สมาคมประกันวินาศภัยไทย
Thai General Insurance Association

ที่ IT. 2 / 2564

12 มีนาคม 2564

เรื่อง เชิญเข้าร่วมอบรมหลักสูตร "SOC (Security Operation Centre) Operation"

เรียน กรรมการผู้จัดการ

สิ่งที่ส่งมาด้วย รายละเอียดหลักสูตร

ด้วยคณะกรรมการพัฒนาธุรกิจและวิชาการประกันภัย โดยชมรมไอทีประกันภัย (Insurance IT Club) ได้กำหนดจัด**อบรมหลักสูตร "SOC (Security Operation Centre) Operation"** ขึ้น โดยมีวัตถุประสงค์เพื่อให้ผู้เข้าร่วมอบรมมีความรู้ความเข้าใจเกี่ยวกับแนวทางในการจัดตั้งศูนย์เฝ้าระวังทางไซเบอร์ (SOC) รวมทั้งบทบาทและหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องในศูนย์ฯ ตลอดจนให้ผู้เข้าร่วมอบรมสามารถวิเคราะห์หาสาเหตุหรือตรวจสอบข้อมูลในระบบที่ถูกแก้ไขเปลี่ยนแปลงไปโดยไม่ได้รับอนุญาต รวมถึงช่องทางการบุกรุกหรือการเข้าถึงเครือข่ายและระบบสารสนเทศที่ผิดปกติได้ เพื่อนำไปสู่การแก้ไขปัญหาได้อย่างถูกต้องแม่นยำ ซึ่งการอบรมในครั้งนี้ได้รับเกียรติจาก อ.วัชรพล วงศ์อภัย บริษัท ACIS Professional Center จำกัด ซึ่งเป็นผู้เชี่ยวชาญในเรื่องดังกล่าวมาเป็นวิทยากร

การอบรมในครั้งนี้ จัดขึ้นระหว่าง***วันจันทร์ที่ 26 ถึงวันพุธที่ 28 เมษายน 2564 เวลา 09.00 – 16.00 น. ณ ห้องประชุม 501 ชั้น 5 สมาคมประกันวินาศภัยไทย ซอยสุขุมวิท 64/1 และอบรมผ่านระบบออนไลน์ (Google Meet)*** **(จำนวน 3 ครั้ง)** (รายละเอียดตามสิ่งที่ส่งมาด้วย)

ดังนั้น จึงใคร่ขอเรียนเชิญท่านพิจารณาส่งผู้แทนเข้าร่วมอบรมในครั้งนี้ บริษัทละ 2 ท่าน โดยไม่เสียค่าใช้จ่ายใดๆ ทั้งสิ้น และหากมีผู้สนใจเข้าร่วมอบรมเพิ่มต้องเสียค่าใช้จ่ายท่านละ 600 บาท โดยท่านสามารถเข้าไปลงทะเบียนได้ที่ https://forms.gle/KFUrhpTrrHaUKRy27 **ภายในวันศุกร์ที่ 16 เมษายน 2564** จักขอบคุณยิ่ง

จึงเรียนมาเพื่อโปรดพิจารณา

ขอแสดงความนับถือ

(นายชูชัย วชิรบรรจง)
รักษาการประธานชมรมไอทีประกันภัย

ฝ่ายวิชาการทั่วไป (ทศพล)
โทรศัพท์ 0-2108-8399 ต่อ 1104

QR Code สำหรับลงทะเบียน

25 ซอยสุขุมวิท 64/1 ถนนสุขุมวิท แขวงพระโขนงใต้ เขตพระโขนง กรุงเทพฯ 10260
25 Soi Sukhumvit 64/1, Sukhumvit Road, Phra Khanong Tai, Phra Khanong, Bangkok 10260, Thailand
+66 2108 8399 +66 2108 8398
general@tgia.org www.tgia.org

SOC (Security Operation Centre) Operation

หลักการและเหตุผล

ในการจัดตั้งหรือบริหารจัดการศูนย์เฝ้าระวังทางไซเบอร์ (SOC) ให้เกิดประโยชน์สูงสุดและมีประสิทธิ์ภาพนั้นจะต้องมีการวางแผนและออกแบบลักษณะของการให้บริการที่สอดคล้องกับรูปแบบการดำเนินธุรกิจ และการบริหารจัดการทั้งด้าน People ,Process ,Technology นั้นมีความซับซ้อนและยังเกิดความผิดพลาดหรือความไม่ต่อเนื่องในการดำเนินการได้ง่ายอีก ทั้งยังใช้งบประมาณในการดำเนินงาน ดังนั้นผู้ที่รับผิดชอบหรือผู้ที่จะทำการออกแบบจัดการศูนย์เฝ้าระวังทางไซเบอร์ (SOC) จะต้องมีองค์ความรู้ในด้านต่าง ๆ เป็นอย่างดี

