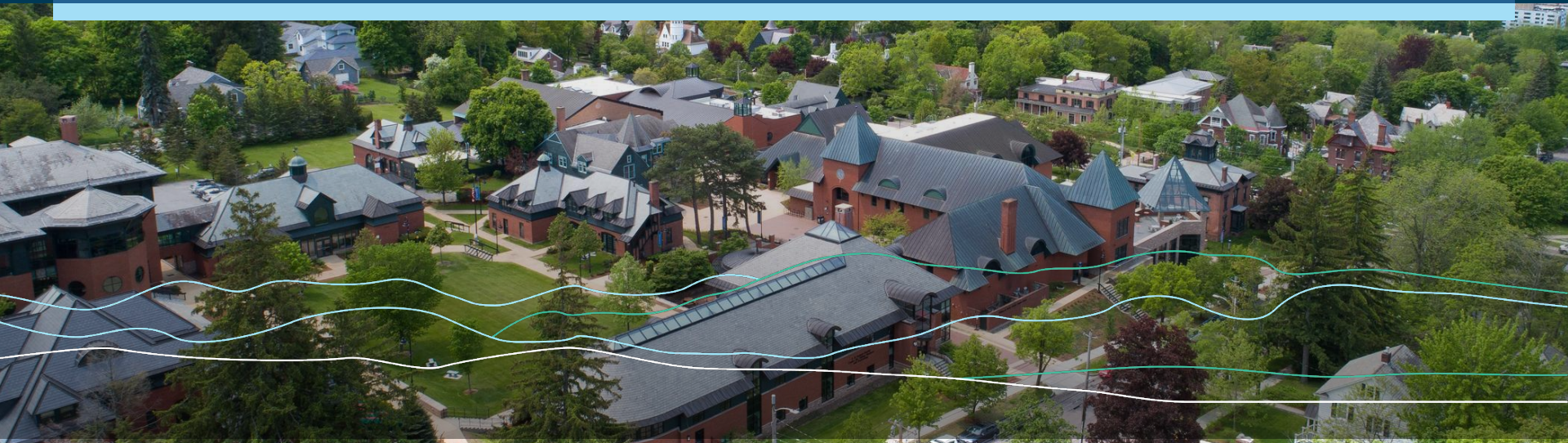
CHAMPLAIN COLLEGE

Mod 6 – System Security

SEC-110



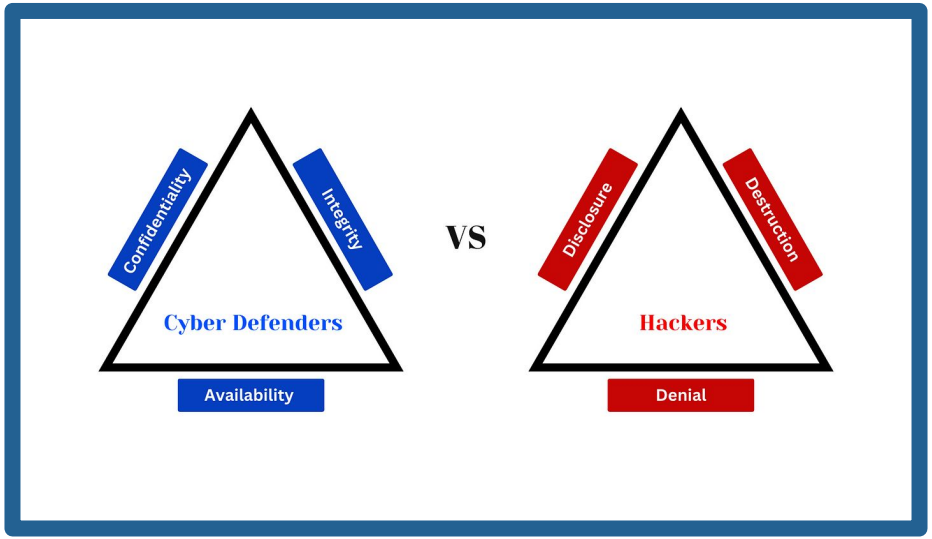
What is System Security?

Definition:

The measures and practices put in place to protect computer systems, networks, and data from **unauthorized access, damage,** or **theft**.

CIA Triad (again!)

