



WORKSHOP 1:

Integrated Cyber Defence Management: A Journey towards Cyber Resilience

About the workshop:

This one-day workshop introduces you to all the recent attacks with 100% live demos and provides a quick brief on latest defence technologies and concluding by sharing the practical knowledge of how to fit them together. This will provide a framework to create a next generation Cyber Defence management layer to build a cyber resilient organisation.

Duration: 1 day (9 am till 5pm)

Prerequisites:

Anyone with the interest to understand Cyber Resilience

Target participants:

Regulators, Security Engineers, CISO, Financial Institutions, Insurance Companies

Workshop Outline

Module 1: Introduction to Cyber Security & 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
- Need of Integrated Cybersecurity Management
- 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: Introduction to Latest Cybersecurity Defence Technologies

- Anti-Virus & Next Generation Anti-Virus (NGAV)
- Deep Learning & Machine Learning & Artificial Intelligence
- Endpoint Detection and Response (EDR)
- EDR vs. NGAV
- Managed Detection and Response
- Security Information and Event Management (SIEM)
- Security Operation Centre (SOC) & Network Operation Centre (NOC)
- Threat Intelligence & Threat Hunting
- Data Leakage Prevention (DLP)
- User Behavior Analytics
- Identity Management
- Machine Learning based APT & Network Monitoring Tools
- Industry 4.0 & Cybersecurity

- IoT Security
- Scada Security
- Cloud Security
- Virtual Dispersive Networking (VDN)
- Web Application Firewall
- Cyber Range

Module 3: Integrated Cyber Defense Platform

- Need for Integrated Cyber Defense Platform
- Components of Cyber Defense Platform
- Limitations of Traditional SOC using SIEM
- Next Generation SOC: Managed Monitoring, Detection, and Response
- SCADA & Critical Infrastructure Security: Detection, Monitoring and Response
- Need for Integrated Incident Response
- Need for Integrated Threat Intel Sharing between Govt and Industry
- Implementing a coordinated Threat Intel sharing within Critical National Infrastructure, Govt agencies, Industries and organizations.
- Implement Capability & Capacity building initiatives
- Case Study & Group Discussion

Trainer Profile



A Principal Technology Architect & Security Professional with Twenty (20) years of IT experience in Security, Ethical Hacking, Cyber Security Framework, Security Risk & Governance, Systems Analysis, Design, Development, Secure Coding, Implementation, Digital Forensics and Project Management.

Founder, CEO of Kaapagam Technologies and Kaapagam Education Services. Chief Technology Officer for Regional Security Operation Centre by Vigilant Asia. A Security Consultant for many Multi-National and leading IT companies in APAC region. A Frequent Speaker in Security Event in APAC.

Awards & Recognition

Recipient of following National and APAC Individual Awards:

1. Cyber Security Educator Asia Pacific of the year 2019
2. Cyber Security Professional of the Year 2017 APAC, awarded by Cyber Security Excellence Awards, USA
3. Cyber Security Professional of the Year 2019, 2017 awarded in Cyber Security Awards, Govt of Malaysia
4. Cyber Security Professional of the Year 2014, awarded in Cyber Security Awards, Govt of Malaysia

Recipient of following National and APAC Company Awards:

1. Top 25 Cyber Security Company in APAC by CIO Outlook
2. Cyber Security Innovation of the Year 2016, awarded in Cyber Security Awards 2016 by CSM
3. Cyber Security Training Provider of the Year 2014, awarded in Cyber Security 2014 by CSM

***For more registration and more information, please contact
sc2019@wsconferences.com***