CyberSecurity MALAYSIA

MINISTRY OF COMMUNICATIONS AND MULTIMEDIA MALAYSIA

CYBERTRONIUM

SECURITY OPERATION CENTER ANALYST (CSOC)

COURSE LEVEL: EXPERT

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.

With Industry 4.0, we connect people, process, technology, and machinery together and it becomes very important to make sure every network is secure. We need in-house Security Professionals to always keep an eye on their infrastructure for attacks using the logs.

Once we equip them with this extra skillset/expertise, they will be able to find latest attacks happening all over in their infrastructure. This way, the Industry 4.0 infrastructure will be able to be more cyber-resilient.

> "Demand for real time access from any location dramatically increases our risk profile.
>
> Convenience exposes more attack points – decreasing our defence systems against malicious entities.

OBJECTIVE

1. Gain in-depth knowledge of security threats, attacks, vulnerabilities, attacker's behaviors, cyber kill chain, SOC processes, procedures, technologies, and automation workflows.
2. 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.
3. Understand SOC and its processes, roles, responsibilities and implementation models
4. Able to monitor and work on alerts generated based on various log sources. Ex: IDS/IPS, AV, EDR, Firewall, Network Monitoring applications, etc.
5. 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.
6. 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.
7. 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)

OUTCOME

1. Attendees will learn in-detail about security threats, attacks, vulnerabilities, attacker's behaviors, cyber kill chain, SOC processes, procedures, technologies, and automation workflows.

2. 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.

3. Attendees will learn SOC and its processes, roles, responsibilities and implementation models

4. 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.

5. 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.

6. 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.

7. 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)

AGENDA

Module 1: Introduction to Cybersecurity & Latest Attack Trends

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

Module 2: Security Operations Center (SOC) – Introduction

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

Module 3 : Understanding Attack DNA

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

Module 4 : Latest Cybersecurity Defence Technologies

- Anti-Virus & Next Generation Anti-Virus (NGAV)
  - How it works and Where is the Gap ?
  - Deep Learning & Machine Learning & Artificial Intelligence
  - Cybersecurity use cases
- 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
- 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
- Security Orchestration, Automation and Response (SOAR)
  - Alert / Notification Handling Challenges
  - Why SOAR ?
  - Sample Automated Playbooks
  - Lab / Demo

GET IN TOUCH 03 - 8800 7999 training@cybersecurity.my www.cyberguru.my

Global Accredited Cybersecurity Education Certification Scheme (Global ACE Certification Scheme)

The certification body for the Global ACE Certification is the Information Security Certification Body or ISCB, a department within CyberSecurity Malaysia.

Global ACE Certification is a national scheme extended to the Organization of Islamic Cooperation (OIC) member countries and the ASEAN region, established to ensure cybersecurity personnel conforms based on the latest international standard issues of ISO/IEC 17024 Conformity assessment – General requirements for bodies operating certification of persons.

ISCB is responsible for the management of impartiality of the Global ACE Certification and the decision on the certification of candidates. These are made under the authority of the Scheme Head through sessions of review and recommendation by the Certification Committee members who are deemed competent, appointed by the Scheme Head. (https://www.cybereducation-scheme.org/)

- Cyber Range
  - Cyber Range Components
  - Cyber Range Simulation Scenarios
- Data Leakage Prevention (DLP)
- User Behavior Analytics
- Identity Management
- Virtual Dispersive Networking (VDN)

Module 5 : Cybersecurity Incident Response

- Introduction to Incident Response
  - Types of Computer Security Incidents
  - Fingerprint of an Incident
  - Incident Categories & Incident Prioritization
  - Why Incident Response?
- 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

- 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
- Role of Threat Intelligence in SOC operations
  - Setting up Threat Intel Framework
  - Enterprise Threat Landscape Mapping
  - Scope & Plan Threat Intel Program
  - Setup Threat Intel Team
  - Threat Intelligence Feeds, Sources & Data Collections
  - Open source Threat Intel Collections (OSINT and more)
  - Dark Web Threat Intel Collections
  - SIEM / Log Sources Threat Intel Collections
  - Pubic Web data Threat Intel Collections (Maltego, OSTrICa, and more)
  - Threat Intel collections with YARA
  - EDR Threat Intel Collections
  - Incorporating Threat Intel into Incident Response
  - Threat Intel & Actionable Contextual Data
- MISP Lab

GET IN TOUCH 03 - 8800 7999 training@cybersecurity.my www.cyberguru.my

TRAINER

Mr. Clement Arul

Chief Executive Officer,
Kaapagam Technologies Sdn Bhd

HDRF TTT CERTIFICATE EMP/0783

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2019

CYBER SECURITY PROFESSIONAL OF THE YEAR - ASIA
(2017, 2018, 2019, 2020)

