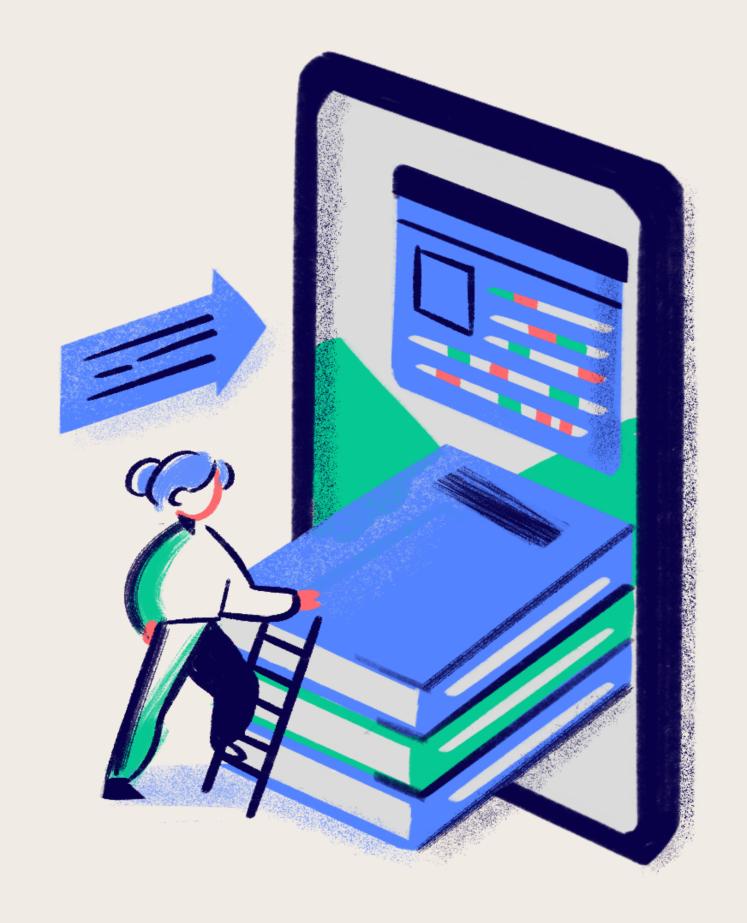
PRESENTED BY JAYESH KAKKAD

MICROSOFT SENTINEL HANDS-ON LAB

8 LABS & 29 EXERCISES



WWW.JAYESH-KAKKAD.COM

LAB 1 - SETTING UP THE ENVIRONMENT

- 1. The Microsoft Sentinel workspace.
- 2. Deploy the Microsoft Sentinel Training Lab Solution.
- 3. Configure Microsoft Sentinel Playbook.

LAB 2 - DATA CONNECTORS

- 1. Enable Azure Activity data connector.
- 2. Enable Azure Defender data connector.
- 3. Enable Threat Intelligence TAXII data connector.

LAB 3 - ANALYTICS

- 1. Analytics Rules overview.
- 2. Enable Microsoft incident creation rule.
- 3. Review Fusion Rule (Advanced Multistage Attack Detection)
- 4. Create a custom analytics rule.
- 5. Review the resulting security incident.

LAB 4 - INCIDENT MANAGEMENT

- 1. Review Microsoft Sentinel incident tools and capabilities.
- 2. Handling Incident "Sign-ins from IPs that attempt sign-ins to disabled accounts".
- 3. Handling "Solorigate Network Beacon" incident.
- 4. Hunting for more evidence.
- 5. Add IOC to Threat Intelligence.
- 6. Handover incident.

LAB 5 - HUNTING

- 1. Hunting on a specific MITRE technique.
- 2. Bookmarking hunting query results.
- 3. Promote a bookmark to an incident.

LAB 6 - WATCHLISTS

- 1. Create a watchlist.
- 2. Whitelist IP addresses in the analytics rule.

LAB 7 - THREAT INTELLIGENCE

- 1. Threat Intelligence data connectors.
- 2. Explore the Threat Intelligence menu.
- 3. Analytics Rules based on Threat Intelligence data.
- 4. Threat Intelligence Workbook.

LAB 8 - MICROSOFT SENTINEL CONTENT HUB

- 1. Explore Microsoft Sentinel Content hub.
- 2. Deploy a new solution.
- 3. Review and enable deployed artifacts.