ขอบเขตของงานและข้อกำหนดคุณลักษณะเฉพาะ
อุปกรณ์ป้องกันระบบแม่ข่าย จำนวน 1 ระบบ
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

1. หลักการและเหตุผล

ด้วยนโยบายของสถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง ที่มุ่งสู่การเป็นมหาวิทยาลัยดิจิทัล (Digital University) อย่างเต็มรูปแบบ เพื่อส่งเสริมการเรียนการสอน การวิจัย และการให้บริการวิชาการผ่านระบบดิจิทัลอย่างมีประสิทธิภาพและทั่วถึง การวางรากฐานด้านโครงสร้างพื้นฐานดิจิทัลและระบบความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) จึงเป็นปัจจัยสำคัญที่ต้องให้ความสำคัญเป็นลำดับต้น เนื่องจากสถาบันต้องพึ่งพาระบบสารสนเทศในแทบทุกกระบวนการของการดำเนินงาน ไม่ว่าจะเป็นด้านบริหารจัดการ การเรียนการสอน การให้บริการนักศึกษา รวมไปถึงระบบฐานข้อมูลกลางของหน่วยงานต่าง ๆ ภายในสถาบัน

ในปัจจุบัน สถาบันมีการพัฒนาและให้บริการระบบสารสนเทศจำนวนมากแก่บุคลากร นักศึกษา และผู้เกี่ยวข้อง อาทิ ระบบทะเบียนนักศึกษา ระบบสารบรรณอิเล็กทรอนิกส์ ระบบฐานข้อมูลกลาง ระบบสารสนเทศทรัพยากรบุคคล รวมถึงระบบฐานข้อมูลที่เกี่ยวข้องกับการจัดการเรียนการสอน ระบบดังกล่าวล้วนเป็นระบบที่มีความสำคัญสูง และมีข้อมูลที่มีความละเอียดอ่อน (Sensitive Data) หากขาดมาตรการด้านความปลอดภัยที่เหมาะสม อาจก่อให้เกิดความเสียหายต่อข้อมูล การให้บริการ หรือกระทบต่อภาพลักษณ์ของสถาบันได้

ด้วยสถานการณ์ภัยคุกคามทางไซเบอร์ในปัจจุบันที่มีแนวโน้มเพิ่มขึ้นทั้งในเชิงความซับซ้อนและความถี่ของการโจมตี อาทิ การโจมตีแบบ DDoS, การบุกรุกระบบแม่ข่าย, การแพร่กระจายมัลแวร์ และการขโมยข้อมูลส่วนบุคคลผ่านช่องโหว่ของระบบ สถาบันจึงมีความจำเป็นต้องดำเนินการจัดหาอุปกรณ์ป้องกันระบบแม่ข่าย (Server Protection Appliance) ที่มีความสามารถในการตรวจจับ ป้องกัน และตอบสนองต่อภัยคุกคามทางไซเบอร์อย่างมีประสิทธิภาพ และสามารถบริหารจัดการแบบรวมศูนย์ได้ (Centralized Security Management)

การจัดหาอุปกรณ์ดังกล่าวจะช่วยเพิ่มความปลอดภัยให้กับระบบสารสนเทศหลักของสถาบัน ลดความเสี่ยงจากการถูกโจมตีหรือรบกวนระบบให้บริการ ตลอดจนเป็นการยกระดับมาตรฐานความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศของสถาบันให้สอดคล้องกับนโยบายการพัฒนาสู่ Digital University อย่างยั่งยืน

2. วัตถุประสงค์

2.1. เพื่อจัดหาอุปกรณ์ป้องกันระบบแม่ข่าย เพื่อเพิ่มความปลอดภัยให้กับระบบสารสนเทศต่างๆ ในสถาบัน

2.2. เพื่อป้องกันการโจมตีจากภัยคุกคามเกี่ยวกับ Cyber Security รวมถึงมีระบบการ Monitor

3. คุณสมบัติของผู้ยื่นข้อเสนอ

3.1. ผู้เสนอราคาจะต้องเป็นนิติบุคคล ที่มีอาชีพรับงานตามที่ระบุไว้ในเอกสารนี้

3.2. ผู้เสนอราคาต้องเป็นผู้ที่มีความสามารถตามกฎหมาย

3.3. ผู้เสนอราคาต้องไม่เป็นบุคคลล้มละลาย

3.4. ผู้เสนอราคาต้องไม่อยู่ระหว่างเลิกกิจการ

3.5. ผู้เสนอราคาต้องไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

3.6. ผู้เสนอราคาต้องไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงาน และได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

