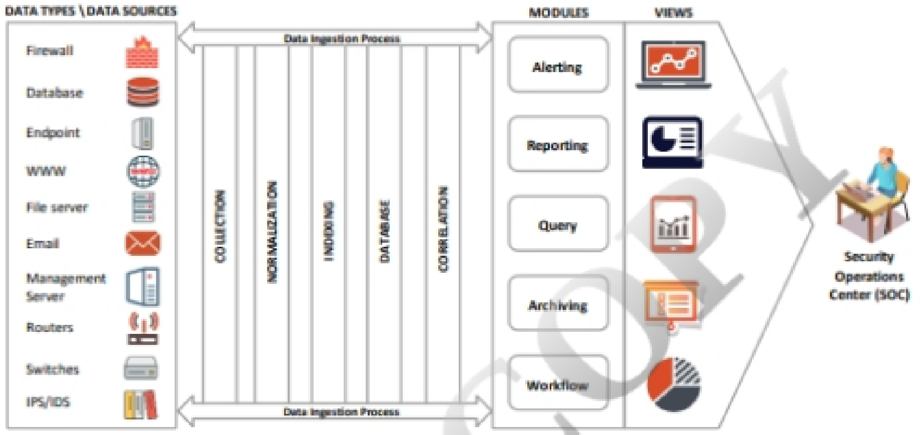
Printed by: shikridat@gmail.com. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.

Security Operations Center (SOC) (Cont'd)



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

SOC Operations

Log Collection

- Logs are collected from the various devices on a network that can have an impact on the security of the organization

Log Retention and Archival

- Collected logs are recovered and stored centrally
- They can be used to perform forensics as well as threat control and prevention

Log Analysis

- Logs are analyzed through SOCs technology to extract important information such as relevant metrics, from the raw data

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

DO NOT COPY shikridat@gmail.com

Notes: ____

____

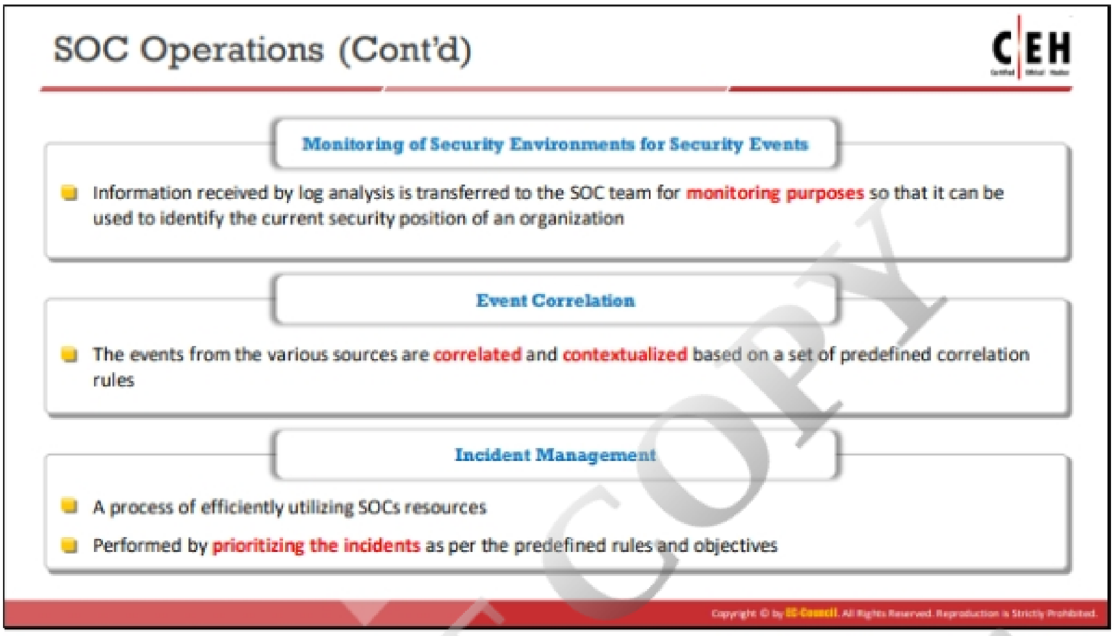
____

____

____

____

Printed by: shikridat@gmail.com. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.



SOC Operations (Cont'd)

Monitoring of Security Environments for Security Events

- Information received by log analysis is transferred to the SOC team for monitoring purposes so that it can be used to identify the current security position of an organization

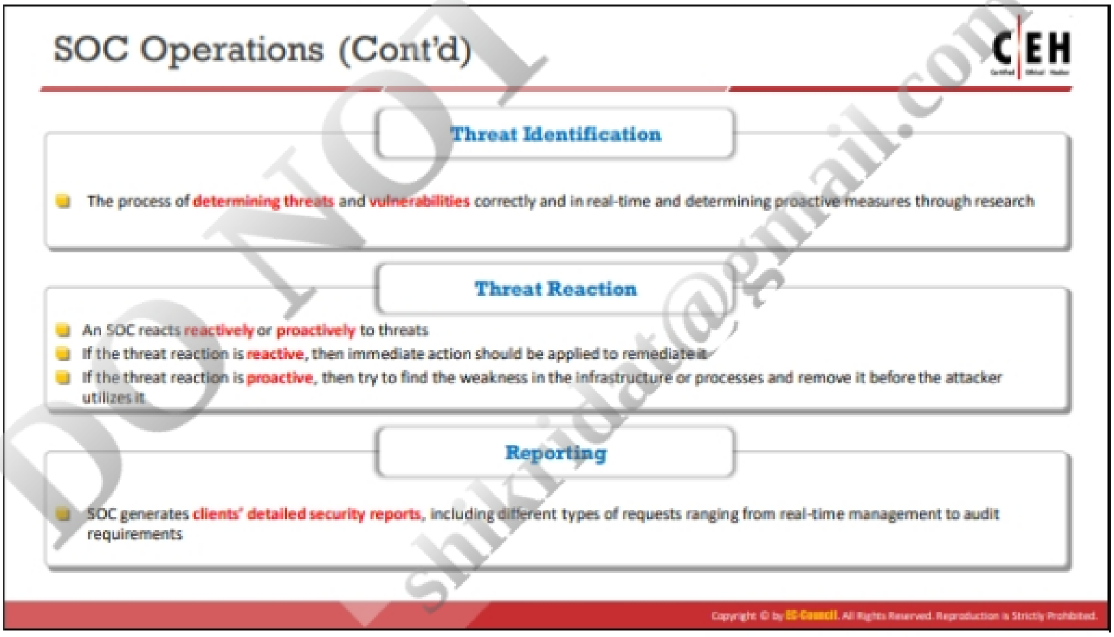
Event Correlation

- The events from the various sources are correlated and contextualized based on a set of predefined correlation rules

Incident Management

- A process of efficiently utilizing SOCs resources
- Performed by prioritizing the incidents as per the predefined rules and objectives

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



SOC Operations (Cont'd)

Threat Identification

- The process of determining threats and vulnerabilities correctly and in real-time and determining proactive measures through research

Threat Reaction

- An SOC reacts reactively or proactively to threats
- If the threat reaction is reactive, then immediate action should be applied to remediate it
- If the threat reaction is proactive, then try to find the weakness in the infrastructure or processes and remove it before the attacker utilizes it

Reporting

- SOC generates clients' detailed security reports, including different types of requests ranging from real-time management to audit requirements

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

DO NOT COPY
shkridat@gmail.com

Notes: ____

____

____

____

____

____