CyberClaw - a cybersecurity Magazine, where we learn, teach and help secure the world.

In this Episode, I will be explaining the IoT and OT Landscape.

Here is a breakdown of what you need to know, starting with the basics and progressing to the cybersecurity considerations:

1. Understanding the Landscape: IoT and OT Defined

IoT (Internet of Things):

Definition: A network of physical objects ("things") embedded with sensors, software, and other technologies that allow them to connect and exchange data with other devices and systems over the internet or other networks.

Examples: Smart home devices (thermostats, lightbulbs, security cameras), wearables (fitness trackers, smartwatches), connected vehicles, smart city infrastructure (traffic sensors, smart grids), and many consumer and enterprise applications.

Key Characteristics:

- Often consumer-focused (but increasingly in enterprise)
- Vast diversity of devices, manufacturers, and operating systems
- Often resource-constrained (limited processing power, memory, battery)
- Usually relies on IP-based networks
- Data generation is often a primary function
- Often relies on cloud services

OT (Operational Technology):

Definition: Hardware and software that monitors and controls physical industrial processes and infrastructure. It is about the "real world" and making things work (like a factory line)

Examples: SCADA (Supervisory Control and Data Acquisition) systems, PLCs (Programmable Logic Controllers), DCS (Distributed Control Systems), robotics, HMIs (Human-Machine Interfaces), and other industrial control equipment.

Key Characteristics:

- Focuses on real-time operations and physical processes
- Often involves specialized protocols and communication methods
- Requires high availability, reliability, and safety
- Operated by engineers and process control specialists, not just IT people
- Typically uses proprietary systems and older technologies
- Direct impact on physical equipment and environments

Key Differences Between IoT and OT (although the lines can blur):

Feature	IoT	OT
Primary Focus	Data collection, interaction, user experience	Control and monitoring of physical processes, safety
Environment	Consumer and enterprise focused	Industrial, manufacturing, critical infrastructure
Typical Users	Consumers, business users	Engineers, process control specialists
Priority	Convenience, efficiency	Reliability, safety, availability
Technology	IP-based networks, Cloud-connected	Industrial protocols, specialized hardware

2. Why IoT and OT Cybersecurity is Critical

- **Vulnerability Landscape:**

  IoT:

  - Massive scale and diversity make it difficult to manage vulnerabilities.
  - Devices often have limited security features (default passwords, lack of updates).
  - Supply chain vulnerabilities can introduce malicious code.
  - Often a lack of user security awareness.
  - Often exposed on internet.

  OT:

  - Legacy systems often lack modern security features.
  - Critical infrastructure impacts (power, water, transportation).
  - Highly targeted by threat actors.
  - Operational demands make patching difficult.
  - Physical security is a major factor.
- **Potential Impacts of a Breach:**

  IoT:

  - Data theft and privacy breaches.
  - Denial of service (DoS) attacks.
  - Botnet creation for malicious activity.
  - Compromise of home/personal networks

  OT:

  - Disruption of critical services (power, water, gas).
  - Equipment damage and safety incidents.
  - Economic losses and business interruption.
  - Environmental impacts.
  - Political instability

3. Essential Cybersecurity Knowledge for IoT and OT

- **Network Architectures:**

  Understanding how IoT and OT networks are structured (e.g., layered architectures).

  Familiarity with Industrial Control System (ICS) architectures and zoning principles (e.g., Purdue model).

  Knowledge of networking protocols specific to IoT and OT.

- **Common Protocols:**

  IoT: MQTT, CoAP, Zigbee, Bluetooth, LoRaWAN, HTTP/S

  OT: Modbus, DNP3, OPC UA, PROFINET, EtherCAT

- **Vulnerabilities and Attack Vectors:**

  Common vulnerabilities associated with each system and their protocols

  Understanding how IoT and OT systems can be attacked (e.g., man-in-the-middle, firmware attacks, PLC injections).

- **Authentication and Authorization:**

  Best practices for securing user and device access in IoT and OT environments.

  Working with authentication protocols and mechanisms used in these domains.

- **Encryption and Data Security:**

  Understanding the importance of encryption for sensitive data at rest and in transit.

  Implementing appropriate encryption methods.

- **Security Monitoring and Incident Response:**

  How to collect and analyze security logs in IoT and OT environments.

  Developing effective incident response plans for breaches

  Dealing with different type of alerts than regular IT

- **Patch Management and Vulnerability Scanning:**

  Strategies for patching and updating IoT and OT devices without disruption.

  Identifying vulnerabilities and their impacts and importance.

- **Segmentation & Micro-segmentation:**

  Using network segmentation and micro-segmentation to limit the impact of breaches.

- **Risk Management:**

  Performing risk assessments specific to IoT and OT.

  Identifying and prioritizing security controls.

- **Compliance and Standards:**

  Understanding relevant regulations, standards, and frameworks (e.g., NIST Cybersecurity Framework, ISA/IEC 62443, GDPR).

- **Physical Security:**

  Recognizing the importance of physical security measures in OT environments.

- **Supply Chain Security:**

Assessing risks associated with vendors, components, and software.

Understanding vulnerabilities introduced via the supply chain.

4. Getting Started as a Cybersecurity Analyst in IoT/OT

- **Focus on learning:**

  Online resources: There are many free courses on cybersecurity, as well as OT and IoT specifically.

  Certifications: Consider certifications such as:

- CompTIA Security+
- GICSP (GIAC Industrial Cyber Security Professional)
- ISA/IEC 62443 cybersecurity certifications

Books and Research: Read about case studies of breaches and understand where their weak points were.

- **Hands-on Practice:**

  Lab environments: Set up virtual or physical lab environments to test and practice security controls.

  Open-source tools: Experiment with open-source security tools designed for IoT and OT.

- **Networking:**

  Connect with professionals in the field via online communities and industry events.

- **Stay Updated:**

  IoT and OT security is rapidly evolving; stay updated on the latest threats and best practices.

Key Takeaways

- IoT and OT security is a challenging but rewarding field.
- A strong understanding of both IT and operational environments is essential.
- The cybersecurity of IoT and OT is a complex domain requiring specialized knowledge and practices.

- Start by building a strong foundation in cybersecurity fundamentals and gradually dive deeper into the specifics of each domain.

1. Focus on Awareness and Understanding

- **Learn the Basics:** Continue your learning journey, as outlined previously. The more you understand about IoT and OT, the better you'll be at spotting anomalies.
- **Know Your Environment:**

  Inventory: Understand what IoT and OT devices are present on the network. Even at a basic level, you should be aware of the broad categories (e.g., smart cameras, PLCs, HMIs)

Network Topology: Get familiar with how your organization's IoT and OT networks are segmented and connected.

- **Understand Key Assets:** Identify the most critical devices and the potential impact of a compromise (e.g., an electric substation PLC).
- **Shadow Senior Analysts:** Work alongside more experienced analysts to learn how they handle IoT/OT-related security incidents. Ask questions and take notes.

2. Monitoring and Detection:

- **Monitor for Suspicious Traffic:**

  Network Baselines: Work with other team members to establish baseline network activity for IoT and OT devices. Look for deviations from that norm.

  Protocol Awareness: Watch for abnormal usage of IoT and OT protocols (e.g., unusual Modbus requests).

  Unusual Connections: Flag devices communicating with unusual destinations or on suspicious ports.

  Data Spikes: Look for sudden increases in data flows, which could indicate data exfiltration.

- **Alert Triage and Analysis:**

  Recognize Relevant Alerts: Learn how to distinguish between normal IoT/OT traffic and security alerts.

  First-Level Analysis: Perform an initial analysis of alerts to determine if they require escalation. Don't be afraid to ask for help, remember your level.

  Alert Enrichment: Gather information about the affected devices and potential impact.

- **Log Review:**

  Focus on Critical Devices: Prioritize log reviews of critical OT devices and infrastructure.

  Look for Anomalies: Identify unusual login attempts, configuration changes, or error messages.

3. Response and Containment:

- **Follow Defined Procedures:** Understand and strictly adhere to your organization's incident response procedures for IoT and OT.
- **Isolate Affected Devices:** Work with network teams to isolate compromised devices or segments of the network.

- **Collect Incident Evidence:** Help to gather logs, packet captures, and other evidence for further investigation.
- **Assist in Containment:** Provide first-level support during incident containment activities, such as shutting down suspicious processes.

4. Security Control Implementation (Assisting):

- **User Access Management:** Work with IT/OT teams to enforce strong passwords and multi-factor authentication.
- **Assist with Network Segmentation:** Support implementation of network segmentation efforts that limits access to IoT/OT devices.
- **Assist in Patching:** Contribute by verifying patch schedules, not performing the patching operation itself.
- **Monitor the Effectiveness of Controls:** Help verify if new controls are working as expected in your daily work.

5. Communication and Collaboration

- **Documentation:** Contribute to incident reports, playbooks, and knowledge bases, creating reusable information.
- **Communication:** Be a bridge between IT and OT teams. Use clear, simple language and take notes for cross-team communication.
- **Raise Concerns:** Don't hesitate to raise security concerns to your senior analyst, even if you aren't sure.

Practical Steps for Your Role:

- **Learn your organization's SOC tools:** Get good at using the SIEM, firewalls, and other security tools used to analyze IoT and OT data.
- **Create Checklists:** Develop checklists for common tasks, like alert analysis or incident response steps.
- **Test your skills:** Use sandbox environments to experiment and test potential threats against IoT/OT devices.
- **Stay Curious and Inquisitive:** Ask questions, research vulnerabilities, and keep learning about new threats.
- **Participate in regular training sessions:** Take advantage of internal and external training opportunities to upskill.
- **Document your work:** Keep detailed notes of all activities you perform and what you observe.

What you SHOULD NOT do as a Level 1 SOC Analyst:

- **Implement major architectural changes:** Stay away from modifying any critical infrastructure without supervision.
- **Perform unauthorized system changes:** Don't adjust device settings or install software without explicit permission and guidance.
- **Bypass security protocols:** Always adhere to established processes and procedures.

- **Share sensitive information improperly:** Handle all information with utmost care and follow security protocols.
- **Panic or make assumptions:** Stay calm, ask questions, and follow protocols to correctly identify threats.

Key for Level 1:

Your job as a level 1 is to be a **watcher, alerter, and assistor** when it comes to IoT/OT security. Focus on learning, monitoring, responding according to established procedures, and clearly communicating security issues that you observe. You are a critical part of the team and a bridge between the IT and OT departments, so make sure to work to ensure all parties stay informed and secure.

1. Network Security Implementations

- **Network Segmentation:**

  What it is: Dividing the network into smaller, isolated segments to limit the impact of a breach. This can involve physical or logical separation.

  Why it's important: Prevents an attacker who breaches one segment from moving laterally across the entire network.

  How it impacts you: You need to know which devices belong to which segments to understand the scope of an alert.

  Example: Separating the OT network from the corporate IT network; further isolating critical PLCs.

- **Firewalls:**

  What it is: A system that controls network traffic based on predefined rules.

  Why it's important: Prevents unauthorized access to the network and blocks malicious traffic.

  How it impacts you: Understanding firewall rules allows you to identify legitimate and suspicious traffic. You may need to check if blocked traffic is expected or not.

