

ระบบป้องกันการโจมตีทางเครือข่าย(Firewall)

จำนวน 1 ระบบ

มีรายละเอียดคุณลักษณะดังต่อไปนี้

### ข้อกำหนดทั่วไป

จัดหาและติดตั้งอุปกรณ์ ดังนี้

- 1) อุปกรณ์รักษาความปลอดภัยระบบเครือข่าย (NGFW) จำนวน 1 ชุด
- 2) ระบบซอฟต์แวร์บริหารจัดการอุปกรณ์รักษาความปลอดภัย (Firewall) จำนวน 1 ชุด
- 3) ระบบวิเคราะห์ระบบเฝ้าระวังและป้องกันภัยคุกคามไซเบอร์อัจฉริยะ จำนวน 1 ระบบ

### ข้อกำหนดคุณลักษณะเฉพาะด้านเทคนิค

จัดหาและติดตั้งระบบป้องกันการโจมตีทางเครือข่าย(Firewall)  
มีคุณลักษณะเฉพาะขั้นต่ำ เทียบเท่าหรือดีกว่า ดังนี้

1. อุปกรณ์รักษาความปลอดภัยระบบเครือข่าย (NGFW) จำนวน 1 ชุด

โดยมีคุณสมบัติเฉพาะขั้นต่ำหรือเทียบเท่าหรือดีกว่าดังต่อไปนี้

1.1 เป็นอุปกรณ์ Next-generation Firewall (NGFW) ทำหน้าที่ตรวจจับและควบคุม Application, User, Content โดยเฉพาะ (Application Firewall)

1.2 เป็นอุปกรณ์ที่ออกแบบมาเป็น Chassis หรือ เป็นอุปกรณ์แบบ Appliance ที่แยกหน่วยประมวลผลสำหรับการบริหารจัดการ (Control Plane หรือ Management Plane) และ หน่วยประมวลผลสำหรับการจัดการข้อมูล (Data Plane) ออกจากกันภายในตัวอุปกรณ์

1.3 มี Threat Prevention Throughput ไม่น้อยกว่า 5 Gbps ในแบบ appmix หรือ Enterprise testing condition หรือ Enterprise traffic mix โดยสามารถรองรับ Max Sessions ได้ไม่น้อยกว่า 1.2M sessions และ New Sessions ไม่น้อยกว่า 120,000 session ต่อวินาที

1.4 มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) รายละเอียดอย่างน้อยดังนี้

1.4.1 ช่องเชื่อมต่อแบบ 1G/2.5G/5G/10G หรือดีกว่า ไม่น้อยกว่า 12 ช่อง

1.4.2 ช่องเชื่อมต่อแบบ 1G/10Gt SFP/SFP+ หรือดีกว่า ไม่น้อยกว่า 10 ช่อง

1.4.3 ช่องเชื่อมต่อแบบ 25G SFP28 หรือดีกว่า ไม่น้อยกว่า 4 ช่อง

1.4.4 ช่องเชื่อมต่อสำหรับบริหารจัดการโดยเฉพาะ (Out of Band Management) ไม่น้อยกว่า 1 ช่อง

1.4.5 ช่องเชื่อมต่อแบบ 10G SFP+ สำหรับ High Availability ไม่น้อยกว่า 1 ช่อง

1.5 สามารถทำ Routing แบบ Static, RIP, BGP, OSPF, Multicast และ Policy Based แบบ Policy based Forwarding หรือ Policy based Routing ได้เป็นอย่างดี

1.6 สามารถทำการตรวจสอบทราฟฟิกที่เข้ารหัส SSL ด้วยการทำ SSL decryption (ทั้งแบบ Inbound และ Outbound ) รวมทั้งการทำ decryption mirroring และ SSL decryption broker หรือ Network Packet Broker หรือ SSL Security Service Chain ได้ หรือนำเสนออุปกรณ์ภายนอกเพิ่มเติมเพื่อให้สามารถทำงานได้ตามข้อกำหนด

1.7 สามารถรับ syslog จากอุปกรณ์อื่น เช่น Wireless controller, Proxy Server, และ Network Access Control เพื่อใช้ในการพิสูจน์ตัวตนของผู้ใช้แต่ละคน (IP address to username mappings) ได้ เพื่อใช้ในการยืนยันตัวตน ของ User ที่ใช้งาน โดยรองรับทั้ง User Log-in และ User Log-out ได้บนตัวอุปกรณ์

หรือนำเสนออุปกรณ์ภายนอกเพิ่มเติมเพื่อให้สามารถทำงานได้ตามข้อกำหนด



1.8 รองรับการทำให้ Virtual Systems หรือ Virtual Domains ไม่น้อยกว่า 11 Virtual Systems หรือ Virtual Domains

1.9 สามารถป้องกันภัยคุกคามประเภท Vulnerability, Exploits, C2 และ Spyware ได้โดยสามารถมีการอัปเดต Signature ใหม่แบบอัตโนมัติ

1.10 สามารถเรียกดูสรุปข้อมูลของ Data ในรูปแบบของกราฟฟิคได้ และสามารถทำรายงานต่างๆ ได้ หรือ เสนออุปกรณ์อื่นเพิ่มเติมเพื่อให้สามารถทำงานได้อย่างน้อยดังนี้

1.10.1 Top Application, Application Category

1.10.2 Top Source, User, Destination

1.10.3 User activity report

1.10.4 สามารถทำรายงานรวมถึงปรับแต่งรายงานตามความต้องการในรูปแบบ PDF ได้เป็นอย่างดี พร้อมทั้งตั้งเวลาส่งรายงานผ่านทาง Email แบบอัตโนมัติได้ หรือนำเสนออุปกรณ์ภายนอกเพิ่มเติมเพื่อให้สามารถทำงานได้ตามข้อกำหนด

1.11 รองรับการติดตั้งแบบ HA (High Availability) ในรูปแบบ Active - Active และ Active - Passive

1.12 มีแหล่งจ่ายไฟฟ้า (Power Supply) แบบ Redundant

1.13 ต้องได้รับการรับรองมาตรฐาน FCC และ VCCI เป็นอย่างน้อย

1.14 ต้องได้รับการจัดอันดับให้อยู่ในกลุ่ม Leader ของ Gartner Magic Quadrant ในกลุ่มผลิตภัณฑ์ Network Firewalls ปี 2022 หรือปีล่าสุด

1.15 ผู้ยื่นข้อเสนอต้องได้รับการสนับสนุนทางเทคนิคจากบริษัทผู้ผลิต โดยแสดงเอกสารรับรองการสนับสนุนที่ระบุชื่อโครงการนี้ ว่าอุปกรณ์ที่เสนอเป็นอุปกรณ์ใหม่ที่ยังมิได้ทำการติดตั้งใช้งาน ณ ที่ใดมาก่อน และไม่เป็นเครื่องที่ถูกนำมาปรับปรุงสภาพใหม่ (Reconditioned หรือ Rebuilt) และยังอยู่ในสายการผลิต

2. ระบบซอฟต์แวร์บริหารจัดการอุปกรณ์รักษาความปลอดภัย (Firewall) จำนวน 1 ชุด โดยมีคุณสมบัติเฉพาะขั้นต่ำหรือเทียบเท่าหรือดีกว่าดังต่อไปนี้

2.1 เป็นอุปกรณ์บริหารจัดการอุปกรณ์รักษาความปลอดภัยเครือข่ายแบบรวมศูนย์ (Centralized Management Firewall) ในรูปแบบของ Virtual Appliance หรือดีกว่า

2.2 ระบบสามารถบริหารจัดการอุปกรณ์รักษาความปลอดภัยเครือข่ายที่นำเสนอได้ ไม่น้อยกว่า 25 หน่วย

2.3 สามารถเก็บ Log ของอุปกรณ์ Firewall ในข้อ 1 ได้

2.4 มีระบบการพิสูจน์ตัวตนของผู้ดูแลระบบ (Administrator) โดยใช้ฐานข้อมูลจาก Local Database, LDAP และ RADIUS ได้เป็นอย่างดี

2.5 ระบบสามารถทำการบริหารจัดการผ่านทาง Web Interface และ SSH ได้เป็นอย่างดี

2.6 สามารถเรียกดูสรุปข้อมูลของ Applications, URL Categories, Threats และ Data ในรูปแบบของกราฟฟิคได้

2.7 สามารถทำรายงาน รวมถึงปรับแต่งรายงานตามความต้องการ ในรูปแบบ PDF ได้เป็นอย่างดี พร้อมทั้งตั้งเวลาส่งรายงานผ่านทาง Email แบบอัตโนมัติได้

2.8 สามารถสร้าง Role-based administration เพื่อกำหนดสิทธิของการเข้าถึงตัวอุปกรณ์ได้ เช่น Read-only เป็นต้น

2.9 ต้องเป็นอุปกรณ์ภายใต้เครื่องหมายการค้าเดียวกันกับอุปกรณ์รักษาความปลอดภัย (Firewall) ในข้อ 1.



2.10 ผู้ยื่นข้อเสนอต้องได้รับการสนับสนุนทางเทคนิคจากบริษัทผู้ผลิต โดยแสดงเอกสารรับรอง

2.11 ต้องสามารถจัดเก็บ log ได้ไม่น้อยกว่า 1 ปี รับประกัน 5 ปี

3. ระบบวิเคราะห์ระบบเฝ้าระวังและป้องกันภัยคุกคามไซเบอร์อัจฉริยะ จำนวน 1 ระบบ โดยมีคุณลักษณะอย่างน้อย ดังนี้

3.1 เป็น Platform ที่มีความสามารถในการตรวจหาภัยคุกคามที่เกิดขึ้นในองค์กร (Threat Hunting) และหาข้อมูลความเกี่ยวข้องของภัยคุกคามที่เกิดขึ้น (Investigation) ของเครื่องคอมพิวเตอร์ลูกข่าย แม่ข่าย และเครือข่ายได้

3.2 Agent Software

ต้องสามารถป้องกันภัยคุกคามที่เกิดขึ้นบนเครื่องคอมพิวเตอร์ลูกข่าย จำนวนไม่น้อยกว่า 200 ลิขสิทธิ์ โดยมีความสามารถด้านการป้องกันภัยคุกคาม ดังนี้

3.3 ป้องกันการโจมตีที่ช่องโหว่ของระบบ (Exploit Prevention)

3.4 ป้องกันมัลแวร์ หรือไวรัส (Malware Prevention หรือ Antivirus)

3.5 ป้องกันการโจมตีของมัลแวร์ระดับสูง ที่ใช้เทคนิคโจมตีแบบไม่ใช้ไฟล์ (Fileless Attacks)

3.6 ป้องกันการโจมตีโดยใช้เทคนิคของ (AI-based local analysis engine) หรือ Machine Learning

3.7 ป้องกันการโจมตีโดยใช้การวิเคราะห์พฤติกรรม (Behavior)

3.8 ป้องกันมัลแวร์เรียกค่าไถ่ (Ransomware Protection)

3.9 Agent Software ต้องสามารถป้องกัน Exploit และ Malware ในกรณีที่ไม่สามารถติดต่อกับ Management Console ได้ (Offline)

3.10 สามารถค้นหาข้อมูลโดยรองรับการสร้าง Rule เพื่อตรวจจับภัยคุกคามเครื่องคอมพิวเตอร์ลูกข่ายจาก Indicators of compromise (IOCs) และ Behavioral indicators of compromise (BIOCs)

3.11 แสดงข้อมูลเหตุการณ์ภัยคุกคามทางไซเบอร์ โดยมีรายละเอียด อย่างน้อยดังนี้

3.11.1 ระบุประเภทของภัยคุกคาม

3.11.2 วัน-เวลา เริ่มต้นและสิ้นสุดของภัยคุกคาม

3.11.3 ระบุต้นทาง (Source) ปลายทาง (Destination)

3.11.4 ระบุระดับความรุนแรง (Severity)

