เงื่อนไขของการคัดเลือกเป็นผู้ให้บริการ

1. หากได้รับเอกสาร TOR ดังกล่าวแล้วให้แจ้งความจำนงเข้าร่วมคัดเลือกเป็นผู้ร่วมประมูลงานกลับมาที่สำนักงานจัดซื้อและพัสดุ มหาวิทยาลัยรังสิต อีเมล์ rattanasak.k@rsu.ac.th
2. มหาวิทยาลัยรังสิต ขอสงวนสิทธิ์ในการยื่นซองเสนอราคาหาก บริษัท,ห้าง,ร้าน ไม่กระทำตามเงื่อนไข
3. ราคาที่เสนอต้องรวมทุกอย่างเบ็ดเสร็จแล้ว มหาวิทยาลัยรังสิต ขอสงวนสิทธิที่จะเปลี่ยนแปลงราคาภายหลัง
4. บริษัท,ห้าง,ร้าน ที่ร่วมเสนอราคาต้องมีความชำนาญและประสบการณ์งานด้านนี้
5. ผู้เสนอราคาต้อง แยกซองเทคนิคและใบเสนอราคาจากกัน โดยเอกสารใบเสนอราคาให้ บริษัท,ห้าง,ร้าน ถือมาเปิดซองในวันประกวดราคาเท่านั้น
6. ชี้แจงแบบและสอบถามข้อสงสัย ในวันศุกร์ที่ 26 มิถุนายน 2569 ในเวลา 10.00-12.00น. ห้องประชุม 13-301 ชั้น3 อาคาร13 มหาวิทยาลัยรังสิต โดย สำนักบริการเทคโลยีสารสนเทศ
7. กำหนดส่งซองเอกสารเทคนิค แจ้งให้ทราบในวันชี้แจงแบบ หลังจากกำหนดแล้วหากเลยเวลาขอไม่รับซองเอกสารทางเทคนิคในทุกกรณี
8. แจ้งผลทางเทคนิค ยังไม่ได้กำหนด
9. กำหนดการแจ้งผลคัดเลือกเป็นผู้ร่วมประมูลงาน ยังไม่ได้กำหนด
10. มหาวิทยาลัย ทรงไว้ซึ่งสิทธิที่จะไม่รับราคาต่ำสุดหรือราคาหนึ่งราคาใดหรือราคาที่เสนอมาทั้งหมดก็ได้ และ อาจจะพิจารณาเลือกซื้อในจำนวนหรือขนาดหรือเฉพาะรายการ หรือราคาหนึ่งราคาใด หรืออาจจะยกเลิกการเสนอราคาโดยไม่พิจารณาซื้อก็เป็นได้สุดแต่คณะกรรมการจัดซื้อจัดจ้างจะพิจารณาและขอสงวนสิทธิไม่มีการจ่ายเงินมัดจำล่วงหน้าไม่ว่ากรณีใด ๆ ทั้งนี้ เพื่อประโยชน์กับมหาวิทยาลัยรังสิตเป็นสำคัญและให้ถือว่าการตัดสินของคณะกรรมการจัดซื้อจัดจ้าง มหาวิทยาลัยรังสิตถือว่าเป็นเด็ดขาด บริษัท,ห้าง,ร้าน ที่เสนอราคาจะเรียกร้อง สิทธิ หรือค่าเสียหายแบบใด ๆ มิได้
11. บริษัท,ห้าง,ร้านไม่สามารถดำเนินงานได้ทันตามกำหนด มหาวิทยาลัยรังสิตขอสงวนสิทธิที่จะไม่รับงานทั้งหมด หรือปรับตามกฎหมายกำหนด ของมูลค่างานทั้งหมด
12. บริษัท,ห้าง,ร้าน ต่างๆ ที่เสนอราคาต้องทำแผนการดำเนินงานแนบใบเสนอราคามาด้วย ตามกำหนดระยะเวลา ที่กำหนดใน TOR นี้
13. หาก บริษัท,ห้าง,ร้าน ไม่ได้เข้าร่วมการประชุมรับฟังชี้แจง TOR ทางมหาวิทยาลัยรังสิต ทรงไว้ซึ่งสิทธิที่จะไม่อนุญาตให้เข้าร่วมประมูลงานในโครงการดังกล่าวนี้
14. บริษัท,ห้าง,ร้าน ที่ประสงค์เข้าร่วมเสนอราคาต้องมีเอกสาร Pro file ของบริษัทมาด้วย ณ วันรับฟังคำชี้แจง

ขอบเขตของงาน (Terms of Reference: TOR)

