MICAD LIMITED
Advanced Industrial Security Supervisor Training

Lesson 2.5: Activity - Developing a Comprehensive Security Plan

Security Plan: Hypothetical Solar Power Substation

1. Executive Summary:

This security plan outlines the strategies and procedures for protecting the hypothetical "SunPeak" solar power substation from various threats and vulnerabilities. The plan integrates findings from a recent risk assessment, prioritizing the protection of critical infrastructure, sensitive data, and personnel. Key objectives include preventing unauthorized access, mitigating cyber threats, ensuring business continuity, and maintaining compliance with relevant regulations.

2. Introduction:

SunPeak solar power substation is a critical infrastructure asset responsible for generating and distributing renewable energy. This security plan aims to establish a robust security posture, minimizing risks and ensuring the reliable operation of the substation.

3. Risk Assessment Summary:

A comprehensive risk assessment identified the following high-priority risks:

Cyberattacks: Targeting the SCADA system and potentially disrupting operations or causing damage to equipment.
Physical Intrusion: Unauthorized access to the substation, leading to theft, vandalism, or sabotage.
Natural Disasters: Extreme weather events (e.g., floods, wildfires) could damage equipment and disrupt operations.
Insider Threats: Malicious or negligent actions by employees could compromise security.

4. Security Goals and Objectives:

Prevent unauthorized physical access: Maintain 24/7 perimeter security with zero unauthorized intrusions.

Prevent cyberattacks: Maintain the integrity and availability of the SCADA system with zero successful cyberattacks.
Ensure business continuity: Minimize downtime during emergencies and natural disasters.
Maintain regulatory compliance: Comply with all relevant federal, state, and local regulations related to critical infrastructure protection.

5. Security Policies and Procedures:

Access Control: Strict access control measures will be implemented, including physical barriers, security cameras, and biometric authentication. Access logs will be regularly reviewed.
Incident Response: A comprehensive incident response plan will be developed and regularly tested, including procedures for reporting, investigation, and recovery.
Data Security: Sensitive data will be encrypted, and access will be restricted to authorized personnel only. Regular data backups will be performed.
Cybersecurity: Regular vulnerability scans and penetration testing will be conducted on the SCADA system. Network segmentation and firewalls will be implemented to protect the SCADA network from external threats. Intrusion detection systems (IDS) and intrusion prevention systems (IPS) will be deployed.

Personnel Security: Background checks will be conducted on all personnel with access to the substation. Security awareness training will be provided to all employees.

6. Security Measures:

Perimeter Security: Fencing, security cameras, motion detectors, and lighting.
Access Control: Biometric access control system at all entry points. Keycard access for authorized personnel.
Surveillance: 24/7 CCTV monitoring with video analytics capabilities.
Intrusion Detection: Intrusion detection system integrated with the alarm system.
Cybersecurity: Firewall, intrusion detection/prevention system, regular vulnerability assessments, intrusion detection/prevention systems.
Data Backup and Recovery: Regular data backups stored offsite. Disaster recovery plan in place.
Emergency Response: Emergency response plan including procedures for fire, natural disasters, and security breaches.

7. Responsibilities and Accountabilities:

Security Manager: Overall responsibility for the security program.
Security Supervisor: Oversees daily security operations.
IT Security Specialist: Manages cybersecurity systems.
Maintenance Personnel: Responsible for the physical security of equipment.

8. Training and Awareness Programs:

* Annual security awareness training for all personnel.
* Specialized training for security personnel and IT staff.

9. Budget and Resource Allocation:

[Insert a detailed budget outlining resources needed for personnel, equipment, software, maintenance, and training.]

10. Testing and Evaluation:

* Regular penetration testing of SCADA systems.
* Periodic security audits.
* Simulated emergency response drills.

11. Incident Response Plan:

[Include a detailed incident response plan addressing various types of incidents.]

12. Review and Update Schedule:

The security plan will be reviewed and updated at least annually or more frequently as needed, based on risk assessments, security incidents, and changes in the threat landscape.

This is a sample security plan. It needs customization based on a thorough risk assessment specific to the SunPeak substation and its environment. Legal and regulatory compliance should be carefully considered throughout the development and implementation of this plan. The plan should also be regularly tested and updated to ensure its continued effectiveness.