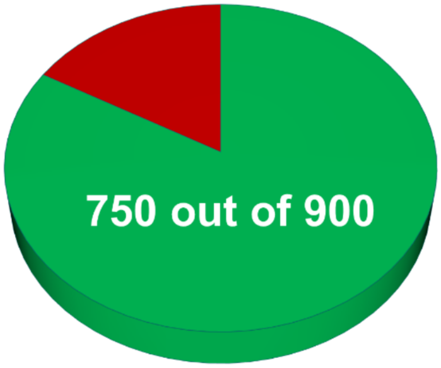
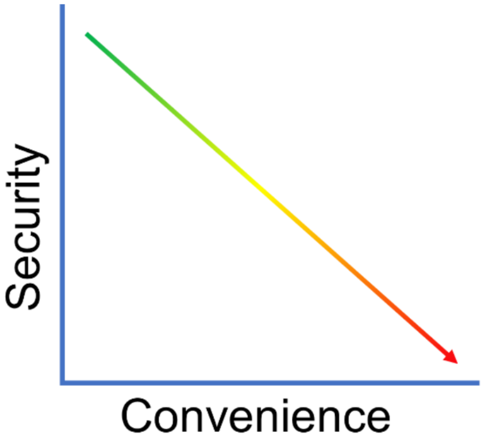
Overview of Security

- **Welcome**
  - **Domains (SYO-501)**
    - Threats, Attacks, and Vulnerabilities (21%)
    - Technologies and Tools (22%)
    - Architecture and Design (15%)
    - Identity and Access Management (16%)
    - Risk Management (14%)
    - Cryptography and PKI (12%)
  - **90 minutes to answer up to 90 questions**
  - **Minimum to Pass**



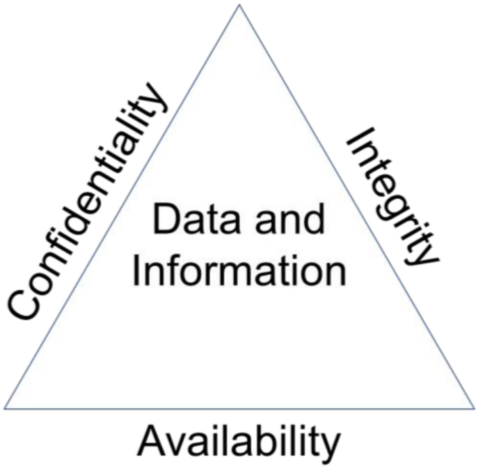
- **Overview of Security**



  - **Information Security**
    - Act of protecting data and information from unauthorized access, unlawful modification and disruption, disclosure, corruption, and destruction
  - **Information Systems Security**
    - Act of protecting the systems that hold and process our critical data

- **Basics and Fundamentals**

- **CIA Triad**



  - **Confidentiality**
    - Information has not been disclosed to unauthorized people
  - **Integrity**
    - Information has not been modified or altered without proper authorization
  - **Availability**
    - Information is able to be stored, accessed, or protected at all times

- **AAA of Security**
  - **Authentication**
    - When a person's identity is established with proof and confirmed by a system
      - Something you know
      - Something you are
      - Something you have
      - Something you do
      - Somewhere you are
  - **Authorization**
    - Occurs when a user is given access to a certain piece of data or certain areas of a building
  - **Accounting**
    - Tracking of data, computer usage, and network resources
    - Non-repudiation occurs when you have proof that someone has taken an action

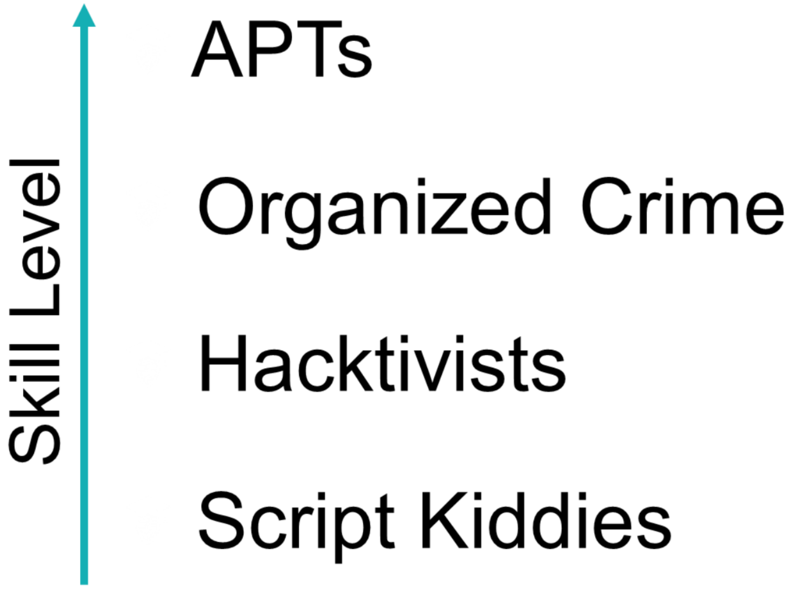
- Security Threats
  - **Malware**
    - Short-hand term for malicious software
  - **Unauthorized Access**
    - Occurs when access to computer resources and data occurs without the consent of the owner
  - **System Failure**
    - Occurs when a computer crashes or an individual application fails
  - **Social Engineering**
    - Act of manipulating users into revealing confidential information or performing other detrimental actions

