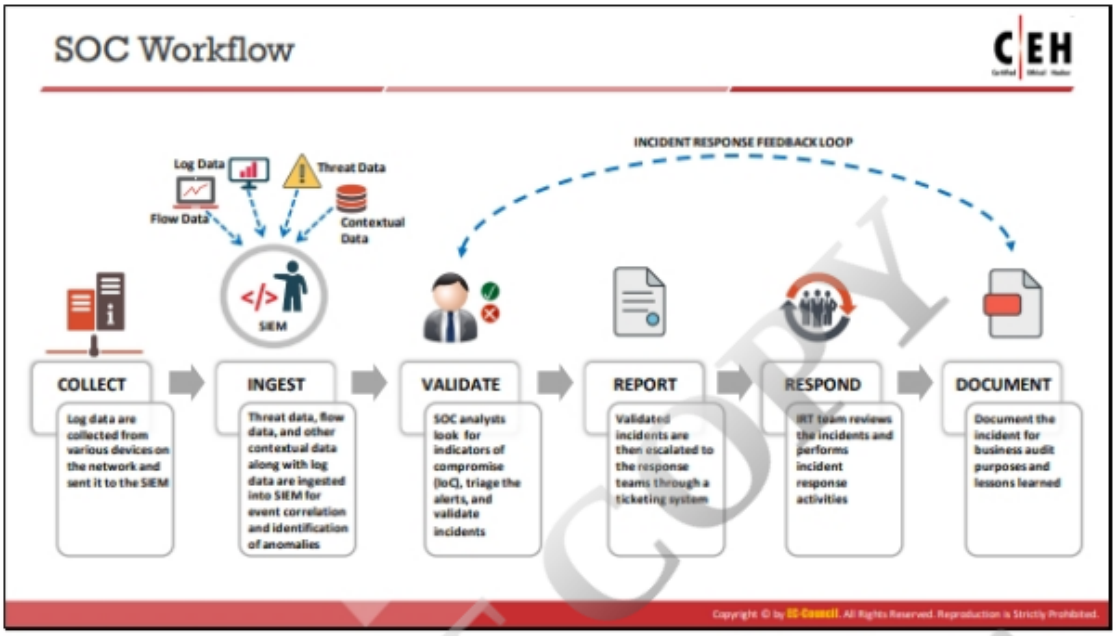

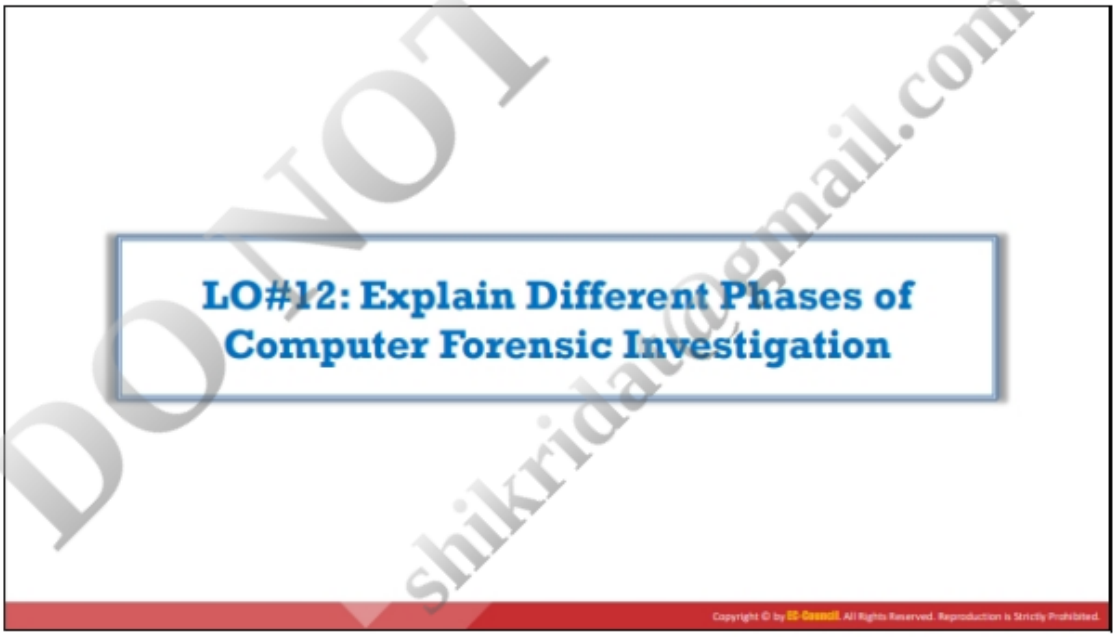

Notes:

Computer Forensics

Computer Forensics refer to a **set of methodological procedures and techniques** that help identify, gather, preserve, extract, interpret, document, and present evidence from computing equipment, whereby any evidence discovered is acceptable during a legal or administrative proceeding

Objectives of Computer Forensics:

1. To track and prosecute cyber crime perpetrators
2. To gather evidence of cyber crimes in a forensically sound manner
3. To estimate the potential impact of a malicious activity on the victim and assess the intent of the perpetrator
4. To find vulnerabilities and security loopholes that help attackers
5. To recover deleted files, hidden files, and temporary data that could be used as evidence

Phases Involved in the Computer Forensics Investigation Process

Pre-investigation Phase	Deals with tasks to be performed prior to commencing the **actual investigation** Involves setting up a **computer forensics lab**, building a forensics workstation, developing an investigation toolkit, setting up an investigation team, gaining approval from the relevant authority, and so on
Investigation Phase	The **main phase** of the computer forensics investigation process Involves the acquisition, preservation, and analysis of **evidentiary data** to identify the **source of the crime** and the culprit behind it
Post-investigation Phase	Deals with the **documentation** of all the actions undertaken and findings uncovered during an investigation Ensures that the **report** is well explicable to the target audience, and provides **adequate** and **acceptable** evidence

Notes: