Introduction

Fundamental Security Concepts

The whole principle is to avoid **Theft, Tampering and Disruption** of the systems through **CIA Triad** (Confidentiality, Integrity and Availability).

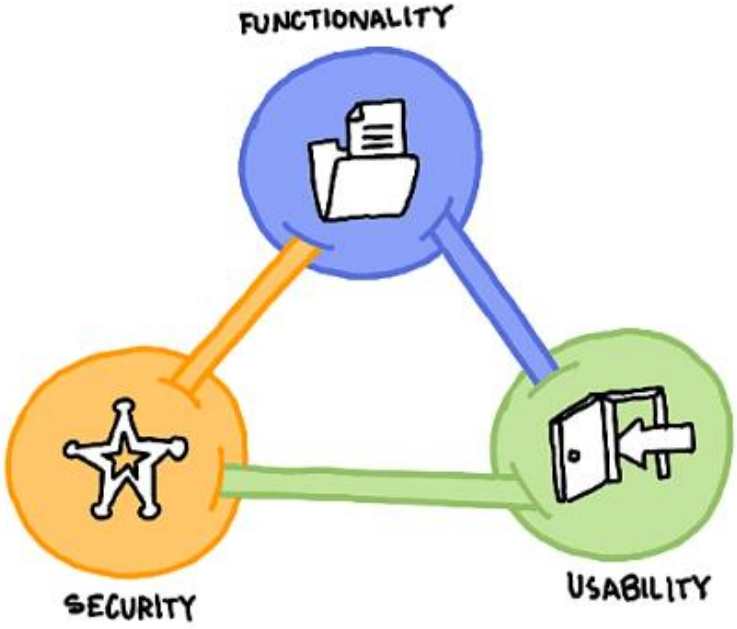
- **Confidentiality** Keeping systems and data from being accessed, seen, read to anyone who is not authorized to do so. Information is accessible only to the autorized personnel.
- **Integrity** TRUSTWORTHINESS OF DATA OR RESOUCES: Protect the data from modification or deletion by unauthorized parties, and ensuring that when authorized people make changes that shouldn't have been made the damage can be undone.
- **Availability** ACCESSIBLE WHEN REQUIRED BY AUTHORIZED USERS: Systems, access channels, and authentication mechanisms must all be working properly for the information they provide and protect to be available when needed.
- **Authenticity** Refers to the characterstic of a communication, document, or any data that ensures the quality of being geniune.

Note: *In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved. (ISO/IEC 27000:2009)*

- **Auditing & Accountability** Basically keep tracking of everthing, like, who's been logging in when are they loggin in whose access this data.
- **Non-Repudiation** Non-repudiation is the assurance that someone cannot deny the validity of something. Non-repudiation is a legal concept that is widely used in information security and refers to a service, which provides proof of the origin of data and the integrity of the data.

Security, Functionality and Usability balance

There is an inter dependency between these three attributes. When **security goes up, usability and functionality come down**. Any organization should balance between these three qualities to arrive at a balanced information system.



Types of Hackers

- **Black Hat** - Hackers that seek to perform malicious activities.
- **Gray Hat** - Hackers that perform good or bad activities but do not have the permission of the organization they are hacking against.
- **White Hat** - Ethical hackers; They use their skills to improve security by exposing vulnerabilities before malicious hackers.

Script Kiddie / Skiddies - Unskilled individual who uses malicious scripts or programs, such as a web shell, developed by others to attack computer systems and networks and deface websites.

State-Sponsored Hacker - Hacker that is hired by a government or entity related.

Hacktivist - Someone who hacks for a cause; political agenda.

Suicide Hackers - Are hackers that are not afraid of going jail or facing any sort of punishment; hack to get the job done.

Cyberterrorist - Motivated by religious or political beliefs to create fear or disruption.

Hacking Vocabulary

- **Hack value** - Perceived value or worth of a target as seen by the attacker.
- **Vulnerability** - A system flaw, weakness on the system (on design, implementation etc).

- **Threat** - Exploits a vulnerability.
- **Exploit** - Exploits are a way of gaining access to a system through a security flaw and taking advantage of the flaw for their benefit.
- **Payload** - Component of an attack; is the part of the private user text which could also contain malware such as worms or viruses which performs the malicious action; deleting data, sending spam or encrypting data.
- **Zero-day attack** - Attack that occurs before a vendor knows or is able to patch a flaw.
- **Daisy Chaining / Pivotting** - It involves gaining access to a network and /or computer and then using the same information to gain access to multiple networks and computers that contains desirable information.
- **Doxxing** - Publishing PII about an individual usually with a malicious intent.
- **Enterprise Information Security Architecture** (EISA) - determines the structure and behavior of organization's information systems through processes, requirements, principles and models.

Threat Categories

- **Network Threats**
  - Information gathering
  - Sniffing and eavesdropping
  - DNS/ARP Poisoning
  - MITM (Man-in-the-Middle Attack)
  - DoS/DDoS
  - Password-based attacks
  - Firewall and IDS attack
  - Session Hijacking
- **Host Threats**
  - Password cracking
  - Malware attacks
  - Footprinting
  - Profiling
  - Arbitrary code execution
  - Backdoor access
  - Privilege Escalation
  - Code Execution
- **Application Threats**
  - Injection Attacks
  - Improper data/input validation
  - Improper error handling and exeception management
  - Hidden-field manipulation
  - Broken session management
  - Cryptography issues
  - SQL injection
  - Phishing
  - Buffer Overflow
  - Information disclosure
  - Security Misconfigurations

Attack Vectors

Path by which a hacker can gain access to a host in order to deliver a payload or malicious outcome

- **APT - Advanced Persistent Threats**
  - An advanced persistent threat is a stealthy threat actor, typically a nation state or state-sponsored group, which gains unauthorized access to a computer network and remains undetected for an extended period; Typically uses zero day attacks.
- **Cloud computing / Cloud based technologies**
  - Flaw in one client's application cloud allow attacker to access other client's data
- **Viruses, worms, and malware**
  - Viruses and worms are the most prevalent networking threat that are capable of infecting a network within seconds.
- **Ransomware**
  - Restricts access to the computer system's files and folders and demands an online ransom payment to the attacker in order to remove the restrictions.
- **Mobile Device threats**
- **Botnets**
  - Huge network of compromised systems used by an intruder to perform various network attacks
- **Insider attacks**
  - Disgruntled employee can damage assets from inside.
  - Huge network of compromised hosts. (used for DDoS).
- **Phishing attacks**
- **Web Application Threats**
  - Attacks like SQL injection, XSS (Cross-site scripting)...
- **IoT Threats**

Attack Types

1. Operating System

Attacks targeting OS flaws or security issues inside such as guest accounts or default passwords.

- **Vectors**: Buffer overflows, Protocol Implementations, software defects, patch levels, authentication schemes

2. Application Level

Attacks on programming code and software logic.

- **Vectors**: Buffer overflows, Bugs, XSS, DoS, SQL Injection, MitM

3. Misconfiguration

Attack takes advantage of systems that are misconfigured due to improper configuration or default configuration.

- **Examples**: Improper permissions of SQL users; Access-list permit all

4. Shrink-Wrap Code

Act of exploiting holes in unpatched or poorly-configured software.

