หลักสูตร CompTIA Cybersecurity Analyst (CySA+)

รายละเอียดหลักสูตร

เมื่อผู้โจมตีบนโลกออนไลน์เรียนรู้ที่จะหลบเลี่ยงโซลูชันที่ใช้วิธีการแบบดั้งเดิม เช่น ไฟร์วอลล์ ทักษะการวิเคราะห์ที่ใช้ในอุตสาหกรรมความปลอดภัยด้านไอทีจึงมีความสำคัญมากขึ้นสำหรับองค์กรส่วนใหญ่

โดยใบประกาศนียบัตรการรับรองความรู้ CompTIA Cybersecurity Analyst (CySA+) คลอบคลุมทักษะการวิเคราะห์พฤติกรรม และการต่อสู้กับมัลแวร์และภัยคุกคามถาวรขั้นสูง (APTs) ซึ่งส่งผลให้ผู้วิเคราะห์สามารถมองเห็นภัยคุกคามได้ดีขึ้น สำหรับใบประกาศนียบัตร CompTIA CySA + เหมาะสำหรับผู้เชี่ยวชาญด้านไอทีที่ต้องการทักษะในการวิเคราะห์ความปลอดภัย ดังต่อไปนี้

- ดำเนินการวิเคราะห์ข้อมูล และตีความหมายเพื่อระบุช่องโหว่ของภัยคุกคาม รวมถึงความเสี่ยงต่อองค์กร
- กำหนดค่า และใช้เครื่องมือตรวจจับภัยคุกคาม
- รักษาความปลอดภัย และป้องกันแอปพลิเคชัน และระบบภายในองค์กร

ทักษะที่ได้รับ

- ด้านการจัดการภัยคุกคาม
  ใช้เทคนิคการสอดแนมสิ่งแวดล้อมโดยใช้เครื่องมือที่เหมาะสม สามารถวิเคราะห์ผลลัพธ์ พร้อมตอบสนองและสามารถนำไปใช้งานตามข้อแนะนำได้
- ด้านการจัดการความเสี่ยง
  ใช้กระบวนการจัดการช่องโหว่ และวิเคราะห์ผลลัพธ์ของการสแกน
- ด้านสถาปัตยกรรมในการรักษาความปลอดภัย และชุดเครื่องมือ
  สามารถใช้ข้อมูลเพื่อแนะนำการแก้ไขปัญหาด้านความปลอดภัยที่เกี่ยวข้องกับข้อมูลประจำตัว และการจัดการการเข้าถึง และแนะนำกลยุทธ์การใช้งานในขณะที่อยู่ร่วมกันในวงจรการพัฒนาซอฟต์แวร์ (SDLC)
- ด้านการตอบโต้เหตุการณ์บนโลกไซเบอร์
  สามารถแยกแยะข้อมูลภัยคุกคาม เพื่อกำหนดผลกระทบของเหตุการณ์ และเตรียมชุดเครื่องมือที่เหมาะสม, สร้างกลยุทธ์การสื่อสาร พร้อมแนวทางปฏิบัติในการตอบโต้

คุณสมบัติของผู้เข้าอบรม

บุคลากรที่มีประสบการณ์ด้านเทคนิคการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศอย่างน้อย 3 - 4 ปี

สายงานที่มีความเกี่ยวข้องกับ CompTIA Cybersecurity Analyst (CySA+)

- นักวิเคราะห์ความปลอดภัยด้านไอที (IT Security Analyst)
- นักวิเคราะห์ ศูนย์ปฏิบัติการรักษาความปลอดภัย (Security Operations Center (SOC) Analyst)
- นักวิเคราะห์ช่องโหว่ (Vulnerability Analyst)
- ผู้เชี่ยวชาญด้านความปลอดภัยทางไซเบอร์ (Cybersecurity Specialist)
- นักวิเคราะห์ข้อมูลภัยคุกคาม (Threat Intelligence Analyst)
- วิศวกรรักษาความปลอดภัย (Security Engineer)
- นักวิเคราะห์ความปลอดภัยทางไซเบอร์ (Cybersecurity Analyst)

ระยะเวลาการอบรม

4 วัน (24 ชั่วโมง)

