ข้อกำหนดและรายละเอียดคุณลักษณะเฉพาะของพัสดุ (Terms of Reference: TOR)
การจัดซื้อระบบตรวจสอบและวิเคราะห์ภัยคุกคามเครื่องคอมพิวเตอร์
(Endpoint Detect and Respond) ของสำนักงาน กสทช. จำนวน ๑ ระบบ

๑. หลักการและเหตุผล

สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.) มีการใช้เทคโนโลยีสารสนเทศมาใช้ในการสนับสนุนระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของสำนักงาน กสทช. สามารถจัดการกับเหตุการณ์ความมั่นคงปลอดภัยในรูปแบบดั้งเดิมได้อย่างมีประสิทธิภาพ แต่ในปัจจุบันภัยคุกคามทางไซเบอร์มีความรุนแรงและซับซ้อนมากขึ้น เพื่อหลบเลี่ยงการตรวจจับจากระบบรักษาความปลอดภัยแบบเดิม ส่งผลให้ระบบบริหารจัดการเดิมไม่สามารถรับมือกับภัยคุกคามรูปแบบใหม่ ๆ ที่มีความซับซ้อนได้อย่างมีประสิทธิภาพ โดยเฉพาะอย่างยิ่งการบริหารจัดการความมั่นคงปลอดภัยในระดับเครื่องลูกข่ายและแม่ข่าย (Endpoint) ซึ่งเป็นจุดที่ตกเป็นเป้าหมายหลักของผู้ไม่หวังดี จำเป็นต้องได้รับการยกระดับเพื่อให้สามารถป้องกัน ตรวจจับ ตอบสนอง และฟื้นฟูจากเหตุการณ์ความมั่นคงปลอดภัยได้อย่างรวดเร็วและทันท่วงที ระบบเดิมที่อาศัยการอัพเดตฐานข้อมูลลายเซ็น (Signature-based Detection) ไม่สามารถรองรับภัยคุกคาม (Zero-day Threats) ได้เต็มที่ และเพิ่มภาระงานของเจ้าหน้าที่ด้านความมั่นคงปลอดภัยในการวิเคราะห์ข้อมูลจำนวนมาก

ด้วยเหตุนี้ สำนักงาน กสทช. จึงจำเป็นต้องจัดหาและนำเทคโนโลยีบริหารจัดการภัยคุกคามในระดับเครื่องลูกข่ายที่ทันสมัยมาใช้ ซึ่งต้องสามารถทำงานได้แบบอัตโนมัติและเรียลไทม์ โดยระบบต้องมีความสามารถวิเคราะห์พฤติกรรม (Behaviour-based Detection) ของผู้ใช้งาน โปรแกรม และกระบวนการต่าง ๆ ภายในเครื่องลูกข่ายและเครื่องแม่ข่าย เพื่อค้นหาความผิดปกติที่อาจเป็นภัยคุกคามได้อย่างแม่นยำ และเมื่อพบเหตุการณ์ที่มีความเสี่ยงต้องสามารถตอบสนองได้โดยอัตโนมัติ เช่น การกักกันเครื่องที่ติดมัลแวร์ การปิดกั้นกระบวนการอันตราย หรือการย้อนรอยตรวจสอบเพื่อป้องกันการแพร่กระจายของภัยคุกคามในระบบ นอกจากนี้ระบบต้องมีความสามารถในการรวมศูนย์จัดการ (Centralized Management) เพื่อให้เจ้าหน้าที่สามารถมองเห็นภาพรวมสถานะความมั่นคงปลอดภัยของเครื่องลูกข่ายและแม่ข่ายทุกเครื่องในระบบของสำนักงานได้อย่างชัดเจน และสามารถสร้างข้อมูลข่าวกรองภัยคุกคามภายในองค์กร (Internal Threat Intelligence) จากเหตุการณ์จริงที่เกิดขึ้นโดยไม่ต้องพึ่งพาฐานข้อมูลภายนอก ตลอดจนรองรับการนำเข้าหรือส่งออกข้อมูลภัยคุกคามตามมาตรฐานสากล เช่น STIX หรือ IOC เพื่อให้สามารถใช้ข้อมูลดังกล่าวในการวิเคราะห์ภัยคุกคามเชิงลึกหรือผสานร่วมกับระบบอื่น ๆ ภายในองค์กรได้อย่างมีประสิทธิภาพ ช่วยให้ยกระดับความมั่นคงปลอดภัยสารสนเทศในระดับเครื่องลูกข่ายและแม่ข่ายได้อย่างรอบ ช่วยลดความเสี่ยงจากการถูกโจมตีที่อาจกระทบต่อความต่อเนื่องในการให้บริการและความเชื่อมั่นของประชาชน รวมถึงช่วยเพิ่มประสิทธิภาพในการบริหารจัดการภัยคุกคามและลดภาระงานของเจ้าหน้าที่ด้านความมั่นคงปลอดภัยสารสนเทศ และยังสอดคล้องกับภารกิจของสำนักงาน กสทช. ในการเสริมสร้างความมั่นคงปลอดภัยทางไซเบอร์ของระบบสารสนเทศภายในองค์กร และสอดคล้องกับแนวทางตามประกาศคณะกรรมการกำกับความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ ซึ่งกำหนดให้หน่วยงานของรัฐต้องมีการเก็บรักษาบันทึกของการเข้าถึงระบบสารสนเทศ ตรวจสอบความผิดปกติ และมีการตอบสนองต่อเหตุการณ์อย่างเหมาะสม

ทั้งนี้ การจัดซื้อระบบตรวจสอบและวิเคราะห์ภัยคุกคามเครื่องคอมพิวเตอร์จึงเป็นสิ่งจำเป็นเพื่อให้สำนักงาน กสทช. สามารถรักษาความมั่นคงแข็งแรงของระบบสารสนเทศ ป้องกันความเสียหายจากภัยคุกคามไซเบอร์รูปแบบใหม่ ๆ ได้อย่างมีประสิทธิภาพ

Proof

๒. วัตถุประสงค์

เพื่อเสริมสร้างความมั่นคงปลอดภัยของระบบสารสนเทศในระดับเครื่องลูกข่ายและแม่ข่าย (Endpoint) ให้มีความสามารถในการป้องกัน ตรวจจับ ตอบสนอง และฟื้นฟูจากภัยคุกคามไซเบอร์ที่มีความซับซ้อนและรุนแรงเพิ่มมากขึ้นอย่างอัตโนมัติและแบบเรียลไทม์ ด้วยเทคโนโลยีวิเคราะห์พฤติกรรม (Behavior-based Detection) ที่ช่วยระบุภัยคุกคามใหม่ ๆ (Zero-day Threats) ได้อย่างมีประสิทธิภาพ พร้อมทั้งเพิ่มประสิทธิภาพในการบริหารจัดการและมองเห็นสถานะความมั่นคงปลอดภัยของเครื่องลูกข่ายและแม่ข่ายทุกเครื่องในระบบสารสนเทศของสำนักงาน กสทช.

๓. คุณสมบัติของผู้ยื่นข้อเสนอ

๓.๑ ผู้ยื่นข้อเสนอต้องมีคุณสมบัติพื้นฐานที่กำหนด ตามพระราชบัญญัติการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. ๒๕๖๐ ตลอดจนแนวปฏิบัติตามหนังสือคณะกรรมการวินิจฉัยปัญหาการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ กรมบัญชีกลาง ตามที่กำหนดในเอกสารประกวดราคาซื้อ ด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ (e-bidding)

๓.๒ ผู้ยื่นข้อเสนอต้องแสดงหนังสือที่มีเนื้อหาระบุการแต่งตั้งให้เป็นตัวแทนจำหน่ายและสนับสนุนการให้บริการซ่อมแซมแก้ไข มีการสนับสนุนด้านเทคนิครวมทั้งการบริการหลังการขาย จากเจ้าของผลิตภัณฑ์ หรือสาขาประจำประเทศไทยของเจ้าของผลิตภัณฑ์

