- Filename: eccouncil-ceh31250-v11-1-8-1-threat-hunting.md
- Show Name: CEHv11 (312-50)
- Topic Name: Intro to Ethical Hacking
- Episode Name: Threat Hunting

==========

Threat Hunting

Objectives:

- Discover data breaches through the careful examination of computer systems
- Define categories of Indicators of Compromise(IoCs)
- List common IoCs

- What is threat hunting?
    - Assuming a breach has already occurred
    - 200 days before breaches are discovered
- How do we perform threat hunting?
    - Hypothesize the most likely attack
    - Look for suspicious/malicious/risky activity based on that hypothesis
    - Threat hunting can generate Indicators of Compromise (IoC) and alerts
- Can you explain the concept of an IoC?
    - Evidence on a device that points to a security breach
    - Usually gathered AFTER a suspicious incident or security event
    - IoC data can be
        - Atomic
            - Self-contained data
                - IP address
                - Email address
        - Computed
            - Derived data
                - Hash values
                - Reg ex
        - Behavioral
            - Logically combining Atomic and Computed
- What are the IoC categories?
    - Email
        - Comprised of email artifacts
            - Sender's email address
            - Subject line
            - Attachments
            - Links
    - Network
        - Artifacts

        - Domain info
        - IP address
    - Host-Based
        - Artifacts
            - File names
            - Hash values
            - Registry entries
            - Drivers
    - Behavioral
        - Artifacts
            - Macros running PowerShell
            - Service accounts running commands like a user would
- Can you give us a few concrete examples of IoC?
    - Anomalies found in Privileged User Activity
    - Red flags found in log-in activity
    - Deviant DNS requests
    - Web traffic with inhuman behavior
    - Unusual activity in outbound network traffic
    - Geographical abnormalities
    - Increased database read volume
    - Unusual HTML response sizes
    - Changes in mobile device profiles
    - Signs of DDoS activity
    - Wrongly placed data bundles
    - Conflicting port-application traffic
    - More requests than usual for the same file
    - Unusual changes in registry and/or system files
    - Abrupt patching of systems