คุณลักษณะเฉพาะ

รายการ ระบบป้องกันไวรัส สำหรับเครื่องลูกข่ายเดิม โดยเป็นระบบที่มีความสามารถมากขึ้น

จำนวน 1 ระบบ

วัตถุประสงค์ ทดแทนระบบป้องกันไวรัส สำหรับเครื่องลูกข่าย เดิม โดยเป็นระบบที่มีความสามารถมากขึ้น

งบประมาณ 7,491,600 บาท

แบบที่ 1: ระบบ Endpoint Protection สำหรับเครื่องคอมพิวเตอร์ลูกข่าย จำนวนไม่น้อยกว่า 2,800 สิทธิ์

1. เป็น Endpoint Protection ที่สามารถตรวจจับภัยคุกคาม และป้องกันแบบหลายชั้น (Multi-Layer Protection)
2. มี Agent Software ที่สามารถติดตั้งได้บน Platform ได้ดังต่อไปนี้
   - 2.1 Windows 10, 11 และ Win Server 2012-2025
   - 2.2 Linux Debian, CentOS, Fedora Server, openSUSE, Oracle Linux, Red Hat Enterprise Linux, Rocky Linux, SUSE Linux Enterprise Server, Ubuntu
   - 2.3 MacOS
3. สามารถติดตั้งบนเครื่อง Endpoint จำนวนไม่น้อยกว่า 2,800 สิทธิ์
4. Agent Software ที่นำเสนอต้องสามารถป้องกันการโจมตีที่ช่องโหว่ของระบบ (Exploit Prevention) ซึ่งรองรับ Platform Windows, Linux และ MacOS
5. Agent Software ที่นำเสนอต้องสามารถป้องกันมัลแวร์ หรือไวรัส (Malware Prevention หรือ Antivirus)
6. Agent Software ที่นำเสนอต้องสามารถป้องกันการโจมตีของมัลแวร์ระดับสูง ที่ใช้เทคนิคโจมตีแบบไม่ใช้ไฟล์ (Fileless Attacks)
7. Agent Software ที่นำเสนอต้องสามารถป้องกันการโจมตีโดยใช้การวิเคราะห์พฤติกรรม (Behavioural Threat Protection)
8. Agent Software ที่นำเสนอต้องสามารถป้องกันมัลแวร์เรียกค่าไถ่ (Ransomware Protection)
9. Agent Software ที่นำเสนอต้องสามารถป้องกัน Exploit และ Malware ในกรณีที่ไม่สามารถติดต่อกับ Management Console ได้ (Offline)
10. สามารถแสดงข้อมูลเหตุการณ์ภัยคุกคามทางไซเบอร์ โดยมีรายละเอียด อย่างน้อยดังนี้
    1. ระบุประเภทของภัยคุกคาม
    2. ระบุระดับความรุนแรง (Severity)
    3. ค่า Artifact, IP address, Host และ Username ที่เกี่ยวข้องกับเหตุการณ์
11. มีวิธีการในการตอบสนองต่อภัยคุกคาม (Response) อย่างน้อยดังนี้
    - 11.1 แยกหรือตัดการเชื่อมต่อเครื่องคอมพิวเตอร์ลูกข่าย (Isolate Endpoint) ได้หลายๆ เครื่องพร้อมๆกัน ผ่านหน้า management console
    - 11.2 สามารถสั่งการดำเนินการ Live Terminal จาก Management Console ได้ และสามารถสั่งการดำเนินการด้วย Python Script, PowerShell และ System command ผ่าน Terminal หรือ Remote Shell จาก Management Console
    - 11.3 เพิ่มค่า Hash ของไฟล์ที่ต้องการป้องกันได้ (Add to Block List)

12. สามารถทำงานร่วมกับ Cloud Sandbox และนำผลลัพธ์มาใช้ในการป้องกันได้
13. ระบบที่นำเสนอจะต้องทำงานมี SLA ไม่น้อยกว่า 99.9%
14. สามารถเก็บ Incident และ Alert Data ได้ไม่น้อยกว่า 180 วัน
15. สามารถกำหนด Password สำหรับถอดการติดตั้ง Agent จาก Management Console แบบโดยรวมหรือแยกราย Endpoint/Group หรือสามารถใช้ Temporary Token เพื่อป้องกันไม่ให้ User ถอนการติดตั้ง Agent software ได้
16. ระบบที่นำเสนอจะต้องสามารถรองรับเชื่อมต่อแบบ Single Sign-on เพื่อนำเข้าข้อมูลบัญชีผู้ใช้งานผ่านโปรโตคอล SAML 2.0 ได้
17. สามารถสร้างแดชบอร์ด หรือ Report ได้ ด้วย Predefined
18. มีความสามารถในการแจ้งเตือน (Alerts, Incidents, Audit agent/management log) ผ่าน Email, Slack และ SYSLOG โดยสามารถเลือกจาก Severity Level ได้เป็นอย่างน้อย
19. ระบบที่นำเสนอจะต้องสามารถบริหารจัดการการเข้าใช้แบบ และ role-based access control (RBAC) และ scope-based access control (SBAC) ได้
20. ระบบที่เสนอต้องอยู่ในกลุ่ม Leader ของ Gartner Magic Quadrant for EPP 2025 และ The Forrester Wave™: Extended Detection And Response Platform, Q2 2024
21. มีการรับประกันสินค้าจากเจ้าของผลิตภัณฑ์รวมทั้งสิทธิ์ในการอัพเกรดระบบที่นำเสนอเป็นเวลาไม่น้อยกว่า 5 ปี
22. มีการฝึกอบรมเจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศ ให้สามารถบริการจัดการ ดูแล รวมถึงการ Update / Upgrade อย่างน้อย 1 วันทำการ
23. มีการประชุมร่วมกับเจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศ อย่างน้อย ทุก 6 เดือน เพื่อตรวจสอบการตั้งค่า ให้คำแนะนำด้านความปลอดภัยของเครื่องลูกข่ายที่ใช้งานผลิตภัณฑ์
24. ผู้เสนอราคาต้องมีหนังสือสนับสนุนทางด้านเทคนิคและการให้บริการจากเจ้าของผลิตภัณฑ์ที่นำเสนอจากบริษัทเจ้าของผลิตภัณฑ์โดยตรง ในการนำเสนองานครั้งนี้เพื่อรับรองว่าผู้ขายสามารถให้คำปรึกษาทางด้านเทคนิครวมถึงการติดตั้งให้เป็นไปตามวัตถุประสงค์ของโครงการและการให้บริการอย่างมีประสิทธิภาพ โดยมีหนังสือแนบมา ณ วันยื่นเสนอราคา

แบบที่ 2: ระบบ Endpoint Detection and Response สำหรับเครื่องแม่ข่าย จำนวนไม่น้อยกว่า 200 สิทธิ์

1. สามารถติดตั้งบนเครื่อง Endpoint จำนวนไม่น้อยกว่า 200 สิทธิ์
2. สามารถแสดงเทคนิคของภัยคุกคามที่ตรวจพบ โดยเทียบเคียงกับ MITRE ATT&CK stage ต่าง ๆ
3. รองรับการ Custom จากการ Query ด้วย XQL เพื่อแสดงข้อมูลในรูปแบบตาราง หรือ Graph/Chart
4. ระบบที่เสนอต้องผ่านการประเมินจาก MITRE ATT&CK Evaluations ปี 2024 (Enterprise) หรือล่าสุด แบบครอบคลุม Technique (80 ครั้ง) โดยผลการตรวจจับที่ไม่มีการเปลี่ยนแปลงค่า (Configuration Change) โดยอ้างอิงจากข้อมูลที่แสดง บนเว็บไซต์ MITRE ATT&CK
5. รองรับการสแกนช่องโหว่ (Vulnerability Scan) บน Windows OS และ Linux OS
6. สามารถสร้าง Indicator of Compromise (IOC) เพื่อตรวจจับ Artifacts ที่ต้องการตรวจจับ เช่น IP, Domain, Hash File, File Path ที่องค์กรต้องการเฝ้าระวังจากเหตุการณ์ที่เคยเกิดขึ้นและคาดว่าจะเกิดได้

