ขอบเขตของงานโครงการจัดหาพร้อมติดตั้งระบบรวบรวม วิเคราะห์ และตอบสนองความปลอดภัยการใช้งานระบบสารสนเทศโดยอัตโนมัติ จำนวน ๑ ระบบ

๑. ความเป็นมา

ศว.สว. ได้รับมอบหมายให้ดูแลข่ายสื่อสาร และเฝ้าระวังความมั่นคงปลอดภัยทางสารสนเทศ ซึ่งต้องรับข้อมูลการใช้งานจากระบบงานของหน่วยงานต่าง ๆ เช่น บท.สท. (การใช้งาน ICT Data Center, End Terminal) วข.บว. (การใช้งาน AIS Data Center, End Terminal) เป็นต้น เพื่อมาวิเคราะห์การใช้งาน และตอบสนอง ต่อเหตุการณ์ต่าง ๆ ที่เกิดขึ้น ซึ่งปัจจุบันยังไม่มีระบบที่จะรวบรวมข้อมูลจากหลาย ๆ แหล่งเข้ามาวิเคราะห์ และหาความเชื่อมโยง ทำให้การวิเคราะห์และตอบสนองต่อเหตุการณ์จึงต้องใช้เจ้าหน้าที่ในการดำเนินการ ทำให้เกิดความล่าช้า และไม่ครบถ้วนสมบูรณ์ จึงมีความจำเป็นต้องจัดหาพร้อมติดตั้งระบบรวบรวมวิเคราะห์ และตอบสนองการใช้งานระบบสารสนเทศโดยอัตโนมัติ เพื่อให้การปฏิบัติงานเฝ้าระวังความมั่นคงปลอดภัยทางสารสนเทศ มีประสิทธิภาพ และครอบคลุมระบบสารสนเทศทั้งหมดของบริษัทฯ

๒. วัตถุประสงค์

เพื่อปรับปรุงและพัฒนา การเฝ้าระวังความมั่นคงปลอดภัยทางสารสนเทศ ให้ทำงานได้อย่างมีประสิทธิภาพ รองรับภัยคุกคามใหม่ๆ ให้คงความมั่นคงปลอดภัยตามประกาศมาตรฐานความมั่นคงปลอดภัยทางสารสนเทศของบริษัทฯ

๓. คุณสมบัติของผู้ยื่นข้อเสนอ

(๑) ผู้ยื่นขอเสนอจะต้องมีคุณสมบัติตามที่ระบุในแบบเอกสารเชิญชวนของคณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐหรือคณะกรรมการวินิจฉัยปัญหาการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนด

(๒) ผู้ยื่นข้อเสนอจะต้องเป็น นิติบุคคล ผู้มีอาชีพขายพัสดุที่ประกวดราคาอิเล็กทรอนิกส์ดังกล่าว

(๓) ผู้ยื่นข้อเสนอต้องไม่มีกรรมการหรือพนักงาน บวท. เป็นผู้จัดการ หุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของบุคคลธรรมดาหรือของนิติบุคคล เป็นหุ้นส่วนในห้างหุ้นส่วนสามัญหรือห้างหุ้นส่วนจำกัด เป็นผู้ถือหุ้นรายใหญ่ในบริษัทจำกัดหรือบริษัทจำกัดมหาชน หรือเป็นที่ปรึกษาของกิจการนั้น

(๔) ผู้ยื่นข้อเสนอต้องเป็นตัวแทนจำหน่ายที่ได้รับการแต่งตั้งจากผู้ผลิตหรือเจ้าของผลิตภัณฑ์ หรือตัวแทนจำหน่ายในประเทศไทย สำหรับระบบอุปกรณ์ที่เสนอในโครงการโดยต้องแสดงเอกสารในวันเสนอราคา

๔. รายละเอียดคุณลักษณะเฉพาะ

ดังรายละเอียดในเอกสารแนบท้ายขอบเขตงานและรายละเอียดคุณลักษณะเฉพาะ

๕. การส่งมอบ

ผู้ขายจะต้องส่งมอบอุปกรณ์ทั้งหมดในโครงการ ณ สำนักงานใหญ่ทุ่งมหาเมฆ ให้แล้วเสร็จภายในเวลา ๑๕๐ วัน (ร้อยห้าสิบวัน) นับจากวันที่ บวท. ลงนามสัญญา

๖. หลักเกณฑ์ในการพิจารณาคัดเลือกข้อเสนอ

เกณฑ์ราคา

๗. วงเงินงบประมาณที่ได้รับจัดสรร

๓๐,๐๐๐,๐๐๐ บาท

๘. งวดงานและการจ่ายเงิน

ผู้ขายจะต้องส่งมอบพร้อมติดตั้งระบบรวบรวม วิเคราะห์ และตอบสนองความปลอดภัยการใช้งานระบบสารสนเทศโดยอัตโนมัติ จำนวน ๑ ระบบ และอุปกรณ์ประกอบพร้อมฝึกอบรมให้แล้วเสร็จทั้งหมดภายใน ๑๕๐ วัน นับถัดจากวันลงนามสัญญาซื้อขาย โดยมีรายละเอียดการส่งมอบดังนี้

๘.๑ ผู้ขายจะต้องดำเนินการนำอุปกรณ์เข้ามาในราชอาณาจักรไทย ส่งมอบพร้อมติดตั้ง ระบบรวบรวม วิเคราะห์ และตอบสนองความปลอดภัยการใช้งานระบบสารสนเทศโดยอัตโนมัติ ให้กับ บวท. ให้แล้วเสร็จภายใน ๑๕๐ วัน นับถัดจากวันลงนามสัญญาซื้อขาย

๘.๒ ผู้ขายต้องดำเนินการฝึกอบรมเกี่ยวกับระบบรวบรวม วิเคราะห์ และตอบสนองความปลอดภัยการใช้งานระบบสารสนเทศโดยอัตโนมัติ ที่เสนอให้กับเจ้าหน้าที่ บวท. ตามข้อ ๑๒. ให้แล้วเสร็จภายใน ๑๕๐ วัน นับถัดจากวันลงนามสัญญาซื้อขาย

ผู้ซื้อจะจ่ายเงินให้แก่ผู้ขายเป็นจำนวนเงินซึ่งได้รวมภาษีมูลค่าเพิ่มตลอดจนภาษีอากรอื่นๆ และค่าใช้จ่ายทั้งปวงด้วยแล้ว โดยกำหนดการจ่ายเงิน ดังนี้