CYBER SECURITY EDUCATOR OF THE YEAR - ASIA
(2017, 2018, 2019, 2020)

MALAYSIA CYBER SECURITY AWARDS

CYBER SECURITY PROFESSIONAL OF THE YEAR
(2014, 2017)

ACADEMIC QUALIFICATION

- Bachelor of Engineering in COMPUTER SCIENCE with 1st Class Distinction, Bangalore University, India. University Topper in 6 subjects: Artificial Intelligence, Operations Research, Communication Systems, Advanced Microprocessor, and Discrete Structures

PROFESSIONAL MEMBERSHIP

- BSI Certified ISO 27001 Lead Auditor
- EC-Council Certified Ethical Hacker (CEH)
- EC-Council Certified Hacking Forensic Investigator (CHFI)
- EC-Council Certified Encryption Specialist (CES)
- EC-Council Certified Secure Programmer (ECSP)
- EC-Council Certified Security Analyst (ECSA)
- EC-Council Certified Disaster Recovery Professional (EDRP)
- EC-Council Certified Licensed Penetration Tester (LPT)
- Certified EC-Council Instructor (CEI)
- Certified Secure Application Developer (CSAD)
- Microsoft Certified Professional Developer (MCPD) on ASP.NET Developer 3.5
- Microsoft Certified Technology Specialist (MCTS) on Virtualization,
- Microsoft Certified Technology Specialist (MCTS) on ASP.NET 3.5,
- Microsoft Certified Technology Specialist (MCTS) on SQL Server 2008
- Microsoft Certified Technology Specialist (MCTS) on Exchange 2010
- Microsoft Certified IT Professional (MCITP) on Business Intelligence Developer
- Microsoft Certified IT Professional (MCITP) on Enterprise Messaging Administrator

INDUSTRIAL EXPERIENCE

- A Principal Technology Architect, Consultant, Security Professional and an Evangelist with Twenty Two (22) years of IT experience in Cyber Security, Ethical Hacking, Cyber Security Framework, Security Risk & Governance, Big Data, IoT, Systems Analysis, Design, Development, Secure Coding, Implementation, Digital Forensics and Project Management.
- Founder and CEO of Kaapagam Technologies Sdn. Bhd. and Kaapagam Education Services Sdn. Bhd. Also, Founder and Chief Technology Officer of Vigilant Asia (M) Sdn. Bhd.
- He has contributed to National Cyber Security Framework and many more national initiatives and now working with few ASEAN governments in developing and implementing National Cyber Security Frameworks. He was also part of the Secure Implementation of Nigerian ID system Project in 2019 as the prime security expert consultant.
- Presented in more than 120 public conferences and Talks in last Year and more than 600+ in last 5 Years across ASEAN
- Chief Architect for KALAM – IT Security Collaboration Platform : An MOHE Award Winning Platform
- Chief Architect for VALARI : Common Criteria Certified (the only) Malaysian Web Application Firewall
- Chief Architect for SOC 2.0 – A Regional Managed Detection and Response Platform for SME Security Consultant for many Multi-National and Leading IT Companies and Agencies in ASEAN Region
- Specializes in Payment Gateway Hacking, Application Security & Penetration Testing, Big Data & IoT Security.
- A Frequent Speaker in Security Events in ASEAN.
- Issued 100+ Web Vulnerability Disclosure Documents in last 4 years on Vulnerabilities
- discovered in Government, Corporate, Banks, Online Payment Gateways and e-Shopping websites in ASEAN.
- Provide Penetration Testing, Vulnerability Assessments, Security Consultations, Security Frameworks, Disaster Recovery & Business Continuity, and Security Audit Services for Customers in APAC Region.
- Conduct Workshops across ASEAN region on Penetration Test, Mobile Security, IoT Security, Forensics Investigations, Secure Programming, Disaster Recovery, Incident Handling, Business Data Analytics, and many more.
- Master of myriad of technologies and languages such as C#.Net, ASP.Net, VB.Net, AJAX, Web Services, WCF, WPF, HTML 5.0, XML, H.323, T.120, Real Time Communications, Media Technologies, MPEG4, SVG, Java, JavaScript, Active Directory, Windows Server 2016, Share Point, SQL Server 2012 / 2016.
- Bachelor of Engineering in COMPUTER SCIENCE with 1st Class Distinction, Bangalore University, India. University Topper in 6 subjects: Artificial Intelligence, Operations Research, Communication Systems, Advanced Microprocessor, and Discrete Structures