Section Introduction, Lessons Learned and Reporting

This section of the Incident Response domain focuses on reflecting on the incident once recovery has concluded. This is to determine what went well and what could be improved, with the overall objective of developing security controls to prevent similar incidents, and reviewing the response process to identify any potential weaknesses and enhance response in the future.

LEARNING OBJECTIVES

By the end of this section you will have achieved the following objectives:

- How to review on what went well during the incident, and what could be improved upon if a similar event occurred in the future.
- Understand ways that security teams can improve their response to security incidents.
- Understand the importance of documentation, updating the incident response plan, and updating or creating new run-books.
- Understand why metrics are collected and used to identify strengths and weakness to aid incident response development.