3.11.5 รายละเอียดเหตุการณ์และพฤติกรรม

3.11.6 ค่าคะแนน (Scoring) ของภัยคุกคามเมื่อเกิดขึ้นกับ IP address, Host และ Username ที่มีความสำคัญสูง ได้เป็นอย่างน้อย

3.11.7 สามารถแสดงเทคนิคของภัยคุกคามที่ตรวจพบ โดยเทียบเคียงกับ MITRE ATT&CK stage ต่าง ๆ

3.12 ระบบ Detection and Response ในการตรวจจับภัยคุกคาม และรวบรวมข้อมูลจากกิจกรรมต่างๆ ที่เกิดขึ้น โดยทั้งระบบที่นำเสนอต้องมีความสามารถรวมกัน อย่างน้อยดังนี้

3.12.1 Endpoint Detection and Response (EDR) (ตรวจจับและตอบสนองต่อเครื่องแม่ข่าย)

3.12.2 Root Cause Analysis (วิเคราะห์หาต้นตอของปัญหาที่เกิดขึ้น)

3.12.3 Timeline analysis of alerts (สามารถแสดง Timeline ของเหตุการณ์ที่เกิดขึ้น)

3.12.4 Threat Hunting (การตรวจหาภัยคุกคาม อาจเกิดขึ้นในองค์กร)



3.12.5 Incident response and recovery  
(ตอบสนองและกู้คืนระบบจากเหตุการณ์ที่เกิด)

3.12.6 User Behavior Analytics (UBA) หรือ User and Entity Behavior Analytics (UEBA) (ระบบวิเคราะห์สิ่งผิดปกติจากพฤติกรรมของผู้ใช้งาน)

3.13 มีวิธีการในการตอบสนองต่อภัยคุกคาม (Response) อย่างน้อยดังนี้

3.13.1 แยกหรือตัดการเชื่อมต่อเครื่องคอมพิวเตอร์ลูกข่าย (Isolate Endpoint) ได้หลายๆเครื่องพร้อมๆกัน ผ่านหน้า management console

3.13.2 ควบคุมเครื่องคอมพิวเตอร์ลูกข่ายผ่าน Terminal (Live Terminal) หรือหยุดการทำงานของ Process บนเครื่องคอมพิวเตอร์ลูกข่าย (Terminate Process)

3.13.3 เพิ่มค่า Hash ของไฟล์ที่ต้องการป้องกันได้ (Add to Block List)

3.14 สามารถทำงานร่วมกับ Cloud Sandbox หรือ On-Premise Sandbox เพื่อวิเคราะห์ภัยคุกคาม และนำผลลัพธ์มาใช้ในการป้องกันได้ กรณีที่ต้องทำงานร่วมกับ On-Premise Sandbox หรือมีลิขสิทธิ์ในการใช้งานให้เสนอพร้อมใช้งานโดยให้ครอบคลุมและเพียงพอต่อการทำงาน

3.15 สามารถกำหนด Password สำหรับถอดการติดตั้ง Agent จาก Management Console เพื่อป้องกันไม่ให้ User ถอนการติดตั้ง Agent software ได้

3.16 สามารถตรวจสอบช่องโหว่ของระบบปฏิบัติการ (Vulnerability Assessment) บนระบบปฏิบัติการ Windows และ Linux โดยอ้างอิงช่องโหว่ตาม Common Vulnerabilities and Exposures (CVE) โดยไม่ต้องติดตั้ง Agent เพิ่มเติม

3.17 ระบบที่นำเสนอจะต้องสามารถรองรับเชื่อมต่อแบบ Single Sign-on เพื่อนำเข้าข้อมูลบัญชีผู้ใช้งานผ่านโปรโตคอล SAML 2.0 ได้

3.18 สามารถสร้างแดชบอร์ดโดยใช้ XQL (XDR Query Language) มาเป็นเงื่อนไขในการ Filter ข้อมูล

3.19 สามารถวิเคราะห์ตรวจจับภัยคุกคามบนระบบเครือข่ายโดยใช้เทคโนโลยี Machine learning และ AI

ในการวิเคราะห์พฤติกรรมที่เกิดขึ้นโดยการหาความสัมพันธ์ของข้อมูลที่ได้มาจากเครื่อง Endpoint, Log ของอุปกรณ์ตรวจจับภัยคุกคามเครือข่ายระดับแอปพลิเคชัน (Network Sensor), Windows Event Log, AWS Audit Log, Azure Audit Log, GCP Audit Log เป็นต้น

3.20 ระบบที่นำเสนอต้องผ่านการประเมินทดสอบของ The Forrester New Wave™: Extended Detection And Response (XDR) Providers, Q4 2024 โดยถูกจัดให้อยู่ใน Leaders หรือ Strong Performers ได้เป็นอย่างน้อย

3.21 ผู้ยื่นข้อเสนอต้องได้รับการสนับสนุนทางเทคนิคจากบริษัทผู้ผลิต โดยแสดงเอกสารรับรอง ว่าซอฟต์แวร์ที่นำเสนอมีลิขสิทธิ์ถูกต้อง และมีสิทธิ์ในการใช้งานไม่น้อยกว่า 5 ปี

#### ข้อกำหนดการติดตั้งส่งมอบ

#### 4 เงื่อนไขการติดตั้งและการส่งมอบ

4.1 ติดตั้งระบบป้องกันการโจมตีทางเครือข่าย(Firewall) ในข้อ 1,2 และ 3 ให้ทำงานร่วมกันได้กับระบบเครือข่ายของศูนย์หัวใจสิริกิติ์ฯ ได้อย่างมีประสิทธิภาพ รวมถึงมีโมดูลและสาย patch เพื่อเชื่อมต่อสัญญาณต่างๆ ตามการใช้งานจริงอย่างเพียงพอ

4.2 ผู้เสนอราคาจะต้องมีพนักงานประจำที่ทำงานเฉพาะด้านเพื่อการติดตั้งและดูแลระบบ พร้อมแสดงเอกสารหลักฐานประกอบด้วย



4.2.1 ผู้จัดการโครงการ (Project Manager) จำนวน 1 คน  
ที่มีประสบการณ์ในการทำงานด้านระบบเครือข่ายคอมพิวเตอร์มาแล้วไม่น้อยกว่า 3 ปี  
โดยผู้จัดการโครงการจะต้องเข้ามาดูแลการดำเนินโครงการ

4.2.2 วิศวกรอุปกรณ์รักษาความปลอดภัยระบบเครือข่าย (Firewall Engineer)  
จำนวนไม่น้อยกว่า 1 คน ที่มีประสบการณ์ในการทำงานด้านนี้มาแล้วไม่น้อยกว่า 3 ปี หรือ ต้อง  
เคยมีใบรับรอง Certified ของผลิตภัณฑ์ ในระดับไม่ต่ำกว่าระดับ Professional

4.3 ผู้ชนะการประกวดราคาจะต้องทำการจัดการอบรมไม่น้อยกว่า ดังนี้

4.3.1 หลักสูตร PSE Professional Hardware Firewall  
ของผลิตภัณฑ์ให้แก่เจ้าหน้าที่ผู้รับผิดชอบของศูนย์หัวใจสิริกิติ์ จำนวนไม่น้อยกว่า 2 คน

4.3.2 สนับสนุนการสอบใบประกาศนียบัตรจากเจ้าของผลิตภัณฑ์ให้แก่  
เจ้าหน้าที่ผู้รับผิดชอบ อย่างน้อย 1 คน ให้ได้ Certified ภายในระยะเวลา 5 ปี  
(ตามการรับประกัน) หรือ สอบใบประกาศนียบัตรจำนวนไม่น้อยกว่า 2 ครั้ง

4.3.3 อบรมการใช้งานและติดตั้งซอฟต์แวร์ที่เกี่ยวข้องกับโครงการนี้

4.4 ผู้ชนะการประกวดราคาต้องจัดทำสต็อกเกอร์อย่างดีติดบนอุปกรณ์ที่ส่งมอบในครั้งนี้  
ทุกรายการ เครื่องละ 1 ชิ้นโดยข้อมูลบนสต็อกเกอร์ต้องแสดงชื่อของบริษัทผู้ขาย Serial number  
เลขที่สัญญา ชื่องานจ้าง วันเริ่มและวันสิ้นสุดการรับประกันผลิตภัณฑ์

