operating system, software, and applications needed for a complete service to be delivered

**o Infrastructure as a Service (IaaS)**

▪ Provides all the hardware, operating system, and backend software needed to develop your own software or service

**o Platform as a Service (PaaS)**

▪ Provides your organization with the hardware and software needed for a specific service to operate

**o Physical Layer**

▪ Represents the actual network cables and radio waves used to carry data over a network

▪ Bits

**o Data Link Layer**

▪ Describes how a connection is established, maintained, and transferred over the physical layer and uses physical addressing (MAC addresses)

▪ Frames

**o Network Layer**

▪ Uses logical address to route or switch information between hosts, the network, and the internetworks

▪ Packets

**o Transport Layer**

▪ Manages and ensures transmission of the packets occurs from a host to a destination using either TCP or UDP

▪ Segments (TCP) or Datagrams (UDP)

**o Session Layer**

▪ Manages the establishment, termination, and synchronization of a session over the network

**o Presentation Layer**

▪ Translates the information into a format that the sender and receiver both understand

**o Application Layer**

▪ Layer from which the message is created, formed, and originated

▪ Consists of high-level protocols like HTTP, SMTP, and FTP

**o Network Access Control (NAC)**

▪ Security technique in which devices are scanned to determine its current state prior to being allowed access onto a given network

▪ If a device fails the inspection, it is placed into digital quarantine

**o netflow**

▪ A network protocol system created by Cisco that collects active IP network traffic as it flows in or out of an interface, including its point of origin, destination, volume and paths on the network

**o sflow**

▪ Short for “sampled flow”, it provides a means for exporting truncated packets, together with interface counters for the purpose of network monitoring

**o Internet Protocol Flow Information Export (IPfix)**

▪ A universal standard of export for Internet Protocol flow information from routers, probes and other devices that are used by mediation systems, accounting/billing systems and network management systems to facilitate services such as measurement, accounting and billing by defining how IP flow information is to be formatted and transferred from an exporter to a collector

* Network address translation (NAT)
  + a feature found in many firewalls, translates between external and internal IP addresses. With NAT, a private network can use internal, non-routable IP addresses that map to one or more external IP addresses. Furthermore, a single IP address can represent many computers within a network.

**Bluetooth Attacks**

**o Bluejacking**

▪ Sending of unsolicited messages to Bluetooth-enabled devices

**o Bluesnarfing**

▪ Unauthorized access of information from a wireless device over a Bluetooth connection

**o Bluejacking sends information to a device**

**o Bluesnarfing takes information from a device**

**o War Dialing**

**▪ Protect dial-up resources by using the callback feature**

**o Degaussing**

* Exposes the hard drive to a powerful magnetic field which in turn causes previously written data to be wiped from the drive
* You cannot reuse a hard drive once it has been degaussed.

**o Purging (Sanitizing)**

▪ Act of removing data in such a way that it cannot be reconstructed using any known forensic techniques

**o Clearing/Wiping**

* Removal of data with a certain amount of assurance that it cannot be reconstructed
* Data wiping or clearing occurs by using a software tool to overwrite the data on a hard drive to destroy all electronic data on a hard disk or other media. Data wiping may be performed with a 1x, 7x, or 35x overwriting, with a higher number of times being more secure.
* This allows the hard drive to remain functional and allows for hardware reuse.

**o Sarbanes-Oxley (SOX)- Stocks**

▪ Affects publicly-traded U.S. corporations and requires certain accounting methods and financial reporting requirements

**o Gramm-Leach-Bliley Act (GLBA)**

▪ Affects banks, mortgage companies, loan offices, insurance companies, investment companies, and credit card providers

**o Federal Information Security Management (FISMA) Act of 2002**

▪ Requires each agency to develop, document, and implement an agency-wide information systems security program to protect their data

**o Data Owner**

* A senior (executive) role with ultimate responsibility for maintaining the confidentiality, integrity and availability of the information asset
* The data owner is responsible for labeling the asset and ensuring that it is protected with appropriate controls
* The data owner is usually a higher-level executive who makes business decisions regarding the data.

**o Data Steward**

▪ A role focused on the quality of the data and associated metadata

**o Data Custodian**

▪ A role responsible for handling the management of the system on which the data assets are stored, The data custodian manages access rights and sets security controls to the data.

**o Data Privacy/Protection officer**

▪ A role responsible for the oversight of any PII/SPI/PHI assets managed by the company, A privacy officer sets privacy policies and implements privacy processes and procedures.

**Data processor**

The data processor manages the operational use of the data, but not the rights and permissions to the information

**o RAID 0**

▪ Provides data striping across multiple disks to increase performance

**o RAID 1**

▪ Provides redundancy by mirroring the data identically on two hard disks

**o RAID 5**

▪ Provides redundancy by striping data and parity data across the disk Drives

**o RAID 6**

▪ Provides redundancy by striping and double parity data across the disk Drives

**o RAID 10**

▪ Creates a striped RAID of two mirrored RAIDs (combines RAID 1 & RAID 0)

* **LDAP and Kerberos**
  + Lightweight Directory Access Protocol (LDAP)
    - A database used to centralize information about clients and objects on the network
    - Unencrypted
      * Port 389
    - Encrypted
      * Port 636
    - Active Directory is Microsoft’s version

**Kerberos**

* An authentication protocol used by Windows to provide for two-way(mutual) authentication using a system of tickets
* Kerberos
  + Port 88
* A domain controller can be a single point of failure for Kerberos

o dd

▪ A command line utility used to copy disk images using a bit by bit copying process

o FTK Imager

▪ A data preview and imaging tool that lets you quickly assess electronic evidence to determine if further analysis with a forensic tool is needed

o Memdump

▪ A command line utility used to dump system memory to the standard output stream by skipping over holes in memory maps

o WinHex

▪ A commercial disk editor and universal hexadecimal editor used for data recovery and digital forensics

o Autopsy

▪ A digital forensics platform and graphical interface to The Sleuth Kit® and other digital forensics tools

o Browser Exploitation Framework (BeEF)

▪ A tool that can hook one or more browsers and can use them as a beachhead of launching various direct commands and further attacks against the system from within the browser context

* CRLF injection
  + a software application coding vulnerability that occurs when an attacker injects a CRLF character sequence where it is not expected.

● NIDS vs NIPS

o Network Intrusion Detection Systems

▪ Attempts to detect, log, and alert on malicious network activities

▪ NIDS use promiscuous mode to see all network traffic on a segment

o Network Intrusion Prevention Systems

▪ Attempts to remove, detain, or redirect malicious traffic

▪ NIPS should be installed in-line of the network traffic flow

▪ Should a NIPS fail open or fail shut?

▪ NIPS can also perform functions as a protocol analyzer

● Unified Threat Management (UTM)

o Relying on a firewall is not enough

o Unified Threat Management

▪ Combination of network security devices and technologies to provide more defense in depth within a single device

▪ UTM may include a firewall, NIDS/NIPS, content filter, anti-malware, DLP, and VPN

▪ UTM is also known as a Next Generation Firewall (NGFW)

● Remote Access Services

o Password Authentication Protocol (PAP)

▪ Used to provide authentication but is not considered secure since it transmits the login credentials unencrypted (in the clear)

o Challenge Handshake Authentication Protocol (CHAP)

▪ Used to provide authentication by using the user’s password to encrypt a challenge string of random numbers

o Access Control List (ACL)

* An ordered set of rules that a router uses to decide whether to permit or deny traffic based upon given characteristics
* IP Spoofing is used to trick a router’s ACL
* Bet practices of firewall configurations, should include **an implicit deny at the end of your ACL rules**

o Static Analysis

▪ Source code of an application is reviewed manually or with automatic tools without running the code

o Dynamic Analysis

▪ Analysis and testing of a program occurs while it is being executed or run

o Fuzzing

▪ Injection of randomized data into a software program to find system failures, memory leaks, error handling issues, and improper input validation

**o Symmetric Algorithms**

▪ DES, 3DES, IDEA, AES, Blowfish, Twofish, RC4, RC5, RC6

**o Data Encryption Standard (DES)**

▪ Encryption algorithm which breaks the input into 64-bit blocks and uses transposition and substitution to create ciphertext using an effective key

strength of only 56-bits

▪ DES used to be the standard for encryption

**o Triple DES (3DES)**

▪ Encryption algorithm which uses three separate symmetric keys to encrypt, decrypt, then encrypt the plaintext into ciphertext in order to increase the strength of DES

**o International Data Encryption Algorithm (IDEA)**

▪ Symmetric block cipher which uses 64-bit blocks to encrypt plaintext into ciphertext

**o Advanced Encryption Standard (AES)**

▪ Symmetric block cipher that uses 128-bit, 192-bit, or 256-bit blocks and a matching encryption key size to encrypt plaintext into ciphertext

▪ AES is the standard for encrypting sensitive U.S. Government data

**o Blowfish**

▪ Symmetric block cipher that uses 64-bit blocks and a variable lengthencryption key to encrypt plaintext into ciphertext

**o Twofish**

▪ Symmetric block cipher that replaced blowfish and uses 128-bit blocks and a 128-bit, 192-bit, or 256-bit encryption key to encrypt plaintext into ciphertext

**o Rivest Cipher (RC4)**

▪ Symmetric stream cipher using a variable key size from 40-bits to 2048-bits that is used in SSL and WEP

**o Rivest Cipher (RC5)**

▪ Symmetric block cipher with a key size up to 2048-bits

**o Rivest Cipher (RC6)**

▪ Symmetric block cipher that was introduced as a replacement for DES but AES was chosen instead

**o Exam Tips**

▪ RC4 is the only stream cipher covered

**o Asymmetric Algorithms**

▪ Diffie-Hellman, RSA, and ECC

**o Diffie-Hellman (DH)**

▪ Used to conduct key exchanges and secure key distribution over an unsecured network

▪ Diffie-Hellman is used for the establishment of a VPN tunnel using IPSec

**o RSA (Rivest, Shamir, and Adleman)**

▪ Asymmetric algorithm that relies on the mathematical difficulty of factoring large prime numbers

▪ RSA is widely used for key exchange, encryption, and digital signatures

▪ RSA can use key sizes of 1024-bits to 4096-bits

**o Elliptic Curve Cryptography (ECC)**

▪ Algorithm that is based upon the algebraic structure of elliptic curves over finite fields to define the keys

▪ ECC with a 256-bit key is just as secure as RSA with a 2048-bit key

▪ ECDH

● Elliptic Curve Diffie-Hellman

▪ ECDHE

● Elliptic Curve Diffie-Hellman Ephemeral

▪ ECDSA

● Elliptic Curve Digital Signature Algorithm

▪ ECC is most used for mobile devices and low-power computing device

**o Recovery Time Objective (RTO)**

▪ The length of time it takes after an event to resume normal business operations and activities

**o Work Recovery Time (WRT)**

▪ The length of time in addition to the RTO of individual systems to perform reintegration and testing of a restored or upgraded system following an event

**o Recovery Point Objective (RPO)**

▪ The longest period that an organization can tolerate lost data being unrecoverable

▪ Recovery Point Objective (RPO) is focused on how long can you be without your data

▪ MTD and RPO help to determine which business functions are critical and to specify appropriate risk countermeasures

▪ Designing your disaster recovery and continuity of operations plans requires an understanding of your availability and reliability levels

o Disasters can be caused by internal or external forces

**ISO 27701**

designed to enhance privacy controls towards adding or improving a Privacy Information Management System (PIMS).

**▪ Mean Time To Repair (MTTR)**

● Measures the average time it takes to repair a network device when it breaks

**▪ Mean Time Between Failures (MTBF)**

● Measures the average time between failures of a device

**o Sarbanes-Oxley (SOX)-Stocks**

▪ Affects publicly-traded U.S. corporations and requires certain accounting methods and financial reporting requirements

**o Gramm-Leach-Bliley Act (GLBA)**

▪ Affects banks, mortgage companies, loan offices, insurance companies, investment companies, and credit card providers

**o Federal Information Security Management (FISMA) Act of 2002**

▪ Requires each agency to develop, document, and implement an agency-wide information systems security program to protect their data

**o Payment Card Industry Data Security Standard (PCI DSS) is a contractual obligation**

**o Help America Vote Act (HAVA) of 2002**

▪ Provides regulations that govern the security, confidentiality, and integrity of the personal information collected, stored, or processed during the election and voting process

**o SB 1386 requires any business that stores personal data to disclose a breach**

**o General Data Protection Regulation (GDPR)**

▪ Personal data cannot be collected processed or retained without the individual's informed consent

▪ GDPR also provides the right for a user to withdraw consent, to inspect, amend, or erase data held about them

▪ GDPR requires data breach notification within 72 hours

**● Privacy Technologies**

**o Deidentification**

▪ methods and technologies that remove identifying information from data before it is distributed

▪ Deidentification is often implemented as part of database design

**o Data Masking**

▪ Deidentification Method where generic or placeholder labels are substituted for real data while preserving the structure or format of the original data