- **Examples**: Software defect in version 1.0; DEfect in example CGI scripts; Default passwords

Vulnerabilities

- **CVSS - Common Vulnerability Scoring System** [+]
  - Places numerical score based on severity
  -
- **CVE – Common Vulnerabilities and Exposures** [+]
  - Is a list of publicly disclosed vulnerabilities and exposures that is maintained by MITRE.
  -
- **NVD - National Vulnerability Database** [+]
  - is a database, maintained by NIST, that is fully synchronized with the MITRE CVE list; US Gov. vulnerabilities repository.

Vulnerability Categories

- **Misconfiguration** - improperly configuring a service or application
- **Default installation** - failure to change settings in an application that come by default
- **Buffer overflow** - code execution flaw
- **Missing patches** - systems that have not been patched
- **Design flaws** - flaws inherent to system design such as encryption and data validation
- **Operating System Flaws** - flaws specific to each OS
- **Default passwords** - leaving default passwords that come with system/application

Pen Test Phases (CEH)

1. **Pre-Attack Phase** - Reconnaissance and data-gathering.
2. **Attack Phase** - Attempts to penetrate the network and execute attacks.
3. **Post-Attack Phase** - Cleanup to return a system to the pre-attack condition and deliver reports.

 For the exam, EC-Council brings his own methodology and that's all you need for the exam; you can check another pentesting methodologies here if you are interested; In case you are studying to become a professional pentester besides certification content, I recommend the OSSTMM (Open Source Security Testing Methodology Manual).

The Five Stages of Ethical Hacking

1. Reconnaissance

Gathering evidence about targets; There are two types of Recon:

- **Passive Reconnaissance**: Gain information about targeted computers and networks **without direct interaction with the systems**.
    - e.g: Google Search, Public records, New releases, Social Media, Wardrive scanning networks around.
- **Active Reconnaissance**: Envolves direct interaction with the target.
    - e.g: Make a phone call to the target, Job interview; tools like Nmap, Nessus, OpenVAS, Nikto and Metasploit can be considered as Active Recon.

2. Scanning & Enumeration

Obtaining more in-depth information about targets.

- e.g: Network Scanning, Port Scanning, Which versions of services are running.

3. Gaining Access

Attacks are leveled in order to gain access to a system.

- e.g: Can be done locally (offline), over a LAN or over the internet.
    - e.g(2): Spoofing to exploit the system by pretending to be a legitimate user or different systems, they can send a data packet containing a bug to the target system in order to exploit a vulnerability.
    - Can be done using many techniques like command injection, buffer overflow, DoS, brute forcing credentials, social engineering, misconfigurations etc.

4. Maintaining Access

Items put in place to ensure future access.

- e.g: Rookit, Trojan, Backdoor can be used.

5. Covering Tracks

Steps taken to conceal success and intrusion; Not be noticed.

- e.g: Clear the logs; Obfuscate trojans or malicious backdoors programs.

Three Types of Active Defense

- **Annoyance**
    - Involves tracking a hacker and leading him into a fake server, wasting his time — and making him easy to detect.
- **Attribution**
    - Identify an attacker; Uses tools to trace the source of an attack back to a specific location, or even an individual hacker.

- **Attack**
    - That is most controversial. To “hack back,” a company accesses an alleged hacker’s computer to delete its data or even to take revenge. Both of these steps are considered illegal.

Information Assurance (IA)

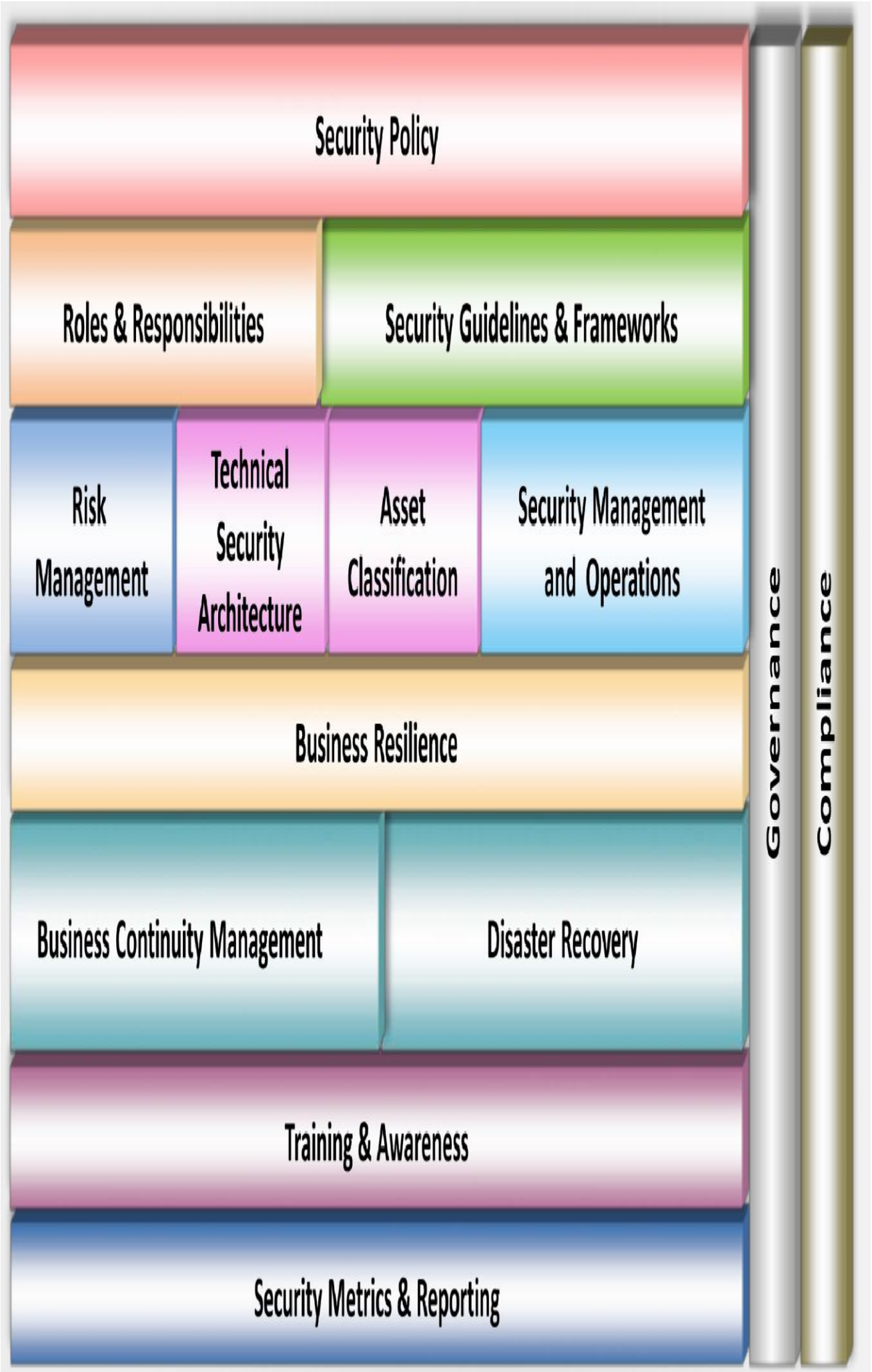
Refers to the assurance of the Integrity, Availability, confidentiality, and authenticity of information and information systems during usage, processing, storage and transmission of information.