โครงการจัดซื้อระบบ Endpoint Detection and Response (EDR)

1. บทนำและความเป็นมา (Introduction and Rationale)

ในปัจจุบัน ภูมิทัศน์ของภัยคุกคามทางไซเบอร์มีการเปลี่ยนแปลงและทวีความซับซ้อนอย่างรวดเร็ว โดยเฉพาะการโจมตีรูปแบบ Advanced Persistent Threat (APT), Ransomware และ Fileless Malware ซึ่งมีพฤติกรรมแฝงตัวและหลบเลี่ยงการตรวจจับได้เป็นเวลานาน ระบบป้องกันอุปกรณ์ปลายทางในรูปแบบดั้งเดิมหรือ Traditional Antivirus (EPP) ที่อาศัยการตรวจจับตามฐานข้อมูล (Signature-based) จึงไม่มีประสิทธิภาพเพียงพอในการรับมือกับภัยคุกคามที่ไม่มีไฟล์หรือการโจมตีผ่านช่องโหว่ Zero-day

เพื่อให้การรักษาความมั่นคงปลอดภัยสารสนเทศขององค์กรสอดคล้องกับมาตรฐานสากล องค์กรจึงมีความประสงค์จัดหาระบบ Endpoint Detection and Response (EDR) เพื่อเพิ่มขีดความสามารถในการมองเห็น (Visibility) กิจกรรมที่เกิดขึ้นบนอุปกรณ์ปลายทางแบบเรียลไทม์ และลดระยะเวลาในการตรวจพบภัยคุกคาม (MTTD) รวมถึงระยะเวลาในการตอบสนองและแก้ไขเหตุการณ์ (MTTR) เพื่อยับยั้งความเสียหายต่อทรัพย์สินดิจิทัลได้อย่างทันท่วงที

2. วัตถุประสงค์และขอบเขตการจัดหา (Objectives and Project Scope)

2.1 วัตถุประสงค์

1) เพื่อป้องกัน ตรวจจับ และตอบสนองต่อภัยคุกคามบนอุปกรณ์ปลายทาง (Endpoints) แบบเรียลไทม์ตลอด 24 ชั่วโมง
2) เพื่อบูรณาการการทำงานร่วมกับโครงสร้างพื้นฐานด้านความปลอดภัยเดิม เช่น Next Generation Firewall และระบบ SIEM
3) เพื่อรองรับการเฝ้าระวังภัยคุกคามเชิงรุก (Proactive Threat Hunting) โดยผู้เชี่ยวชาญเพื่อเพิ่มระดับความปลอดภัยขั้นสูงสุด
4) จัดซื้อสิทธิ์การใช้งาน (License) สำหรับระบบ EDR จำนวน 500 Endpoints ระยะเวลาสัญญา 3 ปี
5) ครอบคลุมการติดตั้ง Software Agent บนระบบปฏิบัติการ Windows, macOS และ Linux
6) บริการติดตั้ง (Installation), การปรับแต่งค่าระบบ (Configuration) และการเชื่อมต่อระบบ (System Integration)
7) การอบรมถ่ายทอดความรู้ (Training) สำหรับผู้ดูแลระบบ แบบ On-site
8) บริการสนับสนุนด้านเทคนิคและบำรุงรักษา (Maintenance) แบบ 24/7 ตลอดอายุสัญญา

2.2 ขอบเขตการจัดหา

ครอบคลุมการจัดซื้อสิทธิ์การใช้งาน การติดตั้ง การปรับแต่งระบบ การเชื่อมต่อกับระบบที่เกี่ยวข้อง การอบรมผู้ดูแลระบบ และการบำรุงรักษาตลอดอายุสัญญา เพื่อให้ระบบสามารถใช้งานได้อย่างมีประสิทธิภาพและสอดคล้องกับความต้องการขององค์กร

3. คุณสมบัติทางเทคนิคที่สำคัญ (Mandatory Technical Requirements)

3.1 การป้องกันและยับยั้ง (Protection & Prevention)

1) ใช้เทคโนโลยี Machine Learning และ AI ในการวิเคราะห์และป้องกันมัลแวร์ทั้งที่รู้จัก (Known) และไม่รู้จัก (Unknown Malware), Adware และโปรแกรมที่ไม่พึงประสงค์ (PUPs)
2) มีระบบป้องกัน Ransomware โดยเฉพาะ สามารถยับยั้งการเข้ารหัสไฟล์ (File Encryption), การเข้าถึง File System และการลบ Volume Shadow Copy
3) สามารถป้องกันการโจมตีผ่านช่องโหว่ (Exploit Prevention) ได้แก่ Heap Spray Pre-allocation, SEH Overwrite Protection, Forced Address Space Layout Randomization และ Null Page Allocation
4) ระบบต้องมีคุณสมบัติ "Offline Protection" สามารถป้องกันภัยคุกคามได้เต็มประสิทธิภาพแม้เครื่องปลายทางจะไม่ได้เชื่อมต่อกับระบบบริหารจัดการ (Console)

3.2 การตรวจจับและการมองเห็น (Detection & Visibility)

1) ตรวจจับตัวบ่งชี้การโจมตี (Indicator of Attack - IOA) และพฤติกรรมต้องสงสัยในหน่วยความจำ (Memory) หรือการใช้ Script ที่ผิดปกติแบบเรียลไทม์
2) ระบบต้องสามารถแสดงการเชื่อมต่อเครือข่ายในระดับ Process โดยระบุรายละเอียดครบถ้วน ได้แก่ ชื่อและ PID ของ Process ที่เป็นต้นเหตุ, Source IP Address และ Port, Destination IP Address และ Port, Protocol (TCP/UDP), และ Connection State แบบ Real-time
3) ระบบต้องสามารถแสดง Process Genealogy (Parent-Child Process Chain) ที่ครอบคลุมตั้งแต่ Parent Process จนถึง Child Process ที่สร้าง Network Connection พร้อม Command Line Arguments ที่ใช้เรียกใช้งาน เพื่อให้ผู้วิเคราะห์เห็นเส้นทางการโจมตีแบบสมบูรณ์
4) ระบบต้องสามารถตรวจจับและแจ้งเตือนการเคลื่อนย้ายภายในเครือข่าย (Lateral Movement) โดยระบุเครื่องต้นทาง เครื่องปลายทาง และ Process หรือ Application ที่ใช้ดำเนินการ เช่น PsExec, WMI, RDP, SMB และ PowerShell Remoting
5) สามารถสร้าง Custom IOA เพื่อตรวจจับพฤติกรรมเฉพาะเจาะจง เช่น Process Creation, File Creation, Network Connection (IPv4/IPv6) และ Domain Name

3.3 การตอบสนองและแก้ไข (Response & Remediation) ระบบต้องมีฟังก์ชัน Live Terminal เพื่อสั่งการเครื่องปลายทางจากระยะไกล โดยรองรับคำสั่งขั้นต่ำดังนี้:

1) ตรวจสอบและหยุดการทำงานของกระบวนการ (List & Kill Processes)
2) ตรวจสอบการเชื่อมต่อเครือข่าย (Show Network Connections)
3) จัดการระบบไฟล์ (Navigate, Get, Delete, Upload Files)
4) สั่งเริ่มระบบใหม่หรือปิดเครื่อง (Remote Restart/Shutdown)
5) รันสคริปต์หรือไฟล์คำสั่ง (Custom Scripts) รองรับภาษา PowerShell, Bash และ Zsh
6) ระบบต้องมีฟังก์ชัน Network Containment เพื่อตัดการเชื่อมต่อเครือข่ายของเครื่องที่ติดเชื้อผ่านระบบบริหารจัดการส่วนกลางได้ทันที (Isolate Host)

3.4 การบริหารจัดการระบบ (System Management)

1) บริหารจัดการผ่าน Cloud-based Management (SaaS) โดยมีการเข้ารหัสข้อมูลสื่อสารแบบ TLS-encrypted
2) ซอฟต์แวร์เอเจนท์ต้องเป็นแบบ Lightweight Agent ที่กินทรัพยากรเครื่องต่ำ
3) การอัปเกรดระบบ Machine Learning และ Indicator of Attack (IOA) ต้องแยกอิสระจากการอัปเดต Patch ของระบบปฏิบัติการ และต้องไม่มีความจำเป็นต้อง Reboot เครื่องทั้งในการติดตั้งและอัปเดต

3.5 การตรวจสอบทรัพย์สินและช่องโหว่ (Asset Inventory & Vulnerability)

1) สามารถตรวจสอบและรายงานรายการช่องโหว่ของระบบปฏิบัติการ (Vulnerability Assessment) ได้
2) สามารถทำรายการทรัพย์สิน (Inventory) ของเครื่องที่ติดตั้งเอเจนท์ ได้แก่ Applications, Users, Disk และ Shares

3.6 การควบคุมอุปกรณ์เชื่อมต่อ (Device Control - USB)

1) สามารถแสดงข้อมูลการใช้งาน USB Device และกำหนดนโยบายตาม Class ของอุปกรณ์ได้แก่ Audio/Video, Imaging, Mass Storage, Mobile (MTP/PTP), Printer และ Wireless
2) สามารถกำหนดระดับการเข้าถึง (Level of Access) ได้แก่ Full Access, Full Block, Read and Write Only (Mass Storage) และ Read Only (Mass Storage)

4. **การเชื่อมต่อและพื้นที่จัดเก็บข้อมูล (Integration and Data Storage)**

1) รองรับการส่งข้อมูล Alert หรือ Log ไปยังระบบ SIEM ผ่านทาง Syslog หรือ API
2) รองรับ Single Sign-On (SSO) ผ่านโปรโตคอล SAML 2.0 (เช่น Okta, Ping และ AD FS)
3) ต้องสามารถรับและวิเคราะห์ Log จากอุปกรณ์ Next Generation Firewall ยี่ห้อ Palo Alto เพื่อเพิ่มความแม่นยำในการตรวจจับ
4) พื้นที่จัดเก็บข้อมูลประวัติเหตุการณ์ (Historical Event Storage) โดยรองรับการจัดเก็บ Log ย้อนหลังไม่น้อยกว่า 90 วันในระดับ Full Telemetry และไม่น้อยกว่า 2 ปี ในระดับ Summary/Alert Log พร้อมความสามารถ Search และ Export ข้อมูลได้ตลอดช่วงเวลาดังกล่าว
5) ผลิตภัณฑ์ต้องอยู่ในกลุ่ม Leader ใน Gartner Magic Quadrant ด้าน Endpoint Protection Platforms (EPP) ประจำปี 2026

5. **ข้อกำหนดบริการและระดับการให้บริการ (SLA & Managed Services)**

1) ผลิตภัณฑ์ต้องอยู่ในกลุ่ม Leader หรือ Strong Performer ในรายงาน Forrester New Wave™ หรือ Forrester Wave (Threat Intelligence/XDR) ภายในระยะเวลาไม่เกิน 2 ปี
2) ผ่านการรับรองมาตรฐานสากลด้านความปลอดภัยอย่างน้อยดังนี้: SOC 2, HIPAA, GDPR, PCI DSS, NIST SP 800-53 Rev. 4 และ CSA-STAR
3) Uptime: ระบบบริหารจัดการต้องมีความพร้อมใช้งานไม่น้อยกว่า 99.9%
4) Threat Hunting: ต้องมีบริการตรวจหาภัยคุกคามเชิงรุก 24/7 โดยผู้เชี่ยวชาญ (Human Analysis) จากเจ้าของผลิตภัณฑ์
5) Response Time: สำหรับเหตุการณ์วิกฤต (Critical Incidents) ต้องตอบกลับภายใน 1 ชั่วโมง และดำเนินการแก้ไข (Remediation/Recovery) ภายใน 4 ชั่วโมง
6) Preventive Maintenance (PM): ดำเนินการตรวจสอบสภาพระบบอย่างน้อย 3 ครั้งต่อปี และตรวจสอบการอัปเกรดเวอร์ชันซอฟต์แวร์ทุก 4 เดือน

6. **คุณสมบัติของผู้เสนอราคาและบุคลากร (Vendor and Personnel Qualifications)**

1) คุณสมบัติบริษัท: เป็นนิติบุคคลที่จดทะเบียนในประเทศไทยไม่น้อยกว่า 5 ปี มีทุนจดทะเบียนชำระแล้วไม่ต่ำกว่า 10,000,000 บาท
2) ประสบการณ์: มีผลงานติดตั้งระบบ EDR ให้กับองค์กรที่มี Endpoints ไม่น้อยกว่า 500 เครื่อง อย่างน้อย 2 โครงการภายใน 3 ปีที่ผ่านมา
3) บุคลากร: วิศวกรหลักต้องถือประกาศนียบัตรวิชาชีพระดับสากล เช่น CISSP หรือ CEH ในทีมจำนวนไม่น้อยกว่า 2 ท่าน และสามารถให้บริการ On-site ได้ 1 ท่านเป็นอย่างน้อย

7. การคุ้มครองข้อมูลส่วนบุคคลและความลับ (PDPA and Confidentiality)

1) การเป็นตัวแทน: ต้องมีหนังสือแต่งตั้งเป็นตัวแทนจำหน่าย (Authorized Partner) อย่างเป็นทางการจากเจ้าของผลิตภัณฑ์
2) ผู้ขายมีสถานะเป็น "ผู้ประมวลผลข้อมูลส่วนบุคคล" (Data Processor) ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
3) ต้องลงนามในบันทึกข้อตกลงไม่เปิดเผยข้อมูล (NDA) และมีมาตรการความปลอดภัยข้อมูลที่เข้มงวด

8. หลักเกณฑ์การพิจารณาและตรวจรับ (Evaluation and Acceptance Criteria)

1) เมื่อสิ้นสุดสัญญา ต้องส่งคืนหรือทำลายข้อมูลตามโปรโตคอลที่ปลอดภัยและแจ้งยืนยันเป็นลายลักษณ์อักษร
2) การพิจารณา: ใช้หลักเกณฑ์การพิจารณาแบบผ่านเกณฑ์คุณสมบัติทางเทคนิค (Mandatory Pass/Fail) ร่วมกับเกณฑ์ราคาประกอบประสิทธิภาพ (Price-Performance)
3) รายละเอียดราคา: ต้องแยกรายละเอียดค่าใช้จ่าย (Cost Breakdown) และยืนราคาไม่น้อยกว่า 90 วัน นับตั้งแต่วันยื่นข้อเสนอ

9. มาตรฐานสากลและการยอมรับ (International Standards and Compliance)

1) ผลิตภัณฑ์ที่นำเสนอต้องผ่านการรับรองมาตรฐานสากลด้านความมั่นคงปลอดภัยสารสนเทศอย่างน้อยดังต่อไปนี้ พร้อมหลักฐานเอกสาร Certificate หรือ Attestation Report ที่ยังมีผลบังคับใช้ ณ วันยื่นข้อเสนอ
2) SOC 2 Type II: รายงานการตรวจสอบโดยผู้ตรวจสอบอิสระ ครอบคลุม Security, Availability และ Confidentiality Trust Service Criteria
3) ISO/IEC 27001: ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS) ครอบคลุมการพัฒนาและให้บริการระบบ
4) GDPR Compliance: มีนโยบายและกระบวนการปฏิบัติตาม General Data Protection Regulation สำหรับข้อมูลส่วนบุคคลของผู้ใช้งาน
5) NIST SP 800-53 Rev. 5 หรือเทียบเท่า: มีการจัดทำ Compliance Mapping แสดงความสอดคล้องกับมาตรการควบคุมด้านความมั่นคงปลอดภัย
6) PCI DSS v4.0: สำหรับกรณีที่ระบบเชื่อมต่อกับสภาพแวดล้อมที่จัดเก็บหรือประมวลผลข้อมูลบัตรชำระเงิน
7) CSA STAR Level 1 ขึ้นไป: ครอบคลุมการประเมินความมั่นคงปลอดภัยของบริการ Cloud ตามหลักเกณฑ์ Cloud Security Alliance

8) MITRE ATT&CK Evaluation: ผลิตภัณฑ์ต้องเคยเข้าร่วมการทดสอบ MITRE ATT&CK Enterprise Evaluation และมีผลการทดสอบตรวจจับได้ไม่น้อยกว่าร้อยละ 90 ของ Techniques ที่ทดสอบ ภายในระยะเวลา 3 ปีที่ผ่านมา

10. เงื่อนไขการชำระเงิน บทลงโทษ และค่าปรับ (Payment Terms and Penalties)

1) เงื่อนไขการชำระเงิน ผู้เช่าซื้อจะต้องชำระค่าเช่าซื้อตามสัญญาเป็นรายเดือน โดยแบ่งชำระออกเป็น 36 งวด ภายในระยะเวลา 3 ปี นับถัดจากวันส่งมอบและตรวจรับเรียบร้อยแล้ว
2) ค่าปรับความล่าช้า (Penalty): กรณีผู้รับจ้างไม่สามารถส่งมอบงานตามกำหนดในแต่ละงวด ให้คิดค่าปรับในอัตราร้อยละ 0.1 (หนึ่งในพัน) ของมูลค่างานในงวดนั้นต่อวัน นับตั้งแต่วันที่ครบกำหนดส่งมอบจนถึงวันที่ส่งมอบจริงและผ่านการตรวจรับ
3) ค่าปรับ SLA: กรณีระบบมี Downtime เกินกว่าที่กำหนด (Uptime ต่ำกว่า 99.9% ต่อเดือน) ผู้รับจ้างต้องขดเชยเครดิตค่าบริการรายเดือนในสัดส่วนที่เท่ากับเวลาที่หยุดให้บริการเกิน โดยเครดิตดังกล่าวจะหักออกจากงวดชำระเงินถัดไป