- Filename: eccouncil-ceh31250-v10-1-3-3-intro_to_ethical_hacking_security_controls_pt3.md
- Show Name: CEHv10 (312-50)
- Topic Name: Introduction
- Episode Name: Intro to Ethical Hacking: Security Controls Pt.3
- Description: In this episode, Daniel and Zach continue their discussion of Security Policies by discussing Physical Security. This includes physical threats and physical controls that could be implemented to mitigate those threats. They then move on to exploring Risk Management and Threat Modeling.

==========

Intro to Ethical Hacking: Security Controls Pt.3

- Physical Security
    - Physical Security Threats
        - Environmental
        - Man-made
    - Physical Security Control Types (DIAGRAM)
        - Preventive
            - Gates, Doors, Locks, Mantrap, Guards
        - Detective
            - Sensors
                - Heat, motion, alarms
            - Video, CCTV
        - Deterrent
            - Warning Signs
        - Recovery
            - BCDR plans
            - Backups
        - Compensating
            - Redundant systems
                - Power
                - Hot-spares
            - Hot-site backup
    - Look for ways you can implement Physical Security Controls
- Risk Management
    - What is Risk?
        - The adverse unknown
        - The probability that unwanted event can and will occur
            - Risk Matrix (DIAGRAM)
    - Risk Management Phases (DIAGRAM)
        - Identification
            - Internal and External
        - Assessment
        - Treatment

        - Implement proper controls to mitigate
    - Tracking
        - Makes sure controls are being implemented
        - Makes sure controls aren't creating any new risks
    - Review
        - Checks the effectiveness of the implemented controls
- Threat Modeling
    - https://www.owasp.org/index.php/Category:Threat_Modeling
    - Process (DIAGRAM)
        - Identify Objectives
            - What are you trying to achieve
            - How much time and effort will it take to achieve
        - Application Overview
            - Laying out all aspects of a system
                - Elements/Components
                - Data/Data flows
                - Security mechanisms
                - Trust boundaries
        - Decompose Application
            - Deep dive into the system
            - Can uncover more threats
        - Identify Threats
        - Identify Vulnerabilities