**o Tokenization**

▪ A deidentification method where a unique token is substituted for real data

**o HVAC**

▪ Heating, Ventilation, and Air Conditioning

**o Humidity should be kept around 40%**

**o HVAC systems may be connected to ICS and SCADA networks**

**● Vendor Relationships**

**o Non-Disclosure Agreement (NDA)**

▪ Agreement between two parties that defines what data is considered confidential and cannot be shared outside of the relationship

▪ NDAs are a binding contract

**o Memorandum of Understanding (MOU)**

▪ A non-binding agreement between two or more organizations to detail an intended common line of action

▪ MOUs can be between multiple organizations

**o Service-Level Agreement (SLA)**

▪ An agreement concerned with the ability to support and respond to problems within a given timeframe and continuing to provide the agreed upon level of service to the user

▪ SLA may promise 99.999% uptime

**o Interconnection Security Agreement (ISA)**

▪ An agreement for the owners and operators of the IT systems to document what technical requirements each organization must meet

**o Business Partnership Agreement (BPA)**

▪ Conducted between two business partners that establishes the conditions of their relationship

▪ A BPA can also include security requirements

**PKI -**

**Key management –**

Management of cryptographic keys, operational considerations, design considerations

**Certificate Authority (CA)**

**Server that** Creates digital certificates and own the policies PKI can include a single CA that serves as root and issuing, but this is not recommended

**Subordinate CA (Policy CA) known as Registration Authority (RA)**

Sits below root CA, regularly issues certificates, difficult to stay offline as often as root ca. The registration authority works with the certificate authority to identify and authenticate the certificate requester.

**Certificate revocation list (CRL)**

contains info about any certificates that have been revoked by a subordinate CA(RA) due to compromises to the certificate or PKI hierarchy

**CAs required to publish CRLs**

**Online Certificate States Protocol (OCSP)**

Offers a faster way to check a certificates status compared to downloading a CRL, the consumer of a certificate can submit a request to the issuing CA to obtain the status of a specific certificate

**Certificate Signing Request (CSR):**

Records identifying information for a person or device that owns a private key as well as information on the corresponding public key, it’s the message that’s sent to the CA to get a digital certificate created

**CN (Common Name)**

Fully qualified domain name (FQDN) on the entity (server)

**Subject alternative name (SAN)**

An extension to the X.509 specification that allows users to specify additional host names for a single SSL certificate, standard practice for SSL certificates, Enables full support for FQDNs from multiple domains in a single certificate

**Expiration**

Certificates are valid for a limited period from the date of issuance as specified on the certificate, current industry guidance on maximum certificate lifetime currently 1 year(398days)

**Types of certificates**

**Wildcard**

Supports multiple FQDNs in the same domain

Ex – contoso.com is the domain, and two servers(web, mail) the wildcard certificate is \*.contoso.com, can be used on multiple servers on the same domain saving costs

**Subject Alternate Name (SAN)** – multiple domains in a single cert

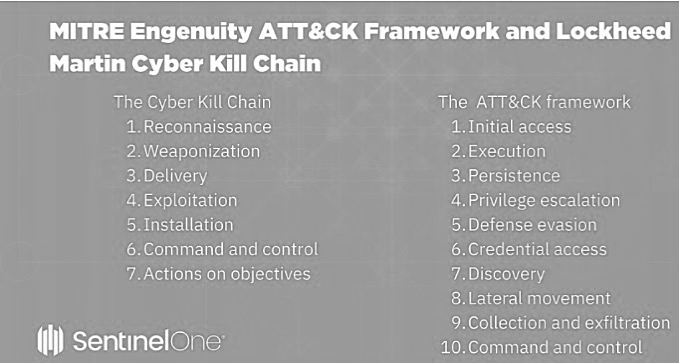
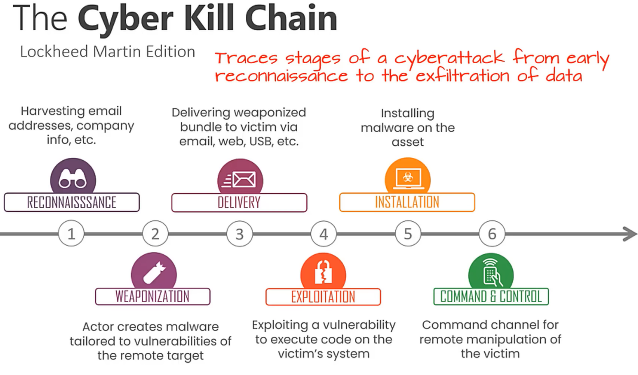
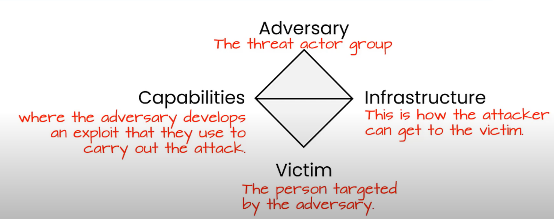
Can be used on multiple names such as xyz.com and abc.com, can also insert info onto the cert such as an IP address