System security is what we need to protect data to ensure it has CIA!



Vulnerabilities

Vulnerabilities are weaknesses in a system that can be exploited by attackers to gain unauthorized access or to cause harm.

Think of a crack in the wall; it may be small, but it gives someone a way to break in.

Common Threats

	Insider Threats	Social Engineering	Malware	Man-in-the-Middle	Denial of Service
Definition	A security risk from inside an organization such as employees	Tricking people into giving away confidential information or access	Malicious software designed to harm, spy on, or take control of systems	When a hacker secretly intercepts communication between parties	An attack that floods a system or website with traffic to make it crash or go offline
Example	An employee misuses their badge access to purposefully let a malicious intruder into the building.	A hacker makes a phone call to a CEO pretending to be IT to gain their login credentials.	A USB keylogger is installed on a computer by a hacker to spy on a user's activity.	While on public Wi-Fi, a hacker intercepts communication between a user and a web server.	A school website is targeted by a DOS attack and goes down during an online exam session.
Image					

Access Control

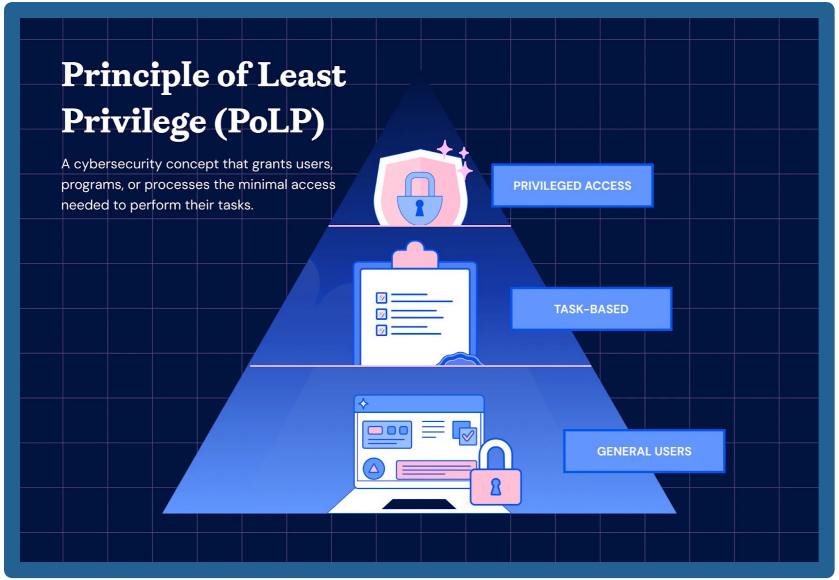
- **Controls *who* can get in, and *what* they can do**
- **Comes in many forms:**
  - Passwords
  - Pins
  - Keycards
  - Biometrics
  - Security Questions
  - OTP Codes

Types of Access Control

- **DAC -** Discretionary Access Control
  - Owner decides who can access resources
- **MAC -** Mandatory Access Control
  - Access based on security labels/classifications
- **RBAC -** Role-Based Access Control
  - Access based on job role
- **ABAC -** Attribute-Based Access Control
  - Access based on attributes (location, role, time)

Principle of Least Privilege

- Users should only have **access to what they need**, NOTHING MORE



- Helps reduce risk if an account is misused or compromised
- **Examples:**
  - Students shouldn't access their teacher's gradebooks
  - Janitors shouldn't access school network settings.

Access is controlled through...

Least Privilege Principle

- Users should only have access to the areas and information necessary to their job

Time-Based Access

- Restricting access during certain hours of the day

Geofencing

- Allowing access only when a user is in a specific location

Where do we control access?

