Half Day Talk : Red, Purple & Blue Team, and Threat Hunting & IR

ISACA Malaysia Chapter

Date/Time : 25 February 2019 (Tuesday), 2:00pm – 5:30pm
Location : Sime Darby Convention Center, Bukit Kiara, Kuala Lumpur

Overview

Cyber threat is getting rampant with the use of internet, cloud, smart phones and IoT; it is only a matter of time when we are getting targeted and breached. Having security protections are no longer enough in preventing these attacks; therefore we need to evaluate our internal people capabilities, incident handling process and escalation as well as conducting regular health checks like threat hunting exercise to ensure the hygiene of our environment. It is also very important to understand qualification and capabilities of our team, making sure that they are well trained to follow incident response process and escalation in dealing with such incidents. This presentation will outline the importance of different team and activities in managing these challenges faced and some useful steps to consider.

Who Should Attend

This talk is suitable for security professionals, auditors, advisors, etc. who want to have a better understanding on Cyber Security topics - Red, Purple and Blue Team, and Threat Hunting & Incident Response.

What You Will Learn

- The overall concept of Cybersecurity
- Understanding the differences: Red vs. Blue vs. Purple team
- The methodology, objective and approach of each team and their characteristics
- Understand the Indicators, and Tactics, Techniques and Procedures (TTP) of Threat Hunting
- Understand what is Cyber Incident Response (IR) - The plan, methodology and approach

3 CPE hours

Half Day Talk: Red, Purple & Blue Team, and Threat Hunting & IR

ISACA Malaysia Chapter

Our Speakers

Jonny Lie is a highly-skilled Cyber Security Consultant with Commissum who has wide exposure to different threats and challenges in the cyber security industry. He has previously worked with one of the world's largest defence and cyber intelligence company and has had hands-on technical experience with security assessment engagements on web applications, mobile applications, wireless security etc. .

Jonny's expertise includes writing customised code to discover and exploit vulnerabilities, designing and managing cybersecurity solutions e.g. SIEM, malware analysis, and using artificial intelligence to detect and exploit vulnerabilities. Jonny holds internationally recognised certifications including Common Criteria Certified Evaluator, SANS Penetration Testing (GPEN), and CREST Practitioner Security Analyst and Offensive Security Certified Professional (OSCP).

Agenda

1:30pm	Registration
2:00pm	Topic 1: Red, Purple and Blue Team
3:15pm	Break / Networking
3:45pm	Topic 2: How to Succeed at Threat Hunting & IR: Think Differently about Data
5:00pm	Q & A Session
5:30pm	The End

Sharat Nautiyal is a Senior Cybersecurity Solutions Architect at ExtraHop. With more than a decade of experience in security engineering domains such as network traffic analysis, network behaviour anomaly detection and visibility, along with rich experience in performance engineering, Mr. Nautiyal has been assisting enterprises in building an integrated security and network operations centre (SNOC). Mr. Nautiyal earned a Masters degree in Telecommunications and Software Engineering from Birla Institute of Technology and Science and an undergraduate degree in Electronics and Communications Engineering from VTU.

Details and Registrations

ISACA Malaysia Chapter

Event: **Half Day Talk : Red, Purple & Blue Team, and Threat Hunting & IR**

Date: 25 February 2020 (Tuesday)

Time: 2.00pm to 5.30pm

Venue: Sime Darby Convention Centre, 1A, Jalan Bukit Kiara 1, 60000 Kuala Lumpur.

Fees: **Free** for ISACA members
RM 150 for non members / guest
(for paying guest, please contact Mr Seelan)

Contact: Mr.Seelan, ISACA Office Administrator
Mobile: +6017 219 6225 | Email: officeadmin@isaca.org.my

Registration via ISACA Malaysia Chapter Website Only!

As good practice, ISACA Malaysia Chapter is informing you that your personal data will be processed, retained and used by ISACA Malaysia Chapter in relation to this training event. Your personal data may also be retained and used by ISACA Malaysia Chapter to market and promote training events conducted by ISACA Malaysia Chapter.

Reservations & Registrations:

Seats are LIMITED. Please register via ISACA MY Chapter website (https://isaca.org/malaysia).

ISACA Malaysia Chapter reserves the right to change the venue, date, speakers, and programme or to cancel the programme should unavoidable circumstances arise. If applicable, a full refund of fees will be made in the event of cancellation.

Payment Details:

Fees are not refundable once registration is confirmed, however, replacements may be sent. Cheques should be made payable to "Information Systems Audit And Control Association" and mailed to: ISACA Malaysia Chapter, Unit 916, 9th Floor, Block A, Damansara Intan, No.1, Jalan SS 20/27, 47400 Petaling Jaya, Selangor.

Alternatively, payment can be banked-in to: Maybank Account number – 512231822725. Bank in slip or Internet Banking confirmation MUST be faxed to 03-7726 1257 or emailed to officeadmin@isaca.org.my, with a cover note stating Event Name, Organisation / Participant(s) Name and Amount Banked In. Payment will not be recognised without this cover note.