  Example: Industrial firewalls that filter communication based on OT protocols.

- **Intrusion Detection/Prevention Systems (IDS/IPS):**

  What it is: Systems that monitor network traffic for malicious activity and can either alert on (IDS) or block (IPS) suspicious behavior.

  Why it's important: Provides real-time detection and prevention of attacks.

How it impacts you: You will receive alerts from these systems that you need to analyze and respond to.

Example: Network-based IDS/IPS specific to OT protocols.

- **Virtual Private Networks (VPNs):**

  What it is: Creates a secure, encrypted connection between two points on a network.

  Why it is important: Allows secure access for remote users and protects data transmitted over insecure networks.

  How it impacts you: Recognizing legitimate VPN use and identifying potentially malicious VPN connections are essential.

- **Micro-segmentation:**

  What it is: Very granular segmentation. Isolating individual assets or groups of assets within the network by implementing firewall rules at the asset level.

  Why it's important: Limits attack impact to very specific devices or areas.

  How it impacts you: May need to know the rules of each micro segment to understand the nature and scope of an incident.

  Example: Firewalls directly embedded into OT assets or devices.

2. Identity and Access Management

- **Multi-Factor Authentication (MFA):**

  What it is: Requires users to provide more than one form of authentication (e.g., password + token).

  Why it's important: Enhances security by adding an extra layer of protection against unauthorized access.

  How it impacts you: You need to understand the MFA policies and look for failed MFA attempts that may indicate a brute-force attack.

- **Role-Based Access Control (RBAC):**

  What it is: Assigning permissions based on a user's role and responsibilities.

  Why it's important: Ensures users only have the necessary access to perform their tasks, limiting potential for abuse or error.

How it impacts you: You need to be aware of user roles and access privileges to detect privilege escalation attempts.

- **Strong Passwords and Password Policies:**

  What it is: Requiring users to create complex passwords that are changed regularly.

  Why it's important: Reduces the risk of password compromise.

  How it impacts you: You may need to investigate accounts that don't conform to password policies or that are being targeted in brute-force attacks.

3. Device Security

- **Device Hardening:**

  What it is: Securing devices by disabling unnecessary features, patching vulnerabilities, and configuring them securely.

  Why it's important: Reduces the attack surface of individual devices.

  How it impacts you: You need to know the baseline configuration for devices and look for deviations.

  Example: Disabling unused network services on a PLC.

- **Firmware Updates:**

  What it is: Applying updates to device firmware to fix bugs and security vulnerabilities.

  Why it's important: Ensures that devices are running the latest, most secure software.

  How it impacts you: You might receive alerts or reports for devices that are running out-of-date firmware versions.

Secure Boot:

What it is: A process that verifies the integrity of the firmware during boot-up to ensure that only trusted software is loaded.

Why it's important: Prevents devices from being booted with malicious or compromised firmware.

How it impacts you: You need to be aware of devices that aren't completing secure boot processes.

4. Data Security

- **Encryption (at rest and in transit):**

  What it is: Encoding data so that it can only be read with a decryption key.

  Why it's important: Protects data confidentiality in case of a breach.

  How it impacts you: You may need to know if data is being properly encrypted in different parts of the infrastructure.

  Example: Encrypting communications between devices and control systems.

Data Loss Prevention (DLP):

  What it is: Systems that prevent sensitive data from leaving the network or being accessed by unauthorized individuals.

  Why it is important: Protects sensitive data and prevents data exfiltration.

  How it impacts you: You may receive alerts when sensitive data is detected leaving the network.

Data backups:

  What it is: Regular copies of the most sensitive information.

  Why it is important: In case of a security breach or system failure, data is not lost.

  How it impacts you: You need to know if and how often this is performed to better understand potential risks.

5. Monitoring and Logging

- **Security Information and Event Management (SIEM):**

  What it is: A system that collects, stores, and analyzes security logs from various sources.

  Why it's important: Provides a centralized view of security events and allows for threat detection.

  How it impacts you: This is one of your primary tools for analyzing alerts and identifying security incidents.

Log Management:

  What it is: The process of collecting, storing, and analyzing log files from various devices and systems.

Why it is important: Provides visibility into system activity, facilitates troubleshooting, and aids in investigations.

How it impacts you: You need to understand what logs are being collected, their formats, and how to interpret them.

6. Incident Response

- **Incident Response Plans:**

  What it is: A detailed plan that outlines the steps to take in the event of a security incident.

  Why it is important: Ensures a coordinated and effective response to security breaches.

  How it impacts you: You need to be familiar with the plan and your role in it.

Regular Drills:

What it is: Simulation of security incidents to test the effectiveness of the incident response plan.

Why it is important: Identifies weaknesses in the response plan and improves team readiness.

How it impacts you: Allows you to practice and improve your response skills and see how systems work.

Key Points for Your Awareness:

- **Functionality:** Focus on understanding what these controls *do*, not necessarily *how* they're configured.
- **Limitations:** Recognize that no security control is perfect. It is important to understand the limitations of each, to take actions accordingly.
- **Impact on Operations:** Be aware of how security controls might impact the operational environment.

Here are numerous mitigation strategies that can be implemented to reduce the risk and impact of attacks on IoT and OT systems. These mitigations span various layers of security and require a defense-in-depth approach. Here is a breakdown of key mitigations, categorized for clarity:

1. Network Security Mitigations

- **Network Segmentation & Micro-segmentation:**

  Mitigation: Isolating IoT and OT networks from the corporate IT network, as well as further segmenting within the OT environment itself (by function, criticality, etc.)

Rationale: Prevents attackers from moving laterally across the network and limits the blast radius of a breach.

Implementation: Use firewalls, VLANs, and physical separation to create distinct zones.

