งานพัฒนาองค์กรและขับเคลื่อนกำลังคน
รับวันที่ 24 ก.พ. 63
เวลา 16.00
เลขที่รับ 165

สถาบันพัฒนาสุขภาวะเขตเมือง
รับวันที่ 21 / ก.พ. / 63
เลขที่ 447
เวลา 10.00 น.

สวทช NSTDA

ที่ อว ๖๐๐๑/ว ๑๖๖๗

๓ กุมภาพันธ์ ๒๕๖๓

กรมอนามัย
เลขรับ ๑๒๕๗๑
วันที่ ๑๙ ก.พ. ๒๕๖๓
เวลา ๑๐.๑๕ น.

เรื่อง ขอเชิญส่งบุคลากรเข้าร่วมการฝึกอบรม

เรียน อธิบดี กรมอนามัย

สิ่งที่ส่งมาด้วย แผ่นพับแนะนำหลักสูตร

ด้วย สถาบันพัฒนาบุคลกรแห่งอนาคต สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ มีกำหนดจัดอบรมหลักสูตรเทคโนโลยีสารสนเทศและการจัดการขั้นสูง ประกอบด้วย

๑. หลักสูตรการบริหารจัดการและการรับมือกับภัยคุกคามทางไซเบอร์ (Cyber Security Incident Management: CSM) อบรมระหว่างวันที่ ๒๔ – ๒๗ มีนาคม ๒๕๖๓ เวลา ๐๙.๐๐–๑๖.๐๐ น. ณ โรงแรมเดอะควอเตอร์อารีย์ บาย ยูเอชจี วัตถุประสงค์เพื่อสร้างความรู้และความเข้าใจเกี่ยวกับ พรบ. ไซเบอร์ การปฏิบัติตามให้สอดคล้องกับความต้องการของ พรบ. ไซเบอร์ มาตรการที่จำเป็นสำหรับการบริหารจัดการภัยคุกคามทางไซเบอร์ มาตรฐาน ISO ที่เกี่ยวข้อง การจัดตั้งทีมบริหารจัดการภัยคุกคามทางไซเบอร์ การจัดทำแผนบริหารจัดการภัยคุกคามทางไซเบอร์ การวิเคราะห์และรับมือกับภัยคุกคามทางไซเบอร์ รวมถึงทักษะการจัดเก็บหลักฐานด้านคอมพิวเตอร์ได้อย่างถูกต้องและมีประสิทธิภาพ

๒. หลักสูตรศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ (Security Operations Center: SOC) รุ่นที่ ๓ อบรมระหว่างวันที่ ๒๑ – ๒๔ เมษายน ๒๕๖๓ เวลา ๐๙.๐๐–๑๖.๐๐ น. ณ โรงแรมเดอะควอเตอร์อารีย์ บาย ยูเอชจี วัตถุประสงค์เพื่อเสริมสร้างความรู้ แนวความคิด และหลักการของศูนย์เฝ้าระวังด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ โดยเน้นการฝึกปฏิบัติการจัดตั้งศูนย์ฯ การจัดทำรายงาน การวิเคราะห์ข้อมูลล็อก และการจัดเก็บหลักฐานเหตุการณ์ด้านความมั่นคงปลอดภัย เพื่อเข้าถึงและแก้ไขการบุกรุกเครือข่ายและระบบสารสนเทศต่างๆ ที่ผิดปกติอย่างรวดเร็วและมีประสิทธิภาพ

ในการนี้ สถาบันฯ จึงขอเชิญท่านหรือผู้แทนเข้าร่วมการฝึกอบรมหลักสูตรดังกล่าว ตามวัน เวลา และสถานที่ดังกล่าวข้างต้น โดยท่านสามารถดูรายละเอียดเพิ่มเติมได้จากเว็บไซต์ www.NSTDAacademy.com หรือสอบถามรายละเอียดเพิ่มเติมได้ที่ สถาบันพัฒนาบุคลากรแห่งอนาคต หมายเลขโทรศัพท์ ๐ ๒๖๔๔ ๘๑๕๐ ต่อ ๘๑๘๙๑, ๘๑๘๙๒ ทั้งนี้ ผู้เข้าอบรมสามารถเบิกค่าลงทะเบียนและไม่ถือเป็นวันลาตามระเบียบกระทรวงการคลัง และค่าใช้จ่ายในการส่งบุคลากรเข้าอบรมของบริษัทหรือห้างหุ้นส่วนนิติบุคคลสามารถนำไปลดหย่อนภาษีได้ ๒๐๐%

