ประกาศคณะกรรมการส่งเสริมการพัฒนาฝีมือแรงงาน

เรื่อง มาตรฐานฝีมือแรงงานแห่งชาติ สาขาอาชีพเทคโนโลยีดิจิทัล
สาขานักปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์

อาศัยอำนาจตามความในมาตรา ๒๒ วรรคหนึ่ง แห่งพระราชบัญญัติส่งเสริมการพัฒนาฝีมือแรงงาน พ.ศ. ๒๕๔๕ และมาตรา ๓๙ (๓) แห่งพระราชบัญญัติส่งเสริมการพัฒนาฝีมือแรงงาน พ.ศ. ๒๕๔๕ ซึ่งแก้ไขเพิ่มเติมโดยพระราชบัญญัติส่งเสริมการพัฒนาฝีมือแรงงาน (ฉบับที่ ๒) พ.ศ. ๒๕๕๗ คณะกรรมการส่งเสริมการพัฒนาฝีมือแรงงานโดยความเห็นชอบของรัฐมนตรีว่าการกระทรวงแรงงาน กำหนดมาตรฐานฝีมือแรงงานแห่งชาติ สาขาอาชีพเทคโนโลยีดิจิทัล สาขานักปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ไว้ ดังนี้

ข้อ ๑ ในประกาศนี้ สาขาอาชีพเทคโนโลยีดิจิทัล สาขานักปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ หมายถึง ผู้ปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ในเครือข่ายระบบคอมพิวเตอร์ โปรแกรม และข้อมูล ที่มีความรู้ ความสามารถของการปฏิบัติในการบริหารจัดการและบำรุงรักษา (Operate and Maintain) รวบรวมข้อมูลและการปฏิบัติการ (Collect and Operate) ป้องกันรักษาความมั่นคงปลอดภัยไซเบอร์ (Protect and Defend) วิเคราะห์การป้องกันความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Defense Analysis) ออกแบบและพัฒนาระบบให้มั่นคงปลอดภัย (Designing and Building Secure Information Technology Systems) วิเคราะห์และแจ้งเตือนภัยคุกคามทางไซเบอร์ (Analyze) สืบสวนหาหลักฐาน (Investigate)

ข้อ ๒ มาตรฐานฝีมือแรงงานแห่งชาติ สาขาอาชีพเทคโนโลยีดิจิทัล สาขานักปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ แบ่งออกเป็น ๒ ระดับ ดังต่อไปนี้

๒.๑ ระดับ ๒ หมายถึง ผู้ที่มีความรู้ ความสามารถของการปฏิบัติในการบริหารจัดการข้อมูล (Data Administration) สนับสนุนทางเทคนิคและให้บริการลูกค้า (Customer Service & Technical Support) บริการเครือข่าย (Network Services) บริหารจัดการระบบ (Systems Administration) รวบรวมข้อมูลด้านความมั่นคงปลอดภัย (Collection Operations) ปฏิบัติการไซเบอร์ (Cyber Operations) วิเคราะห์การป้องกันความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Defense Analysis) สนับสนุนในการป้องกันความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Defense Infrastructure Support) ตอบสนองต่อเหตุการณ์ภัยคุกคามทางไซเบอร์ (Incident Response) ประเมิน ตรวจสอบ และจัดการช่องโหว่ (Vulnerability Assessment and Management) บริหารจัดการความเสี่ยง (Risk Management)

๒.๒ ระดับ ๓ หมายถึง ผู้ที่มีความรู้ ความสามารถของการปฏิบัติในการบริหารจัดการองค์ความรู้ (Knowledge Management) บริหารจัดการระบบ (Systems Administration) วิเคราะห์ความปลอดภัยของระบบ (Systems Analysis Security) รวบรวมข้อมูลและการปฏิบัติการ

(Collect and Operate) จัดทำแผนปฏิบัติการด้านไซเบอร์ (Cyber Operational Planning) ปฏิบัติการไซเบอร์ (Cyber Operations) วิเคราะห์การป้องกันความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Defense Analysis) ตอบสนองต่อเหตุการณ์ภัยคุกคามทางไซเบอร์ (Incident Response) ประเมิน ตรวจสอบ และจัดการช่องโหว่ (Vulnerability Assessment and Management) บริหารจัดการความเสี่ยง (Risk Management) พัฒนาซอฟต์แวร์ (Software Development) ออกแบบสถาปัตยกรรมระบบ (System Architecture) พัฒนาระบบ (System Development) วิเคราะห์และเฝ้าระวังภัยคุกคาม (Threat Analysis) ประเมินระดับความรุนแรงของช่องโหว่ (Exploitation Analysis) วิเคราะห์ข้อมูลแวดล้อมที่มีความเป็นไปได้ในการถูกโจมตีต่อระบบเป้าหมาย (Targets) สืบสวนทางดิจิทัล (Cyber Investigation) พิสูจน์หลักฐานทางดิจิทัล (Digital Forensics)

ข้อ ๓ ข้อกำหนดทางวิชาการที่ใช้เป็นเกณฑ์วัดระดับฝีมือ ความรู้ ความสามารถ และทัศนคติในการทำงานของผู้ประกอบอาชีพในสาขาอาชีพเทคโนโลยีดิจิทัล สาขานักปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ให้เป็นดังต่อไปนี้

๓.๑ มาตรฐานฝีมือแรงงานแห่งชาติ ระดับ ๒ ได้แก่

๓.๑.๑ ความรู้ ประกอบด้วยขอบเขตความรู้ ในเรื่องดังต่อไปนี้

๓.๑.๑.๑ การบริหารจัดการและบำรุงรักษา (Operate and Maintain)

(๑) การบริหารจัดการข้อมูล (Data Administration)

(ก) ความรู้เกี่ยวกับระบบปฏิบัติการ หลักการออกแบบฐานข้อมูล

(ข) การบริการแบบคลาวน์ (Cloud Services) และการติดตั้งซอฟต์แวร์ฐานข้อมูล

(ค) การตั้งค่า (Configuration) กำหนดสิทธิและนโยบาย ของระบบฐานข้อมูล

(ง) ความรู้เกี่ยวกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล

(จ) พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

(ฉ) ความรู้เกี่ยวกับความมั่นคงปลอดภัยของข้อมูล

(ช) การเข้ารหัสข้อมูลด้วยวิธีการต่าง ๆ

(ซ) การติดตั้งโครงสร้างพื้นฐานกุญแจสาธารณะ (Public Key Infrastructure : PKI) หรือเครื่องมือ หรือซอฟต์แวร์ในการเข้ารหัสข้อมูล

