เอกสารหมายเลข ๒

รายละเอียดคุณลักษณะเฉพาะของอุปกรณ์ที่จัดซื้อ

รายละเอียดคุณลักษณะเฉพาะของอุปกรณ์ที่จัดซื้อ
โครงการปรับปรุงประสิทธิภาพการเฝ้าระวังภัยคุกคามด้าน Cyber Security

"ระบบเฝ้าระวังภัยคุกคาม" ที่กรมสรรพสามิต จัดซื้อในครั้งนี้ต้องเป็นของแท้ ของใหม่ ไม่เคยใช้งานมาก่อน ไม่เป็นของเก่าเก็บ ต้องอยู่ในสภาพที่จะใช้งานได้ทันทีและต้องเป็นรุ่นที่ยังอยู่ในสายการผลิต (Production Line) และจำหน่าย ณ วันยื่นข้อเสนอ โดยคุณลักษณะเฉพาะของ **"ระบบเฝ้าระวังภัยคุกคามด้าน Cyber Security"** จะต้องเหมาะสมกับลักษณะงานของกรมสรรพสามิตตามโครงการนี้ และสามารถทำงานร่วมกันและใช้งานร่วมกับระบบงานคอมพิวเตอร์ได้อย่างมีประสิทธิภาพ สะดวกต่อการใช้งาน โดยผู้ประสงค์จะเสนอราคาต้องเสนอระบบเฝ้าระวังภัยคุกคามที่มีคุณลักษณะเฉพาะไม่ต่ำกว่าที่ระบุในเอกสารนี้

เงื่อนไขทั่วไปในการติดตั้ง "ระบบเฝ้าระวังภัยคุกคาม"

ผู้ชนะการประกวดราคาต้องจัดหาอุปกรณ์หรือซอฟต์แวร์ที่จำเป็นสำหรับการทำงานของ "ระบบเฝ้าระวังภัยคุกคาม" ให้สามารถทำงานได้อย่างสมบูรณ์ โดยไม่คิดมูลค่าเพิ่มเติมจากราคาที่เสนอ

๑. เครื่องคอมพิวเตอร์แม่ข่าย (Server) จำนวน ๑ ระบบ มีคุณลักษณะอย่างน้อยดังนี้

๑.๑ เครื่องคอมพิวเตอร์แม่ข่าย (Server) แบบที่ ๑ จำนวน ๑ เครื่อง มีคุณลักษณะอย่างน้อยดังนี้

๑.๑.๑ มีหน่วยประมวลผลกลาง (CPU) ไม่น้อยกว่า ๑๖ แกนหลัก (Core) หรือดีกว่า สำหรับคอมพิวเตอร์แม่ข่าย (Server) โดยเฉพาะและมีความเร็วสัญญาณนาฬิกาพื้นฐานไม่น้อยกว่า ๒.๓ GHz จำนวน ๒ หน่วย

๑.๑.๒ หน่วยประมวลผลกลาง (CPU) รองรับการประมวลผลแบบ ๖๔ bit มีหน่วยความจำแบบ Cache Memory รวมในระดับ (Level) เดียวกัน ไม่น้อยกว่า ๒๐ MB

๑.๑.๓ มีหน่วยความจำหลัก (RAM) ชนิด ECC DDR๔ หรือดีกว่า ขนาดไม่น้อยกว่า ๗๖๘ GB

๑.๑.๔ สนับสนุนการทำงาน RAID ไม่น้อยกว่า RAID ๐, ๑, ๕

๑.๑.๕ มีหน่วยจัดเก็บข้อมูล ชนิด SAS ความเร็วไม่น้อยกว่า ๑๐k rpm จำนวนไม่น้อยกว่า ๑๐ หน่วย โดยมีความจุรวมไม่น้อยกว่า ๒๔ TB และรองรับการถอดเปลี่ยนแบบ Hot-Plug หรือ Hot-swap ได้

๑.๑.๖ มีหน่วยจัดเก็บข้อมูลชนิด SSD หรือดีกว่า จำนวนไม่น้อยกว่า ๒ หน่วย โดยแต่ละหน่วยจะต้องมีความจุไม่น้อยกว่า ๑.๖ TB

๑.๑.๗ มี DVD-ROM หรือดีกว่า แบบติดตั้งภายใน (internal) หรือ ภายนอก (external) จำนวน ๑ หน่วย

๑.๑.๘ มีช่องเชื่อมต่อ Network Interface แบบ ๑๐๐/๑๐๐๐ Base-T หรือดีกว่า จำนวนไม่น้อยกว่า ๒ ช่อง

๑.๑.๙ มีช่องเชื่อมต่อ Network Interface แบบ ๑๐ Gigabit หรือดีกว่า จำนวนไม่น้อยกว่า ๑ ช่อง

๑.๑.๑๐ มี Power Supplies แบบ Redundant หรือ Hot Swap จำนวนอย่างน้อย ๒ หน่วย

๑.๒ เครื่องคอมพิวเตอร์แม่ข่าย (Server) แบบที่ ๒ จำนวน ๔ เครื่อง มีคุณลักษณะอย่างน้อยดังนี้

