ขอบเขตงาน (Term of Reference : TOR)
ระบบป้องกันการโจมตีเครือข่ายคอมพิวเตอร์ของ สป.อว.

1. หลักการและเหตุผล

ด้วย กองระบบและบริหารข้อมูลเชิงยุทธศาสตร์ อววน. (กรข.) สำนักงานปลัดกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม (สป.อว.) ได้ดำเนินการบริหารจัดการระบบเทคโนโลยีสารสนเทศของ สป.อว. ในส่วนของการพัฒนาระบบโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ เพื่อรองรับการปฏิบัติงานและประสานแลกเปลี่ยนข้อมูลผ่านระบบเครือข่ายคอมพิวเตอร์ทั้งภายในและภายนอกองค์กร ตามนโยบายและยุทธศาสตร์ด้านเทคโนโลยีสารสนเทศและการสื่อสารของประเทศ ให้สามารถใช้งานได้ตลอดเวลา และมีความมั่นคงปลอดภัยในการใช้งาน นั้น

ปัจจุบันภัยคุกคามด้านเทคโนโลยีสารสนเทศมีแนวโน้มทวีความรุนแรงและสร้างความเสียหายมากขึ้นเรื่อย ๆ ประกอบกับเทคนิคการโจมตีที่ซับซ้อนมากกว่าในอดีต กรข. จำเป็นต้องติดตาม เฝ้าระวัง และลดความเสี่ยงจากภัยคุกคามที่อาจเกิดขึ้น เพื่อที่จะได้แก้ไขและเตรียมความพร้อมให้ระบบสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่อง ลดปัญหาที่จะทำให้ระบบหยุดชะงัก โดยเฉพาะอย่างยิ่งระบบสารสนเทศที่มีความสำคัญในการบริหารจัดการและปฏิบัติงานด้านต่าง ๆ ที่ให้บริการแก่บุคลากร สป.อว.

ทั้งนี้ กรข. จำเป็นต้องพัฒนาและปรับปรุงโซลูชันด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อที่จะให้ระบบตรวจสอบ วิเคราะห์รูปแบบของภัยคุกคาม รวมถึงแจ้งเตือนและมีกระบวนการรองรับเหตุการณ์หรือภัยคุกคามอย่างทันท่วงที เพื่อเป็นการลดความเสี่ยงที่อาจเกิดขึ้นกับระบบสารสนเทศและเครือข่ายของ สป.อว. และสามารถใช้งานระบบสารสนเทศได้อย่างมั่นคงปลอดภัย และตอบสนองการดำเนินกิจกรรมในการพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS) ขององค์กรตามมาตรฐาน ISO/IEC 27001 ให้มีประสิทธิภาพยิ่งขึ้น

2. วัตถุประสงค์

2.1. เพื่อให้ระบบสารสนเทศภายใน สป.อว. มีความมั่นคงปลอดภัยจากการถูกโจมตีจากภัยคุกคามไซเบอร์ที่มากขึ้นในปัจจุบัน และเพิ่มขีดความสามารถในการป้องกันภัยคุกคามไซเบอร์ให้สามารถทำการป้องกันได้อย่างรวดเร็วและทันท่วงที

2.2. เพื่อเป็นการสร้างความเชื่อมั่นด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศและเครือข่ายองค์กร

2.3. เพื่อตอบสนองต่อการดำเนินการกิจกรรมในการพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System: ISMS) ตามมาตรฐาน ISO/IEC 27001

3. คุณสมบัติของผู้เสนอราคา

3.1. มีความสามารถตามกฎหมาย

3.2. ไม่เป็นบุคคลล้มละลาย

3.3. ไม่อยู่ระหว่างเลิกกิจการ

3.4. ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

3.5. ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

3.6. มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

3.7. เป็นนิติบุคคล ผู้มีอาชีพรับจ้างงานที่ประกวดราคาอิเล็กทรอนิกส์ดังกล่าว

3.8. ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่ สำนักงานปลัดกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

3.9. ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่ รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละสิทธิ์และความคุ้มกันเช่นว่านั้น

3.10. ผู้ยื่นข้อเสนอต้องลงทะเบียนในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (Electronic Government Procurement : e- GP) ของกรมบัญชีกลาง

3.11. ผู้ยื่นข้อเสนอต้องมีประสบการณ์หรือผลงานรับจ้างด้านการจัดทำระบบความมั่นคงปลอดภัยไซเบอร์ หรือให้บริการรักษาความปลอดภัยระบบเครือข่ายสารสนเทศต่าง ๆ หรือ งานที่เกี่ยวข้องกับระบบความมั่นคงปลอดภัย อย่างน้อย 1 โครงการ มูลค่าอย่างน้อย 5,000,000 บาท ภายในระยะเวลาไม่เกิน 2 ปีนับจนถึงวันที่ยื่นซองประกวดราคา และเป็นผลงานที่เป็นคู่สัญญาโดยตรงกับหน่วยงานราชการ รัฐวิสาหกิจ เอกชนที่เชื่อถือได้ หน่วยงานตามกฎหมายว่าด้วยระเบียบบริหารราชการส่วนท้องถิ่น รัฐวิสาหกิจ หรือเอกชน ทั้งนี้ ผู้ยื่นข้อเสนอต้องแนบสำเนาสัญญาหรือหนังสือรับรองผลงานและในกรณีที่ผลงานดังกล่าวเป็นการรับจ้างทำงานให้ผู้ว่าจ้างซึ่งเป็นเอกชนให้แนบสำเนาสัญญาด้วย

4. **ข้อกำหนดทั่วไป**

4.1. การยื่นข้อเสนอทางเทคนิค ให้ผู้ยื่นข้อเสนอยื่นรายการอุปกรณ์ และโปรแกรมที่นำเสนออย่างละเอียด โดยต้องระบุชื่อผลิตภัณฑ์, รุ่น และจำนวนชิ้นส่วนแต่ละรายการให้ครบถ้วนพร้อมทำรายละเอียดคุณลักษณะเฉพาะแยกตามรายการอุปกรณ์และโปรแกรมที่นำเสนอ โดยต้องแนบเอกสารแคตตาล็อก (Catalogue) หรือเอกสารรายละเอียดของอุปกรณ์และโปรแกรมที่นำเสนอทุกรายการในรูปแบบตารางเปรียบเทียบ (Compliance table)

4.2. การส่งมอบอุปกรณ์ กรณีที่ในช่วงเวลาของการส่งมอบ มีสินค้ารุ่นใหม่หรือเทียบเท่า หรือดีกว่าผู้ยื่นข้อเสนอสามารถจัดส่งอุปกรณ์ หรือโปรแกรมในรุ่นที่เทียบเท่า หรือดีกว่า โดยจัดทำเป็นหนังสือแจ้งให้ทาง สป.อว. พิจารณาให้ความเห็นชอบก่อน

4.3. ผู้ยื่นข้อเสนอต้องได้รับการสนับสนุนทางเทคนิคจากบริษัทเจ้าของผลิตภัณฑ์ หรือจากบริษัทสาขาประเทศไทยของเจ้าของผลิตภัณฑ์ที่นำเสนอในโครงการนี้ โดยแสดงเอกสารรับรองประกอบการยื่นข้อเสนอ

4.4. ผู้ยื่นข้อเสนอต้องมีวิศวกรที่ได้รับ Professional Certified ที่ยังคงสถานะ Active และไม่หมดอายุ จำนวนไม่น้อยกว่า 1 คน โดยแนบสำเนาเอกสารใบรับรองดังกล่าวในวันยื่นข้อเสนอด้วย ดังรายละเอียดต่อไปนี้