- **Processes that help achieving IA:**
    - Developing local policy, process, and guidance.
    - Designing network and user authetication strategy.
    - Identifying network vulnerabilities and threats (Vulnerability assessments outline the security posture of the network).
    - Idenfitying problems and resource requirements.
    - Creating plan for identified resource requirements.
    - Applying appropriate IA controls.
    - Performing C&A (Certification and Accreditation) process of information systems helps to trace vulnerabilities, and implement sa fety measures.
    - Providing information assurance training to all personnel in federal and private org.

Information Security Management Program

*Combination of policies, processes, procedures, standards, and guidelines to establish the required **level of information security.***

- Designed to ensure the business operates in a state of reduced risk.
- It encompasses all organizational and operational processes and participants relevant to information security.


Security Policy
Roles & Responsibilities
Security Guidelines & Frameworks
Risk Management
Technical Security Architecture
Asset Classification
Security Management and Operations
Business Resilience
Business Continuity Management
Disaster Recovery
Training & Awareness
Security Metrics & Reporting
Governance
Compliance

 IA focus on risk assessment, mitigation side of things; **InfoSec** focus on actually implementing security measures to safeguard systems.

EISA - Enterprise Information Security Architecture

Set of requirements, process, principles, and models that determines the structure and behavior of an organization's information systems.

- **Goals of EISA**:
  - Help in monitoring and detecting network behaviors
  - Detect and recover from security breaches
  - Prioritizing resources of an organization
  - Help to perform risk assessment of an organization's IT assets.
  - Cost prospective when incorporated in security provisions such as incident response, disaster recovery, event correlation, etc.

Physical Security Controls

- **Preventive control**: Deters the actor from performing the threat.
  - e.g: Fence, Server Locks, Mantraps, etc.
- **Detective control**: Recognizes an actor's threat.
  - e.g: Background check, CCTV.
- **Deterrent control**: Deters the actor from **attempting** the threat.
  - e.g: Warning Sign.
- **Recovery**: Mitigates the impact of a manifested threat.
  - e.g: Backups.
- **Compensating control**: Provides alternative fixes to any of the above functions.

Most of security controls are preventive phase controls.

 Defense in Depth: Multiple layers of security controls; Provides redundancy in the event of a control failure. (e.g.: image below)

Types of Security Controls

Description	Examples
Physical	Guards, lights, cameras, fire extinguishers, flood protection
Administrative	Training awareness, policies, procedures and guidelines to infosec
Technical	IDS/IPS, Firewall, Encryption, Smart cards, Access control lists

Description	Examples
Preventative	authentication, alarm bells
Detective	audits, backups
Corrective	restore operations

Managing the Risk

Risk can be defined as a probability of the occurrence of a threat or an event that may damage, or cause loss or have other negative impact either from internal or external liabilities.

Risk matrix

A **risk matrix** is used during **risk assessment** to define the level of risk by considering the category of **probability or likelihood** against the category of consequence **severity**.

- This is a simple mechanism to increase visibility of risks and assist management decision making.

	Consequence				
Likelihood	**Insignificant**	**Minor**	**Moderate**	**Major**	**Severe**
Almost Certain	Medium	High	High	Extreme	Extreme
Likely	Medium	Medium	High	Extreme	Extreme
Possible	Medium	Medium	High	High	Extreme
Unlikely	Low	Medium	Medium	High	High
Rare	Low	Low	Medium	High	High

Risk Management

Is the identification, evaluation, and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability or impact of unfortunate events or to maximize the realization of opportunities.

Phases of Risk Management

- **Risk Identification**
  - Identifies the sources, causes, consequences of the internal and external risks.
- **Risk Assessment**
  - Assesses the org. risk and provides an estimate on the likelihood and impact of the risk

- **Risk Treatment**
  - Selects and implements appropriate controls on the identified risks
- **Risk Tracking**
  - Ensures appropriate control are implemented to handle risks and identifies the chance of a new risk occurring
- **Risk Review**
  - Evaluates the performance of the implemented risk management strategies

Threat Modeling

Is a risk assessment approach for analyzing the security of an application by capturing, organizing and analyzing all the information that affects the security of an application.

1. Identify Objectives
   - Helps to determine how much effort needs to be put on subsequent steps
2. Application Overview
   - **Identify the components**, data flows, and trust boundaries
3. Decompose Application
   - Find **more relevant details on threats**
4. Identify Threats
   - Identify threats relevant to your control scenario and context using the information obtained in steps 2 and 3
5. Identify Vulnerabilities
   - **Identify weaknesses** related to the threats found using vulnerability categories

Security Policies

1. **Policies** - High-level statements about protecting information; Business rules to safeguard CIA triad; Security Policies can be applied on Users, Systems, Partners, Networks, and Providers.
   - **Common Security Policies examples:**
     - Password Policy
       - Meet the password complexity requirements.
       - e.g: Minimum 8 char length, upper and lower case and alphanumerical.
     - Wireless Security Policy
     - AUP - Acceptable Use-Policy
       - How to properly use company's assets
       - e.g: "Do's and Dont's" with company's computer.
     - Data Retention Policy
       - e.g: Keep the data for X time.
     - Access Control Policies
       - e.g: Accessing servers; Firewalls
2. **Procedures** - Set of details steps to accomplish a goal; Instructions for implementation
3. **Guidelines** - Advice on actions given a situation; Recommended, not mandatory

Security Policy - Examples

- **Access Control Policy**
  - This defines the resources being protected and the rules that control access to them
- **Remote Access Policy**
  - This defines who can have remote access and defines access medium and remote access security controls.
- **Firewall Management Policy**
  - This defines access, management and monitoring of firewalls in an organization.
- **Network Connection Policy**
  - This defines who can install new resources on the network, approve the installation of new devices, document network changes etc.
- **Password Policy**
  - This defines guidelines for using strong password protection on available resources.
- **User Account Policy**
  - This defines the account creation process, authority, rights and responsibility of user accounts.
- **Information Protection Policy**
  - This defines the sensitivity levels of information, who may have access, how it is stored and transmitted, and how it should be deleted from storage media etc.
- **Special Access Policy**
  - This defines the terms and conditions of granting special access to system resources.
- **Email Security Policy**
  - This policy is designed to govern the proper usage of corporate email.
- **Acceptable Use Policy**
  - This defines the acceptable use of system resources.

Security Policiy - Types

1. **Promiscuous Policy** - This policy usually has no restrictions on usage of system resources.
2. **Permissive Policy** - This policy begins wide open and only know dangerous services/attacks or behaviors are blocked. This type of policy has to be updated regularly to stay effective.
3. **Prudent Policy** - This policy provides maximum security while allowing known but necessary dangers. This type of policy will block all services and only safe/necessary services are enabled individually. Everything is logged.
4. **Paranoid Policy** - This policy forbids everything. No Internet connection or severely restricted Internet usage is allowed.

Security Policy - Creation Steps

1. Perform a Risk Assessment
2. Use security Standards and Frameworks as guide
3. Get Management and Staff input
4. Enforce the policy. Use penalties for non-compliance
5. Publish final draft to entire org.

6. Have all staff read/sign that they understood policy
7. Employ tools to help enforce policy
8. Staff training
9. Review and update regularly

Incident Management Process

An incident is an event that could lead to loss of, or disruption to, an organization's operations, services or functions.