4.5 ติดตั้งซอฟต์แวร์ Virtual Appliance ในข้อ 2 ให้สามารถเก็บ log ได้ไม่น้อยกว่า 1 ปี  
โดยคำนวณจาก ปริมาณ log ที่เกิดขึ้นจริง 1 วัน ที่เฉลี่ยจาก 7 วัน แล้วนำไปคูณ 365 วัน  
เป็นอย่างน้อย และผู้ชนะการประกวดราคาต้องรับประกันพื้นที่เก็บ log  
หากภายหลังใช้งานไปแล้วพบว่าพื้นที่เก็บ log ได้น้อยกว่า 1 ปี จะจัดต้องหา Disk , Storage หรือ  
cloud มาเติมให้จนเก็บ log ได้ครบ 1 ปีเหมือนเดิม ตลอดอายุการรับประกัน 5 ปี

4.6 ติดตั้งระบบวิเคราะห์ระบบเฝ้าระวังและป้องกันภัยคุกคามไซเบอร์อัจฉริยะ ในข้อ 3 ให้  
เครื่อง client สามารถอัพเดท Agent Software ผ่านเครือข่ายได้ แม้ไม่มี Internet  
ตลอดระยะเวลารับประกัน

4.7 ผู้ชนะการประกวดราคาต้องจัดทำแผนผังการเชื่อมต่อระบบ (System Diagram)  
และเอกสารเกี่ยวกับการกำหนดค่าของอุปกรณ์ (Configuration) จำนวนไม่น้อยกว่า 1 ชุด

4.8 ผู้ชนะการประกวดราคาจะต้องส่งมอบงานทั้งหมดภายใน 120 วัน

### ข้อกำหนดการรับประกัน

#### 5. การรับประกันความชำรุดบกพร่อง

5.1 ผู้ชนะการประกวดราคาต้องรับประกันอุปกรณ์ในโครงการเป็นเวลา 5 ปี  
โดยไม่คิดค่าใช้จ่ายใด ๆ ทั้งสิ้น นับตั้งแต่วันที่ตรวจรับสมบูรณ์ทั้งหมด

5.2 มีเครื่องสำรองให้ใช้งานถ้าต้องส่งอุปกรณ์ไปซ่อม

5.3 เวลาในการบำรุงรักษาระบบ ได้แก่วันจันทร์ – วันศุกร์ตั้งแต่เวลา 08.30 – 16.30 น.  
ให้มีช่างผู้ชำนาญในการให้บริการ ทำหน้าที่บำรุงรักษาและซ่อมแซมแก้ไขระบบและอุปกรณ์  
ให้อยู่ในสภาพใช้งานได้ต่อเนื่องตลอดระยะเวลาดังกล่าว และจะต้องดูแลบำรุงรักษาระบบ  
อย่างน้อย ปีละ 3 ครั้งเป็นเวลา 5 ปี

5.4 ผู้ชนะการประกวดราคาต้องมีวิศวกรเครือข่ายประจำที่สามารถทำการรีโมทมา  
แก้ไขปัญหาได้หากเกิดเหตุการณ์ด่วนขึ้น หรือตามที่ศูนย์หัวใจสิริกิติ์ฯ แจ้ง

5.5 ผู้ชนะการประกวดราคาต้องให้การสนับสนุนทางเทคนิค  
หรือร่วมซ่อมแผนในส่วนที่เกี่ยวข้องหากศูนย์หัวใจสิริกิติ์ฯ มีการซ่อมระบบสารสนเทศใช้งานไม่ได้

5.6 ศูนย์หัวใจสิริกิติ์ฯ  
สามารถร้องขอให้ปรับการตั้งค่าหรืออัปเดตซอฟต์แวร์ระบบต่างๆในโครงการนี้ได้  
ตลอดโดยไม่คิดค่าใช้จ่ายเพิ่มเติม ตลอดระยะเวลารับประกัน 5 ปี

