SEC014: Security Information and Event Management (SIEM)

แนะนำหลักสูตร:

เทคโนโลยีที่จะช่วยองค์กรในการเก็บรวบรวมข้อมูล Logs จากอุปกรณ์รักษาความปลอดภัยทางไซเบอร์ ซึ่งผู้ที่เกี่ยวข้องในการดูแลระบบไซเบอร์ขององค์กรไม่ว่าจะเป็น Server Administrator, Security Administrator, Security Analyst, Auditor รวมถึงผู้บริหารองค์กร สามารถใช้ประโยชน์จากข้อมูลที่เก็บรวบรวมจากแหล่งต่างๆ มาทำการวิเคราะห์หาพฤติกรรมที่ผิดปกติในระบบเครือข่ายได้

นอกจากนี้การเก็บ Log ขององค์กรยังเป็นสิ่งจำเป็นตามกฎหมายซึ่งองค์กรจะต้องปฏิบัติให้สอดคล้องอีกด้วย การเก็บรวบรวมข้อมูล Logs ไว้ใน SIEM ทำให้องค์กรสามารถทราบถึงภัยคุกคามที่เกิดขึ้น ผู้ที่เกี่ยวข้องสามารถวิเคราะห์หาสาเหตุและดำเนินการแก้ไขได้ การรวบรวมข้อมูลเพื่อจัดทำรายงานนำเสนอผู้บริหารก็สามารถทำได้สะดวกรวดเร็วและมีประสิทธิภาพกว่าการมี Logs กระจัดกระจายอยู่ตามอุปกรณ์ต่างๆ ซึ่งทำให้เสียเวลามากในการรวบรวมข้อมูลเพื่อจัดทำรายงานถึงสถานการณ์ความปลอดภัยทางไซเบอร์ในภาพรวมขององค์กร ข้อจำกัดของ SIEM ก็คือการเก็บข้อมูลที่เป็น Logs ซึ่งไม่ใช่ข้อมูลที่เป็น Real-Time

ดังนั้นในการแก้ปัญหาหาภัยคุกคามที่เกิดขึ้นในระบบไซเบอร์อย่างรวดเร็วทันต่อสถานการณ์ก็คงต้องพึ่งพาเทคโนโลยีที่สามารถวิเคราะห์และตอบสนองต่อภัยคุกคามได้ในแบบ Real-Time ซึ่งอุปกรณ์ดังกล่าวก็สามารถทำงานร่วมกับ SIEM ได้เป็นอย่างดี SIEM จึงทำหน้าที่หลักๆ ในการเก็บรวามรวมข้อมูลเพื่อให้สามารถทำการวิเคราะห์เหตุการณ์ย้อนหลังไปได้เป็นเวลานาน เพราะภัยคุกคามยุคใหม่อย่าง Advanced Persistent Threat นั้นอาจแทรกซึมเข้ามาอยู่ในระบบขององค์กรนานแล้วแต่อุปกรณ์ที่ดูแลความปลอดภัยแบบ Real-Time จะสามารถตรวจจับพฤติกรรมได้ก็ตอนที่มันเริ่มทำการโจมตีซึ่งจะเกิดขึ้นแบบเงียบ ๆ เพื่อไม่ให้เป็นที่สังเกตุของผู้ดูแลระบบหรืออุปกรณ์สามารถที่จะตรวจจับได้ ในการป้องกันที่มีประสิทธิภาพนั้นเมื่ออุปกรณ์ตรวจจับภัยคุกคามในระบบได้แล้ว ในการเก็บรวบรวมหลักฐานก็มีความจำเป็นที่จะต้องไปค้นหาใน SIEM ที่มีข้อมูลย้อนหลังไปหลายเดือนทำให้สามารถสืบทราบได้ว่าต้นตอของปัญหานั้นเข้ามาในองค์กรเมื่อไหร่โดยใคร ซึ่งจะทำให้กระบวนการในการจัดการภัยคุกคามขององค์กรนั้นมีประสิทธิภาพสอดคล้องกับมาตรฐานการจัดการความปลอดภัยทางไซเบอร์ SIEM ที่มีคุณภาพมักจะมีความสามารถในการทำ Correlation เพื่อเชื่อมโยงถึงความสัมพันธ์ของข้อมูล Logs จากแหล่งต่างๆ ทำให้การวิเคราะห์สถานการณ์ทำได้รวดเร็วและมีประสิทธิภาพ

