สมาคมนักวิจัยแห่งประเทศไทย
เลขที่ 196 อาคาร วช.8 ชั้น 2 สำนักงานการวิจัยแห่งชาติ พหลโยธิน จตุจักร กรุงเทพมหานคร 10900
โทร. 087-931-5303, 02 579 0787 Website: www.ar.or.th E-mail: ar@ar.or.th

การอบรมเชิงปฏิบัติการ
Cyber War Game: ฝึกกลยุทธ์รับมือภัยไซเบอร์สำหรับภาครัฐ

หลักการและเหตุผล

ในยุคที่เทคโนโลยีสารสนเทศและการสื่อสารมีบทบาทสำคัญต่อการดำเนินงานของภาครัฐ ความมั่นคงปลอดภัยทางไซเบอร์จึงกลายเป็นปัจจัยสำคัญที่ไม่อาจมองข้าม หน่วยงานภาครัฐต้องเผชิญกับภัยคุกคามทางไซเบอร์ที่มีความซับซ้อนและเปลี่ยนแปลงอย่างรวดเร็ว ไม่ว่าจะเป็นการโจมตีด้วยมัลแวร์ การเจาะระบบ การโจมตีแบบ DDoS หรือการแฮกข้อมูลสำคัญ ซึ่งอาจส่งผลกระทบต่อความมั่นคงของประเทศและความเชื่อมั่นของประชาชน Cyber War Game เป็นเครื่องมือการเรียนรู้เชิงปฏิบัติการที่มีประสิทธิภาพในการเสริมสร้างความเข้าใจและทักษะในการรับมือกับภัยคุกคามไซเบอร์ โดยการจำลองสถานการณ์การโจมตีและการป้องกันในรูปแบบที่ใกล้เคียงกับสถานการณ์จริง ช่วยให้เจ้าหน้าที่สามารถฝึกฝนการวิเคราะห์ การตัดสินใจ และการทำงานเป็นทีมภายใต้สถานการณ์วิกฤต หลักสูตรนี้จึงถูกออกแบบมาเพื่อให้เจ้าหน้าที่ภาครัฐได้เรียนรู้แนวคิดพื้นฐานด้านความมั่นคงปลอดภัยไซเบอร์ เข้าใจบทบาทของตนเองในการป้องกันและตอบสนองต่อเหตุการณ์ไซเบอร์ และสามารถนำความรู้ที่ได้รับไปประยุกต์ใช้ในการปฏิบัติงานจริง รวมถึงสามารถจัดกิจกรรม Cyber War Game ภายในหน่วยงานของตนเองได้อย่างมีประสิทธิภาพ

วัตถุประสงค์

- เสริมสร้างความรู้ความเข้าใจเกี่ยวกับภัยคุกคามไซเบอร์และการรับมือ
- ฝึกทักษะการวางแผน การโจมตี และการป้องกันในสถานการณ์จำลอง
- ส่งเสริมการทำงานเป็นทีมและการตัดสินใจภายใต้สถานการณ์วิกฤต
- พัฒนาศักยภาพในการจัดการ Cyber War Game ภายในหน่วยงาน

กลุ่มเป้าหมายในการอบรม

1. **เจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศ (IT Officer / System Administrator)** ผู้ดูแลระบบเครือข่ายและระบบสารสนเทศของหน่วยงาน มีหน้าที่ในการป้องกันและตอบสนองต่อเหตุการณ์ด้านไซเบอร์
2. **เจ้าหน้าที่ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Officer / SOC Analyst)** ผู้รับผิดชอบในการตรวจจับ วิเคราะห์ และจัดการกับภัยคุกคามทางไซเบอร์ รวมถึงการวางแผนรับมือเหตุการณ์
3. **ผู้บริหารหรือผู้กำหนดนโยบายด้าน IT และ Cybersecurity (IT Manager / CISO / Policy Maker)** ผู้มีบทบาทในการกำหนดทิศทาง กลยุทธ์ และนโยบายด้านความมั่นคงปลอดภัยของหน่วยงาน
4. **เจ้าหน้าที่ด้านการบริหารความเสี่ยงและการวางแผนฉุกเฉิน (Risk Management / Business Continuity Officer)** ผู้มีหน้าที่ประเมินความเสี่ยงและวางแผนการดำเนินงานต่อเนื่องเมื่อเกิดเหตุการณ์ด้านไซเบอร์
5. **เจ้าหน้าที่ฝึกอบรมหรือพัฒนาบุคลากรด้านไซเบอร์ (HRD in Cybersecurity)** ผู้ที่มีหน้าที่จัดการฝึกอบรมหรือพัฒนาศักยภาพบุคลากรในด้านความมั่นคงปลอดภัยไซเบอร์ภายในหน่วยงาน

สมาคมนักวิจัยแห่งประเทศไทย
เลขที่ 196 อาคาร วช.8 ชั้น 2 สำนักงานการวิจัยแห่งชาติ พหลโยธิน จตุจักร กรุงเทพมหานคร 10900
โทร. 087-931-5303, 02 579 0787 Website: www.ar.or.th E-mail: ar@ar.or.th

จำนวนผู้เข้าอบรม 30 คน (นำ Computer Notebook ที่ติดตั้งระบบปฏิบัติการ Windows 10 64 bit, CPU Core i5 GEN 5 ขึ้นไป, Memory ขนาด 12 GB, พื้นที่ Hard disk ขนาด 100 GB)

ประโยนชน์ที่คาดว่าจะได้รับ

1. **เพิ่มพูนความรู้และความเข้าใจเกี่ยวกับภัยคุกคามทางไซเบอร์**
   ผู้เข้าอบรมจะได้เรียนรู้ลักษณะของภัยคุกคามที่สำคัญ เช่น Malware, Ransomware, Phishing และการโจมตีแบบ APT ซึ่งช่วยให้สามารถระบุและประเมินความเสี่ยงได้อย่างแม่นยำยิ่งขึ้น
2. **พัฒนาทักษะการวางแผนและตอบสนองต่อเหตุการณ์ไซเบอร์**
   ผ่านการจำลองสถานการณ์จริง ผู้เข้าอบรมจะได้ฝึกฝนการวิเคราะห์ การตัดสินใจ และการดำเนินการตอบสนองต่อเหตุการณ์ในสถานการณ์ที่มีความกดดัน
3. **เสริมสร้างการทำงานเป็นทีมและการสื่อสารระหว่างหน่วยงาน**
   การแบ่งกลุ่มเป็นทีมผู้โจมตีและผู้ป้องกันช่วยส่งเสริมการทำงานร่วมกัน การแลกเปลี่ยนมุมมอง และการประสานงานระหว่างเจ้าหน้าที่จากหน่วยงานต่าง ๆ
4. **สามารถนำความรู้ไปประยุกต์ใช้ในการปฏิบัติงานจริง**
   ผู้เข้าอบรมจะสามารถนำแนวคิดและประสบการณ์จากการฝึกอบรมไปใช้ในการวางแผนรับมือภัยคุกคามไซเบอร์ในหน่วยงานของตนได้อย่างมีประสิทธิภาพ
5. **เตรียมความพร้อมในการจัดกิจกรรม Cyber War Game ภายในหน่วยงาน**
   ผู้เข้าอบรมจะได้รับแนวทางและเครื่องมือที่สามารถนำไปใช้ในการจัดกิจกรรมฝึกอบรมหรือซ้อมรับมือภัยคุกคามไซเบอร์ภายในองค์กรของตนเอง

สมาคมนักวิจัยแห่งประเทศไทย
เลขที่ 196 อาคาร วช.8 ชั้น 2 สำนักงานการวิจัยแห่งชาติ พหลโยธิน จตุจักร กรุงเทพมหานคร 10900
โทร. 087-931-5303, 02 579 0787 Website: www.ar.or.th E-mail: ar@ar.or.th

กำหนดการอบรมเชิงปฏิบัติการ
Cyber War Game: ฝึกกลยุทธ์รับมือภัยไซเบอร์สำหรับภาครัฐ
วันพุธที่ 16 กรกฎาคม 2568 (โรงแรมอวานี รัชดา กรุงเทพ)

09.00 - 09.10 น.	**ผู้แทนสมาคมฯ กล่าวเปิดการอบรม กล่าวถึงวัตถุประสงค์ของหลักสูตร**
09.10 - 10.30 น.	**การบรรยายหัวข้อ** - ภาพรวมของกระบวนการ Cyber War Game - ความสำคัญของ Cyber War Game สำหรับหน่วยงานภาครัฐ - ภาพรวมภัยคุกคามทางไซเบอร์ที่สำคัญ (Malware, Ransomware, etc.) - หลักการพื้นฐานของการป้องกันและตอบสนองต่อภัยคุกคาม
10.30 - 10.45 น.	**พักรับประทานอาหารว่าง**
10.45 - 12.00 น.	การจำลองสถานการณ์ Cyber War Game เบื้องต้น - แนะนำสถานการณ์จำลอง (Scenario) ที่เกี่ยวข้องกับหน่วยงานภาครัฐ - แบ่งกลุ่มผู้เข้าร่วมและกำหนดบทบาท - อธิบายกฎกติกาและเครื่องมือที่ใช้ในการจำลองสถานการณ์ - เริ่มการจำลองสถานการณ์รอบที่ 1 (เน้นการทำความเข้าใจกลไก)
12.00 - 13.00 น.	**พักรับประทานอาหารกลางวัน**
13.00 - 14.30 น.	**ดำเนินการ Cyber War Game** - ดำเนินการจำลองสถานการณ์รอบที่ 2 (เน้นการวางแผนและตอบสนอง) - ผู้ควบคุมเกม (Facilitator) ให้ข้อมูลเพิ่มเติมและกำกับดูแล - นำเสนอผลลัพธ์และเหตุการณ์สำคัญที่เกิดขึ้นในการจำลองสถานการณ์
14.30 - 14.45 น.	**พักรับประทานอาหารว่าง**
14.45 – 15.45 น.	**การบรรยายหัวข้อ** - การนำความรู้และประสบการณ์จาก Cyber War Game ไปใช้ในการปฏิบัติงานจริง แนวทางการจัดการ Cyber War Game ภายในหน่วยงาน