Physical Perimeter

- Physical barriers that protect outer access
- Example: fences, locked doors, security guards

System Boundary

- Protecting internal systems from malicious damage.
- Example: firewalls filter transmitted packets

Physical Security Monitoring

Access Control

- Keycards, biometrics, PINs

Surveillance

- CCTV, security guards, alarms

Perimeter defense

- Fences, locks, security doors

System Surveillance & Monitoring

By monitoring IT infrastructure, endpoints, networks, and applications, misuse can be caught early

SIEM vs. SOAR vs. XDR: How they compare

SIEM	SOAR	XDR
Collects, aggregates and analyzes event data from multiple sources	Analyzes and prioritizes event data to launch automated responses	Collects and analyzes event data from multiple endpoint sources across the IT ecosystem
Uses AI to baseline event data for analysis	Builds on event data to speed up the process of incident response	Correlates all data for analysis and selection of a response
Data gathered can be used by SOAR for a more effective response	Uses SIEM data into an automated response	Handles all steps of the process, from data collection and analysis to event response

Key Monitoring Tool Types:

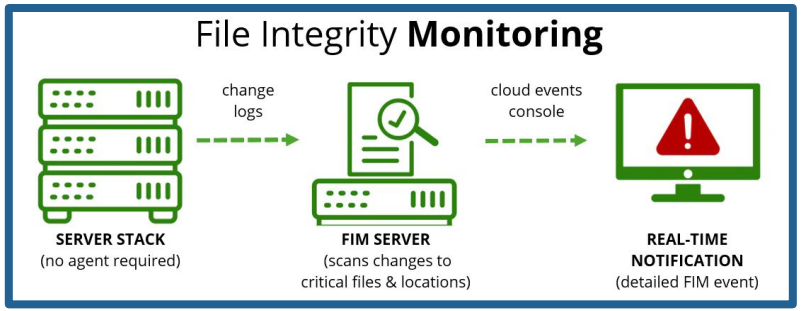
- **SIEM** - Security Information and Event Management
- **SOAR** - Security Orchestration, Automation, and Response
- **XDR** - Extended Detection and Response

Integrity Monitoring

How do we not only monitor confidentiality and availability, but also integrity?

Monitored items for integrity may include:

- System files & configurations
- Logs
- Installed software
- User permissions

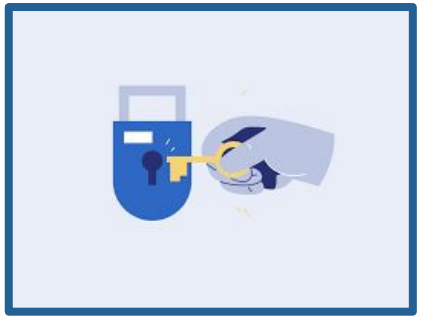


Integrity checking uses **digital fingerprints** - which will be covered in an upcoming module!

IoT and Physical Security

What is IoT?

- *Internet of Things* - Using internet-connected devices to monitor or access physical environments

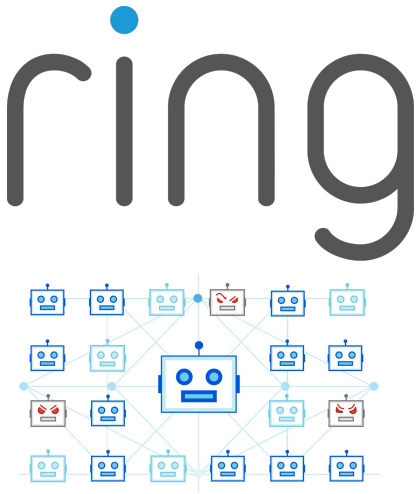


IoT in Physical Security

- Devices - Badge readers, motion detectors, and smart locks
- Cameras and sensors - detect unauthorized access and environmental changes (fire, water leaks, etc.)
- Can act as a form of Multi-Factor Authentication

IoT Risks

On May 28, 2025, thousands of Ring camera owners reported “new” devices logged into their accounts.



In 2016, the Mirai botnet became one of the most infamous examples of a botnet by taking control of unsecured IoT devices.

IoT risks include data privacy breaches, DoS attacks, and hijacking due to their nature as interconnected devices that may lack strong security measures and are difficult to monitor.

Emerging Trends

AI Powered Threat Detection: As machine learning and AI progresses, real time anomaly detection, malware analysis, and more become an increasing need against modern threats using the same technologies.

Zero Trust Architecture: Already commonplace, by never trusting a user / person without verification and authenticity, more bad actors are stopped than standard users affected.

Securing Remote Workforces: As working from home is now firmly established, VPN technology, endpoint protection, and home network security becomes a necessity.

Do’s & Don'ts

A company's cybersecurity is only as strong as their most vulnerable employee; don’t be the one who clicks the link!