ที่ อว 6001/ว.5736

26 มิถุนายน 2568

เรื่อง ขอเชิญส่งบุคลากรเข้าร่วมการฝึกอบรม หลักสูตรด้านเทคโนโลยีสารสนเทศและการจัดการขั้นสูง ประจำปี 2568

เรียน อธิบดีกรมพัฒนาสังคมและสวัสดิการ

สิ่งที่ส่งมาด้วย แผ่นพับแนะนำหลักสูตร

ด้วย สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.) โดยสถาบันพัฒนาบุคลากรแห่งอนาคต มีกำหนดจัดฝึกอบรม หลักสูตรด้านเทคโนโลยีสารสนเทศและการจัดการขั้นสูง ประจำปี 2568 ดังนี้

1. หลักสูตรศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ (Security Operations Center: SOC) รุ่นที่ 5 อบรมระหว่างวันที่ 22 - 25 กรกฎาคม 2568 ณ โรงแรมเซ็นจูรี่ พาร์ค กรุงเทพ โดยมีเนื้อหามุ่งเน้นการเรียนรู้แนวทางการจัดตั้งศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยี สารสนเทศ และฝึกปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ด้วยซอฟต์แวร์ในระดับแนวหน้า เพื่อให้สามารถนำไปปฏิบัติได้จริงด้วยตนเอง ศึกษารายละเอียดเพิ่มเติมได้ที่ www.career4future.com/soc

2. หลักสูตรฝึกอบรมเชิงปฏิบัติการ การทดสอบเจาะระบบและความมั่นคงปลอดภัยด้านเว็บแอปพลิเคชัน รุ่นที่ 2 (Web Application Hacking and Security: WAHS) อบรมระหว่างวันที่ 6 - 8 สิงหาคม 2568 ณ โรงแรมเซ็นจูรี่ พาร์ค กรุงเทพ โดยมีเนื้อหามุ่งเน้นการตรวจสอบช่องโหว่ (Vulnerability Assessment) และการทดสอบเจาะระบบ (Penetration Testing) เว็บแอปพลิเคชัน โดยใช้เครื่องมือในการตรวจสอบแบบเดียวกับแฮ็กเกอร์ (Hacker) แต่เป็นการทดสอบระบบแบบมีจริยธรรมและถูกกฎหมาย เพื่อช่วยค้นหาและเตรียมป้องกันการบุกรุกได้อย่างมีประสิทธิภาพ ศึกษารายละเอียดเพิ่มเติมได้ที่ www.career4future.com/wahs

6. หลักสูตรมาตรฐานการบริหารจัดการความมั่นคงปลอดภัยบนระบบคลาวด์ตามมาตรฐาน CSA 4.x และ ISO/IEC 27001:2022 (Cloud Security Standard) รุ่นที่ 6 อบรมระหว่างวันที่ 13 - 15 สิงหาคม 2568 ณ โรงแรมเซ็นจูรี่ พาร์ค กรุงเทพ เพื่อมุ่งเน้นมุ่งเน้นการบริหารจัดการระบบงานให้มีความมั่นคงปลอดภัยและสอดคล้องตามมาตรฐาน CSA 4.x และ ISO/IEC 27001:2022 ในการรักษาความมั่นคงปลอดภัยด้านระบบสารสนเทศ ที่นำไปติดตั้งและใช้งานบนคลาวด์ ศึกษารายละเอียดเพิ่มเติมได้ที่ www.career4future.com/css

4. หลักสูตรฝึกอบรมเชิงปฏิบัติการ การตรวจสอบช่องโหว่และการทดสอบเจาะระบบ รุ่นที่ 2 (Vulnerability Assessment and Penetration Testing: VAPT) อบรมระหว่างวันที่ 20 - 22 สิงหาคม 2568 ณ โรงแรมเซ็นจูรี่ พาร์ค กรุงเทพ เพื่อให้ผู้เข้าร่วมอบรมมีความเข้าใจในการตรวจสอบช่องโหว่ (Vulnerability Assessment) และทดสอบเจาะระบบ (Penetration Testing) ระบบงานสารสนเทศรูปแบบต่าง ๆ พร้อมการทำรายงานที่ถูกต้อง โดยฝึกปฏิบัติในการตรวจสอบจากสถานการณ์จำลอง ศึกษารายละเอียดเพิ่มเติมได้ที่ www.career4future.com/vapt

/5. หลักสูตร ...

สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ
๑๑๑ อุทยานวิทยาศาสตร์ประเทศไทย ถนนพหลโยธิน ตำบลคลองหนึ่ง อำเภอคลองหลวง จังหวัดปทุมธานี ๑๒๑๒๐
โทรศัพท์ ๐ ๒๕๖๔ ๗๐๐๐ โทรสาร ๐ ๒๕๖๔ ๗๐๐๐-๒

National Science and Technology Development Agency
111 Thailand Science Park, Phahonyothin Road, Khlong Nueng, Khlong Luang, Pathum thani 12120, Thailand
Tel +66 2564 7000 Fax +66 2564 7000-2 http://www.nstda.or.th

5. หลักสูตรฝึกอบรมเชิงปฏิบัติการ การบริหารจัดการความต่อเนื่องทางธุรกิจตามมาตรฐานสากล ISO 22301:2019 รุ่นที่ 6 (Business Continuity Management Standard: BCS) อบรมระหว่างวันที่ 27 - 29 สิงหาคม 2568 ณ โรงแรมเซ็นจูรี่ พาร์ค กรุงเทพ โดยมีเนื้อหามุ่งเน้นการเตรียมความพร้อมเรื่องการกู้คืนระบบงานและการรับมือกับเหตุการณ์หยุดชะงักหรือสภาวะวิกฤติ เพื่อให้เกิดความต่อเนื่องในกระบวนการบริหารจัดการงานตามมาตรฐาน ISO 22301:2019 พร้อมทั้งฝึกปฏิบัติกับกรณีศึกษาที่สามารถนำกลับไปประยุกต์ใช้งานได้จริงในองค์กร ศึกษารายละเอียดเพิ่มเติมได้ที่ www.career4future.com/bcs

6. หลักสูตรการบริหารจัดการและการรับมือกับภัยคุกคามทางไซเบอร์ รุ่นที่ 4 (Cyber Security Incident Management) อบรมระหว่างวันที่ 8 - 11 กันยายน 2568 ณ โรงแรมเซ็นจูรี่ พาร์ค กรุงเทพ เพื่อมุ่งเน้นมุ่งเน้นการเตรียมความพร้อมในการจัดตั้งทีมบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยเพื่อรับมือจากภัยคุกคามทางไซเบอร์จนถึงการกู้คืนระบบกลับคืน ศึกษารายละเอียดเพิ่มเติมได้ที่ www.career4future.com/csm

ในการนี้ สถาบันฯ จึงขอเรียนเชิญท่านหรือส่งบุคลากรในสังกัดเข้าร่วมการฝึกอบรมในหลักสูตรดังกล่าว โดยมอบหมายให้ นายนิพัฒน์ เอี่ยมสมบูรณ์ เป็นผู้ประสานงาน หมายเลขโทรศัพท์ 0 2644 8150 ต่อ 8189 หรือ 08 9777 7492 ไปรษณีย์อิเล็กทรอนิกส์ npd@nstda.or.th ทั้งนี้ ผู้เข้าร่วมอบรมจากหน่วยงานราชการสามารถเบิกค่าลงทะเบียนจากต้นสังกัดได้ตามระเบียบกระทรวงการคลัง และไม่ถือเป็นวันลาเมื่อได้รับการอนุมัติจากผู้บังคับบัญชา และค่าใช้จ่ายในการส่งบุคลากรเข้าอบรมของบริษัทหรือห้างหุ้นส่วนนิติบุคคลสามารถนำไปลดหย่อนภาษีได้ 200%

จึงเรียนมาเพื่อโปรดพิจารณา

หนังสือนี้ใช้ลายมือชื่ออิเล็กทรอนิกส์ซึ่งมีผลใช้บังคับได้

ขอแสดงความนับถือ

(นายอดิสร เตือนตรานนท์)
ผู้ช่วยผู้อำนวยการ
ปฏิบัติการแทนผู้อำนวยการ
สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ

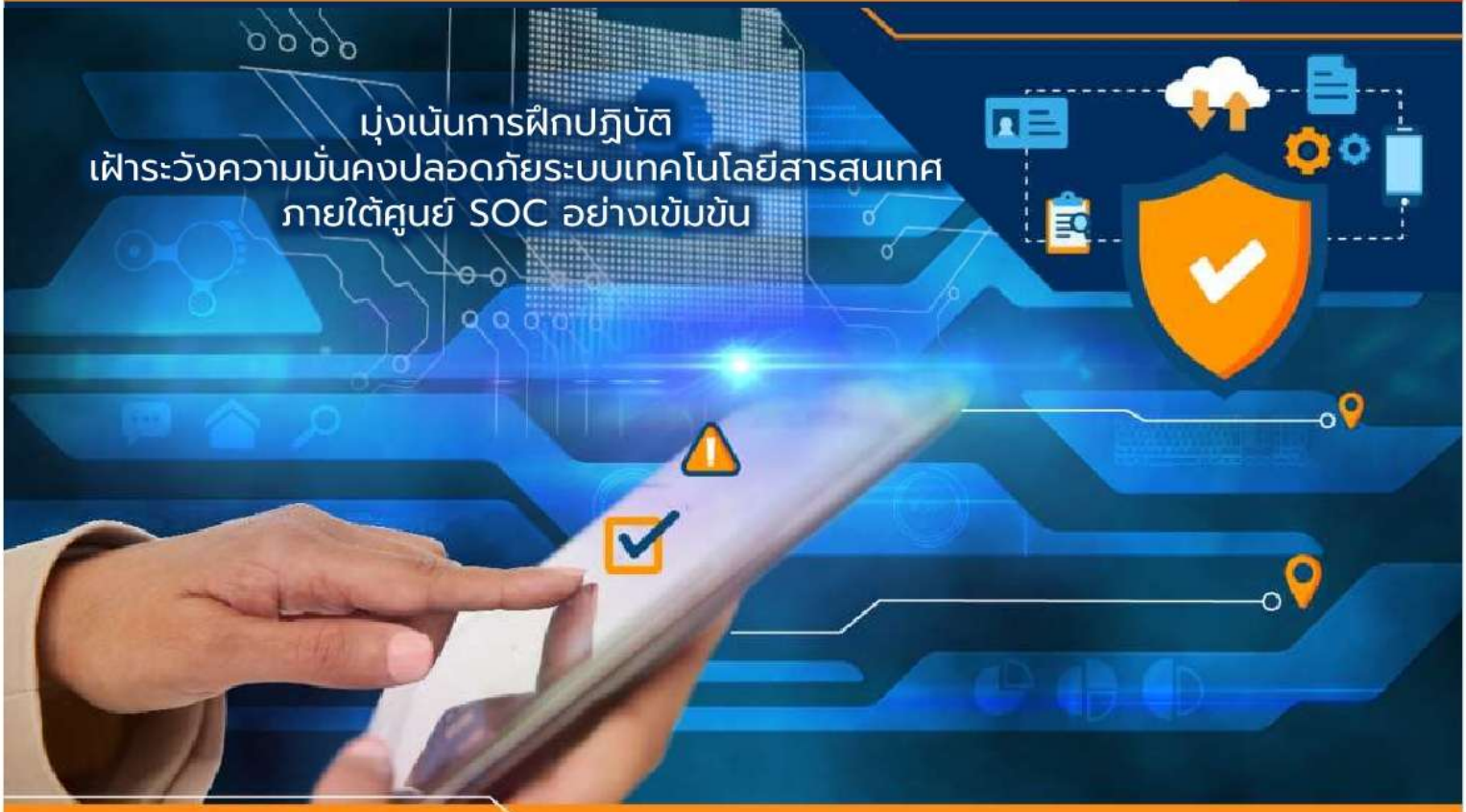
สำนักงานกลาง
สถาบันพัฒนาบุคลากรแห่งอนาคต
โทรศัพท์ 0 2644 8150 ต่อ 81891 (นิพัฒน์)
โปรษณีย์อิเล็กทรอนิกส์ nipat.iam@nstda.or.th

Career for the Future Academy
สถาบันพัฒนาบุคลากรแห่งอนาคต

SOC

Security Operations Center

หลักสูตร
ศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ **รุ่นที่ 5**



Key Highlights

- เรียนรู้แนวทางการจัดตั้งศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ กับวิทยากรผู้ทรงคุณวุฒิด้านความมั่นคงปลอดภัยระบบสารสนเทศระดับประเทศ
- เจาะลึกกระบวนการปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ
- ฝึกปฏิบัติกับซอฟต์แวร์เชิงพาณิชย์ในระดับแนวหน้า เช่น Sprunk Arcsight เพื่อใช้ในการวิเคราะห์ข้อมูลล็อกที่เกี่ยวข้องกับการบุกรุกระบบ
- ฝึกปฏิบัติเข้มข้นมากถึง 10 Workshop ในการปฏิบัติงานเฝ้าระวังความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ เพื่อให้สามารถนำไปปฏิบัติได้จริงด้วยตนเอง

ฉบับแก้ไข วันที่ 3 ธันวาคม 2567

หลักสูตรศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ รุ่นที่ 5
(Security Operations Center: SOC)

ยุคสารสนเทศหรือยุคดิจิทัลในปัจจุบัน ศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศถือเป็นสิ่งสำคัญและมีความจำเป็นอย่างยิ่งต่อองค์กรสำหรับการปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยในโลกไซเบอร์ไม่ว่าจะเป็นสถาบันการเงิน ผู้ให้บริการด้านโครงข่าย ผู้ให้บริการอินเทอร์เน็ต ผู้ให้บริการ Cloud ผู้ให้บริการดูแล Application และอื่นๆ ทั้งนี้เนื่องมาจากการทำงานขององค์กร ผู้ใช้งาน ตลอดจนลูกค้าขององค์กรมีความจำเป็นต้องอาศัยระบบคอมพิวเตอร์ อินเทอร์เน็ต เครือข่ายไร้สาย อุปกรณ์ประเภท Smartphone รวมทั้งอุปกรณ์ประเภท Internet of Things เหล่านี้ล้วนก่อให้เกิดความจำเป็นที่จะต้องมีการเฝ้าระวังและป้องกันระบบและอุปกรณ์ขององค์กรให้มีความมั่นคงปลอดภัยอย่างเพียงพอและตลอดเวลา

Security Operation Center หรือ SOC คือศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ที่ทำหน้าที่เฝ้าระวังและป้องกันระบบหรืออุปกรณ์สำคัญขององค์กรจากการถูกบุกรุกหรือการเข้าถึงโดยไม่ได้รับอนุญาต ซึ่งหากมีเหตุการณ์ด้านความมั่นคงปลอดภัย (Security Incident) เกิดขึ้น เช่น ระบบถูกบุกรุก หรือการเปลี่ยนแปลงแก้ไขข้อมูลโดยไม่ได้รับอนุญาต SOC จะทำหน้าที่ประเมิน ตรวจสอบและแก้ไขเหตุการณ์ที่เกิดขึ้นเพื่อลดผลกระทบและความเสียหายที่อาจเกิดขึ้นกับองค์กรให้อยู่ในระดับที่ไม่รุนแรง

โครงสร้างหลักสูตร

เพื่อสร้างความรู้ความเข้าใจเกี่ยวกับมาตรฐานในการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย แนวทางการจัดตั้งศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ (Security Operations Center: SOC) และฝึกปฏิบัติเข้มข้นทักษะพื้นฐานที่จำเป็นสำหรับการปฏิบัติงานภายใต้ ศูนย์ปฏิบัติการฯ ประกอบด้วย การบรรยาย การฝึกอบรมเชิงปฏิบัติการ รวม 24 ชั่วโมง / 4 วันทำการ

หัวข้อ	ชั่วโมง	ครั้ง (วัน)
บรรยาย และกรณีศึกษา	14	2
ฝึกปฏิบัติการ (Workshop)	10	2
รวม	**24**	**4**

เนื้อหาหลักสูตร ประกอบด้วย

- มาตรฐานและกระบวนการสำหรับการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย
- กระบวนการ บทบาท และหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องในการเฝ้าระวังด้านความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศ
- การแบ่งแยกเหตุการณ์แจ้งเตือน (Event) หรือเหตุการณ์ด้านความมั่นคงปลอดภัยให้ชัดเจน (Security Incident)
- การประเมินผลกระทบหรือระดับความรุนแรงของเหตุการณ์ด้านความมั่นคงปลอดภัยที่เกิดขึ้น
- การจำลองสถานการณ์การโจมตีในรูปแบบต่างๆ เช่น SQL Injection, Cross-site Scripting (XSS), Brute Force เป็นต้น
- การติดตั้ง Agent บนระบบต่างๆ สำหรับการบันทึกข้อมูลล็อก
- การกำหนดกฎเกณฑ์ (Correlation Rules) ที่ใช้ในการวิเคราะห์ข้อมูลจากล็อก
- การวิเคราะห์ข้อมูลจากล็อก
- การวิเคราะห์หาสาเหตุของเหตุการณ์ด้านความมั่นคงปลอดภัย
- การจัดเก็บหลักฐานด้านคอมพิวเตอร์จากข้อมูลล็อกที่จัดเก็บไว้
- การวิเคราะห์หรือตรวจสอบข้อมูลในระบบที่ถูกเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาต
- การจัดทำรายงานประเภทต่างๆ ที่เกี่ยวข้องกับเหตุการณ์ความมั่นคงปลอดภัย ได้แก่ การแจ้ง เตือนประเภทต่างๆ (Alert) และรายงานประเภทสถิติต่างๆ (Dashboard) ที่จำเป็นต่อการใช้งาน
- การใช้เครื่องมือและจัดเก็บข้อมูลล็อกให้สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยขององค์กร ตลอดจนกฎหมาย และระเบียบข้อบังคับที่เกี่ยวข้อง
- การวิเคราะห์หาช่องโหว่ในระบบคอมพิวเตอร์ เพื่อตรวจสอบหาช่องทางการบุกรุกหรือการเข้าถึง เครือข่ายและระบบสารสนเทศที่ผิดปกติ และหาแนวทางป้องกันระบบ
- การใช้เครื่องมือในการเฝ้าระวังและติดตามการทำงานของระบบและอุปกรณ์ต่างๆ