๘.๓ การจ่ายเงิน จ่ายงวดเดียว (ร้อยละ ๑๐๐) เมื่อผู้ขายได้ดำเนินการตามข้อ ๘.๑ และ ๘.๒ ให้ถูกต้องครบถ้วนทุกประการ และคณะกรรมการตรวจรับพัสดุได้ทำการตรวจรับเรียบร้อยแล้ว

๙. อัตราค่าปรับ

บวท. จะคิดค่าปรับในอัตราร้อยละ ๐.๒ (0.2%) ต่อวันของวงเงินรวมตามสัญญานับถัดจากวันครบกำหนดตามสัญญาจนถึงวันส่งมอบการติดตั้งให้แก่ บวท. จนถูกต้องครบถ้วน ในกรณีการจัดหาสิ่งของที่ประกอบกันเป็นชุด ถ้าขาดส่วนประกอบส่วนใดส่วนหนึ่งไปแล้วจะไม่สามารถใช้งานได้สมบูรณ์ แม้ผู้ขายจะส่งมอบสิ่งของภายในกำหนดตามสัญญา แต่ยังขาดส่วนประกอบบางส่วน ต่อมาได้ส่งมอบส่วนประกอบที่ยังขาดนั้นเกินกำหนดสัญญาให้ถือว่าไม่ได้ส่งมอบสิ่งของนั้นเลยให้ปรับเต็มราคา

๑๐. การรับประกัน

ผู้ขายซึ่งได้ทำข้อตกลงเป็นหนังสือหรือสัญญาซื้อขายจะต้องรับประกันความชำรุดบกพร่องของอุปกรณ์ดังนี้

๑๐.๑ ระยะเวลาการรับประกันระบบ/อุปกรณ์ทั้งโครงการ เป็นเวลาอย่างน้อย ๓ ปี (สามปี) และต้องรวมสิทธิ์การอัปเดตฐานข้อมูลภัยคุกคามและซอฟต์แวร์ที่จำเป็นต่อการทำงานด้านความมั่นคงปลอดภัยของระบบตลอดระยะเวลาการรับประกัน นับจากวันที่ บวท. รับมอบสิ่งของครบถ้วนตามสัญญา

๑๐.๒ ถ้าปรากฏว่าสิ่งของที่ส่งมอบดังกล่าวชำรุด ด้วยเหตุใดๆ ก็ตาม ผู้ขายต้องรีบจัดการนำไปซ่อมแซม แก้ไขหรือนำของใหม่มาเปลี่ยนให้เสร็จเรียบร้อยภายใน ๓๐ วัน นับถัดจากวันที่ได้รับแจ้งความชำรุดบกพร่อง

๑๐.๓ กรณีมีอุปกรณ์ใด ๆ ขัดข้องแล้วไม่สามารถแก้ไข ซ่อมแซมที่หน้างานได้ มีความจำเป็นจะต้องนำกลับไปซ่อมนอกสถานที่หรือต้องจัดส่งไปซ่อมยังบริษัทเจ้าของผลิตภัณฑ์ จะต้องนำอุปกรณ์สำรองมาเปลี่ยนภายใน ๗ วัน นับจากวันที่ได้รับแจ้งความชำรุดบกพร่อง ให้สามารถใช้งานทดแทนได้ จนกว่าอุปกรณ์ที่ขัดข้องจะซ่อมเสร็จ โดยไม่มีค่าใช้จ่ายเพิ่มเติมแต่อย่างใด

๑๑. หน้าที่ของผู้ขาย

๑๑.๑ ผู้ขายต้องส่งมอบพร้อมติดตั้งระบบรวบรวม วิเคราะห์ และตอบสนองความปลอดภัยการใช้งานระบบสารสนเทศโดยอัตโนมัติ และดำเนินการอบรมให้กับ บวท. ให้แล้วเสร็จภายใน ๑๕๐ วัน นับถัดจากวันลงนามสัญญาซื้อขาย

๑๑.๒ ผู้ขายจะต้องทำการทดสอบระบบ (VA Scan) พร้อม Hardening อุปกรณ์ในโครงการ หากพบช่องโหว่ต้องดำเนินการแก้ไขและทดสอบระบบอีกครั้ง รวมทั้งต้องจัดทำคู่มือ Configuration Security Baseline โดยต้องส่งแผนการทดสอบระบบให้คณะกรรมการตรวจรับพัสดุพิจารณาเห็นชอบก่อนดำเนินการติดตั้งไม่น้อยกว่า ๗ วัน

๑๑.๓ ผู้ขายต้องเชื่อมต่อระบบที่กำหนดไว้ในหัวข้อที่ ๔. รายละเอียดคุณลักษณะเฉพาะ เข้ากับระบบของ บวท. พร้อมทั้งร่วมดำเนินการทดสอบระบบรวบรวม วิเคราะห์ และตอบสนองความปลอดภัยการใช้งานระบบสารสนเทศโดยอัตโนมัติ กับ บวท. ให้แล้วเสร็จทั้งหมด

๑๑.๔ ผู้ขายจะต้องจัดทำพร้อมส่งมอบคู่มือการติดตั้ง และ คู่มือการซ่อมบำรุง ระบบรวบรวม วิเคราะห์ และตอบสนองความปลอดภัยการใช้งานระบบสารสนเทศโดยอัตโนมัติ ให้แล้วเสร็จภายใน ๑๕๐ วัน นับถัดจากวันลงนามสัญญาซื้อขาย

๑๑.๕ ผู้ขายต้องดำเนินการฝึกอบรมเกี่ยวกับระบบรวบรวม วิเคราะห์ และตอบสนองความปลอดภัยการใช้งานระบบสารสนเทศโดยอัตโนมัติ ที่เสนอให้กับเจ้าหน้าที่ บวท. ตามข้อ ๑๒. ให้แล้วเสร็จภายใน ๑๕๐ วัน นับถัดจากวันลงนามสัญญาซื้อขาย

๑๑.๖ ในกรณีที่ต้องมีอุปกรณ์เพิ่มเติม เพื่อให้อุปกรณ์สามารถทำงานได้ตาม Function ที่กำหนดในหัวข้อที่ ๔. รายละเอียดคุณลักษณะเฉพาะ ผู้ขายต้องจัดหาอุปกรณ์ดังกล่าวส่งมอบให้ บวท. โดยไม่มีค่าใช้จ่ายเพิ่มเติม