๔. รายละเอียดคุณลักษณะเฉพาะ

๔.๑ ข้อกำหนดทั่วไป

๔.๑.๑ ระบบที่เสนอให้มีสิทธิ์ในการใช้งานระบบความปลอดภัยทางไซเบอร์สำหรับอุปกรณ์ปลายทาง (EDR) แบ่งเป็นเครื่องลูกข่าย (Endpoint) จำนวน ๑,๔๖๐ เครื่อง และเครื่องแม่ข่าย (Server) จำนวน ๗๐๐ เครื่อง ซึ่งระบบดังกล่าวต้องมีความสามารถในการตรวจหาและตอบสนองแบบขยายตัว (XDR) อยู่ในระบบ และเป็นตราสัญลักษณ์เดียวกัน

๔.๑.๒ ผู้ขายจะต้องส่งมอบสิทธิ์การใช้งานระบบความปลอดภัยทางไซเบอร์สำหรับอุปกรณ์ปลายทาง (EDR) และเอกสารแสดงการกำหนดค่า Configuration ของระบบทั้งหมดตามที่เสนอ

๔.๑.๓ ผู้ขายจะต้องจัดอบรมพัฒนาบุคลากรให้มีความพร้อมในการใช้งานระบบที่เสนอเพื่อให้สามารถวิเคราะห์ข้อมูลภัยคุกคามทางไซเบอร์ที่เกิดขึ้นบนอุปกรณ์ปลายทางที่ได้ติดตั้ง

๔.๒ ข้อกำหนดทางด้านเทคนิค

สิทธิ์ในการใช้งานระบบความปลอดภัยทางไซเบอร์สำหรับอุปกรณ์ปลายทาง (EDR) ที่มีความสามารถในการตรวจหาและตอบสนองแบบขยายตัว (XDR) ของเครื่องแม่ข่าย (Server) จำนวน ๗๐๐ เครื่อง และลูกข่าย (Endpoint) จำนวน ๑,๔๖๐ เครื่อง มีคุณสมบัติดังต่อไปนี้

๔.๒.๑ ระบบเป็นลักษณะ Software as a Service (SaaS) ที่มี Web-Based Management เพื่อใช้ในการติดตั้ง Security policies และการ updates ไปยังเครื่องคอมพิวเตอร์ จำนวน ๒,๑๖๐ ลิขสิทธิ์ (License) ที่สามารถวิเคราะห์ตรวจจับภัยคุกคามโดยใช้เทคโนโลยี AI หรือ Machine Learning ในการวิเคราะห์พฤติกรรมที่เกิดขึ้นโดยการหาความสัมพันธ์ของข้อมูลที่ได้มาจากเครื่อง Endpoint, Network, Cloud และ ข้อมูลระบุตัวตนของผู้ใช้งาน (Identity) เป็นอย่างน้อยพร้อมทั้งมีระบบ scoring ของแต่ละ Incident แบบอัตโนมัติด้วยเทคโนโลยี AI หรือ Machine Learning เพื่อจัดลำดับความเร่งด่วนในการจัดการกับ Incident และ สามารถรวม Incident เข้าด้วยกัน (Merage Incident) ได้

Proof

๔.๒.๒ มี Agent Software ที่สามารถติดตั้งได้บน Platform ได้ดังต่อไปนี้

๔.๒.๒.๑ Windows

๔.๒.๒.๒ Linux

๔.๒.๒.๓ MacOS

๔.๒.๓ สามารถป้องกัน Exploit และ Malware ในกรณีที่ไม่สามารถติดต่อกับ Management Console ได้ (Offline) รวมถึง สามารถป้องกันการโจมตีที่ช่องโหว่ของระบบ (Exploit Prevention), Malware, Ransomware, ป้องกันการโจมตีโดยใช้การวิเคราะห์พฤติกรรม (Behavior Threat Prevention) ได้

๔.๒.๔ มีความสามารถในการค้นหาและระบุภัยคุกคามที่เกิดขึ้น (Threat Hunting) โดยวิเคราะห์จากพฤติกรรมการใช้งานที่ผิดปกติ (Behavior Threat) และสามารถแสดงรายละเอียดของเครื่องปลายทาง เช่น Application, System Information เป็นต้น