(ฌ) การตรวจสอบสถานะการทำงานของระบบ

(ญ) การปรับปรุงแก้ไข (Tuning) ประสิทธิภาพการทำงานของระบบ

(ฎ) การสำรองข้อมูล และการกู้คืน

(๒) การสนับสนุนทางเทคนิคและให้บริการลูกค้า (Customer Service & Technical Support)

(ก) ความรู้เกี่ยวกับระบบปฏิบัติการ ระบบเครือข่าย และระบบฐานข้อมูล

(ข) การบริการแบบคลาวน์ (Cloud Services, LDAP, Identity Access Management)

(ค) การติดตั้งระบบและอุปกรณ์เครือข่าย

(ง) การบำรุงรักษาอุปกรณ์เครือข่ายและคอมพิวเตอร์

(จ) การกู้คืนความเสียหายและความต่อเนื่องทางธุรกิจ

(ฉ) การบริการจัดการทรัพย์สิน ทักษะการแก้ปัญหา

(ช) การตรวจสอบสถานการณ์ทำงานของระบบและอุปกรณ์เครือข่าย

(ซ) การใช้คำสั่งเพื่อตรวจสอบ หรือทดสอบระบบหรืออุปกรณ์

(๓) การบริการเครือข่าย (Network Services)

(ก) ความรู้เกี่ยวกับ OSI Model, DNS, DCHP, IP Address, NAT, DMZ ACL

(ข) ความรู้เกี่ยวกับ VLAN, Port Security, ACL, Wi-Fi Security

(ค) ความรู้เกี่ยวกับ Application Protocol ประเภทของ Firewall

(ง) ความรู้เกี่ยวกับ WAN, Routing, VPN, IPSec

(จ) ความรู้เกี่ยวกับ SNMP Syslog และการใช้งาน

(ฉ) ความรู้เกี่ยวกับ Application Program (PRTG Cacti)

(ช) การวิเคราะห์ช่องโหว่ และป้องกันช่องโหว่

(ซ) การทดสอบสภาพพร้อมใช้งาน

(ฌ) การอัปเดตและการจัดการการเข้าถึง

(ญ) การติดตั้งและการกำหนดค่าเครือข่าย

(ฎ) การตรวจสอบสภาพแวดล้อม และตรวจสอบการกำหนดค่าเครือข่าย

(ฏ) การตรวจสอบการทำงานของอุปกรณ์

(ฐ) การใช้เครื่องมือสำหรับการวินิจฉัย

(ฑ) วางแผนและออกแบบการบริการเครือข่าย

(ฒ) การเลือกและการจัดซื้ออุปกรณ์

(ณ) การอัปเกรดและการบำรุงรักษา

(๔) การบริหารจัดการระบบ (Systems Administration)

(ก) ความรู้เกี่ยวกับระบบปฏิบัติการ หลักการออกแบบฐานข้อมูล

(ข) ความรู้เกี่ยวกับ Cloud Computing, Backup, Recovery, BCM, BCP

(ค) ความรู้เกี่ยวกับฮาร์ดแวร์ ซอฟต์แวร์ Inventory, Server Health Checkup

(ง) การบริหารจัดการเครื่องคอมพิวเตอร์แม่ข่าย ระบบเครือข่ายคอมพิวเตอร์

(จ) ความรู้เกี่ยวกับ Identity Access Management, Access Control List, LDAP, MS Active Directory

(ฉ) ความรู้เกี่ยวกับ Security Baseline Server hardening VA ISO/IEC27001 PDPA NIST

(ช) ความรู้เกี่ยวกับ Event Log Command Line OS และคู่มือฮาร์ดแวร์

๓.๑.๑.๒ การรวบรวมข้อมูลและการปฏิบัติการ (Collect and Operate)

(๑) การรวบรวมข้อมูลและปฏิบัติการ (Collection and Operations)

(ก) ความรู้ในการใช้เครื่องมือ เช่น Nmap, Nessus, Wireshark, Tcpdump

(ข) ความรู้เกี่ยวกับ Log Management, SIEM (Security Information and Event Management), SOAR (Security Orchestration Automation and Response)

(ค) ความรู้เกี่ยวกับ EDR (Endpoint Detection and Response)

(ง) การบริการแบบคลาวน์ (Cloud Service), Network Attached Storage (NAS)

(จ) Storage Area Network (SAN)

(๒) การปฏิบัติการไซเบอร์ (Cyber Operations)

(ก) ความรู้ในการใช้เครื่องมือ เช่น Nmap, Nessus, Burp Suite Metasploit

(ข) ความรู้เกี่ยวกับ Application Protocol

(ค) ความรู้เกี่ยวกับ IP Address, NAT, DMZ, ACL, IPS, IDS Backup

(ง) ความรู้เกี่ยวกับ Threat Intelligence

(จ) ความรู้เกี่ยวกับ Disaster Recovery forensics Threat Intelligence Backup

๓.๑.๑.๓ การป้องกันรักษาความมั่นคงปลอดภัยไซเบอร์ (Protect and Cybersecurity Defend)

(๑) การวิเคราะห์การป้องกันความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Defense Analysis)

(ก) นโยบาย ข้อกำหนดต่าง ๆ หรือมาตรฐานและกฎหมายที่เกี่ยวข้อง

(ข) ความรู้เกี่ยวกับ Protocol Network security Database encryption algorithm และวิธีการป้องกัน

(ค) การเชื่อมต่อเครือข่าย Access Management (E.G., Public Key Infrastructure, Oauth, OpenID, SAML, SPML)

(ง) ความรู้เกี่ยวกับ Cryptography Cryptographic Key Management

(จ) กระบวนการบริหารจัดการความเสี่ยง

(ฉ) ช่องโหว่ของระบบ การทดสอบช่องโหว่ระบบ

(ช) ความรู้เกี่ยวกับไวรัส มัลแวร์ ที่ส่งผลกระทบต่อองค์กร

(ซ) การจำกัดการแพร่กระจายของมัลแวร์ การกำจัด/ลบ มัลแวร์ออกจากระบบ

(๒) การสนับสนุนการป้องกันความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Defense Infrastructure Support)

(ก) ความรู้เกี่ยวกับ OSI model TCP/IP เครือข่าย Protocol Network security Database Encryption Algorithm และวิธีการป้องกัน

(ข) ความรู้เกี่ยวกับ Backup และ Restore ระบบ

(ค) การรับมือและตอบสนองภัยคุกคาม

(ง) การวิเคราะห์ Packet-Level

(จ) การป้องกันภัยคุกคาม สำหรับการใช้งาน VPN

(ฉ) ระบบเครือข่ายพื้นฐานและเทคนิคการปิดช่องโหว่ของระบบปฏิบัติการ

(ช) ความรู้เกี่ยวกับ Network Protocol (TCP/IP Dynamic Host Configuration Domain Name System (DNS) and Directory Services)

(ซ) การวิเคราะห์การรับ–ส่งข้อมูลบนเครือข่าย

(๓) การตอบสนองต่อเหตุการณ์ภัยคุกคามทางไซเบอร์ (Cyber Threat Incident Response)

(ก) ความรู้เกี่ยวกับ OSI Model TCP/IP เครือข่าย Protocol Network Security Database Encryption Algorithm และวิธีการป้องกัน

(ข) ความรู้เกี่ยวกับ Backup และ Restore ระบบ

(ค) การรับมือและตอบสนองภัยคุกคาม

(ง) การวิเคราะห์ Packet–Level

(จ) การป้องกันภัยคุกคาม สำหรับการใช้งาน VPN

(ฉ) ระบบเครือข่ายพื้นฐานและเทคนิคการปิดช่องโหว่ของระบบปฏิบัติการ

(ช) ความรู้เกี่ยวกับ Network Protocol (TCP/IP Dynamic Host Configuration Domain Name System (DNS) and directory services)

(ซ) การวิเคราะห์การรับ - ส่งข้อมูลบนเครือข่าย (Tools, Tethodologies, Processes)

(ฌ) การเขียนรายงานเพื่ออธิบายเหตุการณ์ที่เกิดขึ้น

(ญ) ความรู้เกี่ยวกับผลกระทบจากภัยคุกคาม

(ฎ) การอ่านและวิเคราะห์ข้อมูลจาก Log

(๔) การประเมิน ตรวจสอบ และจัดการช่องโหว่ (Vulnerability Assessment and Management)

(ก) ความรู้เกี่ยวกับเครือข่าย Protocol Network security Database Encryption Algorithm และวิธีการป้องกัน

(ข) การเชื่อมต่อเครือข่าย Access Management (E.G., Public Key Infrastructure Oauth Open ID SAML SPML)

(ค) ความรู้เกี่ยวกับ Cryptography และ Cryptographic Key Management

(ง) การทดสอบช่องโหว่ระบบ

(จ) ช่องโหว่ของระบบ

(ฉ) ความรู้เกี่ยวกับ TTP

(ช) นโยบาย ข้อกำหนดต่าง ๆ หรือมาตรฐานและกฎหมายที่เกี่ยวข้อง

(ซ) ระบบความปลอดภัย วิธีการและเทคนิคที่ใช้งาน

(ฌ) การจำกัดการแพร่กระจายของมัลแวร์ การกำจัด/ลบ มัลแวร์ออกจากระบบ

(ญ) ภาษาคอมพิวเตอร์ที่เกี่ยวข้อง

(ฎ) ช่องโหว่ทาง Application (OWASP Top10)

๓.๑.๑.๔ การออกแบบและพัฒนาระบบให้มั่นคงปลอดภัย (Designing and Building Secure Information Technology Systems)

- การบริหารจัดการความเสี่ยง (Risk Management)

(ก) การกำหนดกรอบการบริหารความเสี่ยง (Risk Management Framework)

(ข) กฎหมายที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัย

(ค) สถาปัตยกรรมความมั่นคงปลอดภัยเครือข่ายและระบบ

(ง) เครื่องมือการประเมินช่องโหว่ และขีดความสามารถของเครื่องมือ

(จ) เทคโนโลยีสารสนเทศและเทคโนโลยีความมั่นคงปลอดภัย

(ฉ) การวิเคราะห์ความเสี่ยงสารสนเทศ

(ช) วิธีการรวบรวมข้อมูลด้านความมั่นคงปลอดภัย

(ซ) เครื่องมือเฝ้าระวังและตรวจจับด้านความมั่นคงปลอดภัย

(ฌ) กระบวนการและแนวปฏิบัติในการบริหารความเสี่ยง

(ญ) เครื่องมือเฝ้าระวังและตรวจจับด้านความมั่นคงปลอดภัย

๓.๑.๒ ความสามารถ ประกอบด้วยขอบเขตความสามารถในการปฏิบัติงานในเรื่องดังต่อไปนี้

๓.๑.๒.๑ บริหารจัดการและบำรุงรักษา (Operate and Maintain)

(๑) บริหารจัดการข้อมูล (Data Administration)

(ก) ออกแบบและติดตั้งระบบฐานข้อมูล

(ข) เข้ารหัสฐานข้อมูล

(ค) ตรวจสอบและบำรุงรักษาฐานข้อมูล

(ง) สำรองและกู้คืนฐานข้อมูล

(๒) สนับสนุนทางเทคนิค และให้บริการลูกค้า (Customer Service & Technical Support)

(ก) จัดการบัญชีผู้ใช้และสิทธิการเข้าถึงระบบและอุปกรณ์

(ข) แก้ปัญหาฮาร์ดแวร์ และซอฟต์แวร์

(ค) ตรวจสอบ และทดสอบประสิทธิภาพของระบบ

(๓) บริการเครือข่าย (Network Services)

(ก) กำหนดค่าและปรับเพิ่มประสิทธิภาพอุปกรณ์เครือข่าย Hubs Router Switch และ Access Point

(ข) ติดตั้ง Firewall และการตั้งค่าคอนฟิกกำหนด Policy

(ค) รักษาความปลอดภัยเครือข่ายส่วนตัวเสมือน (VPN)

(ง) ตรวจสอบปริมาณการใช้งานและประสิทธิภาพของระบบเครือข่าย

(จ) แก้ไขช่องโหว่ของระบบเครือข่าย

(ฉ) วินิจฉัยปัญหาการเชื่อมต่อระบบเครือข่าย

(ช) ติดตั้งและบำรุงรักษาซอฟต์แวร์ระบบปฏิบัติการอุปกรณ์โครงสร้างพื้นฐานเครือข่าย

(๔) บริหารจัดการระบบ (Systems Administration)

(ก) จัดการทรัพยากรเซิร์ฟเวอร์

(ข) ตรวจสอบและบำรุงรักษา เครื่องแม่ข่ายและระบบ

(ค) จัดการบัญชีผู้ใช้ บริหารสิทธิการเข้าถึงระบบและอุปกรณ์

(ง) บำรุงรักษา การตั้งค่าความปลอดภัยของเครื่องแม่ข่ายหรือระบบ

(จ) แก้ปัญหาเครื่องแม่ข่ายและระบบ

๓.๑.๒.๒ รวบรวมข้อมูลและการปฏิบัติการ (Collect and Operate)

(๑) รวบรวมข้อมูลและปฏิบัติการปลอดภัย (Collection and Operations)

(ก) รวบรวมข้อมูลด้านความมั่นคงปลอดภัยไซเบอร์

(ข) วิเคราะห์ข้อมูลด้านความมั่นคงปลอดภัยไซเบอร์

(ค) เก็บรักษาข้อมูลด้านความมั่นคงปลอดภัยไซเบอร์

(๒) ปฏิบัติการไซเบอร์ (Cyber Operations)

(ก) ระบุและทำความเข้าใจสินทรัพย์โครงสร้างพื้นฐานสำคัญ

(ข) ปกป้องสินทรัพย์โครงสร้างพื้นฐานสำคัญจากภัยคุกคามทางไซเบอร์

(ค) ตรวจจับการโจมตีทางไซเบอร์

(ง) ตอบสนองต่อการโจมตีทางไซเบอร์

(จ) ฟื้นฟูระบบจากการโจมตีทางไซเบอร์

๓.๑.๒.๓ ป้องกันรักษาความมั่นคงปลอดภัยไซเบอร์ (Protect and Cybersecurity Defend)

(๑) วิเคราะห์การป้องกันความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Defense Analysis)

(ก) ตรวจสอบ วิเคราะห์ความผิดปกติที่เกิดขึ้นภายในเครือข่าย และแจ้งเตือนภัยคุกคามที่ตรวจพบ

(ข) วิเคราะห์และรายงานแนวโน้มมาตรการรักษาความปลอดภัยขององค์กร

(ค) ประสานงานเพื่อตรวจสอบการแจ้งเตือนเครือข่าย

(ง) แจ้งข้อมูลกับหน่วยงานที่ดูแลระบบ

(จ) จัดทำรายงานสรุปรายวัน

(๒) สนับสนุนการป้องกันความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Defense Infrastructure Support)

(ก) ติดตั้ง กำหนดค่า และทดสอบระบบเพื่อปิดช่องโหว่ รวมถึงป้องกันภัยคุกคามทางไซเบอร์

(ข) บริหารจัดการ จัดเตรียมการทดสอบ ทดสอบประเมินความเสี่ยง ควบคุมการเข้าถึง และการกำหนดค่าของแพลตฟอร์มต่าง ๆ

(๓) ตอบสนองต่อเหตุการณ์ภัยคุกคามทางไซเบอร์ (Cyber Threat Incident Response)

(ก) รวบรวมการบุก และใช้ข้อมูลเพื่อตอบสนองเหตุการณ์ และป้องกันภัยทางไซเบอร์

(ข) วิเคราะห์ เชื่อมโยงข้อมูลการประเมินภัยคุกคาม

(ค) ตรวจสอบแหล่งข้อมูลภายนอกที่เกี่ยวข้องเพื่อตอบสนองภัยคุกคามและป้องกันภัยทางไซเบอร์ และวิเคราะห์เหตุการณ์

(ง) ดำเนินการจัดการเหตุการณ์การป้องกันทางไซเบอร์แบบเรียลไทม์

(๔) ประเมิน ตรวจสอบ และจัดการช่องโหว่ (Vulnerability Assessment and Management)

(ก) ประเมินความเสี่ยง ตรวจสอบช่องโหว่ของระบบ และประเมินความเสี่ยงบุคลากร รวมถึงปฏิบัติงานในส่วนที่เกี่ยวข้อง

(ข) ให้คำแนะนำ เกี่ยวกับการควบคุมความปลอดภัยของข้อมูล และระบบ

๓.๑.๒.๔ ออกแบบและพัฒนาระบบให้มั่นคงปลอดภัย (designing and building secure information technology systems)

- บริหารจัดการความเสี่ยง (Risk Management)

(ก) กำกับและติดตามแผนการบริหารจัดการความเสี่ยง

(ข) รายงานผลการบริหารจัดการความเสี่ยง

๓.๑.๓ ทัศนคติ ประกอบด้วยความละเอียดรอบคอบ ช่างสังเกต มีสมาธิในการทำงาน ใช้ทักษะการอ่าน การคิดอย่างมีวิจารณญาณ ทำงานร่วมกับผู้อื่นอย่างมีประสิทธิภาพ แสวงหาความรู้อย่างสม่ำเสมอ รับฟังความเห็นผู้อื่น ซื่อสัตย์ เป็นกลาง และตระหนักรู้ด้านจริยธรรมความมั่นคงปลอดภัยไซเบอร์

๓.๒ มาตรฐานฝีมือแรงงานแห่งชาติ ระดับ ๓ ได้แก่

๓.๒.๑ ความรู้ ประกอบด้วยขอบเขตความรู้ ในเรื่องดังต่อไปนี้

๓.๒.๑.๑ การบริหารจัดการและบำรุงรักษา (Operate and Maintain)

(๑) บริหารจัดการองค์ความรู้ (Knowledge Management)

(ก) ความรู้ระบบบริหารจัดการองค์ความรู้

(ข) ความรู้ระบบเครือข่าย หลักการความปลอดภัยไซเบอร์

(ค) ความปลอดภัยของข้อมูล

(ง) การบริหารจัดการสิทธิการเข้าถึง

(จ) การสำรองข้อมูลและกู้คืนระบบ

(๒) การบริหารจัดการระบบ (Systems Administration)

(ก) ความรู้ระบบปฏิบัติการ หลักการออกแบบฐานข้อมูล

(ข) ความรู้เกี่ยวกับ Cloud Computing, Backup, Recovery, BCM, BCP

(ค) ความรู้เกี่ยวกับฮาร์ดแวร์ ซอฟต์แวร์ Inventory, Server Health Checkup

(ง) การบริหารจัดการเครื่องคอมพิวเตอร์แม่ข่าย ระบบเครือข่ายคอมพิวเตอร์

(จ) ความรู้เกี่ยวกับ Identity Access Management, Access Control List, LDAP, MS Active Directory

(ฉ) ความรู้เกี่ยวกับ Security Baseline Server hardening VA ISO, IEC27001 PDPA NIST

(ช) ความรู้เกี่ยวกับ Event Log Command Line OS และคู่มือฮาร์ดแวร์

(๓) การวิเคราะห์ความปลอดภัยของระบบ (System Security Analysis)

(ก) ความรู้เกี่ยวกับแนวคิดและโพรโทคอลเครือข่ายคอมพิวเตอร์ และวิธีการรักษาความปลอดภัยเครือข่าย

(ข) ความรู้เกี่ยวกับกระบวนการบริหารความเสี่ยง

(ค) ความรู้เกี่ยวกับภัยคุกคามและช่องโหว่ทางไซเบอร์

(ง) ความรู้เกี่ยวกับเครื่องมือ วิธีการ และเทคนิคการออกแบบระบบรักษาความปลอดภัย

(จ) ความรู้เกี่ยวกับวิธีการใช้เครื่องมือวิเคราะห์เครือข่ายเพื่อระบุช่องโหว่

(ฉ) ความรู้เกี่ยวกับแนวคิดและโพรโทคอลเครือข่ายคอมพิวเตอร์ และวิธีการรักษาความปลอดภัยเครือข่าย