- Mitigating Threats
  - Physical Controls
    - Alarm systems, locks, surveillance cameras, identification cards, and security guards
  - Technical Controls
    - Smart cards, encryption, access control lists (ACLs), intrusion detection systems, and network authentication
  - Administrative Controls
    - Policies, procedures, security awareness training, contingency planning, and disaster recovery plans
    - User training is the most cost-effective security control to use

- Hackers
  - Five Types of Hackers
    - White Hats
      - Non-malicious hackers who attempt to break into a company's systems at their request
    - Black Hats
      - Malicious hackers who break into computer systems and networks without authorization or permission
    - Gray Hats
      - Hackers without any affiliation to a company who attempt to break into a company's network but risk the law by doing so
    - Blue Hats
      - Hackers who attempt to hack into a network with permission of the company but are not employed by the company
    - Elite
      - Hackers who find and exploit vulnerabilities before anyone else does

        - 1 in 10,000 are elite
    - Script kiddies have limited skill and only run other people's exploits and tools

- **Threat Actors**
    - **Script Kiddies**
        - Hackers with little to no skill who only use the tools and exploits written by others
    - **Hacktivists**
        - Hackers who are driven by a cause like social change, political agendas, or terrorism
    - **Organized Crime**
        - Hackers who are part of a crime group that is well-funded and highly sophisticated
    - **Advanced Persistent Threats**
        - Highly trained and funded groups of hackers (often by nation states) with covert and open-source intelligence at their disposal



Malware

- **Malware**
  - **Malware**
    - Software designed to infiltrate a computer system and possibly damage it without the user's knowledge or consent
      - Viruses
      - Worms
      - Trojan horses
      - Ransomware
      - Spyware
      - Rootkits
      - Spam

- **Viruses**
  - **Virus**
    - Malicious code that runs on a machine without the user's knowledge and infects the computer when executed
    - Viruses require a user action in order to reproduce and spread
      - Boot sector
        - Boot sector viruses are stored in the first sector of a hard drive and are loaded into memory upon boot up
      - Macro
        - Virus embedded into a document and is executed when the document is
          opened by the user
      - Program
        - Program viruses infect an executable or application
      - Multipartite
        - Virus that combines boot and program viruses to first attach itself to the boot sector and system files before attacking other files on the computer
      - Encrypted
      - Polymorphic
        - Advanced version of an encrypted virus that changes itself every time it is executed by altering the decryption module to avoid detection

- Metamorphic
  - Virus that is able to rewrite itself entirely before it attempts to infect a file (advanced version of polymorphic virus)
- Stealth
- Armored
  - Armored viruses have a layer of protection to confuse a program or person analyzing it
- Hoax

- **Worms**
  - **Worm**
    - Malicious software, like a virus, but is able to replicate itself without user interaction
    - Worms self-replicate and spread without a user's consent or action
    - Worms can cause disruption to normal network traffic and computing activities
    - Example
      - 2009: 9-15 million computers infected with conficker

- **Trojans**
  - **Trojan Horse**
    - Malicious software that is disguised as a piece of harmless or desirable software
      - Trojans perform desired functions and malicious functions
  - **Remote Access Trojan (RAT)**
    - Provides the attacker with remote control of a victim computer and is the most commonly used type of Trojan

- **Ransomware**
  - **Ransomware**
    - Malware that restricts access to a victim's computer system until a ransom is received
    - Ransomware uses a vulnerability in your software to gain access and then encrypts your files
    - Example
      - $17 million: SamSam cost the City of Atlanta