Firewall & Access Control Lists (ACLs):

Mitigation: Implementing strict rules to control network traffic based on source, destination, port, and protocol.

Rationale: Blocks unauthorized communication and limits exposure to external threats.

Implementation: Deploy industrial-grade firewalls with deep packet inspection capabilities.

Intrusion Detection/Prevention Systems (IDS/IPS):

Mitigation: Monitoring network traffic for suspicious patterns and blocking malicious activity.

Rationale: Detects and prevents attacks in real time.

Implementation: Use specialized IDS/IPS for OT protocols and customize rules for specific devices.

VPNs & Secure Remote Access:

Mitigation: Requiring secure, encrypted connections for remote access using VPNs with multi-factor authentication (MFA).

Rationale: Prevents eavesdropping and unauthorized access from external networks.

Implementation: Enforce strong authentication protocols and regularly monitor for unusual access.

Network Monitoring:

Mitigation: Continuously monitoring network traffic for anomalies.

Rationale: Detect deviations from baselines and spot potential security issues before they escalate.

Implementation: Use network monitoring tools to track traffic patterns and look for deviations from normal.

2. Device Security Mitigations

- **Device Hardening:**

Mitigation: Disabling unnecessary services, changing default passwords, removing unused accounts, and applying security patches.

Rationale: Reduces the attack surface and removes exploitable vulnerabilities.

Implementation: Use security configuration guides and regularly audit device settings.

Firmware Updates and Patch Management:

Mitigation: Regularly applying firmware and software updates to devices to fix bugs and address vulnerabilities.

Rationale: Ensures that devices have the latest security fixes and are protected against known threats.

Implementation: Implement a robust patch management process for all IoT and OT devices.

Secure Boot:

Mitigation: Ensuring that devices only boot up using verified and trusted firmware and software.

Rationale: Prevents devices from booting with malicious or compromised code.

Implementation: Enable secure boot features that use cryptographic signatures.

Device Authentication:

Mitigation: Requiring devices to authenticate before connecting to the network or other devices.

Rationale: Prevents unauthorized devices from accessing the network.

Implementation: Use digital certificates or other forms of device authentication.

3. Identity & Access Management Mitigations

Multi-Factor Authentication (MFA):

Mitigation: Requiring multiple forms of authentication (e.g., password + token, biometric) for user access.

Rationale: Adds an extra layer of security and protects against compromised passwords.

Implementation: Enforce MFA for all critical systems and user accounts.

Role-Based Access Control (RBAC):

Mitigation: Assigning user permissions based on their job roles and responsibilities.

Rationale: Limits user access to only the necessary resources and prevents privilege escalation attacks.

Implementation: Implement RBAC policies and regularly review user access permissions.

Least Privilege Principle:

Mitigation: Granting users and devices only the minimum privileges required to perform their tasks.

Rationale: Limits the potential damage that can be done by a compromised account or device.

Implementation: Audit user accounts and permissions, remove unnecessary privileges.

4. Data Security Mitigations

Encryption (in transit and at rest):

Mitigation: Encrypting data during transmission and when stored on devices or databases.

Rationale: Protects data confidentiality in case of interception or a breach.

Implementation: Use encryption protocols like TLS for network communications and encrypt data storage.

Data Loss Prevention (DLP):

Mitigation: Implementing systems to prevent sensitive data from leaving the network or being accessed by unauthorized parties.

Rationale: Prevents data exfiltration and data breaches.

Implementation: Deploy DLP solutions and monitor data flows.

Data Backups:

Mitigation: Regular backups of critical system data and configurations to recover from data loss and system failures.

Rationale: Provides a recovery mechanism to help ensure business continuity.

Implementation: Backups should be regular, automated, and kept in a secure location.

5. Application Security Mitigations

- **Secure Coding Practices:**

  Mitigation: Ensuring that software is developed using secure coding practices that prevent vulnerabilities.

  Rationale: Reduces the risk of software vulnerabilities that attackers could exploit.

  Implementation: Use secure coding standards, perform code reviews, and vulnerability assessments.

Input Validation:

  Mitigation: Checking all data inputs for format, length, and validity to prevent injection attacks.

  Rationale: Blocks attackers from manipulating input data and causing unexpected behavior.

  Implementation: Use libraries to implement proper input sanitization and validation.

6. Physical Security Mitigations

Physical Access Controls:

  Mitigation: Limiting physical access to devices and infrastructure through access badges, security cameras, and guards.

  Rationale: Prevents unauthorized individuals from physically tampering with devices or accessing sensitive data.

  Implementation: Implement physical security measures based on a risk assessment.

Environmental Monitoring:

  Mitigation: Monitoring the environment around critical devices to identify unauthorized activity and ensure that systems operate under secure parameters.

  Rationale: Provides added protection in physical spaces where an attack can occur.

  Implementation: Install monitoring systems to detect threats and unusual events.

7. Operational & Organizational Mitigations

Incident Response Plans:

  Mitigation: Having a documented plan that details the steps to take in the event of a security incident.

Rationale: Provides a coordinated approach to handling incidents and reduces potential damage.

Implementation: Regularly test and update incident response plans.

Regular Security Audits and Vulnerability Assessments:

Mitigation: Regularly assessing the security of IoT and OT systems to identify vulnerabilities and weaknesses.

Rationale: Helps to discover and fix vulnerabilities and weaknesses before attackers can exploit them.

Implementation: Perform periodic security audits, vulnerability scans, and penetration testing.

Security Awareness Training:

Mitigation: Training employees on security best practices to raise awareness and reduce the risk of human error.

Rationale: Empowers personnel to recognize and avoid potential security threats.

Implementation: Conduct regular security awareness training for all employees.

Supply Chain Security:

Mitigation: Assessing the security of vendors, components, and software to reduce risks that originate in the supply chain.

Rationale: Prevents attacks from suppliers and reduces the risk of compromised devices and software.

Implementation: Require secure development practices from suppliers and audit vendor security postures.

Key Points:

- **Layered Approach:** It is vital to implement security in multiple layers, so that if one layer is compromised, others provide protection.
- **Risk Assessment:** Mitigations should be based on risk assessments that consider specific threats and vulnerabilities.
- **Continuous Improvement:** Security is not a one-time project; mitigation strategies must be regularly reviewed and improved.

mapping IoT and OT attacks to the MITRE ATT&CK framework. This is a crucial step for understanding the attacker's perspective, identifying potential attack paths, and improving your security posture.

Understanding MITRE ATT&CK

The MITRE ATT&CK framework is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. It's organized into a matrix structure:

- **Tactics:** High-level categories of attacker goals (e.g., Initial Access, Execution, Persistence).
- **Techniques:** Specific methods that attackers use to achieve their tactics (e.g., Phishing, Exploitation of Remote Services, Valid Accounts).
- **Sub-techniques:** More granular descriptions of specific ways to implement a technique.

While MITRE ATT&CK was initially developed for enterprise IT systems, there are now matrices for ICS (Industrial Control Systems), which is a subset of OT. Mapping IoT attacks is still evolving, but we can adapt techniques using both matrices.

Mapping IoT Attacks to ATT&CK

IoT attacks often follow a similar pattern to IT attacks, but with a focus on the unique characteristics of IoT devices:

ATT&CK Tactic	ATT&CK Technique (Example)	IoT Attack Example	Description
Initial Access	T1190: Exploit Public-Facing Application	Exploiting vulnerabilities in a smart camera's web interface	Exploiting known vulnerabilities in IoT device software or firmware that are exposed to the internet.
	T1133: External Remote Services	Brute-forcing default credentials on a smart thermostat	Gaining access through weak or default login credentials on internet-accessible services.
	T1078: Valid Accounts	Using stolen credentials to access an IoT platform	Using legitimate credentials stolen by phishing or other means.
	T1195: Supply Chain Compromise	Compromised firmware installed at the factory, infecting the supply chain	Injecting malicious code into IoT devices during manufacturing or distribution.
Execution	T1059: Command and Scripting Interpreter	Using command injection in a printer's web interface	Executing shell commands using vulnerabilities.
	T1204: User Execution	Getting a user to click on a link and running malicious JavaScript on a browser	Tricking users into unknowingly executing malicious code.
	T1053: Scheduled Task/Job	Scheduling a recurring task to execute a malicious payload in an IP Camera	Scheduling tasks in the device itself to execute malicious code.
Persistence	T1078: Valid Accounts	Creating a new user account for persistent access on the IoT platform	Creating backdoor accounts to maintain persistent access to the devices.

	T1053: Scheduled Task/Job	Creating a scheduled job to run a persistent backdoor in a smart speaker.	Scheduling jobs to persistently execute malicious payloads.
	T1547: Boot or Logon Autostart Execution	Modifying the device bootloader to run malicious code on start-up	Injecting malicious code that runs every time the device boots up.
Privilege Escalation	T1068: Exploitation for Privilege Escalation	Using a vulnerability to gain root access on a smart router	Exploiting vulnerabilities to elevate privileges on the device.
	T1078: Valid Accounts	Using a stolen administrator account on a smart device.	Escalating access privileges using compromised accounts with higher privileges.
Defense Evasion	T1070: Indicator Removal	Deleting log files on a smart camera to cover tracks.	Removing log files or other indicators that would raise suspicions.
	T1027: Obfuscated Files or Information	Obfuscating malicious code in an embedded device.	Obfuscating malware using techniques like encoding or encryption to avoid detection.
	T1027: Obfuscated Files or Information	Encoding communications to the attacker with an IoT protocol	Hiding communication to the attacker from detection systems.
Credential Access	T1081: Credentials in Files	Accessing hardcoded credentials in an IoT device's firmware image	Obtaining credentials embedded in the device itself or its software.
	T1003: OS Credential Dumping	Dumping credentials from an IoT platform's database	Getting valid credentials from the system.
Discovery	T1016: System Network Configuration Discovery	Discovering network information of a controlled device using network scanning tools	Gathering information about the network topology, connected devices, and other hosts.
	T1082: System Information Discovery	Discovering the firmware version of an IoT device using a command	Identifying the operating system and software running on targeted IoT devices.
Lateral Movement	T1021: Remote Services	Moving from a compromised smart TV to other devices on the same network.	Moving through the network using remote services and shared resources.
	T1210: Exploitation of Remote Services	Exploiting a vulnerability in a smart TV to control it from the compromised thermostat.	Leveraging exploitable vulnerabilities in other devices on the same network to pivot.
Collection	T1005: Data from Local System	Accessing video footage from a compromised security camera	Gathering data from the device itself, including sensor data and system logs.

Command and Control	T1071: Application Layer Protocol	Communicating with the C2 server using MQTT or other IoT protocols	Using legitimate application layer protocols for control.
	T1001: Obfuscated C2 Channel	Hiding malicious traffic by using an encrypted MQTT channel	Obfuscating communications to a command and control server to evade detection.
Exfiltration	T1041: Exfiltration Over C2 Channel	Exfiltrating recorded videos from a compromised camera to an attacker-controlled server	Transferring stolen data from the device to an external server.
Impact	T1499: Endpoint Denial of Service	Sending a flood of requests to an IoT device, causing it to become unavailable.	Disrupting availability of devices by crashing them.
	T1498: Data Destruction	Deleting or corrupting data stored in an IoT device	Deleting or modifying data on the devices, causing business interruption.

