



ขอบเขตงาน (Terms of Reference : TOR)

โครงการยกระดับความมั่นคงปลอดภัยทางไซเบอร์ เพื่อป้องกันการเข้าถึงข้อมูลขนาดใหญ่ ของสำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์

1. ความเป็นมา

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศทส.) สำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ (สป.พม.) มีภารกิจสำคัญในการพัฒนาและให้บริการระบบโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่มีประสิทธิภาพและเป็นมาตรฐานเดียวกัน พร้อมทั้งสนับสนุนการเชื่อมโยงข้อมูลสารสนเทศเพื่อรองรับการปฏิบัติราชการในหน่วยงานส่วนกลางและส่วนภูมิภาค ในปัจจุบันภัยคุกคามทางไซเบอร์มีความซับซ้อนและรุนแรงเพิ่มขึ้นอย่างต่อเนื่อง ส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศที่จำเป็นต้องปรับปรุงอย่างต่อเนื่อง เพื่อให้สามารถป้องกัน (Protect) ตรวจพบ (Detect) และตอบสนอง (Respond) ต่อภัยคุกคามได้อย่างมีประสิทธิภาพ รวมถึงปฏิบัติตามกฎหมายและระเบียบข้อบังคับที่เกี่ยวข้อง เช่น

- พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และฉบับที่ 2 พ.ศ. 2560
- พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
- พระราชบัญญัติการปฏิบัติราชการทางอิเล็กทรอนิกส์ พ.ศ. 2565
- ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2564

จึงมีความจำเป็นต้องจัดหาครุภัณฑ์คอมพิวเตอร์และอุปกรณ์ เพื่อทดแทนของเดิมที่หมดอายุการใช้งานประจำปีงบประมาณ 2569 ด้วยวิธีการประกวดราคาอิเล็กทรอนิกส์ (e-bidding)

2. วัตถุประสงค์

1. เพื่อเพิ่มประสิทธิภาพในการเฝ้าระวัง ป้องกัน และตอบสนองต่อภัยคุกคามด้าน Cyber Security ที่อาจส่งผลกระทบต่อระบบสารสนเทศและบริการของ สป.พม. ทั้งในส่วนกลางและส่วนภูมิภาค

2. เพื่อนำเทคโนโลยีสมัยใหม่ เช่น ระบบบริหารเหตุการณ์และข้อมูลการรักษาความมั่นคงปลอดภัย (SIEM) ระบบตรวจจับและตอบสนองภัยคุกคาม (XDR, NDR) และระบบบริหารจัดการภัยคุกคามอัตโนมัติ (SOAR) มาประยุกต์ใช้ในการวิเคราะห์เหตุการณ์ (Log) ตรวจจับความผิดปกติ (Anomaly Detection) และภัยคุกคามซ่อนเร้น รวมถึงการตอบสนองต่อเหตุการณ์อย่างรวดเร็วและมีประสิทธิภาพ

3. เพื่อเพิ่มขีดความสามารถในการเฝ้าระวังภัยคุกคามในระดับผู้ใช้งาน (User) และระบบเครือข่าย โดยสามารถแยกแยะพฤติกรรมผิดปกติได้อย่างแม่นยำ และลดความเสี่ยงที่อาจเกิดจากการละเมิดนโยบายความปลอดภัย

4. เพื่อเสริมสร้างความมั่นคงปลอดภัยของระบบปฏิบัติการ แอปพลิเคชัน และฐานข้อมูล ด้วยการใช้เทคโนโลยีการประเมินช่องโหว่ (Vulnerability Assessment Tool) และระบบป้องกันฐานข้อมูล (Database Firewall)

5. เพื่อให้การดำเนินงานด้าน Cyber Security สอดคล้องกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และกฎหมายที่เกี่ยวข้อง เช่น พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 (และฉบับที่ 2 พ.ศ. 2560) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และพระราชบัญญัติการปฏิบัติราชการทางอิเล็กทรอนิกส์ พ.ศ. 2565 และปฏิบัติตามประกาศและระเบียบข้อบังคับ เช่น หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2564 รวมถึงสร้างความพร้อมในการรับมือภัยคุกคามที่เปลี่ยนแปลงอย่างรวดเร็วในยุคดิจิทัล

3. คุณสมบัติของผู้เสนอราคา

3.1 มีความสามารถตามกฎหมาย

3.2 ไม่เป็นบุคคลล้มละลาย

3.3 ไม่อยู่ระหว่างเลิกกิจการ

3.4 ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการ ตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

3.5 ไม่เป็นบุคคลซึ่งถูกระงับชื่อไว้ในบัญชีรายชื่อผู้ทำงานและได้แจ้งเวียนชื่อให้เป็นผู้ทำงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทำงานเป็นหุ้นส่วน ผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

3.6 มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

3.7 เป็นนิติบุคคลผู้มีอาชีพขายพัสดุที่ประกวดราคาอิเล็กทรอนิกส์ดังกล่าว

3.8 ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้เสนอราคารายอื่นที่เข้ายื่นข้อเสนอให้แก่สำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

3.9 ไม่เป็นผู้ที่ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้เสนอราคาได้มีคำสั่งให้สละสิทธิ์ความคุ้มกันเช่นนั้น

4. รายละเอียดคุณลักษณะเฉพาะ

4.1 ระบบบริหารเหตุการณ์และข้อมูลการรักษาความมั่นคงปลอดภัย (SIEM) มีคุณลักษณะเฉพาะที่สำคัญ ดังนี้

1. เป็นอุปกรณ์ประเภท Hardware Appliance ออกแบบมาสำหรับวิเคราะห์เหตุการณ์ภัยคุกคามด้านความมั่นคงปลอดภัยสารสนเทศ (Security Information and Event Management) โดยเฉพาะ
2. ระบบที่เสนอมีการทำงานแบบ Scalable Architecture
3. ระบบที่เสนอสามารถเสนอซอฟต์แวร์ตรวจสอบและแจ้งเตือนประกอบพร้อมได้ เพื่อให้ระบบมีคุณสมบัติครบถ้วน
4. สามารถทำงานแบบ Cluster หรือทำงานแบบ High Availability (HA) โดยรับและวิเคราะห์ข้อมูลได้ไม่น้อยกว่า 5,000 เหตุการณ์ต่อวินาที (Events per Second) และรองรับการเพิ่มขยายได้สูงสุดไม่น้อยกว่า 20,000 เหตุการณ์ต่อวินาที (Events per Second) ได้ในอนาคตโดยไม่ต้องเสนออุปกรณ์เพิ่มเติม
5. ต้องนำเสนออุปกรณ์ที่ทำหน้าที่รับข้อมูลเหตุการณ์ (Collector) อย่างน้อย 1 อุปกรณ์ โดยมีคุณสมบัติอย่างน้อย ดังนี้
 - 5.1 ต้องมี Network Interface แบบ 1Gbps RJ-45 ไม่น้อยกว่า 4 Port
 - 5.2 มีหน่วยความจำ (Memory) ไม่น้อยกว่า 16GB
 - 5.3 มีพื้นที่ในการจัดการข้อมูล (Storage) ไม่น้อยกว่า 4TB
 - 5.4 มีประสิทธิภาพในการรองรับข้อมูลเหตุการณ์ 5000 EPS, 100 WMI log, 500 SNMP เป็นอย่างน้อย
6. สามารถรองรับเหตุการณ์จากอุปกรณ์ได้อย่างน้อย 100 อุปกรณ์ และมี Agent สำหรับติดตั้งที่ระบบ Windows/Linux Server เพื่อรับข้อมูล log ได้อย่างน้อย 25 อุปกรณ์
7. สามารถเชื่อมโยงเหตุการณ์จาก Source ต่างๆ เข้าด้วยกัน (Correlation) ทั้งแบบ Real-time เพื่อหาต้นตอของภัยคุกคาม โดยมี Predefined Rule หรือ System define Rule มาพร้อมกับระบบไม่น้อยกว่า 500 Rules และสามารถ Customize เพิ่มเติมได้
8. มี Predefined Dashboard มาพร้อมกับระบบ เพื่อใช้สำหรับวิเคราะห์ข้อมูลเหตุการณ์แบบ Real-time ในรูปแบบของแผนภูมิ (Chart) และตาราง (Table) และสามารถ Customize เพิ่มเติมได้
9. รองรับการแบ่งแยกกลุ่มของปุมเหตุการณ์ (Event Log) ตามแผนก สาขา ในการใช้งานระบบใหญ่ๆ ที่มีความซับซ้อน หรือสามารถแบ่งแยกปุมเหตุการณ์ (Event Log) ตามรายชื่อลูกค้าในกรณีที่ใช้งานในลักษณะของ MSSP (Management Security Service Provider) หรือ MSP (Managed Service Provider) เพื่อความสะดวกในการตรวจสอบข้อมูล
10. รองรับการบริหารจัดการรายละเอียดของอุปกรณ์หรือระบบต้นทางของ Log (Asset Management) เช่น ประเภทของอุปกรณ์ และสถานที่ตั้ง เป็นต้น

11. สามารถแสดงผลการวิเคราะห์ข้อมูลได้ทั้งแบบ NOC (Network Operation Center) และ SOC (Security Operation Center) และ MITRE ATT&CK ได้
12. สามารถบันทึกข้อมูล หรือเหตุการณ์ได้ในตัวเองโดยมีความจุไม่น้อยกว่า 30 TB ในรูปแบบของ Harddisk และ 7 TB ในรูปแบบของ SSD หรือดีกว่า
13. สามารถวิเคราะห์เปรียบเทียบข้อมูลระหว่างไอพีแอดเดรส กับรายชื่อผู้ใช้งานที่ใช้งานไอพีแอดเดรสอื่นๆ อยู่ (Identity Mapping) และสามารถทำ event/incident enrichment ได้
14. มีระบบบริหารจัดการเหตุการณ์ (Incident Management) ในตัว (Built-in Ticketing System) โดยต้องไม่อาศัย Third Party อื่น ๆ
15. มี Predefined Report มาพร้อมกับระบบไม่น้อยกว่า 100 รูปแบบ และสามารถ Customize เพิ่มเติมได้ และสามารถส่งออกรายงาน (Report export) ในรูปแบบ PDF และ CSV ได้เป็นอย่างน้อย
16. สามารถแจ้งเตือนแบบ Real-time เมื่อมีเหตุการณ์ตรงตามเงื่อนไขที่สร้างไว้ และ เหตุการณ์ผิดปกติของตัวอุปกรณ์ผ่าน e-Mail ได้เป็นอย่างน้อย
17. สามารถบริหารจัดการผ่าน Web Interface ที่มีการเข้ารหัสได้
18. สามารถจัดทำรายงานแบบ Customized ได้ไม่น้อยกว่า 10 รายงาน และรองรับการทำรายงานที่เกี่ยวข้องกับมาตรฐาน CIS, HIPAA, ISO 27001, NIST800-53/171, SANS Critical Control ได้เป็นอย่างน้อย
19. สามารถกำหนดระยะเวลาการเก็บข้อมูล (Retention Policy) ของแต่ละอุปกรณ์ต้นทาง โดยมีระยะเวลาที่แตกต่างกันได้
20. รองรับคุณสมบัติ UBA หรือ UEBA เพื่อช่วยในการตรวจสอบพฤติกรรมของผู้ใช้ในระบบ
21. สามารถตรวจสอบและแจ้งเตือนเมื่อมีการแก้ไขไฟล์จากเครื่องคอมพิวเตอร์แม่ข่ายที่กำหนดได้
22. ระบบที่เสนอต้องสามารถทำงานร่วมกับระบบในข้อ 4.5 ได้โดยเป็นผลิตภัณฑ์ภายใต้ยี่ห้อหรือแบรนด์เดียวกัน เพื่อให้ทำงานอัตโนมัติ (Automation) และสามารถเรียกใช้งาน Playbook และ connector ของระบบในข้อ 4.5 ได้โดยตรง หรือมี connector สำหรับ Event Tracking for windows
23. มีการรับประกัน (Warranty) และสามารถอัปเดต Signature ด้านความปลอดภัยแบบอัตโนมัติได้เป็นระยะเวลาไม่น้อยกว่า 3 ปี

24. ผลิตภัณฑ์ที่เสนอต้องมีเครื่องหมายการค้าอยู่ใน Gartner Magic Quadrant ด้าน Security Information and Event Management (SIEM) ประจำปี 2024 หรือปีล่าสุด

4.2 ระบบตรวจจับและตอบสนองภัยคุกคามทางเครือข่ายภายใน (NDR)

1. เป็นอุปกรณ์แบบ Appliance ที่ออกแบบมาทำหน้าที่วิเคราะห์ ตรวจสอบความผิดปกติของเครือข่าย และเนื้อหาที่เป็นอันตราย โดยใช้คุณสมบัติ AI แบบ Artificial Neural Networks (ANN) หรือเทียบเท่า และ Machine Learning เป็นอย่างน้อยสามารถจำแนกประเภทของการโจมตีของมัลแวร์ ด้วยคุณสมบัติโครงข่ายประสาทเทียม (ANN) เช่น Ransomware, Fileless, Web Shell, Exploit และ Worm Activity เป็นต้น

2. มีความสามารถตรวจจับ Malware ไม่น้อยกว่า 170,000 ไฟล์ต่อชั่วโมง และ NDR throughput ไม่น้อยกว่า 20 Gbps
3. รองรับการทำงานร่วมกับ IP address ไม่น้อยกว่า 10,000 address
4. สามารถตรวจจับความปลอดภัยทางเครือข่ายเช่น Encrypted attack, Malicious web campaigns, Weak ciphers, Vulnerable protocols, IP and DNS-based botnet attacks ได้เป็นอย่างดี
5. สามารถทำงานร่วมกับระบบอื่นๆ เช่น ระบบ SIEM, SOAR โดยมี pre-define connector, action พร้อมใช้งาน และโปรโตคอล Syslog, REST API, ICAP เป็นต้น
6. สามารถทำการวิเคราะห์ไฟล์ และเน็ตเวิร์คโปรโตคอล ดังต่อไปนี้ TCP, UDP, ICMP, ICMP6, TLS, HTTP, SMB, SMTP, Web based, EXE, PDF, MSOFFICE, HTML, ZIP, POWERSHELL, BAT เป็นอย่างน้อย
7. สามารถติดตั้งแบบ Sniff mode หรือ SPAN mode, ICAP, Network File Share และ File หรือ API submission ได้
8. สามารถทำ Allow list และ Deny list โดยใช้คุณสมบัติของ MD5, SHA1 และ SHA256 มาเป็นตัวกรองได้
9. สามารถทำ Baseline สำหรับการตรวจจับความผิดปกติของทราฟฟิกได้ หรือรองรับการสร้างกฎการตรวจจับ เครือข่าย ในรูปแบบ snort หรือ Suricata ได้
10. สามารถส่งการแจ้งเตือนให้กับผู้ดูแลระบบโดยแบ่งการแจ้งเตือนแต่ละประเภทได้ เช่น เหตุการณ์ของระบบ เช่น High CPU, Low Memory และการโจมตี เช่น Malware Detection, Botnet Detection, Encrypted Attack Detection, Indication of Compromise Detection เป็นต้น
11. สามารถระบุหรืออ้างอิง ประเภทการโจมตีได้ตาม MITRE ATT&CK และสามารถนำข้อมูลออกจากระบบในรูปแบบ CSV ได้
12. สามารถทำ Role Base Access สำหรับผู้ดูแลในแต่ละระดับที่แตกต่างกันได้ เช่น Visual Security Analyst, System Configuration, System Maintenance หรือเทียบเท่าโดยทำงานร่วมกับ Local, LDAP และ RADIUS ได้เป็นอย่างดี
13. มีช่องเชื่อมต่อแบบ 10GE SFP+ ไม่น้อยกว่า 4 ช่อง และ GE Copper ไม่น้อยกว่า 2 ช่อง
14. มี Storage แบบ SSD ขนาดไม่น้อยกว่า 7 TB หลังทำ RAID 1 เป็นอย่างน้อย
15. มี Power Supply แบบ Redundant พร้อมคุณสมบัติ Hot Swappable
16. อุปกรณ์ที่เสนอต้องผ่านมาตรฐาน FCC Part 15 Class A, RCM, VCCI, CE, UL และ CB
17. ผลิตภัณฑ์ที่เสนอต้องมีเครื่องหมายการค้าอยู่ใน Forrester Wave ด้าน Network Analytics and Visibility Wave ประจำปี 2023 หรือปีล่าสุด หรือ KuppingerCole Network Detection and Response ประจำปี 2024 หรือปีล่าสุด

18. ผู้เสนอราคาต้องมีหนังสือแต่งตั้งการเป็นตัวแทนจำหน่ายและได้รับการรับรองจากผู้ผลิตสาขาในประเทศไทยโดยตรงว่าอุปกรณ์ที่เสนอเป็นอุปกรณ์ใหม่ไม่เคยใช้งานมาก่อนและยังอยู่ในสายการผลิต

19. มีการรับประกัน (Warranty) และสามารถอัปเดต Signature ด้านความปลอดภัยแบบอัตโนมัติได้เป็นระยะเวลาไม่น้อยกว่า 3 ปี

20. สามารถทำงานร่วมกับระบบป้องกันภัยคุกคามเครือข่าย Next Generation Firewall ภายใต้แบนด์เดียวกันของ สป.พม. เพื่อ quarantine ภัยคุกคามที่เกิดขึ้นได้แบบอัตโนมัติ

4.3 ระบบรักษาความปลอดภัยและตอบสนองต่อภัยคุกคามด้านไซเบอร์ (XDR) สำหรับเครื่องคอมพิวเตอร์แม่ข่าย

1. เป็นซอฟต์แวร์สำหรับช่วยป้องกัน และตอบสนองต่อเหตุการณ์แบบเรียลไทม์ โดยทำงานร่วมกับเวิร์กสเตชัน, เซิร์ฟเวอร์, ระบบ OT และ IoT ได้เป็นอย่างดี และมีลิขสิทธิ์ในการทำงานไม่น้อยกว่า 500 ลิขสิทธิ์

2. สามารถติดตั้งบนระบบปฏิบัติการต่าง ๆ อย่างน้อยได้ดังนี้

2.1 Windows 10 และ 11 ได้เป็นอย่างดี

2.2 Windows Server 2019, 2022 และ 2025 ได้เป็นอย่างดี

2.3 MacOS

2.4 VDI Environments เช่น VMware Horizons 6-7 หรือใหม่กว่า และ Citrix XenDesktop 7

2.5 Red Hat Enterprise, CentOS (6.8+, 7.2+, 8+, 9+), Ubuntu (16.04.5+, 18.04, 20.4,

22.04 64-bit), Oracle Linux (6.10, 7.7+, 8.2+), Amazon Linux AMI, SUSE

3. สามารถตรวจจับและป้องกันภัยคุกคามประเภท Advanced Threats, Ransomware, File-less Malware, Zero-day Attacks, unauthorized transfer และ malicious exfiltration ได้

4. มีความสามารถในการใช้เทคโนโลยีปัญญาประดิษฐ์ (AI) และ Machine Learning (ML) ในการวิเคราะห์พฤติกรรมของภัยคุกคามและกิจกรรมด้านความปลอดภัยจาก Endpoint หรือรองรับการสแกนในรูปแบบ YARA บนเครื่องคอมพิวเตอร์ (Endpoint) ได้

5. มีความสามารถในการหยุดยั้งภัยคุกคาม (Defuse) ได้ในแบบ Real-time ทันทีที่ตรวจพบพฤติกรรมที่เป็นอันตรายได้ทันที

6. สามารถระบุและตรวจสอบ Application ที่ใช้งานภายในองค์กร รวมถึงระดับความน่าเชื่อถือ (Reputation Score) และรายการช่องโหว่ตาม Common Vulnerability Scoring System (CVSS) ได้

7. ระบบต้องมีความสามารถในการทำ Virtual Patching หรือ HIPS เพื่อลดความเสี่ยงจากการใช้ประโยชน์จากช่องโหว่ (Exploitation) บนระบบปฏิบัติการและแอปพลิเคชันได้

8. ระบบต้องมีความสามารถในการค้นหาและระบุอุปกรณ์ที่ไม่ได้ติดตั้ง Agent (Unmanaged Devices) ในเครือข่าย รวมถึงอุปกรณ์ IoT (Internet of Things) ได้
9. ระบบต้องมีความสามารถในการป้องกันและตรวจจับภัยคุกคามบน End-point ได้อย่างต่อเนื่อง แม้จะไม่ได้เชื่อมต่อกับเครือข่าย (Offline Protection) ได้
10. สามารถย้อนกลับการเปลี่ยนแปลงของระบบที่เกิดจากภัยคุกคามโดยอัตโนมัติ (Automated Rollback)
11. สามารถป้องกันการเข้าถึงเว็บไซต์, โดเมน และ IP ที่ไม่ปลอดภัยได้
12. สามารถแสดงข้อมูลเชิงลึกและการสืบค้นหลักฐาน (Threat Hunting) โดยแสดงรายละเอียดของกิจกรรมบน Endpoint เช่น Processes, Files, URL, Domains, และ Registry ที่เกี่ยวข้องกับเหตุการณ์ความปลอดภัยอย่างละเอียด
13. สามารถควบคุมการใช้งานอุปกรณ์ USB แต่ละประเภทเช่น Audio, Video, Mass Storage และ Printer ได้เป็นอย่างดี
14. สามารถกำหนดแอปพลิเคชันที่ไม่ต้องการให้ใช้งานได้ โดยกำหนดคุณลักษณะได้จาก Filename, Path หรือ Hash ได้ และมีการกำหนดกลุ่มแอปพลิเคชันที่ไม่อนุญาตให้ใช้งาน เช่น Disk Encryption Tool, Network Scanning Tool และ Remote Access Tool เป็นอย่างน้อย
15. เชื่อมต่อกับระบบในข้อ 4.1 สำหรับการวิเคราะห์ Log ข้ามอุปกรณ์ (Data lake) หรือเสนออุปกรณ์รวมข้อมูลขนาด 200GB ต่อวัน เป็นอย่างน้อย
16. สามารถวิเคราะห์ตรวจจับเหตุการณ์ที่มีความเสี่ยงร่วมกับระบบ XDR ที่เสนอในโครงการได้ โดยมีความสามารถ ดังนี้
 - 16.1 Network / Port Scanning / ARP Spoofing
 - 16.2 Brute Force / C2C
 - 16.3 Data Exfiltration / Lateral Movement
 - 16.4 Compromised Credentials / Account
17. สามารถทำงานร่วมกับส่วนควบคุมของ Windows Security Center ได้
18. สามารถแสดงผลภัยคุกคามตาม MITRE attack framework