หลักสูตรนี้เหมาะสำหรับ

- ผู้ปฏิบัติงานในศูนย์ปฏิบัติการป้องระวังความมั่นคงปลอดภัย (เช่น CERT NOC เป็นต้น)
- ผู้ดูแลระบบคอมพิวเตอร์ / ผู้ดูแลเครือข่ายคอมพิวเตอร์
- ผู้จัดการด้านไอที
- ผู้ปฏิบัติงานที่เกี่ยวข้องกับการเฝ้าระวังระบบและอุปกรณ์ต่างๆ ขององค์กร

วิทยากรประจำหลักสูตร

ดร. บรรจง หะรังษี
รองกรรมการผู้จัดการ และ
ที่ปรึกษาด้านความมั่นคงปลอดภัยระบบสารสนเทศ
บริษัท ทีเน็ต จำกัด

อาจารย์ เจษฎา ทองก้านเหลือง
กรรมการผู้จัดการ
บริษัท ทีเน็ต ไอที โซลูชัน จำกัด

ระยะเวลาหลักสูตร

ระหว่างวันที่ 22 - 25 กรกฎาคม 2568
เวลา 9.00 - 16.00 น. (รวมระยะเวลาอบรม จำนวน 4 วัน)

ค่าลงทะเบียน

ท่านละ 32,100 บาท (รวมภาษีมูลค่าเพิ่มแล้ว)
- เฉพาะหน่วยงานภาครัฐ และองค์กรของรัฐ ที่ไม่ใช่ธุรกิจและไม่แสวงหากำไร จะได้รับการยกเว้นภาษีมูลค่าเพิ่ม

สถานที่อบรม

CENTURY PARK HOTEL • BANGKOK

โรงแรมเซ็นจูรี่ พาร์ค กรุงเทพ
เลขที่ 9 ถนนราชปรารภ เขตราชเทวี
กรุงเทพมหานคร

หมายเหตุ
- หากท่านต้องการยกเลิกการลงทะเบียนกรุณาแจ้งยืนยันการยกเลิก เป็นลายลักษณ์อักษร อย่างน้อย 7 วันทำการก่อนวันจัดงาน หากการแจ้งยกเลิกล่าช้ากว่าเวลาที่กำหนดดังกล่าว ทางสถาบันฯ ขอสงวนสิทธิ์หักค่าดำเนินการ คิดเป็นจำนวนเงิน 30% จากค่าลงทะเบียนจำนวนเต็ม
- สถาบันพัฒนาบุคลากรแห่งอนาคต ขอสงวนสิทธิ์ในการเปลี่ยนแปลงเนื้อหาหลักสูตร วิทยากร ตามความเหมาะสมและความจำเป็น เพื่อประโยชน์สูงสุดของผู้เข้ารับการอบรม
- ผู้เข้าอบรมต้องมีเวลาเรียนไม่ต่ำกว่า 80% และทำกิจกรรมทุกหัวข้อของหลักสูตร จึงจะได้รับวุฒิบัตรจากสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.)

ศึกษารายละเอียดเพิ่มเติมได้ที่ https://www.career4future.com/soc

สอบถามรายละเอียดเพิ่มเติมได้ที่ 085-211-9709, 084-051-3564 E-mail: npd@nstda.or.th

ฉบับแก้ไข วันที่ 3 ธันวาคม 2567

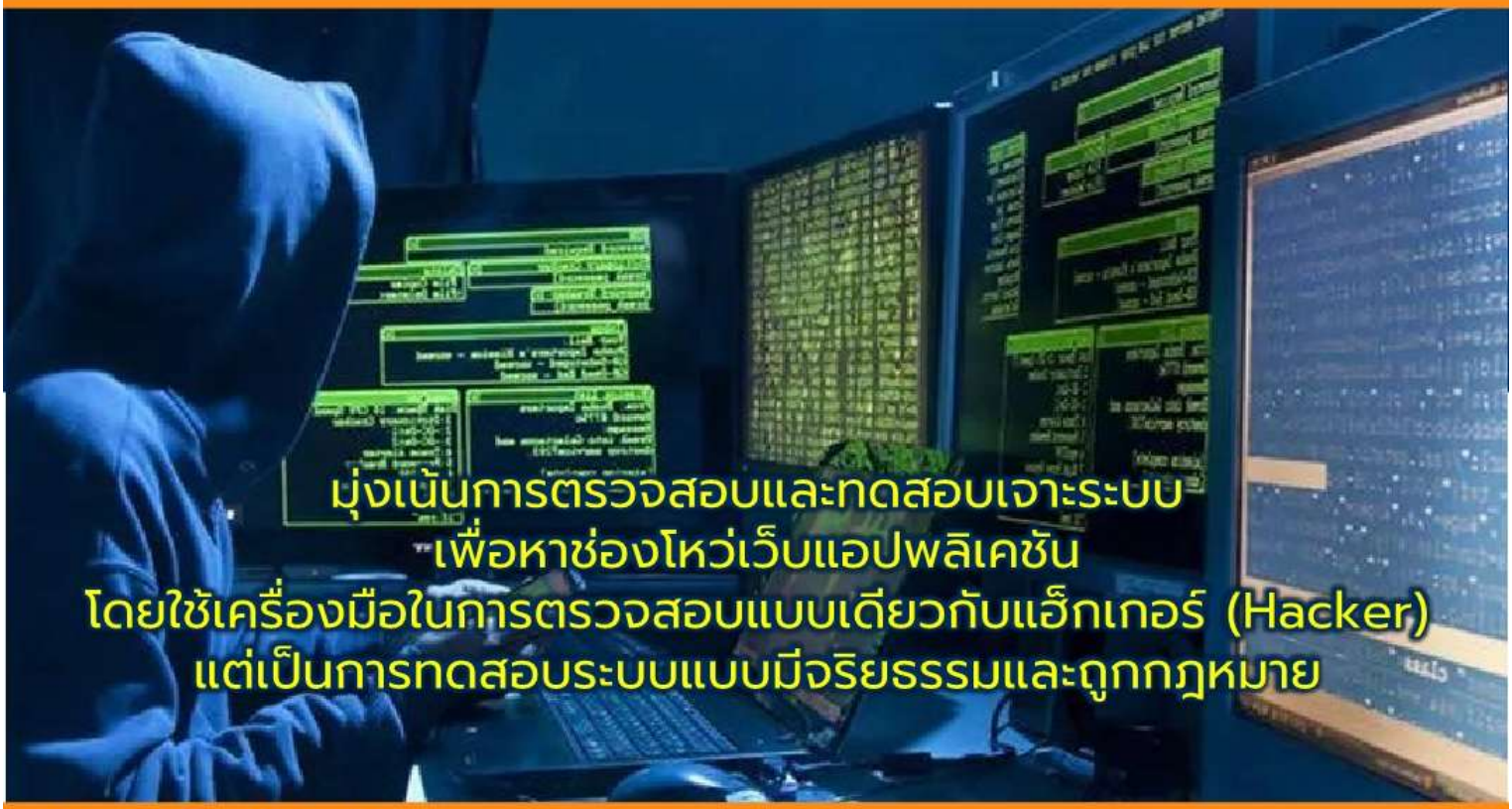
สวทช NSTDA

Career for the Future Academy
สถาบันพัฒนาบุคลากรแห่งอนาคต

W|AHS

Web Application Hacking and Security

หลักสูตรฝึกอบรมเชิงปฏิบัติการ การทดสอบเจาะระบบและความมั่นคงปลอดภัยด้านเว็บแอปพลิเคชัน



มุ่งเน้นการตรวจสอบและทดสอบเจาะระบบ
เพื่อหาช่องโหว่เว็บแอปพลิเคชัน
โดยใช้เครื่องมือในการตรวจสอบแบบเดียวกับแฮ็กเกอร์ (Hacker)
แต่เป็นการทดสอบระบบแบบมีจริยธรรมและถูกกฎหมาย

Key Highlights

- เรียนรู้และเข้าใจสาระสำคัญด้านความปลอดภัยจากการโจมตีเว็บแอปพลิเคชัน
- เรียนรู้มาตราการความมั่นคงปลอดภัยบน HTTP Security Header
- เรียนรู้แนวทางและวิธีการทดสอบเจาะระบบ Penetration Testing Methodologies
- เรียนรู้การทดสอบเจาะระบบ และแนวทางป้องกันรูปแบบการโจมตี บน 10 อันดับความเสี่ยงจาก OWASP
- เข้าใจการทดสอบเจาะระบบในรูปแบบต่าง ๆ พร้อมการทำรายงานที่ถูกต้อง
- ฝึกปฏิบัติเข้มข้นในการทดสอบเจาะระบบในรูปแบบที่หลากหลาย

ฉบับแก้ไข วันที่ 26 พฤษภาคม 2568

หลักสูตรฝึกอบรมเชิงปฏิบัติการ การทดสอบเจาะระบบและความมั่นคงปลอดภัยด้านเว็บแอปพลิเคชัน
Web Application Hacking and Security