Mapping OT Attacks to ATT&CK for ICS

The MITRE ATT&CK for ICS framework is specifically designed for attacks against industrial control systems. Here are some common OT attack techniques, mapped to this framework:

ATT&CK for ICS Tactic	ATT&CK for ICS Technique (Example)	OT Attack Example	Description
Initial Access	TA0001: External Remote Services	Gaining access through a VPN that is not properly secured.	Exploiting externally accessible systems for initial access to the OT network.
	TA0002: Supply Chain Compromise	Malicious software embedded within a contractor's system that is then implemented.	Introducing malicious software via a compromised vendor or service provider.
Execution	TA0006: Native API	Using native protocols to communicate with a PLC from a C2 server	Executing commands using built-in, non-malicious functionality.
	TA0007: Command and Scripting Interpreter	Using Modbus protocol to alter a valve setting on a PLC.	Issuing commands that directly affect physical processes by abusing industrial protocols.
Persistence	TA0009: Boot or Logon Autostart Execution	Modifying a PLC boot sequence for persistence.	Ensuring malicious code is executed at the device start up.
Privilege Escalation	TA0013: Exploitation of Privilege Escalation	Using a vulnerability to elevate privileges on an HMI.	Exploiting vulnerabilities to get higher levels of access.

Defense Evasion	TA0016: Indicator Removal	Clearing logs from an HMI or SCADA server to hide malicious activity.	Removing evidence of malicious activities on the system.
Credential Access	TA0015: OS Credential Dumping	Dumping credentials from an HMI database.	Obtaining valid credentials from control systems and workstations.
Discovery	TA0025: System Discovery	Using network scanning tools to discover devices on the OT network.	Gaining an overview of the systems and their location on the network.
	TA0026: Device Discovery	Using device specific discovery protocols to identify devices.	Discovering the devices and types on the OT network.
Lateral Movement	TA0027: Remote Services	Pivoting from an infected engineering workstation to a PLC.	Using remote services to move from compromised systems to other targets within the network.
Command and Control	TA0032: Application Layer Protocol	Using Modbus protocol for communication with the attacker	Using OT-specific protocols to communicate with the attacker-controlled infrastructure.
	TA0033: Ingress Tool Transfer	Transferring malicious code to the system through an encrypted channel.	Using secure protocols to bypass filtering and security systems.
Collection	TA0037: Data from Local System	Gathering configuration information from an HMI or a SCADA Server.	Obtaining important information from systems.
Impact	TA0040: Process Control Execution	Altering the values of parameters on a PLC causing a physical process to deviate.	Manipulating the parameters controlling the production, to change the final output.
	TA0043: Loss of Control	Causing a safety trip that shuts down a process.	Causing the shut down of important industrial processes.

How This Mapping Helps You

- **Understanding the Attack Lifecycle:** You can follow how an attacker progresses from initial access to impact in your own environment.
- **Identify Gaps:** By mapping your current defenses to the ATT&CK framework, you can see where your security controls are lacking.
- **Prioritize Mitigations:** You can focus on implementing mitigations for techniques that are most relevant to your organization.
- **Improve Detection:** Understanding attacker techniques improves your ability to detect and respond to attacks.
- **Shared Language:** The framework provides a common language for discussing threats across teams.
- **Threat Hunting:** It provides a framework for proactive detection and threat hunting activities.

Excellent! Now that you understand how to map IoT and OT attacks to the MITRE ATT&CK framework, let's discuss how to develop targeted mitigation strategies based on those mappings. This allows for a more focused and effective approach to security.

Using MITRE ATT&CK to Guide Mitigations

The key is to use the ATT&CK framework to identify the specific techniques that are relevant to your environment, and then implement mitigations that directly address those techniques. This is much more effective than a generalized approach.

Mitigation Strategies by ATT&CK Tactics

Here's a breakdown of mitigations, categorized by ATT&CK tactics, with examples focusing on both IoT and OT environments:

1. Initial Access

- **Tactic Goal:** Prevent attackers from gaining initial access to your systems.
- **Mitigation Examples:**

    T1190: Exploit Public-Facing Application:

        Mitigation: Regularly patch IoT and OT devices, use web application firewalls (WAFs), disable unused web interfaces, and implement strong authentication protocols on internet-facing applications.

    T1133: External Remote Services:

        Mitigation: Enforce strong passwords, use MFA for all remote access, restrict remote access to only necessary IP addresses, and monitor for brute-force attacks.

    T1078: Valid Accounts:

        Mitigation: Use MFA, enforce strong password policies, implement account lockout policies, and monitor for suspicious login activity.

    T1195: Supply Chain Compromise:

        Mitigation: Implement vendor risk management programs, use secure development practices, perform code reviews, conduct vulnerability assessments on components, and require verification of the firmware of new devices.

2. Execution

- **Tactic Goal:** Prevent attackers from executing code on your systems.
- **Mitigation Examples:**

T1059: Command and Scripting Interpreter:

Mitigation: Disable or restrict shell access, implement input validation, sanitize inputs, and use least privilege principles.

T1204: User Execution:

Mitigation: Implement email and web content filtering, perform user security awareness training, enforce strict browser security policies, and implement application whitelisting.

T1053: Scheduled Task/Job:

Mitigation: Monitor scheduled tasks for unexpected changes, restrict access to scheduled task creation, and implement code signing and device hardening.

3. Persistence

- **Tactic Goal:** Prevent attackers from maintaining persistent access to your systems.
- **Mitigation Examples:**

T1078: Valid Accounts:

Mitigation: Regular review of user accounts, enforcing least privilege, and monitoring for changes of privileges.