หัวข้อการอบรม:

- ❑ Proof of Concept
  - Auditing commands run by user
  - Amazon AWS infrastructure monitoring
  - Detecting a brute-force attack
  - Monitoring Docker
  - File integrity monitoring
  - Blocking a malicious actor
  - Detecting unauthorized processes
  - Osquery integration
  - Network IDS integration
  - Detecting a Shellshock attack
  - Slack integration
  - Detecting suspicious binaries
  - Detecting and removing malware using Virus Total integration
  - Vulnerability Detector
  - Detecting malware using Yara integration Cisco IOS Configuration Basics

- ❑ Lab Workshop
  - Detect an SSH brute-force attack
  - Detect an RDP brute-force attack
  - Expose hiding processes
  - Detect filesystem changes
  - Change the rules
  - Survive a log flood
  - Detect and react to a Shellshock attack

- Keep watch for malicious command execution
- Catch suspicious network traffic
- Track down vulnerable applications

วิทยากร: อ.เอกฤทธิ์ ธรรมสถิต

- MASTER OF BUSINESS ADMINISTRATION (EXECUTIVE) DEGREE
  SASIN GRADUATE INSTITUTE OF BUSINESS ADMINISTRATION OF CHULALONGKORN UNIVERSITY
- MASTER OF SCIENCE, MAJOR IN INFORMATION
  Technology Faculty of Information Technology
  KING'S MONGKUT INSTITUTE OF TECHNOLOGY LADKRABANG
- BACHELOR OF SCIENCE
  KING'S MONGKUT INSTITUTE OF TECHNOLOGY NORTH BANGKOK
- DIPLOMA PROGRAM FOR MANAGEMENT
  KELLOGG – NORTHWESTERN UNIVERSITY, UNITED STATE OF AMERICA

Certificate:

- Microsoft Certified professional (MCP)
- Microsoft Certified Systems Administrator (MSCA)
- Microsoft Certified Systems Engineer (MSCE)
- Cisco Certified Network Associate (CCNA)
- Certificate of CompTIA Security+
- Certified Technical training CTT+
- Certified Ethical Hacker
- Certified Hacking Forensic Investigator
- Certified Wireless Network Administrator
- Certified Wireless Security Professional

จำนวนชั่วโมงในการฝึกอบรม: 2 วัน (12 ชั่วโมง)
ช่วงเวลาฝึกอบรม: 9.00 - 16.00 น.
กำหนดการอบรม: ตามตารางปฏิทินอบรมประจำปี https://www.career4future.com/trainingprogram
รูปแบบการอบรม: Onsite (Classroom)

ค่าลงทะเบียนอบรม: ท่านละ 13,000 บาท

* ราคาค่าลงทะเบียนอบรม ไม่รวมภาษีมูลค่าเพิ่ม
* สถาบันฯ เป็นหน่วยงานราชการ จึงไม่อยู่ในเกณฑ์ที่ต้องถูกหักภาษี ณ ที่จ่าย
* ค่าใช้จ่ายในการส่งบุคลากรเข้าอบรมทางวิชาชีพของบริษัทหรือห้างหุ้นส่วนนิติบุคคล สามารถนำไปลดหย่อนภาษีได้ 200%
* ขอสงวนสิทธิ์ในการเปลี่ยนแปลงกำหนดการ และปรับรูปแบบการอบรมตามความเหมาะสม
* ในการอบรม สถาบันฯ ขอสงวนสิทธิ์ ไม่บันทึกภาพวีดิโอ หรือบันทึกเสียง ตลอดระยะเวลาการอบรม เนื่องจากเป็นลิขสิทธิ์ร่วมระหว่างวิทยากรกับสถาบันฯ และเพื่อป้องกันการละเมิดข้อมูลส่วนบุคคล ตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล

สถานที่ฝึกอบรม:
สถาบันพัฒนาบุคลากรแห่งอนาคต
เลขที่ 73/1 อาคารสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (NSTDA) ชั้น 6
ถนนพระรามที่ 6 แขวงทุ่งพญาไท เขตราชเทวี กรุงเทพฯ 10400

วิธีการการสำรองที่นั่ง:
ติดต่อสำรองที่นั่งล่วงหน้า ในวัน-เวลาราชการ
โทรศัพท์: 0 2644 8150 ต่อ 81886, 81887
โทรสาร: 0 2644 8110
Website: www.career4future.com
E-mail: training@nstda.or.th