การฝึกยกระดับฝีมือ

หลักสูตร การจัดการเหตุการณ์และการรักษาความมั่นคงปลอดภัยของข้อมูล
(Security Information and Event Management: SIEM)
รหัสหลักสูตร 10120014220501

สถาบันพัฒนาบุคลากรดิจิทัล
กรมพัฒนาฝีมือแรงงาน

ผู้อนุมัติหลักสูตร	นายนิธิภัทร ศรีธัญญา ผู้อำนวยการสถาบันพัฒนาบุคลากรดิจิทัล	
วันที่อนุมัติ 15 มี.ค. 2567	จำนวน ...6...แผ่น	ปรับปรุงครั้งที่ ...-... /...-...

การฝึกยกระดับฝีมือ
หลักสูตร การจัดการเหตุการณ์และการรักษาความมั่นคงปลอดภัยของข้อมูล
(Security Information and Event Management: SIEM)
รหัสหลักสูตร 10120014220501
สถาบันพัฒนาบุคลากรดิจิทัล กรมพัฒนาฝีมือแรงงาน กระทรวงแรงงาน

1. วัตถุประสงค์

เพื่อให้ผู้รับการฝึกมีความรู้และทักษะ ตลอดจนมีทัศนคติที่เกี่ยวกับการดูแลรักษาความปลอดภัยด้านสารสนเทศขององค์กรหรือหน่วยงาน โดยสามารถ

1.1 อธิบายในหลักการของระบบบริหารเหตุการณ์และข้อมูลการรักษาความมั่นคงปลอดภัย (SIEM) ได้

1.2 จัดเก็บข้อมูลเหตุการณ์ต่าง ๆ ที่เกิดขึ้นในระบบสารสนเทศได้

1.3 สืบค้นข้อมูลเหตุการณ์ต่าง ๆ ในระบบสารสนเทศที่จัดเก็บไว้ได้

1.4 เฝ้าระวังและวิเคราะห์เหตุการณ์ภัยคุกคามทางไซเบอร์ และการใช้งานการแจ้งเตือนเมื่อมีเหตุการณ์ตามเงื่อนไขที่กำหนดหรือระบุไว้

1.5 จัดทำรายงานการวิเคราะห์และสรุปเหตุการณ์ในรูปแบบต่าง ๆ ของข้อมูลระบบสารสนเทศที่จัดเก็บไว้ได้

2. ระยะเวลาการฝึก

ผู้รับการฝึกจะได้รับการฝึกทั้งในภาคทฤษฎีและภาคปฏิบัติ โดยหน่วยงานสังกัดกรมพัฒนาฝีมือแรงงานหรือหน่วยงานที่เกี่ยวข้อง ระยะเวลาการฝึก 30 ชั่วโมง

3. คุณสมบัติของผู้รับการฝึก

3.1 มีความรู้พื้นฐาน มีประสบการณ์การทำงาน หรือประกอบอาชีพที่เกี่ยวข้องกับการใช้คอมพิวเตอร์หรือเครือข่ายคอมพิวเตอร์ ไม่น้อยกว่า 2 ปี หรือ

3.2 มีการศึกษาไม่ต่ำกว่าระดับประกาศนียบัตรวิชาชีพ (ปวช.) หรือเทียบเท่า ในสาขาเทคโนโลยีสารสนเทศหรือสาขาด้านคอมพิวเตอร์

3.3 ผ่านการฝึกทักษะออนไลน์ (DSD Online Training) ของกรมพัฒนาฝีมือแรงงาน หลักสูตร Basic Network สำหรับมือใหม่สาย IT

3.4 มีอายุตั้งแต่ 18 ปี ขึ้นไป

3.5 มีความรู้ภาษาอังกฤษเบื้องต้น

3.6 มีสภาพร่างกายที่ไม่เป็นอุปสรรคต่อการฝึก และสามารถเข้ารับการฝึกได้ตลอดหลักสูตร

3.7 กรณีผู้เข้ารับการฝึกเป็นแรงงานในสถานประกอบกิจการ ต้องเป็นผู้ปฏิบัติงานในตำแหน่ง ด้านการดูแลความปลอดภัยด้านสารสนเทศขององค์กรหรือเป็นผู้ปฏิบัติงานที่เกี่ยวข้องกับหลักสูตรหรือเป็นเจ้าหน้าที่ที่สถานประกอบกิจการมอบหมาย

4. วุฒิบัตร

ชื่อเต็ม : วุฒิบัตรพัฒนาฝีมือแรงงาน หลักสูตร การจัดการเหตุการณ์และการรักษาความมั่นคงปลอดภัยของข้อมูล

ชื่อย่อ : วพร. การจัดการเหตุการณ์และการรักษาความมั่นคงปลอดภัยของข้อมูล

ผู้รับการฝึกต้องมีระยะเวลาการฝึกอบรมตามหลักสูตรไม่น้อยกว่าร้อยละ 80 และผ่านการประเมินผลทั้งภาคทฤษฎีและภาคปฏิบัติรวมกันตามเกณฑ์ไม่น้อยกว่าร้อยละ 60 จึงจะถือว่าผ่านการฝึก และได้รับวุฒิบัตรจากกรมพัฒนาฝีมือแรงงาน

5. หัวข้อวิชา

รหัส	หัวข้อวิชา	ชั่วโมง	
		ทฤษฎี	ปฏิบัติ
10122232201	ความรู้เบื้องต้นเกี่ยวกับระบบบริหารเหตุการณ์และข้อมูลการรักษาความมั่นคงปลอดภัย (SIEM)	1	1
10122232202	จัดเก็บข้อมูลเหตุการณ์ ข้อมูลประสิทธิภาพและความพร้อมใช้งาน	3	3
10122232203	การสืบค้นและวิเคราะห์ข้อมูลที่จัดเก็บ	3	4
10122232204	การตรวจจับเหตุการณ์โดยการใช้กฎ	3	4
10122232501	การจัดทำรายงานและแสดงข้อมูลบน Dashboard	3	4
10122219901	การวัดและประเมินผล	1	0
รวม		**14**	**16**
		30	

หมายเหตุ

ทั้งนี้ กรณีที่ผู้ประกอบกิจการตามพระราชบัญญัติส่งเสริมการพัฒนาฝีมือแรงงาน พ.ศ. 2545 ส่งลูกจ้างของตนเข้ารับการฝึกอบรมหรือจัดฝึกอบรมให้กับลูกจ้างของตน ตามคุณสมบัติของผู้รับการฝึกถือเป็นการฝึกตามพระราชบัญญัติส่งเสริมการพัฒนาฝีมือแรงงาน พ.ศ. 2545

6. เนื้อหาวิชา

10122232201 ระบบบริหารเหตุการณ์และข้อมูลการรักษาความมั่นคงปลอดภัย (SIEM) (1 : 1)

วัตถุประสงค์รายวิชา

เพื่อให้ผู้รับการฝึกมีความรู้ความข้าใจพื้นฐานและมองเห็นถึงภาพรวมเกี่ยวกับระบบบริหารเหตุการณ์และข้อมูลการรักษาความมั่นคงปลอดภัย (SIEM)

คำอธิบายรายวิชา

ศึกษาเกี่ยวกับวัตถุประสงค์ของระบบบริหารเหตุการณ์และข้อมูลการรักษาความมั่นคงปลอดภัย (SIEM) วิธีการจัดเก็บข้อมูลเหตุการณ์ รวมถึงการจัดข้อมูลให้เป็นมาตรฐาน (Normalization) และการจัดหมวดหมู่ของข้อมูล (Classification)

ฝึกปฏิบัติเกี่ยวกับการเข้าใช้งานอุปกรณ์บริหารเหตุการณ์และข้อมูลการรักษาความมั่นคงปลอดภัย FortiSIEM ซึ่งครอบคลุมถึงการตั้งค่าพื้นฐานของตัวอุปกรณ์ การตั้งค่าหรือกำหนดสิทธิ์ของผู้ใช้งาน (User Roles) รวมไปถึงการเปลี่ยนรหัสผ่านของผู้ใช้งาน พร้อมทั้งตรวจสอบผลลัพธ์ที่เกิดขึ้น

10122232202 จัดเก็บข้อมูลเหตุการณ์ ข้อมูลประสิทธิภาพและความพร้อมใช้งาน (3 : 3)

วัตถุประสงค์รายวิชา

เพื่อให้ผู้รับการฝึกมีความรู้ และทักษะเกี่ยวกับการจัดเก็บข้อมูลเหตุการณ์จากอุปกรณ์ต่าง ๆ ในระบบเครือข่าย บ่งชี้ข้อมูลที่มีประสิทธิภาพและมีความพร้อมใช้งานบนระบบบริหารเหตุการณ์และข้อมูลการรักษาความมั่นคงปลอดภัย (SIEM)

คำอธิบายรายวิชา

ศึกษาเกี่ยวกับรายละเอียดและวิธีการจัดเก็บข้อมูลเหตุการณ์ บ่งชี้ข้อมูลที่มีประสิทธิภาพและเข้าใจวิธีการจัดเก็บข้อมูลจากอุปกรณ์รักษาความปลอดภัยเครือข่าย และเครื่องคอมพิวเตอร์แม่ข่ายที่ใช้ระบบปฏิบัติการ Windows และ Linux

ฝึกปฏิบัติเกี่ยวกับการใช้งานอุปกรณ์ FortiSIEM ในการการจัดเก็บข้อมูลเหตุการณ์ แสดงข้อมูลที่มีประสิทธิภาพและการตั้งค่าใช้งานตัวอุปกรณ์ FortiSIEM ด้วยวิธีการ Discovery และการติดตั้ง Agent บนเครื่องคอมพิวเตอร์แม่ข่ายที่ใช้ทดสอบบนระบบปฏิบัติการ Window และ Linux รวมทั้งการตรวจสอบข้อมูลที่ถูกจัดเก็บบนตัวอุปกรณ์ FortiSIEM ให้เป็นมาตรฐานและหมวดหมู่ (Normalization and Classification)

10122232203 การสืบค้นและวิเคราะห์ข้อมูลที่จัดเก็บ (3 : 4)

วัตถุประสงค์รายวิชา

เพื่อให้ผู้รับการฝึกมีความรู้ และทักษะเกี่ยวกับการสืบค้นข้อมูลบนระบบบริหารเหตุการณ์และข้อมูลการรักษาความมั่นคงปลอดภัย (SIEM) พร้อมทั้งการเชื่อมโยงข้อมูลที่สืบค้นเพื่อค้นหาเหตุการณ์ที่เกิดขึ้นจากข้อมูลที่ได้ทำการจัดเก็บบนตัวอุปกรณ์

คำอธิบายรายวิชา

ศึกษาเกี่ยวกับแนวทางและวิธีการสืบค้นและวิเคราะห์ข้อมูลที่ได้รับการจัดเก็บบนระบบบริหารเหตุการณ์และข้อมูลการรักษาความมั่นคงปลอดภัย (SIEM) โดยรวมไปถึงการใช้งานคุณสมบัติ Structured Search Operators ต่างๆ เช่น Boolean, CONTAIN, BETWEEN เป็นต้น

ฝึกปฏิบัติเกี่ยวกับการใช้งานอุปกรณ์ FortiSIEM เพื่อทำการสืบค้นเหตุการณ์ภัยคุกคามทางไซเบอร์จากข้อมูลที่ได้จัดเก็บไว้ ด้วยการตั้งค่า Structured Search Operators ต่างๆ พร้อมทั้งตรวจสอบผลลัพธ์ที่เกิดขึ้น

10122232204 การตรวจจับเหตุการณ์โดยการใช้กฎ (3 : 4)

วัตถุประสงค์รายวิชา

เพื่อให้ผู้รับการฝึกมีความรู้เกี่ยวกับวิธีการกำหนดและตรวจจับเหตุการณ์จากข้อมูลที่ได้รับการจัดเก็บบนระบบบริหารเหตุการณ์และข้อมูลการรักษาความมั่นคงปลอดภัย (SIEM)

คำอธิบายรายวิชา

ศึกษาเกี่ยวกับแนวทางและกระบวนการทำงานของการกำหนดและตรวจจับเหตุการณ์ที่เกิดขึ้นตามที่ต้องการจากข้อมูลที่ได้รับการจัดเก็บบนระบบบริหารเหตุการณ์และข้อมูลการรักษาความมั่นคงปลอดภัย (SIEM) พร้อมทั้งวิธีการหรือเงื่อนไขของกฎ และตัวอย่างของกฎที่ถูกใช้งานอย่างแพร่หลายในระบบสารสนเทศจริงขององค์กรหรือหน่วยงานต่าง ๆ

ฝึกปฏิบัติเกี่ยวกับวิธีการสร้างและการใช้งานกฎ (Rule) บนอุปกรณ์ FortiSIEM เพื่อเฝ้าระวังและวิเคราะห์เหตุการณ์ภัยคุกคามทางไซเบอร์ และวิธีการตั้งค่าแจ้งเตือนผู้ดูแลระบบเมื่อมีเหตุการณ์ตรงตามเงื่อนไขที่กำหนดหรือตามที่กฎระบุไว้

