โครงการฝึกอบรมพร้อมสอบมาตรฐานสากล

Empowering The Next Generation of Educators with Global Certify

"เสริมพลังการเรียนรู้ สู่โลกการศึกษาไร้ขีดจำกัด" สำหรับบุคลากรทางการศึกษา

arit

IT Specialist Certification

CYBER SECURITY

CERTIPORT
A PEARSON VUE BUSINESS

INFORMATION TECHNOLOGY SPECIALIST

รายละเอียดหลักสูตร
IT Specialist Certification: Cyber Security

ในยุคที่เทคโนโลยีสารสนเทศมีบทบาทสำคัญในทุกภาคส่วน ความปลอดภัยทางไซเบอร์กลายเป็นปัจจัยที่ไม่สามารถมองข้ามได้ หลักสูตร IT Specialist Certification: Cyber Security ของ Certiport ถูกออกแบบมาเพื่อเสริมสร้างความรู้และทักษะด้านความปลอดภัยทางไซเบอร์ให้กับบุคลากรของมหาวิทยาลัย ไม่ว่าจะเป็นอาจารย์ นักวิจัย หรือเจ้าหน้าที่ฝ่ายไอที

หลักสูตรนี้ครอบคลุมเนื้อหาที่สำคัญหลายประการ

1. **การป้องกันการโจมตีทางไซเบอร์**: ผู้เรียนจะได้เรียนรู้เกี่ยวกับวิธีการป้องกันการโจมตีทางไซเบอร์ที่หลากหลาย เช่น การโจมตีแบบฟิชชิ่งและการแฮ็ก
2. **การจัดการความเสี่ยง**: การประเมินและจัดการความเสี่ยงที่เกี่ยวข้องกับความปลอดภัยของข้อมูลและระบบ
3. **การรักษาความปลอดภัยของข้อมูล**: วิธีการปกป้องข้อมูลสำคัญจากการเข้าถึงโดยไม่ได้รับอนุญาต
4. **การตอบสนองต่อเหตุการณ์**: การเตรียมพร้อมและตอบสนองต่อเหตุการณ์ที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์
5. **การวางแผนการกู้คืนจากภัยพิบัติ**: การวางแผนและดำเนินการกู้คืนระบบและข้อมูลหลังจากเกิดเหตุการณ์ที่ไม่คาดคิด

หลักสูตรนี้เหมาะสำหรับบุคลากรในตำแหน่งต่าง ๆ

- **อาจารย์**: เพื่อเสริมสร้างความรู้และทักษะในการสอนและวิจัยด้านความปลอดภัยทางไซเบอร์
- **นักวิจัย**: เพื่อเพิ่มความสามารถในการปกป้องข้อมูลวิจัยและระบบที่ใช้ในการวิจัย
- **เจ้าหน้าที่ฝ่ายไอที**: เพื่อเพิ่มทักษะในการปกป้องและจัดการระบบเครือข่ายของมหาวิทยาลัย
- **ผู้บริหาร**: เพื่อเข้าใจและสามารถกำหนดนโยบายด้านความปลอดภัยทางไซเบอร์ได้อย่างมีประสิทธิภาพ

วัตถุประสงค์ของหลักสูตร

- เพื่อให้ผู้อบรมมีความรู้ในเรื่องหลักการพื้นฐานด้านความมั่นคงปลอดภัยไซเบอร์
- เพื่อให้ผู้อบรมมีความรู้ในเรื่องการรักษาความปลอดภัยให้กับระบบเครือข่าย
- เพื่อให้ผู้อบรมมีความรู้ในเรื่องเทคโนโลยี Endpoint Security
- เพื่อให้ผู้อบรมมีความรู้ในเรื่องการประเมินช่องโหว่ของระบบและการบริหารจัดการความเสี่ยง
- เพื่อให้ผู้อบรมมีความรู้ในเรื่องการรับมือกับสถานการณ์ด้านความมั่นคงปลอดภัยไซเบอร์

ประโยชน์ที่จะได้รับจากการอบรม

- เข้าใจหน้าที่ ความรับผิดชอบ และงาน (Job Task) ของสายงาน Cyber Security
- มีความรู้และทักษะในด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) สามารถนำไปประยุกต์ใช้เพื่อรักษาความมั่นคงปลอดภัยทางไซเบอร์ให้กับองค์กร
- สามารถเลือกใช้เทคโนโลยีเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ให้กับระบบเครือข่าย
- สามารถเลือกใช้เทคโนโลยีเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ให้กับอุปกรณ์ต่าง ๆ
- สามารถประเมินช่องโหว่ (Vulnerability Assessment) ของระบบสารสนเทศด้วยเครื่องมือที่เหมาะสม
- สามารถระบุ วิเคราะห์ ประเมิน จัดลำดับความสำคัญและเลือกกลยุทธ์ในการจัดการกับความเสี่ยงที่ส่งผลกระทบกับองค์กรได้อย่างเหมาะสม
- สามารถวางแผนรับมือภัยคุกคามทางไซเบอร์ (Incident Response) ได้อย่างเหมาะสม

ค่าลงทะเบียน (ราคาสำหรับ 2 ท่าน)

- 8,500 บาท (รวมภาษีมูลค่าเพิ่ม)
- กรณีประสงค์อบรมออนไซต์ ณ บริษัท เออาร์ไอที จำกัด
  (มีค่าอาหารว่าง อาหารกลางวันเพิ่ม 250 บาทต่อวันต่อคน)

ตัวอย่างใบประกาศนียบัตร Global – Certificate

เนื้อหาการฝึกอบรม ระยะเวลา 2 วัน (12 ชั่วโมง)

เนื้อหาการอบรม วันที่ 1

08:30 – 09:00 น. **ลงทะเบียนเข้ารับการฝึกอบรม**

09:00 – 10:30 น. **หัวข้อที่ 1 หลักการพื้นฐานด้านความมั่นคงปลอดภัยไซเบอร์**

- ความมั่นคงปลอดภัยไซเบอร์ขั้นพื้นฐาน (Cyber Security Principles)
- ภัยคุกคามและช่องโหว่ (Threats and Vulnerabilities)

10:30 – 10:45 น. ***พัก***

10:45 – 12:00 น.

- การบริหารจัดการการเข้าถึงระบบ (Access Control)
- เทคโนโลยีการเข้ารหัส (Encryption)

12:00 – 13:00 น. ***พัก***

13:00 – 14:30 น. **หัวข้อที่ 2 หลักการพื้นฐานการรักษาความปลอดภัยให้กับระบบเครือข่าย**

- ช่องโหว่ของโพรโทคอล TCP/IP
- การวางแผนผังระบบเครือข่ายให้มีความมั่นคงปลอดภัย
- โครงสร้างพื้นฐานและเทคโนโลยีของระบบเครือข่าย

14:30 – 14:45 น. ***พัก***

14:45 – 16:00 น.

- การติดตั้งระบบเครือข่ายไร้สายที่มีความมั่นคงปลอดภัยให้กับสำนักงานขนาดเล็ก
- การติดตั้งและการควบคุมการเข้าถึง (Access Control) ระบบเครือข่ายให้มีความมั่นคงปลอดภัย

เนื้อหาการอบรม วันที่ 2

09:00 – 10:30 น. **หัวข้อที่ 3 หลักการเทคโนโลยี Endpoint Security**

- การรักษาความมั่นคงปลอดภัยให้กับระบบปฏิบัติการ
- การใช้เครื่องมือ Security Endpoint เพื่อเก็บรวบรวมข้อมูลที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์
- คุณสมบัติของเครื่องมือ Security Endpoint ตามมาตรฐานและนโยบายด้านความมั่นคงปลอดภัยทางไซเบอร์
- การอัปเดตซอฟต์แวร์และฮาร์ดแวร์ (Implement software and hardware updates)
- การวิเคราะห์และแปลผล Logs
- การกำจัดมัลแวร์

10:30 – 10:45 น. ***พัก***

10:45 – 12:00 น. **หัวข้อที่ 4 การประเมินช่องโหว่ของระบบและการบริหารจัดการความเสี่ยง**

- การบริหารจัดการช่องโหว่ของระบบ
- การใช้ข่าวกรองด้านภัยคุกคามไซเบอร์ (Threat Intelligence) เพื่อหาช่องโหว่ของระบบ
  ที่มีความเป็นไปได้
- การบริหารจัดการความเสี่ยง
- แผนกู้คืนภัยพิบัติ (DR Plan) และแผนบริหารความต่อเนื่อง (BCP Plan)

12:00 – 13:00 น. ***พัก***

13:00 – 14:30 น. **หัวข้อที่ 5 การรับมือกับสถานการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ (Incident Handling)**

- การรับมือกรณีเมื่อเกิดเหตุการยกระดับสิทธิ (Privilege Escalation)
- การพิสูจน์พยานหลักฐานทางดิจิทัล (Digital Forensic) และกระบวนการพิสูจน์พยานหลักฐานทางดิจิทัล
- กรอบการปฏิบัติตามกฎหมายและระเบียบ (Compliance Frameworks) ที่เกี่ยวข้องกับการจัดการสถานการณ์ด้านความมั่นคงปลอดภัยไซเบอร์
- องค์ประกอบของการตอบสนองต่อสถานการณ์ด้านความมั่นคงปลอดภัยไซเบอร์

14:30 – 14:45 น. ***พัก***

14:45 – 16:00 น. **การสอบมาตรฐานสากล Information Technology Specialist Cybersecurity**