filename:comptia-secplussy0601-9-11-1-attack-frameworks
Showname: Security+ (SY0-601)
Topic: Operational Security and Incident Response
Episode: Incident Response Plans

Summarize the importance of policies, processes, and procedures for incident response.

Description: In this episode, the viewer will identify key component of attack frameworks used to identify adversaries, tactics and techniques used by threat actors against victims used by cybersecurity analysts such as MITRE ATT&CK and the Diamond Model of Intrusion Analysis. The viewer will also identify the cyber kill chain that represents the steps an attacker uses to exploit a victim.

- Attack frameworks
- Attack frameworks - MITRE ATT&CK
- Attack frameworks - The Diamond Model of Intrusion Analysis
- Attack frameworks - The Diamond Model of Intrusion Analysis
    - Meta-features
    - Confidence value
- Cyber Kill Chain