# Cyber Security Symposium

*What you can do to secure your system...even if you don't know what Hex is*

NW3C
NATIONAL WHITE COLLAR CRIME CENTER
INTEGRITY QUALITY SERVICE

# NW3C

- Training, investigative support and research to State, Local , and Tribal Law Enforcement agencies
- Non-profit , grant funded for over three decades (1978)
- For the general public, IC3.gov
  - Report online crime
  - Security Alerts and Tips
  - Annual Reports

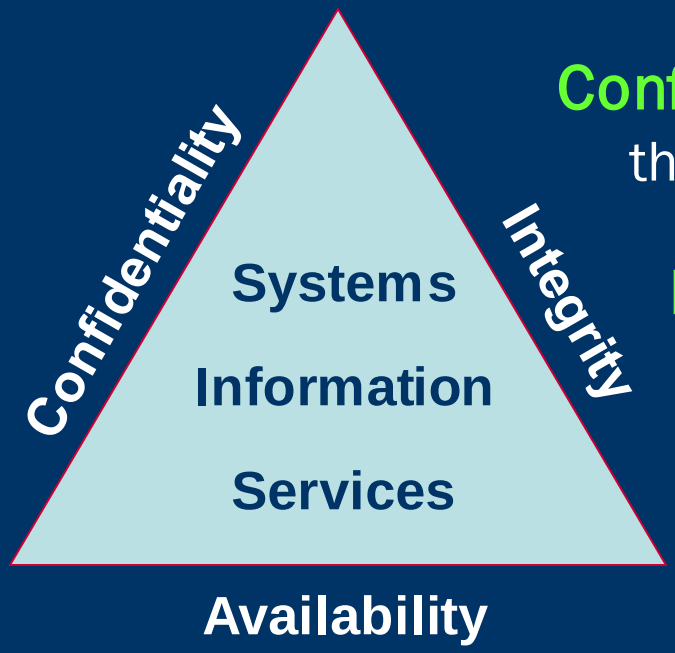
# Objectives

- Describe the CIA concept
- Identify your adversaries and their motives
- Describe the different classes of attack
- Explain the Defense-in-Depth strategy
- Define the principal components of the strategy
- Define the four overlapping layers of defense
- Provide examples of layered defenses

CIA

# Information Security Mission Statement

Provide for confidentiality, integrity, and availability of the systems, information, and services provided




**Confidentiality**— Information only available to those authorized to access it

**Integrity**— Assurance of information and system accuracy by preventing unauthorized alterations

**Availability**— Systems, information, & services available when needed

# Malicious Adversaries

- Terrorists
- Hackers
- Organized Crime Syndicates
- Terminated Employees
- Disgruntled Employees

# Non-Malicious Adversaries

- Reckless Users
- Poorly Trained Users
- “Rogue” Administrators

# Motivations for an Attack

- Gain access to sensitive / private information
- Disrupt operations or communications
- Track and monitor operations / movements
- Personal, commercial, or financial gain
- Discredit or embarrass a given target
- Obtain access to free resources
- Meet or overcome an advanced technical challenge