๑.๒.๑ มีหน่วยประมวลผลกลาง (CPU) ไม่น้อยกว่า ๑๖ แกนหลัก (Core) หรือดีกว่า สำหรับคอมพิวเตอร์แม่ข่าย (Server) โดยเฉพาะและมีความเร็วสัญญาณนาฬิกาพื้นฐานไม่น้อยกว่า ๒.๓ GHz จำนวน ๒ หน่วย

๑.๒.๒ หน่วยประมวลผลกลาง (CPU) รองรับการประมวลผลแบบ ๖๔ bit มีหน่วยความจำแบบ Cache Memory รวมในระดับ (Level) เดียวกัน ไม่น้อยกว่า ๒๐ MB

๑.๒.๓ มีหน่วยความจำหลัก (RAM) ชนิด ECC DDR๔ หรือดีกว่าขนาดไม่น้อยกว่า ๒๕๖ GB

๑.๒.๔ สนับสนุนการทำงาน RAID ไม่น้อยกว่า RAID ๐, ๑, ๕

๑.๒.๕ มีหน่วยจัดเก็บข้อมูล ชนิด SAS ความเร็วไม่น้อยกว่า ๑๐k rpm จำนวนไม่น้อยกว่า ๕ หน่วย โดยมีความจุรวมไม่น้อยกว่า ๑๐ TB และรองรับการถอดเปลี่ยนแบบ Hot-Plug หรือ Hot-swap ได้

๑.๒.๖ มีหน่วยจัดเก็บข้อมูลชนิด SSD หรือดีกว่า จำนวนไม่น้อยกว่า ๒ หน่วย โดยแต่ละหน่วยจะต้องมีความจุไม่น้อยกว่า ๑.๖ TB

๑.๒.๗ มี DVD-ROM หรือดีกว่า แบบติดตั้งภายใน (internal) หรือ ภายนอก (external) จำนวน ๑ หน่วย

๑.๒.๘ มีช่องเชื่อมต่อ Network Interface แบบ ๑๐๐/๑๐๐๐ Base-T หรือดีกว่า จำนวนไม่น้อยกว่า ๒ ช่อง

๑.๒.๙ มีช่องเชื่อมต่อ Network Interface แบบ ๑๐ Gigabit หรือดีกว่า จำนวนไม่น้อยกว่า ๑ ช่อง

๑.๒.๑๐ มี Power Supplies แบบ Redundant หรือ Hot Swap จำนวนอย่างน้อย ๒ หน่วย

๑.๓ เครื่องคอมพิวเตอร์แม่ข่าย (Server) แบบที่ ๓ จำนวน ๒ เครื่อง มีคุณลักษณะอย่างน้อยดังนี้

๑.๓.๑ มีหน่วยประมวลผลกลาง (CPU) ไม่น้อยกว่า ๒๔ แกนหลัก (Core) หรือดีกว่า สำหรับคอมพิวเตอร์แม่ข่าย (Server) โดยเฉพาะและมีความเร็วสัญญาณนาฬิกาพื้นฐานไม่น้อยกว่า ๒.๔ GHz จำนวน ๒ หน่วย

๑.๓.๒ หน่วยประมวลผลกลาง (CPU) รองรับการประมวลผลแบบ ๖๔ bit มีหน่วยความจำแบบ Cache Memory รวมในระดับ (Level) เดียวกัน ไม่น้อยกว่า ๓๐ MB

๑.๓.๓ มีหน่วยความจำหลัก (RAM) ชนิด ECC DDR๔ หรือดีกว่า ขนาดไม่น้อยกว่า ๕๑๒ GB

๑.๓.๔ สนับสนุนการทำงาน RAID ไม่น้อยกว่า RAID ๐, ๑, ๕

๑.๓.๕ มีหน่วยจัดเก็บข้อมูล ชนิด SAS ความเร็วไม่น้อยกว่า ๑๐k rpm จำนวนไม่น้อยกว่า ๒๐ หน่วย โดยมีความจุรวมไม่น้อยกว่า ๕๐ TB และรองรับการถอดเปลี่ยนแบบ Hot-Plug หรือ Hot-swap ได้

๑.๓.๖ มีหน่วยจัดเก็บข้อมูลชนิด SSD หรือดีกว่า จำนวนไม่น้อยกว่า ๒ หน่วย โดยแต่ละหน่วยจะต้องมีความจุไม่น้อยกว่า ๑.๖ TB

๑.๓.๗ มี DVD-ROM หรือดีกว่า แบบติดตั้งภายใน (internal) หรือ ภายนอก (external) จำนวน ๑ หน่วย

๑.๓.๘ มีช่องเชื่อมต่อ Network Interface แบบ ๑๐๐/๑๐๐๐ Base-T หรือดีกว่า จำนวนไม่น้อย กว่า ๒ ช่อง

๑.๓.๙ มีช่องเชื่อมต่อ Network Interface แบบ ๑๐ Gigabit หรือดีกว่า จำนวนไม่น้อยกว่า ๑ ช่อง