19. สามารถกำหนดเงื่อนไขในการแก้ไขปัญหาเมื่อตรวจพบมัลแวร์ได้อย่างน้อย ดังนี้
- 19.1 สามารถกักกัน Endpoint ที่ติดเชื้อ (Isolate/Quarantine) ออกจากเครือข่ายได้ทันที
 - 19.2 สามารถยุติ Process ที่เป็นอันตราย (Terminate Malicious Processes)
 - 19.3 ลบไฟล์ที่เป็นอันตราย (Delete Malicious Files)
 - 19.4 สามารถทำงานร่วมกับระบบป้องกันเครือข่าย (NGFW) เพื่อส่งข้อมูลการตรวจจับ และสามารถดำเนินการตอบสนองอัตโนมัติได้
20. สามารถเชื่อมต่อกับ Threat Intelligence ภายนอกด้วยมาตรฐาน TAXII หรือ JSON ได้เป็นอย่างน้อย
21. สามารถพิสูจน์ตัวตน (Authentication) ผู้ดูแลระบบได้ โดยรองรับฐานข้อมูลผู้ใช้แบบ Local, LDAP, SAML และสามารถทำงานร่วมกับระบบ Two-Factor authentication ได้
22. สามารถทำงานร่วมกับระบบความปลอดภัยอื่นๆ ผ่านตัวเชื่อมต่อ (Connector) หรือ API เช่น Firewall, Sandbox, NAC และมีความสามารถปรับแต่งตัวเชื่อมต่อได้ (Custom Connector)
23. สามารถกำหนดวิธีแก้ไขปัญหา (Action) เมื่อมีเหตุการณ์ด้านความปลอดภัยได้อย่างอัตโนมัติผ่าน Playbook Policies
24. สามารถทำงานร่วมกับ Events-Management Tool เช่น Jira หรือ ServiceNow ได้เป็นอย่างน้อย
25. สามารถเข้าถึงเครื่อง endpoint ได้โดยตรงเพื่อตรวจสอบและรวบรวมข้อมูลผ่านทาง Remote Shell หรือ Remote Connection ได้
26. สามารถส่ง Log ด้วย Syslog ไปยังอุปกรณ์ภายนอก เช่น ระบบ SIEM ได้เป็นอย่างน้อย
27. สามารถทำการแจ้งเตือนผู้ดูแลระบบเมื่อพบมัลแวร์ผ่านทางระบบ e-Mail และ Syslog ได้เป็นอย่างน้อย
28. Agent ของระบบต้องมีขนาดเล็กและใช้ทรัพยากรของ Endpoint ต่ำ (Lightweight Agent) โดยมีผลกระทบต่อประสิทธิภาพการทำงานของ CPU, หน่วยความจำ (RAM) และพื้นที่จัดเก็บข้อมูลน้อยที่สุดเพื่อไม่รบกวนการใช้งานปกติของผู้ใช้
29. ผลิตภัณฑ์ที่เสนอต้องเครื่องหมายการค้าอยู่ใน Forrester Wave ด้าน Extended Detection and Response Platforms ประจำปี 2023 หรือปีล่าสุด และ KuppingerCole XDR Leadership Compass ประจำปี 2024 หรือปีล่าสุด
30. ผลิตภัณฑ์ที่นำเสนอต้องเป็น SaaS (Software as a Service) ที่ทำงานแบบ On-Cloud โดยที่ผลิตภัณฑ์ต้องได้รับมาตรฐาน ISO 27001 หรือ SOC 2 เป็นอย่างน้อย

31. ผู้เสนอราคาต้องมีหนังสือแต่งตั้งการเป็นตัวแทนจำหน่ายจากบริษัทเจ้าของผลิตภัณฑ์ที่มีสาขาในประเทศไทยโดยตรง

4.4 ระบบรักษาความปลอดภัยและตอบสนองต่อภัยคุกคามด้านไซเบอร์ (EDR) สำหรับคอมพิวเตอร์ลูกข่าย

1. เป็นซอฟต์แวร์สำหรับช่วยป้องกันและตอบสนองต่อเหตุการณ์แบบเรียลไทม์ โดยทำงานร่วมกับเวิร์กสเตชัน, เซิร์ฟเวอร์, ระบบ OT และ IoT ได้เป็นอย่างดี และมีประสิทธิภาพในการทำงานไม่น้อยกว่า 1,000 ลิขสิทธิ์

2. สามารถติดตั้งบนระบบปฏิบัติการต่างๆ อย่างน้อยได้ ดังนี้

2.1 Windows 10 และ 11

2.2 Windows Server 2022 และ 2025

2.3 MacOS

2.4 VDI Environments เช่น VMware Horizons 6-7 หรือใหม่กว่า และ Citrix XenDesktop 7

2.5 Red Hat Enterprise, CentOS (6.8+, 7.2+, 8+, 9+), Ubuntu (16.04.5+, 18.04, 20.4, 22.04 64-bit), Oracle Linux (6.10, 7.7+, 8.2+), Amazon Linux AMI, SUSE

2.6 Mobile OS เช่น Android และ iOS

3. สามารถตรวจจับและป้องกันภัยคุกคามประเภท Advanced Threats, Ransomware, File-less Malware, Zero-day Attacks, unauthorized transfer และ malicious exfiltration ได้

4. มีความสามารถในการใช้เทคโนโลยีปัญญาประดิษฐ์ (AI) และ Machine Learning (ML) ในการวิเคราะห์พฤติกรรมของภัยคุกคามและกิจกรรมด้านความปลอดภัยจาก Endpoint หรือรองรับการสแกนในรูปแบบ YARA บนเครื่องคอมพิวเตอร์ (Endpoint) ได้

5. มีความสามารถในการหยุดยั้งภัยคุกคาม (Defuse) ได้ในแบบ Real-time ทันทีที่ตรวจพบพฤติกรรมที่เป็นอันตรายได้ทันที

6. สามารถระบุและตรวจสอบ Application ที่ใช้งานภายในองค์กร รวมถึงระดับความน่าเชื่อถือ (Reputation Score) และรายการช่องโหว่ตาม Common Vulnerability Scoring System (CVSS) ได้

7. ระบบต้องมีความสามารถในการทำ Virtual Patching หรือ HIPS เพื่อลดความเสี่ยงจากการใช้ประโยชน์จากช่องโหว่ (Exploitation) บนระบบปฏิบัติการและแอปพลิเคชันได้

8. ระบบต้องมีความสามารถในการค้นหาและระบุอุปกรณ์ที่ไม่ได้ติดตั้ง Agent (Unmanaged Devices) ในเครือข่าย รวมถึงอุปกรณ์ IoT (Internet of Things) ได้

9. ระบบต้องมีความสามารถในการป้องกันและตรวจจับภัยคุกคามบน End-point ได้อย่างต่อเนื่อง แม้จะไม่ได้เชื่อมต่อกับเครือข่าย (Offline Protection) ได้

10. สามารถย้อนกลับการเปลี่ยนแปลงของระบบที่เกิดจากภัยคุกคามโดยอัตโนมัติ (Automated Rollback)

11. สามารถป้องกันการเข้าถึงเว็บไซต์, โดเมน และ IP ที่ไม่ปลอดภัยได้

12. สามารถแสดงข้อมูลเชิงลึกและการสืบค้นหลักฐาน (Threat Hunting) โดยแสดงรายละเอียดของกิจกรรมบน Endpoint เช่น Processes, Files, URL, Domains, และ Registry ที่เกี่ยวข้องกับเหตุการณ์ความปลอดภัยอย่างละเอียด

13. สามารถควบคุมการใช้งานอุปกรณ์ USB แต่ละประเภทเช่น Audio, Video, Mass Storage และ Printer ได้เป็นอย่างดี

14. สามารถกำหนดแอปพลิเคชันที่ไม่ต้องการให้ใช้งานได้ โดยกำหนดคุณลักษณะได้จาก Filename, Path หรือ Hash ได้ และมีการกำหนดกลุ่มแอปพลิเคชันที่อนุญาตให้ใช้งาน เช่น Disk Encryption Tool, Network Scanning Tool และ Remote Access Tool เป็นอย่างน้อย

15. สามารถทำงานร่วมกับส่วนควบคุมของ Windows Security Center ได้

16. สามารถแสดงผลภัยคุกคามตาม MITRE attack framework

17. สามารถกำหนดเงื่อนไขในการแก้ปัญหาเมื่อตรวจพบมัลแวร์ได้อย่างน้อย

18. สามารถกักกัน Endpoint ที่ติดเชื้อ (Isolate/Quarantine) ออกจากเครือข่ายได้ทันที

19. สามารถยุติ Process ที่เป็นอันตราย (Terminate Malicious Processes)

20. ลบไฟล์ที่เป็นอันตราย (Delete Malicious Files)

21. สามารถทำงานร่วมกับระบบป้องกันเครือข่าย (NGFW) เพื่อส่งข้อมูลการตรวจจับและสามารถดำเนินการตอบสนองอัตโนมัติได้

22. สามารถเชื่อมต่อกับ Threat Intelligence ภายนอกด้วยมาตรฐาน TAXII หรือ API ได้เป็นอย่างดี

23. สามารถพิสูจน์ตัวตน (Authentication) ผู้ดูแลระบบได้ โดยรองรับฐานข้อมูลผู้ใช้แบบ Local, LDAP, SAML และสามารถทำงานร่วมกับระบบ Two-Factor authentication ได้

24. สามารถทำงานร่วมกับระบบความปลอดภัยอื่นๆ ผ่านตัวเชื่อมต่อ (Connector) หรือ API เช่น Firewall, Sandbox, NAC และมีความสามารถปรับแต่งตัวเชื่อมต่อได้ (Custom Connector)

25. สามารถกำหนดวิธีแก้ไขปัญหา (Action) เมื่อมีเหตุการณ์ด้านความปลอดภัยได้อย่างอัตโนมัติผ่าน Playbook Policies

26. สามารถกำหนด Application โดยมี Module Application Control โดยสามารถเลือกทำ Application ให้เป็น Denylist ได้โดยเลือกจาก Files Hash, Certification, Category หรือ Group และสามารถกำหนดการใช้งานเป็นแบบ TEST Rules หรือ Simulation Rules ได้

27. สามารถทำงานร่วมกับ Events-Management Tool เช่น Jira หรือ ServiceNow ได้เป็นอย่างดี

28. สามารถเข้าถึงเครื่อง endpoint ได้โดยตรงเพื่อตรวจสอบและรวบรวมข้อมูลผ่านทาง Remote Shell หรือ Remote Connection ได้

29. สามารถส่ง Log ด้วย Syslog ไปยังอุปกรณ์ภายนอกเช่น ระบบ SIEM ได้เป็นอย่างดี

30. สามารถทำการแจ้งเตือนผู้ดูแลระบบเมื่อพบมัลแวร์ผ่านทางระบบ e-Mail และ Syslog ได้เป็นอย่างดี

31. Agent ของระบบต้องมีขนาดเล็กและใช้ทรัพยากรของ Endpoint ต่ำ (Lightweight Agent) โดยมีผลกระทบต่อประสิทธิภาพการทำงานของ CPU, หน่วยความจำ (RAM) และพื้นที่จัดเก็บข้อมูลน้อยที่สุดเพื่อไม่รบกวนการใช้งานปกติของผู้ใช้

32. ผลิตภัณฑ์ที่เสนอต้องเครื่องหมายการค้าอยู่ใน Forrester Wave ด้าน Extended Detection and Response Platforms ประจำปี 2023 หรือปีล่าสุด และ KuppingerCole XDR Leadership Compass ประจำปี 2024 หรือปีล่าสุด

33. ผลิตภัณฑ์ที่นำเสนอต้องเป็น SaaS (Software as a Service) ที่ทำงานแบบ On-Cloud โดยที่ผลิตภัณฑ์ต้องได้รับมาตรฐาน ISO-27001 หรือ SOC 2 เป็นอย่างน้อย

34. ผู้เสนอราคาต้องมีหนังสือแต่งตั้งการเป็นตัวแทนจำหน่ายจากบริษัทเจ้าของผลิตภัณฑ์ที่มีสาขาในประเทศไทยโดยตรง

4.5 ระบบบริหารจัดการและตอบสนองเหตุการณ์ภัยคุกคามด้านไซเบอร์อย่างอัตโนมัติ (SOAR)

1. เป็นระบบทำหน้าที่จัดการ หรือเรียบเรียงการตอบสนองด้านความปลอดภัยแบบอัตโนมัติ (Security Orchestration Automation and Response: SOAR) เพื่อสนับสนุนการทำงานทีม SOC โดยเฉพาะ

2. ระบบที่นำเสนอต้องมีเครื่องหมายการค้าเดียวกันกับระบบ SIEM ที่เสนอในโครงการ เพื่อให้สามารถทำงานร่วมกันได้โดยสมบูรณ์

3. มีคุณสมบัติในการจัดการ security alert, incident, indicator, asset และ task ผ่านหน้า GUI ได้
4. มีคุณสมบัติ Role-Based Management เพื่อแบ่งระดับการเข้าถึงข้อมูล หรือ policies และ Dashboard หรือรายงานได้
5. มีลิขสิทธิ์ผู้ใช้งานระบบได้ไม่น้อยกว่า 2 licenses และทำงานได้แบบ Named user และ Concurrent user ได้
6. รองรับการทำงานแบบ Multi-tenancy Distributed Deployment หรือ Share Deployment ได้ โดยสามารถกำหนดการทำงานแบบอัตโนมัติ (Automation Workflow) ระบุแบ่งตาม Tenant ได้เป็นอย่างดี
7. สามารถสร้าง ออกแบบ พัฒนา ควบคุม และใช้งาน Playbook ได้เป็นอย่างดี
8. Manual action and Task
9. ขั้นตอนการตัดสินใจและการอนุมัติ (Decision and Approve)
10. เรียกใช้งาน Playbook ซ้อนกันได้ (Reference Playbook)
11. กำหนดเงื่อนไขและลูปได้ (Condition and Loop)
12. มี build-in connector ที่ทำงานร่วมกับ security platform ได้ไม่น้อยกว่า 600 Connector
13. มี Playbook แบบพร้อมใช้งาน (Pre-Defined) และ สามารถสร้างเพิ่มเติม แก้ไข Playbooks ได้ตามต้องการ (Customize) ในรูปแบบ Drag and Drop (Visual Playbook Builder) ได้
14. สามารถกำหนด SLA (Service Level Agreement) โดยแยกแต่ละ Incident ได้ และสามารถติดตาม SLA พร้อมทั้งสามารถตรวจสอบระยะเวลาของเหตุการณ์
15. สามารถบริหารจัดการวิกฤตเหตุการณ์ (Incident War Room) หรือ Incident management เพื่อมอบหมาย ติดตามและจัดระเบียบการสืบสวน โดยทำงานร่วมกับเครื่องมือภายนอกเช่น MS Team, Slack, Zoom ได้เป็นอย่างดี
16. ผู้ใช้งานสามารถทำงานร่วมกันและแบ่งปันข้อมูล (Collaboration and Information Sharing) ได้
17. สามารถรับข้อมูลจาก PDF file และนำไปสร้างเป็น Indicator ให้กับระบบได้
18. สามารถเชื่อมโยง Incident กับขั้นตอนของ Cyber Kill Chain ได้
19. สามารถทำการแนะนำหรือวิเคราะห์และจัดการข้อมูล (Records) ที่คล้ายกันในระบบ SOAR ด้วย Machine-Learning (ML) ได้

20. สามารถแสดงผลในรูปแบบ Chart, Listing, Counter และ Performance Metric ได้เป็น
อย่างน้อย
21. สามารถแสดงความสัมพันธ์ของ Indicators, Alert และ Incidents ในรูปแบบ Tree view
หรือ Hub and Spoke view หรือ Investigation Graph
22. สามารถออกรายงานในรูปแบบ PDF และ CSV ได้เป็นอย่างน้อย
23. สามารถทำการนำเข้าและส่งออก Playbook รวมถึงเวอร์ชันที่ถูกบันทึกไว้ได้เป็นอย่างน้อย
24. สามารถบริหารจัดการ Event, Incident, playbook action ผ่าน Mobile Application หรือ
Web Application ได้ทั้งระบบ Android และ IOS เป็นอย่างน้อย
25. สามารถทำงานร่วมกับระบบพิสูจน์ตัวตนเช่น Local, LDAP หรือ SAML ได้เป็นอย่างน้อย
26. รองรับการบริหารและรวบรวมข้อมูลภัยคุกคามไซเบอร์ (Threat Intelligence Management)
และสามารถส่งออกตัวบ่งชี้ในรูปแบบ STIX หรือ JSON ได้เป็นอย่างน้อย
27. สามารถสร้างและแก้ไขตัวเชื่อมต่อ (Connector) ภายในผลิตภัณฑ์ได้ผ่าน GUI
28. รองรับการเชื่อมต่อกับ 3rd Party ได้อย่างน้อย ดังต่อไปนี้
- 28.1 Network Firewall: FortiGate, Cisco Meraki Firewall, CISCO Firepower,
Zscaler, RSA Netwitness, PaloAlto Firewall, CISCO ASA, Check Point Firewall
 - 28.2 Vulnerability Management: Rapid7 Nexpose, Kenna, Qualys, Tenable
 - 28.3 Ticket Management: Manage Engine Service Desk, BMC Remedy AR System,
JIRA, ServiceNow
 - 28.4 Endpoint Security: CrowdStrike Falcon, Symantec EDR Cloud, Microsoft
Defender, SentinelOne, FortiEDR
29. ระบบรองรับการทำ High Availability แบบ Active/Active, Active/Passive หรือ Cluster ได้
30. สามารถอัปเดต Threat Intelligence จากฐานข้อมูลของเจ้าของผลิตภัณฑ์ได้อย่างต่อเนื่อง
ตลอดอายุสัญญา มีลิขสิทธิ์ในการใช้งานเป็นระยะเวลาไม่น้อยกว่า 3 ปี

4.6 ระบบรักษาความปลอดภัยสำหรับระบบฐานข้อมูล (Database Firewall)

1. เป็นซอฟต์แวร์ที่ออกแบบมาเพื่อตรวจสอบ ควบคุมและป้องกันการโจมตีฐานข้อมูล เพื่อให้สามารถใช้ข้อมูลจากฐานข้อมูลให้มีความปลอดภัย
2. มีสิทธิ์ในการใช้งานไม่ต่ำกว่า 3 ฐานข้อมูล โดยผู้เสนอราคาจะต้องออกแบบและนำเสนอ Hardware ที่มีความเหมาะสมกับการใช้งาน
3. สามารถตรวจสอบและป้องกันการโจมตีฐานข้อมูลดังต่อไปนี้ได้ ได้แก่, Oracle, Teradata, SAP HANA, Neo4j, PostgreSQL, Hive, MySQL, MS SQL Server, IBM DB2, MongoDB และ Impala ได้เป็นอย่างดี
4. สามารถตรวจสอบและ monitor การใช้งานฐานข้อมูลได้แบบ Real-time
5. สามารถป้องกันการโจมตีฐานข้อมูลด้วยเทคนิค SQL Injection, DDoS Attacks หรือ Rate Limiting, Brute-force รวมถึง Unauthorized Query หรือ Unauthorized SQL ได้เป็นอย่างดี
6. สามารถเก็บ log การใช้งานของผู้ใช้ที่มีการเข้าถึงข้อมูลในฐานข้อมูล โดยจัดเก็บ Query และผลลัพธ์ที่ได้ตลอดจนข้อมูลอื่นๆ ที่เกี่ยวข้องกับผู้ใช้ เช่น IP Address, Username, Client application name เป็นต้น
7. สามารถสร้าง Policy เพื่อควบคุมการเข้าถึงฐานข้อมูล โดยใช้เงื่อนไข Database name (หรือ Host), IP Address (หรือ DB User), Client Application (หรือ Application) และ Query (หรือ Regular Expression) ได้เป็นอย่างดี
8. สามารถทำ Data Masking เพื่อให้ข้อมูลมีความปลอดภัย โดยต้องรองรับเทคนิค ดังต่อไปนี้
 - oDynamic Data Masking หรือ Data Redaction
 - oStatic Data Masking
 - oIn-place Data Masking หรือ In-Database/In-Export Data Masking
9. สามารถเข้ารหัสข้อมูลและคงรูปแบบเดิมของข้อมูลไว้ได้ (Format-Preserving Encryption)
10. สามารถตรวจสอบและค้นหาข้อมูล Sensitive หรือ Confidential Information ในฐานข้อมูลได้
11. สามารถวิเคราะห์พฤติกรรมการใช้งานของผู้ใช้ (User Behavior) และแจ้งเตือนหากพบพฤติกรรมการใช้งานที่ผิดปกติ
12. สามารถติดตั้งและทำงานทั้งในรูปแบบของ Sniffer Mode หรือ Out of band mode และ Proxy Mode และ Trailing DB audit logs ได้
13. สามารถตรวจสอบ Compliance ได้ตามมาตรฐาน HIPAA, GDPR, PCI DSS, SOX และ ISO 27001 เป็นอย่างดี
14. สามารถตรวจสอบข้อมูลช่องโหว่หรือ Patch ล่าสุดเกี่ยวกับฐานข้อมูล เพื่อ update ให้มีความปลอดภัยล่าสุดได้

15. สามารถเชื่อมต่อกับระบบ SIEM ได้เป็นอย่างดีน้อย และสามารถสร้างรายงานในรูปแบบ PDF และ CSV ได้

4.7 ระบบตรวจสอบและรายงานช่องโหว่ของระบบปฏิบัติการและแอปพลิเคชัน (Vulnerability Assessment Tool)

1. ระบบที่นำเสนอต้องถูกออกแบบมาเพื่อทำหน้าที่ตรวจสอบและบริหารจัดการความเสี่ยงจากช่องโหว่ (Vulnerability Management) ในรูปแบบ Cloud โดยเฉพาะ
2. ต้องรองรับการตรวจหาช่องโหว่ในระบบได้จำนวนไม่น้อยกว่า 150 Assets
3. สามารถรองรับการตรวจสอบได้ทั้งในรูปแบบ Active scan และ Agent scan เพื่อการตรวจสอบช่องโหว่แบบเต็มรูปแบบ
4. สามารถบริหารจัดการผ่านทาง Secure Web Browser (HTTPS) ได้
5. สามารถตั้งค่าการตรวจสอบได้ทั้งในรูปแบบของ IPv4 และ IPv6 ได้
6. สามารถตั้งค่าการตรวจสอบได้ทั้งในรูปแบบของ Single IP, List of IP, IP range และ Subnet ได้
7. สามารถแสดงข้อมูลที่ได้จากการตรวจสอบช่องโหว่ในรูปแบบของรูปภาพ (Dashboard) ได้
8. สามารถตรวจสอบช่องโหว่ของระบบปฏิบัติการ เช่น Microsoft Windows, Linux, Solaris, OS X, FreeBSD และ VMware ได้เป็นอย่างดีน้อย
9. สามารถตรวจสอบช่องโหว่ของ Database เช่น SQL Server, Oracle, MongoDB, MySQL, และ PostgreSQL ได้เป็นอย่างดีน้อย
10. สามารถตรวจสอบช่องโหว่ของอุปกรณ์ได้ทั้งแบบ Credentialed หรือ Authenticated และ Non-Credentialed หรือ Unauthenticated
11. สามารถจัดลำดับความรุนแรงของช่องโหว่ตามมาตรฐาน CVSS ได้
12. มีข้อมูลสำหรับการตรวจสอบช่องโหว่ (Plugin) หรือ Detections ไม่น้อยกว่า 210,000 plugins
13. สามารถทำการเลือกประเภทของช่องโหว่เพื่อทำการตรวจสอบเฉพาะช่องโหว่ที่ต้องการได้ (Plugin Family) หรือ Category
14. มีฐานข้อมูลช่องโหว่ตาม CVE (Common Vulnerabilities and Exposures) ไม่น้อยกว่า 87,000 ช่องโหว่

15. มีกระบวนการในการจัดลำดับความสำคัญของช่องโหว่ โดยอาศัยการวิเคราะห์เชิงลึก และการคาดการณ์ได้ (Prioritize Vulnerabilities)
16. สามารถตรวจสอบการตั้งค่า (Configuration audit) ตามมาตรฐาน CIS ได้เป็นอย่างดี
17. สามารถบอกรายละเอียด (Description) ให้คำแนะนำวิธีในการแก้ไขปัญหาของช่องโหว่ (Solution) รวมถึงการแสดงผลอ้างอิง ต่าง ๆ ได้
18. สามารถสร้างรูปแบบในการตรวจสอบ (Scan Template) ได้
19. สามารถตั้งค่าการตรวจสอบช่องโหว่ ตามช่วงเวลาที่กำหนด (Schedule Scan) ได้ทั้งแบบ Daily, Weekly, Monthly และ Yearly ได้
20. สามารถเปรียบช่องโหว่ที่ตรวจพบ กับข้อมูลการถูกโจมตีจาก 3rd party เช่น Core Impact, Metasploit และ Canvas ได้
21. สามารถแจ้งเตือนผลการตรวจสอบช่องโหว่ และรายงานให้ผู้ดูแลระบบผ่านทาง e-Mail ได้
22. สามารถสร้างรายงานตามรูปแบบไฟล์ PDF ได้เป็นอย่างดี
23. สามารถกำหนด User Role เพื่อกำหนดสิทธิ์สำหรับ User ที่ Login เข้ามาในระบบได้
24. ระบบที่นำเสนอต้องเป็นผลิตภัณฑ์ที่อยู่ในกลุ่ม Strong Performers หรือดีกว่า ของ The Forrester Wave ด้าน Vulnerability Risk Management ปี 2025
25. มีซอฟต์แวร์สำหรับตรวจสอบความปลอดภัย Web Application ในรูปแบบ On-cloud โดยมีลิขสิทธิ์การใช้งาน 5 Fully Qualified Domain Name (FQDN) เป็นอย่างน้อย มีคุณสมบัติอย่างน้อย ดังนี้
- สามารถบริหารจัดการผ่านทาง Web Browser (HTTPS) ได้
 - สามารถตรวจสอบช่องโหว่ของ Web Server ที่เกี่ยวกับ Apache, Apache Tomcat, IIS และ NGINX ได้เป็นอย่างดี
 - สามารถตรวจสอบช่องโหว่ของ Open Web Application Security (OWASP Top 10) ได้
 - สามารถตรวจสอบช่องโหว่ของ Web Application ด้วยวิธีการ Crawling
 - สามารถกำหนดเวลาในการตรวจสอบได้ล่วงหน้า (Schedule) ได้แบบรายวัน (Daily), รายสัปดาห์ (Weekly) แบบรายเดือน (Monthly) และรายปี (Yearly) เป็นอย่างน้อย
 - สามารถกำหนดประเภทของการสแกนได้ (Scan type) หรือ profile
 - สามารถกำหนดการตั้งค่าในการสแกน Web Application ในรูปแบบ Domain Name ได้เป็นอย่างดี
 - มีข้อมูลสำหรับการตรวจสอบช่องโหว่ (Plugin) หรือ detections ไม่น้อยกว่า 193,000 plugins หรือ Detections

- สามารถทำการสแกน Web Application ในรูปแบบ Authentication ได้
- สามารถจัดลำดับความรุนแรงของช่องโหว่ตามมาตรฐาน CVSS ได้
- สามารถให้คำแนะนำ วิธีในการแก้ไขปัญหาของช่องโหว่ (Remediation) ได้
- สามารถสร้างรายงานตามรูปแบบไฟล์ PDF หรือ CSV ได้เป็นอย่างน้อย
- ระบบที่นำเสนอต้องเป็นผลิตภัณฑ์ที่อยู่ในกลุ่ม Strong Performers หรือดีกว่า ของ The Forrester Wave ด้าน Vulnerability Risk Management ปี 2025

4.8 เงื่อนไขการเสนอราคา

4.8.1 คุณลักษณะเฉพาะของครุภัณฑ์คอมพิวเตอร์และอุปกรณ์ทุกรายการ ซึ่งผู้เสนอราคาขาย จะต้องเสนอคุณลักษณะไม่ต่ำกว่าคุณลักษณะเฉพาะที่ สป.พม. กำหนด

4.8.2 ครุภัณฑ์คอมพิวเตอร์และอุปกรณ์ที่เสนอ ต้องเป็นรุ่นที่ยังอยู่ในสายการผลิตในวันยื่นข้อเสนอ ราคาและต้องเป็นเครื่องใหม่ที่ยังมิได้ทำการติดตั้งใช้งานที่ใดมาก่อน และไม่เป็นเครื่องที่ถูกนำมาปรับปรุงสภาพ ใหม่ (Reconditioned หรือ Rebuilt) โดยมีหนังสือรับรองจากเจ้าของผลิตภัณฑ์ (สาขาในประเทศไทย) โดยตรง

4.8.3 ครุภัณฑ์คอมพิวเตอร์และอุปกรณ์ที่เสนอ ต้องไม่เป็นผลิตภัณฑ์ของบริษัทที่อยู่ในระหว่างการ คຸ້ມครองเป็นบุคคลหรือนิติบุคคลผู้ล้มละลาย ตามคำสั่งของศาลที่ได้สั่งการตามกฎหมายของประเทศที่บริษัท ของผู้ผลิตตั้งอยู่

4.8.4 ครุภัณฑ์คอมพิวเตอร์และอุปกรณ์ที่เสนอ ให้รวมค่าฮาร์ดแวร์ ซอฟต์แวร์ การตั้งค่าอุปกรณ์ และค่าขนส่ง โดย สป.พม. ไม่ต้องเสียค่าใช้จ่ายใดๆ เพิ่มเติมจากที่ปรากฏในใบเสนอราคา

4.8.5 ผู้เสนอราคาจะต้องส่งแคตตาล็อกและ/หรือแบบรูปรายการรายละเอียดคุณลักษณะเฉพาะ ของครุภัณฑ์คอมพิวเตอร์และอุปกรณ์ไปพร้อมเอกสารส่วนที่ 1 และเอกสารส่วนที่ 2 เพื่อประกอบการพิจารณา

4.8.6 ผู้เสนอราคาต้องทำสัญลักษณ์ เช่น การเน้นข้อความ หรือทำป้ายกำกับที่อ้างอิงคุณลักษณะ ของครุภัณฑ์คอมพิวเตอร์และอุปกรณ์ที่เสนอให้ตรงตามข้อกำหนดไว้ในเอกสารส่วนที่ 2 เพื่อความสะดวก ในการพิจารณาข้อเสนอ

4.8.7 สำหรับแคตตาล็อกที่แนบให้พิจารณาหากเป็นสำเนาอยู่จะต้องรับรองสำเนาถูกต้อง โดย ผู้มีอำนาจทำนิติกรรมแทนนิติบุคคล หากคณะกรรมการประกวดราคามีความประสงค์จะขอดูต้นฉบับ แคตตาล็อก ผู้เสนอราคาจะต้องนำต้นฉบับมาให้คณะกรรมการประกวดราคาตรวจสอบภายใน 2 วัน

4.8.8 ครุภัณฑ์คอมพิวเตอร์และอุปกรณ์ที่เสนอทั้งหมดต้องสามารถใช้กับระบบไฟฟ้า 220 VAC 50 Hz และต้องทำงานได้ดีในสภาพแวดล้อมปกติของประเทศไทย

4.8.9 ครุภัณฑ์คอมพิวเตอร์และอุปกรณ์ที่เสนอต้องมีเอกสารหรือคู่มือการใช้งานที่เป็นชุดต้นฉบับ

4.9 เงื่อนไขการดำเนินงานและการติดตั้ง

4.9.1 ผู้ขายต้องมีทีมงาน เจ้าหน้าที่ ที่มีความรู้ ความสามารถในการติดตั้ง ตั้งค่าอุปกรณ์ตามที่เสนอพร้อมจัดทำเอกสารแสดงรายละเอียดของบุคลากร พร้อมทั้งแนบสำเนาหลักฐานประกอบด้วย ประวัติส่วนตัว ประวัติการทำงาน คุณวุฒิการศึกษา ผลงาน และสำเนาหลักฐานประสบการณ์การทำงาน ใบประกอบวิชาชีพ (ถ้ามี) หรือเอกสารประกอบอื่นๆ ที่เกี่ยวข้องและจำเป็นในการพิจารณาคุณสมบัติของเจ้าหน้าที่ดังกล่าว ในวันที่ยื่นข้อเสนอตามแบบที่กำหนด ดังเอกสาร ภาคผนวก 1

4.9.2 ผู้ขายจะต้องทำการศึกษาระบบเดิมของ สป.พม. พร้อมทั้งวิเคราะห์ ออกแบบระบบที่จัดหาใหม่ให้สามารถใช้งานร่วมกันได้อย่างเต็มประสิทธิภาพ พร้อมทั้งติดตั้งและเดินสายสัญญาณเครือข่ายเชื่อมต่อกับอุปกรณ์เดิมลงในตู้จัดเก็บอุปกรณ์เครือข่ายของ สป.พม. ทั้งนี้ผู้ขายต้องจัดหาสายสัญญาณเครือข่าย คอมพิวเตอร์และอุปกรณ์อื่นๆ ที่เกี่ยวข้องกับการติดตั้งโดยไม่มีค่าใช้จ่ายเพิ่มเติม

4.9.3 ผู้ขายต้องวาดผังการติดตั้งอุปกรณ์ และอธิบายการตั้งค่าอุปกรณ์แต่ละชิ้น รวมถึงการจัดทำ playbook ของแต่ละอุปกรณ์ และคู่มือการใช้งานเป็นภาษาไทย โดยให้จัดทำเป็นเอกสารจำนวน 3 ชุด พร้อม (Soft copy) หรือไฟล์ที่สามารถแก้ไขได้

4.9.4 ผู้ขายต้องจัดหาเครื่องคอมพิวเตอร์สำหรับใช้ในการติดตั้งระบบหรือบริหารจัดการระบบตามข้อ 4.3 – 4.7 ระบบละ 1 เครื่อง

4.9.5 ผู้ขายต้องทำการตั้งค่าอุปกรณ์แต่ละรายการให้มีการตรวจจับ ป้องกัน วิเคราะห์ และแจ้งเตือนให้กับผู้ใช้งาน โดยต้องตั้งค่าอุปกรณ์ต่างๆ ให้เชื่อมโยงกันอย่างเป็นระบบตามข้อเสนอแนะของบริษัท รวมทั้งตั้งค่าการป้องกันให้เป็นอัตโนมัติ

4.9.6 ระหว่างการส่งมอบและตรวจรับพัสดุ สป.พม. มีสิทธิ์ที่จะใช้ครุภัณฑ์คอมพิวเตอร์และอุปกรณ์ในส่วนที่ส่งมอบได้ และหากมีเหตุให้ต้องเลิกสัญญาอันเนื่องจากความผิดของผู้ขาย ในกรณีนี้ผู้ขายไม่มีสิทธิ์ที่จะเรียกร้องค่าเสียหายใดๆ อันเกิดจากการใช้เครื่องคอมพิวเตอร์และอุปกรณ์ ในระหว่างที่การตรวจรับยังไม่สมบูรณ์

4.9.7 การตรวจรับพัสดุ สป.พม. จะดำเนินการทดสอบการใช้งานครุภัณฑ์คอมพิวเตอร์และอุปกรณ์ หากพบว่ามีครุภัณฑ์คอมพิวเตอร์หรืออุปกรณ์เครื่องใดมีปัญหาไม่สามารถใช้งานได้ในช่วงการทดสอบ ผู้ขายจะต้องดำเนินการเปลี่ยนเครื่องใหม่ให้ทันที

4.9.8 ผู้ขายจะต้องส่งมอบเอกสารคู่มือ และ/หรือ CD/DVD ต่อไปนี้

- 1) คู่มือการติดตั้งใช้งานอุปกรณ์ทั้งหมด
- 2) เอกสารการรับประกัน
- 3) เอกสารแสดงลิขสิทธิ์ซอฟต์แวร์

4.10 เงื่อนไขอื่น ๆ

4.10.1 ผู้ขายจะต้องจัดทำแผนการดำเนินงาน โดยระบุรายละเอียดต่างๆ เช่น ขอบเขตงานและ กิจกรรมหลัก (Scope & Key Activities) ระยะเวลาและกำหนดการ (Timeline) เป็นอย่างน้อย โดยผู้ขายจะต้อง จัดทำแผนดังกล่าวส่งให้ สป.พม. ภายใน 15 วัน นับถัดจากวันลงนามในสัญญา โดยถือว่าแผนการดำเนินงาน ที่ส่งมา เป็นส่วนหนึ่งของเอกสารประกอบสัญญาด้วย

4.10.2 อุปกรณ์ที่ผู้ขายจะส่งมอบทุกชนิด ต้องเป็นของแท้ ของใหม่ ไม่เคยใช้งานมาก่อน ไม่เป็น ของเก่าเก็บ อยู่ในสภาพพร้อมที่จะใช้งานได้ทันที

4.10.3 ผู้ขายเป็นผู้รับผิดชอบค่าใช้จ่ายทั้งสิ้นในการส่งมอบอุปกรณ์ทั้งหมดที่เสนอในโครงการ และ ส่งมอบงานตามโครงการ

4.10.4 ผู้ขายต้องรับผิดชอบต่อความผิดพลาดเสียหายที่เกิดขึ้นแก่งานนี้ ตลอดจนทรัพย์สินใดๆ ของ สป.พม. และบุคคลผู้ใดได้รับความเสียหายจากการปฏิบัติงานนี้รวมถึงเหตุแห่งความล่าช้าในการปฏิบัติงาน ไม่อาจจะ ปฏิบัติงานให้แล้วเสร็จสมบูรณ์ ปฏิบัติงานด้วยความประมาทเลินเล่อ เจตนาทุจริต ปฏิบัติงานผิดวัตถุประสงค์ หรือรายละเอียด ไม่ปฏิบัติตามวิธีช่างหรือวิธีการที่ถูกต้องหรือปฏิบัติงานด้วยความรู้เท่าไม่ถึงการณ์ หรือสาเหตุ ใดก็ตามที่ก่อให้เกิดความเสียหาย ก่อให้เกิดอัตราย ทำความเสียหายให้แก่ทรัพย์สินโปรแกรมคอมพิวเตอร์ และระบบคอมพิวเตอร์ของ สป.พม. ตลอดจนก่อความเสียหายให้แก่บุคคลใด ผู้ขายต้องยอมชดเชยค่าเสียหาย ตามมูลค่าความเสียหายนั้นและทำการซ่อมแซมหรือรื้อถอนเปลี่ยนอุปกรณ์ที่เสียหายนั้นให้ใหม่ พร้อมติดตั้งให้ ใช้งานได้ติดตั้งเต็ม ตามที่ ศทส. เห็นสมควร และผู้ขายจะนำมาเป็นเหตุอ้าง เพื่อยืดเวลาแล้วเสร็จในการปฏิบัติงาน ของผู้ขายออกไปอีกไม่ได้

4.10.5 ให้ผู้ขายปฏิบัติงานในเวลาทำงานปกติของ สป.พม. โดยไม่กระทบต่อการปฏิบัติงานของ สป.พม. ในกรณีมีความประสงค์จะดำเนินงานในวันหยุดประจำสัปดาห์ วันหยุดตามประเพณีนิยม หรือนอกเวลา ทำงานปกติ จะต้องได้รับการอนุญาตจาก ศทส. ก่อน เพื่อ ศทส. จะได้ให้คณะกรรมการตรวจรับพัสดุ และ/หรือผู้ที่ เกี่ยวข้องมาตรวจสอบเฝ้าดูแล และอำนวยความสะดวก หรือรู้เห็นในการดำเนินงานตลอดเวลา และผู้ขายจะต้อง ยินยอมจ่ายค่าล่วงเวลาและค่าใช้จ่ายในการเดินทางให้แก่คณะกรรมการตรวจรับพัสดุ และ/หรือผู้ที่เกี่ยวข้อง

5. การส่งมอบงาน

ผู้ขายต้องจัดหาและส่งมอบครุภัณฑ์คอมพิวเตอร์ อุปกรณ์ เอกสาร คู่มือ ทุกรายการตามที่ปรากฏ ในขอบเขตงาน ให้แล้วเสร็จภายใน 150 วัน นับถัดจากวันลงนามในสัญญา

6. การจ่ายเงิน

สป.พม. จะชำระเงินตามจำนวนที่ระบุไว้ในสัญญาซื้อขาย หลังจากที่ได้ตรวจรับพัสดุ ถูกต้องเรียบร้อยแล้ว และผู้ขายได้ปฏิบัติถูกต้องครบถ้วนตามที่กำหนด

7. การรับประกันความชำรุดบกพร่อง การบำรุงรักษาและซ่อมแซมแก้ไข

7.1 ผู้ขายจะต้องรับประกันความชำรุด บกพร่อง หรือข้อบกพร่องของอุปกรณ์ที่ส่งมอบทั้งหมด เป็นระยะเวลาไม่น้อยกว่าที่ระบุในคุณลักษณะเฉพาะ นับถัดจากวันที่คณะกรรมการตรวจรับพัสดุตรวจรับงานเสร็จเรียบร้อยแล้ว

7.2 ในกรณีอุปกรณ์เกิดชำรุด บกพร่อง หรือใช้งานไม่ได้ โดยความชำรุดนี้มิได้เกิดจากความผิดของ สป.พม. ผู้ขายต้องเริ่มจัดการซ่อมแซมแก้ไขให้อยู่ในสภาพที่ได้ดั่งเดิม โดยไม่คิดค่าใช้จ่ายใดๆ จาก สป.พม.

7.3 ในกรณีที่อุปกรณ์ใช้การไม่ได้ตามปกติ ผู้ขายจะต้องจัดการซ่อมแซมแก้ไขให้อยู่ในสภาพที่ใช้การได้ดั่งเดิม ภายใน 3 วัน นับจากวันที่ได้รับแจ้ง หากเกินกำหนด ผู้ขายต้องนำอุปกรณ์ที่มีประสิทธิภาพเทียบเท่าหรือดีกว่า มาเปลี่ยนแทนชั่วคราวในช่วงเวลาที่ซ่อมอุปกรณ์ โดยไม่คิดค่าใช้จ่ายใดๆ ทั้งสิ้น และภายใน 30 วัน หากไม่สามารถแก้ไขให้ใช้งานได้ดั่งเดิม ผู้ขายจะต้องยินยอมให้ สป.พม. คิดค่าปรับตามสัญญา

8. อัตราค่าปรับ

กรณีผู้ขายไม่สามารถส่งมอบงานได้ตามที่กำหนดในสัญญา ผู้ขายจะต้องจ่ายค่าปรับในอัตราร้อยละ 0.20 ของราคาค่าสิ่งของที่ยังมิได้รับมอบต่อวัน

9. หลักเกณฑ์การพิจารณาคัดเลือกข้อเสนอ

ในการพิจารณาผู้ชนะการยื่นข้อเสนอ สป.พม. จะใช้หลักเกณฑ์การประเมินค่าประสิทธิภาพต่อราคา (Price Performance) โดยพิจารณาให้คะแนนตามปัจจัยและน้ำหนักที่กำหนด โดยจะนำคะแนนข้อเสนอ ด้านราคา และข้อเสนอด้านเทคนิคมารวมกัน เพื่อพิจารณาคัดเลือกผู้ชนะการเสนอราคา ซึ่งผู้ที่ได้รับคะแนนสูงสุดจะเป็นผู้ชนะ หรือได้รับการคัดเลือก ดังนี้

1) ราคาที่ยื่นข้อเสนอ (Price) กำหนดน้ำหนักเท่ากับร้อยละ 60

2) ข้อเสนอทางเทคนิคและข้อเสนออื่นๆ ที่เป็นประโยชน์ต่อทางราชการ กำหนดน้ำหนักเท่ากับ ร้อยละ 40

การพิจารณาเกณฑ์ด้านเทคนิคและข้อเสนออื่นๆ ที่เป็นประโยชน์ต่อทางราชการ โดยพิจารณาจากแนวคิดหรือข้อเสนอที่แสดงให้เห็นว่าผู้รับจ้างมีความเข้าใจตามขอบเขตงานจ้างฯ และสามารถเริ่มงานได้ทันทีที่เริ่มสัญญาจ้าง ทั้งนี้ เพื่อประโยชน์สูงสุดของทางราชการ ซึ่งกำหนดให้มีหัวข้อและกำหนดคะแนนเต็ม 100 คะแนน ดังต่อไปนี้

9.1 การพิจารณาคัดเลือกข้อเสนอที่ครบถ้วนตามขอบเขตงานโดยใช้หลักเกณฑ์การประเมินค่าประสิทธิภาพต่อราคา (Price Performance) ในการพิจารณาผู้ชนะการเสนอราคา โดยมีหลักเกณฑ์ ดังตาราง

ตัวแปร	น้ำหนัก
1. ราคาที่ยื่นข้อเสนอ	60
2. ข้อเสนอทางเทคนิคและข้อเสนออื่นๆ	40
รวมทั้งสิ้น	100

เกณฑ์การให้คะแนน

- ราคาที่ยื่นข้อเสนอ จะถูกพิจารณาให้คะแนนจากระบบการจัดซื้อจัดจ้างภาครัฐตามน้ำหนักคะแนนที่กำหนด
- หลักเกณฑ์การประเมินค่าประสิทธิภาพ แบ่งออกเป็น

รายละเอียดข้อเสนอทางเทคนิคและข้อเสนออื่นๆ	คะแนน
1. มีทีมงาน เจ้าหน้าที่ ที่มีความรู้ ความสามารถในการติดตั้ง ตั้งค่าอุปกรณ์ตามที่เสนอ 20 คะแนน โดยเกณฑ์การให้คะแนนจะแบ่งการให้คะแนนประสบการณ์อยู่ 2 ด้านประกอบด้วย - ประสบการณ์ด้าน Cyber Security พร้อมใบรับรองสากล โดยอ้างอิงตาม พผนวก 2 - ประสบการณ์ด้าน ติดตั้ง ตั้งค่าอุปกรณ์ตามผลิตภัณฑ์ที่เสนอ	
ไม่แนบประวัติ คุณสมบัติ และประสบการณ์ ของบุคลากร	0 คะแนน
มีเจ้าหน้าที่ที่จบปริญญาตรีขึ้นไป ด้านที่เกี่ยวข้องกับคอมพิวเตอร์	5 คะแนน
มีเจ้าหน้าที่ที่จบปริญญาตรีขึ้นไป ด้านที่เกี่ยวข้องกับคอมพิวเตอร์ และมีประสบการณ์ด้าน Cyber Security พร้อมใบรับรองสากลที่สอดคล้องกับประสบการณ์ หรือเทียบเท่า หรือ มีประสบการณ์ด้าน ติดตั้ง ตั้งค่าอุปกรณ์ตามผลิตภัณฑ์ที่เสนอ พร้อมใบรับรองระดับ Professional หรือเทียบเท่า จำนวน 1 คน ขึ้นไป	10 คะแนน
มีเจ้าหน้าที่ที่จบปริญญาตรีขึ้นไปด้านที่เกี่ยวข้องกับคอมพิวเตอร์ และมีประสบการณ์ด้าน Cyber Security พร้อมใบรับรองสากลที่ สอดคล้องกับประสบการณ์ และมีประสบการณ์ ด้าน ติดตั้ง ตั้งค่าอุปกรณ์ตามผลิตภัณฑ์ที่เสนอ พร้อมใบรับรองระดับ Professional หรือเทียบเท่า จำนวน 1 คน ขึ้นไป	15 คะแนน
มีเจ้าหน้าที่ที่จบปริญญาตรีขึ้นไปด้านที่เกี่ยวข้องกับคอมพิวเตอร์ และมีประสบการณ์ด้าน ติดตั้ง ตั้งค่าอุปกรณ์ตามผลิตภัณฑ์ที่เสนอ พร้อมใบรับรองระดับ Expert หรือ Specialist หรือเทียบเท่าจำนวน 1 คน ขึ้นไป	15 คะแนน
มีเจ้าหน้าที่ที่จบปริญญาตรีขึ้นไปด้านที่เกี่ยวข้องกับคอมพิวเตอร์ และมีประสบการณ์ด้าน Cyber Security พร้อมใบรับรองสากล ที่สอดคล้องกับประสบการณ์ และมีประสบการณ์ ด้านติดตั้ง ตั้งค่าอุปกรณ์ตามผลิตภัณฑ์ที่เสนอ พร้อมใบรับรองระดับ Expert หรือ Specialist หรือเทียบเท่า จำนวน 1 คน ขึ้นไป	20 คะแนน

2.มีการออกแบบ Architecture ที่รองรับการทำงานร่วมกัน 20 คะแนน การออกแบบ Architecture ที่รองรับการทำงานร่วมกันระหว่าง SIEM-SOAR-NDR-XDR-EDR พร้อมการทำงานร่วมกับระบบ NGFW และ IPS ของ สป.พม. และนำเสนอการออกแบบสถาปัตยกรรมของระบบตรวจจับ และวิเคราะห์ฯ พร้อมระบุคุณสมบัติของฮาร์ดแวร์ และซอฟต์แวร์ ที่แสดงให้เห็นถึงความเหมาะสมในการจัดการทรัพยากรควบคู่ไปกับการรักษาความมั่นคงปลอดภัย ตั้งแต่การออกแบบระบบ การติดตั้ง และการเฝ้าระวังฯ	
ไม่มีการนำเสนอ	0 คะแนน
มีผังการออกแบบ Architecture ที่รองรับการทำงานร่วมกันระหว่าง SIEM-SOAR-NDR-XDR-EDR พร้อมการทำงานร่วมกับระบบ NGFW และ IPS ของ สป.พม.	10 คะแนน
มีผังการออกแบบ และมีการนำเสนอการออกแบบสถาปัตยกรรมของระบบตรวจจับ และวิเคราะห์ฯ พร้อมระบุคุณสมบัติของฮาร์ดแวร์ และซอฟต์แวร์	15 คะแนน
มีผังการออกแบบ และมีการนำเสนอการออกแบบสถาปัตยกรรมที่แสดงให้เห็นถึงความเหมาะสม ในการจัดการทรัพยากรควบคู่ไปกับการรักษาความมั่นคง ปลอดภัย ตั้งแต่การออกแบบระบบ การติดตั้ง และการเฝ้าระวังฯ	20 คะแนน
3. สถานการณ์ภัยคุกคามที่สามารถตรวจจับจากระบบตรวจจับและวิเคราะห์ ฯ 20 คะแนน การนำเสนอตัวอย่างสถานการณ์ภัยคุกคามที่สามารถตรวจจับจากระบบตรวจจับและวิเคราะห์ฯ อย่างน้อย 3 เหตุการณ์ โดยจะต้องแสดงองค์ประกอบอย่างน้อย ดังนี้ - เกณฑ์ พร้อมแนวทางในการประเมินระดับความรุนแรงของเหตุการณ์ภัยคุกคาม - ขั้นตอนการวิเคราะห์ พร้อมแหล่งข้อมูลเพิ่มเติมที่อาจนำมาใช้ในการวิเคราะห์	
ไม่มีการนำเสนอตัวอย่าง	0 คะแนน
มีการนำเสนอตัวอย่างสถานการณ์ภัยคุกคามที่สามารถตรวจจับจากระบบตรวจจับและวิเคราะห์ ฯ จำนวน 1 เหตุการณ์	5 คะแนน
มีการนำเสนอตัวอย่างสถานการณ์ภัยคุกคามที่สามารถตรวจจับจากระบบตรวจจับและวิเคราะห์ ฯ จำนวน 2 เหตุการณ์	10 คะแนน
มีการนำเสนอตัวอย่างสถานการณ์ภัยคุกคามที่สามารถตรวจจับจากระบบตรวจจับและวิเคราะห์ ฯ จำนวน 3 เหตุการณ์	20 คะแนน

4.การนำเสนอรายงานผลการวิเคราะห์ เหตุการณ์ภัยคุกคามบนระบบตรวจจับและวิเคราะห์ ฯ 20 คะแนน การนำเสนอรายงานผลการวิเคราะห์ เหตุการณ์ภัยคุกคามบนระบบตรวจจับและวิเคราะห์ ฯ อย่างน้อย 1 เหตุการณ์ (Use Case) ซึ่งควรเป็นเหตุการณ์ที่อยู่ในระดับความรุนแรงสูง และมีความซับซ้อน โดยในส่วนของ การวิเคราะห์เหตุการณ์ภัยคุกคาม ต้องจำแนกพฤติกรรมการโจมตีที่สอดคล้องตาม MITRE ATT&CK ได้ และนำเสนอการออกแบบการจัดทำ playbook ของแต่ละอุปกรณ์ให้สามารถเชื่อมโยงการทำงานได้อย่างมีประสิทธิภาพ แสดงเป็น Flow chart แสดงขั้นตอนการทำงานของอุปกรณ์ที่เกี่ยวข้อง	
ไม่มีการนำเสนอ	0 คะแนน
นำเสนอรายงานผลการวิเคราะห์ เหตุการณ์ภัยคุกคามบนระบบตรวจจับและวิเคราะห์ ฯ	5 คะแนน
นำเสนอรายงานผลการวิเคราะห์ เหตุการณ์ภัยคุกคามบนระบบตรวจจับและวิเคราะห์ ฯ และจำแนกพฤติกรรมการโจมตีที่สอดคล้องตาม MITRE ATT&CK	10 คะแนน
นำเสนอรายงานผลการวิเคราะห์ เหตุการณ์ภัยคุกคามบนระบบตรวจจับและวิเคราะห์ ฯ และจำแนกพฤติกรรมการโจมตีที่สอดคล้องตาม MITRE ATT&CK และนำเสนอการออกแบบการจัดทำ playbook	15 คะแนน
นำเสนอรายงานผลการวิเคราะห์ เหตุการณ์ภัยคุกคามบนระบบตรวจจับและวิเคราะห์ ฯ และจำแนกพฤติกรรมการโจมตีที่สอดคล้องตาม MITRE ATT&CK และนำเสนอการออกแบบการจัดทำ playbook โดยมี Flow chart แสดงขั้นตอนการทำงานของอุปกรณ์ที่เกี่ยวข้อง	20 คะแนน
5. การนำเสนอหน้าจอ Dashboard ที่ออกแบบมาเพื่อการ ตรวจจับภัยคุกคามในลักษณะต่างๆ 10 คะแนน	
ไม่มีการนำเสนอ	0 คะแนน
มีการนำเสนอหน้าจอ Dashboard จำนวน 1 แบบ	5 คะแนน
มีการนำเสนอหน้าจอ Dashboard จำนวน 2 แบบ ขึ้นไป	10 คะแนน
6.ความสามารถของซอฟต์แวร์และแพลตฟอร์มการจัดการความเสี่ยงของช่องโหว่ 10 คะแนน เป็นผลิตภัณฑ์ที่อยู่ในระดับ/กลุ่ม Strong Performers หรือดีกว่า ของ The Forrester Wave ด้าน Vulnerability Risk Management ปี 2025	
เป็นผลิตภัณฑ์ที่อยู่ในระดับ Contenders	0 คะแนน
เป็นผลิตภัณฑ์ที่อยู่ในระดับ Strong Performers	5 คะแนน
เป็นผลิตภัณฑ์ที่อยู่ในระดับ Leaders	10 คะแนน

