หลักสูตรการฝึกอบรม Cyber Security

หลักสูตรการฝึกอบรมหนึ่งวันสำหรับผู้เชี่ยวชาญด้าน IT ในองค์กรที่มีผลกระทบต่อ **Cyber Security** ได้รับการพัฒนาขึ้นโดยอ้างอิงจากความต้องการด้าน **Future Skills Set (FSS)** ในอุตสาหกรรมดิจิทัลและความมั่นคงแห่งชาติ รวมถึงประสบการณ์ความเชี่ยวชาญของวิทยากร (**นฤดม รุ่งสิริวงศ์**)

หลักสูตรนี้เน้นทักษะสำคัญ ได้แก่ **สถาปัตยกรรมด้านความปลอดภัย (Security Architecture), การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Management), การประเมินความเสี่ยงและการตรวจสอบช่องโหว่ของระบบ (Vulnerability Testing)** และ **ระบบประมวลผลแบบคลาวด์ (Cloud Computing)**

กลุ่มเป้าหมาย: ผู้เชี่ยวชาญด้าน IT ในองค์กร (เช่น สถาปนิกระบบ นักพัฒนา และผู้จัดการด้านความมั่นคงปลอดภัย) ที่รับผิดชอบดูแลระบบที่มีความสำคัญต่อความมั่นคงแห่งชาติ

หัวข้อที่ 1: ธรรมาภิบาลเชิงกลยุทธ์และการจัดการความเสี่ยง

➔ สถาปัตยกรรมด้านความปลอดภัย (Security Architecture), การประเมินและตรวจสอบระบบความปลอดภัย (Security Assessment), การจัดการโครงสร้างด้านความปลอดภัย (Security Configuration) และ การบริหารจัดการด้านการกู้คืนระบบ (Disaster Recovery Management)

หัวข้อ	ผลลัพธ์การเรียนรู้/รายละเอียดสำคัญ
ภูมิทัศน์ภัยคุกคามความมั่นคงแห่งชาติ	การวิเคราะห์ภัยคุกคามไซเบอร์ที่มุ่งเป้าไปที่โครงสร้างพื้นฐานสำคัญ และบทบาทของผู้เชี่ยวชาญด้าน IT ในองค์กรต่อความมั่นคงของประเทศ
สถาปัตยกรรมความปลอดภัยที่อิงความเสี่ยง	การประยุกต์ใช้แนวทางที่อิงตามความเสี่ยงเพื่อรักษาความมั่นคงปลอดภัยที่สอดคล้องกับ **NIST Cybersecurity Framework** เพื่อเชื่อมโยงกลยุทธ์ทางธุรกิจกับการดำเนินงานด้านความปลอดภัย
การประเมินและตั้งค่าความปลอดภัย	ระเบียบวิธีปฏิบัติสำหรับการทำ **Security Assessment** และการจัดการ **Security Configuration** ที่มีประสิทธิภาพและรัดกุมทั่วทั้งองค์กร
การบริหารจัดการความต่อเนื่องทางธุรกิจและการกู้คืนระบบ	การพัฒนาแผนเชิงกลยุทธ์สำหรับ **Disaster Recovery Management (การบริหารจัดการด้านการกู้คืนระบบ)** เพื่อให้มั่นใจว่าระบบยังคงสามารถใช้งานได้หลังเกิดเหตุการณ์ไม่คาดคิด

หัวข้อที่ 2: ความมั่นคงปลอดภัยในสภาพแวดล้อม Cloud และ Hybrid

➔ Cloud Computing, Infrastructure Design

หัวข้อ	ผลลัพธ์การเรียนรู้/รายละเอียดสำคัญ
กลยุทธ์ Cloud และ Hybrid/Multi-Cloud	ภาพรวมของการนำ **Cloud Computing (การประมวลผลแบบคลาวด์ที่สามารถเข้าถึงระบบและทรัพยากรได้จากทุกที่ทุกเวลา)** มาใช้ และการย้ายแอปพลิเคชันจากระบบ On-Premise
การลดความเสี่ยงใน Hybrid Cloud	การวิเคราะห์เชิงลึกเกี่ยวกับความเสี่ยงที่เกี่ยวข้องกับ Hybrid Cloud โดยอาศัยความเชี่ยวชาญของวิทยากรในฐานะผู้มีส่วนร่วมใน **Cloud Security Alliance (CSA)**
ข้อกำหนดการเชื่อมต่อ Cloud ที่ปลอดภัย	การทำความเข้าใจและการประยุกต์ใช้ข้อกำหนดสำหรับการเชื่อมต่อที่ปลอดภัยของ Hybrid Cloud (**Secure Connection Requirements of Hybrid Cloud**)
การออกแบบและปรับใช้โครงสร้างพื้นฐานที่ปลอดภัย	แนวทางปฏิบัติที่ดีสำหรับ **Infrastructure Design (การออกแบบโครงสร้างพื้นฐานของระบบเครือข่าย)** และ **Infrastructure Deployment (การปรับใช้โครงสร้างพื้นฐาน)** เพื่อรับรองความปลอดภัยในระดับสากล