3.7. ผู้เสนอราคาต้องมีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

3.8. ผู้เสนอราคาไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่ รัฐบาลของผู้เสนอราคาได้มีคำสั่งให้สละสิทธิ์ความคุ้มกันเช่นว่านั้น

3.9. ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ามายื่นข้อเสนอให้แก่หน่วยงานของรัฐ ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันราคาอย่างเป็นธรรมในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

4. สถานที่ดำเนินการ

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

เลขที่ 1 ซอยฉลองกรุง 1 ถนนฉลองกรุง แขวงลำปลาทิว เขตลาดกระบัง กรุงเทพมหานคร 10520

5. รายการครุภัณฑ์ที่จะซื้อ อุปกรณ์ป้องกันระบบแม่ข่าย จำนวน 1 ระบบ ประกอบไปด้วยรายการดังนี้

5.1. อุปกรณ์ออกรายงาน และจัดเก็บข้อมูล (Logs/Events) สำหรับอุปกรณ์รักษาความปลอดภัยเครือข่าย จำนวน 1 ระบบ

5.1.1. เป็นอุปกรณ์ Hardware Appliance ที่สามารถเก็บรวบรวมเหตุการณ์ (Logs or Events) ที่เกิดขึ้นบนอุปกรณ์ป้องกันเครือข่าย (Next Generation Firewall) ที่ทางหน่วยงานใช้งานอยู่ในปัจจุบันหรือที่นำเสนอมาพร้อมกันในโครงการได้ และอยู่ภายใต้เครื่องหมายการค้าเดียวกัน

5.1.2. มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ GE RJ45 จำนวนไม่น้อยกว่า 2 พอร์ต หรือดีกว่า และแบบ 25 GE SFP28 จำนวนไม่น้อยกว่า 2 พอร์ต หรือดีกว่า

5.1.3. มี Storage ขนาด 4TB จำนวนไม่น้อยกว่า 8 หน่วย หรือ Storage รวมขนาดไม่น้อยกว่า 32 TB หรือดีกว่า

5.1.4. มีอัตราความสามารถในการจัดเก็บข้อมูล Log เพื่อวิเคราะห์ได้ไม่น้อยกว่า 20,000 logs per second

5.1.5. สามารถรองรับจำนวนการจัดเก็บข้อมูล log ได้ไม่น้อยกว่า 660 GB ต่อวัน

5.1.6. มีคุณสมบัติรองรับการป้องกันการเสียหายของข้อมูล (RAID level) แบบ RAID 0, RAID 1, RAID 5, RAID 6, RAID 10, RAID 50 และ RAID 60 โดยสามารถเลือกใช้งานแบบใดแบบหนึ่งได้เป็นอย่างน้อย

5.1.7. มีระบบแสดงผลทั้งแบบ NOC (Network Operations Center) และ SOC (Security Operations Center) ได้เป็นอย่างน้อย

5.1.8. สามารถแสดงข้อมูล Log ในลักษณะ Custom view หรือ Log view ได้เป็นอย่างน้อย

5.1.9. มีรูปแบบรายงานสำหรับพร้อมใช้ (Report) จำนวนไม่น้อยกว่า 70 รูปแบบ และสามารถแสดงรายงานในรูปแบบของ PDF หรือ HTML ได้เป็นอย่างน้อย

5.1.10. มีรูปแบบของ datasets, charts และ macros ที่พร้อมใช้งานรวมกันจำนวนไม่น้อยกว่า 2,000 รูปแบบ

5.1.11. มีคุณสมบัติในการวิเคราะห์และแสดงข้อมูลแบบ Real-Time และ Historical ได้เป็นอย่างน้อย

5.1.12. สามารถทำงานในลักษณะ Multi-Tenancy เพื่อเพิ่มความสะดวกในการบริหารจัดการแต่ละบัญชีผู้ใช้ได้เป็นอย่างน้อย

5.1.13. สามารถส่งต่อ Log ไปยังอุปกรณ์ภายนอกหรืออุปกรณ์ Third-Party ได้

5.1.14. อุปกรณ์มีคุณสมบัติรองรับ Trusted Platform Moule (TPM) เป็นอย่างน้อย

5.1.15. มีคุณสมบัติรองรับการใช้งานในลักษณะ High Availability แบบ Active-Passive ได้

5.1.16. มี Power Supply รองรับการใช้งานแบบ Redundant Hot Swappable

5.1.17. อุปกรณ์ต้องได้รับรองมาตรฐาน FCC, VCCI และ CE เป็นอย่างน้อย

5.1.18. อุปกรณ์ต้องเป็นยี่ห้อเดียวกันกับ อุปกรณ์รักษาความปลอดภัยเว็บไซต์ และ ระบบวิเคราะห์ ตรวจจับภัยคุกคาม และตอบสนองในระบบเครือข่าย ที่เสนอภายในโครงการเพื่อให้ระบบทำงานร่วมกันอย่างมีประสิทธิภาพ

5.1.19. มีการรับประกันอุปกรณ์ (Warranty) เป็นระยะเวลาไม่น้อยกว่า 3 ปี

5.1.20. ผู้เสนอราคาต้องมีหนังสือแต่งตั้งการเป็นตัวแทนจำหน่ายจากบริษัทเจ้าของผลิตภัณฑ์ที่มีสาขาในประเทศไทยโดยตรง และมีเอกสารรับรองว่าอุปกรณ์ที่เสนอเป็นอุปกรณ์ใหม่ ไม่เคยถูกใช้งานมาก่อน และยังอยู่ในสายการผลิต

5.2. ระบบวิเคราะห์ ตรวจจับภัยคุกคาม และตอบสนองในระบบเครือข่าย (Network Detection and Response) จำนวน 1 ระบบ

5.2.1. เป็นอุปกรณ์แบบ Hardware Appliance ที่ออกแบบมาทำหน้าที่วิเคราะห์ ตรวจจับความผิดปกติของเครือข่ายและเนื้อหาที่เป็นอันตราย โดยมีคุณสมบัติ Artificial Neural Networks เพื่อสนับสนุนการตรวจสอบภัยคุกคามขั้นสูง (Advanced Malware Detection) ได้

5.2.2. สามารถลดเวลาในการตรวจสอบและตรวจจับ Malware จากระดับนาทีเป็นระดับวินาที หรือดีกว่าได้

5.2.3. มีประสิทธิภาพในการทำงานแบบ Sniffer Throughput สูงสุดไม่น้อยกว่า 10 Gbps

5.2.4. มีประสิทธิภาพรองรับการทำงานแบบ Dual Port Sniffer Throughput สูงสุดไม่น้อยกว่า 20 Gbps

5.2.5. มีประสิทธิภาพในการการตรวจจับ Malware ได้สูงสุดไม่น้อยกว่า 170,000 ไฟล์ต่อชั่วโมง

5.2.6. มีประสิทธิภาพรองรับการทำงานแบบ Netflow ได้สูงสุดไม่น้อยกว่า 100,000 Flows per second

5.2.7. มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) อย่างน้อย ดังนี้

5.2.7.1. พอร์ตแบบ 10/100/1000 RJ45 จำนวนไม่น้อยกว่า 2 พอร์ต หรือดีกว่า

5.2.7.2. ช่องสำหรับติดตั้ง Transceiver แบบ 10GE SFP+ จำนวนไม่น้อยกว่า 4 ช่อง หรือดีกว่า

5.2.7.3. พอร์ตสำหรับ Console แบบ GE RJ45 จำนวนไม่น้อยกว่า 1 พอร์ต หรือดีกว่า

5.2.8. มีหน่วยเก็บข้อมูล (Storage) ขนาดไม่น้อยกว่า 7 TB จำนวนไม่น้อยกว่า 2 หน่วย หรือดีกว่า

5.2.9. สามารถตรวจจับความปลอดภัยทางเครือข่าย เช่น Botnets, Weakciphers, และ North/South/East/West intrusions ได้เป็นอย่างน้อย

5.2.10. รองรับการทำงานร่วมกับระบบอื่น ๆ เช่น Third Party API call ได้เป็นอย่างน้อย

5.2.11. รองรับการทำงานแบบ Files Submission หรือ ICAP Server ได้เป็นอย่างน้อย

5.2.12. สามารถทำงานร่วมกับไฟล์ และโปรโตคอล ดังต่อไปนี้เป็นอย่างน้อย

5.2.12.1. NDR engine: TCP, UDP, ICMP, ICMP6, TLS, HTTP, SMB, SMTP, SSH, FTP, POP3, DNS, IRC, IMAP, RTSP, RPC, SIP, RDP, SNMP, MYSQL, MSSQL, PGSQL, and their behaviors

5.2.12.2. File-based analyses: 32-bit and 64-bit PE - Web based, text, and PE files such as EXE, PDF, MSOFFICE, HTML, ZIP, TAR, POWERSHELL, BAT, SHELLSCRIPT, PERLSCRIPT, DLL, DOC, XLS, PPT, DOCX, XLSX, PPTX, PYTHON, CSS, AUTOITSCRIPT, JPEG, GIF, TIFF, PNG, BMP, MPEG, MOV, MP3, WMA, WAV, AVI

5.2.13. สามารถติดตั้งใช้งานแบบ Standalone mode หรือ Sensor mode ได้เป็นอย่างน้อย

5.2.14. สามารถทำ Allow list และ Deny list โดยใช้คุณสมบัติของ Hash มาเป็นตัวกรองได้เป็นอย่างน้อย

5.2.15. สามารถตรวจสอบรายการความผิดปกติที่ตรวจพบจาก Machin Learning ได้ และสามารถเพิ่มความคิดเห็นเชิงลบ หรือเชิงบวก (Feedback) สำหรับการตรวจจับได้เป็นอย่างน้อย

5.2.16. สามารถส่งการแจ้งเตือนให้กับผู้ดูแลระบบโดยแบ่งการแจ้งเตือนแต่ละประเภทได้ เช่น Network Attack Detection, Botnet Anomaly, Encrypted Attack, และ Machine Learning Detection ได้เป็นอย่างน้อย

5.2.17. สามารถจำแนก Malware หรือการโจมตีออกเป็นหลากหลายสถานการณ์ (Attack Scenario) เช่น Botnet, Ransomware, Worm Activity, Rootkit, Generic Trojan, Banking Trojan, Exploit, Application, Cryptojacking, DoS, Backdoor, Web Shell, Wiper, Data Leak, Fileless, และ Phishing ได้เป็นอย่างน้อย เพื่อใช้ข้อมูลดังกล่าวสนับสนุนการวิเคราะห์ความปลอดภัยบนระบบเครือข่าย

5.2.18. สามารถกำหนดรูปแบบการเข้าใช้งานของผู้ดูแล (Admin Profile) ในแต่ละระดับที่แตกต่างกันได้ เช่น Visual Security Analyst, System Status, System Configuration, หรือ System Maintenance ได้เป็นอย่างน้อย

5.2.19. สามารถออกรายงานของการวิเคราะห์ และการระบาดของ Malware (Outbreak) แบบ CSV, PDF และ JSON ได้เป็นอย่างน้อย

5.2.20. มี Power Supply รองรับการใช้งานแบบ Redundant Hot Swappable

5.2.21. อุปกรณ์ต้องได้รับรองมาตรฐาน FCC, CE และ VCCI เป็นอย่างน้อย

5.2.22. อุปกรณ์ต้องเป็นยี่ห้อเดียวกันกับ อุปกรณ์รักษาความปลอดภัยเว็บไซต์ และ ระบบออกรายงาน และจัดเก็บข้อมูล ที่เสนอภายในโครงการเพื่อให้ระบบทำงานรวมกันอย่างมีประสิทธิภาพ

5.2.23. มีการรับประกันอุปกรณ์ (Warranty) เป็นระยะเวลาไม่น้อยกว่า 3 ปี

5.2.24. ผู้เสนอราคาต้องมีหนังสือแต่งตั้งการเป็นตัวแทนจำหน่ายและได้รับการรับรองจากผู้ผลิตสาขาในประเทศไทยโดยตรงว่าอุปกรณ์ที่เสนอเป็นอุปกรณ์ใหม่ไม่เคยใช้งานมาก่อนและยังอยู่ในสายการผลิต

5.3. อุปกรณ์รักษาความปลอดภัยเว็บไซต์ (Web Application Firewall) จำนวน 1 ระบบ

5.3.1. เป็นอุปกรณ์แบบ Appliance สำหรับทำหน้าที่เป็น Web Application Firewall (WAF) โดยเฉพาะ โดยสามารถป้องกัน Web Application จากภัยคุกคามทางไซเบอร์ได้

5.3.2. สามารถทำงานได้โดยไม่จำกัดสิทธิ์ของจำนวน Application ที่ใช้งาน (Unlimited Application Licenses)

5.3.3. มีช่องการเชื่อมต่อระบบเครือข่าย (Network Interfaces) 10/100/1000 (RJ45) จำนวนไม่น้อยกว่า 4 พอร์ต โดยมีคุณสมบัติ bypass ครบทุกพอร์ต และช่องใส่ Transceiver แบบ 10G SFP+ จำนวนไม่น้อยกว่า 4 ช่อง หรือดีกว่า

5.3.4. มีหน่วยเก็บข้อมูล Storage แบบ SSD ขนาด 480 GB จำนวนไม่น้อยกว่า 2 หน่วย

5.3.5. สามารถรองรับ Throughput ได้ไม่น้อยกว่า 5 Gbps และมีค่าความหน่วง (Latency) น้อยกว่า 5 ms

5.3.6. รองรับการใช้งานในลักษณะ Administrative Domains ได้ไม่น้อยกว่า 64 Domains

5.3.7. สามมารถป้องกันการโจมตีผ่านทางเว็บแอพพลิเคชั่นได้ตาม OWASP Top 10 รวมถึง Cross Site Scripting, SQL Injection, Cross Site Request Forgery และ Session Hijacking ได้เป็นอย่างน้อย

5.3.8. สามารถป้องกันการโจมตีผ่านทาง API ได้ เช่น XML and JSON protocol conformance, Machine Learning Based API Discovery and Protection และ Web Services Signatures

5.3.9. มีคุณสมบัติรองรับการใช้งานด้านความปลอดภัย เช่น Protocol validation, Brute force protection, Cookie signing and encryption, Data Leak Prevention, DoS Prevention, Virtual Patching, Malware Detection และ Operating system intrusion signatures เป็นอย่างน้อย

5.3.10. มีความสามารถในการเฝ้าระวังการเปลี่ยนแปลงเว็บไซต์ (Web Defacement) และสามารถ restore website content จากส่วนที่ backup ไว้ ได้โดยอัตโนมัติ

5.3.11. มีความสามารถในการทำ File Upload Scanning ด้วย Antivirus (AV) ได้ บนตัวอุปกรณ์เอง

5.3.12. มีความสามารถในการตรวจสอบ IP Reputation เพื่อป้องกัน Botnets, Spammers, Anonymous Proxies, Malicious Sources ได้

5.3.13. สามารถป้องกันการโจมตีด้วยเทคนิค Credential Stuffing ได้ โดยตรวจสอบข้อมูลการ กับฐานข้อมูล compromised credential เจ้าของผลิตภัณฑ์ได้ หรือเสนอระบบเพิ่มเติม เพื่อให้มีคุณสมบัติตามที่กำหนด

5.3.14. สามารถป้องกันภัยคุกคามขั้นสูง (Advance Threat Protection) โดยส่งไฟล์ต้องสงสัยไปตรวจสอบกับระบบ Cloud-based Sandbox ที่ให้บริการโดยเจ้าของผลิตภัณฑ์ได้ หรือเสนอระบบเพิ่มเติม เพื่อให้มีคุณสมบัติตามที่กำหนด

5.3.15. มีคุณสมบัติ Threat Analytics เพื่อช่วยตรวจสอบภัยคุกคามได้อย่างชัดเจน

5.3.16. สามารถทำงานแบบ Dual-Layer Machine learning เพื่อตรวจจับการร้องขอไม่ปกติ (Anomaly) และป้องกันการใช้งานที่เป็นอันตราย (Threats) ได้

5.3.17. สามารถแสดงข้อมูลการโจมตีที่เกิดขึ้น (Geo IP Analytics) และตั้งค่าการป้องกันตามประเทศ (IP Address Geolocation) ได้

5.3.18. มีคุณสมบัติรองรับการใช้งานในรูปแบบ Reverse proxy, Inline Transparent, Span (Offline Sniffing) และ WCCP ได้เป็นอย่างน้อย

5.3.19. สามารถตรวจสอบช่องโหว่ของเว็บแอพพลิเคชั่น (Vulnerability Scan) จากตัวอุปกรณ์ได้ และรองรับการทำงานร่วมกับ 3rd Party vulnerability scanner เช่น Acunetix, HP WebInspect, IBM AppScan, Qualys ได้เป็นอย่างน้อย

5.3.20. สามารถทำ SSL Offloading หรือ SSL Inspection เพื่อลดภาระงาน web server ได้

5.3.21. สามารถตรวจสอบและป้องกันการใช้งานผ่าน WebSocket Protocol ได้

5.3.22. รองรับการตรวจสอบข้อมูล API ในรูปแบบ XML, JSON และ OpenAPI ได้เป็นอย่างน้อย

5.3.23. สามารถป้องกัน Mobile API โดยการตรวจสอบ JWT-token field และกำหนดเงื่อนไขให้ Alert, Deny และ Period Block ได้

5.3.24. สามารถทำหน้าที่เป็น API Gateway ได้ โดยสามารถจำกัดการเข้าถึงจาก user ด้วย API Key พร้อมสามารถระบุ IP และ HTTP Referrer ได้

5.3.25. สามารถเก็บ Log และส่งออกไปยัง Syslog ได้

5.3.26. สามารถทำรายงาน (Report) เป็นรายชั่วโมง รายวัน รายสัปดาห์ ได้เป็นอย่างน้อย โดยเลือกเป็นรูปแบบ PDF, HTML และ MS Word ได้เป็นอย่างน้อย

5.3.27. สามารถส่ง Alert E-Mail ได้ ตามเงื่อนไขของ Event หรือ Log ที่ตรวจพบ

5.3.28. สามารถบริหารจัดการอุปกรณ์ได้บนตัวอุปกรณ์เอง โดยไม่ต้องติดตั้งระบบบริหารจัดการส่วนกลาง ผ่าน HTTPS (Web User Interface) และ SSH (Command Line Interface) ได้เป็นอย่างน้อย

5.3.29. มีคุณสมบัติรองรับการทำ High Availability แบบ Active/Passive หรือ Active/Active Clustering ได้

5.3.30. สามารถอัพเดท Signature ด้านความปลอดภัยได้ตลอดระยะเวลาภายใต้อายุการรับประกัน (Warranty) ที่นำเสนอ

5.3.31. อุปกรณ์ที่เสนอต้องผ่านการรับรองมาตรฐานด้านความปลอดภัยจาก FCC, VCCI และ CE เป็นอย่างน้อย

5.3.32. ผลิตภัณฑ์ที่เสนอมีเครื่องหมายการค้าหรือระบบปฏิบัติการที่อยู่ในกลุ่มผู้นำ (Leader) ของ KuppinggerCole – Leadership Compass ด้าน Web Application Firewall ประจำปี 2024 หรือปีล่าสุด และ GigaOM - Application and API Security ประจำปี 2024 หรือปีล่าสุด

5.3.33. อุปกรณ์ต้องเป็นยี่ห้อเดียวกันกับ ระบบออกรายงาน และจัดเก็บข้อมูล และ ระบบวิเคราะห์ ตรวจจับภัยคุกคาม และตอบสนองในระบบเครือข่าย ที่เสนอภายในโครงการเพื่อให้ระบบทำงานรวมกันอย่างมีประสิทธิภาพ

5.3.34. มีการรับประกัน (Warranty) และเป็นระยะเวลาไม่น้อยกว่า 3 ปี

5.3.35. ผู้เสนอราคาต้องมีหนังสือแต่งตั้งการเป็นตัวแทนจำหน่ายจากบริษัทเจ้าของผลิตภัณฑ์ที่มีสาขาในประเทศไทยโดยตรง และมีเอกสารรับรองว่าอุปกรณ์ที่เสนอเป็นอุปกรณ์ใหม่ ไม่เคยถูกใช้งานมาก่อน และยังอยู่ในสายการผลิต

5.4. ระบบบริหารจัดการตรวจสอบสิทธิการเข้าถึงของผู้ใช้งาน (Privileged Access and Session Management) จำนวน 1 ระบบ

5.4.1. ระบบที่เสนอต้องเป็นอุปกรณ์ Virtual Appliance หรือ Software ที่ออกแบบมาเพื่อทำหน้าที่เป็น Privileged Access and Session Management โดยเฉพาะ

5.4.2. มีความสามารถในการบริหารจัดการบัญชีผู้ใช้ (Privileged Account Management), กำหนดสิทธิการเข้าถึงของผู้ใช้งาน (Role-Based Access Control) และตรวจสอบกิจกรรมของผู้เข้าใช้งาน (Session Monitoring) ได้เป็นอย่างน้อย

5.4.3. มีลิขสิทธิ์สำหรับรองรับผู้ใช้งานระบบพร้อมกัน จำนวนไม่น้อยกว่า 20 ผู้ใช้งาน

5.4.4. สามารถบริหารจัดการผู้ใช้งานในรูปแบบ Local User หรือพิสูจน์ตัวตน (Authentication) ผู้ใช้งานกับระบบ LDAP, RADIUS และ SAML ได้เป็นอย่างน้อย

5.4.5. มี Template สำหรับการเข้าใช้งาน Windows Domain Account, Unix SSH, Web Account, Cisco Device และ FortiGate ได้เป็นอย่างน้อย

5.4.6. มี Launcher สำหรับเชื่อมต่อไปยังทรัพยากรปลายทาง ดังต่อไปนี้

- 5.4.6.1. Web Launcher
- 5.4.6.2. Web SSH
- 5.4.6.3. Web RDP
- 5.4.6.4. Web VNC
- 5.4.6.5. Web SFTP

5.4.6.6. Web SMB

5.4.6.7. WinSCP

5.4.7. สามารถกำหนด policy สำหรับบัญชีผู้ใช้งานเพื่อทำการเปลี่ยนรหัสผ่าน (Password) ได้

5.4.8. มีคุณสมบัติในการบริหารจัดการรหัสผ่าน (password) ของทรัพยากรดังต่อไปนี้

5.4.8.1. Verify Password

5.4.8.2. Periodical Password Changer

5.4.9. สามารถควบคุมการเข้าใช้งาน โดยกำหนดให้ผู้ใช้งานทำการขอสิทธิจากผู้อนุมัติเพื่อเข้าใช้งาน (Request Approval) และมีคุณสมบัติดังต่อไปนี้

5.4.9.1. สามารถกำหนดผู้อนุมัติได้สูงสุดไม่น้อยกว่า 3 Tiers

5.4.9.2. สามารถทำ Request Review and Approve ได้

5.4.9.3. สามารถทำการแจ้งเตือน Request ได้

5.4.10. สามารถเฝ้าระวังผู้ใช้งาน (User Monitor) และตรวจสอบการใช้งานที่กำลังดำเนินการ (Active Session Monitor) ได้เป็นอย่างน้อย

5.4.11. สามารถทำการบันทึกการใช้งานเป็นวิดีโอ (Session Video Recording) เพื่อตรวจสอบการเข้าใช้งานของผู้ใช้ได้เป็นอย่างน้อย

5.4.12. สามารถกำหนดระยะเวลาสูงสุด (Max Duration) ในการเข้าใช้งานของผู้ใช้งานได้

5.4.13. มีคุณสมบัติรองรับการอนุญาตให้ผู้ใช้งานสามารถเข้าถึงทรัพยากรต่าง ๆ ในกรณีฉุกเฉิน (Glass Breaking) ได้

5.4.14. มีคุณสมบัติรองรับการใช้งานพิสูจน์ตัวตนแบบ Multi Factor Authentication (MFA) หรือ 2 Factor Authentication (2FA) สำหรับ Local user และ Remote User เช่น LDAP user, RADIUS user หรือ SAML user ได้เป็นอย่างน้อย

5.4.15. สามารถป้องกันการส่งคำสั่งไม่ปลอดภัย (Dangerous Commands) ผ่านช่องทาง SSH แบบอัตโนมัติได้

5.4.16. สามารถป้องกันการเข้าใช้งานทรัพยากรพร้อมกันของผู้ใช้งานได้ (Check-out/Check-in Protection)

5.4.17. มีคุณสมบัติรองรับการตรวจสอบและป้องกันไวรัส (Anti-Virus) ในการถ่ายโอนไฟล์ผ่านช่องทางเว็บ (Web-based file transfer) ได้เป็นอย่างน้อย

5.4.18. มีคุณสมบัติในการป้องกันข้อมูลรั่วไหล (Data Leak Prevention) โดยตรวจสอบจากชนิดของไฟล์หรือขนาดของไฟล์ได้เป็นอย่างน้อย

5.4.19. มีคุณสมบัติรองรับการใช้งาน Zero Trust Network Access (ZTNA) เพื่อยกระดับความปลอดภัยในการเข้าใช้งานได้

5.4.20. มีคุณสมบัติรองรับการทำ High Availability แบบ Active-Passive ได้เป็นอย่างน้อย

5.4.21. สามารถทำการ Backup Configuration แบบอัตโนมัติได้

5.4.22. สามารถแสดงรายการของการใช้งานและเหตุการณ์ในรูปแบบ Log เช่น System event, User event เพื่อตรวจสอบย้อนหลัง (Audit) ได้เป็นอย่างน้อย

5.4.23. มีคุณสมบัติรองรับการทำ Virtual Trusted Platform Module (vTPM) สำหรับ KVM และ VMWare เพื่อยกระดับการป้องกัน Private Keys ของผู้ใช้งานได้

5.4.24. อุปกรณ์ต้องเป็นยี่ห้อเดียวกันกับ อุปกรณ์รักษาความปลอดภัยเว็บไซต์ และ ระบบออกรายงาน และจัดเก็บข้อมูล และ ระบบวิเคราะห์ ตรวจจับภัยคุกคาม และตอบสนองในระบบเครือข่ายที่เสนอภายในโครงการ เพื่อให้ระบบทำงานรวมกันอย่างมีประสิทธิภาพ

5.4.25. ระบบที่เสนอมีระยะเวลาการรับประกันจำนวนไม่น้อยกว่า 3 ปี

5.4.26. ระบบที่เสนอสามารถ Update Firmware หรือ Software ได้ตลอดระยะเวลาการรับประกัน

5.4.27. ผู้เสนอราคาต้องมีหนังสือแต่งตั้งการเป็นตัวแทนจำหน่าย และได้รับการรับรองจากผู้ผลิตที่มีสาขาในประเทศไทยโดยตรงว่าอุปกรณ์ที่เสนอเป็นอุปกรณ์ใหม่ไม่เคยใช้งานมาก่อนและยังอยู่ในสายการผลิต

6. การส่งมอบงาน

การจ่ายเงินจะจ่ายเมื่อทำการส่งมอบงานสมบูรณ์ และได้ทำการตรวจรับโดยคณะกรรมการตรวจรับพัสดุเป็นที่เรียบร้อยแล้ว โดยจะจ่ายเป็นจำนวนร้อยละ 100 ของมูลค่าที่กำหนดในสัญญา

7. การประกันความชำรุดบกพร่อง

รับประกันความชำรุดบกพร่อง เป็นระยะเวลา 3 ปี

8. คุณสมบัติผู้เสนอราคา

สถาบันจะพิจารณาคุณสมบัติของข้อเสนอตามในกรณีเป็นผู้เสนอราคามีคุณสมบัติครบถ้วนตามที่ได้กำหนดดังต่อไปนี้

8.1. ผู้เสนอราคาจะต้องแนบเอกสารหลักฐานที่เกี่ยวข้องกับการเสนอราคาให้ครบถ้วนในวันที่เสนอราคา

9. ระยะเวลาดำเนินการ

120 วัน

10. วงเงินงบประมาณ

วงเงินในการดำเนินการ จำนวนรวมทั้งสิ้น 20,300,575 (ยี่สิบล้านสามแสนห้าร้อยเจ็ดสิบห้าบาทถ้วน) โดยราคาดังกล่าวได้รวมภาษีแล้วทุกกรณี

11. หน่วยงานผู้รับผิดชอบดำเนินการ

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

12. หลักเกณฑ์การพิจารณาการจัดจ้าง การพิจารณาข้อเสนอจะดำเนินการโดยคณะกรรมการจัดจ้างดังนี้

12.1. คณะกรรมการจะพิจารณาคุณสมบัติของผู้ยื่นข้อเสนอ หากคุณสมบัติไม่เป็นไปตามระเบียบสถาบันที่กำหนดไว้ คณะกรรมการฯจะไม่พิจารณาการเสนอราคา

12.2. ในกรณีที่ไม่สามารถคัดเลือกผู้ดำเนินการที่มีคุณสมบัติและราคาที่เหมาะสมได้ สถาบันขอสงวนสิทธิ์ที่จะยกเลิกการยื่นเสนอราคา ทั้งนี้ ผู้เสนอราคาจะเรียกร้องค่าใช้จ่ายใดๆ ทั้งสิ้นไม่ได้

12.3. หากมีผู้ผ่านเกณฑ์ตามระเบียบสถาบันเพียงรายเดียวให้อยู่ในดุลพินิจของคณะกรรมการจัดจ้างที่พิจารณาแล้วเห็นว่ามีความเหมาะสม และเป็นประโยชน์สูงสุดต่อสถาบัน โดยไม่จำเป็นต้องเป็นผู้เสนอราคาต่ำสุด แต่ทั้งนี้จะต้องอยู่ภายในวงเงินงบประมาณที่ได้รับการจัดสรร

12.4. คณะกรรมการจะพิจารณาโดยใช้เกณฑ์ราคา

12.5. ทั้งนี้ จะดำเนินการเซ็นสัญญา หลังจากได้รับงบประมาณจัดสรรเรียบร้อยแล้ว