๑.๓.๑๐ มี Power Supplies แบบ Redundant หรือ Hot Swap จำนวนอย่างน้อย ๒ หน่วย

๒. ระบบบริหารจัดการความปลอดภัยสารสนเทศ (SIEM) จำนวน ๑ ระบบ มีคุณลักษณะดังนี้

๒.๑ เป็นฮาร์ดแวร์ appliance หรือซอฟต์แวร์ที่ออกแบบมาเพื่อทำงานเป็นระบบ SIEM (Security Information and Event Management) โดยเฉพาะ

๒.๒ สามารถจัดเก็บ Log พร้อมสิทธิ์การใช้งานที่ครอบคลุมไม่น้อยกว่า ๔๐๐ Gigabyte/day หรือไม่น้อยกว่า ๖๐,๐๐๐ Events Per Second (EPS) หรือไม่น้อยกว่า ๘๐๐ Devices

๒.๓ สามารถจัดเก็บ Log จากอุปกรณ์ประเภทดังต่อไปนี้เป็นอย่างน้อย รวมจำนวนไม่น้อยกว่า ๔๐๐ ชนิด เช่น

๒.๓.๑ ข้อมูลจากกลุ่มอุปกรณ์ทางด้านความมั่นคงปลอดภัย

๑) Web Application Firewall (WAF)

๒) Network Firewall

๓) Intrusion Prevention System

๔) Internet Proxy/Web Filtering System

๕) Advanced Threat Protection System

๒.๓.๒ ข้อมูลจากกลุ่มอุปกรณ์ทางด้านระบบไอทีพื้นฐาน (IT Infrastructure)

๑) Mail Server

๒) Mail Gateway

๓) Web Server

๔) Network Switch

๒.๓.๓ ข้อมูลจากกลุ่มอุปกรณ์ประเภทเครื่องแม่ข่าย (Server)

๑) Microsoft Windows Server

๒) Unix-based Server

๓) Virtualization Hypervisor เช่น VMware ESX, VMware vCenter, Hyper-V เป็นต้น

๒.๓.๔ ข้อมูลจากข้อมูลเครือข่าย Network Flow เช่น Net flow เป็นต้น

๒.๓.๕ รองรับการเพิ่มขยายเพื่อเก็บข้อมูลจากผู้ให้บริการระบบคลาวด์ (Cloud Provider)

๑) AWS

๒) Azure

๓) Office ๓๖๕

๔) Google

๒.๓.๖ ข้อมูลจากแหล่งอื่น ๆ

๑) File เช่น FTP, SFTP เป็นต้น

๒) SNMP

๓) ODBC

๔) Syslog

๒.๔ สามารถจัดเก็บ Log และรักษาความถูกต้องของข้อมูลที่เก็บบันทึกไว้ด้วยวิธีการปลอดภัยตามแนวมาตรฐานสากล เช่น การทำ Hashing แบบ SHA๑ หรือ SHA-๒ หรือ SHA๒๕๖ หรือ MD๕ ได้

๒.๕ พื้นที่จัดเก็บ Log ต้องมีเทคโนโลยีที่ยืดหยุ่นและเพิ่มขยายได้ (Scalable) โดยทำงานในลักษณะที่รองรับข้อมูลขนาดใหญ่ได้ (Big Data architecture) ไม่ใช่ Relational Database Management System (RDBMS) เพื่อประสิทธิภาพในการรองรับปริมาณข้อมูลและการสืบค้น (Search)

๒.๖ สามารถสืบค้นข้อมูล Log จากอุปกรณ์ต่าง ๆ ได้ตามช่วงเวลาที่ระบุ ทั้งแบบย้อนหลังและแบบ Near Real-time โดยต้องสามารถเลือกข้อมูล (Filter) ตามชนิดอุปกรณ์และ IP Address ได้เป็นอย่างน้อย

๒.๗ รองรับการจัดเก็บข้อมูลย้อนหลังเพื่อการค้นหาไม่น้อยกว่า ๑ ปี

๒.๘ สามารถสร้างและแสดงความสัมพันธ์ (Correlation) ของข้อมูล Log จากอุปกรณ์ต่าง ๆ ตามประเภทหัวข้อที่สนใจ และรองรับการสร้างข้อมูล Meta Data หรือ Context โดยอิงตัวตนผู้ใช้งาน (Identity) หรืออิงสินทรัพย์ (Asset) เป็นต้น เพื่อนำมาใช้ในการทำ Correlation ได้

๒.๙ สามารถแจ้งเตือน (Alert) เหตุการณ์ผิดปกติที่เกิดขึ้นในระบบได้ตามเงื่อนไข Scenario หรือ Use Case ที่กรมสรรพสามิต. กำหนด โดย Alert ผ่านทาง Email ได้

๒.๑๐ สามารถบริหารจัดการผ่าน Web-Based GUI หรือ Console ได้อย่างปลอดภัย โดยทำงานร่วมกับระบบ Active Directory หรือ LDAP ของกรมสรรพสามิตเพื่อรองรับการกำหนดและควบคุมสิทธิ์ผู้ใช้งานในการเข้าใช้ระบบได้

๒.๑๑ มีระบบรายงานสถานะแบบ Dashboard ที่สามารถปรับแต่งตามรายผู้ใช้ได้ (Customizable) และสามารถกรองตามเงื่อนไขต่าง ๆ เช่น geographical location, Device type, attack type เป็นต้น

๒.๑๒ รองรับการนำเข้า Threat intelligence ทั้งของผู้ผลิตเองและผู้ผลิตรายอื่น (๓rd party)

๒.๑๓ ผู้เสนอราคาต้องปรับแต่งระบบให้มีประสิทธิภาพอย่างสม่ำเสมอ

๒.๑๔ ผู้เสนอราคาจะต้องปรับแต่ง Parser ของระบบ SIEM ตลอดอายุสัญญาให้สอดคล้องกับรายการอุปกรณ์ที่เปลี่ยนแปลง เพื่อให้ระบบสามารถทำงานได้อย่างต่อเนื่อง

๒.๑๕ สิทธิ์การใช้งานที่เสนอต้องเป็นแบบสิทธิ์ขาด (Perpetual) หากไม่สามารถเสนอแบบสิทธิ์ขาดได้ สามารถเสนอสิทธิ์การใช้งานแบบรายปี (Subscription) ระยะเวลาไม่น้อยกว่า ๕ ปี

๓. ระบบวิเคราะห์ตัวตนและผู้ใช้ (User and Entity Behavior Analysis หรือ UEBA) จำนวน ๑ ระบบ มีคุณลักษณะดังนี้

๓.๑ เป็นฮาร์ดแวร์หรือซอฟต์แวร์หรือโมดูล (Module) ที่ออกแบบมาเพื่อทำงานเป็นระบบ User Entity Behavior Analytic และต้องสามารถทำงานร่วมกับระบบบริหารจัดการความปลอดภัยสารสนเทศ (SIEM) ที่เสนอในโครงการได้อย่างมีประสิทธิภาพ

๓.๒ สามารถตรวจสอบผู้ใช้งาน ไม่น้อยกว่า ๕,๐๐๐ ผู้ใช้งาน

๓.๓ สามารถสร้าง user activity timeline ได้โดยใช้ข้อมูลจาก log หรือ events หรือ network เพื่อตรวจจับเหตุการณ์ปกติ และไม่ปกติ (normal and abnormal/anomalous events)

๓.๔ สามารถระบุ host name และ user ID หรือ user name โดยดูจาก source ip ได้

๓.๕ มีโมเดลการตรวจจับพฤติกรรมพร้อมใช้ (Out of the box behavioral models) เพื่อใช้เรียนรู้ในการสร้าง user profile และ baseline

๓.๖ มีหน้าจอแบบ GUI สำหรับปรับแต่ง behavioral model ได้

๓.๗ สามารถกำหนด Risk score ให้กับ attribute เหล่านี้เป็นอย่างน้อย

๓.๗.๑ user

๓.๗.๒ assets หรือ devices หรือ entities

๓.๘ สามารถเชื่อมโยง log หรือ event ในลักษณะเรียงลำดับเวลา (time-ordered) ของแต่ละ session ของผู้ใช้ได้

๓.๙ สามารถเชื่อมโยงผู้ใช้ไปยังกลุ่มผู้ใช้ที่คล้ายคลึงในระบบได้ (Peer Grouping) เพื่อให้สามารถเปรียบเทียบความแตกต่างของผู้ใช้ที่มีโปรไฟล์คล้ายคลึงกัน เช่น ทำงานตำแหน่งหน้าที่เดียวกัน ในหน่วยงานเดียวกัน เป็นต้น

๓.๑๐ สามารถวิเคราะห์พฤติกรรมผู้ใช้โดยใช้ข้อมูลบริบท (Context Analysis) โดยสามารถแยกแยะว่าเป็นข้อมูลเกี่ยวกับ user หรือ server ได้เองโดยอัตโนมัติ

๓.๑๑ มี Security Use Case พร้อมใช้โดยครอบคลุมหัวข้อเหล่านี้ เป็นอย่างน้อย

๓.๑๑.๑ High Privilege Account Monitor

๓.๑๑.๒ Data Exfiltration Detection

๓.๑๑.๓ Data Reconnaissance Detection

๓.๑๑.๔ Cyber Threat Detection

๓.๑๑.๕ Suspicious Application Activity

๓.๑๑.๖ Identity and Access Anomalies

๓.๑๑.๗ Lateral Movement Detection

๓.๑๑.๘ Abnormal files and resources access Detection

๓.๑๑.๙ Credential misuse

๓.๑๑.๑๐ Privilege and Authorization Management

๓.๑๑.๑๑ Threats Related to Internet of Things (IOT)

๓.๑๒ สามารถเชื่อมโยงข้อมูลการยืนยันตัวตนกับระบบเหล่านี้ได้เป็นอย่างน้อย (Authentication)