# Classifying Attacks

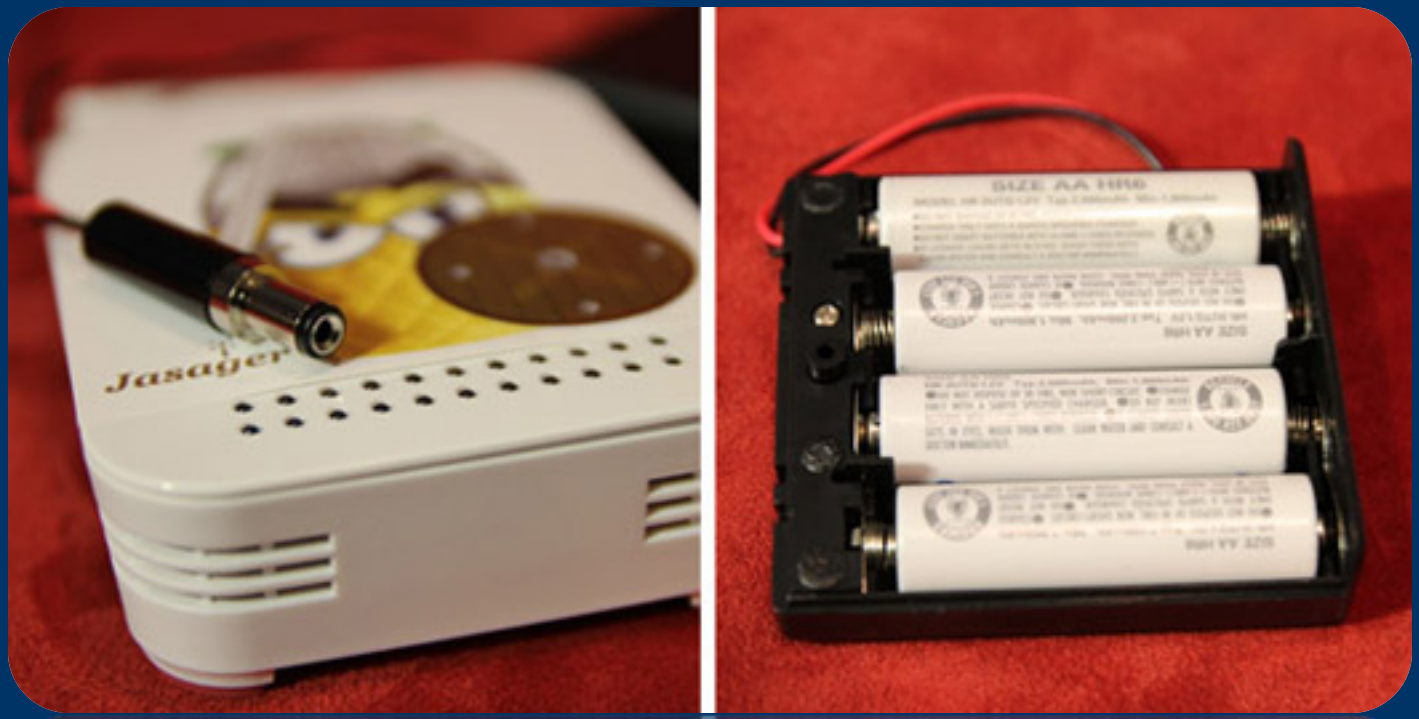
- System attacks have unique characteristics and signatures
  - Countermeasures are developed and implemented with those characteristics in mind
- Attacks are categorized into three classes
  - Passive attacks
  - Active attacks
  - Insider attacks

# Passive Attacks

- Monitoring of communications sent over public media such as public switched networks, Wi-Fi, satellite
  - Password sniffing
  - Monitoring plain-text communications
  - Decrypting weakly encrypted traffic

# Passive Attacks

- Pineapple Wi-Fi



# Active Attacks

- Circumventing security measures by exploiting software vulnerabilities or inserting malicious code to gain access to a system
  - Trojans & Viruses
  - Rootkits
  - Denial of Service
  - Buffer Overflows

# Insider Attacks

- Performed by persons who have authorized access to the system either locally or through some form of remote access
- May be malicious or non-malicious

# Insider Attacks

- Usually overlooked and typically harder to detect than other classes of attack
  - Unauthorized manipulation of information
  - Creation of covert channels or unauthorized network connections
  - Physical damage or destruction of a system

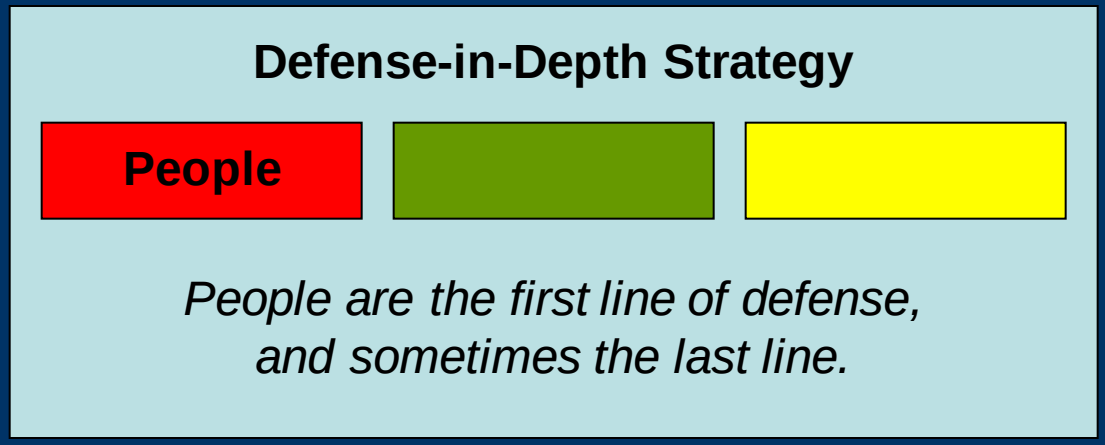
# Defense-in-Depth Strategy

*"Best practices" strategy for protecting information and information systems against attack; the integration of people, technology, and operations to achieve an effective and multi-layered security posture.*

# Defense-in-Depth Strategy

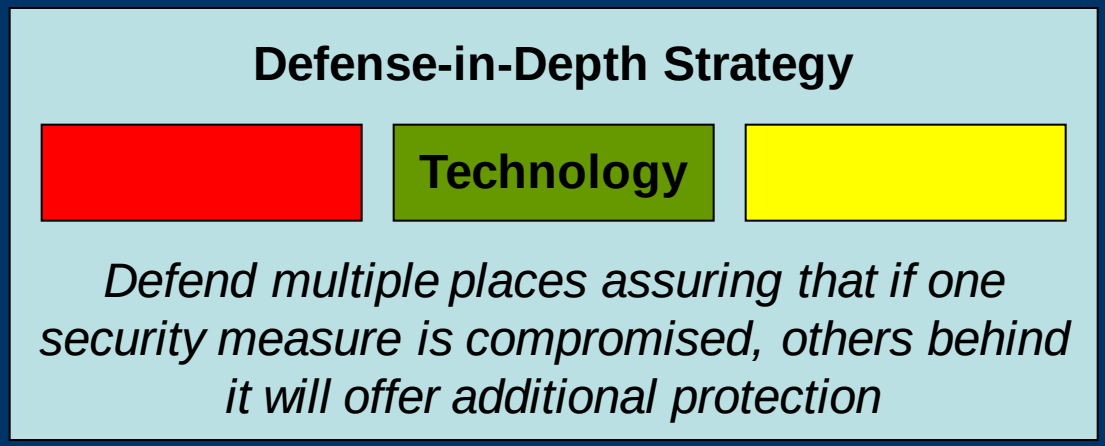
- Balanced focus on three principal components
  - People, Technology, & Operations
- Not a “one-man” solution & requires organizational support
- Layered approach to Information Security because no single countermeasure is sufficient
- If one security measure is compromised, others will provide added protection

# Principal Components



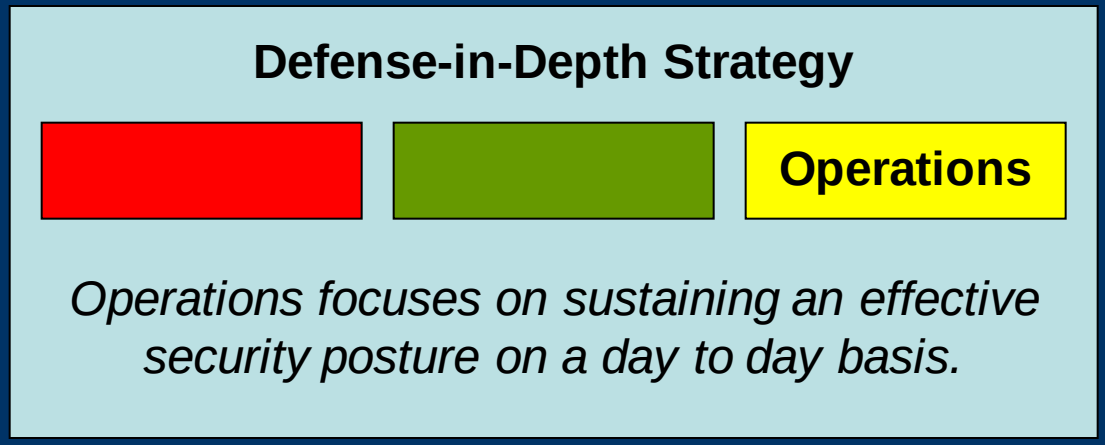

- Overall Philosophy
- Organizational Support
- Policies & Procedures
- Roles & Responsibilities
- Separation of Duties
- Training & Awareness

# Principal Components




- Identification & Authentication
- Access Control
- Threat Detection
- Encryption
- Content Filtering

