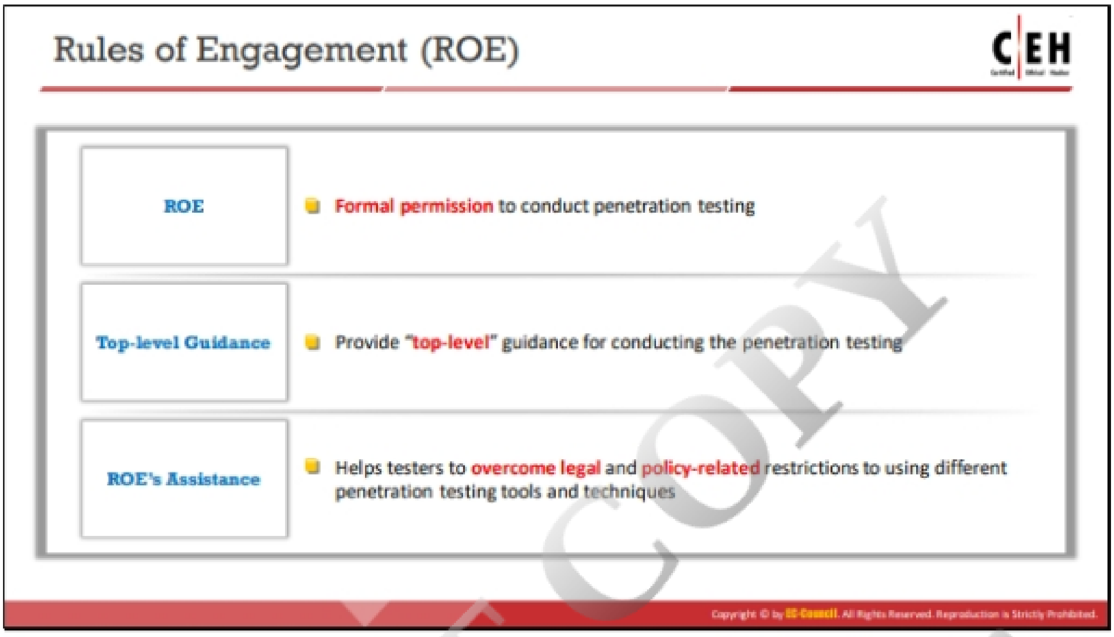
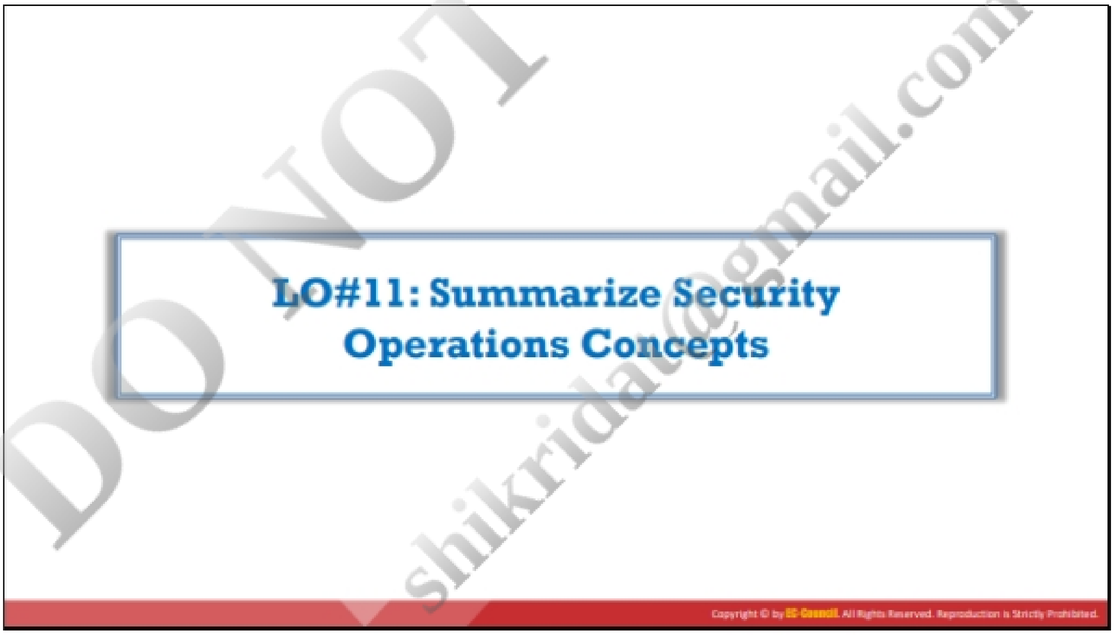