***Incident management** is a term describing the activities of an organization to identify, analyze, and correct hazards to prevent a future re-occurrence.*

1. **Preparation:** Select people, assign rules, define tools to handle the incident.
2. **Detection & Analysis:** Determine an incident has ocurred (IDS, SIEM, AV, Someone reporting, etc).
3. **Classification and Prioritization:**
4. **Notification:** Identify minor and major incident; who and how to notify an incident.
5. **Containment:** Limit the damage; Isolate hosts; Contact system owners.
6. **Forensic Investigation:** Investigate the root cause of the incident using forensic tools; System logs, real-time memory, network device logs, application logs, etc;
7. **Eradicate & Recovery:** Remove the cause of incident; Patch if needed. Recovery: get back into production; Monitor affected systems.
8. **Post-incident Activities:** Document what happened and why; Transfer knowledge.

Incident Response Team Duties

1. Managing security issues by taking a proactive approach towards the customer's security vulnerabilities
2. Developing or reviewing processes and procedures that must be followed
3. Managing the response to an incident and ensuring that all procedures are followed correctly in order to minimize and control the damage
4. Identifying and analyzing what has happened during an incident, including impact and threat
5. Providing a single point of contact for reporting seucirty incidents and issues
6. Reviewing changes in legal and regulatory requirements to ensure that all processes and procedures are valid
7. Reviewing existing controls and recommending steps and technologies to prevent future incidents
8. Establishing relationship with local law enforcement agency, gov. agencies, key partners and suppliers

SIEM - Security Information and Event Management

Collects data points from network, including log files, traffic captures, SNMP messages, and so on, from every host on the network. SIEM can collect all this data into one centralized location and correlate it for analysis to look for security and performance issues, as well negative trends all in real time.

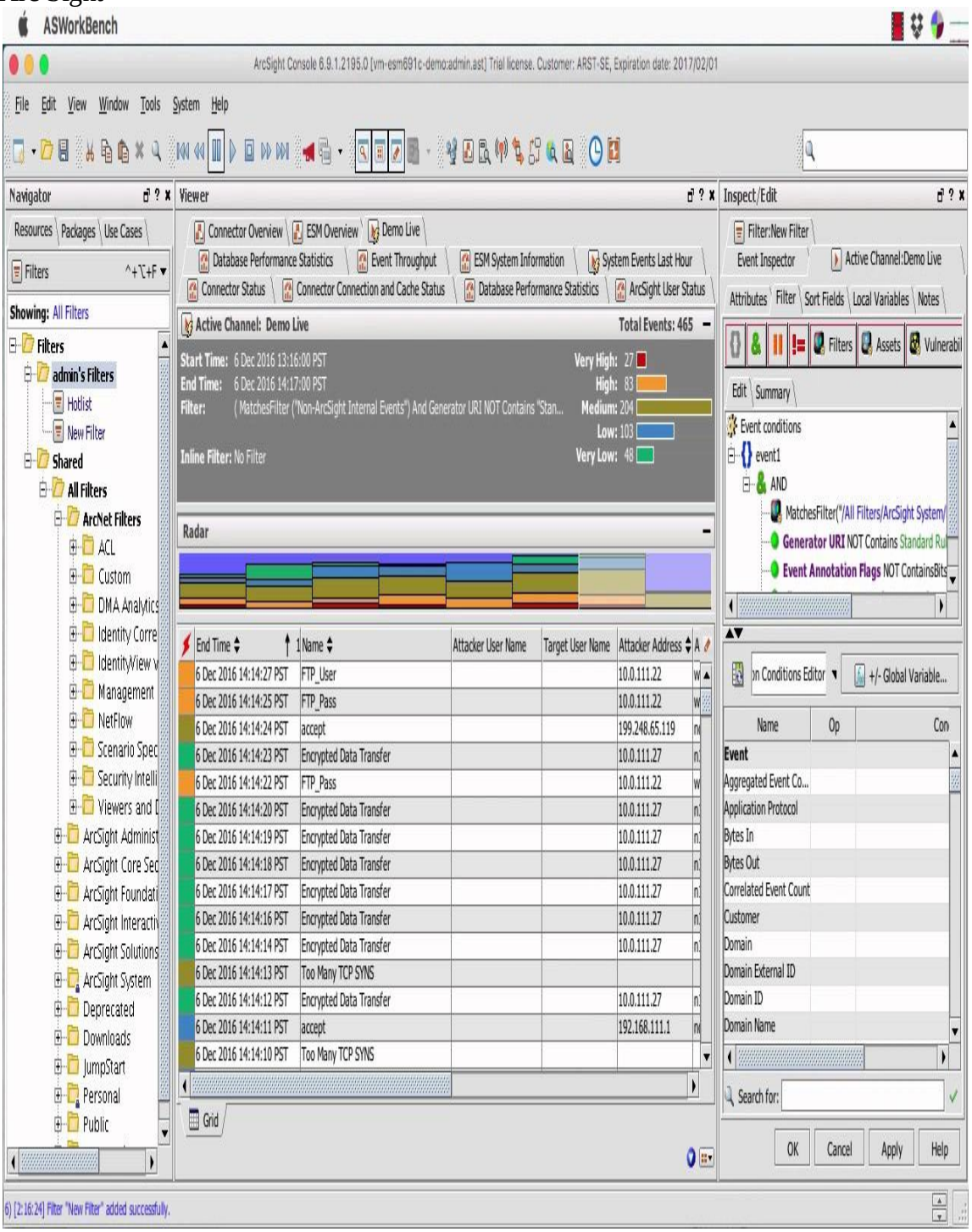
- **Aggregation**: Collecting data from disparate sources and organizing the data into a single format. Any device within a SIEM system that collects data is called collector or an aggregator.

- **Correlation**: Is the logic that looks at data from disparate sources and can make determinations about events taking place on your network. (Could be in-band or out-of-band, depending on the placement of the NIDS/NIPS).
    - **Alerts** - For notification if something goes bad.
    - **Triggering** - Exceeding thresholds.
- **Normalization**: Will actually create multiple tables / organize in such a way that the data can become more efficient and allows our analysis and reports tools to work better.
- **WORM - Write Once Read Many**: The concept being is that log files are precious, and a lot of times you might want to look at them in an archival way, so that we can use optical media like WORM drives to store them.