# Principal Components

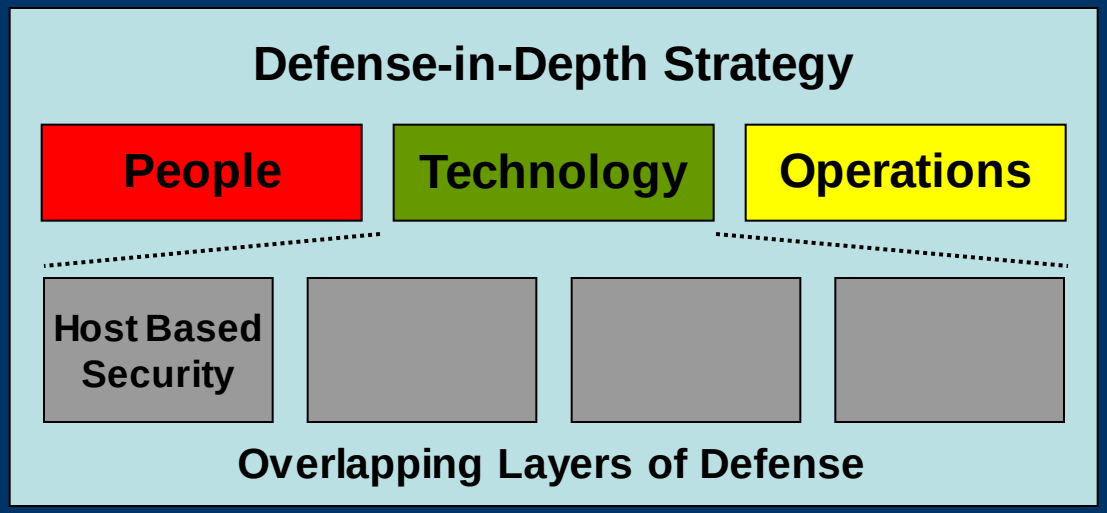



- User/System Administration
- Risk Management
- Disaster Recovery
- Incident Response
- Threat Assessment
- Monitoring & Auditing
- Interoperability Issues

# Layered Defense Concept

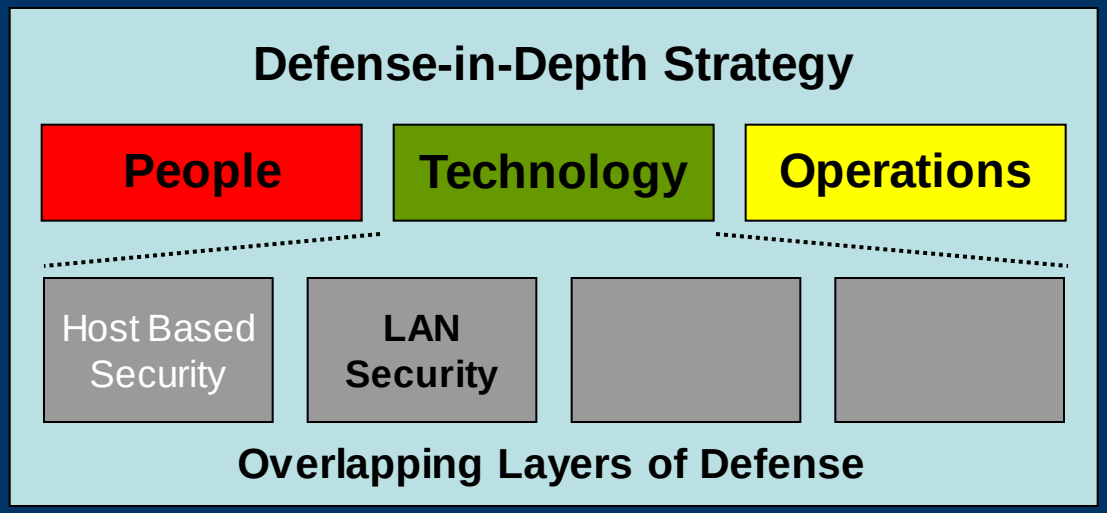
- Stresses deploying multiple, overlapping layers of defense between the adversary and his target
  - A single line of defense is not sufficient
  - All security products / solutions have vulnerabilities
    - Only a matter of time before they are exploited
- There are four overlapping layers of defense
  - Host-Based Security
  - LAN Security
  - Perimeter Security
  - Physical Security