9.2 ผู้เสนอราคาต้องจัดทำข้อเสนอด้านราคาเป็นเงินบาท และต้องสอดคล้องกับข้อเสนอด้านเทคนิค ทั้งนี้ ราคาที่เสนอต้องรวมภาษีมูลค่าเพิ่ม ภาษีอากรอื่นๆ และค่าใช้จ่ายทั้งปวงไว้แล้ว และต้องเสนอราคา ค่าใช้จ่ายต่างๆ ที่จำเป็น อนึ่งหากผู้เสนอราคาไม่ได้รับการพิจารณา จะเรียกร้องค่าเสียหายใดๆ จาก สป.พม. ไม่ได้

10. วงเงินในการจัดซื้อ

ภายในวงเงินงบประมาณ 40,000,000 บาท (สี่สิบล้านบาทถ้วน) ซึ่งเป็นราคาที่รวมค่าครุภัณฑ์คอมพิวเตอร์ และอุปกรณ์ทุกรายการที่กำหนด ค่าดำเนินการ และค่าภาษีมูลค่าเพิ่มไว้ด้วยแล้ว

11. การรักษาความลับ

11.1 ผู้ขายจะต้องจัดเก็บรักษาข้อมูลต่าง ๆ ที่เกี่ยวกับการดำเนินงานที่ผู้ขายได้รับจาก สป.พม. และข้อมูลต่างๆ ที่ผู้ขายได้จัดทำขึ้นเนื่องจากการดำเนินงานตามสัญญาถือเป็นความลับของ สป.พม. ซึ่งต่อไปในสัญญานี้เรียกว่า “ข้อมูลที่เป็นความลับ” โดยผู้ขายต้องห้ามมาตรการในการจัดเก็บข้อมูลที่เป็นความลับให้มิได้ขจัดรวมทั้งไม่เปิดเผย หรือเผยแพร่ หรือกระทำการด้วยวิธีการใดให้บุคคลอื่นใดที่มีใช้คู่สัญญาภายใต้สัญญานี้ หรือมิใช่บุคคลที่ สป.พม. ได้อนุญาตเป็นลายลักษณ์อักษรให้มีส่วนเกี่ยวข้องที่จะรับทราบข้อมูลที่เป็นความลับภายใต้สัญญานี้ ได้ทราบถึงข้อมูลที่เป็นความลับดังกล่าว เว้นแต่จะเป็นการเปิดเผยข้อมูลดังกล่าวให้แก่เจ้าหน้าที่ผู้ปฏิบัติงานของ ผู้ขายที่ต้องเกี่ยวข้องโดยตรงกับข้อมูลดังกล่าวเท่านั้น และผู้ขายจะต้องจัดให้เจ้าหน้าที่ผู้ปฏิบัติงานดังกล่าวได้ ผูกพันและปฏิบัติตามเงื่อนไขในการรักษาข้อมูลที่เป็นความลับเช่นว่านั้นด้วย

11.2 หากผู้ขายมิได้ปฏิบัติตามข้อ 11.1 ผู้ขายจะต้องรับผิดชอบต่อ สป.พม. หรือบุคคลอื่นที่เป็นเจ้าของข้อมูลที่เป็นความลับนั้นในความเสียหายใดๆ ที่เกิดขึ้นเนื่องจากการที่ข้อมูลที่เป็นความลับดังกล่าวได้ถูกเปิดเผย ไม่ว่าทั้งหมดหรือแต่บางส่วน และ สป.พม. มีสิทธิบอกเลิกสัญญาได้ทันที

11.3 ผู้ขายจะยังคงต้องผูกพันตามข้อกำหนดเกี่ยวกับการรักษาข้อมูลที่เป็นความลับตามข้อ 11.1 ต่อไป ตราบที่ข้อมูลที่เป็นความลับดังกล่าวยังคงเป็นความลับอยู่ แม้ว่าการซื้อขายตามสัญญานี้ได้สิ้นสุดลงแล้ว ไม่ว่าด้วยเหตุใดก็ตาม

สถานที่ติดต่อเพื่อทราบข้อมูลเพิ่มเติม

สถานที่ติดต่อ สำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์

1034 ถนนกรุงเกษม แขวงคลองมอหานาค

เขตป้อมปราบศัตรูพ่าย กรุงเทพฯ 10100

โทรศัพท์ 0 2659 6506 โทรสาร 0 2659 6511

e-Mail: pc-treasury.cad@m-society.go.th

ผนวก 1

ตารางที่ 1 : ประวัติ คุณสมบัติ และประสบการณ์ ของบุคลากร

ประวัติ คุณสมบัติ และประสบการณ์ ของบุคลากร

ชื่อ - สกุล
 สัญชาติ ที่อยู่
 อาชีพ ตำแหน่งปัจจุบัน
 จำนวนปีที่ทำงาน

ตำแหน่งและหน้าที่ความรับผิดชอบที่ได้รับในโครงการ

ตำแหน่ง	หน้าที่ความรับผิดชอบ

ประวัติการศึกษา

ตั้งแต่ - ถึง	ชื่อสถานศึกษา/ประเทศ	วุฒิการศึกษา	วิชาเอก

ประวัติการทำงาน

ตั้งแต่ - ถึง	ชื่อหน่วยงาน/ประเทศ	ตำแหน่ง	ขอบเขตและหน้าที่ความรับผิดชอบ

ประวัติการฝึกอบรม ดูงาน ฝึกงาน ผลงาน

ตั้งแต่ - ถึง	ชื่อสถานศึกษา/ชื่อ หน่วยงาน/ประเทศ	ชื่อหลักสูตร/ ชื่อผลงาน	ขอบเขต/ รายละเอียด	ประโยชน์และการ นำไปใช้งาน

ใบรับรอง (Certificate)

--

ข้าพเจ้าขอรับรองว่ารายละเอียดตามรายการข้างต้นเป็นความจริงทุกประการ และยินยอมให้สำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ตรวจสอบข้อมูล ตลอดจนใช้ข้อมูลดังกล่าวในการใดๆ อันเกี่ยวกับการจ้างพัฒนาระบบงานของสำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ตรวจสอบได้

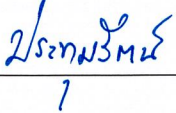
ลงชื่อเจ้าของประวัติ.....
 (.....)

ลงชื่อ.....
 ประทับตรา (.....)
 (ถ้ามี) ตำแหน่ง.....
 บริษัท.....
 ผู้ยื่นข้อเสนอ
 วันที่.....

หน้าที่ 25

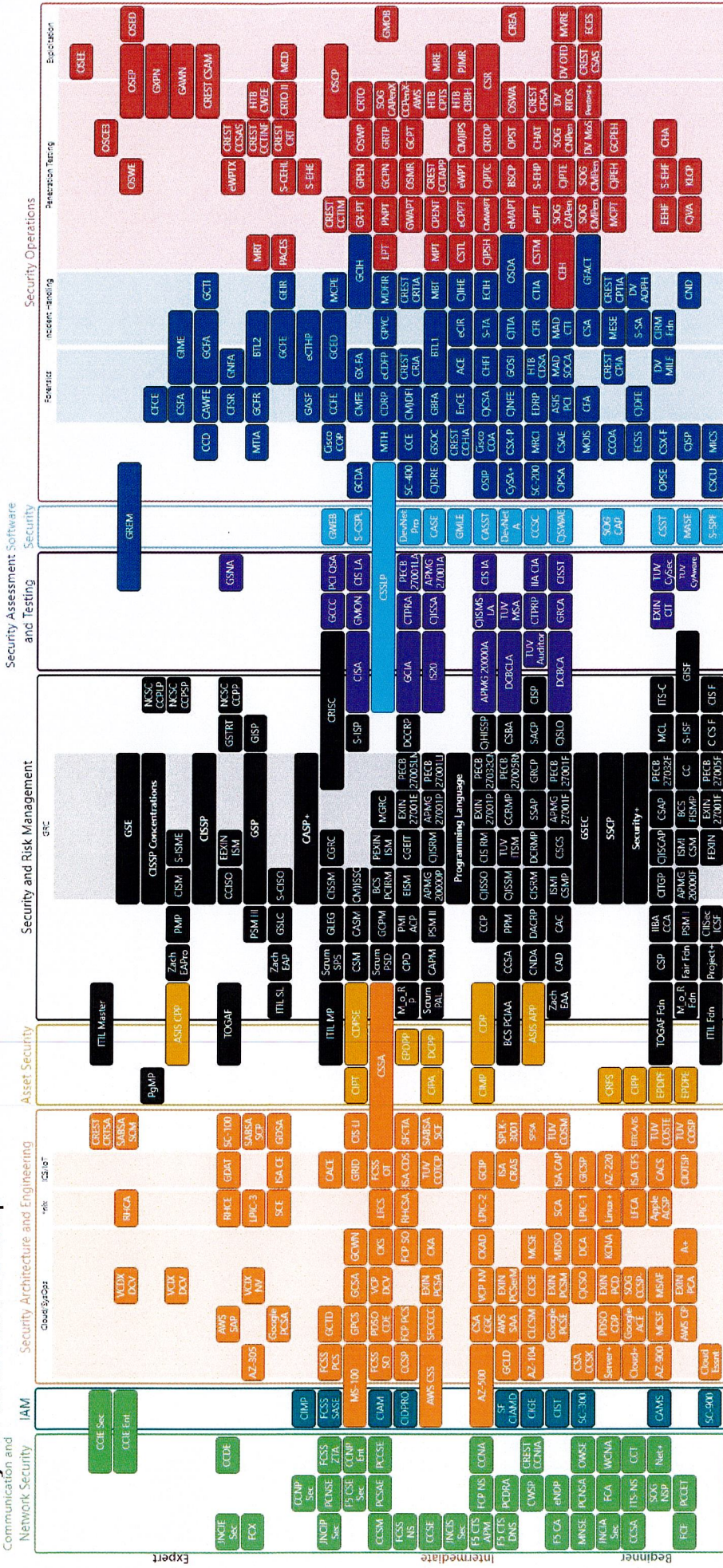
ประธานกรรมการ 

กรรมการ 

กรรมการ 
 1

Security Certification Roadmap

แผนก 2



481 certifications listed | July 2024

รูปแสดงการเปรียบเทียบ Security Certification
อ้างอิงจาก <https://pauljerimy.com/security-certification-roadmap/>

ประธานกรรมการ กรรมการ กรรมการ