๓.๒.๑.๒ การรวบรวมข้อมูลและการปฏิบัติการ (Collect and Operate)

(๑) การรวบรวมข้อมูลและปฏิบัติการ (Collection and Operations)

(ก) ความรู้ในการใช้เครื่องมือ เช่น Nmap, Nessus, Wireshark, Tcpdump

(ข) ความรู้เกี่ยวกับ Log Management, SIEM (Security Information and Event Management), SOAR (Security Orchestration Automation and Response)

(ค) ความรู้เกี่ยวกับ EDR (Endpoint Detection and Response)

(ง) การบริการแบบคลาวน์ (Cloud Service), Network Attached Storage (NAS)

(จ) Storage Area Network (SAN)

(๒) จัดทำแผนปฏิบัติการด้านไซเบอร์ (Cyber Operational Planning)

(ก) ความรู้ในการใช้เครื่องมือ Nmap, Nessus, Burp Suite, Metasploit, Threat Intelligence

(ข) ความรู้เกี่ยวกับ NIST Cybersecurity Framework

(ค) ความรู้เกี่ยวกับ ISO, IEC 27001

(ง) ความรู้เกี่ยวกับ OWASP Risk Assessment Methodology

(จ) ความรู้เกี่ยวกับ Kali Linux, Nessus, Metasploit

(ฉ) ความรู้เกี่ยวกับ SIEM (Security Information and Event Management)

(๓) การปฏิบัติการไซเบอร์ (Cyber Operations)

(ก) ความรู้ในการใช้เครื่องมือ เช่น Nmap, Nessus, Burp Suite Metasploit

(ข) ความรู้เกี่ยวกับ Application Protocol

(ค) ความรู้เกี่ยวกับ IP Address, NAT, DMZ, ACL, IPS, IDS Backup

(ง) ความรู้เกี่ยวกับ Threat Intelligence

(จ) ความรู้เกี่ยวกับ Disaster Recovery Forensics Threat Intelligence Backup

๓.๒.๑.๓ การป้องกันรักษาความมั่นคงปลอดภัยไซเบอร์ (Protect and Cybersecurity Defend)

(๑) การวิเคราะห์การป้องกันความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Defense Analysis)

(ก) นโยบาย ข้อกำหนดต่าง ๆ หรือมาตรฐานและกฎหมายที่เกี่ยวข้อง

(ข) ความรู้เกี่ยวกับ Protocol Network Security Database Encryption Algorithm และวิธีการป้องกัน

(ค) การเชื่อมต่อเครือข่าย Access Management (E.G., Public Key Infrastructure, Oauth, OpenID, SAML, SPML)

(ง) ความรู้เกี่ยวกับ Cryptography Cryptographic Key Management

(จ) กระบวนการบริหารจัดการความเสี่ยง

(ฉ) ช่องโหว่ของระบบ การทดสอบช่องโหว่ระบบ

(ช) การออกแบบเครือข่ายเพื่อให้ปลอดภัย

(ซ) ความรู้เกี่ยวกับไวรัส มัลแวร์ ที่ส่งผลกระทบต่อองค์กร

(ฌ) การจำกัดการแพร่กระจายของมัลแวร์ การกำจัด/ลบ มัลแวร์ออกจากระบบ

(๒) การตอบสนองต่อเหตุการณ์ภัยคุกคามทางไซเบอร์ (Cyber Threat Incident Response)

(ก) ความรู้เกี่ยวกับ OSI Model TCP, IP เครือข่าย Protocol Network Security Database Encryption Algorithm และวิธีการป้องกัน

(ข) ความรู้เกี่ยวกับ Backup และ Restore ระบบ

(ค) การรับมือและตอบสนองภัยคุกคาม

(ง) การวิเคราะห์ Packet–Level

(จ) การป้องกันภัยคุกคาม สำหรับการใช้งาน VPN

(ฉ) ระบบเครือข่ายพื้นฐานและเทคนิคการปิดช่องโหว่ของระบบปฏิบัติการ

(ช) ความรู้เกี่ยวกับ Network Protocol (TCP, IP Dynamic Host Configuration Domain Name System (DNS) and directory services)

(ซ) การวิเคราะห์การรับ - ส่งข้อมูลบนเครือข่าย (Tools, Tethodologies, Processes)

(ฌ) การเขียนรายงานเพื่ออธิบายเหตุการณ์ที่เกิดขึ้น

(ญ) ความรู้เกี่ยวกับผลกระทบจากภัยคุกคาม

(ฎ) การอ่านและวิเคราะห์ข้อมูลจาก Log

(๓) การประเมิน ตรวจสอบและจัดการช่องโหว่ (Vulnerability Assessment and Management)

(ก) ความรู้เกี่ยวกับเครือข่าย Protocol Network Security Database Encryption Algorithm และวิธีการป้องกัน

(ข) การเชื่อมต่อเครือข่าย Access Management (E.G., Public Key Infrastructure Oauth OpenID SAML SPML)

(ค) ความรู้เกี่ยวกับ Cryptography และ Cryptographic Key Management

(ง) การทดสอบช่องโหว่ระบบ

(จ) ช่องโหว่ของระบบ

(ฉ) ความรู้เกี่ยวกับ TTP

(ช) นโยบาย ข้อกำหนดต่าง ๆ หรือมาตรฐานและกฎหมายที่เกี่ยวข้อง

(ซ) ระบบความปลอดภัย วิธีการและเทคนิคที่ใช้งาน

(ฌ) การจำกัดการแพร่กระจายของมัลแวร์ การกำจัด ลบ มัลแวร์ออกจากระบบ

(ญ) ภาษาคอมพิวเตอร์ที่เกี่ยวข้อง

(ฎ) ช่องโหว่ทาง Application (OWASP Top10)

๓.๒.๑.๔ การออกแบบและพัฒนาระบบให้มั่นคงปลอดภัย (Designing and Building Secure Information Technology Systems)

(๑) การบริหารจัดการความเสี่ยง (Risk Management)

(ก) ความรู้เกี่ยวกับกระบวนการและแนวปฏิบัติในการบริหารจัดการความเสี่ยง

(ข) สถาปัตยกรรมความมั่นคงปลอดภัยเครือข่ายและระบบ

(ค) วิธีการและเทคนิคในการระบุความเสี่ยง

(ง) การประเมินและวิเคราะห์ความเสี่ยงที่เกิดขึ้น

(จ) เครื่องมือเฝ้าระวังและตรวจจับด้านความมั่นคงปลอดภัย

(ฉ) การสื่อสารและการจัดทำรายงานการบริหารจัดการความเสี่ยง

(ช) การวิเคราะห์การทำงานที่ถูกต้องของระบบรักษาความมั่นคงปลอดภัยสารสนเทศ ขีดความสามารถ และผลกระทบต่อการทำงานของระบบ

(ซ) การจัดทำและประเมินระบบเทคโนโลยีสารสนเทศ

(๒) การพัฒนาซอฟต์แวร์ (Software Development)

(ก) ความรู้เกี่ยวกับสถาปัตยกรรมด้านความมั่นคงปลอดภัยเครือข่ายคอมพิวเตอร์ ข้อมูล และระบบสารสนเทศสำหรับองค์กร

(ข) ความรู้เกี่ยวกับช่องโหว่และภัยคุกคามด้านความมั่นคงปลอดภัยระบบและแอปพลิเคชั่น

(ค) ความรู้เกี่ยวกับวงจรการพัฒนาซอฟต์แวร์

(ง) การออกแบบซอฟต์แวร์

(จ) การเขียนโปรแกรมให้มีความมั่นคงปลอดภัย

(ฉ) การติดตั้งและทดสอบซอฟต์แวร์ให้มีความมั่นคงปลอดภัย

(๓) ออกแบบสถาปัตยกรรมระบบ (System Architecture)

(ก) ความรู้เกี่ยวกับวงจรการพัฒนาระบบ

(ข) ความรู้เกี่ยวกับสถาปัตยกรรมความปลอดภัย

(ค) การตรวจสอบระบบและสถาปัตยกรรมให้สอดคล้องกับแนวทางสถาปัตยกรรมความมั่นคงปลอดภัยขององค์กร

(ง) การประเมินสถาปัตยกรรมและการออกแบบความมั่นคงปลอดภัยเพื่อความเหมาะสมกับองค์กร

(๔) การพัฒนาระบบ (System Development)

(ก) ความรู้เกี่ยวกับวงจรการพัฒนาระบบ

(ข) ความรู้เกี่ยวกับวงจรการพัฒนาซอฟต์แวร์

(ค) การออกแบบและพัฒนาระบบ

(ง) การกำกับดูแลความมั่นคงปลอดภัยข้อมูลระบบเครือข่าย

(จ) การสำรองข้อมูลและระบบโปรแกรม

(ฉ) การพัฒนาแผนและแนวทางปฏิบัติการกู้คืนข้อมูลและระบบโปรแกรมเพื่อความต่อเนื่องในการปฏิบัติงาน

(ช) ความรู้เกี่ยวกับการบำรุงรักษา และการจัดการระบบเพื่อความมั่นคงปลอดภัย

๓.๒.๑.๕ การวิเคราะห์และแจ้งเตือนภัยคุกคามทางไซเบอร์ (Analyze)

(๑) การวิเคราะห์และเฝ้าระวังภัยคุกคาม (Threat Analysis)

(ก) การประเมินความเสี่ยง

(ข) ความรู้ด้านกฎหมายที่เกี่ยวข้อง

(ค) วิธีการและเทคนิคของภัยคุกคาม

(ง) การโจมตีระบบ

(จ) ระบบเครือข่ายคอมพิวเตอร์

(ฉ) ระบบการรักษาความปลอดภัยไซเบอร์

(ช) ข้อมูลส่วนบุคคล

(ซ) การวิเคราะห์ Network Traffic

(ฌ) ประเภทของภัยคุกคามและช่องโหว่

(ญ) การโจมตีทางไซเบอร์

(ฎ) ผลิตภัณฑ์ประเภทต่าง ๆ เพื่อให้รู้ถึงการโจมตีและช่องโหว่ที่อาจมีผลกระทบ

(๒) การประเมินระดับความรุนแรงของช่องโหว่ (Exploitation Analysis)

(ก) หลักการโพรโทคอลของระบบเครือข่ายคอมพิวเตอร์และความรู้ด้าน network security

(ข) ช่องโหว่และเทคนิคของการโจมตีช่องโหว่

(ค) ผลิตภัณฑ์ยี่ห้อต่าง ๆ

(ง) วิธีการและเทคนิคของภัยคุกคามประเภทต่าง ๆ

(จ) ภัยคุกคามด้านไซเบอร์และช่องโหว่ต่าง ๆ

(ฉ) การระบุช่องโหว่และเทคนิคของการโจมตีช่องโหว่

(ช) การใช้ Tools และ Script ในการทดสอบ

(ซ) การประเมินและวิเคราะห์ข้อมูลปริมาณมาก

(ฌ) อุปกรณ์พื้นฐานทางเครือข่ายและการตั้งค่า

(ญ) หลักการของระบบปฏิบัติการ

(ฎ) ประเภท หน้าที่ และการจัดการข้อมูลของเว็บไซต์

(ฏ) ความรู้เกี่ยวกับ OSI Model TCP, IP Protocol Network security Database Encryption Algorithm และวิธีการป้องกัน

(ฐ) ความรู้เกี่ยวกับ Risk Management Process

(ฑ) การทดสอบช่องโหว่ระบบ

(ฒ) ความรู้เกี่ยวกับ Backup และ Restore ระบบ

(ณ) นโยบาย ข้อกำหนดต่าง ๆ หรือมาตรฐานและกฎหมายที่เกี่ยวข้อง

(ด) การวิเคราะห์ Packet-Level

(ต) การป้องกันภัยคุกคามสำหรับการใช้งาน VPN

(ถ) ระบบเครือข่ายพื้นฐาน และเทคนิคการปิดช่องโหว่ของระบบปฏิบัติการ

(ท) ความรู้เกี่ยวกับ Network Protocol (TCP, IP, Dynamic Host Configuration, Domain Name System (DNS), and Directory Services)

(ธ) การวิเคราะห์การรับ-ส่งข้อมูลบนเครือข่าย

(น) กระบวนการบริหารจัดการความเสี่ยงและการประเมินความเสี่ยง

(บ) วิธีการค้นหา วิเคราะห์

(ป) ขั้นตอนของการ Attack

(ผ) ประเภทของภัยคุกคามและช่องโหว่

(ฝ) ข้อมูลช่องโหว่และแนวทางในการป้องกัน

(๓) การวิเคราะห์ข้อมูลแวดล้อมที่มีความเป็นไปได้ในการถูกโจมตีต่อระบบเป้าหมาย (Targets)

(ก) หลักการ โพรโทคอลของระบบเครือข่ายคอมพิวเตอร์และความรู้ด้าน network security

(ข) การระบุช่องโหว่และอธิบายเทคนิคของการโจมตีช่องโหว่ได้

(ค) ความรู้เกี่ยวกับผลิตภัณฑ์ยี่ห้อต่าง ๆ ว่ามีช่องโหว่อะไรบ้าง

(ง) วิธีการและเทคนิคของภัยคุกคามประเภทต่าง ๆ

๓.๒.๑.๖ การสืบสวนหาหลักฐาน (Investigate)

(๑) การสืบสวนทางไซเบอร์ (Cyber Investigation)

(ก) ความรู้เบื้องต้นเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

(ข) การวิเคราะห์พฤติกรรมอาชญากรรมไซเบอร์

(ค) การวิเคราะห์ช่องโหว่และจุดอ่อนของระบบ

(ง) การหาสาเหตุจากอาชญากรรมไซเบอร์ที่เกิดขึ้นกับระบบและองค์กร

(จ) การเข้าถึงทรัพยากรของระบบ

(ฉ) ลักษณะและรูปแบบของอาชญากรรมไซเบอร์

(ช) การสืบสวนอาชญากรรมไซเบอร์

(ซ) การติดตามร่องรอยอาชญากรรมไซเบอร์

(๒) การตรวจพิสูจน์ทางดิจิทัล (Digital Forensics)

(ก) การระบุพยานหลักฐานทางดิจิทัล

(ข) การจัดเก็บพยานหลักฐานทางดิจิทัล

(ค) การเก็บรักษาพยานหลักฐานทางดิจิทัล

(ง) การวิเคราะห์พยานหลักฐานทางดิจิทัล

(จ) การตรวจพิสูจน์พยานหลักฐานทางดิจิทัล

(ฉ) เทคนิคการวิเคราะห์และตรวจพิสูจน์พยานหลักฐานทางดิจิทัล

(ช) การเขียนรายงานผลการตรวจพิสูจน์ทางดิจิทัล

(ซ) การนำเสนอผลการตรวจพิสูจน์ทางดิจิทัล

๓.๒.๒ ความสามารถ ประกอบด้วยขอบเขตความสามารถในการปฏิบัติงานในเรื่องดังต่อไปนี้

๓.๒.๒.๑ บริหารจัดการและบำรุงรักษา (Operate and Maintain)

(๑) บริหารจัดการองค์ความรู้ (Knowledge Management)

(ก) ออกแบบ ติดตั้ง ระบบบริหารจัดการความรู้สำหรับองค์กร

(ข) จัดการการเข้าถึงองค์ความรู้ขององค์กร

(ค) ตรวจสอบการใช้องค์ความรู้

(ง) บำรุงรักษาระบบบริหารจัดการความรู้

(๒) บริหารจัดการระบบ (Systems Administration)

(ก) จัดการทรัพยากรเซิร์ฟเวอร์ รวมถึงประสิทธิภาพ ความจุ ความพร้อมใช้งาน ความสามารถในการให้บริการ และความสามารถในการกู้คืน

(ข) จัดทำเอกสารขั้นตอนการปฏิบัติงานมาตรฐานการบริหารระบบ

(ค) บำรุงรักษา การตั้งค่าความปลอดภัยของเครื่องแม่ข่ายหรือระบบ

(ง) แก้ปัญหาเครื่องแม่ข่ายและระบบ พร้อมทั้งแนวทางป้องกัน

(๓) การวิเคราะห์ความปลอดภัยของระบบ (System Security Analysis)

(ก) สแกนช่องโหว่และรับรู้ช่องโหว่ในระบบรักษาความปลอดภัย

(ข) วิเคราะห์จากผลการประเมินความเสี่ยงช่องโหว่จากการอ่านค่าความเสี่ยง

(ค) ประเมินความเสี่ยงระบบเครือข่ายคอมพิวเตอร์ภายนอกองค์กร และภายในองค์กร LAN WAN Cloud SASE

๓.๒.๒.๒ รวบรวมข้อมูลและการปฏิบัติการ (Collect and Operate)

(๑) รวบรวมข้อมูลและปฏิบัติการ (Collection Operations)

(ก) บริหารจัดการข้อมูลด้านความมั่นคงปลอดภัยไซเบอร์

(ข) วิเคราะห์ข้อมูลด้านความมั่นคงปลอดภัยไซเบอร์

(ค) นำเสนอผลลัพธ์ด้านความมั่นคงปลอดภัยไซเบอร์

(๒) จัดทำแผนปฏิบัติการด้านไซเบอร์ (Cyber Operational Planning)

(ก) วิเคราะห์ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

(ข) กำหนดเป้าหมายด้านความมั่นคงปลอดภัยไซเบอร์

(ค) กำหนดกลยุทธ์ด้านความมั่นคงปลอดภัยไซเบอร์

(ง) จัดทำแผนปฏิบัติการด้านความมั่นคงปลอดภัยไซเบอร์

(จ) ดำเนินการและติดตามผลด้านความมั่นคงปลอดภัยไซเบอร์

(๓) ปฏิบัติการไซเบอร์ (Cyber Operations)

(ก) ระบุและทำความเข้าใจสินทรัพย์โครงสร้างพื้นฐานสำคัญ

(ข) ปกป้องสินทรัพย์โครงสร้างพื้นฐานสำคัญจากภัยคุกคามทางไซเบอร์

(ค) ตรวจจับการโจมตีทางไซเบอร์ได้อย่างรวดเร็ว

(ง) ตอบสนองต่อการโจมตีทางไซเบอร์อย่างมีประสิทธิภาพ

(จ) ฟื้นฟูระบบจากการโจมตีทางไซเบอร์

๓.๒.๒.๓ ป้องกันรักษาความมั่นคงปลอดภัยไซเบอร์ (Protect and Cybersecurity Defend)

(๑) วิเคราะห์การป้องกันความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Defense Analysis)

(ก) วิเคราะห์ความผิดปกติที่เกิดขึ้นภายในเครือข่าย พร้อมทั้งทำการแจ้งเตือนภัยคุกคามที่ตรวจพบ

(ข) กำหนดกลยุทธ์ เทคนิค และขั้นตอนในการทำการป้องกันการบุกรุก

(ค) วิเคราะห์และรายงานแนวโน้มมาตรการรักษาความปลอดภัยขององค์กร

(ง) ประสานงานกับเจ้าหน้าที่ป้องกันทางไซเบอร์ที่เกี่ยวข้องในองค์กร เพื่อตรวจสอบการแจ้งเตือนเครือข่าย

(๒) ตอบสนองต่อเหตุการณ์ภัยคุกคามทางไซเบอร์ (Cyber Threat Incident Response)

(ก) รวบรวมการบุกรุก และใช้ข้อมูลที่พบตอบสนองเหตุการณ์และป้องกันภัยทางไซเบอร์

(ข) วิเคราะห์ เชื่อมโยงข้อมูลการประเมินภัยคุกคาม

(ค) ตรวจสอบแหล่งข้อมูลภายนอกที่เกี่ยวข้องเพื่อตอบสนองภัยคุกคามและป้องกันภัยทางไซเบอร์