๑๒. การอบรม

๑๒.๑ ผู้ขายต้องดำเนินการฝึกอบรมเกี่ยวกับอุปกรณ์ Application Firewall และ อุปกรณ์ Network Traffic ในโครงการจัดหาพร้อมติดตั้งระบบรวบรวม วิเคราะห์ และตอบสนองความปลอดภัยการใช้งานระบบสารสนเทศโดยอัตโนมัตินี้ ให้กับเจ้าหน้าที่ บวท. โดยอบรมแบบ onsite จำนวนไม่เกิน ๑๐ คน และแบบ online ไม่จำกัดจำนวนผู้เข้าอบรม เป็นจำนวนไม่น้อยกว่า ๑ รุ่นเป็นเวลาไม่น้อยกว่า ๕ วัน เพื่อให้ผู้เข้ารับการฝึกอบรมมีความรู้ความเข้าใจเกี่ยวกับการทำงานของระบบ/อุปกรณ์ สามารถทำการติดตั้งใช้งาน โยกย้าย บำรุงรักษา และแก้ไขปัญหาเมื่อเกิดเหตุขัดข้องได้

๑๒.๒ ผู้ขายต้องดำเนินการฝึกอบรมเกี่ยวกับ ระบบ Security Automation Analysis และ ระบบ Attack Surface Management ในโครงการจัดหาพร้อมติดตั้งระบบรวบรวม วิเคราะห์ และตอบสนองความปลอดภัยการใช้งานระบบสารสนเทศโดยอัตโนมัตินี้ ให้กับเจ้าหน้าที่ บวท. โดยอบรมแบบ onsite จำนวนไม่เกิน ๑๐ คน และแบบ online ไม่จำกัดจำนวนผู้เข้าอบรม เป็นจำนวนไม่น้อยกว่า ๑ รุ่นเป็นเวลาไม่น้อยกว่า ๕ วัน เพื่อให้ผู้เข้ารับการฝึกอบรมมีความรู้ความเข้าใจเกี่ยวกับการทำงานของระบบ/อุปกรณ์ สามารถทำการติดตั้งใช้งาน โยกย้าย บำรุงรักษา และแก้ไขปัญหาเมื่อเกิดเหตุขัดข้องได้

๑๒.๓ ผู้ขายต้องรับผิดชอบค่าใช้จ่ายในการจัดหาวิทยากร สถานที่ในการอบรมในเขตกรุงเทพฯ หรือปริมณฑล และห้องอบรม Online พร้อมเอกสารสำหรับการฝึกอบรม และอุปกรณ์ต่างๆ ในการฝึกอบรมให้ครบถ้วนตามจำนวนผู้เข้ารับการฝึกอบรม

๑๒.๔ การฝึกอบรมต้องอบรมโดยวิทยากรจากเจ้าของผลิตภัณฑ์หรือตัวแทนจำหน่าย ที่มีประสบการณ์/ความสามารถเป็นอย่างดีในการฝึกอบรม และมีความรู้เกี่ยวกับอุปกรณ์ ทั้งนี้หากพบว่าวิทยากรผู้ฝึกอบรม ไม่สามารถดำเนินการฝึกอบรมได้ตามวัตถุประสงค์ บวท. ขอสงวนสิทธิ์ในการให้ผู้ขายเปลี่ยนตัววิทยากร และเริ่มการฝึกอบรมใหม่ และผู้ขายต้องเป็นผู้รับผิดชอบค่าใช้จ่ายที่เกิดขึ้นทั้งหมด

๑๒.๔ ผู้ขายจะต้องส่ง Course Outline ให้คณะกรรมการตรวจรับพัสดุ พิจารณาก่อนการดำเนินการ ๑๐ วัน

๑๓. <u>การยืนราคา</u>

ผู้ขายจะต้องกำหนดยืนราคาไม่น้อยกว่า ๑๒๐ วัน (หนึ่งร้อยยี่สิบวัน)

เอกสารแนบท้ายขอบเขตงานและรายละเอียดคุณลักษณะเฉพาะ โครงการจัดหาพร้อมติดตั้งระบบรวบรวม วิเคราะห์ และตอบสนองความปลอดภัยการใช้งานระบบสารสนเทศโดยอัตโนมัติ จำนวน ๑ ระบบ

๑. คุณสมบัติระบบตอบสนองความปลอดภัยการใช้งานสารสนเทศอัตโนมัติจำนวน ๑ ระบบ มีคุณสมบัติดังนี้

๑.๑.อุปกรณ์รักษาความปลอดภัยบนเครือข่ายคอมพิวเตอร์ในระดับแอพพลิเคชั่น (Application Firewall) จำนวน ๒ ชุด แต่ละชุดโดยมีคุณสมบัติอย่างน้อยดังนี้

๑.๑.๑. เป็นอุปกรณ์ประเภท Next-Generation Firewall (NGFW) แบบ Appliance-Based

๑.๑.๒. มี Network Interface อย่างน้อย ดังนี้

๑.๑.๒.๑. Interface แบบ 1G (RJ45) หรือดีกว่าไม่น้อยกว่า ๔ พอร์ท

๑.๑.๒.๒. Interface แบบ 10G (RJ45) หรือดีกว่าไม่น้อยกว่า ๔ พอร์ท

๑.๑.๒.๓. Interface แบบ 10G/25G SFP+/SFP28 หรือดีกว่า ไม่น้อยกว่า ๔ ช่อง พร้อมเสนอ Transceiver Module แบบ 25GBase-LR จำนวนชุดละ 2 Module และ 10GBase-LR จำนวนชุดละ 2 Module

๑.๑.๓. มี Interface HA แบบ 1G (RJ45) หรือดีกว่าไม่น้อยกว่า ๑ พอร์ท และมี Interface แบบ 1G (RJ45) หรือดีกว่าสำหรับบริหารจัดการ (Management Port) ไม่น้อยกว่า ๑ พอร์ท โดยทั้งหมดไม่นับรวมกับ interface จากข้อที่ ๑.๑.๒.