7. สามารถตรวจจับรูปแบบของพฤติกรรม (Behavioral Indicator : BIOC) ที่ต้องการกำหนดได้ (Custom Behavioral Indicator)
8. สามารถค้นหาข้อมูลการใช้งาน Source IP address, Domain และ Event ที่เกี่ยวข้องกับข้อมูลการใช้งาน (Activity) ได้
9. เป็น Endpoint Protection ที่สามารถตรวจจับภัยคุกคาม และป้องกันแบบหลายชั้น (Multi-Layer Protection)
10. มี Agent Software ที่สามารถติดตั้งได้บน Platform ได้ดังต่อไปนี้
    10.1 Windows 10, 11 และ Win Server 2012-2025
    10.2 Linux Debian, CentOS, Fedora Server, openSUSE, Oracle Linux, Red Hat Enterprise Linux, Rocky Linux, SUSE Linux Enterprise Server, Ubuntu
    10.3 MacOS

11. Agent Software ที่นำเสนอต้องสามารถป้องกันการโจมตีที่ช่องโหว่ของระบบ (Exploit Prevention) ซึ่งรองรับ Platform Windows, Linux และ MacOS
12. Agent Software ที่นำเสนอต้องสามารถป้องกันมัลแวร์ หรือไวรัส (Malware Prevention หรือ Antivirus)
13. Agent Software ที่นำเสนอต้องสามารถป้องกันการโจมตีของมัลแวร์ระดับสูง ที่ใช้เทคนิคโจมตีแบบไม่ใช้ไฟล์ (Fileless Attacks)
14. Agent Software ที่นำเสนอต้องสามารถป้องกันการโจมตีโดยใช้การวิเคราะห์พฤติกรรม (Behavioural Threat Protection)
15. Agent Software ที่นำเสนอต้องสามารถป้องกันมัลแวร์เรียกค่าไถ่ (Ransomware Protection)
16. Agent Software ที่นำเสนอต้องสามารถป้องกัน Exploit และ Malware ในกรณีที่ไม่สามารถติดต่อกับ Management Console ได้ (Offline)
17. สามารถแสดงข้อมูลเหตุการณ์ภัยคุกคามทางไซเบอร์ โดยมีรายละเอียด อย่างน้อยดังนี้
    4. ระบุประเภทของภัยคุกคาม
    5. ระบุระดับความรุนแรง (Severity)
    6. ค่า Artifact, IP address, Host และ Username ที่เกี่ยวข้องกับเหตุการณ์
18. มีวิธีการในการตอบสนองต่อภัยคุกคาม (Response) อย่างน้อยดังนี้
    19. แยกหรือตัดการเชื่อมต่อเครื่องคอมพิวเตอร์ลูกข่าย (Isolate Endpoint) ได้หลายๆ เครื่องพร้อมๆกัน ผ่านหน้า management console
    20. สามารถสั่งการดำเนินการ Live Terminal จาก Management Console ได้ และสามารถสั่งการดำเนินการด้วย Python Script, PowerShell และ System command ผ่าน Terminal หรือ Remote Shell จาก Management Console
    21. เพิ่มค่า Hash ของไฟล์ที่ต้องการป้องกันได้ (Add to Block List)
22. สามารถทำงานร่วมกับ Cloud Sandbox และนำผลลัพธ์มาใช้ในการป้องกันได้
23. ระบบที่นำเสนอจะต้องทำงานมี SLA ไม่น้อยกว่า 99.9%
24. สามารถเก็บ Incident และ Alert Data ได้ไม่น้อยกว่า 180 วัน