จึงเรียนมาเพื่อโปรดพิจารณา

ขอแสดงความนับถือ

(นายศิริชัย กิตติวราพงศ์)
ผู้อำนวยการ
สถาบันพัฒนาบุคลากรแห่งอนาคต
ปฏิบัติการแทนผู้อำนวยการ
สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ

เรียน หน่วยงานในสังกัดกรมอนามัย
ทั้งส่วนกลางและส่วนภูมิภาค
เพื่อโปรดทราบ จะเป็นพระคุณ

๑๙ ก.พ. ๖๓
(นายวิโรจน์ วัชระเกียรติศักดิ์)
นักวิชาการสิ่งแวดล้อมชำนาญการพิเศษ
ปฏิบัติหน้าที่เลขานุการกรม

สถาบันพัฒนาบุคลากรแห่งอนาคต
โทร. ๐ ๒๖๔๔ ๘๑๕๐ ต่อ ๘๑๘๙๒ (เมธภัค)
โทรสาร ๐ ๒๖๔๔ ๘๑๑๐

CSM+SOC3

(นายเกษม เวชสุทธานนท์)
ผู้อำนวยการสถาบันพัฒนาสุขภาวะเขตเมือง

สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ
๑๑๑ อุทยานวิทยาศาสตร์ประเทศไทย ถนนพหลโยธิน ตำบลคลองหนึ่ง อำเภอคลองหลวง จังหวัดปทุมธานี ๑๒๑๒๐ โทรศัพท์ ๐ ๒๕๖๔ ๗๐๐๐ โทรสาร ๐ ๒๕๖๔ ๗๐๐๒-๕
National Science and Technology Development Agency
111 Thailand Science Park, Phahonyothin Road, Khlong Nueng, ...
Tel. +66 2564 7000 Fax. +66 2564 7002-5 http://www.nstda.or.th

(นายยงยุส หัถพรสวรรค์)
นายแพทย์เชี่ยวชาญ (ด้านเวชกรรม)
รองผู้อำนวยการสถาบันพัฒนาสุขภาวะเขตเมือง

12471

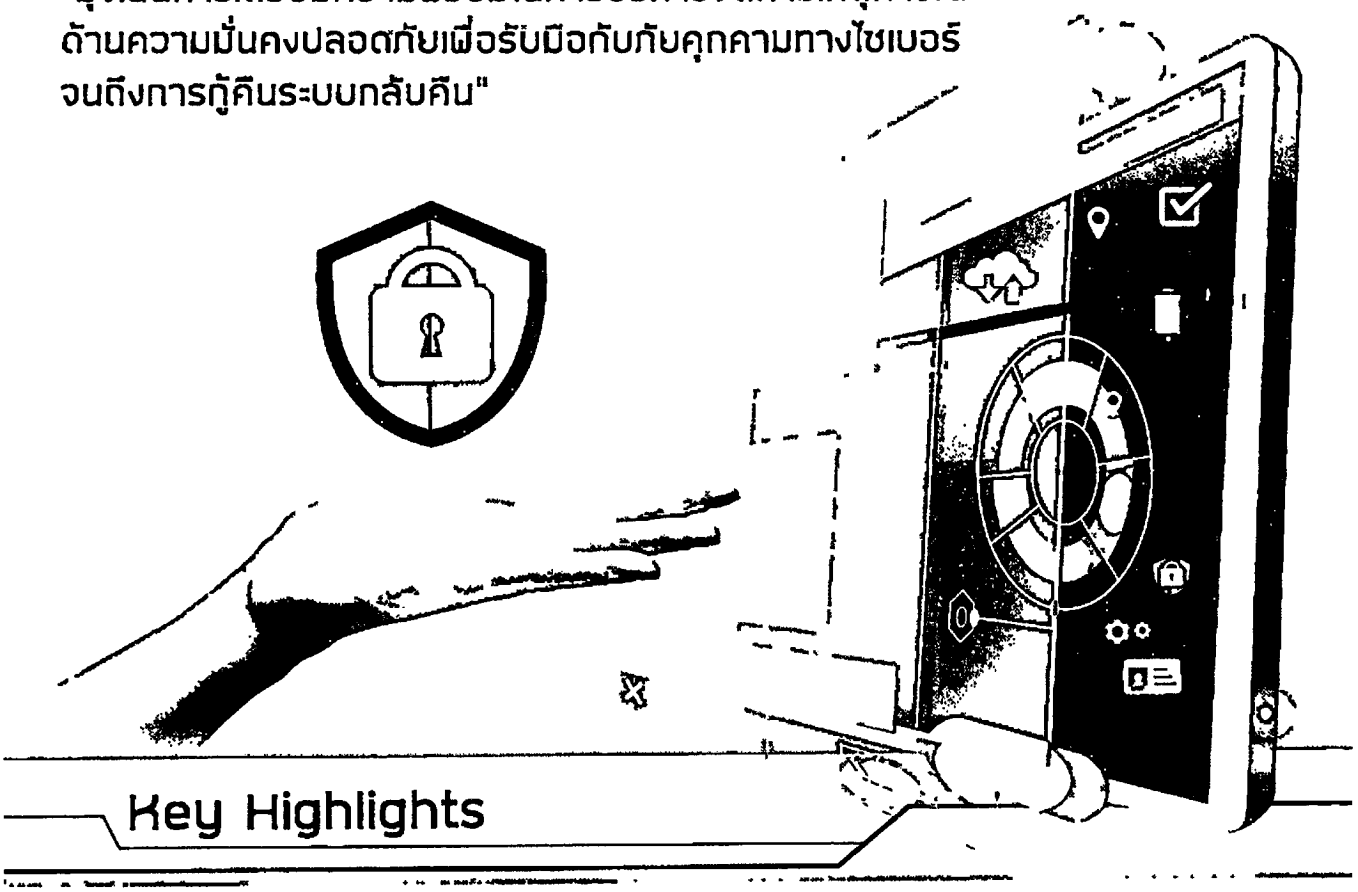
Career for the Future Academy
สถาบันพัฒนาบุคลากรแห่งอนาคต
สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ

หลักสูตร

การบริหารจัดการและการรับมือกับภัยคุกคามทางไซเบอร์

Cyber Security Incident Management: CSM

"มุ่งเน้นการเตรียมความพร้อมในการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยเพื่อรับมือกับภัยคุกคามทางไซเบอร์ จนถึงการกู้คืนระบบกลับคืน"



Key Highlights

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

http://www.NSTDAAcademy.com/csm

CSM หลักสูตรการบริหารจัดการและการรับมือกับภัยคุกคามทางไซเบอร์
Cyber Security Incident Management: CSM

โครงสร้างหลักสูตร

หลักสูตรนี้มุ่งเน้นการสร้างความรู้ความเข้าใจเกี่ยวกับ พรบ. ไซเบอร์ การปฏิบัติตามให้สอดคล้องกับความต้องการของ พรบ. ไซเบอร์ มาตรการที่จำเป็นสำหรับการบริหารจัดการภัยคุกคามทางไซเบอร์ มาตรฐาน ISO ที่เกี่ยวข้อง การจัดตั้งทีมบริหารจัดการภัยคุกคามทางไซเบอร์ และการจัดทำแผนบริหารจัดการภัยคุกคามทางไซเบอร์ ตลอดจนฝึกปฏิบัติอย่างเข้มข้นในการวิเคราะห์และรับมือกับภัยคุกคามทางไซเบอร์ รวมถึงฝึกทักษะการจัดเก็บหลักฐานด้านคอมพิวเตอร์
รวม 24 ชั่วโมง / 4 วันทำการ

บรรยาย	14	2
ปฏิบัติการ (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

วิทยากรประจำหลักสูตร

ดร. บรรจง ทะรังษี
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

หลักสูตรนี้เหมาะสำหรับ

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

ค่าลงทะเบียน

ท่านละ 34,900 บาท (ราคานี้รวมภาษีมูลค่าเพิ่มแล้ว)
โปรโมชั่นพิเศษ!! หากชำระเงินภายในวันที่ 13 มีนาคม 2563
รับส่วนลดทันที 10% เหลือชำระเพียง 31,410 บาท
(รวมภาษีมูลค่าเพิ่มแล้ว)
หมายเหตุ: หากท่านต้องการยกเลิกการลงทะเบียนกรุณาแจ้งยืนยันการยกเลิกเป็นลายลักษณ์อักษรอย่างน้อย 7 วันทำการก่อนวันจัดงาน หากการแจ้งยกเลิกล่าช้ากว่าเวลาที่กำหนดดังกล่าว ทางสถาบันฯ ขอสงวนสิทธิ์ในการหักค่าดำเนินการคิดเป็นจำนวนเงิน 30% จากค่าลงทะเบียนเต็มจำนวน

ระยะเวลาของหลักสูตร

ระหว่างวันที่ 24-27 มีนาคม 2563
เวลา 9.00-16.00 น. (รวมระยะเวลาอบรม จำนวน 4 วัน)

สถานที่ฝึกอบรม

ณ โรงแรมเดอะควอเตอร์อารีย์ บาย ยูเอชจี

หมายเหตุ:
1. สถาบันพัฒนาบุคลากรแห่งอนาคต ขอสงวนสิทธิ์ในการเปลี่ยนแปลงเนื้อหาหลักสูตร วิทยากร ตามความเหมาะสมและความจำเป็น เพื่อประโยชน์สูงสุดของผู้เข้ารับการฝึกอบรม
2. ผู้เข้าอบรมต้องมีเวลาเรียนไม่ต่ำกว่า 80% และทำกิจกรรมทุกหัวข้อของหลักสูตร จึงจะได้รับวุฒิบัตรจากสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.)

