หลักสูตร CompTIA Advanced Security Practitioner (CASP+)

รายละเอียดหลักสูตร

ใบประกาศนียบัตร CASP+ เป็นสมรรถนะขั้นสูงในเรื่องการบริหารจัดการความเสี่ยง การดำเนินด้านความปลอดภัยขององค์กรและสถาปัตยกรรม การวิจัยและความร่วมมือ และการบูรณาการด้านความปลอดภัยขององค์กร สำหรับผู้ที่สนใจหลักสูตร ใบประกาศนียบัตร CASP+ ควรมีความรู้ความเข้าใจดังต่อไปนี้

- สามารถขยายความปลอดภัยของโดเมนในองค์กรเพื่อรวมการบริหารจัดการและแนวคิดสถาปัตยกรรม เทคนิค และข้อกำหนดได้
- ให้ความสำคัญกับการวิเคราะห์ความเสี่ยงโดยการตีความข้อมูลแนวโน้ม และการคาดการณ์การป้องกันทางไซเบอร์ เพื่อให้บรรลุเป้าหมายทางธุรกิจ
- ขยายหัวข้อการควบคุมความปลอดภัย ให้ครอบคลุมอุปกรณ์มือถือ และอุปกรณ์ขนาดเล็ก รวมถึงช่องโหว่ของซอฟต์แวร์
- ครอบคลุมการรวมเทคโนโลยีคลาวด์ และการจำลองเสมือน เข้ากับสถาปัตยกรรมขององค์กรได้อย่างปลอดภัย
- สามารถรวมการใช้เทคนิคการเข้ารหัส เช่น Block chain- Crypto currency และการเข้ารหัสอุปกรณ์มือถือ

ทักษะที่ได้รับ

- ด้านการจัดการความเสี่ยง
  สามารถวิเคราะห์ความเสี่ยง และกรอบความปลอดภัยที่มาพร้อมกับภัยคุกคามในอุตสาหกรรมแบบเฉพาะได้ เข้าใจข้อกำหนดขององค์กร และบริหารกลยุทธ์ในการลดความเสี่ยงได้
- ด้านการดำเนินงานด้านความปลอดภัยขององค์กร
  สามารถตอบสนองเหตุการณ์ต่างๆ ที่เกิดขึ้น และมีความรู้ในการกระบวนการกู้คืนข้อมูล ดำเนินการประเมินความปลอดภัยโดยใช้เครื่องมือที่เหมาะสม
- การบูรณาการด้านเทคนิคความปลอดภัยขององค์กร
  สามารถรวบรวมโฮสต์ ที่เก็บข้อมูล เครือข่าย และแอปพลิเคชันเข้ากับสถาปัตยกรรมองค์กรได้อย่างปลอดภัยโดยใช้เทคโนโลยีคลาวด์ และระบบเสมือนจริง
- ด้านการวิจัย การพัฒนา และความร่วมมือ
  สามารถใช้การวิจัย เพื่อกำหนดแนวโน้มของอุตสาหกรรม และผลกระทบที่มีต่อองค์กร

คุณสมบัติของผู้เข้าอบรม

มีประสบการณ์ในการบริหารเทคโนโลยีสารสนเทศอย่างน้อย 10 ปี รวมถึงมีประสบการณ์ด้านความปลอดภัยในเชิงปฏิบัติการอย่างน้อย 5 ปี

สายงานที่มีความเกี่ยวข้องกับ CompTIA Advanced Security Practitioner (CASP+)

- สถาปนิกด้านการรักษาความปลอดภัย (Security Architect)
- นักวิเคราะห์เชิงผู้นำด้านเทคโนโลยี (Technical Lead Analyst)
- วิศวกรด้านความปลอดภัยของโปรแกรม (Application Security Engineer)
- วิศวกรด้านความปลอดภัย (Security Engineer)

ระยะเวลาการอบรม

4 วัน (24 ชั่วโมง)

รายละเอียดหลักสูตร

ที่	เนื้อหาหลักสูตร
1	**Risk Management**
	อิทธิพลของความเสี่ยงด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศที่มีต่อธุรกิจและอุตสาหกรรม เช่น ปัจจัยภายใน, ปัจจัยภายนอก, การเปลี่ยนรูปแบบ (Model) ทางธุรกิจ
	เปรียบเทียบและแยกความแตกต่างระหว่างความปลอดภัยทางเทคโนโลยีสารสนเทศ, นโยบายด้านความเป็นส่วนตัว, ขั้นตอนการปฏิบัติงานให้เป็นไปตามความต้องการขององค์กร เช่น Memorandum of understanding (MOU), Service-level agreement (SLA), Non-disclosure agreement (NDA), Incident response
	กลยุทธ์การบรรเทาความเสี่ยง (risk mitigation) เช่น กระบวนการบริหารจัดการความเสี่ยง (Risk management processes), ROI, RTO, RPO, MTTR, MTBF
	วิเคราะห์ตัวชี้วัด (Metric) ด้านความเสี่ยงของความปลอดภัยทางเทคโนโลยีสารสนเทศที่ส่งผลกระทบต่อองค์กร เช่น KPIs, KRIs, Metrics and attributes to ensure meet business needs
2	**Enterprise Security Architecture**
	วิเคราะห์ภาพรวมและสถาปัตยกรรมของระบบเครือข่ายให้ตรงกับความต้องการด้านความปลอดภัยทางเทคโนโลยีสารสนเทศ เช่น ความปลอดภัยของอุปกรณ์ภายในระบบเครือข่าย, การออกแบบระบบเครือข่ายให้มีความปลอดภัย, การตั้งค่าความปลอดภัยให้กับอุปกรณ์ภายในระบบเครือข่าย
	การตั้งค่าความปลอดภัยให้กับอุปกรณ์ต่าง ๆ เช่น Trusted OS, Endpoint security software, Host hardening, Boot loader protections
	การตั้งค่าความปลอดภัยให้กับอุปกรณ์เคลื่อนที่และคอมพิวเตอร์แบบ Small Form Factor เช่น Enterprise mobility management, Security implications/privacy concerns, Wearable technology
	การป้องกันช่องโหว่ (Vulnerability) ของซอฟต์แวร์อย่างเหมาะสม เช่น การป้องกัน SQL injection, การป้องกัน Buffer overflow, การป้องกัน Click-jacking

ที่	เนื้อหาหลักสูตร
3	**Enterprise Security Operations**
	ประเมินความปลอดภัยโดยการใช้เครื่องมือที่เหมาะสม เช่น Malware sandboxing, Penetration testing, Vulnerability assessment
	วิเคราะห์สถานการณ์หรือผลลัพธ์และเลือกเครื่องมือที่เหมาะสมสำหรับการประเมินความปลอดภัย เช่น Port scanners, Vulnerability scanners, Protocol analyzer, Command line tools
	การตอบสนองต่อ Incident และขั้นตอนการกู้คืน (Recovery) เช่น E-discovery, Incident and emergency response, Incident response support tools
4	**Technical Integration of Enterprise Security**
	การผสาน (Integrate) ระบบคอมพิวเตอร์เพื่อสร้างความปลอดภัยทางเทคโนโลยีสารสนเทศให้กับองค์กร เช่น Data security considerations, Resources provisioning and deprovisioning, Network secure segmentation and delegation, Security and privacy considerations of storage integration
	การผสานระบบคลาวด์และระบบเสมือน (Virtualization) เพื่อสร้างความปลอดภัยทางเทคโนโลยีสารสนเทศให้กับองค์กร เช่น Cloud augmented security services, Security advantages and disadvantages of virtualization
	การผสานและแก้ไขปัญหาของระบบการพิสูจน์ตัวตน (Authentication and Authorization) เพื่อสร้างความปลอดภัยทางเทคโนโลยีสารสนเทศให้กับองค์กร เช่น Single sign-on, 802.1x, OpenID, LDAP, AD, RADIUS
	เทคนิคการเข้ารหัส (Cryptographic) เช่น Hashing, Digital signature, Steganography, Cryptocurrency, PKI
	เลือกเครื่องมือที่เหมาะสมในการควบคุมความปลอดภัยด้านการสื่อสารและการทำงานร่วมกัน เช่น Remote access, Instant messaging, Email, Social media
5	**Research, Development and Collaboration**
	ประยุกต์ใช้งานวิจัยและทฤษฎีเพื่อวิเคราะห์แนวโน้มของอุตสาหกรรมที่ส่งผลกระทบต่อองค์กร เช่น Threat intelligence, Research security implications of emerging business tools
	การออกแบบวงจรการพัฒนาเทคโนโลยี (Technology Life Cycle) ให้มีความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ เช่น Systems development life cycle, Software development life cycle, Asset management
	อธิบายถึงความสำคัญของความเกี่ยวข้องและความมีปฏิสัมพันธ์ระหว่างหน่วยธุรกิจที่ส่งผลต่อความสำเร็จในเรื่องความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