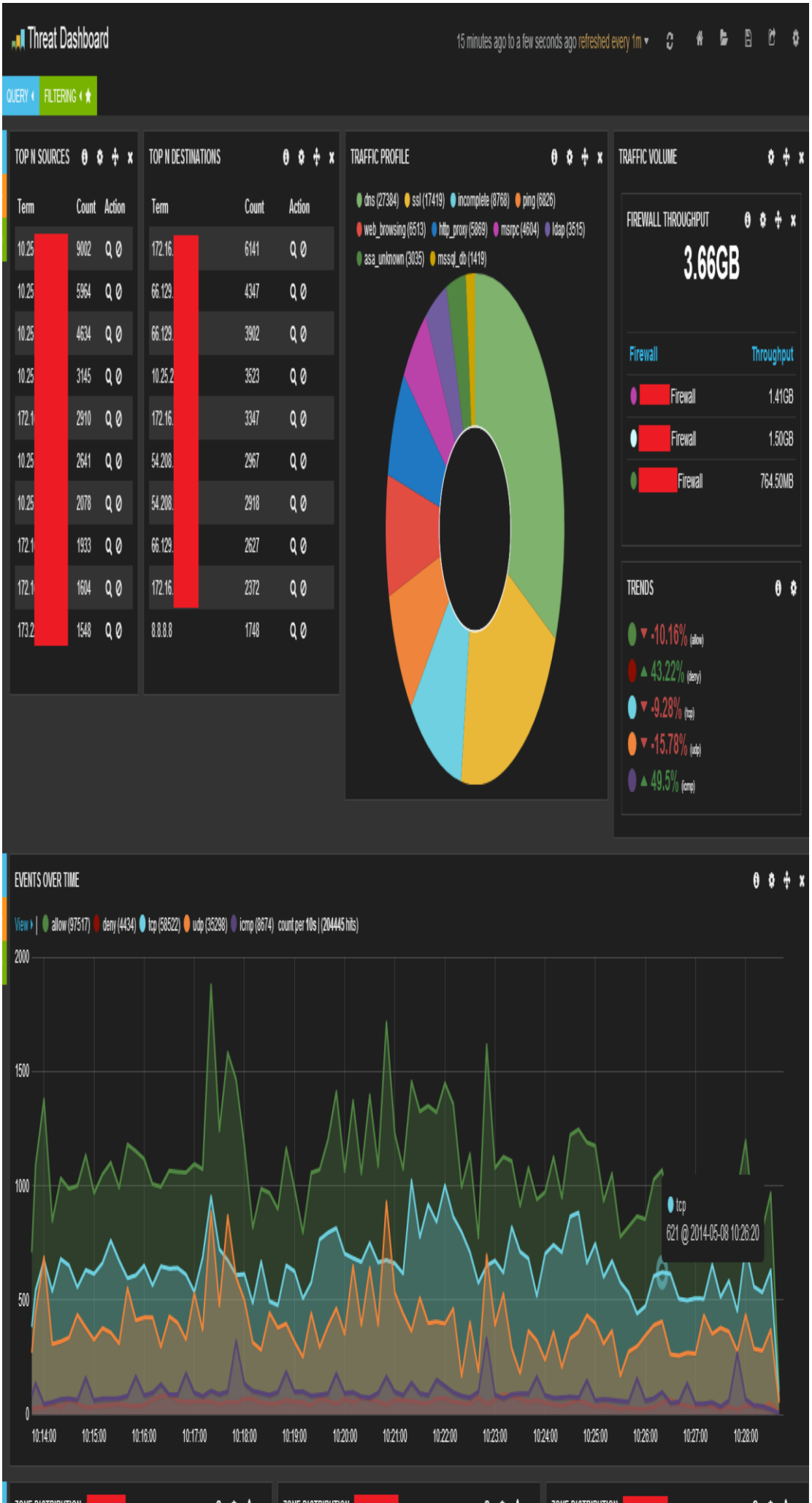
Most Popular SIEM Tools:

- **Splunk**

- Arc Sight


ASWorkBench
ArcSight Console 6.9.1.2195.0 [vm-esm691c-demo:admin.ast] Trial license. Customer: ARST-SE, Expiration date: 2017/02/01
File Edit View Window Tools System Help
Navigator
Resources Packages Use Cases
Filters
Showing: All Filters
Filters
admin's Filters
Hotlist
New Filter
Shared
All Filters
ArcNet Filters
ACL
Custom
DMA Analytics
Identity Corre
IdentityView
Management
NetFlow
Scenario Spec
Security Intelli
Viewers and D
ArcSight Administ
ArcSight Core Sec
ArcSight Foundati
ArcSight Interacti
ArcSight Solutions
ArcSight System
Deprecated
Downloads
JumpStart
Personal
Public
Viewer
Connector Overview
ESM Overview
Demo Live
Database Performance Statistics
Event Throughput
ESM System Information
System Events Last Hour
Connector Status
Connector Connection and Cache Status
Database Performance Statistics
ArcSight User Status
Active Channel: Demo Live
Total Events: 465
Start Time: 6 Dec 2016 13:16:00 PST
End Time: 6 Dec 2016 14:17:00 PST
Filter: (MatchesFilter ("Non-ArcSight Internal Events") And Generator URI NOT Contains "Stan...
Inline Filter: No Filter
Very High: 27
High: 83
Medium: 204
Low: 103
Very Low: 48
Radar
End Time
Name
Attacker User Name
Target User Name
Attacker Address
6 Dec 2016 14:14:27 PST FTP_User 10.0.111.22
6 Dec 2016 14:14:25 PST FTP_Pass 10.0.111.22
6 Dec 2016 14:14:24 PST accept 199.248.65.119
6 Dec 2016 14:14:23 PST Encrypted Data Transfer 10.0.111.27
6 Dec 2016 14:14:22 PST FTP_Pass 10.0.111.22
6 Dec 2016 14:14:20 PST Encrypted Data Transfer 10.0.111.27
6 Dec 2016 14:14:19 PST Encrypted Data Transfer 10.0.111.27
6 Dec 2016 14:14:18 PST Encrypted Data Transfer 10.0.111.27
6 Dec 2016 14:14:17 PST Encrypted Data Transfer 10.0.111.27
6 Dec 2016 14:14:16 PST Encrypted Data Transfer 10.0.111.27
6 Dec 2016 14:14:14 PST Encrypted Data Transfer 10.0.111.27
6 Dec 2016 14:14:13 PST Too Many TCP SYNS
6 Dec 2016 14:14:12 PST Encrypted Data Transfer 10.0.111.27
6 Dec 2016 14:14:11 PST accept 192.168.111.1
6 Dec 2016 14:14:10 PST Too Many TCP SYNS
Grid
Inspect/Edit
Filter:New Filter
Event Inspector
Active Channel:Demo Live
Attributes Filter Sort Fields Local Variables Notes
Filters
Assets
Edit Summary
Event conditions
event1
AND
MatchesFilter("/All Filters/ArcSight System/
Generator URI NOT Contains Standard Ru
Event Annotation Flags NOT ContainsBits
+/- Global Variable...
Name
Op
Event
Aggregated Event Co...
Application Protocol
Bytes In
Bytes Out
Correlated Event Count
Customer
Domain
Domain External ID
Domain ID
Domain Name
Search for:
OK
Cancel
Apply
Help
6) [2:16:24] Filter "New Filter" added successfully.