25. สามารถกำหนด Password สำหรับถอดการติดตั้ง Agent จาก Management Console แบบโดยรวมหรือแยกราย Endpoint/Group หรือสามารถใช้ Temporary Token เพื่อป้องกันไม่ให้ User ถอนการติดตั้ง Agent software ได้
26. ระบบที่นำเสนอจะต้องสามารถรองรับเชื่อมต่อแบบ Single Sign-on เพื่อนำเข้าข้อมูลบัญชีผู้ใช้งานผ่านโปรโตคอล SAML 2.0 ได้
27. สามารถสร้างแดชบอร์ด หรือ Report ได้ ด้วย Predefined
28. มีความสามารถในการแจ้งเตือน (Alerts, Incidents, Audit agent/management log) ผ่าน Email, Slack และ SYSLOG โดยสามารถเลือกจาก Severity Level ได้เป็นอย่างน้อย
29. ระบบที่นำเสนอจะต้องสามารถบริหารจัดการการเข้าใช้แบบ และ role-based access control (RBAC) และ scope-based access control (SBAC) ได้
30. ระบบที่เสนอต้องอยู่ในกลุ่ม Leader ของ Gartner Magic Quadrant for EPP 2025 และ The Forrester Wave™: Extended Detection And Response Platform, Q2 2024
31. มีการรับประกันสินค้าจากเจ้าของผลิตภัณฑ์รวมทั้งสิทธิ์ในการอัพเกรดระบบที่นำเสนอเป็นเวลาไม่น้อยกว่า 5 ปี
32. มีการฝึกอบรมเจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศ ให้สามารถบริการจัดการ ดูแล รวมถึงการ Update / Upgrade อย่างน้อย 1 วันทำการ
33. มีการประชุมร่วมกับเจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศ อย่างน้อย ทุก 6 เดือน เพื่อตรวจสอบการตั้งค่า ให้คำแนะนำด้านความปลอดภัยของเครื่องลูกข่ายที่ใช้งานผลิตภัณฑ์
34. ผู้เสนอราคาต้องมีหนังสือสนับสนุนทางด้านเทคนิคและการให้บริการจากเจ้าของผลิตภัณฑ์ที่นำเสนอจากบริษัทเจ้าของผลิตภัณฑ์โดยตรง ในการนำเสนองานครั้งนี้เพื่อรับรองว่าผู้ขายสามารถให้คำปรึกษาทางด้านเทคนิครวมถึงการติดตั้งให้เป็นไปตามวัตถุประสงค์ของโครงการและการให้บริการอย่างมีประสิทธิภาพ โดยมีหนังสือแนบมา ณ วันยื่นเสนอราคา
35. ผู้ขายจะต้องส่งมอบและติดตั้งให้ถูกต้องครบถ้วนตามที่ระบุไว้ในสัญญาพร้อมทั้งทดสอบระบบทั้งหมดให้แล้วเสร็จภายใน 90 วัน

เงื่อนไขการซ่อมครุภัณฑ์ในระยะประกัน

- รับประกันคุณภาพ 5 ปี นับจากวันที่ตรวจรับ
- หากครุภัณฑ์ชำรุดบกพร่องผู้ขายต้องดำเนินการแก้ไขให้ใช้งานได้ภายใน 7 วัน โดยนับจากวันที่คณะแพทย-ศาสตร์แจ้ง ให้ทราบทางโทรศัพท์หรือโทรสาร ก่อนเวลา 12.00 น. นับเป็นวันที่ 1 หาก หลัง 12.00 น. ให้นับวันถัดไปเป็นวันที่ 1
- หากผู้ขายซ่อมเกิน 7 วัน ผู้ขายต้องชำระค่าปรับวันละ 0.2% ของราคาเครื่อง/วัน จนกว่าจะซ่อมเสร็จให้ดีดังเดิม โดยชำระค่าปรับภายในกำหนดเวลาที่คณะแพทยศาสตร์มีหนังสือแจ้ง หรือไม่ต้องชำระค่าปรับหาก มีเครื่องสำรองให้ใช้ทดแทนระหว่างดำเนินการซ่อม
- นอกเหนือจากการปรับข้างต้น หากในระยะประกันครุภัณฑ์ชำรุดและต้องใช้เวลาซ่อมให้ดีดังเดิมมากกว่า 7 วัน เกิน 3 ครั้ง/ปี ผู้ขายต้องเปลี่ยนเครื่องใหม่ ให้คณะแพทยศาสตร์ ภายใน 60 วัน นับจากวันที่ คณะแพทยศาสตร์มีหนังสือแจ้งให้เปลี่ยน โดยครุภัณฑ์ใหม่ต้องเป็นเครื่องใหม่ที่มีคุณภาพไม่ต่ำกว่าครุภัณฑ์เดิม