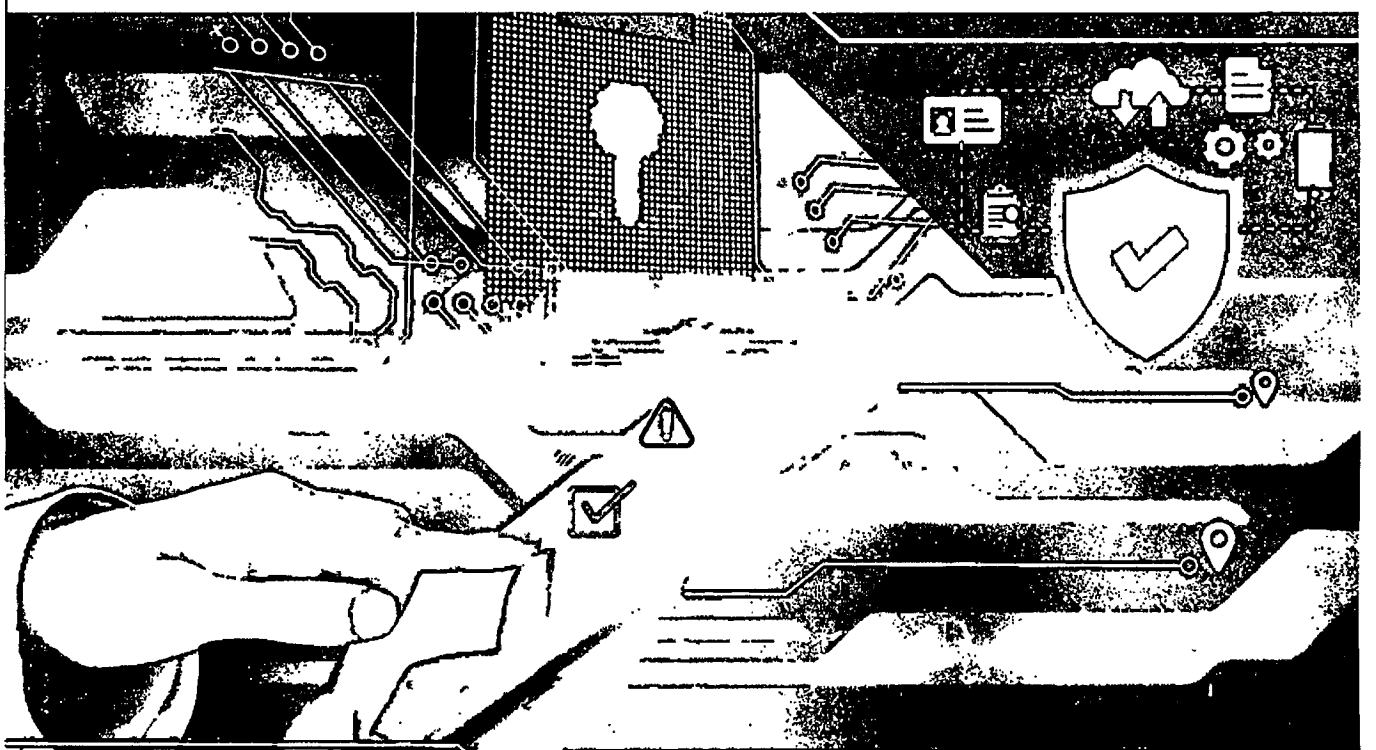
ศึกษารายละเอียดเพิ่มเติมได้ที่ http://www.NSTDAAcademy.com/csm
สอบถามรายละเอียดเพิ่มเติมได้ที่ 0 2644 8150 ต่อ 81891, 81892 E-mail: npd@nstda.or.th

Career for the Future Academy
สถาบันพัฒนาบุคลากรแห่งอนาคต
สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ

หลักสูตรศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ รุ่นที่ 3

Security Operations Center: SOC

มุ่งเน้นการฝึกปฏิบัติเฝ้าระวังความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศภายใต้ศูนย์ SOC อย่างเข้มข้น"



Key Highlights

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

SOC หลักสูตรศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ รุ่นที่ 3

Security Operations Center: SOC

โครงสร้างหลักสูตร

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

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

เนื้อหาหลักสูตร ประกอบด้วย

- มาตรฐานและกระบวนการสำหรับการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย
- กระบวนการ บทบาท และหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องในการเฝ้าระวังด้านความมั่นคง ปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศ
- การแบ่งแยกเหตุการณ์แจ้งเตือน (Event) หรือ เหตุการณ์ด้านความมั่นคงปลอดภัยให้ชัดเจน (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 เพื่อตรวจสอบหาช่องทางการบุกรุกหรือการเข้าถึงเครือข่ายและระบบสารสนเทศที่ผิดปกติ และหาแนวทางป้องกันระบบ
- การใช้เครื่องมือในการเฝ้าระวังและติดตามการทำงานของระบบและอุปกรณ์ต่างๆ

วิทยากรประจำหลักสูตร

ดร. บรรจง ทะรังษี
รองกรรมการผู้จัดการ และที่ปรึกษาด้านความมั่นคงปลอดภัยระบบสารสนเทศ
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

นายเจษฎา ทองก้านเหลือง
ผู้จัดการฝ่ายความมั่นคงปลอดภัย
บริษัท ที-เน็ต จำกัด
Cisco Certified Network Associate (CCNA),
Certified Ethical Hacker (CEH),
Certified Hacking Forensic Investigator (CHFI),
Certified Security Analyst (ECSA),
Peplink Certified Engineer (PCE),
Peplink Sales Specialist (PSS), CompTIA Network+,
CompTIA CySA+

หลักสูตรนี้เหมาะสำหรับ

- ผู้ปฏิบัติงานในศูนย์ปฏิบัติการป้องกันและระมัดระวังความมั่นคงปลอดภัย (เช่น CERT NOC เป็นต้น)
- ผู้ดูแลระบบ
- ผู้ดูแลเครือข่าย
- ผู้จัดการด้านไอที
- ผู้ปฏิบัติงานที่เกี่ยวข้องกับการเฝ้าระวังระบบและอุปกรณ์ต่างๆ ขององค์กร

ค่าลงทะเบียน

ท่านละ 34,900 บาท (รวมภาษีมูลค่าเพิ่มแล้ว)
โปรโมชั่นพิเศษ!!! ลงทะเบียนหน่วยงานเดียวกันตั้งแต่ 2 ท่านขึ้นไป
รับส่วนลดทันที 10% เหลือชำระเพียงท่านละ 31,410 บาท
(ออกใบเสร็จรับเงินรวมกัน 1 ใบ)
หมายเหตุ: หากท่านต้องการยกเลิกการลงทะเบียนกรุณาแจ้งยืนยันการยกเลิกเป็นลายลักษณ์อักษรอย่างน้อย 7 วันทำการก่อนวันจัดงาน หากการแจ้งยกเลิกล่าช้ากว่าเวลาที่กำหนดดังกล่าว ทางสถาบันฯ ขอสงวนสิทธิ์ในการหักค่าดำเนินการคิดเป็นจำนวนเงิน 30% จากค่าลงทะเบียนเต็มจำนวน

ระยะเวลาของหลักสูตร

ระหว่างวันที่ 21-24 เมษายน 2563
เวลา 9.00 - 16.00 น. (รวมระยะเวลาอบรม จำนวน 4 วัน)

สถานที่ฝึกอบรม

โรงแรมเดอะควอเตอร์อารีย์ บาย ยูเอชจี

หมายเหตุ:
1. สถาบันพัฒนาบุคลากรแห่งอนาคต ขอสงวนสิทธิ์ในการเปลี่ยนแปลงเนื้อหาหลักสูตร วิทยากร ตามความเหมาะสมและความจำเป็น เพื่อประโยชน์สูงสุดของผู้เข้ารับการฝึกอบรม
2. ผู้เข้าอบรมต้องมีเวลาเรียนไม่ต่ำกว่า 80% และทำกิจกรรมทุกหัวข้อของหลักสูตร จึงจะได้รับวุฒิบัตรจากสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.)

ศึกษารายละเอียดเพิ่มเติมได้ที่ http://www.NSTDAAcademy.com/soc

สอบถามรายละเอียดเพิ่มเติมได้ที่ 0 2644 8150 ต่อ 81891, 81892 E-mail: npd@nstda.or.th