ระบบวิเคราะห์และจัดการข้อมูลความปลอดภัยสารสนเทศ
แขวงคลองเตยเหนือ เขตวัฒนา กรุงเทพมหานคร จำนวน 1 ระบบ
สำนักคอมพิวเตอร์ มหาวิทยาลัยศรีนครินทรวิโรฒ

รายละเอียดคุณลักษณะเฉพาะ

1. เป็นระบบสำหรับวิเคราะห์ข้อมูล ตรวจสอบและตอบสนองต่อภัยคุกคามภายในระบบเครือข่ายคอมพิวเตอร์ ที่สามารถทำงานร่วมกับอุปกรณ์อื่น ๆ ได้
2. สามารถวิเคราะห์ภัยคุกคามทางไซเบอร์ที่เกิดขึ้นได้ไม่น้อยกว่า 6,500 EPS
3. สามารถติดตั้งแบบ On-premise ในรูปแบบ Virtualization ได้
4. สามารถนำเข้าข้อมูล (Log) จาก อุปกรณ์ Network เพื่อตรวจสอบภัยคุกคาม เช่น Network Security Log ,HTTP และ DNS Audit Log ได้เป็นอย่างน้อย
5. สามารถนำเข้าข้อมูล (Log) จาก Endpoint เพื่อตรวจสอบภัยคุกคาม เช่น Process termination, DNS query, File creation, Port monitoring, Scheduled task creation, Service creation และ Service deletion ได้เป็นอย่างน้อย
6. สามารถนำเข้าข้อมูล (Log) จาก เครื่องคอมพิวเตอร์แม่ข่าย เพื่อตรวจสอบภัยคุกคาม เช่น Windows server และ Linux server ได้เป็นอย่างน้อย
7. สามารถนำเข้าข้อมูล (Log) จากการระบบเครือข่ายคอมพิวเตอร์ เพื่อตรวจสอบภัยคุกคาม โดยผ่าน Security sensor หรือ Virtual sensor โดยต้องเสนออุปกรณ์รวบรวมข้อมูลภายในระบบเครือข่าย Security Sensor หรือ Virtual sensor เพื่อรวบรวมข้อมูลภายในระบบเครือข่ายได้ โดยมีคุณสมบัติของ Sensor ดังนี้
   7.1 มี throughput ไม่น้อยกว่า 2 Gbps
   7.2 สามารถรวบรวมข้อมูลภายในระบบเครือข่ายด้วยวิธีการ SPAN หรือ Mirrored Traffic จากอุปกรณ์ Switch ได้
   7.3 เป็น Sensor หรือ Network Traffic Analysis หรือ Event Receiver หรือ Event/Flow Collector หรือเทียบเท่าสำหรับวิเคาะห์ Logs หรือ Network Traffic จากตัวอุปกรณ์ต้นทาง และต้องไม่เป็นอุปกรณ์ประเภท Next Generation Firewall หรือ Intrusion Prevention System (IPS)
8. สามารถทำงานร่วมกับระบบ Cloud threat intelligence ได้
9. มีระบบตรวจสอบ สำหรับวิเคราะห์การโจมตี ดังนี้ AI intelligence analysis engine, Behavior engine , Ransomware protection, Fileless protection , IOA (Indicator of Attack) และ IOC (Indicator of Compromise) ได้เป็นอย่างน้อย