หัวข้อที่ 3: การพัฒนาซอฟต์แวร์ดิจิทัลที่ปลอดภัย (DevSecOps)

➔ การประเมินความเสี่ยงและตรวจสอบช่องโหว่ของระบบ (Vulnerability Testing), การพัฒนาซอฟต์แวร์แบบ Agile (Agile Software Development), การออกแบบและพัฒนาแอปพลิเคชัน (Application Development) และ การทดสอบซอฟต์แวร์ (Software Testing)

หัวข้อ	ผลลัพธ์การเรียนรู้/รายละเอียดสำคัญ
การบูรณาการความปลอดภัยเข้าสู่ SDLC	การสร้างกระบวนการพัฒนาซอฟต์แวร์ที่ปลอดภัยสำหรับแนวทางการพัฒนาซอฟต์แวร์แบบ **Agile Software Development**
Threat Modeling ภาคบังคับ	การดำเนินการตามกระบวนการ **Threat Modeling** ในระหว่างขั้นตอนการออกแบบซอฟต์แวร์และระบบ
แนวปฏิบัติด้านความปลอดภัยของแอปพลิเคชัน	การนำความรู้ไปใช้ในการรวบรวมข้อกำหนดด้านความปลอดภัย การให้คำปรึกษาด้านการออกแบบที่ปลอดภัย และการตรวจสอบโค้ดให้มีความปลอดภัย

การตรวจสอบและยืนยันความปลอดภัย	เทคนิคสำหรับ **Vulnerability Testing (การตรวจสอบช่องโหว่)** และ **Application Penetration Testing** รวมถึงการตรวจจับการบุกรุกแอปพลิเคชัน (**Application Intrusion Detection**) และ **Software Testing (การทดสอบซอฟต์แวร์)** ที่ครอบคลุม

หัวข้อที่ 4: การตรวจจับและการตอบสนองภัยคุกคามขั้นสูง

➔ การบริหารจัดการภัยคุกคามต่อระบบ (Cyber Incident Management), Data Science, Security Assessment, Cyber Security

หัวข้อ	ผลลัพธ์การเรียนรู้/รายละเอียดสำคัญ
การตรวจจับภัยคุกคามแบบเรียลไทม์ด้วย Data Science	การวางรากฐานสำหรับการตรวจจับภัยคุกคามอัตโนมัติแบบเรียลไทม์ที่มีความแม่นยำ โดยใช้ **AI/ML** และการประยุกต์ใช้ **Data Science (การวิเคราะห์และใช้ข้อมูลขนาดใหญ่)** เพื่อการตรวจจับรูปแบบและความสัมพันธ์ของข้อมูล
แนวปฏิบัติที่ดีที่สุดของ Security Operations Center (SOC)	การทบทวนการดำเนินงานของบริการบริหารความเสี่ยง (Managed Risk) และบริการด้านความมั่นคงปลอดภัยสารสนเทศ รวมถึงการบำรุงรักษาและปรับปรุงกระบวนการ **ISMS** สำหรับการเฝ้าระวังและการปฏิบัติการด้านความปลอดภัย
Cyber Incident Management	สมรรถนะในการบริหารจัดการและรับมือกับภัยคุกคามต่อระบบ รวมถึงบทเรียนจากการประสานงานในกลุ่มแบ่งปันข้อมูล เช่น **TB-CERT**
บทบาทสถาปนิก IT ในฐานะที่ปรึกษาด้านความปลอดภัย	การแบ่งปันความรู้และบทบาทที่ปรึกษาด้านความมั่นคงปลอดภัยไซเบอร์ (**Cybersecurity Advisory**) แก่ทีมพัฒนาซอฟต์แวร์ ซึ่งเป็นสมรรถนะสำคัญด้าน Cyber Security