๑.๑.๔. มี Interface สำหรับ Console ไม่น้อยกว่า ๑ พอร์ท พร้อมกับสาย Console

๑.๑.๕. มี Application Firewall Throughput ไม่น้อยกว่า 30 Gbps ในแบบ Appmix หรือ Enterprise test conditions หรือ Enterprise traffic mix

๑.๑.๖. มี Threat prevention Throughput ไม่น้อยกว่า 14 Gbps ในแบบ Appmix หรือ Enterprise test conditions หรือ Enterprise traffic mix

๑.๑.๗. มี Concurrent Sessions ไม่น้อยกว่า 2,800,000 sessions ที่สามารถประมวลผลพร้อมกันได้ในสภาพแวดล้อมปกติ และมี New Sessions ไม่น้อยกว่า 250,000 Sessions ต่อวินาที

๑.๑.๘. มี storage ชนิด SSD สำหรับจัดเก็บข้อมูลระบบ (System Storage) ขนาดไม่ต่ำกว่า 480 GB หรือดีกว่า

๑.๑.๙. สามารถรองรับการทำงานของ Routing Protocols แบบ Static, RIP, BGP, OSPF, Multicast และ Policy Based Forwarding หรือ Policy Based Routing ได้เป็นอย่างน้อย

๑.๑.๑๐. สามารถทำการตรวจสอบ Traffic ที่เข้ารหัส SSL ด้วยการทำ SSL decryption (ทั้งแบบ Inbound และ Outbound) หรือนำเสนอระบบอื่นๆเพิ่มเติมที่มีมาตรฐานเทียบเท่า เพื่อให้สามารถทำได้ตามข้อกำหนด

๑.๑.๑๑. สามารถทำงานร่วมกับระบบการพิสูจน์ตัวตน (Authentication Systems) ได้แก่ Active Directory, LDAP, Radius เพื่อระบุตัวตนผู้ใช้งาน (User Identity) ได้เป็นอย่างน้อย

๑.๑.๑๒. สามารถควบคุมประเภทของไฟล์ (File Type Control) ที่อนุญาตให้ Download หรือ Upload ผ่านแต่ละ Application ได้

๑.๑.๑๓. สามารถตรวจสอบและป้องกันการรั่วไหลของข้อมูล (Data Filtering/DLP/Data Patterns) จากเครือข่าย

๑.๑.๑๔. สามารถตรวจจับและป้องกันภัยคุกคาม (Threat Prevention) ประเภท Vulnerability และ Malware/Spyware ได้ โดยสามารถทำการอัพเดท Signature และ Threat Intelligence แบบอัตโนมัติ เพื่อให้การป้องกันเป็นปัจจุบัน

๑.๑.๑๕. สามารถตรวจจับและป้องกันภัยคุกคามประเภท Zero-Day Malware ได้แบบ Inline Prevention (Real time) และสามารถเสนอระบบเสริม (เช่น Sandboxing, Advanced Threat Prevention) เพื่อให้เป็นไปตามข้อกำหนด

๑.๑.๑๖. สามารถกำหนดนโยบายและควบคุมการเข้าถึง website (URL Filtering) สามารถติดตามและควบคุมการเข้าถึงเว็บได้ตาม Category, Block list, Allow list ที่กำหนดได้

๑.๑.๑๗. สามารถบริหารจัดการอุปกรณ์แบบ Web-based Management (HTTPS) , Command Line Interface ได้

๑.๑.๑๘. สามารถสรุปและแสดงผลข้อมูลในรูปแบบกราฟิก (Graphical Report) รวมถึงรองรับการสร้างรายงานได้อย่างน้อยดังนี้

๑.๑.๑๘.๑. Top Application, Application Category

๑.๑.๑๘.๒. Top Source, User, Destination

๑.๑.๑๘.๓. User activity report

๑.๑.๑๙. สามารถสร้างรายงานและปรับแต่งรายงานได้ตามความต้องการ

๑.๑.๒๐. รองรับการติดตั้งเพื่อทำงานในรูปแบบ High Availability (HA) ได้ทั้งแบบ Active-Active และ Active-Passive

๑.๑.๒๑. มีแหล่งจ่ายไฟฟ้า (Power Supply) แบบ redundant หรือรองรับการถอดเปลี่ยน (Hot-swappable) ได้ โดยไม่มีผลกระทบต่อการให้บริการ

๑.๑.๒๒. ต้องได้รับการจัดอันดับให้อยู่ในกลุ่ม Leader ของ Gartner Magic Quadrant ในกลุ่มผลิตภัณฑ์ Hybrid Mesh Firewalls ปี ๒๐๒๕ หรือปีล่าสุด

๑.๑.๒๓. ต้องรับประกันอุปกรณ์เป็นเวลาอย่างน้อย ๓ ปี และต้องรวมสิทธิ์การอัปเดตฐานข้อมูลภัยคุกคามและซอฟต์แวร์ที่จำเป็นต่อการทำงานด้านความมั่นคงปลอดภัยของระบบตลอดระยะเวลาการรับประกัน

๑.๑.๒๔. ผู้เสนอราคาต้องแสดงหลักฐานการมีสิทธิ์เสนอราคาสำหรับโครงการนี้ โดยต้องได้รับการแต่งตั้งเป็นตัวแทนจำหน่ายจากบริษัทเจ้าของผลิตภัณฑ์ พร้อมการได้รับการบริการหลังการขาย และได้รับการสนับสนุนทางด้านเทคนิค ตลอดช่วงระยะเวลาการรับประกันโดยตรงจากบริษัทฯ เจ้าของผลิตภัณฑ์หรือบริษัทฯ สาขาของเจ้าของผลิตภัณฑ์ประจำประเทศไทย สำหรับผลิตภัณฑ์ที่เสนอในโครงการนี้โดยเฉพาะ โดยมีเอกสารหรือหลักฐานแสดง ณ วันยื่นเอกสารประกวดราคาอิเล็กทรอนิกส์ เพื่อรองรับการให้บริการทางเทคนิคและบริการหลังการขายเป็นอย่างดี

๑.๒. อุปกรณ์เฝ้าระวังการโจมตีและวิเคราะห์ภัยคุกคามบนระบบเครือข่าย (Network Traffic Analysis) จำนวน ๑ ชุด โดยมีคุณสมบัติดังนี้

๑.๒.๑. เป็นอุปกรณ์แบบ Appliance-Based หรือ Virtual appliance ที่ออกแบบมาเพื่อการวิเคราะห์ ตรวจจับ และเฝ้าระวังภัยคุกคามทางไซเบอร์บนเครือข่าย (Network-based threat detection) โดยเฉพาะ และต้องอยู่ภายใต้ผู้ผลิตเดียวกันกับอุปกรณ์รักษาความปลอดภัยเครือข่ายในระดับแอปพลิเคชัน (Application Firewall) ที่นำเสนอในโครงการนี้

๑.๒.๒. มี Network Interface แบบ 1G (RJ45) หรือดีกว่าไม่น้อยกว่า ๘ พอร์ท

๑.๒.๓. มี Interface แบบ 1G (RJ45) หรือดีกว่าสำหรับบริหารจัดการ (Management Port) ไม่น้อยกว่า ๑ พอร์ท โดยทั้งหมดไม่นับรวมกับ interface จากข้อที่ ๑.๒.๒.

๑.๒.๔. มี Interface สำหรับ Console ไม่น้อยกว่า ๑ พอร์ท พร้อมกับสาย Console

๑.๒.๕. มี Application Firewall Throughput ไม่น้อยกว่า 4.5 Gbps ในแบบ Appmix หรือ Enterprise test conditions หรือ Enterprise traffic mix

๑.๒.๖. มี Threat prevention Throughput ไม่น้อยกว่า 3 Gbps ในแบบ Appmix หรือ Enterprise test conditions หรือ Enterprise traffic mix

๑.๒.๗. มี Concurrent Sessions ไม่น้อยกว่า 400,000 sessions ที่สามารถประมวลผลพร้อมกันได้ในสภาพแวดล้อมปกติ และมี New Sessions ไม่น้อยกว่า 65,000 Sessions ต่อวินาที

๑.๒.๘. มี storage ชนิด SSD หรือ eMMC สำหรับจัดเก็บข้อมูลระบบ (System Storage) ขนาดไม่ต่ำกว่า 128GB หรือดีกว่า

๑.๒.๙. สามารถติดตั้งในรูปแบบ Transparent Mode, Monitoring Mode (Tap/Span/Mirror), L2 และ L3 หรือเทียบเท่าได้

๑.๒.๑๐. สามารถทำการตรวจสอบ Traffic ที่เข้ารหัส SSL ด้วยการทำ SSL decryption (ทั้งแบบ Inbound และ Outbound) หรือนำเสนอระบบอื่นๆเพิ่มเติมที่มีมาตรฐานเทียบเท่า เพื่อให้สามารถทำได้ตามข้อกำหนด

๑.๒.๑๑. สามารถทำงานร่วมกับระบบการพิสูจน์ตัวตน (Authentication Systems) ได้แก่ Active Directory, LDAP, Radius เพื่อระบุตัวตนผู้ใช้งาน (User Identity) ได้เป็นอย่างน้อย

๑.๒.๑๒. สามารถตรวจจับและเฝ้าระวังการถ่ายโอนไฟล์ (File Type Control) ที่อนุญาตให้ Download หรือ Upload ผ่านแต่ละ Application ได้

๑.๒.๑๓. สามารถตรวจจับและเฝ้าระวังการรั่วไหลของข้อมูล (Data Filtering/DLP/Data Patterns) ออกจากระบบเครือข่าย

๑.๒.๑๔. สามารถตรวจจับและเฝ้าระวังภัยคุกคาม (Threat Prevention) ประเภท Vulnerability และ Malware/Spyware ได้ โดยสามารถทำการอัพเดท Signature และ Threat Intelligence แบบอัตโนมัติ เพื่อให้การป้องกันเป็นปัจจุบัน

๑.๒.๑๕. สามารถการตรวจจับและเฝ้าระวัง ภัยคุกคามประเภท Zero-Day Malware ได้แบบ Inline Prevention (Real-time) และสามารถเสนอระบบเสริม (เช่น Sandboxing, Advanced Threat Prevention) เพื่อให้เป็นไปตามข้อกำหนด

๑.๒.๑๖. สามารถกำหนดนโยบายและเฝ้าระวังการเข้าถึง website (URL Filtering) สามารถติดตามและเฝ้าระวัง การเข้าถึงเว็บได้ตาม Category, Block list, Allow list ที่กำหนดได้

๑.๒.๑๗. สามารถบริหารจัดการอุปกรณ์แบบ Web-based Management (HTTPS) , Command Line Interface

๑.๒.๑๘. สามารถรับข้อมูล Log จากระบบภายนอก เช่น Proxy, Authentication Server, Wi-Fi Controller หรือระบบอื่นที่มีอยู่ได้ เพื่อใช้ในการพิสูจน์ตัวตน หรือ ดำเนินการเชื่อมโยงข้อมูลผู้ใช้งาน (User Identity Mapping) ของผู้ใช้งานที่อยู่ในระบบภายนอกข้างต้น หรือนำเสนอระบบอื่นๆที่มีมาตรฐานเทียบเท่าเพิ่มเติม เพื่อให้สามารถทำได้ตามข้อกำหนด

๑.๒.๑๙. สามารถสร้างรายงานและปรับแต่งรายงานได้ตามความต้องการ

๑.๒.๒๐. ต้องรับประกันอุปกรณ์เป็นเวลาอย่างน้อย ๓ ปี และต้องรวมสิทธิ์การอัปเดตฐานข้อมูลภัยคุกคามและซอฟต์แวร์ที่จำเป็นต่อการทำงานด้านความมั่นคงปลอดภัยของระบบตลอดระยะเวลาการรับประกัน

๑.๒.๒๑. ผู้เสนอราคาต้องแสดงหลักฐานการมีสิทธิ์เสนอราคาสำหรับโครงการนี้ โดยต้องได้รับการแต่งตั้งเป็นตัวแทนจำหน่ายจากบริษัทเจ้าของผลิตภัณฑ์ พร้อมการได้รับการบริการหลังการขาย และได้รับการสนับสนุนทางด้านเทคนิค ตลอดช่วงระยะเวลาการรับประกันโดยตรงจากบริษัทฯ เจ้าของผลิตภัณฑ์หรือบริษัทฯ สาขาของเจ้าของผลิตภัณฑ์ประจำประเทศไทย สำหรับผลิตภัณฑ์ที่เสนอในโครงการนี้โดยเฉพาะ โดยมีเอกสารหรือหลักฐานแสดง ณ วันยื่นเอกสารประกวดราคาอิเล็กทรอนิกส์ เพื่อรองรับการให้บริการทางเทคนิคและบริการหลังการขายเป็นอย่างดี

๑.๓. ระบบรวบรวมและวิเคราะห์เพื่อหาสาเหตุของภัยคุกคามทางไซเบอร์แบบอัตโนมัติ จำนวน ๑ ระบบ โดยมีคุณสมบัติดังนี้

๑.๓.๑. เป็นระบบที่ให้บริการในรูปแบบ Software as a Service (SaaS) หรือ ทำงานบนระบบคลาวด์ (Cloud-based) โดย ผู้ให้บริการต้องได้รับการรับรองมาตรฐาน ด้านความมั่นคงปลอดภัยสารสนเทศ (ISO/IEC 27001) เป็นอย่างน้อย

๑.๓.๒. เป็นระบบที่ถูกออกแบบมาเพื่อให้สามารถบริหารจัดการและตอบสนองต่อเหตุการณ์ภัยคุกคามที่เกิดขึ้นบนระบบเครือข่ายคอมพิวเตอร์ได้อย่างอัตโนมัติ และมีระบบ Threat Intelligence หรือ Threat Prevention อยู่ภายในระบบเดียวกัน แบบพร้อมใช้งานภายในระบบดังกล่าว หรือนำเสนอ Threat Intelligence เพิ่มเติม

๑.๓.๓. ระบบที่นำเสนอต้องมีลิขสิทธิ์การใช้งานสำหรับผู้ใช้งานในระดับ Administrator ไม่น้อยกว่า ๑๐ ผู้ใช้งาน และระดับ Operation ไม่น้อยกว่า ๑๒ ผู้ใช้งาน

๑.๓.๔. สามารถเข้าใช้งานในรูปแบบของ web base GUI ผ่าน Browser เช่น Chrome หรือ Firefox หรือ Microsoft Edge เป็นอย่างน้อย

๑.๓.๕. มีการรับประกันความพร้อมใช้งาน (Service Level Agreement: SLA) ไม่น้อยกว่า 99.9% เพื่อให้มั่นใจว่าระบบสามารถให้บริการได้อย่างต่อเนื่อง

๑.๓.๖. สามารถพิสูจน์ตัวตนของผู้ใช้ระบบบน Local system หรือ รองรับการทำ Single sign-on (SSO) ผ่านโปรโตคอล SAML2.0 เป็นอย่างน้อย

๑.๓.๗. สามารถจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยด้านสารสนเทศ (Security Incident) ได้ โดยสามารถมอบหมายเหตุการณ์ให้กับผู้ดูแลแต่ละคนได้

๑.๓.๘. ระบบสามารถทำงานร่วมกันระหว่างเจ้าหน้าที่ด้านความมั่นคงปลอดภัยไซเบอร์ ผ่านหน้าจอ Incident หรือ Case Management โดยสามารถแสดงข้อมูลเหตุการณ์ การวิเคราะห์ และการตอบสนองร่วมกันได้ในลักษณะ Virtual War Room หรือโต้ตอบผ่านความเห็น (Comment) ได้

๑.๓.๙. ระบบสามารถกำหนด Response Workflow หรือ Automation Workflow ผ่านส่วนติดต่อผู้ใช้งานแบบกราฟิก (เช่น Drag and Drop หรือ Rule-based) โดยมี Predefined Integration / Connector และ Predefined Automated Response Action ให้พร้อมใช้งาน (Out-of-Box)

๑.๓.๑๐. ระบบต้องสามารถสร้างและเรียกใช้งานกระบวนการตอบสนองต่อเหตุการณ์ (Response Workflow) ได้ทั้งแบบอัตโนมัติ (Automated Response) หรือ กึ่งอัตโนมัติ (Semi-Automated)

๑.๓.๑๑. ระบบต้องรองรับการออกแบบกระบวนการตอบสนองต่อเหตุการณ์ (Response Workflow) โดยมีความสามารถอย่างน้อยดังนี้

๑.๓.๑๑.๑. รองรับ Manual Action / Analyst Task ภายใน Incident

๑.๓.๑๑.๒. รองรับการกำหนดขั้นตอนการตัดสินใจ การอนุมัติ หรือการยืนยันจากผู้ใช้งาน ก่อนดำเนินการตอบสนองในขั้นตอนถัดไป (Approval)

๑.๓.๑๑.๓. รองรับการกำหนดเงื่อนไข (Condition-based Logic) หรือการวนซ้ำของกระบวนการทำงานตามเหตุการณ์

๑.๓.๑๑.๔. รองรับการกำหนดพฤติกรรมเมื่อเกิดข้อผิดพลาด เช่น การหยุดการทำงาน การแจ้งเตือน หรือการดำเนินการต่อโดยอัตโนมัติ

๑.๓.๑๒. ระบบสามารถตรวจสอบโดยใช้ Indicator of Compromise (IOC) จากข้อมูลที่อยู่ภายในไฟล์ เช่น PDF หรือ Image โดยอัตโนมัติ ผ่านเทคโนโลยีการวิเคราะห์ไฟล์หรือการประมวลผลข้อมูล (เช่น OCR, File Analysis หรือ Threat Intelligence)

๑.๓.๑๓. ระบบสามารถจัดการ Response Workflow หรือมีความสามารถในการย้อนกลับ (Revert) เพื่อให้สามารถย้อนกลับหรือแก้ไขเมื่อเกิดความผิดพลาดได้

๑.๓.๑๔. ระบบสามารถจำลองหรือทดสอบ Response Workflow ก่อนนำไปใช้งานจริง เพื่อประเมินผลกระทบและความถูกต้องของการตอบสนอง

๑.๓.๑๕. ระบบต้องสามารถรับและบริหารจัดการข้อมูลภัยคุกคามจากแหล่ง Threat Intelligence ที่เชื่อถือได้ และเป็นที่ยอมรับในระดับสากล เช่น MITRE ATT&CK, Cyber Threat Alliance (CTA) หรือองค์กรด้าน Cybersecurity อื่น ๆ ที่เป็นที่ยอมรับ

๑.๓.๑๖. ระบบสามารถส่งอีเมลโต้ตอบกับผู้ใช้งานเพื่อขอให้ดำเนินการหรือให้ข้อมูลเพิ่มเติม

๑.๓.๑๗. ระบบสามารถปรับแต่ง Response Workflow ผ่าน Custom Script หรือ API อย่างน้อยหนึ่งภาษา เช่น Python, PowerShell, JavaScript หรือ REST API

๑.๓.๑๘. ระบบสามารถจัดเก็บและบริหารจัดการ Indicator ภายในระบบ Threat Intelligence หรือ Threat Repository

๑.๓.๑๙. ระบบต้องมี Dashboard สำหรับแสดงภาพรวมเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ (Incident Review) โดยสามารถแสดงรายละเอียดเหตุการณ์ ระดับความรุนแรง (Severity) และระดับความเร่งด่วน (Urgency) หรือระดับความเชื่อถือ (Confidence) เพื่อสนับสนุนการจัดลำดับความสำคัญในการตอบสนอง

๑.๓.๒๐. ระบบที่นำเสนอต้องสามารถแสดงผล (Dashboard) และรายงาน (Report) ได้ โดยผู้ใช้งานสามารถกำหนดรูปแบบการแสดงผลและโครงสร้างรายงานตามความต้องการ และสามารถจัดทำรายงานในรูปแบบไฟล์ PDF ได้เป็นอย่างน้อย

๑.๓.๒๑. ระบบที่นำเสนอต้องสามารถแจ้งเตือน (Notification) และแสดงข้อมูล Audit Log ทั้งจาก Agent และ Management ผ่านทาง E-mail, Collaboration Platform (เช่น Slack หรือเทียบเท่า) หรือ Syslog ได้ รวมทั้งสามารถแจ้งเตือนและแสดงข้อมูลเหตุการณ์ด้านความปลอดภัย โดยผู้ใช้งานสามารถกำหนดการแจ้งเตือนตามระดับความรุนแรง (Severity Level) ได้

๑.๓.๒๒. ระบบต้องสามารถแจ้งเตือนโดยอัตโนมัติเมื่อปริมาณข้อมูลที่จัดเก็บใกล้ถึงหรือเกินขีดจำกัดของ License ที่กำหนด และต้องมีมาตรการป้องกันการสูญเสียข้อมูลในกรณีที่สามารถดำเนินการได้

๑.๓.๒๓. ระบบที่นำเสนอต้องสามารถนำข้อมูลมาประมวลผลเพื่อวิเคราะห์ภัยคุกคาม และสามารถสืบค้นย้อนหลังได้ไม่น้อยกว่า ๓๐ วัน

๑.๓.๒๔. ระบบสามารถรับข้อมูล Log ได้หลากหลายรูปแบบ เช่น Syslog (UDP/TCP), HTTP/HTTPS หรือการเชื่อมต่อผ่าน API โดยอาจเป็นแบบ Agent-based หรือ Agentless ตามความเหมาะสม

๑.๓.๒๕. ระบบต้องสามารถรับเหตุการณ์ (Log) จาก Log Source ได้ในรูปแบบ Syslog, CEF ได้เป็นอย่างน้อย

๑.๓.๒๖. ระบบที่นำเสนอต้องสามารถทำ Normalization หรือ Correlation ข้อมูลเหตุการณ์ (Event, Log) ให้อยู่ในรูปแบบโครงสร้างข้อมูลที่เป็นมาตรฐานเดียวกัน เพื่อความสะดวกในการวิเคราะห์และการใช้งานข้อมูลร่วมกัน

๑.๓.๒๗. ระบบที่นำเสนอต้องมีการจัดเตรียม Predefined Analytic หรือ Detection Model หรือ UEBA หรือ Detection Catalog จากผู้ให้บริการ และสามารถรับการอัปเดตได้อย่างสม่ำเสมอ เพื่อรองรับภัยคุกคามใหม่ๆ และต้องครอบคลุม Use Case มาตรฐาน เช่น MITRE ATT&CK, Network Threat, Endpoint Threat เป็นต้น

๑.๓.๒๘. ระบบที่นำเสนอต้องสามารถวิเคราะห์และตรวจจับภัยคุกคามบนระบบเครือข่ายโดยใช้เทคโนโลยี Machine Learning และ AI (ML/AI) ในการวิเคราะห์พฤติกรรม โดยอาศัยการหาความสัมพันธ์ของข้อมูลที่ได้จาก Endpoint, Log ของอุปกรณ์ตรวจจับภัยคุกคามเครือข่ายระดับแอปพลิเคชัน (Network Sensor) เป็นต้น โดยทำงานในรูปแบบอัตโนมัติ

๑.๓.๒๙. รองรับการค้นหาและระบุภัยคุกคามที่เกิดขึ้น (Threat Hunting) ที่อาจไม่ถูกตรวจจับด้วย Signature-based detection โดยวิเคราะห์จากพฤติกรรมการใช้งานที่ผิดปกติ (Behavior Threat) และสามารถแสดงรายละเอียดของเครื่องปลายทาง เช่น Application, System Information, Process, Connection เป็นต้น

๑.๓.๓๐. ระบบต้องมีความสามารถในการสร้าง Rule หรือ Query โดยรองรับการใช้เงื่อนไขทางตรรกะ (Logical Operations) และกฎแบบซ้อน (Nested Rules) เพื่อให้สามารถรวม วิเคราะห์ ปรับเปลี่ยน และแสดงผลข้อมูลได้อย่างยืดหยุ่น เช่น การใช้ฟังก์ชันหรือคำสั่งในการประมวลผลข้อมูล (เช่น stats, eval, append, join, convert, rex, regex หรือเทียบเท่า)

๑.๓.๓๑. ระบบต้องมีความสามารถในการสืบค้น (Query) เพื่อสนับสนุนการทำงานด้านการวิเคราะห์และจัดการเหตุการณ์ ไม่ว่าจะเป็นการทำ Correlation, การรายงาน (Reporting) ตลอดจนการเชื่อมโยงข้อมูล Log เข้ากับข้อมูลบริบท เช่น ข้อมูลทรัพย์สิน (Assets) หรือข้อมูลผู้ใช้งาน (Users) เป็นต้น

๑.๓.๓๒. สามารถวิเคราะห์และเรียนรู้จากพฤติกรรมภายในระบบ (Behavior Analytics) โดยใช้เทคนิค เช่น Machine Learning (ML), Statistical Analysis และ Anomaly Detection เพื่อสร้างรูปแบบพฤติกรรมปกติ (Baseline) ของผู้ใช้งาน แอปพลิเคชัน และระบบเครือข่าย จากนั้นสามารถตรวจจับเหตุการณ์ที่เบี่ยงเบนออกจากค่าปกติได้โดยอัตโนมัติ พร้อมทั้งระบุความเสี่ยงหรือความผิดปกติที่อาจบ่งบอกถึงภัยคุกคาม เช่น การเข้าสู่ระบบผิดเวลา ปริมาณการรับส่งข้อมูลที่ผิดปกติ หรือการใช้งานแอปพลิเคชันที่ไม่เคยปรากฏมาก่อน ได้