๓.๑๒.๑ Microsoft Active Directory

๓.๑๒.๒ CyberArk

๓.๑๒.๓ Beyond Trust

๓.๑๒.๔ Okta

๓.๑๒.๕ LDAP

๓.๑๓ สามารถเชื่อมโยงข้อมูลการยืนยันตัวตนของกรมสรรพสามิตได้

๓.๑๔ ระบบบริการข้อมูลภัยด้านไซเบอร์ (Threat Intelligence) สามารถเชื่อมต่อระบบวิเคราะห์ตัวตนและผู้ใช้ (User and Entity Behavior Analysis หรือ UEBA) ที่เสนอในโครงการได้ โดยระบบบริการข้อมูลภัยด้านไซเบอร์ (Threat Intelligence) สามารถให้บริการดังต่อไปนี้

๓.๑๔.๑ ข้อมูลภัยคุกคาม (Threat Intelligence) ที่มีรายละเอียดในเชิงลึก โดยมีข้อมูลตัวชี้วัด หรือ IOC (Indicators of Compromise) ของภัยคุกคามนั้น ๆ มีการปรับปรุงข้อมูลอย่างต่อเนื่อง (Up-to-date)

๓.๑๔.๒ ข้อมูลรายละเอียดที่เกี่ยวกับการโจมตีและภัยคุกคามเช่น Malware IPs, Ransomware IPs, Tor IPs, Reputation domains และ Web Phishing เป็นต้น

๔. พัฒนาและจัดทำ use case และการแจ้งเตือนการเฝ้าระวังด้านความปลอดภัย จำนวน ๑ งาน โดยมีขอบเขตงานดังนี้

๔.๑ ตรวจสอบและแจ้งเตือน (Alert) บัญชีผู้ใช้งาน Login เข้าระบบสารสนเทศนอกเวลางาน หรือตามที่กรมสรรพสามิตกำหนด โดยใช้ระบบ LOG ของกรมสรรพสามิต

๔.๒ ตรวจสอบและแจ้งเตือน (Alert) การเข้าใช้งานระบบสารนเทศ (Login Failed) ผิดพลาดเกินจำนวนครั้งที่กำหนดหรือตามที่กรมสรรพสามิตกำหนด โดยใช้ระบบ LOG ของกรมสรรพสามิต

๔.๓ ตรวจสอบและแจ้งเตือน (Alert) บัญชีผู้ใช้งานที่มีสิทธิ์ (Privilege Account) เข้า Login ทั้งแบบ Login สำเร็จและไม่สำเร็จ หรือตามที่กรมสรรพสามิตกำหนด โดยใช้ระบบ LOG ของกรมสรรพสามิต

๔.๔ ตรวจสอบและแจ้งเตือน (Alert) บัญชีผู้ใช้งาน เช่น Account Locked, Account Unlocked, Reset Password เป็นต้น หรือตามที่กรมสรรพสามิตกำหนด

๔.๕ ตรวจสอบและแจ้งเตือน (Alert) เมื่อมีการเครือข่ายภายในองค์กรเชื่อมต่อไปยังเครือข่ายต้องสงสัย (Blacklist IP, Malicious และ Anonymous Access หรือตามที่กรมสรรพสามิตกำหนด

๔.๖ ตรวจสอบและแจ้งเตือน (Alert) เมื่อมีการเปลี่ยนรหัสผ่านของบัญชีผู้ใช้งานที่มีสิทธิ์สูง (Privilege Account) หรือตามที่กรมสรรพสามิตกำหนด

๔.๗ ตรวจสอบและแจ้งเตือน (Alert) เมื่อมีการลบหรือแก้ไข Audit Log หรือตามที่กรมสรรพสามิตกำหนด

๔.๘ ตรวจสอบและแจ้งเตือน (Alert) กรณีอุปกรณ์ไม่สามารถส่ง Log หรืออุปกรณ์ส่ง Log หยุดทำงาน หรือตามที่กรมสรรพสามิตกำหนด

๔.๙ ตรวจสอบและแจ้งเตือน (Alert) กรณีเกิดภัยคุกคามประเภท Zero Day, APT หรือตามที่กรมสรรพสามิตกำหนด

๔.๑๐ use case โดยใช้ Machine Learning (ML) ในการตรวจสอบและแจ้งเตือน (Alert) พฤติกรรมที่ผิดปกติจาก baseline ที่ได้ learning ไว้ ได้อย่างน้อย ดังนี้

๔.๑๐.๑ ตรวจสอบการเข้าใช้งานระบบสารสนเทศของผู้ใช้งาน

๔.๑๐.๒ ตรวจสอบการเข้าใช้งานผ่าน VPN

๔.๑๐.๓ ตรวจสอบการติดต่อสื่อสารภายในเครือข่าย

๔.๑๐.๔ ตรวจสอบการใช้งานอินเทอร์เน็ต

๔.๑๐.๕ ตรวจสอบสถานะใช้งานของระบบสารสนเทศ เช่น CPU usage, Memory usage เป็นต้น

๕. พัฒนาและจัดทำหน้าจอรายงานการแจ้งเตือนการเฝ้าระวังด้านความปลอดภัย จำนวน ๑ งาน โดยมีขอบเขตงานดังนี้

๕.๑ ต้องจัดทำหน้าจอรายงาน ในการเฝ้าระวังความปลอดภัย (Security Monitoring) ไม่น้อยกว่า ๑๐ รายงาน

๕.๒ ต้องจัดทำหน้าจอรายงาน สรุปการตรวจสอบและแจ้งเตือน (Alert) บัญชีผู้ใช้งาน Login เข้าระบบสารสนเทศนอกเวลางาน หรือตามที่กรมสรรพสามิตกำหนด

๕.๓ ต้องจัดทำหน้าจอรายงาน สรุปการตรวจสอบและแจ้งเตือน (Alert) การเข้าใช้งานระบบสารสนเทศ (Login Failed) ผิดพลาดเกินจำนวนครั้งที่กำหนด หรือตามที่กรมสรรพสามิตกำหนด

๕.๔ ต้องจัดทำหน้าจอรายงาน สรุปการตรวจสอบและแจ้งเตือน (Alert) บัญชีผู้ใช้งานที่มีสิทธิ์ (Privilege Account) เข้า Login ทั้งแบบ Login สำเร็จและไม่สำเร็จ หรือตามที่กรมสรรพสามิตกำหนด

๕.๕ ต้องจัดทำหน้าจอรายงาน สรุปการตรวจสอบและแจ้งเตือน (Alert) บัญชีผู้ใช้งาน เช่น Account Locked, Account Unlocked, Reset Password เป็นต้น หรือตามที่กรมสรรพสามิตกำหนด

๕.๖ ต้องจัดทำหน้าจอรายงาน สรุปการตรวจสอบและแจ้งเตือน (Alert) เมื่อมีเครือข่ายภายในองค์กรเชื่อมต่อไปยังเครือข่ายต้องสงสัย (Blacklist IP, Malicious และ Anonymous Access หรือตามที่กรมสรรพสามิตกำหนด

๕.๗ ต้องจัดทำหน้าจอรายงาน ตรวจสอบและแจ้งเตือน (Alert) เมื่อมีการเปลี่ยนรหัสผ่านของบัญชีผู้ใช้งานที่มีสิทธิ์สูง (Privilege Account) หรือตามที่กรมสรรพสามิตกำหนด

๕.๘ ต้องจัดทำหน้าจอรายงาน ตรวจสอบและแจ้งเตือน (Alert) เมื่อมีการลบหรือแก้ไข Audit Log หรือตามที่กรมสรรพสามิตกำหนด

๕.๙ ต้องจัดทำหน้าจอรายงาน ตรวจสอบและแจ้งเตือน (Alert) กรณีอุปกรณ์ไม่สามารถส่ง Log หรืออุปกรณ์ส่ง Log หยุดทำงาน หรือตามที่กรมสรรพสามิตกำหนด

๕.๑๐ ต้องจัดทำหน้าจอรายงาน ตรวจสอบและแจ้งเตือน (Alert) กรณีเกิดภัยคุกคามประเภท Zero Day, APT หรือตามที่กรมสรรพสามิตกำหนด

๕.๑๑ ต้องจัดทำหน้าจอรายงาน การตรวจสอบการเข้าใช้งานผ่าน VPN

๕.๑๒ ต้องจัดทำหน้าจอรายงาน Incident Posture หน้าแสดงผลรวมของเหตุการณ์ภัยคุกคามต่าง ๆ เช่น Blacklist IP, Malicious Site, Tor and Anonymous Access ที่เกิดขึ้นทั้งหมดในแต่ละวันได้ หรือตามที่กรมสรรพสามิตกำหนด

๕.๑๓ ต้องจัดทำหน้าจอรายงาน Windows Access หน้าแสดงผลรวมของเหตุการณ์ภัยคุกคามที่เกี่ยวกับ Windows Event ที่เกิดขึ้นทั้งหมดในแต่ละวัน เช่น ผู้ใช้งาน Login เข้าระบบสารสนเทศนอกเวลางาน, ผู้ใช้งาน Login เข้าระบบสารสนเทศล้มเหลว, ผู้ใช้งาน Login เข้าระบบสารสนเทศสำเร็จ, บัญชีผู้ใช้งานที่สำคัญ (High Privilege) เข้า Login ทั้งแบบ Login สำเร็จและไม่สำเร็จหรือตามที่กรมสรรพสามิตกำหนด

๕.๑๔ ต้องจัดทำหน้าจอรายงาน Authentication หน้าแสดงผลรวมของเหตุการณ์การยืนยันสิทธิ์ผู้ใช้งานในแต่ละอุปกรณ์ที่เกิดขึ้นทั้งหมดในแต่ละวัน หรือตามที่กรมสรรพสามิตกำหนด

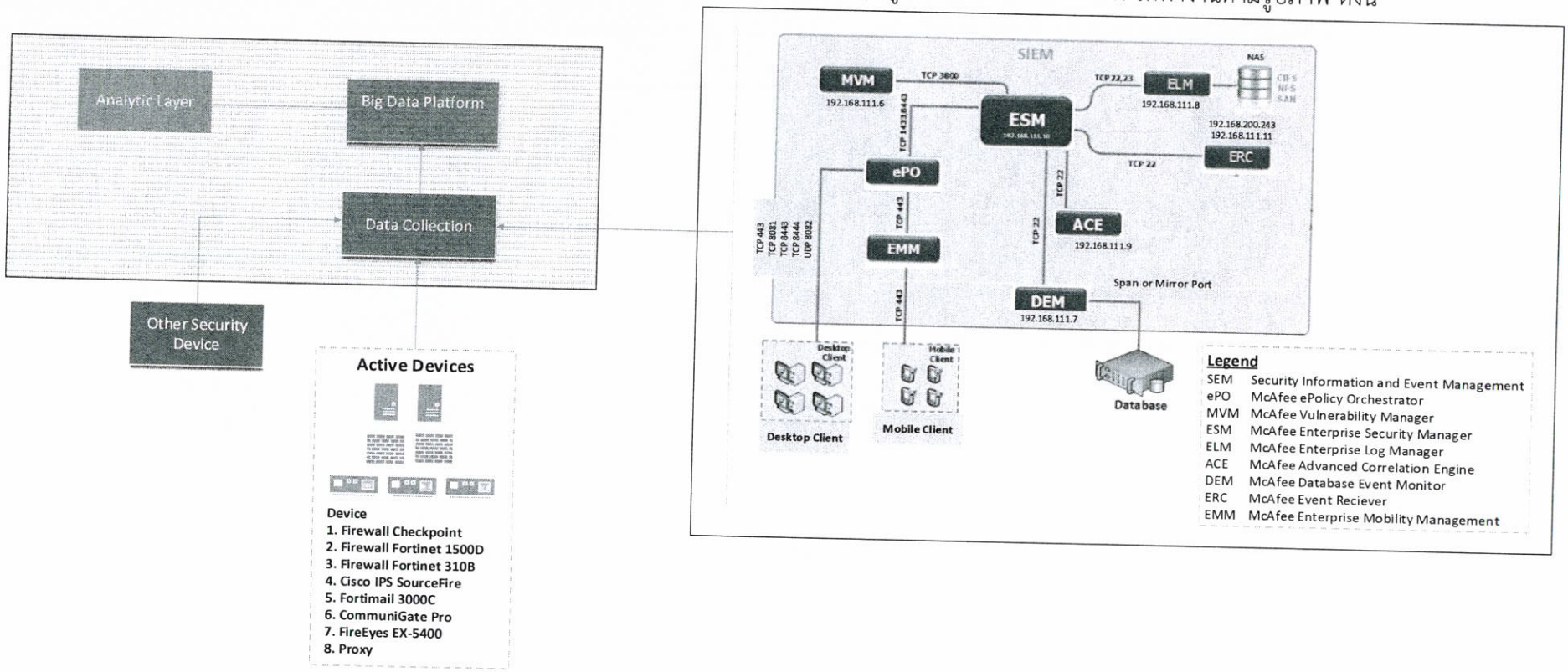
๕.๑๕ ต้องจัดทำหน้าจอรายงาน Investigation หน้าแสดงผลการตรวจสอบเหตุการณ์ (Incident) ที่เกิดขึ้นโดยต้องสามารถตรวจสอบเหตุการณ์ใด ๆ หรือเหตุการณ์ที่มีความสัมพันธ์กับเหตุการณ์ที่เกิดขึ้น (Incident) แบบ Drill Down เหตุการณ์เพื่อดูรายละเอียดเพิ่มเติมได้ หรือตามที่กรมสรรพสามิตกำหนด

๕.๑๖ ต้องจัดทำหน้าจอรายงาน (Report) Executive Report หน้าแสดงผลเหตุการณ์รวมสำหรับหัวหน้างานหรือผู้บริหารที่ต้องการทราบเหตุการณ์รายวัน รายสัปดาห์ รายเดือน ได้ หรือตามที่กรมสรรพสามิตกำหนด

๕.๑๗ ต้องจัดทำกลุ่มรายงานในหน้า Dashboard ตามความเหมาะสม หรือตามที่กรมสรรพสามิตกำหนด

๖. การออกแบบและติดตั้งระบบ

ผู้ชนะการประกวดราคาต้องดำเนินการติดตั้งระบบเฝ้าระวังภัยคุกคามด้าน Cyber Security ศูนย์เทคโนโลยีสารสนเทศ ให้ทำงานตามรูปภาพ ดังนี้



รูปที่ ๑ แสดงการเชื่อมโยงระบบเฝ้าระวังภัยคุกคามด้าน Cyber Security

(๑) ..... (๒) ..... (๓) ..... (๔) .....

๖.๑ ดำเนินการออกแบบการทำงานและเชื่อมต่อระบบ SIEM ที่นำเสนอกับระบบ SIEM เดิม

๖.๒ เสนอแผนการดำเนินงานต่อกรมสรรพสามิตภายใน ๓๐ วันนับจากวันที่ลงนามในสัญญา

๖.๓ ดำเนินการติดตั้งระบบ SIEM ที่เสนอทั้ง Hardware และ Software ให้มีประสิทธิภาพและทำงานร่วมกันได้ตามที่กรมสรรพสามิตกำหนด

๖.๔ จัดหาและติดตั้งอุปกรณ์ Network เพิ่มเติม หากพบว่าอุปกรณ์ Network ของกรมสรรพสามิตไม่เพียงพอต่อการใช้งานของระบบ SIEM ที่นำเสนอ

๖.๕ จัดหาและติดตั้งสายสัญญาณเพื่อให้ระบบใช้งานได้อย่างสมบูรณ์

๖.๖ ดำเนินการติดตั้งระบบเฝ้าระวังภัยคุกคามมีรายละเอียดดังนี้

๖.๖.๑ ดำเนินการติดตั้งระบบจัดเก็บข้อมูลและรวบรวมข้อมูล LOG ของอุปกรณ์

๖.๖.๒ ดำเนินการปรับแต่งข้อมูล LOG (Parsing) เพื่อให้สามารถนำข้อมูลไปวิเคราะห์และแจ้งเตือนได้

๖.๖.๓ ดำเนินการจัดทำ Dashboard ตามข้อกำหนดพัฒนาและจัดทำหน้าจอรายงานการแจ้งเตือนการเฝ้าระวังด้านความปลอดภัย จำนวน ๑ งาน

๖.๖.๔ ดำเนินการจัดทำเหตุการณ์ภัยคุกคาม cyber (use case) อย่างน้อย ๑๐ Use case ตามข้อกำหนดพัฒนาและจัดทำ use case และการแจ้งเตือนการเฝ้าระวังด้านความปลอดภัย จำนวน ๑ งาน

๗. การรับประกัน

๗.๑ ผู้รับจ้างต้องรับประกันความชำรุดบกพร่องของอุปกรณ์และระบบต่าง ๆ เป็นระยะเวลา ๑ ปี นับจากวันที่กรมสรรพสามิตได้ตรวจรับเป็นที่เรียบร้อยแล้ว

๗.๒ ระหว่างการรับประกันความชำรุดบกพร่อง และซ่อมแซมแก้ไขอุปกรณ์และระบบต่าง ๆ ผู้รับจ้างต้องรับประกันความชำรุดบกพร่อง และซ่อมแซมแก้ไขอุปกรณ์ดังกล่าว ให้เป็นไปตามมาตรฐานของเจ้าของผลิตภัณฑ์ในลักษณะการเข้ามาดำเนินการแก้ไขซ่อมแซมอุปกรณ์ (On-site Service) (เข้ามาตรวจสอบแก้ไข ณ กรมสรรพสามิตในกรณีที่เกิดการขัดข้องในการใช้งาน) โดยผู้รับจ้างจะต้องนำเสนอแผนและวิธีซ่อมแซมแก้ไขอุปกรณ์ และระบบต่าง ๆ มาพร้อมกับเอกสารข้อเสนอโครงการในครั้งนี้ด้วยเพื่อประกอบการพิจารณาของกรมสรรพสามิต

๗.๓ กรณีที่ระบบมีปัญหาหรือขัดข้อง ผู้รับจ้างต้องตอบรับทราบต่อการแจ้งเหตุและต้องทำการซ่อมแซมแก้ไขระบบหรือติดตั้งอุปกรณ์/ชิ้นส่วนสำรองมีประสิทธิภาพทัดเทียมกันมาใช้แทนให้อยู่ในสภาพใช้การได้ดีดังเดิม หรือสามารถใช้งานได้ตามปกติไม่เกิน ๔ ชั่วโมง (หลังจากรับแจ้ง จากกรมสรรพสามิต)

๗.๔ กรณีผู้รับจ้างดำเนินการซ่อมแซมแก้ไขระบบโดยใช้อุปกรณ์/ชิ้นส่วนทดแทน ซึ่งแตกต่างจากอุปกรณ์เดิมที่นำเสนอ ผู้รับจ้างต้องดำเนินการซ่อมแซมแก้ไขอุปกรณ์/ชิ้นส่วนที่ชำรุดบกพร่องให้แล้วเสร็จภายใน ๗๒ ชั่วโมง ทั้งนี้ เมื่ออุปกรณ์/ชิ้นส่วนที่ชำรุดดังกล่าวได้รับการซ่อมแซมแก้ไขเป็นที่เรียบร้อยแล้ว ผู้รับจ้างต้องนำมาติดตั้งให้สามารถใช้งานได้ดีดังเดิม โดยระยะเวลาที่ใช้สำหรับการติดตั้งหรือเปลี่ยนอุปกรณ์ไม่เกิน ๔ ชั่วโมง