- Filename: eccouncil-ceh31250-v11-9-2-1-insider-threats.md
- Show Name: CEHv11 (312-50)
- Topic Name: Network and Perimeter Hacking: Social Engineering
- Episode Name: Insider Threats
  ==========

Insider Threats

Objectives:

- Define Insider Threat
- List the types of Insider Threats
- Explain the dangers of Insider Threats
- Describe the goals and motivations behind Insider Threats
- Uncover the presence of an Insider Threat based on behavioral indicators

---

- Let's dive into the concept of the Insider Threat.
    - Insider = employee or trusted person
    - Threat = potential for negative
        - Insiders can cause damage for long periods of time with detection
            - Due to their inherent trust
        - Easy to pull off
        - Difficult to prevent
        - Attribution can be difficult
- What types of Insider Threats
    - Malicious insider (Disgruntled/Terminated Employees)
    - Negligent/Accidental Threat
    - Professional Insider
    - Compromised Insider (blackmail)
- Why would someone do this?
    - Money
    - Revenge
    - Competitive advantage
    - Hacktivism
    - Coercion
- Insider Threat Indicators
    - Discovery of data exfil
        - Covert channel
            - IM/Chat
            - FTP
            - Online storage
        - Email
    - Multiple logins from different devices
    - Attempting to access or has accessed restricted areas
    - Strange working hours
    - Behavioral abnormalities
    - Odd or suspicious network activity
    - Possession of sensitive data