- Filename: eccouncil-ceh31250-v12-5-2-1-vulnerability-management-life-cycle.md
- Show Name: CEHv12 (312-50)
- Topic Name: System Hacking Phases and Attack Techniques - Vulnerability Analysis
- Episode Name: Vulnerability Management Lifecycle
  ================================================================================

## Vulnerability Management Lifecycle

## Objectives:

- Define the Vulnerability Management Life-Cycle process
- List the VMLC phases in order
- Explain the purpose of each phase of the VMLC

---

- EC-Council talks about this Vulnerability Management Lifecycle (see link).
  Can you walk us through this and give us a little more insight?
    - https://egs.eccouncil.org/wp-content/uploads/2020/12/Risk-and-Vulnerability-Assessment-Do-You-Know-the-Other-Side.pdf
        - Pre-Assessment Phase
            - Identify Assets / Create Baseline
                - Understanding the business and its processes
                - Assets
                    - Ranking / Categorization
                    - Configurations
                - Security Controls
                - Standards
                - Policies
                - Scope
        - Vulnerability Assessment Phase
            - Vulnerability Assessment Scan (what you do in this phase)
                - Physical Security
                - Security Misconfigurations
                - Run the vuln scan software
                    - Selecting the correct scan type
                - Identify vulnerabilities
                    - False positives & False Negatives
                - Validate vulnerabilities
                - Generate a report
        - Post Assessment Phase
            - Risk Assessment
                - Categorize Risks
                - Determine Risk Likelihood and Impact
                - Determine threat level
            - Remediation
                - Recommend and prioritize mitigations
                - Root Cause Analysis
                - Implement fixes/patches/controls
                - Perform training
                - Lessons learned
            - Verification
                - Rescan
            - Monitoring

- Logging
- SIEM
- IDS/IPS