



TB-CERT
Thailand Banking Sector CERT

CYBERSECURITY ANNUAL CONFERENCE 2023

SUSTAINABLE CYBERSECURITY

Date: 22 September 2023
Time: 14.00-16.00 hrs.
Venue: 2nd Floor, The Athenee Hotel Bangkok





If you would like to join Technical Special Workshop, Please feel free to register.

ภายในงานยังเปิด Session ให้ ผู้ที่สนใจเรียนรู้เชิงลึกแบบลงมือปฏิบัติ โดยจำกัด Session ละ ไม่เกิน **30** คน เท่านั้น

สนใจลงทะเบียนเพื่อเลือกเข้าอบรม Session นี้ได้ที่ >>>>

[▶ REGISTRATION](#)

HANDS-ON-WORKSHOPS

Topic	14:00 - 16:00 hrs.
 <p>Cyber Incident Handling and Investigation Workshop</p> <p>This workshop will cover the simulated APT attack scenario with data set and allow attendees to do hand-on investigation by following the Cyber Kill Chain steps and find out information related to the attack, for example; attacker infrastructure, associated malware, compromised credential and attack vectors. This workshop provides users a way to gain experience in searching and analyzing to answer specific questions related to an investigation. These questions are similar to what would be asked in their own organizations.</p>	<p>London 1 Room</p>
 <p>Guarding Your Inbox: Navigating the Email Security Landscape</p> <p>Email has become an indispensable part of our daily work lives, but it's also a prime target for cybercriminals. Join us for an engaging and informative workshop on email security, where we delve into the latest cyber threat trends, share insights from our cybersecurity report, and empower you with the knowledge and tools to protect your digital communication.</p>	<p>London 2 Room</p>
 <p>Strengthening API Security: From Afterthought to Forefront</p> <ul style="list-style-type: none"> • Learn the evolution of the application architecture in a digitally transformed world • Understand OWASP API Security Risks 2023, and API security best practices • Explore mitigation strategies with Akamai API security • Akamai API Security Demo 	<p>London 3 Room</p>
 <p>Implementing Zero Trust Network Access Workshop: From Strategy to Action</p> <p>This workshop is designed to simplify understanding Zero-Trust Network Access while maintaining an official and informative tone. By the end of the session, attendees will be equipped with the expertise needed to confidently deploy and manage ZTNA solutions in accordance with Zero-Trust architecture and standard, ensuring comprehensive security, visibility, and control across diverse deployment environments.</p>	<p>Japan Room</p>

****Remark : All workshop participant, Please bring your own computer.**

splunk> turn data into doing™

Incident handling with Splunk Workshop

Overview

Investigating with Splunk is a modular, hands-on workshop designed to familiarize participants with how to investigate and handling incidents using Splunk and open source. This workshop provides users a way to gain experience searching in Splunk to answer specific questions related to an investigation. These questions are similar to what would be asked in their own organizations. Users will leave with a better understanding of how Splunk can be used to investigate in their enterprise.

The workshop agenda is approximately 2 hours and includes:

Agenda

14.00-14.15pm: Basic Search Command Overview
14.15-15.45pm: Hand-On (APT Scenario)
15.45-16.00pm: Wrap up & Gifts

Max: 30 Seats

Workshop Data

The workshop data focusing on network and host data including:

- Suricata IDS
- Fortinet NGFW
- Splunk for Stream (wire data)
- Windows Event Logs
- Microsoft Sysmon

Attendees will Benefit

The workshop is designed for all personas on a Security Operations teams responsible for security monitoring and incident response. The workshop has three goals:

1. Understand the types of questions that need to be asked during an investigation
2. Identify the data required to find the answer to these questions in Splunk
3. Develop searches in Splunk that provide answers to the questions in order to advance your investigation



Workshop Logistics

This workshop is hands-on and each user will need access to a modern web browser with internet connectivity. Splunk will provide a cloud environment where the Splunk software and data will reside.

- Laptop with Browser
- Internet Connectivity

Get free Splunk T-Shirt swag for joining.





<<Topic>>

"Guarding Your Inbox: Navigating the Email Security Landscape"

<<Synopsis>>

Email has become an indispensable part of our daily work lives, but it's also a prime target for cybercriminals. Join us for an engaging and informative workshop on email security, where we delve into the latest cyber threat trends, share insights from our cybersecurity report, and empower you with the knowledge and tools to protect your digital communication.

<<Event Highlights>>

1. **Cybersecurity Report Insights:** We will unveil the findings of our comprehensive cybersecurity report, highlighting the most pressing email security threats and vulnerabilities in today's digital landscape. Gain insights into the tactics used by cybercriminals and learn how to spot potential risks.
2. **Email Attack Trends:** Stay ahead of the curve as we dissect the latest email attack trends. Explore real-world case studies and understand the evolving strategies of attackers, including phishing, spear-phishing, ransomware, and more.
3. **Email Security Best Practices:** Arm yourself with practical strategies and best practices to fortify your email security defenses. Discover effective methods for secure email communication, encryption, and user awareness training.
4. **Hands-On Cyber Range Game:** Put your newfound knowledge to the test in our interactive cyber range game. Face simulated email security challenges and see if you can defend against various cyber threats. Prizes await the top performers!



Topic: Strengthening API Security: From Afterthought to Forefront

Time: 14.00-16.00 hrs., 22 September 2023

Participation: 30 seats

Agenda:

1. [30min] Insights from Akamai State of the Internet research report - State of the Internet
2. [20min] API Security problem case sharing
3. [30min] Akamai API Security overview and demo
4. [20min] Managed Hunting overview
5. [20min] Q&A

Attendees will benefit:

- Learn the evolution of the application architecture in a digitally transformed world
- Understand OWASP API Security Risks 2023, and API security best practices
- Explore mitigation strategies with Akamai API security
- Akamai API Security Demo

Pre-requisite:

- Workshop will benefit those with existing familiarity of cybersecurity principles, OWASP and API security
-

FORTINET

Japan Room

Topic: **Implementing Zero Trust Network Access Workshop: From Strategy to Action**

Time: 14.00-16.00 hrs., 22 September 2023

Participation: 30 seats

Agenda:

	Topic	Time	Prerequisite
Lab 1:	Introduction, Topology and Agenda	30 Minutes	-
Lab 2:	Integrated EMS Security Fabric	25 Minutes	-
Lab 3:	Remote Worker	40 Minutes	Lab 2
Lab 4:	On-Premises Access Control	25 Minutes	Lab 2
Lab 5:	Conclusion		

Workshop content:

- Integrating Endpoint Management for Robust Security
 - Learn to seamlessly incorporate an Endpoint Management Server (EMS) within your Security Fabric.
- Establishing Zero Trust Policies for Enhanced Protection
 - Dive into Zero Trust policies and rules that provide foolproof protection for corporate and remote users.
- Enabling Secure Remote Application Access
 - Discover how to set up a ZTNA HTTPS Application Gateway that guarantees secure access to applications from remote locations.
- Dynamic On-Premises Access Control
 - Learn the art of configuring ZTNA IP/MAC Based Access Control for adaptable access within on-premises environments.

Attendees will benefit:

This workshop is designed to simplify understanding Zero-Trust Network Access while maintaining an official and informative tone. By the end of the session, attendees will be equipped with the expertise needed to confidently deploy and manage ZTNA solutions in accordance with Zero-Trust architecture and standard, ensuring comprehensive security, visibility, and control across diverse deployment environments.

Pre-requisite: none

Preparation: (any laptop, browser, etc.)

- A laptop with a web browser installed.
- Fortinet Training Account (can register for an account at the event)