ในปัจจุบันภัยคุกคามทางไซเบอร์จากแฮ็กเกอร์ (Hacker) หรือผู้ไม่ประสงค์ดียิ่งทวีความรุนแรงมากขึ้นเรื่อย ๆ โดยเฉพาะการโจมตีเว็บแอปพลิเคชัน ซึ่งเป็นช่องทางสำคัญในการเข้าถึงข้อมูลขององค์กร เป้าหมายของแฮ็กเกอร์อาจเป็นการขโมยข้อมูลสำคัญ ทำลายชื่อเสียงขององค์กร หรือเรียกร้องผลประโยชน์ในรูปแบบต่าง ๆ ส่งผลให้หน่วยงานภาครัฐและเอกชนได้รับความเสียหายอย่างมาก หลักสูตรนี้ถูกออกแบบมาเพื่อสร้างความเข้าใจและความเชี่ยวชาญด้านความมั่นคงปลอดภัยของระบบ รวมถึงสร้างความรู้ความสามารถในการตรวจสอบความมั่นคงปลอดภัยของเว็บแอปพลิเคชัน โดยมุ่งเน้นการตรวจสอบและทดสอบเจาะระบบเพื่อหาช่องโหว่โดยใช้เครื่องมือในการตรวจสอบแบบเดียวกับที่แฮ็กเกอร์ (Hacker) ใช้ แต่เป็นการทดสอบระบบแบบมีจริยธรรมและถูกกฎหมาย ผู้เข้าอบรมจะได้พัฒนาทักษะในการป้องกันภัยทางไซเบอร์และช่วยให้องค์กรสามารถรับมือกับการโจมตีได้อย่างมีประสิทธิภาพ

โครงสร้างหลักสูตร

หลักสูตรนี้เป็นหลักสูตรที่สร้างความรู้ความเข้าใจเกี่ยวกับการทดสอบเจาะระบบและความมั่นคงปลอดภัยด้านเว็บแอปพลิเคชัน ตลอดจนฝึกปฏิบัติเพื่อพัฒนาทักษะที่จำเป็นอย่างเข้มข้น รวมจำนวน 18 ชั่วโมง / 3 วันทำการ

หัวข้อ	ชั่วโมง	ครั้ง (วัน)
บรรยาย และกรณีศึกษา	9	1.5
ฝึกปฏิบัติการ (Workshop)	9	1.5
รวม	**18**	**3**

เนื้อหาหลักสูตร ประกอบด้วย

- Introduction to Web Application
- HTTP Security Headers
- Introduction to Web Application Security
- Penetration Testing Methodology
- Penetration Testing Framework
- Types of Web Penetration Testing
- Web Application Penetration Testing Tools
- Web Application Penetration Testing Checklist
- Web Application Penetration Testing Certifications
- The Penetration Testing Process
- Web Application Proxies
- Using Hacking Tools
- Open Web Application Security Project (OWASP)
  - OWASP TOP 10 2013: SQL Injection
  - OWASP TOP 10 2013: Broken Authentication and Session Management
  - OWASP TOP 10 2013: Cross-site Scripting
  - OWASP TOP 10 2013: Security Misconfiguration
  - OWASP TOP 10 2017: XML External Entities (XXE)
  - OWASP TOP 10 2017: Insecure Deserialization
  - OWASP TOP 10 2021: Insecure Design
  - OWASP TOP 10 2021: Software and Data Integrity Failures
  - OWASP TOP 10 2021: Server-Side Request Forgery

ระยะเวลาหลักสูตร

อบรมระหว่างวันที่ 6 - 8 สิงหาคม 2568
เวลา 9.00 - 16.00 น. (รวมระยะเวลา 3 วัน)

หลักสูตรนี้เหมาะสำหรับ

- นักพัฒนาโปรแกรมด้านเว็บแอพพลิเคชัน
- ผู้ดูแลระบบ (System Administrator)
- นักทดสอบเจาะระบบ (Penetration Tester)
- ปรึกษาด้านความมั่นคงปลอดภัยสารสนเทศ (IT Security Consultant)

วิทยากรประจำหลักสูตร

อาจารย์ เจษฎา ทองก้านเหลือง
กรรมการผู้จัดการ
บริษัท ที-เน็ต ไอที โซลูชัน จำกัด
- Certified Ethical Hacker (CEH)
- Certified Hacking Forensic Investigator (C|HFI)
- Certified Security Analyst (E|CSA)
- IT Specialist Certification (ITS): Cyber Security

ค่าลงทะเบียน

ท่านละ 24,500 บาท (รวมภาษีมูลค่าเพิ่มแล้ว)
- เฉพาะหน่วยงานภาครัฐ และองค์กรของรัฐ ที่ไม่ใช่ธุรกิจและไม่แสวงหากำไร จะได้รับการยกเว้นภาษีมูลค่าเพิ่ม
- โปรโมชั่นพิเศษ!!! ลงทะเบียนหน่วยงานเดียวกันตั้งแต่ 2 ท่านขึ้นไป รับส่วนลดทันที 10%

สถานที่อบรม

CENTURY PARK HOTEL - BANGKOK

โรงแรมเซ็นจูรี่ พาร์ค กรุงเทพ
เลขที่ 9 ถนนราชปรารภ เขตราชเทวี
กรุงเทพมหานคร

หมายเหตุ
- หากท่านต้องการยกเลิกการลงทะเบียน กรุณาแจ้งยืนยันการยกเลิกเป็นลายลักษณ์อักษร อย่างน้อย 7 วันทำการก่อนวันจัดงาน หากการแจ้งยกเลิกล่าช้ากว่าเวลาที่กำหนดดังกล่าว ทางสถาบันฯ ขอสงวนสิทธิ์หักค่าดำเนินการ คิดเป็นจำนวนเงิน 30% จากค่าลงทะเบียนจำนวนเต็ม
- สถาบันพัฒนาบุคลากรแห่งอนาคต ขอสงวนสิทธิ์ในการเปลี่ยนแปลงเนื้อหาหลักสูตร วิทยากร ตามความเหมาะสมและความจำเป็น เพื่อประโยชน์สูงสุดของผู้เข้ารับการอบรม
- ผู้เข้าอบรมต้องมีเวลาเรียนไม่ต่ำกว่า 80% และทำกิจกรรมทุกหัวข้อของหลักสูตร จึงจะได้รับวุฒิบัตรจากสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.)

ศึกษารายละเอียดเพิ่มเติมได้ที่ https://www.career4future.com/wahs

สอบถามรายละเอียดเพิ่มเติมได้ที่ 0 2644 8150 ต่อ 81891 E-mail: npd@nstda.or.th

ฉบับแก้ไข วันที่ 26 พฤษภาคม 2568

สวทช NSTDA

Career for the Future Academy

สถาบันพัฒนาบุคลากรแห่งอนาคต

CSS

Cloud Security Standard

หลักสูตรมาตรฐานการบริหารจัดการความมั่นคงปลอดภัยบนระบบคลาวด์ ตามมาตรฐาน CSA 4.x และ ISO/IEC 27001: 2022 รุ่นที่ 6

มุ่งเน้นการบริหารจัดการระบบงานให้มีความมั่นคงปลอดภัยและสอดคล้อง
ตามมาตรฐาน CSA 4.x และ ISO/IEC 27001: 2022

Key Highlights

- เจาะลึกแนวทางในการนำระบบงานขึ้นคลาวด์ให้มีความมั่นคงปลอดภัย
- เรียนรู้มาตรฐานสากล CSA 4.x และ ISO/IEC 27001: 2022 ในการรักษาความมั่นคงปลอดภัยด้านระบบสารสนเทศ ที่นำไปติดตั้งและใช้งานบนคลาวด์
- เข้าใจโดเมนและมาตรฐาน ด้านความมั่นคงปลอดภัย CSA 4.x และ ISO/IEC 27001: 2022 พร้อมอัพเดทข้อมูลล่าสุด
- เรียนรู้มาตรการ CSA 4.x ทั้ง 17 โดเมน เพื่อลดความผิดพลาดต่างๆ ก่อนที่จะเกิดขึ้น

ISO หลักสูตรนี้ได้รับการออกแบบตามมาตรฐานการประกันคุณภาพสำหรับการจัดฝึกอบรมและการศึกษา ISO 10015

ฉบับแก้ไข วันที่ 12 ธันวาคม 2567

หลักสูตรมาตรฐานการบริหารจัดการความมั่นคงปลอดภัยบนระบบคลาวด์ ตามมาตรฐาน CSA 4.x และ ISO/IEC 27001: 2022 รุ่นที่ 6 (Cloud Security Standard : CSS)

ปัจจุบันหลายองค์กรได้เริ่มปรับเปลี่ยนการทำงานจากการติดตั้ง ดูแล และบริหารจัดการเซิร์ฟเวอร์และระบบงานต่างๆ ภายในศูนย์คอมพิวเตอร์ไปติดตั้งและบริหารจัดการระบบโดยใช้บริการจากผู้ให้บริการคลาวด์แทน ซึ่งมีความรู้ ความสามารถ และน่าเชื่อถือ เพื่อประหยัดค่าใช้จ่ายในการลงทุนด้านเซิร์ฟเวอร์ โครงสร้างพื้นฐานด้านเครือข่าย และการจัดทำศูนย์คอมพิวเตอร์ จากความจำเป็นหรือความต้องการในการนำระบบงานต่างๆ ขององค์กรขึ้นไปติดตั้งบนคลาวด์ของผู้ให้บริการ ประเด็นปัญหาและอุปสรรคสำคัญในฐานะผู้ใช้บริการคลาวด์คือ ประเด็นความมั่นคงปลอดภัยด้านสารสนเทศที่ทุกองค์กรที่จะนำระบบงานไปติดตั้งบนคลาวด์ต้องเผชิญ หลักสูตรนี้จึงเล็งเห็นถึงความจำเป็นในการนำระบบงานขององค์กรไปขึ้นคลาวด์ให้มีความมั่นคงปลอดภัย ทั้งนี้เพื่อให้เกิดความมั่นใจต่อผู้ใช้บริการคลาวด์นั่นเอง

