TB-CERT
Thailand Banking Sector CERT

CYBERSECURITY ANNUAL CONFERENCE 2024

TOMORROW'S CYBERSECURITY IN THE AGE OF AI

WORKSHOP SYNOPSIS 29 AUGUST 2024

Speaker

Forcepoint

10:30 - 12:30 hrs.

(At President Room4)

Building Data Security Everywhere at the AI Era

Khun Alongkot Wongyam, Sr. Security Consultant, Thailand & Indochina, Forcepoint

This workshop focuses on creating a robust data security strategy to protect your data everywhere – in cloud apps, web, email, network and endpoint with unified policy management as well as AI-Mesh technology to give you visibility into what data is being used in unparallelled accuracy. In this session, we seek to equip attendees with knowledge about the latest AI-driven security solutions, real-world applications, and strategies for effectively integrating AI into their security frameworks.

Our experts will share:
- importance of a comprehensive data security strategies and its key components
- integrate AI into your data security framework to identify and evaluate risks
- design AI-Driven Security Framework through discovery, classification, prioritisation, response and recovery
- implement AI-driven security measures with continuously monitoring and compliance
- Case Studies and real-world applications

For Technical Related.
*Hands-on experience on configuring and implementing policies in minutes and unifying report with real-time alerts to secure data everywhere

No pre-requisite required.

Speaker

Akamai

13:00 - 15:00 hrs.

(At President Room4)

API Security Technical Workshop

This workshop is for technical professionals and managers who are interested in learning what Application Programming Interfaces (APIs) are and understand the risks associated with APIs. Attendees will get hands-on experience with techniques that are used to exploit vulnerable APIs — resulting in unintended data exposure. The API Security workshop will also look at the actual traffic and how it is analyzed and viewed within the Akamai API Security platform through the use of its posture management and runtime protection.

- Review and understand API vulnerabilities and corresponding threats
- Understand the OWASP API Top10 and the associated security risk around the number one vulnerability to APIs - Broken Object Level Authorization (BOLA)
- Automating issue detection, Issue comprehension and remediation strategies

Prerequisite: Developers, DevOps, SecDevOps, or any other technical professional interested in learning what APIs are and their use in the real world. Attendees to bring own laptop.

Khun Pongphop Laochaikun, Major Account Executive, Akamai Technologies
Pongphop Laochaikun (AKA "Chong") is a seasoned Security Sales Specialist based in Thailand, with over a decade of experience in the IT and cybersecurity industry. Currently serving as a Account Manager at Akamai Technologies, Chong excels in promoting Akamai's Secured and Intelligent Connected Cloud solutions. He has gained extensive experience in postsales, presales, and product management extensively in the past 12 years.

He further enhanced his expertise as a Security Sales Engineer and then as a Regional Security Expert for about 2 years in global cybersecurity companies. At Akamai, Chong has been instrumental in addressing customer needs in Application and API Security, Zero Trust Related Solution, Brand security, and security in cloud infrastructure. His technical acumen and customer-centric approach have made him a trusted advisor in the cybersecurity landscape.

Speaker

STelligence

GEMINI

10:30 - 11:15 hrs. | 11:15 - 12:00 hrs. | 13:00 - 13:45 hrs. | 13:45 - 14:30 hrs.

(At President Room3)

Build Your Cyber AI Assistant with No Hallucination (Showcase)

Are you tired of AI assistants that hallucinate and give you inaccurate information? Get ready for a breath of fresh air with Gemini Enterprise, the AI assistant that's here to revolutionize the way SOCs access insights.

Join us for our upcoming workshop, Build Your Cyber AI Assistant Now: Accelerate Analytic and Investigation with No Hallucinations, at the Cyber Security Annual Conference 2024, you'll discover how Gemini Data leveraged generative AI and GraphRAG to eliminate costly model training and accelerate speed to cyber security incident investigation and reporting, the Cyber AI Assistant that will change the game.

Here's what you'll learn from this workshop:
- Connect cyber security data and turn them into consumable knowledge
- Easily build a simple, secure, and trustworthy generative AI experience to accelerate enterprise cyber security analytics and investigation
- AI-Powered Cyber Security Incident Reporting at your finger-tips.
- Safety RAG, the ultimate weapon against hallucinations
- A glimpse into Gemini Enterprise's transformative architecture.

Mr. Johnny Lin, Founder & CEO Gemini Data, Inc.
Johnny co-founded Gemini Data together with Splunk Co-founder and CEO Michael Baum where he drives Gemini Data's global go-to-market and product strategy. Johnny has demonstrated a proven track record in launching disruptive technologies to the market. He has not only helped multiplied tech companies developed their international footprints, His strategic insight has driven substantial business growth for companies like Foundstone (acquired by McAfee), AirDefense (acquired by Motorola), SPI Dynamics, and ArcSight (both acquired by HP), and most recently, Splunk (acquired by Cisco).

Before founding Gemini Data, Johnny also held multiple management roles at Systex Group including Assistant Vice President of International Business, Head of Splunk Lab and Managing Director of Systex Southeast Asia. Johnny is a BA from Fu Jen Catholic University.

Khun Montri Rungroj, Sr.Cloud Infrastructure Engineer, STelligence.
Montri Rungroj is a seasoned technical leader with over 20 years of experience in the field of TCP/IP networking. He holds dual CCIE certifications (Routing & Switching, Service Provider) and has a proven track record in leading and executing large-scale LAN and WAN projects, including those for internet service providers, Data Center and nationwide MPLS infrastructures. As a consultant, Montri has provided technical guidance and problem-solving expertise to major banking institutions, service providers, and mobile operators across Thailand and ASEAN.