รายละเอียดหลักสูตร

ที่	เนื้อหาหลักสูตร
1	**Threat Management**
	1.1 การใช้เครื่องมือ (Tools) และเทคนิคที่เหมาะสมในการเก็บรวบรวมข้อมูลเป้าหมาย เช่น NMAP, IDS/IPS, Syslog
	1.2 การวิเคราะห์ผลระบบเครือข่ายที่ได้จากการเก็บรวบรวมข้อมูล เช่น Event log, IDS Report, Firewalls log
	1.3 วิธีการป้องกันและรับมือภัยคุกคามทางระบบเครือข่ายอย่างเหมาะสม เช่น Network Isolation, Honeypot, Hardening
	1.4 อธิบายวัตถุประสงค์ของการรักษาความปลอดภัยทางสารสนเทศภายในองค์กร
2	**Vulnerability Management**
	2.1 ขั้นตอนการบริหารจัดการช่องโหว่ด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ
	วิเคราะห์ผลลัพธ์ที่ได้จากการสแกนหาช่องโหว่
	เปรียบเทียบและหาความแตกต่างของช่องโหว่พื้นฐานกับช่องโหว่ที่พบภายในองค์กร
3	**Cyber Incident Response**
	แยกความแตกต่างระหว่างภัยคุกคามกับพฤติกรรมที่ส่งผลกระทบต่อ Incident เช่น Threat classification

ที่	เนื้อหาหลักสูตร
	เลือกและใช้เครื่องมือที่เหมาะสมในการรวบรวมพยานหลักฐานทางดิจิทัล เช่น Forensics kit, Forensic investigation suite
	ความสำคัญของการสื่อสารระหว่างเกิดเหตุการณ์ Incident เช่น การสื่อสารกับ Stakeholder, วัตถุประสงค์ของการสื่อสาร (Purpose of communication processes), บทบาทและความรับผิดชอบ (Role-based responsibilities)
	วิเคราะห์อาการที่พบบ่อยเพื่อเลือกทางเลือกที่ดีที่สุดในการตอบสนองต่อเหตุการณ์ Incident เช่น Bandwidth consumption, Memory consumption, Unauthorized software, Unauthorized privileges, Memory overflows
	สรุปรวบรวม Incident ที่เกิดขึ้นและขั้นตอนหลังจากเกิด Incident แล้ว เช่น Reverse engineering, Patching, Reconstruction/reimage, Update incident response plan
4	**Security Architecture and Tool Sets**
	อธิบายความสัมพันธ์ของกรอบการทำงาน (Frameworks), นโยบาย (Policies), การควบคุม (Controls), ขั้นตอนการปฏิบัติงาน (Procedures) เช่น NIST, ISO, COBIT, ITIL, Password policy, Physical controls, Control testing procedures
	ใช้ข้อมูลเพื่อบรรเทาปัญหาด้านความปลอดภัยทางสารสนเทศ เช่น Security issues associated with context-based authentication, Security issues associated with identities, Security issues associated with federation and single sign-on
	ตรวจสอบสถาปัตยกรรมความปลอดภัยทางเทคโนโลยีสารสนเทศและนำข้อเสนอแนะมาปรับปรุงแผนการดำเนินงานให้ดีขึ้น เช่น Security data analytics, Defense in depth
	ใช้แอปพลิเคชันที่ปลอดภัยในขณะที่อยู่ในช่วงพัฒนาโปรแกรม (SDLC) เช่น Best practices during software development, Secure coding best practices
	เปรียบเทียบและหาความแตกต่างของวัตถุประสงค์พร้อมเหตุผลในการใช้เครื่องมือที่หลากหลายด้านความปลอดภัยทางเทคโนโลยีสารสนเทศ เช่น การเลือกใช้เครื่องมือสำหรับรวบรวมข้อมูล (Collective), การใช้เครื่องมือสำหรับป้องกัน (Preventative), การใช้เครื่องมือสำหรับวิเคราะห์ (Analytical), การใช้เครื่องมือสำหรับหาช่องโหว่ (Exploit), การใช้เครื่องมือสำหรับการตรวจพิสูจน์พยานหลักฐานทางดิจิทัล (Forensics)