โดยมาตรฐานสากลสำหรับการรักษาความมั่นคงปลอดภัยสารสนเทศบนคลาวด์ที่นิยมใช้หรืออ้างอิงกันอยู่คือมาตรฐาน CSA (Cloud Security Alliance) มาตรฐานนี้เป็นมาตรฐานที่พัฒนาต่อยอดมาจาก ISO/IEC 27001 ซึ่งเป็นมาตรฐานหลักด้านการรักษาความมั่นคงปลอดภัยสารสนเทศที่เป็นที่นิยมและปัจจุบันมีหลายหน่วยงานทั้งภาครัฐและเอกชนปฏิบัติตามอยู่ หลักสูตรนี้ได้อ้างอิงตามมาตรฐาน CSA 4.x (เวอร์ชั่นปัจจุบันล่าสุด) และ มาตรฐาน ISO/IEC 27001: 2022 (เวอร์ชั่นปัจจุบันล่าสุด)

โครงสร้างหลักสูตร

หลักสูตรนี้มุ่งเน้นให้ผู้เข้าอบรมทราบแนวทาง วิธีการนำระบบงานขึ้นคลาวด์ให้มีความมั่นคงปลอดภัย ตามมาตรฐาน CSA 4.x และ ISO/IEC 27001: 2022 การบริหารจัดการฐานข้อมูล ระบบบริหารจัดการเว็บซอฟแวร์ต่างๆ ที่เกี่ยวข้อง แอพพลิเคชันของระบบงาน จนกระทั่งสามารถใช้งานระบบได้ โดยสามารถนำแนวทางดังกล่าวไปต่อยอดหรือปรับใช้กับระบบงานของตนเองได้ รวม 18 ชั่วโมง / 3 วันทำการ

หัวข้อ	ชั่วโมง	ครั้ง (วัน)
บรรยาย และกรณีศึกษา	12	2
ฝึกปฏิบัติการ (Workshop)	6	1
รวม	**18**	**3**

หลักสูตรนี้เหมาะสำหรับ

- เจ้าหน้าที่เทคนิค ได้แก่ ผู้ดูแลระบบ ผู้ดูแลเครือข่าย ผู้พัฒนาระบบ Helpdesk
- เจ้าหน้าที่ด้านความมั่นคงปลอดภัยระบบสารสนเทศ (IT Security)
- ผู้ที่อยู่ในตำแหน่งงานด้านไอซีทีต่างๆ ที่สนใจงานด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
- ผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศ

วิทยากรประจำหลักสูตร

ดร. บรรจง หะรังษี
รองกรรมการผู้จัดการ และ
ที่ปรึกษาด้านความมั่นคงปลอดภัยระบบสารสนเทศ
บริษัท ที-เน็ต จำกัด

- ISO/IEC 27001 (Certified of Lead auditor)
- ISO/IEC 20000 (Auditor Certificate) BCMS 25999
- Introduction to Capability Maturity Model Integration V1.2 Certificate

สิ่งที่คาดว่าจะได้รับ

ผู้เข้าอบรมจะได้รับ

- ความรู้ความเข้าใจในการนำระบบงานขึ้นคลาวด์ให้มีความมั่นคงปลอดภัยด้านสารสนเทศตามมาตรฐาน CSA และ ISO/IEC 27001: 2022
- ได้แนวทางที่สอดคล้อง ในการบริหารจัดการระบบงานให้เข้ากับมาตรฐานในโดเมนต่างๆ
- ความรู้จากกรณีศึกษาในห้องเรียน ที่จะนำไปปรับใช้งานกับองค์กรของตนเองได้อย่างมีประสิทธิภาพ

ระยะเวลาหลักสูตร

ระหว่างวันที่ 13 - 15 สิงหาคม 2568
เวลา 9.00 - 16.00 น. (รวมระยะเวลาอบรม จำนวน 3 วัน)

ค่าลงทะเบียน

ท่านละ 22,470 บาท (รวมภาษีมูลค่าเพิ่มแล้ว)

- เฉพาะหน่วยงานภาครัฐ และองค์กรของรัฐ ที่ไม่ใช่ธุรกิจและไม่แสวงหากำไร จะได้รับการยกเว้นภาษีมูลค่าเพิ่ม

สถานที่อบรม

โรงแรมเซ็นจูรี่ พาร์ค กรุงเทพ
เลขที่ 9 ถนนราชปรารภ เขตราชเทวี
กรุงเทพมหานคร

หมายเหตุ

- หากท่านต้องการยกเลิกการลงทะเบียนกรุณาแจ้งยืนยันการยกเลิก เป็นลายลักษณ์อักษร อย่างน้อย 7 วันทำการก่อนวันจัดงาน หากการแจ้งยกเลิกล่าช้ากว่าเวลาที่กำหนดดังกล่าว ทางสถาบันฯ ขอสงวนสิทธิ์หักค่าดำเนินการ คิดเป็นจำนวนเงิน 30% จากค่าลงทะเบียนจำนวนเต็ม
- สถาบันพัฒนาบุคลากรแห่งอนาคต ขอสงวนสิทธิ์ในการเปลี่ยนแปลงเนื้อหาหลักสูตร วิทยากร ตามความเหมาะสมและความจำเป็น เพื่อประโยชน์สูงสุดของผู้เข้ารับการอบรม
- ผู้เข้าอบรมต้องมีเวลาเรียนไม่ต่ำกว่า 80% และทำกิจกรรมทุกหัวข้อของหลักสูตร จึงจะได้รับวุฒิบัตรจากสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.)

ศึกษารายละเอียดเพิ่มเติมได้ที่ https://www.career4future.com/css

สอบถามรายละเอียดเพิ่มเติมได้ที่ 085-211-9709, 084-051-3564 E-mail: npd@nstda.or.th

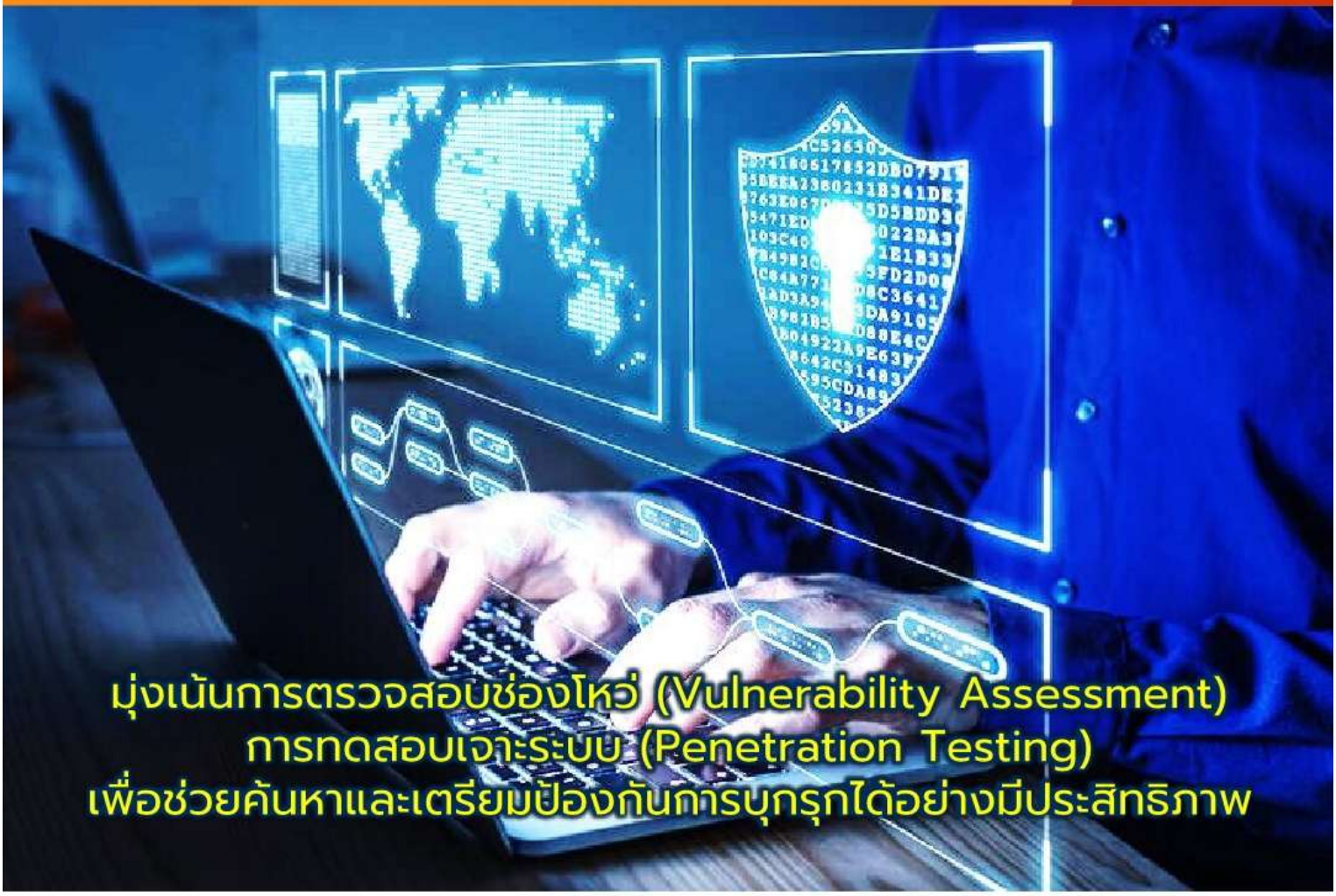
ฉบับแก้ไข วันที่ 12 ธันวาคม 2567

Career for the Future Academy
สถาบันพัฒนาบุคลากรแห่งอนาคต

VAPT

Vulnerability Assessment and Penetration Testing

หลักสูตรฝึกอบรมเชิงปฏิบัติการ การตรวจสอบช่องโหว่และการทดสอบเจาะระบบ รุ่นที่ 2



มุ่งเน้นการตรวจสอบช่องโหว่ (Vulnerability Assessment)
การทดสอบเจาะระบบ (Penetration Testing)
เพื่อช่วยค้นหาและเตรียมป้องกันการบุกรุกได้อย่างมีประสิทธิภาพ

- เรียนรู้สาระสำคัญด้านความปลอดภัยจากการโจมตีเว็บแอปพลิเคชั่น
- เข้าใจการทดสอบเจาะระบบในรูปแบบต่าง ๆ พร้อมการทำรายงานที่ถูกต้อง
- ทดลองใช้เครื่องมือตรวจสอบช่องโหว่ (Vulnerability Assessment)
- ฝึกปฏิบัติเข้มข้นในการทดสอบเจาะระบบ (Penetration Testing)

ฉบับแก้ไข วันที่ 26 พฤษภาคม 2568

หลักสูตรฝึกอบรมเชิงปฏิบัติการ การตรวจสอบช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing) รุ่นที่ 2

ในปัจจุบันภัยคุกคามที่เกิดขึ้นจากผู้ไม่ประสงค์ดี/แฮ็กเกอร์ (Hacker) ได้ทวีความรุนแรงขึ้นทุกวัน โดยมุ่งเน้นการโจมตีหน่วยงานภาครัฐ เอกชน และมหาวิทยาลัย จากทั้งภายในและภายนอกประเทศ เพื่อขโมยข้อมูลหรือทำลายชื่อเสียงและเรียกร้องสิทธิต่าง ๆ ตามที่ต้องการ ซึ่งสาเหตุหลักที่โดนบุกรุกเนื่องจากผู้ไม่ประสงค์ดีสามารถเข้าถึงภายในระบบจากที่ใดก็ได้บนโลกผ่านระบบเครือข่ายอินเทอร์เน็ต ทำให้ง่ายต่อการบุกรุก หลักสูตรนี้เป็นหลักสูตรที่สร้างความเข้าใจและความเชี่ยวชาญด้านความมั่นคงปลอดภัยของระบบรวมถึงสร้างความรู้ความสามารถในการตรวจสอบความมั่นคงปลอดภัยของระบบสารสนเทศและเครือข่ายขององค์กร โดยมุ่งเน้นการตรวจสอบและทดสอบเจาะระบบเพื่อหาช่องโหว่โดยใช้เครื่องมือในการตรวจสอบแบบเดียวกับที่แฮ็กเกอร์ (Hacker)ใช้ แต่เป็นการทดสอบระบบแบบมีจริยธรรมและถูกกฎหมาย

โครงสร้างหลักสูตร

เพื่อสร้างความรู้ความเข้าใจเกี่ยวกับการตรวจสอบช่องโหว่และการทดสอบเจาะระบบ และฝึกปฏิบัติเข้มข้นทักษะพื้นฐานที่จำเป็นสำหรับการปฏิบัติงานเพื่อพัฒนาทักษะที่จำเป็นอย่างเข้มข้น รวมจำนวน 18 ชั่วโมง / 3 วันทำการ

หัวข้อ	ชั่วโมง	ครั้ง (วัน)
บรรยาย และกรณีศึกษา	9	1.5
ฝึกปฏิบัติการ (Workshop)	9	1.5
รวม	**18**	**3**

เนื้อหาหลักสูตร ประกอบด้วย

- ความรู้เบื้องต้นเกี่ยวกับการตรวจสอบช่องโหว่ (Introduction to Vulnerability Assessment)
- ความรู้เบื้องต้นเกี่ยวกับการทดสอบการเจาะระบบ (Introduction to Penetration Testing)
- การรวบรวมข้อมูล (Information Gathering)
- การสแกนเครือข่าย (Scanning Networks)
- การค้นหาช่องโหว่ (Vulnerability Assessment)
- การทดสอบเจาะระบบ (Penetration Testing)
- การแฮ็กเว็บ (Hacking Web)
- การแฮ็กระบบ (System Hacking)
- การใช้งานระบบปฏิบัติการ Kali Linux
- การใช้งานเครื่องมือ Metasploit

หลักสูตรนี้เหมาะสำหรับ

- นักพัฒนาโปรแกรมด้านเว็บแอพพลิเคชัน
- ผู้ดูแลระบบ (System Administrator)
- นักทดสอบเจาะระบบ (Penetration Tester)
- ปรึกษาด้านความมั่นคงปลอดภัยสารสนเทศ (IT Security Consultant)

ค่าลงทะเบียน

ท่านละ 26,900 บาท (รวมภาษีมูลค่าเพิ่มแล้ว)

- เฉพาะหน่วยงานภาครัฐ และองค์กรของรัฐที่ไม่ใช่ธุรกิจและไม่แสวงหากำไร จะได้รับการยกเว้นภาษีมูลค่าเพิ่ม
- โปรโมชั่นพิเศษ!!! ลงทะเบียนหน่วยงานเดียวกันตั้งแต่ 2 ท่านขึ้นไป รับส่วนลดทันที 10%

วิทยากรประจำหลักสูตร

อาจารย์ เจษฎา ทองก้านเหลือง
กรรมการผู้จัดการ
บริษัท ทีเน็ต ไอที โซลูชัน จำกัด

- Certified Ethical Hacker (CEH)
- Certified Hacking Forensic Investigator (C|HFI)
- Certified Security Analyst (E|CSA)
- IT Specialist Certification (ITS): Cyber Security

ระยะเวลาหลักสูตร

ระหว่างวันที่ 20-22 สิงหาคม 2568
เวลา 9.00 - 16.00 น. (รวมระยะเวลาอบรม จำนวน 3 วัน)

สถานที่อบรม

โรงแรมเซ็นจูรี่ พาร์ค กรุงเทพ
เลขที่ 9 ถนนราชปรารภ เขตราชเทวี
กรุงเทพมหานคร

หมายเหตุ

- หากท่านต้องการยกเลิกการลงทะเบียนกรุณาแจ้งยืนยันการยกเลิก เป็นลายลักษณ์อักษร อย่างน้อย 7 วันทำการก่อนวันจัดงาน หากการแจ้งยกเลิกล่าช้ากว่าเวลที่กำหนดดังกล่าว ทางสถาบันฯ ขอสงวนสิทธิ์หักค่าดำเนินการ คิดเป็นจำนวนเงิน 30% จากค่าลงทะเบียนจำนวนเต็ม
- สถาบันพัฒนาบุคลากรแห่งอนาคต ขอสงวนสิทธิ์ในการเปลี่ยนแปลงเนื้อหาหลักสูตร วิทยากร ตามความเหมาะสมและความจำเป็น เพื่อประโยชน์สูงสุดของผู้เข้ารับการอบรม
- ผู้เข้าอบรมต้องมีเวลาเรียนไม่ต่ำกว่า 80% และทำกิจกรรมทุกหัวข้อของหลักสูตร จึงจะได้รับวุฒิบัตรจากสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.)

ศึกษารายละเอียดเพิ่มเติมได้ที่ https://www.career4future.com/vapt

สอบถามรายละเอียดเพิ่มเติมได้ที่ 0 2644 8150 ต่อ 81891 E-mail: npd@nstda.or.th

ฉบับแก้ไข วันที่ 26 พฤษภาคม 2568

Career for the Future Academy
สถาบันพัฒนาบุคลากรแห่งอนาคต

BCS

Business Continuity Management Standard

หลักสูตรฝึกอบรมเชิงปฏิบัติการ
การบริหารจัดการความต่อเนื่องทางธุรกิจตามมาตรฐานสากล ISO 22301:2019 **รุ่นที่ 6**

มุ่งเน้นการเตรียมความพร้อมเรื่องการกู้คืนระบบงาน และการรับมือกับเหตุการณ์หยุดชะงักหรือสภาวะวิกฤติ เพื่อให้เกิดความต่อเนื่องในกระบวนการบริหารจัดการงานตามมาตรฐาน ISO 22301:2019

Key Highlights

- เจาะลึก ISO 22301:2019 มาตรฐานสากลหลักที่ใช้ในการอ้างอิงและบริหารจัดการความต่อเนื่องทางธุรกิจ เพื่อการบริหารจัดการภัยคุกคามแบบองค์รวม
- ทราบหลักการการประเมินความเสี่ยง ผลกระทบ การกำหนดลำดับของงานในการกู้คืนระบบ ตลอดจนการกำหนดระยะเวลาเป้าหมายในการกู้คืนระบบงานที่เหมาะสม
- วางแผนเตรียมความพร้อมด้านกลยุทธ์ในการป้องกันหรือรับมือกับเหตุวิกฤติ หรือภัยพิบัติ เพื่อลดความเสียหาย สร้างความยืดหยุ่น และสามารถดำเนินธุรกิจได้อย่างต่อเนื่อง
- เรียนรู้วิธีการจัดทำแผนกู้คืนระบบงาน (Business Continuity Plan) และแผนรับมือกับเหตุการณ์หยุดชะงักที่เกิดขึ้น (Incident Management Plan) โดยอ้างอิงตามมาตรฐาน ISO 22301:2019
- ฝึกปฏิบัติเข้มข้นกว่า 10 Workshop กับกรณีศึกษาที่สามารถนำกลับไปประยุกต์ใช้งานได้จริงในองค์กร

ฉบับแก้ไข วันที่ 26 พฤษภาคม 2568

หลักสูตรฝึกอบรมเชิงปฏิบัติการ การบริหารจัดการความต่อเนื่องทางธุรกิจตามมาตรฐานสากล ISO 22301:2019 รุ่นที่ 6
(Business Continuity Management Standard)

การดำเนินธุรกิจในปัจจุบันจำเป็นอย่างยิ่งที่จะต้องพึ่งพาระบบงานไอทีมาสนับสนุนในการบริหารจัดการ เพื่อให้องค์กรสามารถดำเนินการไปได้อย่างรวดเร็วและมีประสิทธิภาพ แต่ด้วยปัจจัยการเปลี่ยนแปลงที่รวดเร็ว และความไม่แน่นอนของสถานการณ์ที่ไม่สามารถคาดการณ์ได้ ไม่ว่าจะเป็นสถานการณ์น้ำท่วม ไฟไหม้ หรือถูกปิดล้อมโดยฝูงชน หากระบบงานหรือบุคลากรหยุดทำงานเป็นระยะเวลานานเกินกว่าระยะเวลาที่รับได้ จะก่อให้เกิดความเสียหายและส่งผลกระทบต่อการดำเนินธุรกิจ ชื่อเสียง ภาพลักษณ์ ความเชื่อมั่น และกิจกรรมที่สร้างมูลค่าเพิ่มให้กับองค์กร ดังนั้นหลายองค์กรจึงได้ให้ความสำคัญกับการเตรียมพร้อมในการรับมือกับเหตุการณ์ สภาวะวิกฤติ หรือภัยคุกคามที่อาจเกิดขึ้น และเตรียมพร้อมในเรื่องของการกู้คืนระบบงานไอทีให้กลับคืนมาดำเนินกิจกรรมได้ภายในระยะเวลาที่เหมาะสม

โครงสร้างหลักสูตร

หลักสูตรนี้มุ่งเน้นให้ผู้เรียนเข้าใจแนวคิดและหลักการของมาตรฐาน ISO 22301:2019 ซึ่งเป็นมาตรฐานสากลที่ใช้ในการบริหารจัดการความต่อเนื่องทางธุรกิจ (Business Continuity Management Systems) ในการชี้บ่งภัยคุกคาม เพื่อนำมาปรับปรุงประสิทธิภาพและสร้างกลไกเตรียมความพร้อมเรื่องการกู้คืนระบบงานไอทีในองค์กรที่มีความซับซ้อนในการออกแบบกระบวนการป้องกันและรับมือกับภัยคุกคาม นอกจากนี้หลักสูตรนี้ยังได้กำหนดให้มีการฝึกปฏิบัติตามกรณีศึกษาโดยผู้เรียนสามารถนำแผนกู้คืนระบบงานขององค์กรมาฝึกปฏิบัติได้ ซึ่งจะทำให้เข้าใจภาพรวมทั้งหมดของการกู้คืนระบบงานไอทีและสามารถต่อยอดความรู้ที่ได้กลับไปปรับใช้งานกับองค์กรของตนเองได้อย่างมีประสิทธิภาพ รวม 18 ชั่วโมง / 3 วันทำการ

หัวข้อ	ชั่วโมง	ครั้ง (วัน)
บรรยาย และกรณีศึกษา	9	1.5
ฝึกปฏิบัติการ (Workshop)	9	1.5
รวม	**18**	**3**

หลักสูตรนี้เหมาะสำหรับ

- ผู้บริหารด้านไอซีทีในทุกระดับ หัวหน้าศูนย์เทคโนโลยีสารสนเทศ ผู้จัดการด้านไอซีที
- เจ้าหน้าที่ทางเทคนิคด้านไอซีที เช่น ผู้วิเคราะห์และออกแบบระบบ ผู้พัฒนาระบบ ผู้ดูแลระบบ ผู้ดูแลเครือข่าย
- ผู้ตรวจสอบไอซีที

วิทยากรประจำหลักสูตร

ดร. บรรจง หะรังษี
รองกรรมการผู้จัดการ และ
ที่ปรึกษาด้านความมั่นคงปลอดภัยระบบสารสนเทศ
บริษัท ที-เน็ต จำกัด

- ISO/IEC 27001 (Certified of Lead auditor)
- ISO/IEC 20000 (Auditor Certificate) BCMS 25999
- Introduction to Capability Maturity Model Integration V1.2 Certificate

ค่าลงทะเบียน

ท่านละ 24,500 บาท (รวมภาษีมูลค่าเพิ่มแล้ว)

- เฉพาะหน่วยงานภาครัฐ และองค์กรของรัฐที่ไม่ใช่ธุรกิจและไม่แสวงหากำไร จะได้รับการยกเว้นภาษีมูลค่าเพิ่ม
- โปรโมชั่นพิเศษ!!! ลงทะเบียนหน่วยงานเดียวกันตั้งแต่ 2 ท่านขึ้นไป รับส่วนลดกันที 10%

สิ่งที่คาดว่าจะได้รับ

ผู้เข้าอบรมจะได้รับ

- การนำบริบทขององค์กร หรือสภาพขององค์กรที่เป็นอยู่ในปัจจุบันมาใช้เป็นประเด็นสำคัญในการวางแผนงานสำหรับการบริหารความต่อเนื่องทางธุรกิจ
- การกำหนด Scenario ซึ่งเป็นเหตุการณ์ความเสี่ยงที่ส่งผลต่อการหยุดชะงักของระบบงานสำคัญขององค์กร
- การประเมินผลกระทบกรณีระบบงานสำคัญขององค์กรเกิดการหยุดชะงัก
- การกำหนดลำดับของงานในการกู้คืนระบบ
- การกำหนดระยะเวลาเป้าหมายในการกู้คืนระบบ
- การประเมินความเสี่ยงเพื่อบริหารจัดการกับเหตุต่างๆ ที่จะทำให้เกิดการหยุดชะงัก
- การระบุทรัพยากรที่จำเป็นสำหรับการกู้คืนระบบงาน
- การจัดทำแผนการรับมือหรือจัดการกับเหตุหยุดชะงัก
- การจัดทำแผนกู้คืนระบบ
- การซ้อมการกู้คืนระบบ
- การจัดทำแผนการสื่อสารในระหว่างที่เกิดเหตุ

ระยะเวลาหลักสูตร

ระหว่างวันที่ 27 - 29 สิงหาคม 2568
เวลา 9.00 - 16.00 น. (รวมระยะเวลาอบรม จำนวน 3 วัน)

สถานที่อบรม

โรงแรมเซ็นจูรี่ พาร์ค กรุงเทพ
เลขที่ 9 ถนนราชปรารภ เขตราชเทวี
กรุงเทพมหานคร

หมายเหตุ

- หากท่านต้องการยกเลิกการลงทะเบียนกรุณาแจ้งยืนยันการยกเลิก เป็นลายลักษณ์อักษร อย่างน้อย 7 วันทำการก่อนวันจัดงาน หากการแจ้งยกเลิกล่าช้ากว่าเวลาที่กำหนดดังกล่าว ทางสถาบันฯ ขอสงวนสิทธิ์หักค่าดำเนินการ คิดเป็นจำนวนเงิน 30% จากค่าลงทะเบียนจำนวนเต็ม
- สถาบันพัฒนาบุคลากรแห่งอนาคต ขอสงวนสิทธิ์ในการเปลี่ยนแปลงเนื้อหาหลักสูตร วิทยากร ตามความเหมาะสมและความจำเป็น เพื่อประโยชน์สูงสุดของผู้เข้ารับการอบรม
- ผู้เข้าอบรมต้องมีเวลาเรียนไม่ต่ำกว่า 80% และทำกิจกรรมทุกหัวข้อของหลักสูตร จึงจะได้รับวุฒิบัตรจากสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.)

ศึกษารายละเอียดเพิ่มเติมได้ที่ https://www.career4future.com/bcs

สอบถามรายละเอียดเพิ่มเติมได้ที่ 0 2644 8150 ต่อ 81891 E-mail: npd@nstda.or.th

ฉบับแก้ไข วันที่ 26 พฤษภาคม 2568

สวทช NSTDA

Career for the Future Academy
สถาบันพัฒนาบุคลากรแห่งอนาคต

CSM

Cyber Security Incident Management

หลักสูตร
การบริหารจัดการและการรับมือกับภัยคุกคามทางไซเบอร์ **รุ่นที่ 4**

"มุ่งเน้นการเตรียมความพร้อมในการบริหารจัดการเหตุการณ์
ด้านความมั่นคงปลอดภัยเพื่อรับมือกับภัยคุกคามทางไซเบอร์
จนถึงการกู้คืนระบบกลับคืน"

Key Highlights

- เรียนรู้และเข้าใจสาระสำคัญของพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
- เจาะลึกมาตรฐานและมาตรการสำหรับการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย
- เตรียมความพร้อมในการจัดตั้งทีมบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย
- ฝึกวิเคราะห์อย่างเข้มข้น เพื่อรับมือจากภัยคุกคามทางไซเบอร์
  จนถึงการกู้คืนระบบกลับคืน มากกว่า 10 Workshop

ฉบับแก้ไข วันที่ 26 พฤษภาคม 2568

หลักสูตรการบริหารจัดการและการรับมือกับภัยคุกคามทางไซเบอร์ รุ่นที่ 4
(Cyber Security Incident Management: CSM)

ด้วยความก้าวหน้าทางเทคโนโลยีสารสนเทศที่เติบโตอย่างรวดเร็ว สามารถเข้าถึงได้ง่าย สะดวก รวดเร็ว และครอบคลุมทุกอุปกรณ์สื่อสาร เรามักจะพบข่าว การหลอกลวงล้วงข้อมูล การโจมตีระบบ การขโมยข้อมูลทางอิเล็กทรอนิกส์ มากขึ้นทุกวัน ซึ่งเหล่านี้เป็นภัยคุกคามทางไซเบอร์ เป็นสิ่งที่หลีกเลี่ยงไม่ได้และปัจจุบันทวีความรุนแรงมากขึ้นเรื่อยๆ ซึ่งอาจส่งผลกระทบและความเสียหายต่อทั้งระดับบุคคล ระดับองค์กร และระดับประเทศ หน่วยงานหรือองค์กรจึงจำเป็นต้องมีกลไกสำหรับการบริหารจัดการความมั่นคงปลอดภัยสำหรับภัยคุกคามด้านไซเบอร์อย่างเป็นรูปธรรม โดยจำเป็นที่จะต้องมีการบริหารจัดการภัยคุกคามทางไซเบอร์ที่มีโอกาสเกิดขึ้นอย่างมืออาชีพ หลักสูตรนี้จึงมีความประสงค์ต้องการให้ผู้เข้าร่วมฝึกอบรม มีความรู้ความเข้าใจ ตลอดจนทักษะที่จำเป็นในประเด็นต่างๆ ดังต่อไปนี้

- สาระสำคัญของ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 (พรบ. ไซเบอร์)
- สิ่งที่องค์กรต้องดำเนินการให้สอดคล้องกับ พรบ. ไซเบอร์
- มาตรการที่จำเป็นต้องนำมาปฏิบัติเพื่อให้สอดคล้องกับความต้องการของ พรบ. ไซเบอร์ (อ้างอิงจากมาตรฐาน Framework for Improving Critical Infrastructure Cybersecurity)
- มาตรฐาน ISO ที่เกี่ยวข้อง ตลอดจนการฝึกปฏิบัติเพื่อให้ผู้เข้าร่วมฝึกอบรมได้พัฒนาทักษะที่จำเป็นสำหรับการรับมือและบริหารจัดการภัยคุกคามทางไซเบอร์ที่เกิดขึ้น

โครงสร้างหลักสูตร

หลักสูตรนี้เป็นหลักสูตรที่ให้ความรู้และความเข้าใจเกี่ยวกับ พรบ. ไซเบอร์ การปฏิบัติตามให้สอดคล้องกับความต้องการของ พรบ. ไซเบอร์ มาตรการที่จำเป็นสำหรับการบริหารจัดการภัยคุกคามทางไซเบอร์ มาตรฐาน ISO ที่เกี่ยวข้อง การจัดตั้งทีมบริหารจัดการภัยคุกคามทางไซเบอร์ และการจัดทำแผนบริหารจัดการภัยคุกคามทางไซเบอร์ ตลอดจนฝึกปฏิบัติอย่างเข้มข้นกับการวิเคราะห์และรับมือกับภัยคุกคามทางไซเบอร์ รวมถึงทักษะการจัดเก็บหลักฐานด้านคอมพิวเตอร์ รวม 24 ชั่วโมง / 4 วันทำการ

หัวข้อ	ชั่วโมง	ครั้ง (วัน)
บรรยาย และกรณีศึกษา	14	2
ฝึกปฏิบัติการ (Workshop)	10	2
รวม	**24**	**4**

เนื้อหาหลักสูตร ประกอบด้วย

- สาระสำคัญของ พรบ. ไซเบอร์
- สิ่งที่องค์กรต้องปฏิบัติตามเพื่อให้สอดคล้องกับ พรบ. ไซเบอร์
- มาตรฐานและมาตรการสำหรับการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย
- มาตรฐาน ISO ที่เกี่ยวข้องกับการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย
- ทีมบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย บทบาทและหน้าที่ความรับผิดชอบ
- นโยบายการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย
- แผนบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย
- การจัดสรรทรัพยากรเพื่อสนับสนุนและรองรับแผนบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย
- การซ้อมแผนการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย
- การวิเคราะห์กรณีศึกษาเหตุการณ์ด้านความมั่นคงปลอดภัย แต่ละกรณีจะต้องวิเคราะห์
    - การจำกัดหรือลดผลกระทบของเหตุที่เกิดขึ้น
    - การจัดเก็บข้อมูลหลักฐานด้านคอมพิวเตอร์
    - การขจัดปัญหาที่สาเหตุ
    - การกู้คืนระบบ

หลักสูตรนี้เหมาะสำหรับ

- ผู้ปฏิบัติงานในศูนย์ปฏิบัติการป้องระวังความมั่นคงปลอดภัย (เช่น CERT NOC เป็นต้น)
- ผู้ดูแลระบบคอมพิวเตอร์
- ผู้ดูแลเครือข่ายคอมพิวเตอร์
- เจ้าหน้าที่วิเคราะห์และออกแบบระบบ
- เจ้าหน้าที่พัฒนาระบบ
- ผู้จัดการด้านไอที

วิทยากรประจำหลักสูตร

ดร. บรรจง หะรังษี
รองกรรมการผู้จัดการ และ
ที่ปรึกษาด้านความมั่นคงปลอดภัยระบบสารสนเทศ
บริษัท ที-เน็ต จำกัด
- ISO/IEC 27001 (Certified of Lead auditor)
- ISO/IEC 20000 (Auditor Certificate) BCMS 25999
- Introduction to Capability Maturity Model Integration V1.2 Certificate

ค่าลงทะเบียน

ท่านละ 34,900 บาท (รวมภาษีมูลค่าเพิ่มแล้ว)
- เฉพาะหน่วยงานภาครัฐ และองค์กรของรัฐ ที่ไม่ใช่ธุรกิจและไม่แสวงหากำไร จะได้รับการยกเว้นภาษีมูลค่าเพิ่ม
- โปรโมชั่นพิเศษ!!! ลงทะเบียนหน่วยงานเดียวกันตั้งแต่ 2 ท่านขึ้นไป รับส่วนลดทันที 10%

ระยะเวลาหลักสูตร

ระหว่างวันที่ 8 - 11 กันยายน 2568
เวลา 9.00 - 16.00 น. (รวมระยะเวลาอบรม จำนวน 4 วัน)

สถานที่อบรม

โรงแรมเซ็นจูรี่ พาร์ค กรุงเทพ
เลขที่ 9 ถนนราชปรารภ เขตราชเทวี
กรุงเทพมหานคร

หมายเหตุ
- หากท่านต้องการยกเลิกการลงทะเบียนกรุณาแจ้งยืนยันการยกเลิก เป็นลายลักษณ์อักษร อย่างน้อย 7 วันทำการก่อนวันจัดงาน หากการแจ้งยกเลิกล่าช้ากว่าเวลาที่กำหนดดังกล่าว ทางสถาบันฯ ขอสงวนสิทธิ์หักค่าดำเนินการ คิดเป็นจำนวนเงิน 30% จากค่าลงทะเบียนจำนวนเต็ม
- สถาบันพัฒนาบุคลากรแห่งอนาคต ขอสงวนสิทธิ์ในการเปลี่ยนแปลงเนื้อหาหลักสูตร วิทยากร ตามความเหมาะสมและความจำเป็น เพื่อประโยชน์สูงสุดของผู้เข้ารับการอบรม
- ผู้เข้าอบรมต้องมีเวลาเรียนไม่ต่ำกว่า 80% และทำกิจกรรมทุกหัวข้อของหลักสูตร จึงจะได้รับวุฒิบัตรจากสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.)

ศึกษารายละเอียดเพิ่มเติมได้ที่ https://www.career4future.com/csm

สอบถามรายละเอียดเพิ่มเติมได้ที่ 0 2644 8150 ต่อ 81891, 81898 E-mail: npd@nstda.or.th

ฉบับแก้ไข วันที่ 26 พฤษภาคม 2568