# Layers of Defense



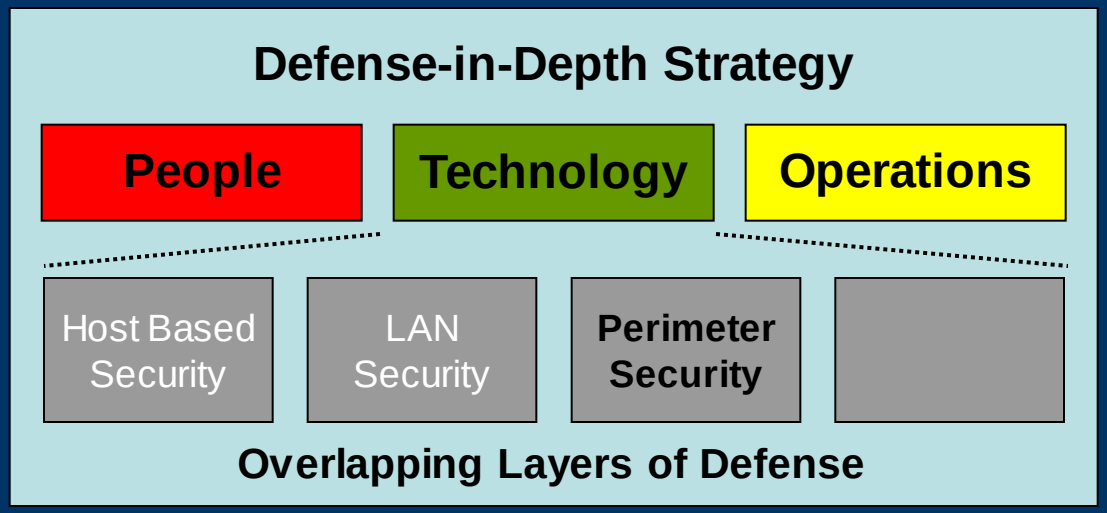

- User/System Administration
- Patch Management
- Malware Protection
- File System Permissions
- Logon Banner
- Host-Based Firewall
- Event Logging

# Layers of Defense



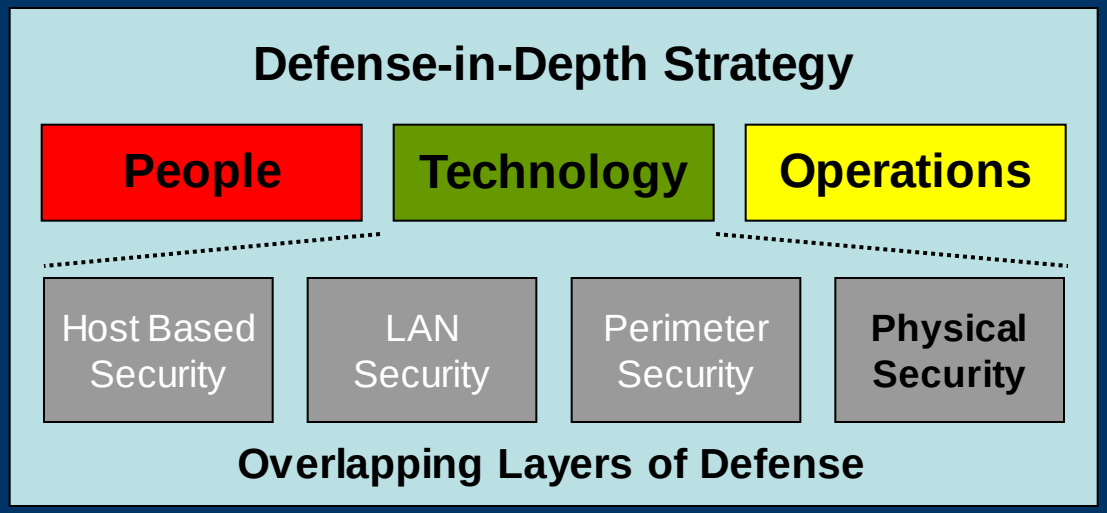

- Port Scanning
- Traffic Monitoring
- Switches over Hubs
- Network Segmentation
- Rogue Wireless APs
- Content Filtering

# Layers of Defense




- Routers
- Firewalls
- Access Control Lists
- Packet Filtering
- Virtual Private Networks
- Log Analysis

# Layers of Defense




- Physical Access
- Access Tracking / Auditing
- Physical Location
- Environmental Issues
- Backups & Images
  - Offsite Storage

# Examples

| Threat / Vulnerability | 1st Layer of Defense | 2nd Layer of Defense |
|---|---|---|
| The introduction of malicious code (e.g. virus, trojan, rootkit) | Host based anti-virus software | LAN-based anti-virus software |
| Unauthorized access confidential information | Hardware firewall | Host-based software firewall |
| Unauthorized use of systems | Fingerprint authentication | Login password |
| Monitoring plain-text communications | Prevent the use of wireless data transmission | Encrypt information during transmission |

# Review

- What is the CIA concept?
- What is the difference between a malicious and non-malicious adversary?
  - What are some examples of both?
- What are the three principal components of the Defense-in-Depth strategy?
- What are the four overlapping layers of defense?
- Why is a single layer of defense not sufficient?

# Questions/Comments?