



SOC

Security Operations Center



หลักสูตร

ศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

รุ่นที่ 5

มุ่งเน้นการฝึกปฏิบัติ
เฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ
ภายใต้ศูนย์ SOC อย่างเข้มข้น



Key Highlights

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



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 เหล่านี้ส่วนก่อให้เกิดความจำเป็นที่จะต้องมีการเฝ้าระวังและป้องกันระบบและอุปกรณ์ขององค์กรให้มีความมั่นคงปลอดภัยอย่างเพียงพอและตลอดเวลา

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 ที่เกี่ยวข้องกับการเฝ้าระวังความมั่นคงปลอดภัย ได้แก่ การแจ้ง เตือนประเภทต่างๆ (Alert) และรายงานประเภทสถิติต่างๆ (Dashboard) ที่จำเป็นต่อการใช้งาน
- การใช้เครื่องมือและจัดเก็บข้อมูลล็อกให้สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยขององค์กร ตลอดจนกฎหมาย และระเบียบข้อบังคับที่เกี่ยวข้อง
- การวิเคราะห์หาช่องโหว่ในระบบคอมพิวเตอร์ เพื่อตรวจสอบหาช่องทางการบุกรุกหรือการเข้าถึง เครือข่ายและระบบสารสนเทศที่ผิดปกติ และหาแนวทางป้องกันระบบ
- การใช้เครื่องมือในการเฝ้าระวังและติดตามการทำงานของระบบและอุปกรณ์ต่างๆ

หลักสูตรนี้เหมาะสำหรับ

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

วิทยากรประจำหลักสูตร



ดร. อรรถ หงษ์ศรี

รองกรรมการผู้จัดการ และที่ปรึกษาด้านความมั่นคงปลอดภัยระบบสารสนเทศ บริษัท ที-เน็ต จำกัด



อาจารย์ เจษฎา ทองกันเหลือง

กรรมการผู้จัดการ บริษัท ที-เน็ต ไอที โซลูชัน จำกัด

ระยะเวลาหลักสูตร

ระหว่างวันที่ 18 - 21 พฤศจิกายน 2568
เวลา 9.00 - 16.00 น. (รวมระยะเวลาอบรม จำนวน 4 วัน)

ค่าลงทะเบียน

ท่านละ 32,100 บาท (รวมภาษีมูลค่าเพิ่มแล้ว)

- เฉพาะหน่วยงานภาครัฐ และองค์กรของรัฐที่ไม่ใช้รัฐกิจและไม่แสวงหากำไร จะได้รับการยกเว้นภาษีมูลค่าเพิ่ม

สถานที่อบรม



โรงแรมเซ็นจูรี่ พาร์ค กรุงเทพฯ
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

ใบลงทะเบียน

หลักสูตรศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ รุ่นที่ 5 (Security Operations Center: SOC)

รายละเอียดผู้เข้ารับการอบรม (กรุณาเขียนตัวบรรจง ครบถ้วน และถูกต้อง เพื่อใช้ในการออกวุฒิบัตร)

ประเภทหน่วยงาน

- ราชการ
- รัฐวิสาหกิจ
- เอกชน
- ส่วนตัว

ต้องการออกใบเสร็จในนาม

- องค์กร
- ส่วนบุคคล (โปรดระบุเลขบัตรประชาชน)

ต้องการระบุชื่อผู้เข้าอบรมในใบเสร็จหรือไม่

- ต้องการ
- ไม่ต้องการ

1

คำนำหน้า (ไทย) นาย/นาง/นางสาว/อื่นๆ
ชื่อ-สกุล (ไทย)
ชื่อ-สกุล (อังกฤษ)
ตำแหน่งงาน โทรศัพท์/มือถือ
E-mail (ใช้เป็น Log in เข้าสู่ระบบ)

2

คำนำหน้า (ไทย) นาย/นาง/นางสาว/อื่นๆ
ชื่อ-สกุล (ไทย)
ชื่อ-สกุล (อังกฤษ)
ตำแหน่งงาน โทรศัพท์/มือถือ
E-mail (ใช้เป็น Log in เข้าสู่ระบบ)

3

คำนำหน้า (ไทย) นาย/นาง/นางสาว/อื่นๆ
ชื่อ-สกุล (ไทย)
ชื่อ-สกุล (อังกฤษ)
ตำแหน่งงาน โทรศัพท์/มือถือ
E-mail (ใช้เป็น Log in เข้าสู่ระบบ)