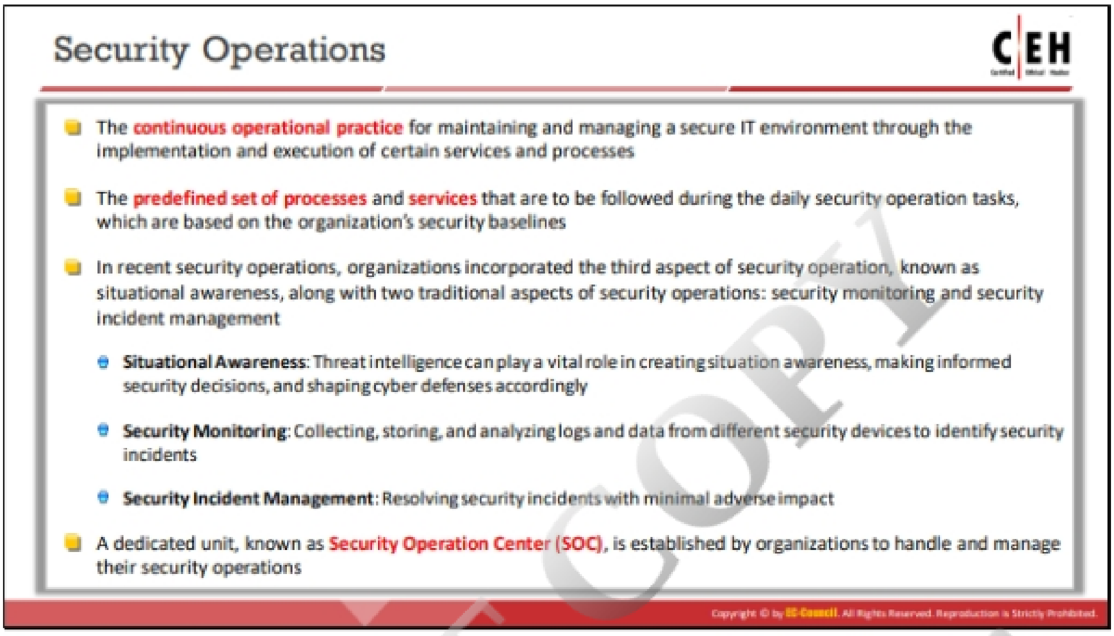
Rules of Engagement (ROE)

ROE	Formal permission to conduct penetration testing
Top-level Guidance	Provide "top-level" guidance for conducting the penetration testing
ROE's Assistance	Helps testers to overcome legal and policy-related restrictions to using different penetration testing tools and techniques



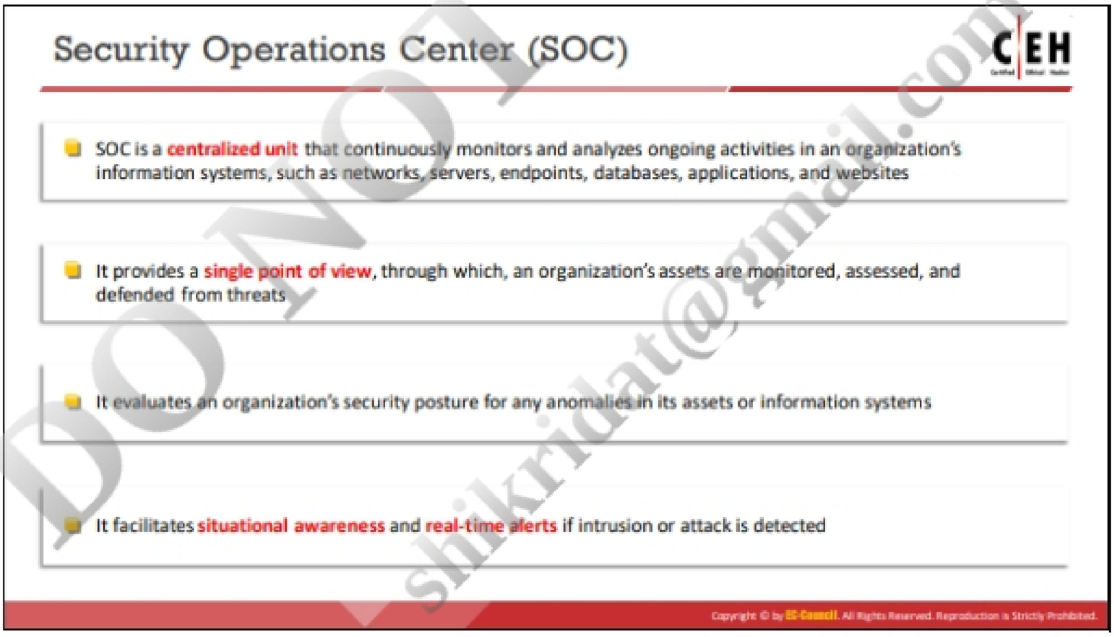
LO#11: Summarize Security Operations Concepts

Notes:



Security Operations

- The continuous operational practice for maintaining and managing a secure IT environment through the implementation and execution of certain services and processes
- The predefined set of processes and services that are to be followed during the daily security operation tasks, which are based on the organization's security baselines
- In recent security operations, organizations incorporated the third aspect of security operation, known as situational awareness, along with two traditional aspects of security operations: security monitoring and security incident management
  - **Situational Awareness**: Threat intelligence can play a vital role in creating situation awareness, making informed security decisions, and shaping cyber defenses accordingly
  - **Security Monitoring**: Collecting, storing, and analyzing logs and data from different security devices to identify security incidents
  - **Security Incident Management**: Resolving security incidents with minimal adverse impact
- A dedicated unit, known as Security Operation Center (SOC), is established by organizations to handle and manage their security operations



Security Operations Center (SOC)

- SOC is a centralized unit that continuously monitors and analyzes ongoing activities in an organization's information systems, such as networks, servers, endpoints, databases, applications, and websites
- It provides a single point of view, through which, an organization's assets are monitored, assessed, and defended from threats
- It evaluates an organization's security posture for any anomalies in its assets or information systems
- It facilitates situational awareness and real-time alerts if intrusion or attack is detected

Notes: