เอกสารหมายเลข ๒
คุณลักษณะเฉพาะของระบบคอมพิวเตอร์

รายละเอียดคุณลักษณะเฉพาะของระบบคอมพิวเตอร์

"ระบบคอมพิวเตอร์" ที่กรมสรรพสามิต จัดซื้อในครั้งนี้ต้องเป็นของแท้ ของใหม่ ไม่เคยใช้งานมาก่อน ไม่เป็นของเก่าเก็บ ต้องอยู่ในสภาพที่จะใช้งานได้ทันที โดยคุณลักษณะเฉพาะของ **"ระบบคอมพิวเตอร์"** จะต้องเหมาะสมกับลักษณะงานของกรมสรรพสามิตตามโครงการนี้ และสามารถทำงานได้อย่างมีประสิทธิภาพ สะดวกต่อการใช้งาน โดยผู้ประสงค์จะเสนอราคาต้องเสนอ "ระบบคอมพิวเตอร์" ที่มีคุณลักษณะเฉพาะไม่ต่ำกว่าที่ระบุในเอกสารนี้ ประกอบด้วย

เงื่อนไขทั่วไปในการติดตั้ง "ระบบคอมพิวเตอร์"

กรมสรรพสามิตจัดหาเครื่องคอมพิวเตอร์แม่ข่ายให้สำหรับติดตั้งซอฟต์แวร์ที่จำเป็นสำหรับการทำงานของโครงการจัดหาระบบป้องกันภัยคุกคามทางไซเบอร์เพิ่มเติม ให้สามารถทำงานได้อย่างสมบูรณ์ โดยมีรายละเอียดคุณลักษณะเฉพาะ ดังนี้

๑. อุปกรณ์ระบบยืนยันตัวตนเพื่อใช้งานเครือข่ายภายในกรมสรรพสามิต จำนวน ๑ ระบบ โดยมีคุณลักษณะอย่างน้อย ดังนี้

๑.๑ อุปกรณ์รองรับการตรวจจับและควบคุมเครื่องคอมพิวเตอร์ หรืออุปกรณ์ที่มาเชื่อมต่อกับระบบเครือข่ายได้ไม่น้อยกว่า ๑๐,๐๐๐ เครื่อง

๑.๒ อุปกรณ์ที่นำเสนอจะต้องเป็นอุปกรณ์แบบ Hardware Appliance ที่ได้รับการออกแบบมาโดยเฉพาะสำหรับทำหน้าที่เป็นอุปกรณ์ยืนยันตัวตนและควบคุมการเข้าถึงระบบเครือข่าย (NAC) จำนวน ๒ ชุดโดยแต่ละชุดมีคุณลักษณะอย่างน้อยดังนี้

๑.๒.๑ มีช่องเชื่อมต่อเครือข่ายแบบ ๑๐/๑๐๐/๑๐๐๐ Mbps Copper ไม่น้อยกว่า ๔ ช่อง

๑.๒.๒ มีช่องเชื่อมต่อเครือข่ายแบบ ๑๐G Fiber ไม่น้อยกว่า ๔ ช่อง พร้อมโมดูล หรือเสนออุปกรณ์เพิ่ม เพื่อให้มีคุณสมบัติตามที่กำหนด

๑.๒.๓ มีหน่วยจัดเก็บข้อมูล (Hard Drive) ขนาดความจุไม่น้อยกว่า ๑ TB จำนวนไม่น้อยกว่า ๒ หน่วย

๑.๒.๔ มี Power Supply แบบ Redundant หรือ Hot Swap จำนวนไม่น้อยกว่า ๒ หน่วย

๑.๒.๕ อุปกรณ์มีขนาดมาตรฐาน สามารถติดตั้งในตู้ Rack ขนาด ๑๙ นิ้วได้

๑.๓ มีซอฟต์แวร์ระบบยืนยันตัวตนเพื่อใช้งานเครือข่าย โดยมีรายละเอียดคุณลักษณะอย่างน้อยดังนี้

๑.๓.๑ เป็นระบบที่ติดตั้งบนอุปกรณ์ระบบยืนยันตัวตนเพื่อใช้งานเครือข่าย

๑.๓.๒ มีลิขสิทธิ์ในการควบคุมและลิขสิทธิ์ซอฟต์แวร์ Agent สำหรับติดตั้งบนเครื่องลูกข่ายที่เป็นระบบปฏิบัติการ Microsoft Windows และ macOS ได้ไม่น้อยกว่า ๑๐,๐๐๐ เครื่อง

๑.๓.๓ ระบบสามารถทำงานแบบ High Availability แบบ Active/Standby ได้เป็นอย่างน้อย

๑.๓.๔ สามารถกำหนด Policy การใช้งานของเครื่องคอมพิวเตอร์และอุปกรณ์ในระบบเครือข่ายได้

๑.๓.๕ สามารถตรวจจับการโจมตีแบบ ARP Spoofing หรือ MAC Address Spoofing ได้ และระบบต้องไม่ทำการควบคุมระบบเครือข่ายโดยการใช้วิธี ARP Spoofing

๑.๓.๖ สามารถทำ HTTP Redirection และ HTTP Notification หรือ Splash Page เพื่อประกาศข่าวสารแก่ผู้ใช้งานได้

๑.๓.๗ สามารถทำ Web Authentication แก่ผู้ใช้งานระบบเครือข่าย เพื่อทำการยืนยันตัวตนก่อนใช้งานได้ โดยตรวจสอบความถูกต้องของข้อมูลผู้ใช้งานผ่านทาง Directory Service เช่น LDAP, RADIUS และ Microsoft Active Directory ได้

๑.๓.๘ สามารถควบคุม Guest ได้ โดยมี Web Portal สำหรับให้ Guest ทำการลงทะเบียนด้วยตนเองได้

๑.๓.๙ รองรับการทำงานกับมาตรฐาน ๘๐๒.๑X

๑.๓.๑๐ สามารถทำงานร่วมกับ Network Switch และ Wireless Controller ผ่านทางโปรโตคอล SNMP ได้เป็นอย่างน้อย โดยรองรับการกำหนดนโยบาย (policy) และเปลี่ยนแปลงการตั้งค่า (Configuration) อุปกรณ์ภายใต้เครื่องหมายการค้า Cisco, HP, ๓COM, Aruba, H๓C, Juniper, Extreme, Fortinet, Checkpoint และ Sonicwall ได้เป็นอย่างน้อย

๑.๓.๑๑ สามารถแยกประเภทของอุปกรณ์ที่ตรวจพบออกเป็นประเภทได้อย่างน้อยดังนี้

(๑) Windows

(๒) Linux

(๓) VoIP Devices

(๔) Mobile Devices (iOS/Android)

(๕) Printer

(๖) MacOS

๑.๓.๑๒ สามารถตรวจจับข้อมูลของเครื่องลูกข่ายปลายทางได้อย่างน้อยดังนี้

(๑) IP Address และ MAC Address

(๒) NIC Vendor

(๓) NetBIOS Domain/Hostname

๑.๓.๑๓ สามารถทำงานได้ทั้งแบบ Agent และ Agentless โดยซอฟต์แวร์ Agent สำหรับติดตั้งในเครื่องคอมพิวเตอร์ของผู้ใช้งานต้องรองรับระบบปฏิบัติการอย่างน้อย ดังนี้

(๑) Windows

(๒) macOS

๑.๓.๑๔ สามารถตรวจสอบการใช้งานของโปรแกรม Antivirus และวันที่ Update ฐานข้อมูลของ Antivirus ได้

๑.๓.๑๕ สามารถตรวจสอบการเปิดใช้งาน Personal Firewall ในเครื่องคอมพิวเตอร์ระบบปฏิบัติการ Windows ของผู้ใช้งานได้

๑.๓.๑๖ สามารถตรวจสอบ หรือรับข้อมูลช่องโหว่ของระบบปฏิบัติการ Windows (Microsoft vulnerability) ได้

๑.๓.๑๗ สามารถตรวจสอบการเชื่อมต่ออุปกรณ์ประเภท USB Device บนเครื่องผู้ใช้งานได้

๑.๓.๑๘ สามารถแจ้งเตือนผู้ใช้งานผ่านทาง Email และ Balloon Notification ได้เป็นอย่างน้อย

๑.๓.๑๙ สามารถกำหนด policy ตามเงื่อนไข Location, user or host group และตามช่วงเวลา (Schedule) ได้

๑.๓.๒๐ สามารถกำหนด portal สำหรับการเชื่อมต่อเครือข่าย และลงทะเบียนได้ โดยสามารถแยกตาม user/host profile ได้

๑.๓.๒๑ สามารถทำ policy simulator โดยการจำลอง host, adapter และ user เพื่อทดสอบ policy ก่อนใช้งานจริงได้

๑.๓.๒๒ สามารถเชื่อมต่อกับระบบอื่นผ่าน REST API

๑.๓.๒๓ สามารถออกรายงานเกี่ยวกับเครื่องลูกข่ายปลายทางและผลการบังคับใช้นโยบายแบบ PDF และ CSV ได้เป็นอย่างน้อย

๑.๓.๒๔ สามารถตรวจสอบ หรือรับข้อมูลพฤติกรรมผิดปกติที่เกิดจาก Threat ในเครือข่ายได้ เช่น Vertical UDP/TCP Scan, Horizontal UDP/TCP Scan และ Ping Sweep Scan (ICMP) ได้เป็นอย่างน้อย

๑.๓.๒๕ สามารถบริหารจัดการผ่านทาง GUI โดยมีระบบค้นหา (Search) เพื่อเรียกดูข้อมูลผู้ใช้งานได้

๒. ระบบตรวจจับภัยคุกคามจากเครือข่าย และป้องกันภัยคุกคามจากเครือข่าย จำนวน ๑ ระบบ โดยมีคุณลักษณะอย่างน้อย ดังนี้

๒.๑ อุปกรณ์ที่เสนอจะต้องเป็นอุปกรณ์แบบ Hardware Appliance และสามารถทำงานได้โดยไม่ต้องเชื่อมต่ออินเทอร์เน็ต

๒.๒ อุปกรณ์ที่เสนอจะต้องเก็บข้อมูลทั้งหมดของกรมสรรพสามิตไว้ภายในระบบเครือข่าย โดยที่จะต้องไม่ส่งข้อมูลออกไปภายนอกเครือข่าย

๒.๓ สามารถทำงานได้เต็มประสิทธิภาพจากข้อมูล Mirror/Span หรือ Raw Traffic จากระบบเครือข่าย โดยไม่ต้องใช้ข้อมูลจากแหล่งอื่นเพิ่ม

๒.๔ รองรับการขยายในลักษณะ Scale-Out และมีสถาปัตยกรรมแบบกระจาย (Distributed Architecture) โดยที่ข้อมูลจากระบบเครือข่าย ไม่จำเป็นต้องส่งมาที่จุดใดจุดหนึ่งเพียงจุดเดียว

๒.๕ มี Throughput ไม่น้อยกว่า ๑๐Gbps

๒.๖ สามารถใช้งานกับอุปกรณ์ได้ ไม่น้อยกว่า ๕๐,๐๐๐ เครื่อง พร้อม License การใช้งานของอุปกรณ์

๒.๗ สามารถวิเคราะห์ข้อมูล Layer ๒ ถึง Layer ๗ ได้

๒.๘ สามารถระบุข้อมูล (Identifying) และทำ Profiling ของอุปกรณ์ได้ โดยใช้ข้อมูลจากพฤติกรรมการใช้งานของอุปกรณ์ (Behavioral) โดยที่ไม่ต้องทำงานร่วมกับ Solution อื่นเพิ่มเติม

๒.๙ สามารถทำ Profiling ของอุปกรณ์ โดยสามารถติดตามอุปกรณ์ (Tracking Endpoint) ได้

๒.๑๐ สามารถค้นหาชื่อผู้ใช้งาน (User) หรือชื่ออุปกรณ์ (Device) ได้

๒.๑๑ สามารถจัดกลุ่มอุปกรณ์ที่คล้ายคลึงกันได้โดยอัตโนมัติเพื่อสะดวกต่อการทำ Forensic

๒.๑๒ รองรับ Data Science Methods อย่างน้อย ดังนี้

(๑) Supervised Machine Learning

(๒) Unsupervised machine learning

(๓) Deep neural networks

(๔) Belief propagation

(๕) Multi-dimensional clustering

(๖) Decision tree classification

(๗) Outlier detection

๒.๑๓ สามารถระบุข้อมูลการเข้าโดเมน (Domains) จากเครือข่ายภายในได้ โดยสามารถระบุข้อมูลวันแรกและวันสุดท้ายที่เข้า, ข้อมูลจากฐานข้อมูล WHOIS, Protocol ที่ใช้, และปริมาณข้อมูลที่รับส่ง (Bytes Transferred) ได้เป็นอย่างน้อย รวมถึงสามารถแสดงคะแนนความเสี่ยง (Risk Score) และประเภทกลุ่มของโดเมน (Domain Category) ได้

๒.๑๔ สามารถตรวจจับภัยคุกคามจากข้อมูลที่ถูกเข้ารหัส (Encrypted Traffic) ได้

๒.๑๕ สามารถค้นหาข้อมูลดังต่อไปนี้ได้

(๑) MAC Address

(๒) TLS Cipher Suite

(๓) TLS Server Name

(๔) TLS Certificate Fields

(๕) Operating System Version

(๖) JA๓ Value

๒.๑๖ สามารถตรวจจับการโจรกรรมข้อมูล (Data Exfiltration) โดยวิธี DNS และ ICMP tunneling ได้เป็นอย่างน้อย

๒.๑๗ สามารถตรวจจับการโจมตีโดยการใช้เครื่องมือ (Tools) PSExec, PowerShell, และ WMI ได้เป็นอย่างน้อย

๒.๑๘ ระบบแสดงวิธีการตรวจจับการโจมตี (Definition for Threat Detection Techniques) และสามารถแก้ไขหรือดัดแปลงได้

๒.๑๙ สามารถดึงข้อมูล PCAP ได้ตาม Device และ Network Activity ได้เป็นอย่างน้อย

๒.๒๐ สามารถตรวจจับการส่งข้อมูล Username/Password แบบไม่เข้ารหัส (Unencrypted Credentials) บนเครือข่ายได้

๒.๒๑ สามารถตรวจสอบ (Monitor), ติดตาม (Track) และดึงข้อมูล (extract) จากข้อมูล SMB ดังต่อไปนี้ได้

(๑) NTLM Domain

(๒) NTLM Target Name

(๓) NTLM Username

(๔) NTLM Workstation

ประธานกรรมการ..... กรรมการ..... กรรมการ..... กรรมการ..... กรรมการ.....

(๕) Bytes Read
(๖) Bytes Written
(๗) Connection End Time
(๘) Connection Start Time
(๙) File Actions
(๑๐) File Name
(๑๑) File Share
(๑๒) Share Path
(๑๓) Share Type

๒.๒๒ สามารถปรับแต่ง Dashboard ได้

๒.๒๓ สามารถตรวจจับและค้นหาภัยคุกคามย้อนหลังได้สูงสุดไม่น้อยกว่า ๙๐ วัน

๒.๒๔ สามารถทำงานร่วมกับ SIEM, EDR, and SOAR solutions ได้

๒.๒๕ ต้องเสนอราคาพร้อม License โดยที่สามารถ Upgrades Software และสามารถ Update Features และ Threat Detection Models ใหม่ในอนาคตได้โดยไม่มีค่าใช้จ่ายเพิ่มเติม ตลอดระยะเวลาของสัญญา

๒.๒๖ ค่าใช้จ่ายสำหรับ Licenses ที่จำเป็นในการใช้งานกับ ๓rd party จะต้องรวมอยู่ใน Solution ตั้งแต่แรก การใช้งานร่วมกับ ๓rd party ในอนาคตจะต้องไม่มีค่าใช้จ่ายเพิ่มเติม ตลอดระยะเวลาของสัญญา

๒.๒๗ ระบบที่เสนอต้องมีอุปกรณ์ Network Packet Broker Controller จำนวน ๒ หน่วย ซึ่งแต่ละหน่วยมีคุณลักษณะอย่างน้อยดังนี้

๒.๒๗.๑ เป็นอุปกรณ์แบบ Hardware Appliance หรือ Virtual Appliance โดยหากเสนอเป็น Virtual Appliance จะต้องนำเสนอพร้อมกับเครื่องแม่ข่าย โดยที่ Hardware Appliance หรือเครื่องแม่ข่ายที่เสนอ มีคุณลักษณะอย่างน้อยดังนี้

(๑) มีหน่วยประมวลผล (Processor) ไม่น้อยกว่า ๑๐ Cores จำนวนอย่างน้อย ๒ หน่วย
(๒) มีหน่วยความจำ (Memory) ไม่น้อยกว่า ๖๔ GB
(๓) มีหน่วยเก็บข้อมูล (Hard Drive) ขนาดความจุไม่น้อยกว่า ๒ TB
(๔) มี Network Interface แบบ ๑Gb อย่างน้อย ๒ พอร์ต
(๕) มี Network Interface แบบ ๑๐ Gb อย่างน้อย ๒ พอร์ตพร้อม Module
(๖) มี Power Supplies แบบ Redundant หรือ Hot Swap จำนวนไม่น้อยกว่า ๒ หน่วย

๒.๒๗.๒ สามารถทำงานแบบ High-Availability (HA) แบบ Active/Standby ได้เป็นอย่างน้อย

๒.๒๗.๓ สามารถทำงานแบบ Zero Touch Provisioning (ZTP) หรือ Zero Touch Fabric (ZTF) หรือเทียบเท่าได้

๒.๒๗.๔ สามารถกำหนด Policy ให้กับอุปกรณ์ Network Packet Broker Switch ที่เสนอได้

๒.๒๗.๕ สามารถ Upgrade Firmware ให้กับอุปกรณ์ Network Packet Broker Switch ที่เสนอได้

๒.๒๗.๖ สามารถแสดงค่าการใช้งานทรัพยากร (Resources) ของระบบได้ เพื่อให้สะดวกในการวางแผนการใช้งาน

๒.๒๗.๗ สามารถแสดงภาพการเชื่อมต่อ (Topology) ได้

๒.๒๗.๘ สามารถตรวจสอบ (Monitor) อุปกรณ์ในระบบเครือข่ายได้ โดยสามารถแสดงค่า MAC address, และ IP address ได้เป็นอย่างน้อย

๒.๒๗.๙ รองรับ IPv๖ Management Address

๒.๒๗.๑๐ รองรับการบริหารจัดการผ่าน GUI, REST API, และ CLI ได้

๒.๒๗.๑๑ สามารถทำงานร่วมกับระบบ TACACS+ และ RADIUS เพื่อใช้ในการ Authentication/ Authorization ได้

๒.๒๗.๑๒ สามารถกำหนดสิทธิการใช้งานแบบ Role-Based Access Control (RBAC) สำหรับแต่ละผู้ใช้งานได้

๒.๒๗.๑๓ การเก็บ Log ของผู้เข้าใช้งานอุปกรณ์ได้ โดยที่เก็บข้อมูลอย่างน้อย ดังนี้

(๑) CLI Commands

(๒) Login/Logout

(๓) Queries to the REST server

๒.๒๗.๑๔ สามารถทำงานร่วมกับอุปกรณ์ Network Packet Broker Switch ที่เสนอได้อย่างมีประสิทธิภาพ

๒.๒๘ ระบบที่เสนอจะต้องมีอุปกรณ์ Network Packet Broker Switch จำนวน ๒ ชุด โดยแต่ละชุดมีคุณลักษณะอย่างน้อยดังนี้

๒.๒๘.๑ มีพอร์ตการเชื่อมต่อแบบ ๑/๑๐/๒๕ Gigabit Ethernet ไม่น้อยกว่า ๔๘ พอร์ต โดยทุกพอร์ตสามารถทำงานแบบ Wire Speed หรือ Wire Rate หรือ Non-Blocking โดยพร้อมใช้งานทุกพอร์ต

๒.๒๘.๒ มีพอร์ตการเชื่อมต่อแบบ ๔๐/๑๐๐ Gigabit Ethernet ได้ไม่น้อยกว่า ๘ พอร์ต โดยพร้อมใช้งานทุกพอร์ต

๒.๒๘.๓ มีขนาดของ Switching Capacity หรือ Switching Throughput ไม่น้อยกว่า ๔ Tbps และมี Forwarding Rate ไม่น้อยกว่า ๑ Bpps (Billion packets per second)

๒.๒๘.๔ มีขนาดของ System Memory หรือ DRAM ไม่น้อยกว่า ๘GB และมีขนาดของ Flash Memory หรือ SSD ไม่น้อยกว่า ๘ GB

๒.๒๘.๕ มีขนาดของ Packet Buffer Memory ไม่น้อยกว่า ๓๒MB

๒.๒๘.๖ สามารถ Filter Packet โดยใช้ข้อมูล L๒/L๓/L๔ ได้ โดยรองรับทั้ง IPv๔ และ IPv๖

๒.๒๘.๗ สามารถทำ Packet Replication เพื่อทำสำเนาข้อมูลจากขาเข้า (Ingress) เพื่อส่งไปที่ขาออก (Egress) หลายทางได้

๒.๒๘.๘ สามารถทำ Link Aggregation หรือเทียบเท่าได้

๒.๒๘.๙ มี Power Supplies แบบ Redundant หรือ Hot Swap จำนวนไม่น้อยกว่า ๒ หน่วย

๒.๒๘.๑๐ อุปกรณ์ต้องผ่านการรับรองตามมาตรฐานความปลอดภัย IEC, FCC, UL และ EN เป็นอย่างน้อย

๒.๒๙ มีอุปกรณ์ Network Tap แบบ ๑๐ GB หรือดีกว่า ที่สามารถทำ Network Tap ได้ ไม่น้อยกว่า ๔ Segment และสามารถทำ Traffic Bypass ได้กรณีอุปกรณ์ขัดข้อง จำนวน ๑ ชุด

๓. ระบบจำลองการบุกรุกภัยคุกคามทาง Cyber จำนวน ๑ ระบบ โดยมีคุณลักษณะอย่างน้อยดังนี้

๓.๑ ระบบที่นำเสนอต้องเป็นระบบที่ออกแบบมาเพื่อวิเคราะห์และประเมินความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Validation System) โดยเฉพาะ โดยสามารถทดสอบความสามารถและความถูกต้องของระบบรักษาความปลอดภัยเทคโนโลยีสารสนเทศด้วยวิธีการจำลองการโจมตีทางไซเบอร์ได้

๓.๒ สามารถบริหารจัดการผ่าน Cloud ของเจ้าของผลิตภัณฑ์โดยตรง (On-Cloud) ผ่าน Web Browser ได้เป็นอย่างน้อย โดยมีสิทธิการใช้งานพร้อมกันได้ไม่น้อยกว่า ๑ ผู้ใช้งาน ซึ่งสามารถเข้าใช้งานได้เมื่อต้องการ (On-Demand Access) และไม่จำกัดจำนวนครั้งตลอดระยะเวลาของสัญญา

๓.๓ มี Agent หรือ Actor เฉพาะของระบบเป็นตัวรับการทดสอบหรือจำลองการโจมตี ที่สามารถทำงานบนระบบปฏิบัติการ Windows, MAC และ Linux ได้ จำนวนไม่น้อยกว่า ๒ Licenses

๓.๔ สามารถจำลองการโจมตีด้วยวิธีการหรือกระบวนการอ้างอิงตามฐานข้อมูลที่เป็นที่ยอมรับของสากลได้ เช่น MITRE ATT&CK Framework

๓.๕ สามารถสร้างและปรับเปลี่ยนการจำลองการโจมตีแบบกำหนดเองได้

๓.๖ สามารถจำลองการโจมตีผ่านทาง Email เพื่อทดสอบ Email Gateway โดยสร้าง Email จำลองส่งเข้ามาในระบบโดยแนบ Malicious Payload เช่น Ransomware, Worms, Trojans และ Links ของ Malicious Websites โดยต้องมี Template ของ Email มาพร้อมกับระบบที่นำเสนอ ทั้งนี้ผู้ใช้งานสามารถนำเข้า (Upload) URL และ Payload ได้ด้วยตนเอง

๓.๗ สามารถจำลองการโจมตีผ่านทาง Website เพื่อทดสอบ Web Gateway โดยจำลองการเข้าถึง Malicious Website และการดาวน์โหลด Malicious File จาก Website โดยต้องมีรายชื่อ Malicious Website และ Malicious File มาพร้อมกับระบบที่นำเสนอ ทั้งนี้ผู้ใช้งานสามารถนำเข้า (Upload) URL และ Payload ได้ด้วยตนเอง

๓.๘ สามารถจำลองการโจมตีผ่านทาง Endpoint เพื่อทดสอบ Endpoint Security โดยทดสอบ Run Ransomware, Worms, Trojans และ Virus ได้เป็นอย่างน้อย โดยต้องมี Malware มาพร้อมกับระบบที่นำเสนอ

๓.๙ สามารถจำลองการโจมตีตามเวลาที่กำหนด (Schedule หรือ Automated) และเวลาที่ต้องการ (On-Demand) ได้ โดยไม่จำกัดจำนวนครั้งที่ต้องการทดสอบ

๓.๑๐ สามารถจำลองการโจมตีแบบ Phishing Awareness หรือเสนอ Professional Service จากเจ้าของผลิตภัณฑ์ เพื่อตรวจสอบผลจากการตอบสนอง (Action) ของบุคคลากรที่ได้รับ Email ครั้งละ ไม่น้อยกว่า ๕,๐๐๐ คน ได้อย่างน้อยดังต่อไปนี้

๓.๑๐.๑ การเปิด Email (Opening)

๓.๑๐.๒ การเปิดไปยังเว็บไซต์ที่แนบมากับอีเมล์ (Clicking)

๓.๑๐.๓ การกรอกข้อมูลผู้ใช้งานและรหัสผ่าน (Entering Credentials)

๓.๑๑ มี Dashboard แสดงภาพรวมประสิทธิผล และความถูกต้องของระบบรักษาความปลอดภัยเทคโนโลยีสารสนเทศได้จากจุดเดียว (Centralized)

๓.๑๒ สามารถแสดงผลการทดสอบเป็นรายกิจกรรม โดยมีการแสดงให้เห็นว่าระบบที่ทดสอบสามารถป้องกันการโจมตีสำเร็จหรือไม่ ด้วยกระบวนการใด

๓.๑๓ ระบบต้องแสดงถึงหลักฐาน (Evidence) ที่เกิดจากการโจมตีที่เกิดขึ้นจากการทดสอบได้ อาทิ ตำแหน่งและไฟล์ที่ถูกเข้ารหัสจาก Ransomware บนเครื่องที่จำลอง เป็นต้น

๓.๑๔ สามารถบันทึกผลการทดสอบและตรวจสอบข้อมูลผลการทดสอบย้อนหลังได้ พร้อมทั้งมีการแสดงวิธีการแก้ไขหรือข้อแนะนำ เมื่อระบบไม่ผ่านการทดสอบ

๓.๑๕ มีการแจ้งเตือน (Alerts) ไปยังผู้ใช้งานได้ เมื่อทดสอบเสร็จสิ้น ผ่านทาง Email

๓.๑๖ สามารถแสดงรายงานในรูปแบบของ HTML หรือ PDF ได้เป็นอย่างน้อย

๓.๑๗ รองรับการทดสอบประสิทธิภาพการตรวจจับของอุปกรณ์ SIEM เช่น Humio, IBM Qradar, Rapid๗ insightIDR, LogRhythm, McAfee ESM, Microsoft Azure Sentinel, Splunk และ Sumo Logic SIEM ได้เป็นอย่างน้อย โดยแสดงเหตุการณ์ที่มีการแจ้งเตือนด้วย SIEM ในระบบวิเคราะห์และประเมินความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Validation System)

๓.๑๘ รองรับการเชื่อมต่อกับระบบ security orchestration automation and response (SOAR) เช่น Palo Alto Networks Cortex XSOAR ได้เป็นอย่างน้อย เพื่อตรวจสอบ incident และสร้างการตอบโต้กับ incident (incident response) เหล่านั้น

๓.๑๙ ต้องสามารถคำนวณและแสดงค่าความเสี่ยง (risk score) ของแต่ละการโจมตี โดยการคำนวณต้องอ้างอิงจาก risk assessment model เช่น NIST SP ๘๐๐-๓๐ และ CVSS v๓.๐ เป็นอย่างน้อย

๓.๒๐ ระบบที่นำเสนอต้องสามารถ Upgrade Software และปรับปรุงฐานข้อมูลการทดสอบได้แบบอัตโนมัติ เป็นเวอร์ชั่นล่าสุด โดยผู้ใช้งานต้องสามารถตั้งค่าให้มีการทดสอบการโจมตีแบบอัตโนมัติเมื่อมีการอัพเดทการโจมตีใหม่เข้ามา และสามารถเลือกจำลองการโจมตีด้วย IOC (Indicator of compromise) จากเจ้าของผลิตภัณฑ์ที่นำเสนอโดยไม่ต้องนำเข้าจากระบบอื่น อาทิ HAFNUIM for Exchange Server, Emotet Malware, Mikubot และ Follina เป็นต้น

๓.๒๑ ระบบที่เสนอต้องอยู่ในกลุ่มของ Best Breach and Attack Simulation (BAS) Software ในเว็บไซต์ www.g๒.com และอยู่ในกลุ่ม Frost Radar: Global Breach and Attack Simulation Market ของ Frost & Sullivan ปี ๒๐๒๐ หรือใหม่กว่า และในเอกสาร The Cyber Research Databank ของ CyberDB หัวข้อ Automated Breach Simulation Market ปี ๒๐๑๗ หรือใหม่กว่า

๓.๒๒ ผู้ยื่นข้อเสนอต้องแสดงหลักฐานเพื่อเป็นการยืนยันถึงความปลอดภัยของข้อมูลที่ถูกจัดเก็บไว้ในระบบฯ โดยผลิตภัณฑ์ที่เสนอต้องได้รับมาตรฐานความปลอดภัย SOC ๒ Type ๒, ISO ๒๗๐๐๑ และ CSA STAR Level ๑ (Cloud Control Matrix) เป็นอย่างน้อย

๓.๒๓ มีลิขสิทธิ์การใช้งานได้ไม่น้อยกว่า ๑ ปี นับถัดจากวันที่กรมสรรพสามิตตรวจรับงานเสร็จสมบูรณ์ทั้งหมด

๔. อุปกรณ์ระบบรักษาความปลอดภัย DNS ภายในเครือข่ายของกรมสรรพสามิต จำนวน ๑ ชุด โดยมีคุณลักษณะอย่างน้อย ดังนี้