- **Spyware**
  - **Spyware**
    - Malware that secretly gathers information about the user without their consent
    - Captures keystrokes made by the victim and takes screenshots that are sent to the attacker
  - **Adware**
    - Displays advertisements based upon its spying on you
  - **Grayware**
    - Software that isn't benign nor malicious and tends to behave improperly without serious consequences

- **Rootkits**
  - **Rootkit**
    - Software designed to gain administrative level control over a system without detection
    - DLL injection is commonly used by rootkits to maintain their persistent control
  - **DLL Injection**
    - Malicious code is inserted into a running process on a Windows machine by taking advantage of Dynamic Link Libraries that are loaded at runtime
  - **Driver Manipulation**
    - An attack that relies on compromising the kernel-mode device drivers that operate at a privileged or system level
    - A shim is placed between two components to intercept calls and redirect them
  - **Rootkits are activated before booting the operating system and are difficult to detect**

- **Spam**
  - **Spam**
    - Activity that abuses electronic messaging systems, most commonly through email
    - Spammers often exploit a company's open mail relays to send their messages
    - CAN-SPAM Act of 2003

- **Summary of Malware**
  - **Virus**
    - Code that infects a computer when a file is opened or executed
  - **Worm**
    - Acts like a virus but can self-replicate
  - **Trojan**
    - Appears to do a desired function but also does something malicious
  - **Ransomware**
    - Takes control of your computer or data unless you pay
  - **Spyware**
    - Software that collects your information without your consent
  - **Rootkit**
    - Gains administrative control of your system by targeting boot loader or kernel
  - **Spam**
    - Abuse of electronic messaging systems

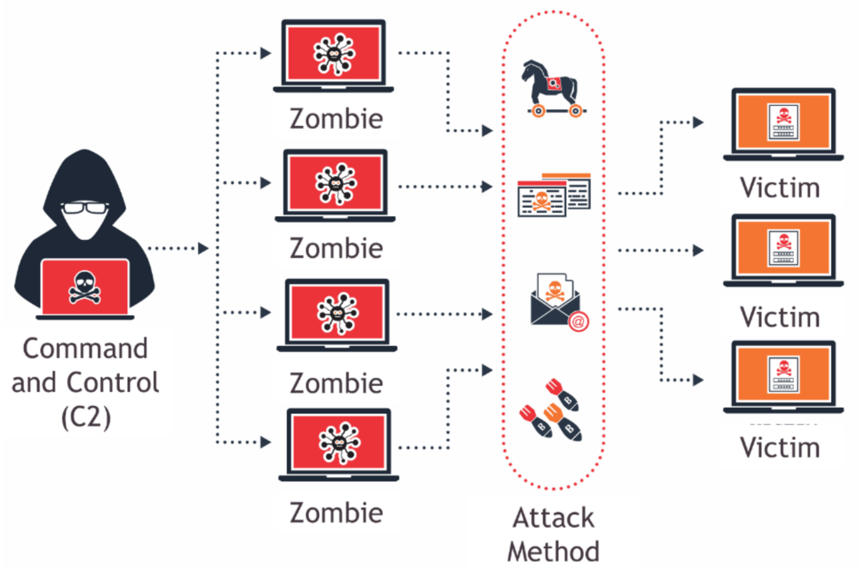
Malware Infections

- **Malware Infection**
  - **Threat Vector**
    - Method used by an attacker to access a victim's machine
  - **Attack Vector**
    - Method used by an attacker to gain access to a victim's machine in order to infect it with malware

- **Common Delivery Methods**
  - **Malware infections usually start within software, messaging, and media**
  - **Watering Holes**
    - Malware is placed on a website that you know your potential victims will access

DionTraining.com
DionTrainings.com

- **Botnets and Zombies**
  - **Botnet**
    - A collection of compromised computers under the control of a master node



- Botnets can be utilized in other processor intensive functions and activities

- **Active Interception & Privilege Escalation**
  - **Active Interception**
    - Occurs when a computer is placed between the sender and receiver and is able to capture or modify the traffic between them

  - **Privilege Escalation**
    - Occurs when you are able to exploit a design flaw or bug in a system to gain access to resources that a normal user isn't able to access

- **Backdoors and Logic Bombs**
  - **Backdoors are used to bypass normal security and authentication functions**
  - **Remote Access Trojan (RAT) is placed by an attacker to maintain persistent access**
  - **Logic Bomb**
    - Malicious code that has been inserted inside a program and will execute only when certain conditions have been met
  - **Easter Egg**
    - Non-malicious code that when invoked, displays an insider joke, hidden message, or secret feature
  - **Logic bombs and Easter eggs should not be used according to secure coding standards**