T1053: Scheduled Task/Job:

Mitigation: Monitoring and alerting on changes to scheduled tasks, restrict creation of scheduled tasks, and implement integrity controls of the execution files.

T1547: Boot or Logon Autostart Execution:

Mitigation: Use secure boot features, implement boot integrity verification, and monitor for unauthorized bootloader changes.

4. Privilege Escalation

- **Tactic Goal:** Prevent attackers from elevating their access privileges.
- **Mitigation Examples:**

T1068: Exploitation for Privilege Escalation:

Mitigation: Regularly patch systems, disable unused services, and implement least privilege.

T1078: Valid Accounts:

Mitigation: Implement RBAC, monitor for suspicious privilege escalations, and restrict administrative access.

5. Defense Evasion

- **Tactic Goal:** Make it difficult for attackers to evade security controls.
- **Mitigation Examples:**

T1070: Indicator Removal:

Mitigation: Secure and centralize logging, monitor for log deletion or modification, and use SIEM for log analysis and correlation.

T1027: Obfuscated Files or Information:

Mitigation: Use static and dynamic code analysis, implement endpoint detection and response (EDR) solutions, and monitor for anomalous behavior.

6. Credential Access

- **Tactic Goal:** Prevent attackers from obtaining valid credentials.
- **Mitigation Examples:**

T1081: Credentials in Files:

Mitigation: Avoid storing credentials in files, use secure credential management, and implement file integrity monitoring.

T1003: OS Credential Dumping:

Mitigation: Use credential protection mechanisms, implement strong access control, and monitor for unauthorized memory access.

7. Discovery

- **Tactic Goal:** Limit the attacker's ability to discover information about your environment.
- **Mitigation Examples:**

T1016: System Network Configuration Discovery:

Mitigation: Segment networks, restrict network scanning, and monitor for network reconnaissance activity.

T1082: System Information Discovery:

Mitigation: Restrict access to device and system information, and monitor for reconnaissance activities.

8. Lateral Movement

- **Tactic Goal:** Prevent attackers from moving laterally across your network.
- **Mitigation Examples:**

    T1021: Remote Services:

        Mitigation: Enforce least privilege, segment networks, use network access control lists, and monitor remote connections.

    T1210: Exploitation of Remote Services:

        Mitigation: Keep systems patched, use strong access controls and restrict remote access to only necessary IPs.

9. Collection

- **Tactic Goal:** Prevent attackers from collecting sensitive information.
- **Mitigation Examples:**

    T1005: Data from Local System:

        Mitigation: Encrypt data at rest, implement access controls, and monitor for unusual file access.

10. Command and Control

- **Tactic Goal:** Disrupt the attackers' communication channel.
- **Mitigation Examples:**

    T1071: Application Layer Protocol:

        Mitigation: Use network intrusion prevention systems, monitor for unauthorized protocols, and implement allow-lists for communications.

    T1001: Obfuscated C2 Channel:

        Mitigation: Use deep packet inspection, monitor for unusual traffic patterns, and implement traffic analysis.

11. Exfiltration

- **Tactic Goal:** Prevent the attacker from exfiltrating data.
- **Mitigation Examples:**

    T1041: Exfiltration Over C2 Channel:

Mitigation: Use DLP solutions, monitor network traffic for unauthorized data transfer, and implement egress filtering.

12. Impact

Tactic Goal: Reduce the impact of attacks.

Mitigation Examples:

T1499: Endpoint Denial of Service:

Mitigation: Implement rate limiting, use traffic shaping mechanisms and implement robust backup and recovery procedures.

T1498: Data Destruction:

Mitigation: Use backups, regularly perform integrity checks of data and limit access to data destruction functionalities.

Applying These Mitigations

- **Prioritize:** Not all techniques are equally likely or impactful. Focus on the ones that are most relevant to your environment.
- **Layered Approach:** Implement multiple mitigations for each technique for a defense-in-depth approach.
- **Regularly Test:** Validate the effectiveness of mitigations through regular testing and red teaming exercises.
- **Adapt:** The threat landscape is constantly evolving, so you must regularly review and adjust your security controls.
- **Document:** Ensure that you document all your mitigations and keep the information updated.

Your Role as a Level 1 SOC Analyst:

While you will not might not be implementing these mitigations yourself, you play a crucial role in:

- **Recognizing** how they work.
- **Monitoring** the effectiveness of these mitigations.
- **Raising Alerts** when a mitigation may be failing.
- **Supporting** incident response and post-incident analysis.

By using the MITRE ATT&CK framework as a roadmap, you can implement more targeted and effective mitigation strategies for IoT and OT environments.

As a cybersecurity analyst monitoring IoT and OT environments, you need a keen eye for specific anomalies and patterns that could indicate malicious activity. Here is a breakdown of what you should be on the lookout for, categorized for clarity:

1. Network Traffic Anomalies:

- **Unusual Source/Destination IPs:**

  What to look for: IoT/OT devices communicating with unexpected external IPs, especially those associated with known malicious actors.

  Why: Could indicate command-and-control (C2) communication or data exfiltration.

Unexpected Protocols:

What to look for: IoT devices using protocols outside their normal operations (e.g., an IP camera communicating via Modbus). OT devices talking via HTTP when the communication should be through a control protocol.

Why: Could indicate an attacker attempting to establish a backdoor channel or use a known protocol vulnerability.

Abnormal Traffic Volume:

What to look for: Sudden spikes or decreases in traffic from/to IoT/OT devices, especially if the volume is outside expected baselines.

Why: Could indicate a denial-of-service (DoS) attack or exfiltration of large amounts of data.

Unusual Ports:

What to look for: Devices communicating over unexpected ports, especially those associated with remote access or malicious activity.