10122232501 การจัดทำรายงานและแสดงข้อมูลบน Dashboard (3 : 4)

วัตถุประสงค์รายวิชา

เพื่อให้ผู้รับการฝึกมีความรู้ และทักษะเกี่ยวกับวิธีการนำข้อมูลที่ได้รับการจัดเก็บบนระบบบริหารเหตุการณ์และข้อมูลการรักษาความมั่นคงปลอดภัย (SIEM) มาจัดทำรายงาน และแสดงข้อมูลบน Dashboard ในรูปแบบกราฟฟิกที่เรียกว่า Visualizations

คำอธิบายรายวิชา

ศึกษาเกี่ยวกับแนวทางและกระบวนการในการจัดทำรายงานในรูปแบบต่าง ๆ จากข้อมูลที่ได้รับการจัดเก็บ พร้อมกับวิธีการจัดทำ Dashboard เพื่อใช้ในการตรวจสอบและเฝ้าระวังเหตุการณ์ของระบบบริหารเหตุการณ์และข้อมูลการรักษาความมั่นคงปลอดภัย (SIEM)

ฝึกปฏิบัติเกี่ยวกับการวิธีการสร้างรายงาน รูปแบบของรายงานที่พร้อมใช้งานต่าง ๆ (predefined report) การตั้งค่า Schedule reports เพื่อทำการออกรายงานที่ต้องการแบบอัตโนมัติตามเวลาที่กำหนด และการตั้งค่าเพื่อแสดงข้อมูลบน Dashboard ของอุปกรณ์ FortiSIEM พร้อมทั้งตรวจสอบผลลัพธ์ที่เกิดขึ้น

10122219901 การวัดและประเมินผล (1 : 0)

ประเมินความรู้ ความสามารถของผู้เข้ารับการฝึก โดยการทดสอบภาคทฤษฎีและภาคปฏิบัติระหว่างการฝึกอบรม

คณะผู้จัดทำหลักสูตร

1. นายนายอดิศร นิลวิสุทธิ์	สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
2. นายเกรียงศักดิ์ นามโคตร	บริษัท โจดอย ไอทีแอนด์เซอร์วิส จำกัด
3. ดร.พุทธคุณ พุทธวัฒนกุล	สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
4. ดร.รัฐติ์พงษ์ พุทธเจริญ	บริษัท ฟอร์ทิเนท ซีเคียวริตี้ เน็ทเวิร์ค (ประเทศไทย) จำกัด
5. นายนที ราชฉวาง	ผู้อำนวยการกลุ่มงานพัฒนาหลักสูตรและเทคโนโลยีการฝึก กองพัฒนาผู้ฝึกและเทคโนโลยีการฝึก
6. นายทวีศักดิ์ เจริญศิลป์	นักวิชาการพัฒนาฝีมือแรงงานชำนาญการ สถาบันพัฒนาฝีมือแรงงาน 13 กรุงเทพมหานคร
7. นายพจเร มัดจันทร์	นักวิชาการพัฒนาฝีมือแรงงานชำนาญการ สถาบันพัฒนาบุคลากรดิจิทัล
8. นางสาวกฤติการ์ พะกะจ่าง	นักวิชาการพัฒนาฝีมือแรงงานปฏิบัติการ สถาบันพัฒนาบุคลากรดิจิทัล
9. นางสาวอินทุอร พุทธรัตน์	นักวิชาการพัฒนาฝีมือแรงงาน สถาบันพัฒนาบุคลากรดิจิทัล

ลงนาม.....ผู้เสนอหลักสูตร
(นางสาวกฤติการ์ พะกะจ่าง)
นักวิชาการพัฒนาฝีมือแรงงานปฏิบัติการ
หัวหน้าฝ่ายแผนงานและนโยบาย

ลงนาม.....ผู้เห็นชอบหลักสูตร
(นายนพณัฐ คงจิตงาม)
นักวิชาการพัฒนาฝีมือแรงงานปฏิบัติการ
หัวหน้าฝ่ายพัฒนาฝีมือแรงงาน

ลงนาม.....ผู้อุมัติ
(นายนิธิภัทร ศรีธัญญา)
ผู้อำนวยการสถาบันพัฒนาบุคลากรดิจิทัล