4.4.1. CompTIA Secure Infrastructure Expert (CSIE)

4.4.2. Certified Information Security Professional (CISSP)

4.4.3. Certified Ethical Hacker (CEH)

4.4.4. Certified Data Privacy Solutions Engineer (CDPSE)

4.4.5. ITIL4 - IT Service Management

4.5. ผู้ยื่นข้อเสนอต้องเป็นผู้ให้บริการการบริหารจัดการระบบความปลอดภัยสารสนเทศที่มีศูนย์ปฏิบัติการเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cybersecurity Operations Center: CSOC) ตั้งอยู่ในประเทศไทย

4.6. ผู้ยื่นข้อเสนอต้องมีศูนย์ปฏิบัติการฯ Cybersecurity Operations Center (CSOC) มีความพร้อมในการให้บริการเฝ้าระวังและแจ้งเตือนเหตุการณ์ภัยคุกคามตลอด 7 วัน 24 ชั่วโมง (7 x 24)

4.7. ผู้ยื่นข้อเสนอต้องมี Disaster Recovery Site (DR Site) ที่ทำหน้าที่เป็นศูนย์สำรอง ในกรณีที่ศูนย์หลักของผู้ให้บริการไม่สามารถให้บริการได้ หรือ ระบบการเฝ้าระวังของผู้ให้บริการไม่สามารถให้บริการได้

5. **รายละเอียดคุณลักษณะเฉพาะด้านเทคนิค**

5.1. **ซอฟต์แวร์ป้องกันและควบคุมการใช้งานโปรแกรมของเครื่องปลายทาง (Endpoint Protection) จำนวน 500 Licenses โดยมีคุณลักษณะอย่างน้อยดังต่อไปนี้**

5.1.1. เป็นซอฟต์แวร์ประเภท Next-Generation Antivirus และสามารถทำ Endpoint Detection & Response Solutions (EDR) ได้ใน Agent เดียว

5.1.2. เป็นผลิตภัณฑ์ที่อยู่ในกลุ่ม Leader Gartner Magic Quadrant ด้าน Endpoint Protection Platforms ปี 2023 และต้องเป็นผลิตภัณฑ์ที่อยู่ในกลุ่ม Leader The Forrester Wave ด้าน Threat Intelligence Services ปี 2023

5.1.3. ซอฟต์แวร์ (agent) ที่ติดตั้งใน Windows, Windows Server, Linux และ MacOS จะต้องเป็นผลิตภัณฑ์ที่มีเครื่องหมายการค้าเดียวกันในทุกระบบปฏิบัติการที่ติดตั้ง

5.1.4. มีระบบบริหารจัดการอยู่แบบ Cloud management (SaaS) และการเชื่อมต่อระหว่าง Agent กับ Cloud management ต้องมีการเข้ารหัสแบบ TLS-encrypted เพื่อความปลอดภัย

5.1.5. สามารถตรวจจับ Malware โดยไม่อาศัย signature และไม่ต้องทำการ update signature บนเครื่องลูกข่าย

5.1.6. สามารถป้องกัน Malware และ การโจมตีที่ไม่เกิดจากมัลแวร์ (Malware-free attack) ด้วยเทคโนโลยี Machine learning และ Indicator of Attack (IOA) ได้เป็นอย่างน้อย

5.1.7. สามารถป้องกัน Known and Unknown malware, Adware และ potentially unwanted programs (PUPs) ด้วยเทคโนโลยี Machine learning

5.1.8. สามารถทำการตัดการเชื่อมต่อระบบเครือข่าย (Network Containment) ของเครื่องคอมพิวเตอร์ที่มีการติดตั้ง Agent ผ่านระบบบริหารจัดการส่วนกลาง (Centralize Management)

5.1.9. สามารถติดตั้งซอฟต์แวร์ป้องกันการโจมตีของเครื่องคอมพิวเตอร์ลูกข่ายผ่านทาง Active Directory (AD) ได้สำหรับเครื่องคอมพิวเตอร์ที่ทำงานบนระบบปฏิบัติการ Windows

5.1.10. สามารถนำข้อมูลการแจ้งเตือนภัยคุกคาม (Alerts) มาแปลงให้อยู่ในรูปแบบ MITRE ATT&CK framework เพื่อง่ายต่อการทำความเข้าใจ

5.1.11. สามารถป้องกันผู้ใช้งานที่ไม่มีสิทธิ์หรือมัลแวร์ที่พยายามถอนการติดตั้ง Agent หรือ Disable Agent ของเครื่องคอมพิวเตอร์ลูกข่ายได้

5.1.12. สามารถแสดงผลของภัยคุกคามที่เกิดขึ้นออกมาเป็นรูปภาพ Process Tree, Process Table และ Process Activity ได้

5.1.13. มี Dashboard ที่ Monitor Incidents ของบริการค้นหาภัยคุกคามเชิงรุก (Threat Hunting service) อย่างน้อยดังนี้

1) Total hunting leads requiring investigation
2) Hunting leads by host type
3) Hunting leads by resolution

5.1.14. สามารถสร้าง custom hash เพื่อทำการ Detect, Blocklist และ Allow list ได้

5.1.15. สามารถกำหนดการแจ้งเตือนตาม Priority Score ได้เป็นอย่างน้อย

5.1.16. สามารถเชื่อมต่อกับไปยังเครื่องปลายทาง (Real Time Response) เพื่อทำการ run command ต่างๆ ได้อย่างน้อยดังนี้

1) List running processes and kill processes
2) Show network connections
3) Navigate the file system, get or delete files
4) Upload files
5) Remotely restart or shut down a host
6) Manage and run custom scripts or executables (powershell, zsh, bash)

5.1.17. สามารถเปิดการทำงานในรูปแบบ Endpoint Detection and Response (EDR) เพื่อเก็บข้อมูลการใช้งาน (Activity) ของเครื่อง Endpoint ต่างๆ และนำมาวิเคราะห์หาภัยคุกคามแบบ Realtime ได้

5.1.18. สามารถป้องกันการ Exploit ไปยังช่องโหว่ (Vulnerability) เพื่อป้องกันการยึดเครื่อง (Compromised) ได้อย่างน้อยดังนี้

1) Forced Address Space Layout Randomization
2) Forced Data Execution Protection
3) Null Page Allocation
4) Heap Spray Preallocation
5) SEH Overwrite Protection

5.1.19. สามารถป้องกัน Ransomware ในรูปแบบต่างๆ ได้อย่างน้อยดังนี้

1) ป้องกันการลบ volume shadow copy
2) ป้องกันการเข้ารหัสไฟล์ (File Encryption)
3) ป้องกันไม่ให้ ransomware เข้าไป Access File System
4) ป้องกันการลบ Volume Shadow Copy
5) ป้องกัน ransomware ประเภท Cryptowall
6) ป้องกัน ransomware ประเภท Locky

5.1.20. สามารถป้องกันการทำงานของ Registry ที่มีพฤติกรรมที่ต้องสงสัยได้ (Suspicious Registry Operations)

5.1.21. สามารถเก็บข้อมูลภายในระบบปฏิบัติการ (kernel-mode) ได้ไม่น้อยกว่า 400 Raw events เพื่อนำมาย้อนรอยภัยคุกคามที่เกิดขึ้น (Incident)

5.1.22. สามารถสร้าง custom IOA เพื่อตรวจจับพฤติกรรมที่ผิดปกติ (Malicious behaviors) หรือต้องการตรวจจับพฤติกรรมการทำงานที่องค์กรต้องการเฝ้าระวังได้อย่างน้อยดังนี้

1) Process Creation
2) File Creation
3) Network Connection (IPv4, IPv6)
4) Domain Name

5.1.23. สามารถค้นหาข้อมูลการใช้งานภายในที่เกี่ยวข้อง (Host Search) ได้อย่างน้อยดังนี้

1) Host info
2) External network connections
3) Map of external network connections
4) Detection history
5) Local and External Ips
6) User Logon Activities
7) Unique Executables Written
8) Unique Injected Threads
9) Unique DLL Injections
10) Java injected Threads
11) Command History

5.1.24. สามารถค้นหาข้อมูลการใช้งาน Hash (Hash Search) ได้อย่างน้อยดังนี้

1) PE file info
2) Detect History
3) Unresolved Detects
4) Process Executions

5.1.25. สามารถค้นหาข้อมูลการใช้งาน Username (User Search) ได้อย่างน้อยดังนี้

1) User Logon Activities
2) Detect History
3) Unresolved Detects
4) Process Executions
5) Admin tool usage

5.1.26. โปรแกรมที่ติดตั้งในเครื่อง Endpoint ต้องใช้งาน CPU ไม่เกิน 5% และต้องสามารถติดตั้งใช้งานได้เต็มประสิทธิภาพโดยไม่มีความจำเป็นต้อง reboot (no reboot)

5.1.27. สามารถทำการยืนยันตัวตนกับระบบ 2 Factor Authentication ได้ หรือดีกว่า

5.1.28. สามารถ Upgrade Machine learning และ Indicator of Attack (IOA) โดยแยกจากการ Update patch ของ Operating System เพื่อให้สามารถทำการ Update ได้อย่างอิสระและไม่จำเป็นต้อง reboot (no reboot)

5.1.29. สามารถกำหนด Policy ตามกลุ่มของเครื่อง (Host Groups) ได้

5.1.30. มีบริการในการค้นหาภัยคุกคามเชิงรุก (Threat Hunting service) โดยผู้เชี่ยวชาญ (Human Analysis) แบบ 24/7 ครอบคลุมทุกเครื่องคอมพิวเตอร์ที่ติดตั้ง Agent Software โดยจะต้องเป็นบริการจากบริษัทที่มีเครื่องหมายการค้าเดียวกันโปรแกรมที่นำเสนอ เพื่อให้มีประสิทธิภาพในการรับมือภัยคุกคาม

5.1.31. มีบริการแจ้งเตือน Incident จากผู้เชี่ยวชาญด้านการทำ Threat hunting โดยการแจ้งเตือน Incident ที่ตรวจพบผ่านทาง email notification เป็นอย่างน้อย

5.1.32. มีระยะเวลาการรับประกันและลิขสิทธิ์การใช้งานไม่น้อยกว่า 2 ปี

5.2. **ระบบตรวจจับและตอบสนองภัยคุกคามบนระบบเครือข่ายคอมพิวเตอร์ (Network Detection and Response) จำนวน 1 ระบบ มีคุณลักษณะอย่างน้อยดังต่อไปนี้**

5.2.1. เป็นอุปกรณ์แบบ Hardware Appliance ที่สามารถติดตั้งในตู้ Rack แบบ 19 นิ้ว ได้ โดยมีคุณลักษณะอย่างน้อยดังนี้

1) Admin interface แบบ 1000 BASE-T จำนวนอย่างน้อย 1 พอร์ต
2) Remote management interface แบบ 1000 BASE-T จำนวนอย่างน้อย 1 พอร์ต
3) Copper analysis interface แบบ 1000 BASE-T จำนวนอย่างน้อย 3 พอร์ต พร้อมอุปกรณ์หรือโมดูลเพิ่มเติมให้สามารถทำงานร่วมกับอุปกรณ์กระจายสัญญาณเดิมของ สป.อว. ได้
4) Fiber analysis interface แบบ 10Gbe/1Gbe SFP+ จำนวนอย่างน้อย 2 พอร์ต พร้อมอุปกรณ์หรือโมดูลเพิ่มเติมให้สามารถทำงานร่วมกับอุปกรณ์กระจายสัญญาณเดิมของ สป.อว. ได้
5) Power Supply แบบ Dual

5.2.2. สามารถรองรับ Throughput ได้ไม่น้อยกว่า 3 Gbps

5.2.3. สามารถรองรับปริมาณข้อมูลได้ไม่น้อยกว่า 200,000 connections per minute และไม่น้อยกว่า 400,000 events per minute

5.2.4. สามารถรองรับการประมวลผลข้อมูลได้อย่างน้อย 2,500 devices

5.2.5. รองรับการขยายระบบในลักษณะ Distributed architecture ซึ่งข้อมูลจากต้นทาง สามารถถูกรวบรวม วิเคราะห์ และประมวลผลแบบ Local ที่ต้นทาง และทำการส่งข้อมูลเฉพาะ metadata มายังส่วนกลาง โดยต้องมีการเชื่อมต่อมายังส่วนกลางแบบ SSL encryption

5.2.6. มีระบบบริหารจัดการจากส่วนกลาง ที่สามารถแสดงผลในรูปแบบรายงาน (Reporting) และ Dashboard โดยมีหน้า System status แสดงผลข้อมูลแบบละเอียดของ System health เช่น Hardware utilization metrics, Throughput, Software bundle versions, Component health และ modeled devices.

5.2.7. สามารถตรวจจับภัยคุกคามด้วยการวิเคราะห์ข้อมูล Network Traffic ผ่านทาง Mirror port หรือ SPAN หรือ Network TAP โดยไม่จำเป็นต้องติดตั้ง Agent ใดๆ บนเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่าย

5.2.8. มีเทคโนโลยี Self-Learning AI และ Unsupervised machine learning ที่สามารถเรียนรู้และปรับตัวอย่างต่อเนื่อง เพื่อปกป้องภัยคุกคามไซเบอร์ประเภท Unknown และ Unpredictable โดยไม่ต้องอาศัยการเขียนกฎล่วงหน้า (pre-defined rule)

5.2.9. มี API สำหรับเข้าถึงข้อมูลหรือเชื่อมต่อทำงานร่วมกับระบบอื่นๆ ได้ ตลอดจนรองรับการเชื่อมต่อผ่าน TAXII servers และ import STIX XML files

5.2.10. สามารถค้นหาอุปกรณ์ ด้วยวิธีดังต่อไปนี้ ได้เป็นอย่างน้อย

1) Hostname
2) IP address
3) MAC address
4) Username of user logged into that device.

5.2.11. มีระบบการค้นหาขั้นสูง (Advance Search) ที่สามารถค้นหา metadata log แบบละเอียดจากการวิเคราะห์ข้อมูล network traffic และ event log พร้อมกับสามารถสร้าง complex query syntax เพิ่มเติมได้

5.2.12. สามารถทำ packet capture จาก connection ที่รวบรวม เพื่อทำการตรวจสอบเพิ่มเติมต่อไปได้

5.2.13. สามารถกำหนด watched domain เช่น part of a DNS request หรือ HTTP activity ได้ และสามารถแจ้งเตือนกรณี watched domain นั้นถูกตรวจจับได้

5.2.14. สามารถกำหนด Tags ให้กับ network devices, credentials หรือ SaaS users เพื่อใช้สำหรับระบุแหล่งข้อมูลที่สำคัญ และง่ายต่อการควบคุมการทำงาน

5.2.15. สามารถสร้างรายงาน (Report) เพื่อนำเสนอภาพรวม coverage ของระบบเครือข่ายและ user engagement

5.2.16. สามารถแสดงข้อมูลการตรวจจับและป้องกันภัยคุกคามตาม Timeline นับตั้งแต่จุดเริ่มต้นจนถึงจุดสิ้นสุดในหน้าจอเดียวกัน

5.2.17. มี Mobile application เพื่อได้รับการแจ้งเตือน (Alert) อย่างทันท่วงที โดยสามารถดาวน์โหลด Mobile application ได้จาก App Store และ Google Play Store.

5.2.18. รองรับการแสดงรายการช่องโหว่ของระบบปฏิบัติการ (Vulnerability Assessment) และ Inventory ต่างๆ ของเครื่อง โดยครอบคลุมระบบปฏิบัติการ Windows และ Linux

5.2.19. สามารถแสดงข้อมูลเหตุการณ์ภัยคุกคามทางไซเบอร์ โดยให้คะแนน (Scoring) ของภัยคุกคามเมื่อเกิดขึ้นกับ IP address, Host และ Username ที่มีความสำคัญสูง ได้เป็นอย่างน้อย

5.2.20. สามารถแสดงข้อมูลเหตุการณ์ภัยคุกคามทางไซเบอร์ที่ตรวจพบ โดยเทียบเคียงกับ MITRE ATT&CK และ NIST CSF ได้

5.2.21. รองรับการตอบสนองต่อภัยคุกคาม (Response) โดยสามารถทำงานร่วมกับ Firewall ของ สป.อว. และซอฟต์แวร์ป้องกันและควบคุมการใช้งานโปรแกรมของเครื่องปลายทาง (Endpoint Protection) ในรายการที่ 1 ได้เป็นอย่างน้อย

5.2.22. เป็นผลิตภัณฑ์ที่อยู่ในกลุ่ม Leader ประเภท Innovation/Platform Play ของ GigaOm Radar for Network Detection and Response (NDR) ปี 2023

5.2.23. มีระยะเวลาการรับประกันและลิขสิทธิ์การใช้งานได้ไม่น้อยกว่า 3 ปี

5.3. **ระบบบันทึกข้อมูลเพื่อการวิเคราะห์ และรักษาความปลอดภัยระบบคอมพิวเตอร์ (SIEM) จำนวน 1 ระบบ มีคุณลักษณะอย่างน้อยดังต่อไปนี้**

5.3.1. เป็นผลิตภัณฑ์ที่ถูกจัดอันดับให้อยู่ในกลุ่ม Leader จากการจัดอันดับของ Gartner Magic Quadrant for SIEM (Security Information and Event Management) สำหรับปี 2023 หรือล่าสุด

5.3.2. สามารถรับข้อมูลจราจร (log) หรือเหตุการณ์ด้านความปลอดภัย (event) สำหรับทำงานด้าน SIEM จำนวนไม่น้อยกว่า 2,000 EPS (Event per Second) หรือไม่น้อยกว่า 50 GB/day

5.3.3. รองรับลิขสิทธิ์การใช้งานแบบ Perpetual

5.3.4. มีฟีเจอร์หรือฟังก์ชัน Threat Intelligence ภายใต้เครื่องหมายการค้าเดียวกันกับระบบ SIEM

5.3.5. มีฟีเจอร์หรือฟังก์ชันสำหรับการรับ Threat Intelligence Feed ได้จากหลายแหล่ง

5.3.6. สามารถจัดเก็บและประมวลผล Log หรือ Event จากระบบและอุปกรณ์ต่าง ๆ เช่น Firewall, Network Devices, ระบบปฏิบัติการและระบบฐานข้อมูล ได้เป็นอย่างน้อย

5.3.7. รองรับการติดตั้ง (Installation) แบบ Appliance หรือ Virtual Appliance ได้

5.3.8. สามารถทำงานได้ในลักษณะ All-In-One หรือ Distributed ได้

5.3.9. รองรับการทำงานผ่านระบบเครือข่ายด้วย IPv4 และ IPv6 ได้

5.3.10. สามารถเพิ่ม Log Source ได้ทั้งแบบ Manual และ Automatic ด้วยวิธีการค้นหาอุปกรณ์ต้นทาง

5.3.11. รองรับการเก็บข้อมูลของ Network flow ในรูปแบบ Net flow, J-Flow, S-Flow ได้เป็นอย่างน้อย

5.3.12. สามารถรับและดึงข้อมูล Log จากอุปกรณ์ต่าง ๆ (Log Source) ในรูปแบบดังนี้ได้เป็นอย่างน้อย

1) Syslog ทั้ง TCP และ UDP
2) Database หรือ ODBC หรือ SQL
3) FTP หรือ File Transfer
4) OPSEC หรือ LEA Protocol
5) SDEE Protocol

5.3.13. มีรูปแบบความสัมพันธ์ (Correlation Rules) สำหรับใช้วิเคราะห์ข้อมูลภัยคุกคามแบบ Near Real-Time หรือดีกว่า และหาความสัมพันธ์ของเหตุการณ์ต่าง ๆ (Correlation) ได้

5.3.14. ระบบฐานข้อมูลเกี่ยวกับภัยคุกคาม (Threat Intelligence) ที่มาพร้อมระบบ SIEM ต้องสามารถตรวจสอบความเสี่ยงจาก IP, file, Application และ MD5 ได้เป็นอย่างน้อย

5.3.15. สามารถวิเคราะห์พฤติกรรมผู้ใช้ User behavior analytics (UBA) ได้ไม่น้อยกว่า 40,000 ผู้ใช้ และสามารถเพิ่มหน่วยความจำหรือหน่วยประมวลผลหรืออุปกรณ์อื่น ๆ เพื่อให้รองรับผู้ใช้งานได้สูงสุด 220,000 ผู้ใช้งาน

5.3.16. มี Machine Learning Model มาให้พร้อมใช้งานได้ไม่น้อยกว่า 15 Models โดยสามารถ Custom Model โดยใช้รูปแบบภาษา AQL ได้ และต้องรองรับรูปแบบ Model แบบ Hour to Hour Analytics ได้

5.3.17. มี Rule สำหรับใช้ในการวิเคราะห์พฤติกรรมผู้ใช้ได้ดังนี้เป็นอย่างน้อย

1) Access and Authentication
2) Accounts and Privileges
3) Browsing Behavior
4) DNS Analyzer
5) Geography
6) Threat Intelligence

5.3.18. มี Predefined Rules มาพร้อมระบบที่เสนอเพื่อวิเคราะห์พฤติกรรมการใช้งานของผู้ใช้ด้วยข้อมูลจาก Threat Intelligence Platform ดังนี้ ได้เป็นอย่างน้อย

1) Detect IOCs For Locky
2) Detect IOCs for WannaCry
3) Shell Bags Modified By Ransomware
4) User Accessing Risky IP Anonymization
5) Multiple Sessions to Monitored Log Sources (NIS Directive)

5.3.19. สามารถจัดรูปแบบของ Events หรือ Logs ที่ได้รับจากอุปกรณ์ต้นทาง ให้อยู่ในรูปแบบเดียวกันเพื่อที่ระบบจะสามารถทำการวิเคราะห์ได้ (Parsed/Normalized)

5.3.20. สามารถเก็บรักษา Log ไว้บนระบบในรูปแบบที่สามารถสืบค้นเพื่อใช้วิเคราะห์และทำรายงานได้ทันที (Online Log) โดยมีพื้นที่จัดเก็บข้อมูล Logs ได้ไม่น้อยกว่า 90 วัน

5.3.21. สามารถยืนยันความถูกต้องของข้อมูล Log หรือ Event ที่เก็บรักษาว่าไม่มีการถูกเปลี่ยนแปลงแก้ไข (Data Integrity) ด้วย Hashing Algorithm แบบ SHA-1 หรือ SHA-256 หรือเทียบเท่าหรือดีกว่า

5.3.22. สามารถบริหารจัดการผ่าน Web Interface หรือ GUI ได้เป็นอย่างน้อย

5.3.23. สามารถประมวลผลและวิเคราะห์ข้อมูล Log หรือ Event ในแบบแยกเป็นรายหน่วยงาน หรือสามารถทำงานแบบ Multi-Tenanted ได้

5.3.24. สามารถกำหนดสิทธิ หรือ Role ในการเข้าถึงระบบ SIEM ของผู้ดูแลระบบแต่ละคนได้

5.3.25. มี Framework หรือ Extension ในการทำ Compliance หรือ Reporting ที่มาพร้อมกับระบบได้ดังนี้เป็นอย่างน้อย

1) General Data Protection Regulation (GDPR)
2) Good Practice Guide 13 (GPG13)
3) Gramm-Leach-Bliley Act (GLBA)
4) Payment Card Industry (PCI)

5.3.26. สามารถแสดงรายงานในรูปแบบตาราง, Bar Chart, Pie Chart และออกรายงานในรูปแบบ HTML หรือ PDF ได้เป็นอย่างน้อย

5.3.27. สามารถออกรายงานตามช่วงเวลาที่กำหนด (Scheduled Report) ได้

5.3.28. มี Application/Module พร้อมให้เลือกใช้งานสำหรับติดตั้งบนระบบที่เสนอ โดยสามารถรองรับ Categories ดังนี้ ได้เป็นอย่างน้อย

1) Cloud Services
2) Compliance and Reporting
3) Endpoint
4) Escalation
5) File Activity Monitoring
6) Firewall and Network Protection
7) Identity and Enrichment
8) Web Application

5.3.29. มีเครื่องคอมพิวเตอร์แม่ข่ายสำหรับระบบบริหารจัดการ SIEM โดยมีคุณลักษณะอย่างน้อยดังต่อไปนี้

5.3.29.1. เป็นเครื่องคอมพิวเตอร์แม่ข่าย (Server) แบบติดตั้งบน Rack โดยเฉพาะ ที่มีความสูงไม่เกิน 1U พร้อมรางเลื่อน

5.3.29.2. มีหน่วยประมวลผลกลางที่มี Core ไม่น้อยกว่า 16 Core หรือดีกว่า จำนวนไม่น้อยกว่า 2 หน่วย โดยแต่ละหน่วยมีความเร็วสัญญาณนาฬิกาไม่ต่ำกว่า 2.9 GHz

5.3.29.3. หน่วยประมวลผลกลาง (CPU) รองรับการ ประมวลผลแบบ 64 bit มีหน่วยความจำแบบ Cache Memory รวมในระดับ (Level) เดียวกันไม่น้อยกว่า 24 MB

5.3.29.4. มีหน่วยความจำหลักขนาดไม่น้อยกว่า 32 GB แบบ DDR4 RDIMM หรือ LRDIMM หรือดีกว่า จำนวนไม่น้อยกว่า 4 หน่วย โดยรองรับการขยายได้รวมสูงสุดไม่น้อยกว่า 8.0 TB

5.3.29.5. มีระบบควบคุมการจัดเก็บข้อมูล (Controller) แบบ SAS / SATA หรือดีกว่า รองรับการทำ RAID 0,1,5 ได้เป็นอย่างน้อย โดยมีหน่วยความจำไม่น้อยกว่า 4GB

5.3.29.6. มีหน่วยจัดเก็บข้อมูลชนิด SSD หรือดีกว่า จำนวนไม่น้อยกว่า 7 หน่วย โดยแต่ละหน่วยจะต้องมีความจุไม่น้อยกว่า 1.92 TB และรองรับการถอดเปลี่ยนแบบ Hot-Plug หรือ Hot-swap ได้

5.3.29.7. มี Network Interface แบบ 10 Gigabit Ethernet Base-T หรือดีกว่า จำนวนไม่น้อยกว่า 2 ช่อง

5.3.29.8. มี Power Supplies ขนาดไม่ต่ำกว่า 800W จำนวน 2 หน่วย และรองรับการถอดเปลี่ยนแบบ Hot Plug หรือ Hot Swap ได้

5.3.29.9. มี I/O Expansion Slot แบบ PCI-e หรือดีกว่า จำนวนอย่างน้อย 2 ช่อง และรองรับการขยายเพิ่มได้อีกไม่น้อยกว่า 1 ช่อง

5.3.29.10. มีช่องสำหรับใส่หน่วยจัดเก็บข้อมูลแบบ Disk ขนาด 2.5 นิ้ว ไม่ต่ำกว่า 8 หน่วย

5.3.29.11. มีพอร์ตเชื่อมต่ออุปกรณ์แบบ USB 3.0 ไม่น้อยกว่า 5 ports

5.3.29.12. มี Remote Management Port อย่างน้อย 1 พอร์ต

5.3.29.13. เครื่องคอมพิวเตอร์แม่ข่ายที่เสนอมา ได้รับการรับรองตามมาตรฐานอย่างน้อย ดังนี้

1) มาตรฐานการแพร่กระจายคลื่นแม่เหล็กไฟฟ้าตาม FCC หรือ EN หรือ VCCI หรือ CE
2) มาตรฐานความปลอดภัยด้านไฟฟ้าตาม UL หรือ EN หรือ TUV หรือ CSA หรือ IEC
3) มาตรฐานการประหยัดพลังงานตาม Energy Star หรือ ASHRAE A3/A4

5.3.30. มีเครื่องคอมพิวเตอร์แม่ข่ายสำหรับ Syslog โดยมีคุณลักษณะอย่างน้อยดังต่อไปนี้

5.3.30.1. เป็นเครื่องคอมพิวเตอร์แม่ข่าย (Server) แบบติดตั้งบน Rack โดยเฉพาะ ที่มีความสูงไม่เกิน 1U พร้อมรางเลื่อน

5.3.30.2. มีหน่วยประมวลผลกลางที่มี Core ไม่น้อยกว่า 16 Core หรือดีกว่า จำนวนไม่น้อยกว่า 2 หน่วย โดยแต่ละหน่วยมีความเร็วสัญญาณนาฬิกาไม่ต่ำกว่า 2.9 GHz

5.3.30.3. หน่วยประมวลผลกลาง (CPU) รองรับการ ประมวลผลแบบ 64 bit มีหน่วยความจำแบบ Cache Memory รวมในระดับ (Level) เดียวกันไม่น้อยกว่า 24 MB

5.3.30.4. มีหน่วยความจำหลักขนาดไม่น้อยกว่า 32 GB แบบ DDR4 RDIMM หรือ LRDIMM หรือดีกว่า โดยรองรับการขยายได้รวมสูงสุดไม่น้อยกว่า 8.0 TB

5.3.30.5. มีระบบควบคุมการจัดเก็บข้อมูล (Controller) แบบ SAS / SATA หรือดีกว่า รองรับการทำ RAID 0,1,5 ได้เป็นอย่างน้อย โดยมีหน่วยความจำไม่น้อยกว่า 4GB

5.3.30.6. มีหน่วยจัดเก็บข้อมูลชนิด SAS หรือดีกว่า จำนวนไม่น้อยกว่า 4 หน่วย โดยแต่ละหน่วยจะต้องมีความจุไม่น้อยกว่า 2 TB และรองรับการถอดเปลี่ยนแบบ Hot-Plug หรือ Hot-swap ได้

5.3.30.7. มี Network Interface แบบ 10 Gigabit Ethernet Base-Tหรือดีกว่า จำนวนไม่น้อยกว่า 2 ช่อง

5.3.30.8. มี Power Supplies ขนาดไม่ต่ำกว่า 800 W จำนวน 2 หน่วย และรองรับการถอดเปลี่ยนแบบ Hot Plug หรือ Hot Swap ได้

5.3.30.9. มี I/O Expansion Slot แบบ PCI-e หรือดีกว่า จำนวนอย่างน้อย 2 ช่อง และรองรับการขยายเพิ่มได้อีกไม่น้อยกว่า 1 ช่อง

5.3.30.10. มีช่องสำหรับใส่หน่วยจัดเก็บข้อมูลแบบ Disk ขนาด 2.5 นิ้ว ไม่ต่ำกว่า 8 หน่วย

5.3.30.11. มีพอร์ตเชื่อมต่ออุปกรณ์ ประกอบด้วย USB 3.0 ไม่น้อยกว่า 5 ports

5.3.30.12. มี Remote Management Port อย่างน้อย 1 พอร์ต

5.3.30.13. เครื่องคอมพิวเตอร์แม่ข่ายที่เสนอมา ได้รับการรับรองตามมาตรฐานอย่างน้อย ดังนี้

1) มาตรฐานการแพร่กระจายคลื่นแม่เหล็กไฟฟ้าตาม FCC หรือ EN หรือ VCCI หรือ CE
2) มาตรฐานความปลอดภัยด้านไฟฟ้าตาม UL หรือ EN หรือ TUV หรือ CSA หรือ IEC
3) มาตรฐานการประหยัดพลังงานตาม Energy Star หรือ ASHRAE A3/A4

5.3.31. มีระยะเวลาการรับประกันและลิขสิทธิ์การใช้งานได้ไม่น้อยกว่า 3 ปี

6. ขอบเขตการดำเนินงาน

6.1. ผู้รับจ้างจะต้องจัดทำเอกสารและเสนอแผนการเข้าดำเนินงานในการติดตั้ง ให้กับคณะกรรมการตรวจรับพิจารณาเห็นชอบก่อนดำเนินการ

6.2. ผู้รับจ้างจะต้องดำเนินการติดตั้งอุปกรณ์ โปรแกรมหรือซอฟต์แวร์ต่าง ๆ ที่ได้นำเสนอในโครงการนี้ทั้งหมดให้สามารถใช้งานได้ และตรงตามคุณสมบัติที่ระบุไว้ข้างต้น

6.3. ผู้รับจ้างต้องให้คำแนะนำในการออกแบบระบบจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log) เพื่อจัดเก็บข้อมูล ณ ศูนย์ข้อมูลสารสนเทศของ สป.อว. ให้สอดคล้องตามนโยบายหรือข้อบังคับที่ต้องปฏิบัติตาม

6.4. ผู้รับจ้างต้องจัดให้มีผู้เชี่ยวชาญสำหรับดำเนินการเข้าเตรียมพร้อมและส่งผ่านข้อมูลจราจรทางคอมพิวเตอร์ เพื่อใช้ในการเฝ้าระวังฯ (On-boarding process) ดังนี้

6.4.1.ตรวจสอบความพร้อมใช้ของระบบและอุปกรณ์ต้นกำเนิดข้อมูลจราจรทางคอมพิวเตอร์ที่จะใช้ในการเฝ้าระวัง

6.4.2.ระบุแหล่งที่มาของข้อมูลจราจรทางคอมพิวเตอร์และจัดหมวดหมู่ของอุปกรณ์ต้นกำเนิด

6.4.3.ออกแบบและจัดทำ Monitoring usecase รวมทั้งรวมทั้งกำหนดประเภทข้อมูลจราจรทางคอมพิวเตอร์ (Log) ที่ต้องใช้ในการวิเคราะห์

6.4.4.จัดทำ Dashboard และ Alert ให้สอดคล้องกับ Monitoring Use-case เพื่อใช้ในการแจ้งเตือนและรายงานต่าง ๆ

6.5. ผู้รับจ้างต้องจัดเตรียมหน่วยปฏิบัติการตอบสนองต่ออุบัติการณ์ด้านความมั่นคงปลอดภัยทางคอมพิวเตอร์ (CSIRT) พร้อมที่จะปฏิบัติหน้าที่ในการตอบสนองต่อภัยคุกคามหรือการบุกรุกระบบอย่างทันท่วงที หรือเข้าดำเนินการสืบสวนและวิเคราะห์หาสาเหตุของปัญหา ภัยคุกคามที่เกิดขึ้น รวมถึงการตรวจพิสูจน์พยานหลักฐานทาง Digital เมื่อมีการร้องขอบริการจากทางผู้ใช้บริการภายในระยะเวลา 4 ชั่วโมงนับตั้งแต่ที่ร้องขอ ไม่เกินกว่า 4 เหตุการณ์ต่อปี พร้อมจัดทำรายงานผลการดำเนินงานสรุปข้อมูลหลักฐานต่าง ๆ ที่ได้จากการตอบสนองต่อเหตุการณ์ภัยคุกคาม รวมถึงแนวทางในการป้องกันการเกิดซ้ำในอนาคต (Incident Response and Recommendations Report) ทันทีที่สามารถดำเนินการได้

6.6. ผู้รับจ้างต้องดำเนินการเฝ้าระวังความมั่นคงปลอดภัยทางไซเบอร์ วิเคราะห์เหตุการณ์ และแจ้งเตือนภัยคุกคามทางไซเบอร์ ให้แก่ผู้ใช้บริการ ณ ศูนย์ปฏิบัติการฯ ของผู้เสนอราคา โดยให้บริการแบบตลอดเวลา 24 ชั่วโมงของทุกวัน ไม่มีวันหยุด (7 x 24) ตลอดระยะเวลาของสัญญา

6.7. ผู้ผู้รับจ้างต้องมีระบบบริหารจัดการ ซึ่งแสดงสถานการณ์ตรวจสอบข้อมูลความปลอดภัยของระบบเครือข่าย และข้อมูลการแจ้งเตือนและติดตามเหตุการณ์ (Ticket Management) เพื่อให้ผู้ใช้บริการสามารถตรวจสอบข้อมูลได้ตลอดเวลา

6.8. ผู้รับจ้างต้องแจ้งเตือนภัยคุกคามด้านความมั่นคงปลอดภัย สำหรับเหตุการณ์ที่อยู่ในขอบข่ายภัยคุกคามทางไซเบอร์ โดยจะต้องแจ้งเตือนผ่านทางอีเมลหรือทางโทรศัพท์ หรือช่องทางอื่นใด ตามที่จะตกลงกับผู้ใช้บริการ ให้เป็นไปตาม Severity Level Agreement (SLA) อย่างน้อยดังต่อไป ดังนี้

ระดับความรุนแรง	แจ้งเตือนผู้รับบริการ	ให้คำแนะนำในการแก้ไข
วิกฤติ	30 นาที	2 ชั่วโมง
สูง	1 ชั่วโมง	4 ชั่วโมง
กลาง	6 ชั่วโมง	8 ชั่วโมง

