







Certification

Terminal Objectives

- Gain in-depth knowledge of security threats, attacks, vulnerabilities, attacker's behaviors, cyber kill chain, SOC processes, procedures, technologies, and automation workflows.
- Understand the MITRE ATT&CK Framework and Able to identify attacker techniques, tactics, and procedures (TTP) to investigate on indicators of compromise (IOCs) and provide automated / manual responses to eliminate the attack/incident.
- Understand SOC and its processes, roles, responsibilities and implementation models
- Able to monitor and work on alerts generated based on various log sources.
 Ex: IDS/IPS, AV, EDR, Firewall, Network Monitoring applications, etc.
- Gain in-depth knowledge on all the latest defense technologies that are used in next generation SOC deployments. Ex : NGAV, SIEM, EDR, SOAR, TI, UEBA, IAM/PAM, etc.
- Gain knowledge of Incident Response Methodology, processes and in-depth knowledge on how to integrate SOC processes with Incident Response processes and learn how to automate them as a single workflow.
- Able to understand the concepts of Threat Intelligence and gain in-depth knowledge on how to integrate Threat Intelligence with the SIEM, SOAR, EDR and other SOC technologies to reduce the Mean time to Detect (MTTD) and Mean time to Respond (MTTR)

Accredited by:

GL@BAL ACE

Certified Security Operation Center Analyst (CSOC)

As you are reading this document, more than 100 successful hacking has occurred in the world per minute. With all the news stories about hackers, botnets, and breaches involving personal information, it's easy for the security message to sound over-used and tired. It's easy for people to say, "It won't happen here." Currently, Security Operation Centre (SOC) Analyst role is being only used in Security Operation Centers (SOC) that are monitoring financial institutions. Instead, we can upscale every IT person in an organization by equipping them with the skillset of a SOC Analyst so that they have the ability to review logs and identify attacks that are happening in their own organization and enable their organization to respond to them effectively.

Learning Outcome

- Attendees will learn in-detail about security threats, attacks, vulnerabilities, attacker's behaviors, cyber kill chain, SOC processes, procedures, technologies, and automation workflows.
- Attendees will learn MITRE ATT&CK Framework and will be able to identify attacker techniques, tactics, and procedures (TTP) to investigate on indicators of compromise (IOCs) and provide automated / manual responses to eliminate the attack/incident.
- Attendees will learn SOC and its processes, roles, responsibilities and implementation models
- Attendees will be able to monitor and work on alerts generated based on various log sources. Ex: IDS/IPS, AV, EDR, Firewall, Network Monitoring applications, etc.
- Attendees will be able to learn latest defense technologies that are used in next generation SOC deployments. Ex : NGAV, SIEM, EDR, SOAR, TI, UEBA, IAM/PAM, etc.
- Attendees will be able to learn Incident Response Methodology, processes and in-depth knowledge on how to integrate SOC processes with Incident Response processes and will be able to automate them as a single workflow.
- Attendees will be able to learn the concepts of Threat Intelligence and learn to integrate Threat Intelligence with the SIEM, SOAR, EDR and other SOC technologies to reduce the Mean time to Detect (MTTD) and Mean time to Respond (MTTR)

Program Outline

Module 1: Introduction to Cybersecurity & Latest Attack Trends

- 1. What is Security, Vulnerabilities & O-Days, Attack life Cycle, **Different Attack Vectors**
- 2. Threats Vs. Risks, Why Perimeter defenses are failing? Why Anti-Virus is not enough?
- 3. Financial Implications of a Cyber Attack
- 4. Business Email Compromise (BEC) (Demo)
- 5. Ransomware (Demo)
- 6. Advanced Persistent Threat (Demo)
- File-less Malwares (Demo) 7.
- 8. Mobile Malwares (Demo)
- 9. Identity Theft (Demo)
- 10.Web Data Breach (Demo)
- 11.Malvertising (Demo)
- 12.Payment Gateway based attacks (Demo)
- 13.Social Media based attacks (Demo)
- 14.Password based attacks (Password Stuffing, Account Takeover, Phishing, etc) (Demo)
- 15.State sponsored attacks (Case Study)
- 16.Distributed Denial of Service (Case Study)
- 17.Insider Threat (Case Study)

Module 2: Security Operations Center (SOC) - Introduction

- 1. What is a Security Operations Center and why we need it ?
- 2. NOC vs. SOC
- 3. Overview of Continuous Adaptive Risk and Trust Assessment (CARTA)
- 4. SOC v1.0 vs SOC v2.0
- 5. SOC v2.0 : Components
- 6. Security Operations Center roles and responsibilities
- 7. SOC team roles and responsibilities
- 8. Challenges of Security Operations Center
- 9. Measuring the ROI of Security Operations Center

