Defensive Security

Wednesday, July 9, 2025 12:26 AM

1. Preventing intrusions form occurring
2. Detecting intrusions when they occur and responding properly

Blue Hats are part of the defensive security landscape

- Related defensive security
    - User cyber security awareness: Training users about cyber security helps protect against attacks targeting their systems.
    - Documentation and Managing assets: We need to know the systems and devices we must manage and protect adequately.
    - Updating and patching systems: Ensuring that computers, servers and network devices are correctly updated and patched against any known vulnerability (weakness).
    - Setting up preventative security devices: Firewall and intrusion prevention systems (IDS/IPS) are critical components of preventative security. Firewalls control what network traffic can go inside and what can leave the system or network. IPS blocks any network traffic that matches present rules and attack signatures.
    - Setting up logging and monitoring devices: Proper network logging and monitoring are essential for detecting malicious activities and intrusions. If a new unauthorized device appears on our network, we should be able to detect it.
3. Security Operations Center (SOC)
4. Threat Intelligence
5. Digital Forensics and Incident Response (DFIR)
6. Malware Analysis

A (SOC) is a team of cyber security professionals that monitors the network and its systems to detect malicious cyber security events. Some of the main areas of interest for a SOC are

- Vulnerabilities
- Policy Violations
- Unauthorized activity
- Network intrusions

Threat Intelligence- Threat informed defense

- This covers Security Intelligence / and cyber threat intelligence
    - Security intelligence
        - the process where data is generated and is then collected, processed, analyzed, and disseminated to provide insights into the security status of information systems.
    - Cyber Threat Intelligence
        - Investigation, collection, analysis, and dissemination of information about emerging threats and threat sources to provide data about the external threat landscape.
            - Narrative Reports
            - Data Feed

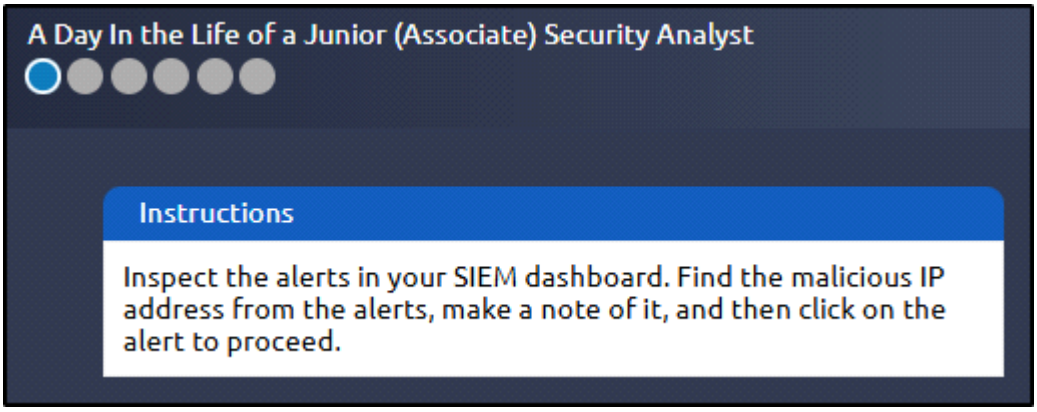
Digital Forensics and Incident Response (DFIR)

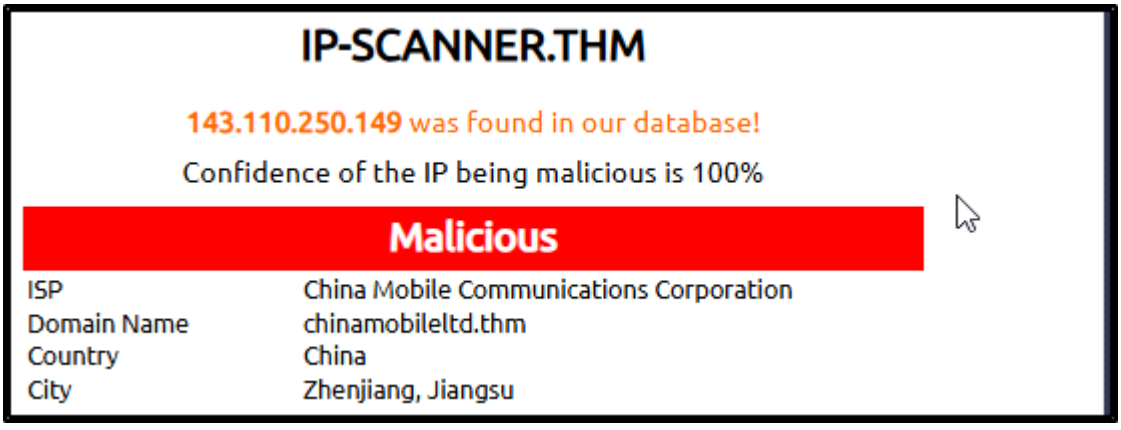
- Digital Forensics
    - Application of Science to investigate crimes and establish facts.
        - File Systems
            - forensics image (low-level copy)
                - installed programs
                - created files
                - partially overwritten files
                - deleted files
        - System Memory

        - □ if malware runs in memory without saving it to the disk
        - □ taking a forensic image (low-level copy) of the system is the best way to analyze its contents and learn about the attack.
      - System Logs
        - □ Each client and server computer maintains different log files about what is happening.
        - □ even if deleted some traces will remain
      - Network Logs
        - □ Logs of the network packets that have traversed a network would help answer more questions about whether an attack is occurring and what it entails.
- Incident Response
  - refers to a data breach
  - Cyber attack
  - misconfiguration
  - intrusion attempt
  - policy violation.
    - An attacker can make our network or systems
      - □ inaccessible (ransomware)
      - □ defacing the public website
      - □ data breach (stealing company data)
  - Method to respond to these incidents.
    - reduce damage
    - recover systems in the shortest time possible
      - □ Preparation
      - □ Detection and Analysis
      - □ Containment, Eradication, and Recovery
      - □ Post-Incident Activity
- Malware Analysis
  - Virus is a piece of code that attaches itself to a program. Designed to spread from one computer to another and works by altering, overwriting, and deleting files once it infects a computer. Resulting from performance becoming slow to unusable.
  - Trojan Horse - is a program that shows one desirable function but hides a malicious function underneath. Like downloading a video player that give the attacker complete control over their system.
  - Ransomware is a malicious program that encrypts the user's files. Encryption makes the files unreadable without knowing the encryption password. The attacker offers the user the encryption password if the user is willing to pay a "ransom".

1. Static analysis works by inspecting the malicious program without running it. This usually requires solid knowledge of assembly language (the processor's instruction set, the computer's fundamental instructions).
2. Dynamic analysis works by running the malware in a controlled environment and monitoring its activities. It lets you observe how the malware behaves when running.

Simulation Practice SOC security information event management





I got the okay from escalating to management, to block IP address. Using AbuseIPDB. Added 143.110.250.149 to the block list.