๔.๑ ระบบที่นำเสนอต้องเป็น Hardware Appliance หรือ Virtual Appliance ที่ออกแบบมาสำหรับระบบ DNS โดยเฉพาะ ในกรณีที่นำเสนอ Virtual Appliance ต้องสามารถติดตั้งบน KVM และ Xen ได้เป็นอย่างน้อย และต้องนำเสนอ Hardware Server พร้อม Hypervisor มาด้วย

๔.๒ มี Network Interface แบบ ๑๐GE SFP+ จำนวนไม่น้อยกว่า ๒ พอร์ต พร้อม Module

๔.๓ มี Network Interface แบบ ๑๐๐/๑๐๐๐ จำนวนไม่น้อยกว่า ๔ พอร์ต พร้อม Module

๔.๔ สามารถทำ DNSSEC (DNS Security Extensions) และ DNSSEC Validation เพื่อป้องกันการโจมตีข้อมูล DNS ได้

๔.๕ สามารถป้องกันการโจมตี DNS DDoS แบบ NXDOMAIN Attack และ Phantom Domain Attack ได้ หรือผ่านอุปกรณ์เสริมภายนอกที่เสนอเพิ่มได้ เพื่อให้สามารถทำงานได้ตามข้อกำหนดและทำงานร่วมกันได้

๔.๖ สามารถทำ DNS Firewall เพื่อป้องกันมัลแวร์ติดต่อกับ C&C Sites และ Bots ผ่าน DNS ได้ โดยสามารถกำหนด Policy ให้ Block, Redirect และ Log ได้เป็นอย่างน้อย พร้อมทั้งมี Threat Intelligence Feed ที่สามารถอัพเดทได้

๔.๗ สามารถป้องกันการขโมยข้อมูลผ่าน DNS (Data Exfiltration over DNS Queries) ได้ หรือผ่านอุปกรณ์เสริมภายนอกที่เสนอเพิ่มได้ เพื่อให้สามารถทำงานได้ตามข้อกำหนดและทำงานร่วมกันได้

๔.๘ สามารถให้บริการ DNS, DHCP, IPAM ได้เป็นอย่างน้อย

๔.๙ สามารถรองรับ DNS Query ได้ไม่น้อยกว่า ๕๐,๐๐๐ Queries per Second

๔.๑๐ สามารถทำ IP Discovery เพื่อตรวจหาเครื่อง (Hosts) ที่ใช้งานอยู่บนเครือข่าย โดยสามารถแสดงข้อมูล IP Address, MAC Address และ Name ได้เป็นอย่างน้อย แบบ Immediately หรือ Schedule ได้

๔.๑๑ สามารถบริหารจัดการอุปกรณ์จากศูนย์กลางแบบ Centralized Management หรือแบบ Grid ผ่านการเชื่อมต่อแบบ Secure Communications ได้

๔.๑๒ สามารถใช้งานกับ DNS Record แบบ A, AAAA, PTR, NS, MX, CNAME และ TXT ได้เป็นอย่างน้อย

๔.๑๓ สามารถทำงานแบบ Authoritative DNS ทั้งแบบ Primary (Master) และ Secondary (Slave) ได้ โดยรองรับ DNS Single, DNS Multi Master, Stealth Mode หรือ Hidden DNS Server เพื่อความปลอดภัยของระบบ

๔.๑๔ สามารถทำ Software Upgrades ให้กับอุปกรณ์ทั้งหมดผ่านศูนย์กลางได้ โดยรองรับทั้งแบบ Manual หรือ Schedule และสามารถคืนกลับ (Revert) Software Version ก่อนหน้าได้

๔.๑๕ มี Power Supply แบบ Redundant หรือ Hot Swap

๔.๑๖ อุปกรณ์มีขนาดมาตรฐาน สามารถติดตั้งในตู้ Rack ขนาด ๑๙ นิ้วได้

๔.๑๗ สามารถ Customized Templates ในการ Monitoring ระบบ DNS, DHCP และ IPAM ได้

๔.๑๘ สามารถทำงานในรูปแบบ Hybrid DNS Engine ได้แก่ BIND, Unbound และNSD เป็นอย่างน้อย เพื่อเพิ่มความปลอดภัยหาก Engine หลักเกิดช่องโหว่

๔.๑๙ มีกลไกความปลอดภัยของ DHCP ที่สามารถป้องกันการโจมตีของ DHCP Storm attack (DOS) ได้

๔.๒๐ สามารถ Custom Report ได้ เช่น CSV, Excel และ PDF ได้เป็นอย่างน้อย