- **ELK - Elastic Search, Log Stash and Kibana (Open Source)**


Threat Dashboard
15 minutes ago to a few seconds ago refreshed every 1m
QUERY
FILTERING
TOP N SOURCES
Term Count Action
10.25 9002
10.25 5964
10.25 4634
10.25 3145
172.1 2910
10.25 2641
10.25 2078
172.1 1933
172.1 1604
173.2 1548
TOP N DESTINATIONS
Term Count Action
172.16. 6141
66.129. 4347
66.129. 3902
10.25.2 3523
172.16. 3347
54.208. 2967
54.208. 2918
66.129. 2627
172.16. 2372
8.8.8.8 1748
TRAFFIC PROFILE
dns (27384) ssl (17419) incomplete (8768) ping (6826)
web_browsing (6513) http_proxy (5869) msrpc (4604) ldap (3515)
asa_unknown (3035) mssql_db (1419)
TRAFFIC VOLUME
FIREWALL THROUGHPUT
3.66GB
Firewall Throughput
Firewall 1.41GB
Firewall 1.50GB
Firewall 764.50MB
TRENDS
-10.16% (allow)
43.22% (deny)
-9.28% (tcp)
-15.78% (udp)
49.5% (icmp)
EVENTS OVER TIME
View | allow (97517) deny (4434) tcp (58522) udp (35298) icmp (8674) count per 10s | (204445 hits)
2000
1500
1000
500
0
tcp
621 @ 2014-05-08 10:26:20
10:14:00 10:15:00 10:16:00 10:17:00 10:18:00 10:19:00 10:20:00 10:21:00 10:22:00 10:23:00 10:24:00 10:25:00 10:26:00 10:27:00 10:28:00

Identity and Access Management

Identification, Authentication, Authorization, and **Accounting** work together to manage assets securely.

1. Identification

The information on credentials identifies the user.

- **Example**:
  - Your name, username, ID number, employee number, SSN etc.

2. Authentication

"Prove you are the legitimate User". – Should always be done with Multifactor Authentication!

- **Authentication Factors:**
  - Something you **know** (e.g. - password)
  - Something you **have** (e.g. - smart card)
  - Something you **are** (e.g. - fingerprint)
  - Something you **do** (e.g. - android pattern; manual signature)
  - **Somewhere** you are (e.g. - geolocation)

 Multi-factor authentication *generally uses two of this examples (e.g. - Something you* ***Know(1)*** *and Something you* ***Have(2)****, never on same category*

3. Authorization concepts

What are you allowed to access – We use Access Control models, what and how we implement depends on the organization and what our security goals are.

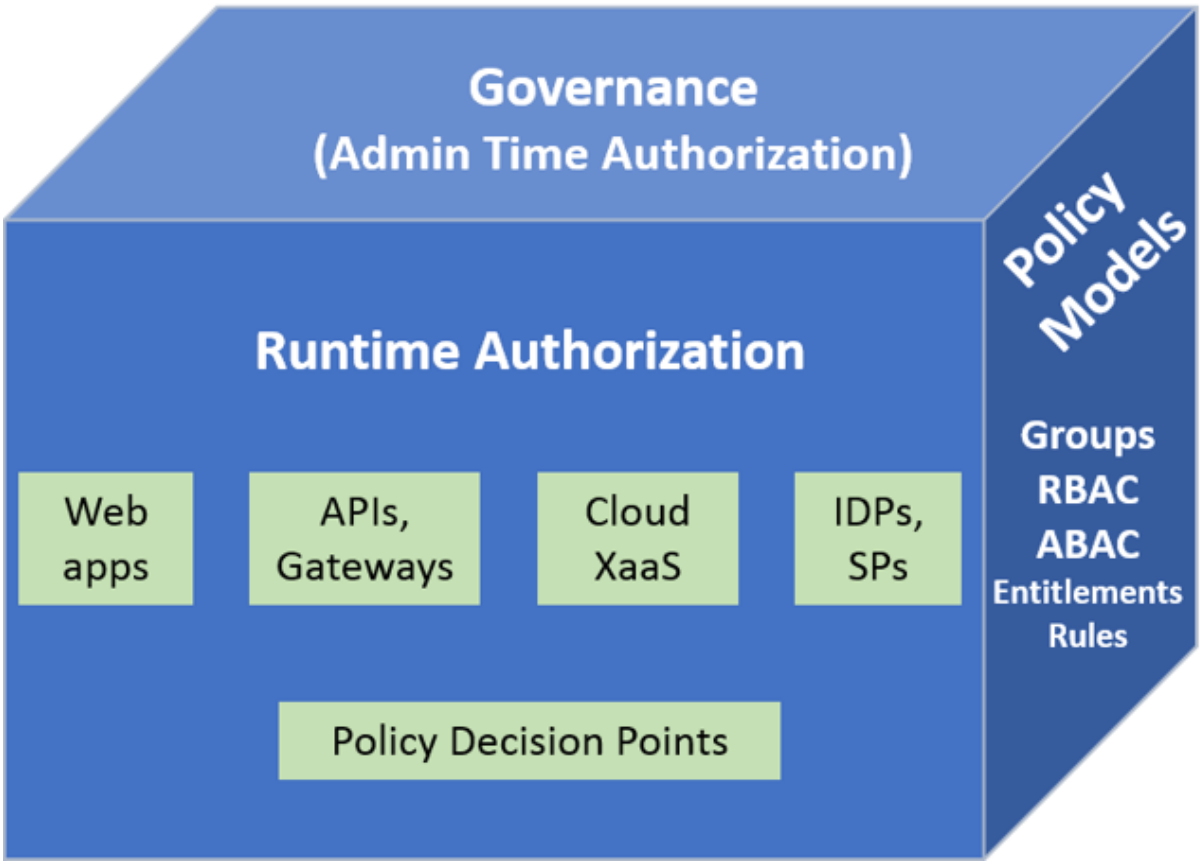
- **Permissions**:
  - Applied to resources
- **Rights** / **Privileges**:
  - Assign at system level
- **Authorization strategies**:
  - Least privileged
  - Separation of Duties

4. Accouting

Trace an Action to a Subjects Identity:

- Prove who/what a given action was performed by (non-repudiation); Logging

Access Controls Models



- **Mandatory Access Control (MAC)**:
  - Every object gets a **label**
    - Confidential, secret, top secret, etc
  - The administrator decides who gets access to what security level; Users cannot change these settings
  - Used on old systems (e.g. Top Secret Gov. information)
- **Discretionary Access Control (DAC)**:
  - Used in most OS
  - Owner of the data defines access
  - Very flexible access control; Very weak security
- **Role-based Access Control (RBAC)**:
  - Access to resources is defines by a set of rules defined by a role in your organization/job function (Manager, Director etc)
  - Administrators provide access based on the role of the user
    - Rights are gained implicity instead of explicity
  - In Windows, use **Groups** to provide role-based access control
    - e.g. Admin Groups --> Rights and Perms,
    - Sales Group --> Rights and Perms

 Access is defined by ACL, Access Control List. **Implicity deny** prevents access unless specifically permitted.