ที่อยู่สำหรับออกใบกำกับภาษี/ใบเสร็จรับเงิน

ชื่อองค์กร (ไทย)
ชื่อองค์กร (อังกฤษ)
หมายเลขประจำตัวผู้เสียภาษี สำนักงานใหญ่ สาขา (โปรดระบุ)
ห้อง ชั้น อาคาร/หมู่บ้าน เลขที่ หมู่ที่ ซอย
ถนน แขวง/ตำบล เขต/อำเภอ
จังหวัด รหัสไปรษณีย์ โทรศัพท์ ต่อ โทรสาร
ชื่อ-สกุล ผู้ประสานงาน โทรศัพท์ ต่อ E-mail

ท่านได้รับข่าวสารการจัดงานนี้จาก

- จดหมายเชิญ
- เว็บไซต์ career4future.com
- Facebook/Twitter
- Line
- เพื่อนหรือคนรู้จักแนะนำ
- ช่องทางอื่น (โปรดระบุ)

รายละเอียดค่าลงทะเบียน (รวมภาษีมูลค่าเพิ่มแล้ว)

| หลักสูตร | ค่าลงทะเบียน (บาท) |
|---|--------------------|
| หลักสูตร ศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ รุ่นที่ 5 (Security Operations Center: SOC) วันที่ 18 - 21 พฤศจิกายน 2568 ณ โรงแรมเซ็นจูรี่ พาร์ค กรุงเทพฯ | 32,100 |

เฉพาะหน่วยงานภาครัฐ และองค์กรของรัฐ ที่ไม่ใช้ธุรกิจและไม่แสวงหากำไร จะได้รับการยกเว้นภาษีมูลค่าเพิ่ม

4 ช่องทางการลงทะเบียน


- Website: www.career4future.com/css
- Call Center: ศูนย์บริการ 02-644-8150
ต่อ 81892 มือถือ 085-211-9709,
คุณสุรีย์ 02-644-8150 ต่อ 81904
มือถือ 084-051-3564
- E-mail: npd@nstda.or.th


วิธีการชำระเงิน

ท่านสามารถชำระเงินโดย การโอนเงินหรือนำฝากเช็คธนาคาร ได้ทั้ง 2 ธนาคารดังนี้

ชื่อบัญชี (ภาษาไทย): สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ

ชื่อบัญชี (ภาษาอังกฤษ): National Science and Technology Development Agency

 ธนาคารกรุงเทพ สาขา: อุทยานวิทยาศาสตร์ เลขที่บัญชี: 080-0-00001-0 ประเภทบัญชี: เงินฝากสะสมทรัพย์

 ธนาคารกรุงไทย สาขา: ตลาดไท เลขที่บัญชี: 152-1-32668-1 ประเภทบัญชี: ออมทรัพย์

แล้วส่งหลักฐานการโอนเงินมาที่ e-mail: npd@nstda.or.th

หมายเหตุ

- กรุณาชำระเงินภายใน วันที่ 10 พฤศจิกายน 2568
- ค่าลงทะเบียนรวม อาหารกลางวัน และอาหารว่าง 2 มื้อต่อวัน เอกสารประกอบการอบรม และภาษีมูลค่าเพิ่ม
- ขอสงวนสิทธิ์ในการเปลี่ยนแปลงกำหนดการตามความเหมาะสม
- สถาบันฯ เป็นหน่วยงานราชการ ได้รับการยกเว้นไม่ต้องหักภาษี ณ ที่จ่าย 3%
- ข้าราชการมีสิทธิ์เบิกค่าลงทะเบียนได้ตามระเบียบกระทรวงการคลัง และเข้าร่วมอบรมสัมมนาได้ โดยไม่ต้องเป็นวันลา
- ค่าใช้จ่ายในการส่งบุคลากรเข้าอบรมทางวิชาชีพของบริษัทหรือห้างหุ้นส่วนนิติบุคคล สามารถนำไปลดหย่อนภาษีได้ 200%
- หากท่านต้องการยกเลิกการลงทะเบียน กรุณาแจ้งยืนยันการยกเลิกเป็นลายลักษณ์อักษร อย่างน้อย 7 วันทำการ ก่อนวันจัดงาน หากการแจ้งยกเลิกล่าช้ากว่าเวลาที่กำหนดดังกล่าว ทางสถาบันฯ ขอสงวนสิทธิ์ในการหักค่าดำเนินการ คิดเป็นจำนวนเงิน 30% จากค่าลงทะเบียนจำนวน

สถานที่อบรม

โรงแรมเซ็นจูรี่ พาร์ค กรุงเทพฯ
เลขที่ 9 ถนนราชปรารภ เขตราชเทวี
กรุงเทพมหานคร



สถาบันพัฒนาบุคลากรแห่งอนาคต (Career for the Future Academy)
73/1 อาคารสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.) ชั้น 6
ถนนพระรามที่ 6 แขวงทุ่งพญาไท เขตราชเทวี กรุงเทพฯ 10400
โทรศัพท์ 0 2644 8150 โทรสาร 0 2644 8110

Follow Us: <https://www.facebook.com/Career4FutureAcademy>

