****

**­­­­­**

|  |
| --- |
| **CAPSTONE PROJECT**  Note:  Front page will be amended to include pictured title with both SIM and IBM logos. |
|  |

**Facilitator’s Guide**

**DOCUMENT VERSION CONTROL RECORD**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version Number** | **Effective Date of Release** | **Summary of Included Changes** | **Author** |
| 1.0 | TBA | First Edition | IBM/SIM |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

© 2025. Singapore Institute of Management Group Ltd. All rights reserved.

This Facilitator’s Guide is the exclusive property of Singapore Institute of Management and IBM Singapore Pte Ltd. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of Singapore Institute of Management, except in the case of brief quotations embodied in critical reviews and certain other non-commercial uses permitted by law.

Any unauthorised use of this material may violate copyright laws and result in legal action. For permission requests, please contact Singapore Institute of Management at simacademy@sim.edu.sg.

**Table of Contents**

[1. Course Overview - 4 -](#_Toc205320851)

[2. Learning Outcomes - 5 -](#_Toc205320852)

[3. Structure and Duration of Training & Assessment - 6 -](#_Toc205320853)

[Summary of Assessment Requirement: - 7 -](#_Toc205320854)

[4. Lesson Plan - 8 -](#_Toc205320855)

[Session One (3 hours, Virtual) - 8 -](#_Toc205320856)

[Session Two (3 hours, Virtual) - 11 -](#_Toc205320857)

[Session Three (3 hours, Virtual) - 13 -](#_Toc205320858)

[Session Four (3 hours, Virtual) - 16 -](#_Toc205320859)

[Session Five (3 hours, Virtual) - 18 -](#_Toc205320860)

[Session Six (3 hours, Virtual) - 20 -](#_Toc205320861)

[Session Seven (3 hours, Virtual) - 22 -](#_Toc205320862)

[Session Eight (3 hours, Virtual) - 24 -](#_Toc205320863)

[Session Nine (7 hours, Virtual) - 27 -](#_Toc205320864)

[Session Ten (3 hours, Virtual) - 31 -](#_Toc205320865)

[Session Eleven (3 hours, Virtual) - 33 -](#_Toc205320866)

[Session Twelve (3 hours, Classroom) - 35 -](#_Toc205320867)

[5. Annexes - 36 -](#_Toc205320868)

Report 2 – Cybersecurity Project Documentation  
Learning Outcomes: LO3 to LO7  
Module: [Module Name]  
Learner Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Learner ID: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Section 1 – LO3: Incident Analysis & Timeline Correlation

1.1 Task 1 – Initial Triage  
Objective: Identify initial indicators of compromise from process and network capture logs.

Target Logs: traffic.pcap.log, pstree.log

Steps Taken:  
[Describe the log analysis process, tools used, and key observations]

Findings:

* Suspicious Domain Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* Resolved IP Address: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* Anomalous Process Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* Process ID (PID): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* Parent Process Name/PID: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Evidence:

* Screenshot or excerpt from traffic.pcap.log showing suspicious DNS query.
* Screenshot or excerpt from pstree.log showing anomalous process and PID.

1.2 Task 2 – Evidence Correlation & Timeline Creation  
Objective: Link findings from initial triage to establish a full incident timeline.

Steps Taken:  
[Describe how netscan.log was analysed and cross-referenced with triage findings]

Correlated Evidence:

* Destination IP in netscan.log matches DNS resolved IP from traffic.pcap.log.
* Network activity confirmed for suspicious PID.

Incident Timeline:  
[List events in chronological order with timestamps]

Supporting Evidence:

* Log excerpts or screenshots for each event.

Observations:  
[Summarise the significance of the correlation and timeline]

Section 2 – LO4: Malware Analysis

2.1 Task – Static Analysis of Malware Sample  
Objective: Examine suspicious executable without executing it to identify characteristics and potential behaviours.

Steps Taken:  
[List tools used – e.g., strings, file, hash calculation]

Findings:

* File Type: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* Hash Values (MD5/SHA1/SHA256): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* Embedded Strings of Interest: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* Suspicious Imports / API Calls: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Evidence:  
[Attach excerpts, screenshots of analysis tool outputs]

2.2 Task – Dynamic Analysis in Isolated Environment  
Objective: Execute sample in a sandbox or VM to observe runtime behaviour.

Steps Taken:  
[List setup, monitoring tools used – e.g., Procmon, Wireshark]

Findings:

* Processes Spawned: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* Files Created/Modified: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* Registry Changes (if applicable): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* Network Connections Attempted: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Evidence:  
[Attach screenshots, sandbox reports]

Observations:  
[Discuss how findings match known malware behaviours]

Section 3 – LO5: Threat Intelligence Integration

3.1 Task – IOC Enrichment  
Objective: Use threat intelligence sources to enrich identified Indicators of Compromise (IOCs).

Steps Taken:  
[List online sources, TI platforms, or databases used]

Findings:

* Domain/IP Reputation: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* Malware Family (if identified): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* Associated Campaigns / Actors: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Evidence:  
[Screenshots or links to TI report references]

3.2 Task – Reporting & Intelligence Sharing  
Objective: Prepare a threat intelligence summary for dissemination.

Summary Report:  
[Provide brief but complete overview of threat, IOCs, and relevance]

Section 4 – LO6: Incident Response Plan (IRP) Development

4.1 Task – Plan Creation  
Objective: Develop a structured IRP for handling similar incidents.

Plan Components:

* Preparation Steps: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* Detection & Analysis Process: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* Containment Measures: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* Eradication & Recovery Steps: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* Post-Incident Review: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Evidence:  
[Attach final IRP document or excerpt]

Section 5 – LO7: Post-Incident Reporting & Recommendations

5.1 Task – Final Incident Report  
Objective: Document full investigation and provide actionable recommendations.

Report Contents:

* Executive Summary: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* Incident Timeline Overview: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* Key Findings: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* Root Cause: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* Impact Assessment: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* Recommendations:
  + Technical: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
  + Policy/Process: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
  + Training/Awareness: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Evidence:  
[Attach final report screenshots or excerpts]

Section 6 – Checklist – Learner Self-Verification

Before submitting Report 2, ensure you have:  
☐ All analysis steps clearly documented.  
☐ All relevant logs/screenshots attached.  
☐ Incident timeline completed for LO3.  
☐ Malware analysis details and evidence for LO4.  
☐ IOC enrichment and TI summary for LO5.  
☐ Full IRP documented for LO6.  
☐ Final incident report with recommendations for LO7.  
☐ File saved in correct group folder.