ความเร่งด่วน	ผลกระทบ	การดำเนินการ
วิกฤติ (Critical)	ระบบโครงสร้างพื้นฐานสำคัญไม่สามารถให้บริการได้ การดำเนินธุรกิจหยุดชะงักและจำเป็นต้องแก้ไขอย่างเร่งด่วนที่สุด	ต้องตรวจสอบรวมถึงส่งคำแนะนำและขั้นตอนการดำเนินการแก้ไขเชิงเทคนิคแก้ไขปัญหาโดยเร่งด่วน
สูง (High)	ระบบสารสนเทศหยุดชะงักและมีผลกระทบต่อประสิทธิภาพการทำงานมีความจำเป็นต้องแก้ไขอย่างเร่งด่วน	ต้องตรวจสอบเฝ้าระวังรวมถึงส่งคำแนะนำและขั้นตอนกาดำเนินการแก้ไขเชิงเทคนิคแก้ไขปัญหาโดยเร่งด่วน
ปานกลาง (Medium)	มีผลกระทบต่อประสิทธิภาพการทำงานทั่วไปและมีผลกระทบต่อการดำเนินธรกิจภาพรวมเล็กน้อย	ควรตรวจสอบหรือเฝ้าระวัง

6.9. ดำเนินการวิเคราะห์แบบรวมศูนย์และจัดทำเงื่อนไขการโจมตี เพื่อช่วยในการเฝ้าระวังและแจ้งเตือนภัยคุกคามด้วยรูปแบบและมาตรฐานของผู้รับจ้าง (Standard Usecase) รวมทั้งปรับปรุงและจัดทำการแจ้งเตือนภัยคุกคามด้วยรูปแบบเงื่อนไขเฉพาะ หรือเงื่อนไขอื่น ๆ เพิ่มเติม (Custom Usecase) ให้เหมาะสมจำนวนไม่น้อยกว่า 5 Usecases ต่อปี

6.10. การแจ้งเตือนจะต้องมีรายละเอียด อย่างน้อยดังนี้

6.10.1. ระบุประเภทของภัยคุกคาม

6.10.2. วัน-เวลา เริ่มต้นของภัยคุกคาม

6.10.3. ระบุต้นทาง (Attacker) และปลายทาง (Target)

6.10.4. ระบุระดับความรุนแรง (Severity)

6.10.5. รายละเอียดเหตุการณ์และพฤติกรรม

6.10.6. คำแนะนำและขั้นตอนการดำเนินการแก้ไขด้านเทคนิค (Action & Recommendation)

6.11. ผู้รับจ้างต้องรายงานผลการดำเนินการจัดเก็บและวิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์และสรุปผลการดำเนินการเฝ้าระวังภัยคุกคามเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศที่เกิดขึ้นโดยมีการวิเคราะห์ภัยคุกคาม เป็นรายเดือน (Monthly report) ภายใน 10 วันทำการ ซึ่งมีเนื้อหาอย่างน้อยดังนี้

6.11.1. สรุปเหตุการณ์ตามประเภทและระดับความรุนแรง (Incident Report)

6.11.2. สรุป 10 อันดับสูงสุดของการโจมตี

6.11.3. สรุป 10 อันดับสูงสุดของเป้าหมายที่โดยโจมตี

6.11.4. สรุป 10 อันดับสูงสุดของผู้โจมตี

6.11.5. สรุป 10 อันดับสูงสุดของช่องทางที่ถูกใช้โจมตี

6.11.6. สรุปปริมาณและสถานะการใช้งานข้อมูลจราจรทางคอมพิวเตอร์ประจำเดือน

6.11.7. บทวิเคราะห์แนวโน้มของภัยคุกคามต่าง ๆ ที่เกิดขึ้นในเดือนที่ผ่านมา

6.11.8. สรุปคำแนะนำ

6.12. ผู้รับจ้างต้องจัดทำรายงานสรุปสำหรับผู้บริหาร (Executive Summary) เพื่ออธิบายผู้บริหารให้เข้าใจสถานะความเสี่ยงและสภาพปัจจุบันเป็นรายไตรมาส (Quarterly)

6.13. ผู้รับจ้างต้องให้บริการรวบรวมข้อมูลภัยคุกคามทางไซเบอร์ที่มีการปรับปรุงให้ทันสมัยอยู่เสมอจากแหล่งต่าง ๆ จากทั่วทุกมุมโลก (Threat Intelligence) เพื่อการวิเคราะห์ข้อมูลภัยคุกคามร่วมกับระบบ SIEM หรือ CSOC Technology เพิ่มเติม เพื่อทำให้สามารถรับมือกับภัยคุกคามไซเบอร์ได้อย่างมีประสิทธิภาพมากยิ่งขึ้น

6.14. ผู้รับจ้างต้องมีการแจ้งข่าวสารซึ่งเกี่ยวข้องกับระบบรักษาความปลอดภัยทางไซเบอร์ เช่น

6.14.1. รายชื่อ และคุณลักษณะของมัลแวร์ (Malware)

6.14.2. ช่องโหว่ใหม่ (Vulnerability) ของอุปกรณ์ในระบบเครือข่าย (Network Equipment)

6.14.3. ช่องโหว่ใหม่ (Vulnerability) ของระบบปฏิบัติการ (Operating System)

6.14.4. ช่องโหว่ใหม่ (Vulnerability) ของระบบฐานข้อมูลหลัก (Database)

6.15. ผู้รับจ้างต้องเข้าร่วมประชุมรายไตรมาส ทั้งแบบประชุมทางไกล (Video Conference Quarterly Meeting) หรือ เข้าประชุม ณ ที่ทำการสำนักงานใหญ่ (On -Site Quarterly Meeting) เพื่อสรุปผลงานบริการวิเคราะห์เฝ้าระวังภัยคุกคามต่างๆ ที่เกิดขึ้นกับผู้ใช้บริการ ตลอดสัญญาของการให้บริการ

7. เอกสารส่งมอบ

7.1. ผู้รับจ้างต้องจัดส่งเอกสารในรูปแบบเอกสารจำนวน 3 ชุด และรูปแบบ Electronic File จำนวน 1 ชุด โดยมีป้ายแสดงระดับชั้นความลับให้กับ สป.อว. อย่างน้อยดังนี้

7.1.1.ผังภาพโครงสร้างการเชื่อมต่อของอุปกรณ์ที่นำเสนอกับระบบเครือข่าย ของ สป.อว.

7.1.2.เอกสารคู่มือการติดตั้งอุปกรณ์ที่นำเสนอในโครงการนี้

7.1.3.รายละเอียดการกำหนดค่าการใช้งานอุปกรณ์ (System Configuration)

7.1.4.รายงานผลการทดสอบการติดตั้งอุปกรณ์ทั้งหมดในโครงการนี้

7.1.5.เอกสารสิทธิ์การใช้งาน (License) ในโครงการนี้ทั้งหมด โดยระบุในนามของสำนักงานปลัดกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม (สป.อว.) **หรือ Ministry of Higher Education, Science, Research and Innovation. (MHESI) เท่านั้น**

7.2. ในกรณีที่เอกสารส่งมอบประกอบไปด้วยข้อมูลที่สำคัญของหน่วยงาน อาธิเช่น หมายเลข IP address, เอกสารการกำหนดการตั้งค่าอุปกรณ์หรือระบบฯ, เอกสารลิขสิทธิ์ (License), ของอุปกรณ์หรือระบบฯ, ข้อมูลส่วนบุคคล รวมถึงบัญชีและรหัสผ่านของผู้ใช้งานระบบสารสนเทศระดับผู้ใช้งานทั่วไป เป็นต้น ทางผู้ให้บริการต้องจัดทำป้ายแสดงระดับชั้นความลับ ให้มีตราหรือเครื่องหมาย หรือชื่อขององค์กร และมีข้อความระบุว่า “Confidential” หรือคำว่า “ลับ” จำนวน 1 ชุด บนเอกสาร และจัดทำเอกสารรูปแบบเฉพาะที่ปิดบังข้อมูลที่สำคัญของหน่วยงาน โดยมีข้อความว่า “Internal Use” หรือคำว่า “ใช้ภายใน” จำนวน 2 ชุดบนเอกสาร ที่จะจัดส่งให้กับทาง สป.อว. (รวมทั้งหมด 3 ชุด) และข้อมูลแบบ Electronic File ซึ่งต้องทำการเข้ารหัสข้อมูล (Encrypted) เพื่อป้องกันการเข้าถึงข้อมูลที่สำคัญ โดยต้องมีข้อความระบุว่า “Confidential” หรือคำว่า “ลับ” บนเอกสารซองเอกสารทึบแสงที่ปิดผนึกเรียบร้อยนำส่งมองให้กับทาง สป.อว. จำนวน 1 ชุด พร้อมดำเนินการส่งรหัสผ่านให้กับผู้ดูแลระบบผ่านทางช่องทางที่ สป.อว. เป็นผู้กำหนด ด้วยโปรแกรม WinZip หรือ 7Zip เป็นต้น