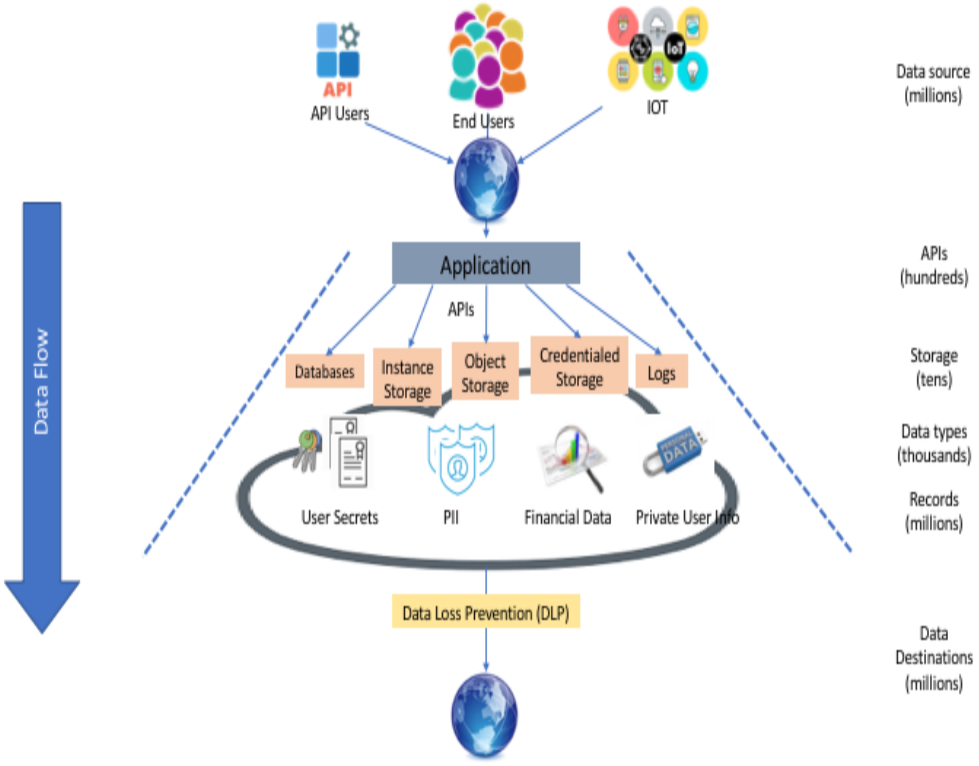
Data Loss Prevention (DLP)

Data Loss Prevention (DLP) is the practice of **detecting and preventing data breaches, exfiltration, or unwanted destruction of sensitive data**. Organizations use DLP to protect and secure their data and comply with regulations.

- The DLP term refers to defending organizations against both data loss and data leakage prevention.

Organizations typically use DLP to:

- Protect Personally Identifiable Information (PII) and comply with relevant regulations
- Protect Intellectual Property critical for the organization
- Achieve data visibility in large organizations
- Secure mobile workforce and enforce security in Bring Your Own Device (BYOD) environments
- Secure data on remote cloud systems



Data Backup

Data backup plays a crucial role in maintaining business continuity by helping org. recover from IT disasters, security breaches, application failures, human error, etc.

All regulatory compliance such as COBIT, SSAE, SOCII, PCI-DSS, HIPPA, SOX, FINRA, FISMA, GDPR, etc. require business to maintain data backups of critical data for specified duration.

Backup Strategies

1. Identifying the critical business data
2. Selecting the backup media
3. Selecting a backup technology
4. Selecting the appropriate RAID levels
5. Selecting an appropriate backup method

3 Backup methods

1. Cold backup

- **Empty site, no hardware, no data, no people**
- **It takes weeks to bring online**
- Basic office spaces (e.g building, chairs, AC...)
- No operational equipment
- Cheapest recovery site

2. Warm backup

- **Somewhere between cold and hot - Just enough to get going (Big room with rack space, you bring the hardware)**

- Hardware is ready and waiting - you bring the software and data
- **It takes days to bring online**
- Operational equipment but little or no data

3. Hot backup

- **Exact replica of production systems**
- Applications and software are constantly updated
- Flip a switch and everyting moves
- **It take hours to bring online**
- Real-time synchronization
- Almost all data ready to go - often just a quick update
- Very expensive

Penetration Test - Basics

A penetration test, colloquially known as a pen test, pentest or ethical hacking, is an authorized simulated cyberattack on a computer system, performed to evaluate the security of the system.

 Not to be confused with a vulnerability assessment.

- Clearly defined, full scale test of security controls
- Phases
    - **Preparation** - Contracts and team determined
    - **Assessment** - All hacking phases (reconnaissance, scanning, attacks, etc.)
    - **Post-Assessment** - Reports & conclusions
- Types
    - **Black Box** - Done without any knowledge of the system or network.
    - **White Box** - When the attacker have complete knowledge of the system provided by the owner/target.
    - **Gray Box** - When the attacker has some knowledge of the system and/or network

Law Categories

- **Criminal** - Laws that protect public safety and usually have jail time attached.
- **Civil** - Private rights and remedies.
- **Common** - Laws that are based on societal customs.

Laws and Standards:

OSSTM Compliance

"Open Source Security Testing Methodology Manual" maintained by ISECOM , defines three types of compliance.

- **Legislative** - Deals with government regulations (Such as SOX and HIPAA).
- **Contractual** - Deals with industry / group requirement (Such as PCI DSS).
- **Standards based** - Deals with practices that must be followed by members of a given group/organization (Such as ITIL ,ISO and OSSTMM itself).
- **OSSTM Controls**
    - **OSSTM Class A - Interactive Controls**
        - *Authentication* - Provides for identification and authorization based on credentials.
        - *Indemnification* - Provided contractual protection against loss or damages.
        - *Subjugation* - Ensures that interactions occur according to processes defined by the asset owner.
        - *Continuity* - Maintains interactivity with assets if corruption of failure occurs.
        - *Resilience* - Protects assets from corruption and failure.
- **OSSTM Class B - Process Controls**
    - *Non-repudiation* - Prevents participants from denying its actions
    - *Confidentiality* - Ensures that only participants know of an asset
    - *Privacy* - Ensures that only participants have access to the asset
    - *Integrity* - Ensures that only participants know when assets and processes change
    - *Alarm* - Notifies participants when interactions occur

PCI-DSS

"Payment Card Industry Data Security Standard" Standard for organizations handling Credit Cards, ATM cards and other POS cards.

ISO 27001

This International Standard has been prepared to provide requirements for establishing, implementing, maintaining and continually improving an information security management system.

ISO 27002 AND 17799

Based on BS799 but focuses on security objectives and provides security controls based on industry best practice.

HIPAA

"Health Insurance Portability and Accountability Act" a law that set's privacy standards to protect patient medical records and health information shared between doctors, hospitals and insurance providers.

SOX

"Sarbanes-Oxley Act" Law that requires publicly traded companies to submit to independent audits and to properly disclose financial information.

DMCA

"The Digital Millennium Copyright Act" is a 1998 United States copyright law that implements two 1996 treaties of the World Intellectual Property Organization. It criminalizes production and dissemination of technology, devices, or services intended to circumvent measures that control access to copyrighted works.

FISMA

"Federal Information Security Modernization Ac Of 2002" A law updated in 2004 to codify the authority of the Department of Homeland Security with regard to implementation of information security policies. *(For GOV. agencies)*

NIST-800-53

Catalogs security and privacy controls for federal information systems, created to help implementation of FISMA.

FITARA

"Federal Information Technology Acquisition Reform Act" A 2013 bill that was intended to change the framework that determines how the US GOV purchases technology.

COBIT

"Control Object for Information and Related Technology" IT Governance framework and toolset, created by ISACA and ITGI

GLBA

"U.S Gramm-Leach-Bliley Act" Law that protects the confidentiality and integrity of personal information that is collected by financial institutions.

CSIRT

"Computer Security Incident Response Team" CSIRT provided a single point of contact when reporting computer security incidents

ITIL

"Information Technology Infrastructure Library" - An operational framework developed in the '80s that standardizes IT management procedures

Essential Knowledge

OSI Model and TCP Model

- **The OSI Model** we just looked at is just a reference/logical model. It was designed to describe the functions of the communication system by dividing the communication procedure into smaller and simpler components.
- **The TCP/IP model** is a concise version of the OSI model. It contains four layers, unlike seven layers in the OSI model.