(ง) วิเคราะห์เหตุการณ์ที่ส่งผลกระทบต่อองค์กร

(จ) จัดการเหตุการณ์การป้องกันทางไซเบอร์แบบเรียลไทม์ เพื่อสนับสนุนทีมตอบสนองเหตุการณ์ (IRT) ที่ปรับใช้ได้

(๓) ประเมิน ตรวจสอบและจัดการช่องโหว่ (Vulnerability Assessment and Management)

(ก) ดำเนินการประเมินความเสี่ยง ตรวจสอบช่องโหว่ของระบบ และประเมินความเสี่ยงบุคลากร รวมถึงปฏิบัติงานในส่วนที่เกี่ยวข้อง

(ข) วิเคราะห์นโยบายและการกำหนดค่าการป้องกันทางไซเบอร์ขององค์กร และประเมินการปฏิบัติตามกฎระเบียบและคำสั่งขององค์กร

(ค) ดำเนินการ/สนับสนุนการทดสอบการเจาะระบบที่ได้รับอนุญาตบนเครือข่ายขององค์กร

๓.๒.๒.๔ ออกแบบและพัฒนาระบบให้มั่นคงปลอดภัย (Designing and Building Secure Information Technology Systems)

(๑) บริหารจัดการความเสี่ยง (Risk Management)

(ก) พัฒนากระบวนการและวิธีการประเมินความเสี่ยง

(ข) ระบุความเสี่ยง

(ค) ประเมินความเสี่ยง

(ง) กำกับและติดตามแผนการบริหารจัดการความเสี่ยง

(จ) รายงานผลการบริหารจัดการความเสี่ยง

(๒) พัฒนาซอฟต์แวร์ (Software Development)

(ก) วิเคราะห์ความต้องการขององค์กรและจัดทำแผนการพัฒนาโปรแกรม

(ข) พัฒนาแผนผังการทำงานและออกแบบการทำงานของโปรแกรม

(ค) กำหนดการพัฒนาโปรแกรมให้เกิดความมั่นคงปลอดภัย

(ง) ทดสอบซอฟต์แวร์ด้านความมั่นคงปลอดภัย

(จ) ประเมินและสรุปประเด็นด้านการรักษาความมั่นคงปลอดภัย

(๓) ออกแบบสถาปัตยกรรมระบบ (System Architecture)

(ก) จัดทำนโยบายและขั้นตอนปฏิบัติการรักษาความมั่นคงปลอดภัย

(ข) กำกับดูแลรักษาความมั่นคงปลอดภัย

(ค) ดำเนินการทดสอบและตรวจสอบความมั่นคงปลอดภัย

(๔) พัฒนาระบบ (System Development)

(ก) ออกแบบและพัฒนาแผนการพัฒนาระบบ

(ข) วิเคราะห์และออกแบบความต้องการของระบบ

(ค) ดำเนินการกำกับและดูแลการพัฒนาระบบให้เป็นไปตามแผนงาน

(ง) ดำเนินการทดสอบความมั่นคงปลอดภัยและรายงานผลการตรวจสอบ

(จ) รายงานการประเมินประสิทธิผลของการพัฒนาระบบ

๓.๒.๒.๕ วิเคราะห์และแจ้งเตือนภัยคุกคามทางไซเบอร์ (Analyze)

(๑) วิเคราะห์และเฝ้าระวังภัยคุกคาม (Threat Analysis)

(ก) ตรวจจับภัยคุกคาม

(ข) ร่วมหารือกับหน่วยงานที่เกี่ยวข้องในการจัดทำแผนป้องกัน และรับมือกับภัยคุกคามทางไซเบอร์

(ค) วิเคราะห์เชิงลึก และระบุเทคนิคและวิธีการของภัยคุกคาม

(ง) เฝ้าระวังภัยคุกคาม รายงานเหตุการณ์เครือข่ายและการบุกรุก

(๒) ประเมินระดับความรุนแรงของช่องโหว่ (Exploitation Analysis)

(ก) ค้นหา ระบุ ประเมินระดับความรุนแรงของช่องโหว่ที่มีความเป็นไปได้ในการถูกโจมตีระบบที่เป็นเป้าหมาย

(ข) ทดสอบความเป็นไปได้ในการโจมตีระบบที่เป็นเป้าหมาย (Penetration Testing)

(ค) ทดสอบการเจาะตามที่จำเป็นสำหรับแอปพลิเคชันใหม่หรือแอปพลิเคชันที่อัปเดต

(ง) เฝ้าระวัง ติดตาม สรุปรายงานแนวโน้มของ Cyber threat ที่เปลี่ยนแปลงอย่างรวดเร็ว

(๓) วิเคราะห์ข้อมูลแวดล้อมที่มีความเป็นไปได้ในการถูกโจมตีต่อระบบเป้าหมาย (Targets)

(ก) วิเคราะห์ ทบทวนแหล่งข้อมูล ระบุกลุ่มเป้าหมาย และประเมินช่องโหว่ที่ความสำคัญที่อาจจะทำให้เกิดภัยคุกคาม

(ข) รายงานเหตุการณ์เครือข่าย การบุกรุก และรายงานความก้าวหน้าในการรับมือกับภัยคุกคาม

๓.๒.๒.๖ สืบสวนหาหลักฐาน (Investigate)

(๑) สืบสวนทางไซเบอร์ (Cyber Investigation)

(ก) วิเคราะห์และหาสาเหตุของอาชญากรรมทางไซเบอร์ที่เกิดขึ้นกับระบบ

(ข) สืบสวนติดตามร่องรอยของผู้กระทำความผิดที่โจมตีระบบ

(๒) ตรวจพิสูจน์ทางดิจิทัล (Digital Forensics)

(ก) ระบุ จัดเก็บและการเก็บรักษาพยานหลักฐานทางดิจิทัล

(ข) วิเคราะห์และตรวจพิสูจน์พยานหลักฐานทางดิจิทัล

(ค) รายงานผลและนำเสนอการตรวจพิสูจน์ทางดิจิทัล

๓.๒.๓ ทัศนคติ ประกอบด้วย ความละเอียดรอบคอบ ช่างสังเกต มีสมาธิในการทำงาน ใช้ทักษะการอ่านการคิดอย่างมีวิจารณญาณ ทำงานร่วมกับผู้อื่นอย่างมีประสิทธิภาพ แสวงหาความรู้อย่างสม่ำเสมอ รับฟังความเห็นผู้อื่น ซื่อสัตย์ เป็นกลาง และตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์

ประกาศ ณ วันที่ ๒๕ มีนาคม พ.ศ. ๒๕๖๘
บุญสงค์ ทัพชัยยุทธ์
ปลัดกระทรวงแรงงาน
ประธานกรรมการส่งเสริมการพัฒนาฝีมือแรงงาน