8. การปกปิดความลับทางด้านข้อมูล (Non-disclosure agreement)

ผู้รับจ้างหรือเจ้าหน้าที่ของผู้รับจ้างจะต้องดำเนินการลงนามการปกปิดความลับทางด้านข้อมูล (Non-disclosure agreement) กับ สป.อว. สำหรับโครงการนี้ เพื่อเป็นการรักษาความลับทางด้านข้อมูลไม่ให้รั่วไหลสู่สาธารณะโดยไม่ได้รับอนุญาต

9. การอบรม

ผู้รับจ้างต้องจัดอบรมการใช้งาน และการแก้ปัญหาเบื้องต้นของอุปกรณ์ หรือ โปรแกรมที่นำเสนอให้กับผู้ดูแลระบบ สป.อว. จำนวนไม่น้อยกว่า 5 คน ณ สป.อว. โดยผู้รับจ้างจะต้องเป็นผู้รับผิดชอบค่าใช้จ่ายทั้งหมด ในการจัดหาเอกสารประกอบการอบรมแต่ละหลักสูตรให้กับ สป.อว.

10. การรับประกัน

10.1. ผู้รับจ้างต้องเป็นผู้ประสานงานหลักในการแก้ไขปัญหา กรณีที่มีการแจ้งปัญหาการใช้งาน ไปยังบริษัทเจ้าของผลิตภัณฑ์ที่นำเสนอในโครงการนี้ กรณีหากมีค่าใช้จ่ายเกิดขึ้น ผู้รับจ้างต้องเป็นผู้รับผิดชอบค่าใช้จ่ายทั้งหมด ซึ่งต้องถือปฏิบัติตลอดอายุการรับประกัน

10.2. ผู้รับจ้างต้องติดตั้งเครื่องหมายแสดงการรับประกันซึ่งต้องระบุชื่อบริษัทผู้รับประกันและระยะเวลารับประกันพร้อมเบอร์โทรศัพท์ หรือ E-Mail ไว้อย่างชัดเจน

11. วงเงินงบประมาณ 12,860,000 บาท (สิบสองล้านแปดแสนหกหมื่นบาทถ้วน)

12. การชำระเงิน

สป.อว. จะชำระเงินให้แก่ผู้รับจ้าง เมื่อผู้รับจ้างดำเนินการติดตั้งระบบที่ได้นำเสนอ ในโครงการนี้ ให้สามารถใช้งานได้กับระบบเครือข่ายคอมพิวเตอร์ของ สป.อว. ตรงตามคุณสมบัติที่ระบุไว้ข้างต้น และทางคณะกรรมการตรวจรับพัสดุได้ดำเนินการตรวจรับไว้ โดยครบถ้วนแล้ว โดยแบ่งเป็น 3 งวด นับถัดจากวันลงนามในสัญญา

งวดที่ 1 ชำระในอัตราร้อยละ 30 (สามสิบ) ของราคาจ้างทั้งหมด ซึ่งรวมภาษีมูลค่าเพิ่มแล้ว เมื่อส่งมอบงานตามขอบเขตงานงวดที่ 1

งวดที่ 2 ชำระในอัตราร้อยละ 40 (สี่สิบ) ของราคาจ้างทั้งหมด ซึ่งรวมภาษีมูลค่าเพิ่มแล้ว เมื่อส่งมอบงานตามขอบเขตงานงวดที่ 2

งวดที่ 3 ชำระในอัตราร้อยละ 30 (สามสิบ) ของราคาจ้างทั้งหมด ซึ่งรวมภาษีมูลค่าเพิ่มแล้ว เมื่อส่งมอบงานตามขอบเขตงานงวดที่ 3

13. การส่งมอบงาน

งวดที่	สิ่งส่งมอบงาน	ระยะเวลาการส่งมอบ
1	1) แผนดำเนินโครงการ (Project Plan) จำนวน 1 ฉบับ	ภายใน 15 วัน นับถัดจากวันลงนามในสัญญา
2	1) ลิขสิทธิ์ซอฟแวร์ป้องกันและควบคุมการใช้งานโปรแกรมของเครื่องปลายทาง (Endpoint Protection) จำนวนไม่น้อยกว่า 500 License ตามข้อ 5.1 2) ลิขสิทธิ์ระบบตรวจจับและตอบสนองภัยคุกคามบนระบบเครือข่ายคอมพิวเตอร์ (Network Detection and Response) จำนวน 1 ชุด ตามข้อ 5.2 3) ลิขสิทธิ์ซอฟต์แวร์สำหรับการบันทึกข้อมูล Log เพื่อการวิเคราะห์ และรักษาความปลอดภัยระบบคอมพิวเตอร์ จำนวน 1 ชุด ตามข้อ 5.3	ภายใน 60 วัน นับถัดจากวันลงนามในสัญญา

งวดที่	สิ่งส่งมอบงาน	ระยะเวลาการส่งมอบ
	4) เครื่องแม่ข่ายสำหรับซอฟต์แวร์สำหรับการบันทึกข้อมูล Log เพื่อการวิเคราะห์ และรักษาความปลอดภัยระบบคอมพิวเตอร์ จำนวนอย่างน้อย 2 ชุด ตามข้อ 5.3.29 – 5.3.30	
3	1) รายงานการติดตั้ง จำนวน 1 ชุด 2) เอกสารแผนผังการติดตั้งระบบจำนวน 1 ชุด 3) เอกสารประกอบการอบรมทั้งหมดในโครงการ จำนวน 1 ชุด	ภายใน 90 วัน นับถัดจากวันลงนามในสัญญา

14. หลักเกณฑ์การพิจารณาคัดเลือกข้อเสนอ

เกณฑ์การพิจารณาผู้ชนะการเสนอราคา ใช้เกณฑ์ราคาและพิจารณาจากราคารวม

15. ค่าปรับ

หากผู้รับจ้างไม่สามารถส่งมอบงานและอุปกรณ์ในโครงการนี้ให้แล้วเสร็จตามเวลาที่กำหนดไว้ในสัญญาผู้รับจ้างจะต้องชำระค่าปรับให้แก่ทาง สป.อว. เป็นรายวันอัตราร้อยละ 0.10 (ศูนย์จุดหนึ่งศูนย์) ของมูลค่าตามสัญญา แต่ไม่ต่ำกว่าวันละ 100 บาท

(นางสาวศุภกร สาระวงศ์)
เจ้าหน้าที่ระบบงานคอมพิวเตอร์

(นายทวีศักดิ์ นาเมืองรักษ์)
นักวิชาการคอมพิวเตอร์ชำนาญการ

(นายพฤทธิ์ แกะกระโทก)
นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