**Code Signing-**

When code is distributed over the internet, it is essential that users can trust that it was actually produced by the claimed sender, proof of content integrity

Self-Signed

|  |  |  |
| --- | --- | --- |
|  | 6 Phases of Incident Response |  |
| 1 | Preparation | Where incident response plants are written and configs. Documented |
| 2 | Identification | Determining whether or not an org. has been breached, is it really an incident? |
| 3 | Containment | Limiting Damage (scope) of incident, isolate |
| 4 | Eradication | Once affected systems are identified, coordinated isolation or shutdown, rebuild and notifications |
| 5 | Recovery | Root cause is addressed and time to turn to normal operations is estimated and executed |
| 6 | Lessons Learned | Helps prevent recurrence, improve IR process |



The **ALE** (Annual Loss Expectancy) is the total amount of the loss over an entire year.

**SLE** (Single Loss Expectancy) describes the loss for a single incident.

**SLA** (Service Level Agreement) is a contractual agreement that specifies a minimum service level.

An **ARO** (Annualized Rate of Occurrence) is the number of times an event is expected to occur in a year.

Most Volatile

1. CPU registers/CPU Cache
2. Router Table, ARP Cache, Process Table, Kernel Statistics, Memory
3. Temp file systems
4. Disk
5. Remote logging & monitoring data
6. Phys. Config., network topology
7. Archival Media

ISO 27701

The ISO (International Organization for Standardization) 27701

standard extends the ISO 27001 and 27002 standards to include detailed

management of PII (Personally Identifiable Information) and data privacy.

ISO 31000

The ISO 31000 standard sets international standards for risk management

practices.

ISO 27002

Information security controls are the focus of the ISO 27002 standard.

ISO 27001

The ISO 27001 standard is the foundational standard for Information

Security Management Systems (ISMS).

Trusted Boot

The Trusted Boot portion of the startup process verifies the operating

system kernel signature and starts the ELAM (Early Launch

Anti-Malware) process.

Measured Boot

Measured Boot occurs after the Trusted Boot process and verifies that

nothing on the computer has been changed by malicious software or other

processes.

Secure Boot

Secure Boot is a UEFI BIOS boot feature that checks the digital signature

of the bootloader.

Obfuscation

Obfuscation is the process of making something difficult for humans to

read or understand.

Data custodian

The data custodian manages access rights and sets security controls

to the data.

Data processor

The data processor manages the operational use of the data, but not the

rights and permissions to the information.

Data owner

The data owner is usually a higher-level executive who makes business

decisions regarding the data.

Privacy officer

A privacy officer sets

Data owner

The data owner is accountable for specific data, and is often a senior officer

of the organization.

Data protection officer

The data protection officer (DPO) is responsible for the organization's

data privacy. The DPO commonly sets processes and procedures for

maintaining the privacy of data.

Data steward

The data steward manages access rights to the data. In this example, the IT

team would be the data steward.

Data processor

The data processor

**o Data Owner**

* A senior (executive) role with ultimate responsibility for maintaining the confidentiality, integrity and availability of the information asset
* The data owner is responsible for labeling the asset and ensuring that it is protected with appropriate controls
* The data owner is usually a higher-level executive who makes business decisions regarding the data.

**o Data Steward**

▪ A role focused on the quality of the data and associated metadata

**o Data Custodian**

▪ A role responsible for handling the management of the system on which the data assets are stored, The data custodian manages access rights and sets security controls to the data.

**o Data Privacy/Protection officer**

▪ A role responsible for the oversight of any PII/SPI/PHI assets managed by the company, A privacy officer sets privacy policies and implements privacy processes and procedures.

**Data processor**

The data processor manages the operational use of the data, but not the rights and permissions to the information

CASB

Visibility

-determine apps being used

-are they authorized to use the apps?

Compliance

-are users complying with HIPAA? PCI?

Threat prevention

-allow access by authorized users, prevent attacks

Data Security

-ensure all data transfers are encrypted

-protect transfer of PII with DLP