CyberSecurity MALAYSIA

MINISTRY OF COMMUNICATIONS AND MULTIMEDIA MALAYSIA

KAAPAGAM EDUCATION

CERTIFIED THREAT INTELLIGENCE [TI] ANALYST

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, Cyber Threat Intel (CTI) 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 CTI Analyst so that they have the ability to collect intelligence on the attacks that are happening in their industry, correlate them with their own infrastructure and come up with defenses including firewall rulesets to protect their organization from those attacks. This way, the Industry 4.0 company would be able to implement an effective, preventive, and proactive strategy.

This workshop introduces attendees with the basics concepts of Threat Intelligence and take them thru the entire process of setting up a Threat Intel Platform and also enables the attendees to share intelligence on malwares and attacks back to the community.

> “Evidence-based knowledge about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject’s response to that menace or hazard.
>
> **- Gartner’s definition of Threat Intelligence**

OBJECTIVE

1. Gain in-depth knowledge of security threats, attacks, vulnerabilities, attacker’s behaviours, cyber kill chain.
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. 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)
4. Able to Understand and learn how to setup a Threat Intelligence Framework and platform for your organization and consume community and commercial feeds to understand attacks and defend your organization from future attacks.
5. Gain in-depth knowledge on Malware Information Sharing Platform (MISP) and learn to setup a working instance with configurations and integrations that can be used immediately in your organisation.
6. Gain knowledge of Incident Response Methodology, processes and in-depth knowledge on how to integrate Threat Intelligence processes with Incident Response processes using HIVE and learn how to automate them as a single workflow.

OUTCOME

1. Attendees will learn in-detail about security threats, attacks, vulnerabilities, attacker's behaviours, cyber kill chain.
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 the concepts of Threat Intelligence and will be able 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)
4. Attendees will be able to setup a Threat Intelligence Framework and platform for their organization and consume community and commercial feeds to understand attacks and defend their organization from future attacks.
5. Attendees will be able to setup Malware Information Sharing Platform (MISP) with configurations and integrations that can be used immediately in organisation.
6. Attendees will be able to setup Incident Response Methodology, processes and integrate Threat Intelligence processes with Incident Response processes using HIVE and will be able to automate them as a single workflow.

AGENDA

Module 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)
- Threat Intelligence & SOC
- Incident Response & Threat Intelligence
- Applications of Threat Intelligence
- Threat Intelligence Frameworks (CIF, MISP, TAXII)
- Role of Threat Intelligence Analyst & Threat Hunters

Module 2 : Technical Deep Dive on Latest Attacks

- 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?
- Introduction to Cyber Kill Chain
- Indicators of Compromise (IOC) & IOC Sources (OTX, MISP)
- Business Email Compromise (BEC) (Lab) with Indicators of Compromise
- Ransomware (Lab) with Indicators of Compromise
- Advanced Persistent Threat (Lab) with Indicators of Compromise
- File-less Malwares (Lab) with Indicators of Compromise
- Mobile Malwares (Lab) with Indicators of Compromise
- Web Data Breach (Lab) with Indicators of Compromise
- Malvertising (Lab) with Indicators of Compromise
- Social Media based attacks (Lab) with Indicators of Compromise
- Password based attacks (Password Stuffing, Account
- Takeover, Phishing, etc) (Lab)
- What is MITRE ATT&CK Framework ?
- Tactics, Techniques and Procedures (TTP)
- Threat Actors
- ATT&CK Navigator
- The ThreatHunter-Playbook
- Atomic Red Team Library
- Threat-Based Adversary Emulation with ATT&CK
- Behavioral-based analytic detection using ATT&CK
- Mapping to ATT&CK from Raw Data – Lab
  Storing and analyzing ATT&CK-mapped intel

Module 3 : 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
- Commercial Threat Intel Feed Providers (RecordedFuture, BlueLiv, etc.)
- Commercial Threat Intel Platforms (Anamoli, DigitalShadows, etc.)

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/)

Malware Information Sharing Platform (MISP)

- MISP Project Overview
- MISP Features & Use cases
- Events, Objects and Attributes in MISP
- MISP Data model & Core data structure
- MISP - Creating and populating events
- MISP - Distribution and Topology
- Information Sharing and Taxonomies
- MISP Galaxy
- MISP Object Templates
- MISP Deployment and Integrations
- Normalizing OSINT and other community & Private Feeds
- SIEM and MISP Integration
- Incident Response and threat hunting using MISP
- Viper and MISP
- MISP Administration
- MISP feeds - A simple and secure approach to generate, select and collect intelligence
- MISP and Decaying of Indicators
- Workflow of a security analyst using Viper as a management console for malware analysis

Malware Information Sharing Platform (MISP)

- Introduction to Incident Response
- Incident Response & Handling Methodology
- MISP & HIVE Integrations
- HIVE Implementation
- Malware Analysis Use case using MISP & HIVE

Consideration

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.

Implementation

With Industry 4.0, cybersecurity is utmost important for all. Hence, we recommend at least 250 employees be trained under this program to start with. This 5-day course can be run continuously with 25pax/class for next 5 months to prepare for a secure Industry 4.0 adaption and implementation.

Impacts Post MCO

According to Trend Micro & Recorded Future, the cyber-attacks have increased by a range of 660% to 2000% during MCO and this will increase Post MCO. Hence it is good for our companies to get their staff trained to identify the attacks and defend themselves and their organizations.

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

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