ในหลักสูตรนี้จะพูดถึงการออกแบบในการจัดตั้งและบริหารจัดการ ศูนย์เฝ้าระวังทางไซเบอร์ (SOC) ทั้งในด้าน People ,Process ,Technology ให้มีความสอดคล้องและเหมาะสมต่อรูปแบบธุรกิจอีกทั้งสามารถดำเนินการได้อย่างมีประสิทธิ์ภาพ และช่วยลดงานหรืองบประมาณในการดำเนินการได้

วัตถุประสงค์

- มีความรู้ความเข้าใจในการจัดตั้งศูนย์เฝ้าระวังทางไซเบอร์ (SOC) ให้สอดคล้องต่อความต้องการของธุรกิจและงบประมาณ
- มีความรู้ความเข้าใจในการออกแบบแผนและรูปแบบการดำเนินงานได้อย่างเหมาะสม
- มีความรู้ความเข้าใจในการพัฒนาขีดความสามารถในศูนย์เฝ้าระวังทางไซเบอร์ (SOC) ได้อย่างมีประสิทธิ์ภาพ
- มีความรู้ความเข้าใจในการดำเนินงานในศูนย์เฝ้าระวังทางไซเบอร์ (SOC) ให้มีความต่อเนื่องและมีประสิทธิ์ภาพ

หลักสูตรนี้เหมาะสำหรับ

- Senior Security Analyst
- Operation Manager
- SOC Manager

ความรู้พื้นฐาน

- IT Management Level
- Basic Knowledge of Cybersecurity

เนื้อหาหลักสูตร

- Need for a Security Operations Centre (SOC)
- Building SOC
    - Components of an effective SOC
    - Define SOC Goal
    - SOC Functions
    - SOC Services
    - SOC Architecture
    - SOC Facilities

SOC (Security Operation Centre) Operation

- SOC GAP Analysis
- Sizing SOC
- Budgeting
- In-House SOC vs MSSP

- Risk Assessment & BIA Analysis
  - Identified Business Function and Critical Services
  - Review Company Infrastructure
  - Identified Threats and Vulnerability
  - Security Control Mapping and Log Source determination
- Use Case Development
  - Identified Risk Scenarios
  - Determine Log Sources
  - Use Case Development and Log Correlations
  - Deploy Use Case
- SOC Technology and Infrastructure
  - Identified Log Sources
  - Log Analysis (SIEM) Technology
  - Design for Security Operation Centre (SOC) Infrastructure
  - Design for Security Operation Centre (SOC) Capacity
    - Event per Second
    - Bandwidth
    - Logs Transmission
- SOC Roles and Responsibility
  - Design Operation team and Structure
  - SOC Organization Chart
  - SOC Team Job Description
    - SOC Manager
    - Security Analyst
      - Tier 1
      - Tier 2
      - Tier 3
    - Incident Response Team
  - SOC's Team Competency
- Security Analyst Skills and Certification
  - Technical Skill sets
  - Soft Skill
  - Training Courses
  - Useful Security Analyst Certification
  - Good Knowledge for Security Analyst
- Vulnerability Management
  - Vulnerability Management

- CVSSv3 Scoring
- Incident Prioritization
  - Impact Analysis
  - Incident Severity
- Incident Categorization

- SOC Operation Management
  - Design resource for Daily Operation
  - Shift Rotation
  - Daily Checklist
  - Design for SOC Procedure
  - Design KPI
  - Design SLA
  - Design OLA
- SOC Processes
  - Building SOC Process & Procedure
  - Design for Communication
  - Design Workflow and Documentation
  - Incident Management Process
- Deliverable
  - Type of Report
    - Incident Report
    - Daily Report
    - Monthly Report
  - Design for SOC Report
- Introduction of Incident Management
  - Incident Response vs. Incident Handling
  - Incident Management Tools
- Incident Handling Methodology
  - Prepare
  - Detect & Analysis
  - Containment, Eradication, Recovery
  - Post-Incident