ภาคผนวก ๒

การให้บริการโปรแกรมป้องกันและกำจัดไวรัสคอมพิวเตอร์ พร้อมการตรวจสอบและวิเคราะห์ภัยคุกคามเครื่องคอมพิวเตอร์แบบ Endpoint Detection and Response (EDR) และ Extended Detection and Response (XDR)

๑. คุณลักษณะเฉพาะของโปรแกรม EDR (Endpoint Detection and Response)

๑.๑ มีลิขสิทธิ์สำหรับเครื่องลูกข่ายไม่น้อยกว่า ๓,๐๐๐ ลิขสิทธิ์

๑.๒ สามารถติดตั้งบนระบบปฏิบัติการ Windows และ Mac OS เวอร์ชันล่าสุด ได้

๑.๓ สามารถป้องกันจาก Malware (Virus, Spyware, Bots, Backdoors, Key Loggers, Root Kits, Dialers, Adware, Trojans, Phishing และ Worm) แบบ Real time protection

๑.๔ สามารถปรับปรุงฐานข้อมูลไวรัส (Update Pattern) ของเครื่องคอมพิวเตอร์ลูกข่ายผ่านระบบ Cloud ของผลิตภัณฑ์โดยตรง

๑.๕ มีระบบบริหารจัดการและระบบจัดทำรายงาน โดยให้บริการผ่านระบบ Cloud

๑.๖ สามารถเชื่อมต่อและอัพเดตฐานข้อมูล ผ่านเทคโนโลยี Smart protection network หรือ Global intelligence network หรือ Global Threat Intelligence หรือ Global Protective Network

๑.๗ ผู้ดูแลระบบสามารถบริหารจัดการลักษณะ Enterprise management ใน Console เดียวโดยต้องสามารถเข้าถึงทาง web-based ได้ และ ควบคุมนโยบายได้ทั้งหมดโดยไม่ต้องลงโปรแกรม console เพิ่มเติม

๑.๘ มีเทคโนโลยีในการตรวจจับ Malware แบบ Signature-based, Cloud Technology โดยสามารถวิเคราะห์พฤติกรรม (Heuristic Technology) อย่างน้อยดังนี้

- Virtual Patching หรือ Intrusion Prevention หรือ Network Attack Defense
- Behaviour Monitoring หรือ Ransomware Protection
- Machine Learning

๑.๙ สามารถทำงานแบบ Personal Firewall หรือทำงานร่วมกับ Windows Firewall และสามารถทำการตรวจจับการโจมตีผ่านทางระบบเครือข่าย พร้อมทั้งแสดงถึงแหล่งที่มาของการโจมตีเหล่านั้นได้ (Intrusion Detection System หรือ Intrusion Prevention System หรือ Network Threat Protection หรือ Network Attack Defense)

๑.๑๐ สามารถป้องกันการปิด Service ของโปรแกรม Antivirus ได้ ถึงแม้ว่าจะมีสิทธิเป็น Administrator ของเครื่องคอมพิวเตอร์ลูกข่ายก็ตาม

๑.๑๑ มี Password ซึ่งกำหนดจาก Server หรือระบบบริหารจัดการ ในการป้องกันการตั้งค่าตัวโปรแกรม เพื่อไม่ให้ User สามารถแก้ไข หรือ Uninstall โปรแกรมได้

๑.๑๒ สามารถทำการตรวจสอบเฉพาะไฟล์สร้างใหม่หรือมีการเปลี่ยนแปลงโดยใช้เทคโนโลยี iSwift หรือ iChecker หรือ Cache Scan หรือ on-access scan หรือเทคโนโลยีอื่นที่ดีกว่า เพื่อลดเวลาในการตรวจสอบไฟล์

๑.๑๓ สามารถกำหนดการยกเว้นการ Scan โดยระบุเป็น นามสกุลไฟล์ได้ สามารถทำการสั่ง Scan โดย On-Demand ได้

๑.๑๔ สามารถส่งอีเมล หรือ Alert Message ไปยังผู้ดูแลระบบได้ เมื่อเครื่อง Server ตรวจพบไวรัส สามารถนำ Alert Message ออกรายงานในรูปแบบ HTML หรือ Text หรือ PDF หรือ CSV ได้

๑.๑๕ สามารถกู้คืนความเสียหายที่เกิดขึ้นจากพฤติกรรมของไวรัสได้

๑.๑๖ สามารถกำหนด อนุญาต/ไม่อนุญาต/แจ้งเตือน การเข้าใช้งาน website ของ user แต่ละคนได้

๑.๑๗ สามารถอนุญาต/ไม่อนุญาต/ตรวจสอบ การใช้งานโปรแกรมที่ใช้อยู่ในเครื่องได้

๑.๑๘ สามารถกำหนดนโยบายการเข้าถึง Files, Launch process บนเครื่องคอมพิวเตอร์ในองค์กรได้ (Application Control)

๑.๑๙ สามารถกำหนด Policy หรือ Custom Rules ได้ โดยมีคุณสมบัติ TCP Ports Blocking ICMP Port Blocking และ Shared Folders Blocking เป็นอย่างน้อย

๑.๒๐ สามารถสั่งการ Quarantine หรือ Isolate เครื่องคอมพิวเตอร์ที่สงสัยว่าติดไวรัสออกจากเครือข่ายได้

๑.๒๑ สามารถแสดงรายละเอียดช่องโหว่ของโปรแกรมที่ติดตั้งบนเครื่องคอมพิวเตอร์ และแจ้งแพตช์สำหรับอัปเดตเพื่อปิดช่องโหว่เหล่านั้นได้ (Vulnerability assessment)

๑.๒๒ สามารถแสดงรายละเอียดการเข้าใช้งานบริการคลาวด์ต่างๆ ของผู้ใช้งานเครื่องคอมพิวเตอร์ได้ (Cloud Discovery) และทำการ Allow , Block เช่น หมวดหมู่ File sharing, Messengers, Email

๑.๒๓ สามารถอนุญาต/ไม่อนุญาต ใช้งานอุปกรณ์พกพาเช่น flash drive , cd-dvd

๑.๒๔ สามารถตรวจสอบถึงพฤติกรรมอันตรายของไฟล์

๑.๒๕ ต้องมีการป้องกันภัยคุกคามทางไซเบอร์ในรูปแบบ EDR (Endpoint Detection and Response)

๑.๒๖ มีฟังก์ชัน Windows Desktop sharing โดยสามารถเชื่อมต่อไปยังเครื่องลูกข่าย และแม่ข่ายได้โดยไม่จำเป็นต้องใช้งานโปรแกรม remote desktop

๒. คุณลักษณะเฉพาะของโปรแกรม XDR (Extended Detection and Response)

๒.๑ มีลิขสิทธิ์สำหรับเครื่องแม่ข่ายไม่น้อยกว่า ๔๐ ลิขสิทธิ์

๒.๒ สามารถติดตั้งบนระบบปฏิบัติการ Windows Server 2016, Windows Server 2019, Windows Server 2022 และ Linux ได้เป็นอย่างน้อย

๒.๓ เป็น XDR รูปแบบ Open หรือ Native XDR

๒.๔ มีความสามารถด้านการป้องกันภัยคุกคาม อย่างน้อยดังนี้

(๑) Exploit Prevention

(๒) Malware Prevention

(๓) Fileless Attacks

(๔) AI-based / Machine Learning analysis

(๕) Behavior Threat Protection

(๖) Ransomware Protection

๒.๕ มีเทคโนโลยีการทำงานแบบ EDR (Endpoint Detection and Response)

๒.๖ สามารถวิเคราะห์ต้นตอของปัญหาเชิงลึก (Root Cause Analysis) ได้

๒.๗ สามารถวิเคราะห์และเชื่อมโยงพฤติกรรมเทคนิค หรือรูปแบบการโจมตี พร้อมแสดงรายละเอียดเพื่อสนับสนุนการตรวจสอบและตอบสนองต่อภัยคุกคามได้

๒.๘ มีหน้า Dashboard หรือหน้าต่างสรุปรวมเหตุการณ์ภัยคุกคาม โดยสามารถแสดงข้อมูลที่ช่วยให้ผู้ดูแลระบบพิจารณาและจัดลำดับความสำคัญของเหตุการณ์ได้

๒.๙ สามารถแสดงข้อมูลการตรวจจับและป้องกันภัยคุกคามในรูปแบบ Timeline นับตั้งแต่จุดเริ่มต้นจนถึงจุดสิ้นสุด หรือแสดงเป็นแผนภาพเหตุการณ์ (Incident Graph) ในหน้าจอเดียวกัน

๒.๑๐ มีเครื่องมือสำหรับค้นหาและสืบสวนภัยคุกคามเชิงรุกย้อนหลัง

๒.๑๑ สามารถค้นหาข้อมูลหรือเก็บข้อมูลย้อนหลังได้ โดยมีพื้นที่สำหรับเก็บข้อมูลสำหรับระบบไม่น้อยกว่า ๙๐ วัน

๒.๑๒ สามารถป้องกันภัยคุกคามจากการใช้ประโยชน์จากช่องโหว่ของโปรแกรม (Anti-Exploit) ได้

๒.๑๓ สามารถป้องกันเครื่องที่ติด Ransomware ทำการเข้ารหัสบน Share Folders, Map drive ได้ และกำหนดเวลาในการเข้าใช้งาน Share Folders หลังจากทำการป้องกันแล้ว (Anti-Cryptor)

๒.๑๔ สามารถทำการกู้คืนไฟล์เอกสารที่ถูกเข้ารหัสไฟล์ (Recovery) โดยสามารถกำหนดค่าการกู้คืนไฟล์ได้ทั้งแบบอัตโนมัติ (Automatic) หรือ กำหนดเอง (On-demand) ได้

๒.๑๕ สามารถป้องกันภัยคุกคามจากการใช้ประโยชน์จากช่องโหว่ด้านเครือข่าย (Network Attack Defense)

๒.๑๖ สามารถทำการ Update ฐานข้อมูลไวรัสจากเครื่องที่กำหนดในเครือข่าย และจาก Cloud ของผลิตภัณฑ์นั้นได้โดยตรงกรณีที่มีการนำเครื่องลูกข่ายไปใช้งานนอกระบบเครือข่าย

๒.๑๗ สามารถส่งไฟล์ที่ต้องสงสัย (Suspicious files) จากเครื่องคอมพิวเตอร์ลูกข่าย (Endpoint) ไปยัง Cloud Sandbox เพื่อวิเคราะห์หา Malware แบบอัตโนมัติได้ และสามารถส่ง File virus จากหน้าตัวบริหารจัดการและ Manual เพื่อนำไปตรวจสอบบนระบบ Cloud sandbox โดยต้องสามารถรายงานโดยละเอียดถึงการทำงานเช่น suspicious , network activities , Extracted files ของระบบ Threat intelligence ได้

๒.๑๘ มีเทคโนโลยีการทำงานแบบ EDR (Endpoint Detection and Response) แบบ Cloud Technology เพื่อทำงานร่วมกับระบบป้องกันไวรัส ได้

๒.๑๙ มี EDR Sensor ที่ทำงานร่วมกับซอฟต์แวร์ป้องกันไวรัสที่ใช้งานอยู่แบบ Single Agent โดยสามารถรองรับระบบปฏิบัติการทั้ง Windows, Linux และ macOS

๒.๒๐ สามารถบริหารจัดการจากศูนย์กลาง (Centralized Management) ผ่าน Web Browser

๒.๒๑ สามารถทำการตรวจจับ process ที่ต้องสงสัยในระบบปฏิบัติการ หรือ ป้องกันการเปลี่ยนแปลงสิทธิ (privilege escalation), สร้างไฟล์และซ่อน process การทำงานได้

๒.๒๒ สามารถทำการยกเว้นการตรวจสอบการสแกนไวรัส โดยกำหนดรูปแบบ File, Folder, Extension, Process, File Hash, Threat Name ได้เป็นอย่างน้อย

๒.๒๓ สามารถทำการกู้คืนไฟล์ (Restore) ไฟล์ที่ถูกกักกัน (Quarantine) กลับไปยังตำแหน่งเดิม หรือตำแหน่งใหม่ หรือ สามารถกำหนดค่ายกเว้นการสแกนไฟล์ (Exclusion) ที่ทำการกู้คืนใน Policy ได้โดยอัตโนมัติผ่านทางการบริหารจัดการจากส่วนกลาง

๒.๒๔ สามารถเชื่อมต่อการจัดการแบบ Respond ในระบบ User domain เพื่อเพิ่มการจัดการเพิ่มอีกระดับภายในองค์กรที่ใช้งาน Domain ได้ เช่น Lock และ Reset account, Add และ Delete user ไปยัง Security group อื่นๆ

๒.๒๕ สามารถทำการสั่งรีโมตติดตั้งโปรแกรมและถอนการติดตั้งโปรแกรมป้องกันไวรัสบนเครื่องลูกข่ายจากส่วนกลางได้

๒.๒๖ สามารถกำหนดรหัสผ่านป้องกันการถอนโปรแกรม (Uninstall) และรหัสผ่านสำหรับการแก้ไขการตั้งค่า (Policy) ของโปรแกรมบนเครื่องลูกข่ายโดยแยกคนละรหัสผ่าน

