- Filename: eccouncil-ceh31250-v10-1-3-4-intro_to_ethical_hacking_security_controls_pt4.md
- Show Name: CEHv10 (312-50)
- Topic Name: Introduction
- Episode Name: Intro to Ethical Hacking: Security Controls Pt.4
- Description: In this episode, Daniel and Zach continue their discussion about Security controls and policies. Here they walk you through developing Incident Management and Response procedures as well as introducing you to Security Incident and Event Monitoring (SIEM) systems and User Behavior Analytics (UBA).

==========

Intro to Ethical Hacking: Security Controls Pt.4

- Incident Management and Response
    - Process (DIAGRAM)
        - Preparation
        - Detection and Analysis
        - Classification and Prioritization
        - Notification
        - Containment
        - Forensic Investigation
        - Eradication and Recovery
        - Post-incident Activities
    - IR Team Duties/Responsibilities
        - Proactively assessing and mitigating client's security
        - Quick response to incidents
        - Creating/reviewing/updating the IR procedures/processes
            - Also checking
                - Legalities
                - Regulatory requirements
        - Following procedure/process correctly
            - Minimize the damage
        - Analyze incidents
            - Correctly assess what occurred
            - Assess the impact
            - Uncover the threat
        - Single point of contact to report incidents
        - Recommend mitigations and/or new controls or changes to existing
        - Build relationships
            - LEOs
            - Gov agencies
            - Other orgs/vendors that could make beneficial partnerships
    - Security Incident and Event Management(SIEM)
        - Software used
            - Collect info about security events
            - Report security events
            - Works in real-time
        - Functions
            - Log aggregation, monitoring, and analysis
            - Reporting
            - File/Object access auditing
            - Supervisor Dashboard
            - File Integrity monitoring

        - Alerting
- User Behavior Analytics (UBA)
    - Advanced threat detection
    - Tracks user behavior
        - Identifies behavior patterns
            - Monitors When/Where logins occur
            - Monitors administrative account access
            - Alerts to deviant behavior patterns which may be malicious