Layer	Device Type	OSI Layer	TCP/IP model	TCP/IP New (actual)	Protocols	PDU
7	Gateway	**Application**	Application	Application	HTTP, FTP, POP, SMTP, DNS, RIP	Data
6	-	**Presentation**	Application	Application	HTTP, FTP, POP, SMTP, DNS, RIP, MIME	Data
5	-	**Session**	Application	Application	HTTP, FTP, POP, SMTP, DNS, RIP, SCP	Data
4	-	**Transport**	Transport	Transport	TCP/UDP	Segments
3	Router	**Network**	Internet	Network	IP, ARP, ICMP, IGMP	Packets
2	Switch/bridge	**Data Link**	Link	Data Link	Ethernet, Token Ring	Frames
1	Hubs/Repeater	**Physical**	Link	Physical	Ethernet, Token Ring	Bits

TCP Handshake

The Three-way handshake

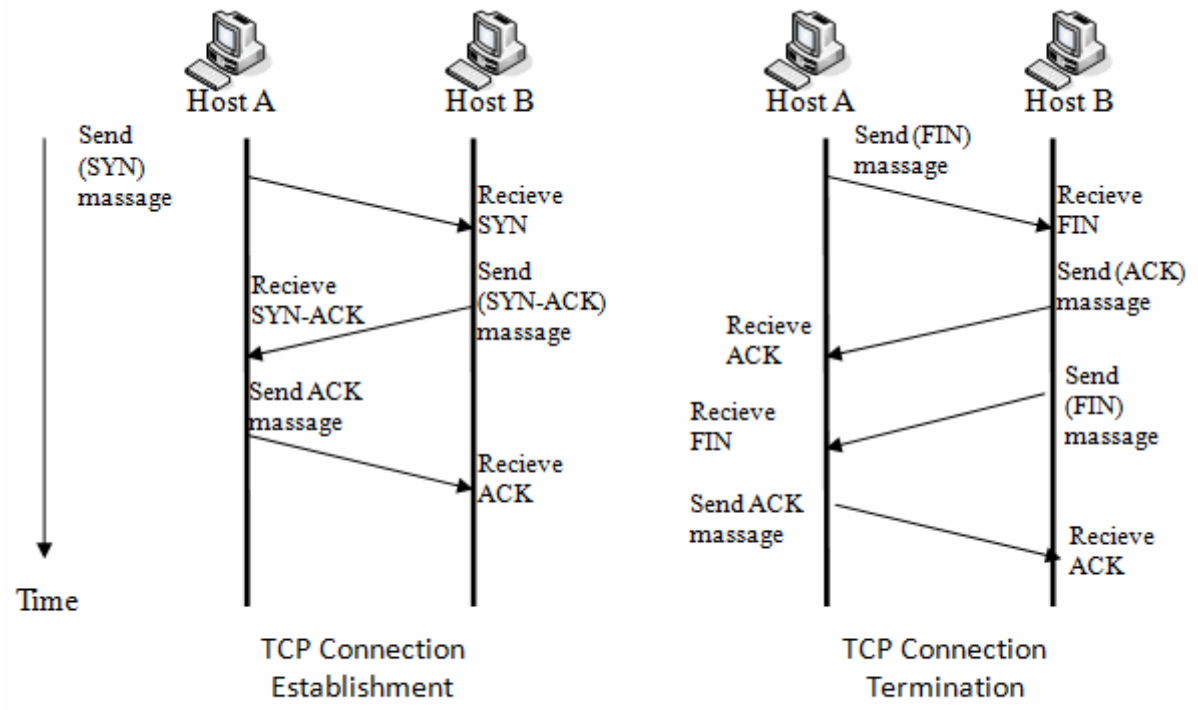


Figure 2.1. TCP session establishment and termination

✓TCP Connection establishment process

1. **Host A** sends out a **SYN** (synchronize) packet with proposed initial sequence number to Host B.
2. **Host B** receives **SYN** message, it returns a packet with both SYN and ACK flags (**SYN-ACK**) set in the TCP header.
3. **Host A** receives the **SYN-ACK**, it sends back **ACK** (Acknowledgment) packet.
4. **Host B** receives **ACK** and at this stage the connection is **ESTABLISHED.**

✗TCP Connection termination

1. **Host A** sends a **FIN** (finish) flag, indicating that is has finished sending the data.
2. **Host B** who receives the **FIN**, doest not terminate the connection but enters into a "passive close" (CLOSE_WAIT) state and sends the **ACK** for the **FIN** back to the Host A.
3. **Host A** enters into a (TIME_WAIT) state, and sends an **ACK** back to the Host B.
4. **Host B** gets the **ACK** from the Host A and **closes the connection.**

 Sequence numbers increase on new communication. Example is computers A and B. A would increment B's sequence number. A would never increment it's own sequence.

TCP Flags

Flag	Name	Function
SYN	Synchronize	Set during initial communication. Negotiating of parameters and sequence numbers
ACK	Acknowledgment	Set as an acknowledgement to the SYN flag. Always set after initial

Flag	Name	Function
		SYN
RST	Reset	Forces the termination of a connection (in both directions)
FIN	Finish	Ordered close to communications
PSH	Push	Forces the delivery of data without concern for buffering
URG	Urgent	Data inside is being sent out of band. Example is cancelling a message

Port Numbers

- **Internet Assigned Numbers Authority** (IANA) - maintains Service Name and Transport Protocol Port Number Registry which lists all port number reservations
- Ranges
    - **Well-known ports** - 0 - 1023
    - **Registered ports** - 1024 - 49,151
    - **Dynamic ports** - 49,152 - 65,535

Port Number	Protocol	Transport Protocol
20/21	FTP	TCP
22	SSH	TCP
23	Telnet	TCP
25	SMTP	TCP
53	DNS	TCP/UDP
67	DHCP	UDP
69	TFTP	UDP
80	HTTP	TCP
110	POP3	TCP
135	RPC	TCP
137-139	NetBIOS	TCP/UDP
143	IMAP	TCP
161/162	SNMP	UDP
389	LDAP	TCP/UDP
443	HTTPS	TCP
445	SMB	TCP
514	SYSLOG	UDP

    - A service is said to be **listening** for a port when it has that specific port open
    - Once a service has made a connection, the port is in an **established** state
    - `Netstat` command:
        - Shows open ports on computer
        - **netstat -an** displays connections in numerical form
        - **netstat -b** displays executables tied to the open port (admin only)

Subnetting

- **IPv4 Main Address Types**
  - **Unicast** - acted on by a single recipient
  - **Multicast** - acted on by members of a specific group
  - **Broadcast** - acted on by everyone on the network
    - **Limited** - delivered to every system in the domain (255.255.255.255)
    - **Directed** - delivered to all devices on a subnet and use that broadcast address
- **Subnet mask** - determines how many address available on a specific subnet
  - Represented by three methods
    - **Decimal** - 255.240.0.0
    - **Binary** - 11111111.11110000.00000000.00000000
    - **CIDR** - x.x.x.x/12 (where x.x.x.x is an ip address on that range)
  - If all the bits in the host field are 1s, the address is the broadcast
  - If they are all 0s, it's the network address
  - Any other combination indicates an address in the range
  -