๒.๒๗ สามารถกำหนด Policy ให้กลุ่มผู้ใช้ตาม location ที่มีการเปลี่ยนแปลงโดยอัตโนมัติ เช่น IP Address, Gateway Address, DNS Server

๒.๒๘ สามารถควบคุมและกำหนดสิทธิการใช้งานอุปกรณ์ต่อพ่วงภายนอก (Device Control) ได้ โดยควบคุมได้ทั้ง Allowed, Blocked, Read-Only ได้และสามารถอนุญาตให้ใช้งานเป็นราย Device ID หรือ Product ID ได้

๒.๒๙ สามารถแสดงรายงานการโจมตีในระบบเน็ตเวิร์ค โดยแสดงชื่อเครื่องต้นทางและเครื่องปลายทาง รวมทั้งประเภทของการโจมตีได้

๒.๓๐ มีบริการอัพเดตฐานข้อมูลไวรัสคอมพิวเตอร์ให้ทันสมัยได้ในลักษณะ Cloud update และเครื่องบริหารจัดการส่วนกลางที่กำหนดเองได้ (Local Update) เพื่อให้บริการกับเครื่องคอมพิวเตอร์ลูกข่ายในระบบ

๒.๓๑ สามารถกำหนดให้เครื่องลูกข่ายบนระบบปฏิบัติการ Windows หรือ Linux ทำหน้าที่กระจายการอัพเดตภายในเครือข่าย รวมทั้งสามารถแสดงรายชื่อเครื่องลูกข่ายที่เข้ามาทำการอัพเดตและรายละเอียดเวอร์ชันของ Products, Signature ที่อัพเดต

๒.๓๒ มีฟังก์ชัน Windows Desktop sharing โดยสามารถเชื่อมต่อไปยังเครื่องลูกข่าย และ แม่ข่าย ได้โดยไม่จำเป็นต้องใช้งานโปรแกรม remote desktop

๒.๓๓ สามารถสั่ง Task remote wipe data ที่เครื่องลูกข่ายได้ โดยระบุเป็น Path Folders or Files , Files by Extension และกำหนด delete แบบถาวรได้จากการตั้งค่าเพื่อไม่ให้สามารถกู้คืน

๒.๓๔ สามารถป้องกันภัยคุกคามจาก Malware ดังต่อไปนี้ Viruses, Worms, Trojans, Spyware, Adware, Keyloggers, Rootkits ได้เป็นอย่างน้อย

๒.๓๕ สามารถป้องกันมัลแวร์ (Antimalware) โดยอ้างอิงจากฐานข้อมูล (Signature) และแบบวิเคราะห์พฤติกรรม (Heuristic analysis) รวมทั้งการเรียนรู้แบบ Machine Learning ได้เป็นอย่างน้อย

๒.๓๖ ต้องมีเครื่องหมายการค้าเดียวกันกับข้อ ๑

๓. ขอบเขตของผู้รับจ้างเพิ่มเติม

ผู้รับจ้างต้องเป็นผู้ดำเนินการติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ จำนวน ๓,๐๔๐ ลิขสิทธิ์ ตามที่สำนักงานการตรวจเงินแผ่นดินกำหนดให้แล้วเสร็จภายใน ๙๐ วัน นับจากวันลงนามในสัญญา พร้อมทั้งจัดทำสรุปรายการติดตั้งโปรแกรมป้องกันไวรัส

กรณีที่เครื่องคอมพิวเตอร์ที่กำหนดไว้ ต้องการติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ภายหลังจากระยะเวลาที่กำหนด ผู้รับจ้างต้องดำเนินการติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ให้แล้วเสร็จหลังจากที่ได้รับแจ้ง

กรณีที่พบเครื่องคอมพิวเตอร์ไม่สามารถติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์หรือติดตั้งแล้วเกิดปัญหาการใช้งาน ผู้รับจ้างต้องหารือกับศูนย์ดิจิทัลและนวัตกรรมการตรวจเงินแผ่นดินเพื่อหาแนวทางการแก้ไขปัญหาร่วมกันให้สามารถติดตั้งและใช้งานได้ ภายใน ๓๐ วันนับจากวันที่รับแจ้ง หากพ้นกำหนดยังไม่สามารถแก้ไขได้ ผู้รับจ้างต้องจัดหาโปรแกรมป้องกันไวรัสคอมพิวเตอร์อื่นมาทดแทนตามจำนวนเครื่องคอมพิวเตอร์ที่มีปัญหา โดยต้องมีคุณสมบัติเทียบเท่าหรือดีกว่า