๔.๒.๕ สามารถแสดงข้อมูลเหตุการณ์ภัยคุกคามทางไซเบอร์ โดยมีรายละเอียด อย่างน้อยดังนี้

๔.๒.๕.๑ ระบุประเภทของภัยคุกคาม

๔.๒.๕.๒ วัน-เวลา เริ่มต้นและสิ้นสุดของภัยคุกคาม

๔.๒.๕.๓ ระบุต้นทาง (Source) ปลายทาง (Destination)

๔.๒.๕.๔ ระบุระดับความรุนแรง (Severity)

๔.๒.๕.๕ รายละเอียดเหตุการณ์และพฤติกรรม

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

๔.๒.๕.๗ สามารถแสดงเทคนิคของภัยคุกคามที่ตรวจพบ โดยเทียบกับ MITRE ATT&CK Techniques และ Tactics ได้

๔.๒.๕.๘ แสดงลำดับเหตุการณ์ที่เกิดขึ้น (Timeline)

๔.๒.๕.๙ แสดงวิธีการแก้ไขสำหรับเหตุการณ์ภัยคุกคามนั้น (Remediation Suggestion)

๔.๒.๖ มีวิธีการในการตอบสนองต่อภัยคุกคาม (Response) อย่างน้อยดังนี้

๔.๒.๖.๑ แยกหรือตัดการเชื่อมต่อเครื่องคอมพิวเตอร์ (Isolate Endpoint) ได้หลายๆ เครื่องพร้อมๆกัน

๔.๒.๖.๒ สามารถสั่งการดำเนินการด้วย Python Script, Powershell และ System command ผ่าน Live Terminal จาก Management Console ได้

๔.๒.๖.๓ เพิ่มค่า Hash ของไฟล์ที่ต้องการป้องกันได้ (Add to Block List)

๔.๒.๗ สามารถทำงานร่วมกับ Cloud Sandbox หรือ On-Premise Sandbox เพื่อวิเคราะห์ภัยคุกคาม และนำผลลัพธ์มาใช้ในการป้องกันได้ กรณีที่ต้องทำงานร่วมกับ On-Premise Sandbox ให้เสนอ On-Premise Sandbox เพิ่มเติมให้ครอบคลุม และเพียงพอต่อการทำงาน

๔.๒.๘ สามารถค้นหาข้อมูลโดยรองรับการสร้าง Rule เพื่อตรวจจับภัยคุกคามจากพฤติกรรมหรือร่องรอยการโจมตี เพื่อให้สามารถสร้าง Alert จากเหตุการณ์ที่เคยเกิดขึ้นในอดีตย้อนหลังได้

๔.๒.๙ สามารสร้างและแก้ไข Correlation rule เพื่อทำการตรวจสอบการโจมตีได้จากหลายเหตุการณ์ (multi-events) และจากหลายแหล่งที่มา (multi-sources) ด้วย Query

Proof

Language ได้ หรือนำเสนอระบบอื่นๆเพิ่มเติม เพื่อสามารถทำได้ตามความต้องการดังกล่าว

๔.๒.๑๐ สามารถตรวจสอบช่องโหว่ (Vulnerability Assessment) บนระบบปฏิบัติการ Windows และ Linux โดยอ้างอิงช่องโหว่ตาม Common Vulnerabilities and Exposures (CVE) โดยสามารถทำได้บน Agent เดียวกัน หรือนำเสนอระบบอื่นๆ เพิ่มเติม เพื่อสามารถทำได้ตามความต้องการดังกล่าว

๔.๒.๑๑ สามารถแสดง Host Inventory เช่น User, Application, Services, Driver, Autorun, Share ของเครื่องคอมพิวเตอร์ได้ เพื่อสามารถตรวจสอบข้อมูลได้อย่างรวดเร็ว หรือนำเสนอระบบอื่นๆเพิ่มเติม เพื่อทำได้ตามความต้องการดังกล่าว

๔.๒.๑๒ มีความสามารถในการแจ้งเตือน (Alert) ผ่าน Email, Slack หรือ SYSLOG โดยสามารถเลือกจาก Severity Level และจากเงื่อนไข (Attribute) อื่นได้ไม่น้อยกว่า ๒ เงื่อนไขพร้อมกันได้

๔.๒.๑๓ สามารถสร้าง Automation Rule เพื่อกำหนดให้ระบบตอบสนองอัตโนมัติเมื่อมี Alert ที่ตรงเงื่อนไขเกิดขึ้นได้ โดยสามารถเลือกจากเงื่อนไข (Attribute) ได้ไม่น้อยกว่า ๒ เงื่อนไขพร้อมกันได้ หรือเสนอระบบภายนอกเพื่อให้สามารถทำงานได้ตามข้อกำหนด

๔.๒.๑๔ สามารถใช้งานระบบ Playbook หรือ Workflows ที่มีเครื่องมือช่วยในการสร้างและปรับแต่งกระบวนการตอบสนอง โดยรองรับการกำหนดเงื่อนไขและการสั่งการแบบอัตโนมัติ

๔.๒.๑๕ สามารถทำการสร้าง Playbook ได้อย่างน้อยดังนี้

๔.๒.๑๕.๑ Manual action and Task

๔.๒.๑๕.๒ การสร้างขั้นตอนในการตัดสินใจและอนุมัติ

๔.๒.๑๕.๓ การเรียกใช้งาน Playbook ที่ซ้อนกันได้

๔.๒.๑๕.๔ การกำหนดเงื่อนไขและลูป

๔.๒.๑๕.๕ การหยุดหรือดำเนินการต่อเมื่อเกิดข้อผิดพลาดใน Playbook

๔.๒.๑๖ สามารถทำการเก็บข้อมูลในรูปแบบ Snapshot เพื่อทำการย้อนกลับ (Roll back) ในกรณีที่ Playbook เกิดปัญหาได้ หรือ การทำ Playbook Version History

๔.๒.๑๗ สามารถส่ง Email แบบโต้ตอบให้กับผู้ใช้งาน เพื่อดำเนินการอนุมัติ (approval) ผ่าน Email ได้โดยตรง เช่น ทำการ block IP บน Firewall เป็นต้น

๔.๒.๑๘ ระบบส่วนกลางสามารถนำเข้าข้อมูลจราจรคอมพิวเตอร์ หรือ Log จากอุปกรณ์ความปลอดภัยเครือข่าย ของสำนักงาน กสทช. ได้ไม่น้อยกว่า ๒๐ GB ต่อวัน เพื่อเชื่อมโยงวิเคราะห์ความสัมพันธ์ของข้อมูลกับการโจมตีบนเครื่องคอมพิวเตอร์ได้ โดยสามารถทำการวิเคราะห์ข้อมูลจากแหล่งข้อมูลที่แตกต่างกัน (เช่น Endpoint Network หรือ Firewall) เพื่อแสดงผลว่าเป็นเหตุการณ์เดียวกันได้

๔.๒.๑๙ สามารถเก็บ Raw Data หรือ Ingested Data ได้ไม่น้อยกว่า ๓๐ วัน และเก็บ Incident Data ได้ไม่น้อยกว่า ๑๘๐ วัน

๔.๒.๒๐ สามารถทำการค้นหา เพื่อทำลายหรือลบไฟล์ต้องสงสัยโดยใช้ Hash และ File Path ในการค้นหาได้ หรือนำเสนอระบบเพิ่มเติมเพื่อสามารถทำได้ตามความต้องการดังกล่าว

๔.๒.๒๑ ระบบที่นำเสนอต้องอยู่ในกลุ่ม Leader ของ The Forrester Wave™: Extended Detection And Response Platform, Q2 2024 หรือปีล่าสุด

Proof

๕. กำหนดเวลาส่งมอบพัสดุ

ผู้ขายจะต้องส่งมอบสิทธิ์ในการใช้งานระบบความปลอดภัยทางไซเบอร์สำหรับอุปกรณ์ปลายทาง (EDR) แบ่งเป็นเครื่องลูกข่าย (Endpoint) จำนวน ๑,๔๖๐ เครื่อง และเครื่องแม่ข่าย (Server) จำนวน ๗๐๐ เครื่อง โดยสิทธิ์การใช้งานดังกล่าวต้องมีระยะเวลาการใช้งาน (Subscription) ไม่น้อยกว่า ๑ ปี และต้องดำเนินการส่งมอบให้แล้วเสร็จภายใน ๙๐ วัน นับถัดจากวันลงนามในสัญญา

๖. หลักเกณฑ์ในการพิจารณาคัดเลือกข้อเสนอ

สำนักงาน กสทช. จะพิจารณาคัดเลือกข้อเสนอโดยใช้เกณฑ์ราคา

๗. วงเงินงบประมาณ

วงเงินรวมทั้งสิ้น ๖,๐๐๐,๐๐๐.- บาท (หกล้านบาทถ้วน) ซึ่งได้รวมภาษีมูลค่าเพิ่มและค่าใช้จ่ายทั้งปวงไว้ด้วยแล้ว โดยเบิกจ่ายจากงบประมาณรายจ่ายประจำปี ๒๕๖๙ ของสำนักเทคโนโลยีสารสนเทศ หมวดครุภัณฑ์ ที่ดิน และสิ่งก่อสร้าง รายการครุภัณฑ์คอมพิวเตอร์

๘. งวดงานและการจ่ายเงิน

สำนักงาน กสทช. จะชำระเงินค่าจัดซื้อทั้งหมดตามสัญญาเมื่อผู้ขายส่งมอบตามข้อ ๕ และคณะกรรมการตรวจรับพัสดุได้ดำเนินการตรวจรับเรียบร้อยแล้ว

๙. อัตราค่าปรับ

ผู้ขายจะต้องติดตั้งและส่งมอบงานแล้วเสร็จตามสัญญา มิฉะนั้นต้องชำระค่าปรับให้สำนักงาน กสทช. เป็นรายวันในอัตราร้อยละ ๐.๒ (๐.๒%) ของมูลค่าพัสดุที่ยังไม่ได้ส่งมอบ จนถึงวันที่ผู้ขายได้ส่งมอบพัสดุให้สำนักงาน กสทช. เป็นที่เรียบร้อยแล้ว

๑๐. เงื่อนไขอื่นๆ

๑๐.๑ ตลอดระยะเวลาที่ใช้สิทธิ์ ผู้ขายจะต้องรับประกันความชำรุดบกพร่อง โดยนับตั้งแต่วันที่สำนักงาน กสทช. ได้รับมอบพัสดุไว้ใช้งานโดยสมบูรณ์ทั้งหมด และผู้ขายจะต้องมี Help Desk ซึ่งสามารถติดต่อประสานงานและร้องขอความช่วยเหลือให้คำปรึกษาทางโทรศัพท์ได้ในเวลาราชการ ตั้งแต่วันจันทร์-ศุกร์ เวลา ๘:๓๐ น. - ๑๖:๓๐ น.

๑๐.๒ หากโปรแกรมคอมพิวเตอร์เกิดการชำรุดบกพร่อง หรือไม่สามารถทำงานได้ครบถ้วนสมบูรณ์ตามที่กำหนดในสัญญานี้ ผู้ขายจะต้องซ่อมแซมแก้ไขโปรแกรมคอมพิวเตอร์ดังกล่าวให้ทำงานได้อย่างสมบูรณ์ หรือติดตั้งโปรแกรมคอมพิวเตอร์อันใหม่ที่ได้มาตรฐานและมีคุณสมบัติเท่ากับหรือดีกว่าโปรแกรมคอมพิวเตอร์ที่ซื้อขายและอนุญาตให้ใช้สิทธิ์ตามสัญญานี้โดยไม่ชักช้า ทั้งนี้ ไม่เกิน ๓ วัน นับถัดจากวันที่ได้รับแจ้งเป็นหนังสือจากผู้ซื้อ โดยไม่คิดค่าใช้จ่ายใด ๆ จากผู้ซื้อทั้งสิ้น

Proof