10. สามารถรับข้อมูล (Collect logs) ผ่าน Protocol มาตรฐาน เช่น Syslog, FTP เพื่อรับข้อมูลจากอุปกรณ์ภายนอกเช่น Anti-DDOS, DLP (Data Loss Prevention), IPS, WAF (Web Application Firewall), Firewall เป็นต้น
11. สามารถทำ Incident Response เพื่อตอบสนองต่อภัยคุกคามทั้งแบบ Manual หรือ Automation ผ่านระบบ SOAR โดยมีชุดข้อมูลแบบ Pre-defined มาให้ในระบบ และสามารถแก้ไขเพิ่มเติมได้ (Customization)
12. ระบบสามารถเชื่อมต่อไปยังอุปกรณ์ Firewall ของมหาวิทยาลัย เพื่อแก้ไข หรือสร้าง Policy เมื่อมีเหตุการณ์ผิดปกติเกิดขึ้น
13. ระบบสามารถแจ้งเหตุการณ์การโจมตี โดยบอกรายละเอียดของ Incident ที่เกิดขึ้น รวมไปถึงสามารถบอกรายละเอียดของ Process ของเครื่องที่ติดตั้ง endpoint บนหน้าจอ Dashboard ได้
14. รองรับการทำงานร่วมกับ NGFW ที่ใช้อยู่ในปัจจุบัน เพื่อตอบสนองต่อเหตุการณ์ด้านความปลอดภัยได้แบบอัตโนมัติ
15. ระบบสามารถเชื่อมต่อไปยังอุปกรณ์ EDR (Endpoint Detection and Response) เพื่อสั่ง Scan Virus หรือนำเครื่องออกจากระบบ (Isolate/Quarantine)) เมื่อมีเหตุการณ์ผิดปกติเกิดขึ้น
16. หน้าจอของระบบ สามารถสรุปรายละเอียดของภัยคุกคามโดยเปรียบเทียบกับเทคนิคการโจมตีในมาตรฐานของ MITRE ATT&CK Framework ได้
17. มีความสามารถในการทำ Asset Management เครื่องที่ติดตั้ง Endpoint เพื่อช่วยตรวจสอบข้อมูลที่เกิดขึ้นเช่น Open ports, Web application, Account information, Running process เป็นต้น
18. สามารถตรวจสอบความเสี่ยง หรือช่องโหว่ในระบบได้ (Vulnerability) โดยมีข้อมูลประกอบเช่น Vulnerability name, Vulnerability type, Discovery time, CVE-ID เป็นต้น
19. รองรับการสร้างรายงาน (Report) สำหรับสรุปภาพรวม Security ได้ และสามารถ Export Report ออกจากระบบได้
20. หน้าจอของระบบ (Dashboard) สามารถแสดงผล โดยมีรายละเอียดอย่างน้อยต่อไปนี้
    20.1 Security Alerts
    20.2 Security Incidents
    20.3 Vulnerabilities
    20.4 Alert Severity
    20.5 Source IP, Destination IP
    20.6 Attack result
21. ระบบรองรับการทำงานในรูปแบบ Cluster หรือ N+1 เพื่อ Balance การใช้งาน resource ของระบบ และสามารถเพิ่ม Node เพื่อรองรับการขยายตัวในอนาคต

22. ผู้ยื่นข้อเสนอต้องเสนอเครื่องคอมพิวเตอร์แม่ข่ายสำหรับติดตั้งระบบฯ จำนวน 3 เครื่อง โดยแต่ละเครื่องมีคุณสมบัติทางเทคนิคดังต่อไปนี้
    22.1 มีหน่วยประมวลผลกลาง (CPU) แบบ Intel ไม่น้อยกว่า 16 Core หรือดีกว่า ไม่น้อยกว่า 1 หน่วย
    22.2 มีหน่วยความจำหลัก (RAM) ความจุรวมไม่น้อยกว่า 128 GB หรือดีกว่า
    22.3 มี Storage แบบ SATA HDD ที่มีขนาดความจุก่อนฟอร์แมตต่อหน่วยไม่น้อยกว่า 4 TB จำนวน 12 หน่วย
    22.4 มีช่องเชื่อมต่อเครือข่าย 10 Gigabit Ethernet แบบ SFP+ ไม่น้อยกว่า 2 พอร์ต
    22.5 มี Transceiver แบบ Multimode 10 GBASE-SR SFP module ไม่น้อยกว่า 2 ชุด
    22.6 มีช่องเชื่อมต่อเครือข่าย 1 Gigabit Ethernet ไม่น้อยกว่า 4 พอร์ต
    22.7 เครื่องคอมพิวเตอร์แม่ข่ายฯ ที่เสนอมีความสูงไม่เกินไม่น้อยกว่า 2 U แบบ Rack Mount โดยสามารถติดตั้งเข้ากับตู้ Rack มาตรฐานขนาด 19 นิ้วได้
23. ติดตั้งที่ห้องคอมพิวเตอร์กลาง สำนักคอมพิวเตอร์ ชั้น 2 อาคารคณะศิลปกรรรมศาสตร์
24. ผู้ยื่นข้อเสนอจะต้องมีหนังสือแสดงการเป็นผู้มีสิทธิจำหน่ายผลิตภัณฑ์ที่เสนอจากผู้ผลิตหรือจากสาขาของผู้ผลิตในประเทศไทย โดยให้ยื่นหนังสือพร้อมยื่นข้อเสนอ และมหาวิทยาลัยขอสงวนสิทธิ์ในการตรวจสอบเอกสาร
25. รับประกันไม่น้อยกว่า 3 ปีแบบ Onsite Services