Module 3 : Understanding Attack DNA

- 1. What is MITRE ATT&CK Framework?
- 2. Tactics, Techniques and Procedures (TTP)
- 3. Indicators of Compromise (IoC) and Indicators of Attack (IoA)
- 4. Mapping to ATT&CK from Raw Data Lab

Module 4: Self-Secure Validation

- 1. Anti-Virus & Next Generation Anti-Virus (NGAV)
 - How it works and Where is the Gap?
 - Deep Learning & Machine Learning & Artificial Intelligence
 - Cybersecurity use cases
- 2. Security Information and Event Management (SIEM)
- How it Works?
- Understanding Logs & Log Correlation
- SIEM Deployment options
- Application Level Incident Detection Use Case Examples
- Network Incident Detection Use Case Examples
- Host Malware Incident Detection Use Case Examples
- Understanding why SIEM is not enough and why Noise/False
- Positives?
- Lab / Demo 3. Endpoint Detection and Response (EDR)
- How it Works ?
- EDR vs. NGAV
- Understanding Memory and Process Detection & Mapping

- What is Managed Detection and Response
- Understanding various Response actions
- Lab / Demo

- 4. Security Orchestration, Automation and Response (SOAR) Alert / Notification Handling Challenges
 - Why SOAR ?
 - Sample Automated Playbooks
 - Lab / Demo
- 5. Cyber Range
 - Cyber Range Components
- Cyber Range Simulation Scenarios 6. Data Leakage Prevention (DLP)
- 7 User Behavior Analytics
- 8. Identity Management
- 9. Virtual Dispersive Networking (VDN)

Module 5 : Cybersecurity Incident Response

- 1. Introduction to Incident Response
 - Types of Computer Security Incidents
 - Fingerprint of an Incident
 - Incident Categories & Incident Prioritization
 - Why Incident Response?
- 2. Incident Reporting
 - Incident Response & Handling Methodology
 - Incident Response Plan
 - Incident Response and Handling: Identification, Incident Recording, Initial Response, Communicating the Incident, Containment, Formulating a Response Strategy, Incident Classification, Incident Investigation, Data Collection, Forensic Analysis, Evidence Protection, Systems Recovery, Incident Documentation, Incident Damage and Cost Assessment, Review and Update the Response Plan and Policies
 - Incident Response Checklist and Best Practices
 - CSIRT & its best practices
 - Incident Response Team .
 - Incident Tracking and Reporting
 - Incident handling: Real Word examples and exercises on Malware, Web Application attacks, Email attacks and Insider attacks.

Module 6 : Threat Intelligence & Threat Hunting

- 1. Introduction to Threat Intelligence
 - Understanding Threats, Threat Modeling and Risk
 - What is Threat Intelligence
 - Need for Threat Intelligence •
 - Benefits of Threat Intelligence
 - . Types of Threat Intelligence
 - Threat Intelligence Life Cycle
 - Sources of Threat Intelligence
 - Technologies contributing to Threat Intelligence (SIEM, EDR, Log Sources)
 - Incident Response & Threat Intelligence
 - Applications of Threat Intelligence
 - Threat Intelligence Frameworks (CIF, MISP, TAXII)
 - Role of Threat Intelligence Analyst & Threat Hunters

Open source Threat Intel Collections (OSINT and more)

Pubic Web data Threat Intel Collections (Maltego, OSTrICa,

Tel: +603 8800 7999 Fax: +603 8008 7000

Email: enquiry@cybersecurity.my Customer Service Hotline: 1 300 88 2999

Website: www.cybersecurity.my

- 2. Role of Threat Intelligence in SOC operations
- Setting up Threat Intel Framework
 - Enterprise Threat Landscape Mapping

Dark Web Threat Intel Collections

 Threat Intel collections with YARA EDR Threat Intel Collections

CyberSecurity Malaysia,

Level 7, Tower 1, Menara Cyber Axis,

Jalan Impact, 63000 Cyberjaya,

Selangor Darul Ehsan, Malaysia

SIEM / Log Sources Threat Intel Collections

 Incorporating Threat Intel into Incident Response Threat Intel & Actionable Contextual Data

- Scope & Plan Threat Intel Program
- Setup Threat Intel Team Threat Intelligence Feeds, Sources & Data Collections

and more)

3. MISP Lab

Recognition of Excellence