Why: Could indicate unauthorized access attempts, backdoors, or data transfer.

Protocol Violations:

What to look for: Malformed or unusual protocol messages (e.g., Modbus requests with invalid function codes).

Why: Could indicate attempts to exploit vulnerabilities in the protocol itself.

Broadcast/Multicast Anomalies:

What to look for: Unexpected increases in broadcast or multicast traffic from IoT/OT devices, particularly if they are not typically using them.

Why: Could indicate reconnaissance activity or DoS attacks.

Egress Traffic with High Bandwidth:

What to look for: High outbound bandwidth that is sustained over a period of time from an unexpected IP or device

Why: Could be exfiltration of data?

2. Device and System Anomalies:

Unusual Logins/Account Activity:

What to look for: Failed login attempts, access from unfamiliar locations, and new accounts created, especially on critical OT systems.

Why: Could indicate brute-force attacks, compromised credentials, or unauthorized access.

Configuration Changes:

What to look for: Unexpected modifications to device settings, firewall rules, or user permissions, particularly on critical devices.

Why: Could indicate an attacker attempting to bypass security measures or gain persistent access.

Firmware Changes:

What to look for: Unexpected firmware updates or changes in device firmware versions.

Why: Could indicate malicious firmware being installed or an attempt to downgrade the firmware to a vulnerable version.

Process Anomalies:

What to look for: Unexpected processes running on IoT/OT devices.

Why: Could indicate malware running on the device.

Resource Utilization:

What to look for: Spikes in CPU or memory usage, especially when there's no legitimate reason for it.

Why: Could indicate a DoS attack, crypto mining, or malware running on the device.

Unexpected Reboots/Crashes:

What to look for: IoT/OT devices unexpectedly rebooting or crashing.

Why: Could indicate a DoS attack, malware infection, or a compromised system.

Clock Changes:

What to look for: Unexpected changes in the device or system clock.

Why: Could be an attempt to avoid time-based security mechanisms or obscure forensic analysis?

Hardcoded Credentials:

What to look for: Credentials hardcoded in the device or application firmware.

Why: Provides an easy entry point for attackers.

Unsigned Code/Applications:

What to look for: If the company has an application or executable whitelisting, process, unsigned code or applications are always a red flag.

Why: Could indicate an unauthorized malicious application being executed.

3. OT-Specific Anomalies:

- **PLC Logic Changes:**

What to look for: Changes to PLC program logic or configuration without proper authorization.

Why: Could indicate an attacker attempting to manipulate a physical process.

HMI Modifications:

What to look for: Changes to HMI screens, graphics, or displayed values without proper authorization.

Why: Could indicate an attacker trying to mislead operators or manipulate the process.

Alarm Suppression:

What to look for: Suppression of alarms or warnings.

Why: Could indicate an attacker attempting to hide malicious activity or process manipulation.

Process Variable Changes:

What to look for: Unexpected or unauthorized changes to process variables (e.g., valve positions, temperature settings) outside of normal operating ranges.

Why: Could indicate an attacker attempting to disrupt or damage the process.

Data Historian Anomalies:

What to look for: Unusual gaps in data logs or modifications to data history.

Why: Could indicate an attacker attempting to hide evidence of malicious activity.

4. Security Tool Alerts:

IDS/IPS Alerts:

What to look for: Alerts triggered by intrusion detection/prevention systems, particularly for OT protocols.

Why: Could indicate an ongoing attack or reconnaissance activity.

SIEM Alerts:

What to look for: Alerts generated by a SIEM platform, focusing on IoT/OT specific alerts.

Why: Indicates suspicious activity detected by the security-monitoring platform.

Endpoint Detection and Response (EDR) Alerts:

What to look for: Alerts generated by EDR products, particularly on IoT devices or workstations with access to OT systems.

Why: Indicates malicious software running on the endpoint.

5. User Behavior Anomalies:

Access outside Normal Hours:

What to look for: Users accessing IoT/OT systems or data outside of their normal work hours.

Why: Could indicate compromised user accounts or malicious activity.

Unusual Access Patterns:

What to look for: Users accessing systems or data that they do not normally access.

Why: Could indicate privilege escalation or a compromised user account.

Multiple Failed Accesses:

What to look for: Many failed attempts to access system resources with one or more user accounts.

Why: Could indicate a brute force attack or a compromised user account.

6. Supply Chain Anomalies:

Device from Unknown Vendor:

What to look for: Devices from unknown vendors installed or connected to the network.

Why: Could indicate a supply chain compromise or shadow IT practices.

Firmware Outdated on New Devices:

What to look for: Newly installed devices that are not running the latest version of their respective firmware.

Why: Could indicate pre-compromised devices.

How to Effectively Monitor:

- **Establish Baselines:** Understand normal network traffic, device behavior, and user activity.
- **Centralized Monitoring:** Collect logs and alerts from all relevant systems in a central location (e.g., SIEM).
- **Alerting Rules:** Create specific alerting rules for IoT/OT environments, focusing on known attack patterns.
- **Stay Informed:** Keep up-to-date on the latest IoT/OT threats and vulnerabilities.
- **Continuous Improvement:** Continuously refine your monitoring and detection capabilities based on new threats and lessons learned.

Key for a Level 1 SOC Analyst

As a Level 1 SOC Analyst, you are not expected to be an expert in all these areas. However, you must be aware of these potential indicators of compromise and learn how to recognize them. Your primary role is to:

- **Identify** the anomalies and suspicious patterns.
- **Triage** the events according to established processes.
- **Escalate** potentially serious incidents to senior analysts.

Keep a vigilant eye on these indicators; you will play a vital role in protecting your organization's IoT and OT environments.


CYBERCLAW
LEARN
TEACH