Currently, Montri is leading the cloud infrastructure and cybersecurity team at STelligence. Before joining STelligence, he served as a Solution Architect at Cisco, where he designed complex network solutions, and as a Network Specialist at IBM.

Montri holds a Bachelor of Electrical Engineering from Chulalongkorn University and an MBA in Finance.

WORKSHOP SYNOPSIS 30 AUGUST 2024

Speaker

imperva
a Thales company

10:30 - 12:30 hrs.

(At President Room4)

DesignYour Playbook to Secure API

Mr. Jared Tan, Sr. Security Engineer, Imperva
Mr. Worachat Sarsa, Principle AppSec and DataSec Engineer, Exclusive Networks

Participants will be able to create their own playbook to secure API for organization.
Get to know how to initial the conversation with related person such as cybersecurity and development teams to make awareness and start secure both existing and new APIs.

- This session is good for whom has responsible to secure API / Web / sensitive data for organization.
- Read through the Securing API 2023 by Gartner.
- Read through the Guideline of using API in financial services by Bank of Thailand.

Speaker

kaspersky

13:00 - 15:00 hrs.

(At President Room4)

Intelligent-driven Incident Response: In depth Investigation on Real-world Cyber Attacks

This workshop focuses on the critical role of threat intelligence in enhancing incident response processes. By examining real-world cyber-attacks, participants will gain a comprehensive understanding of how to effectively leverage threat intelligence to detect, investigate, and mitigate cybersecurity incidents.
- Case Study 1: High-Profile Data Breach
- Case Study 2: Ransomware Attack
- Case Study 3: Advanced Persistent Threat (APT)

Participants will leave the workshop with:
- A deeper understanding of threat intelligence and its applications in incident response.
- Practical insights from real-world case studies on data breaches, ransomware attacks, and APTs.
- Strategies for integrating threat intelligence into their incident response processes.
- Awareness of current challenges and future trends in cybersecurity.

This workshop aims to equip cybersecurity professionals with the knowledge and tools needed to enhance their incident response capabilities through the effective use of threat intelligence.

Prerequisite: This workshop is suitable for CISOs, Security Analysts, System Engineers, Risk Managers, Compliance Officers, Business Continuity Planners.

Attendees must have your own laptop with the following minimum hardware requirements:
- CPU: 4 Cores
- RAM: 16 GB
- Storage: 50 GB min
- Network: Internet access
- Operating System: Windows / Linux / OSX

Virtual Machine will be provided during workshop. If you preferred your own VM, these are the software requirements:
- Python 3.8+ (including pip)
- VirtualBox or VMware (for managing VMs)
- SSH Client (for remote access)
- Wireshark
- CyberChef
- Notepad++
- PowerShell

Mr. Ahmad Zaidi, Digital Forensics and Incident Response (DFIR) Specialist, Kaspersky
Ahmad Zaidi, a Malaysian cybersecurity expert with broad international experience, has more than 12 years of knowledge and experience in the field and has been involved in high-profile cybersecurity incident investigations globally. As Digital Forensics and Incident Response (DFIR) specialist in the Kaspersky Global Emergency Response Team (GERT), Zaidi brings valuable experience in a variety of cyber security domains, including digital forensics and incident response (DFIR), malware analysis and reverse engineering, threat intelligence, and threat hunting. As part of his daily job as a DFIR specialist, he also serves as a trainer for Kaspersky's Expert training and conductor for Table Top Exercise (TTX) service.

Zaidi is a committe member of the Malaysia Cyber Security Community (RawSEC) and active member of the High Technology Crime Investigation Association (HTCIA), both of which contribute to the evolution of the cybersecurity ecosystem through information sharing and collaboration. His expertise has also led him to speak at a number of international and local events, in which he has offered vital insights and best practises with a wide range of audiences.

Speaker

HITB

10:00 - 14:00 hrs.

(At President Room3)

Should you fully bank on your cybersecurity? Practical workshop for banking and financial services

Mr. Konstantin Polishin, Head of Red Team SE in the Penetration Testing Department at Positive Technologies
Konstantin graduated with honors from the MPEI National Research University in 2021 with a degree in information security.

He has been a part of the Positive Technologies team since 2020. Konstantin handles complex red team assessments for Russia's largest companies, requiring seamless teamwork to gain initial access to corporate networks, swiftly escalate attacks, and achieve maximum privileges in the infrastructure while staying under the SOC's radar.

Konstantin specializes in identifying financial risks in major banks by demonstrating potential fund withdrawal threats, bypassing the email security stack of Anti-APT systems, and expanding our expertise in social engineering with results applied in practice.

Konstantin also holds OSCP and OSEP certifications and is a speaker at PHDays forums.

Mr. Maxim Kostikov, Head of Application Security Analysis at Positive Technologies
Maxim graduated from MIREA with a degree in cybersecurity in 2018.

Before joining Positive Technologies, Maxim worked at Advanced Monitoring, where he specialized in penetration testing and web application security analysis.

He joined the Positive Technologies Digital Banking Security Analysis department in 2018. Now Maxim leads teams of over 30 experts specializing in web application, banking system, and mobile app security.

He placed second in the Google Play Security Reward Program on the HackerOne platform. Maxim has spoken at PHDays, VolgaCTF, and OFFZONE conferences, and holds OSCP, eWPTX, and OSEP certifications.