๑.๓.๓๓. สามารถวิเคราะห์พฤติกรรมจาก User และ Asset ประเภท Suspicious authentication, Suspicious VPNs login, Brute force, password spray, and excessive logins, และ Irregular resource access เป็นอย่างน้อย จากพฤติกรรมปกติ (Baseline) แบบอัตโนมัติ

๑.๓.๓๔. ระบบต้องสามารถกำหนดค่า Service Level Agreement (SLA) ตามระดับความรุนแรงของเหตุการณ์ (Incident Severity) ได้

๑.๓.๓๕. ระบบรองรับความสามารถในการยกระดับความรุนแรงของเหตุการณ์ (Incident Severity Escalation) หรือสามารถติดตามเหตุการณ์ (Follow up) ที่มีความสำคัญได้

๑.๓.๓๖. ระบบต้องสามารถเชื่อมโยงเหตุการณ์ด้านความมั่นคงปลอดภัยกับกรอบการวิเคราะห์ MITRE ATT&CK เพื่อสนับสนุนการวิเคราะห์และการตอบสนองต่อภัยคุกคามอย่างเป็นระบบ

๑.๓.๓๗. ระบบต้องสามารถติดตามและบริหารจัดการสถานะของเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ (Incident Status Tracking) โดยต้องมีความสามารถในการจัดการวงจรชีวิตของเหตุการณ์ (Incident Lifecycle Management) หรือการสรุปเหตุการณ์ (Incident Summary) ตั้งแต่การตรวจพบ การวิเคราะห์ การตอบสนอง ไปจนถึงการปิดเหตุการณ์ พร้อมทั้งแสดงประวัติการดำเนินการย้อนหลัง (Audit Trail) เช่น วันเวลา ผู้ดำเนินการ และการกระทำที่เกิดขึ้น ในรูปแบบ Timeline หรือ List activities เพื่อให้สามารถตรวจสอบและติดตามความคืบหน้าได้อย่างเป็นระบบ

๑.๓.๓๘. ระบบสามารถบันทึกและแนบ Note หรือ Comment ภายใน Incident เพื่อใช้ในการสื่อสาร การประสานงาน และการติดตามผลการดำเนินงาน โดยต้องจัดเก็บข้อมูลพร้อมวันเวลาและผู้บันทึกอย่างถูกต้อง สามารถตรวจสอบย้อนหลังได้ และรองรับการเชื่อมโยงกับข้อมูลหรือหลักฐานที่เกี่ยวข้องกับเหตุการณ์

๑.๓.๓๙. ระบบต้องสามารถสืบค้นและเรียกดูข้อมูลที่เกี่ยวข้องกับเหตุการณ์ที่ผ่านมาได้อย่างมีประสิทธิภาพ เช่น Indicator of Compromise (IOC), รายละเอียดเหตุการณ์, ฟิลด์ข้อมูลที่เกี่ยวข้อง และความสัมพันธ์ของเหตุการณ์ เพื่อสนับสนุนการวิเคราะห์ การสอบสวน และการตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์

๑.๓.๔๐. ระบบต้องสามารถแสดงข้อมูลเหตุการณ์ภัยคุกคามทางไซเบอร์ (Incident Details) โดยมีรายละเอียดอย่างน้อยดังนี้

๑.๓.๔๐.๑. ประเภทของภัยคุกคาม

๑.๓.๔๐.๒. วันและเวลา เริ่มต้นและสิ้นสุดของภัยคุกคาม

๑.๓.๔๐.๓. แหล่งที่มา (Source) และปลายทาง (Destination) ที่เกี่ยวข้อง

๑.๓.๔๐.๔. ระดับความรุนแรงของเหตุการณ์ (Severity)

๑.๓.๔๐.๕. รายละเอียดของเหตุการณ์และพฤติกรรมที่ตรวจพบ

๑.๓.๔๐.๖. คะแนนหรือระดับความเสี่ยง (Scoring) ของภัยคุกคามเมื่อเกิดขึ้นกับ IP address, Domain และ User Account ได้เป็นอย่างน้อย

๑.๓.๔๐.๗. การแสดงเทคนิคหรือขั้นตอนของภัยคุกคามที่ตรวจพบ โดยสามารถเชื่อมโยงหรืออ้างอิงกับกรอบการวิเคราะห์ MiTRE ATT&CK

๑.๓.๔๑. ระบบต้องสามารถดำเนินการแก้ไขหรือตอบสนองต่อภัยคุกคาม (Response Action) ได้โดยตรงจากการแจ้งเตือนหรือเหตุการณ์ (Incident) ที่ตรวจพบ ทั้งในรูปแบบอัตโนมัติหรือกึ่งอัตโนมัติ เช่น Block IP , Domain หรือ URL ที่เป็นอันตราย Quarantine, Kill Process, Reset Credential หรือ Isolate Host เป็นต้น เพื่อเพิ่มประสิทธิภาพและความรวดเร็วในการจัดการ

๑.๓.๔๒. ระบบต้องมีความสามารถในการใช้เทคโนโลยี AI และ/หรือ Machine Learning เพื่อประเมินและให้คะแนนเหตุการณ์ (Incident Scoring) หรือลำดับความสำคัญ (priority) โดยอัตโนมัติเพื่อจัดลำดับความเร่งด่วนในการจัดการ

๑.๓.๔๓. ระบบสามารถจัดการกระบวนการตอบสนอง (Response Workflow หรือ Automation Workflow) โดยสามารถบันทึก จัดเก็บ และแลกเปลี่ยนโครงสร้างหรือรูปแบบของกระบวนการทำงานดังกล่าวในรูปแบบไฟล์มาตรฐาน เช่น JSON, YAML หรือรูปแบบอื่นที่เทียบเท่า เพื่อให้สามารถปรับใช้กับระบบหรือแพลตฟอร์มอื่นได้อย่างยืดหยุ่น

๑.๓.๔๔. สามารถเชื่อมโยงกับอุปกรณ์อื่นจากผู้ผลิตภายนอก (3rd Party Integration) ผ่านการเรียกใช้ API และรองรับมาตรฐาน API สากล เช่น RESTful, JSON, XML หรือ SOAP ได้อย่างใดอย่างหนึ่งเป็นอย่างน้อย

๑.๓.๔๕. ระบบสามารถรับ ประมวลผล และวิเคราะห์ข้อมูลเหตุการณ์หรือข้อมูลจราจร (Event / Log / Telemetry) สำหรับการทำระบบวิเคราะห์พฤติกรรมผู้ใช้งานและอุปกรณ์ (UEBA : User and Entity Behavior Analytics) ได้ไม่น้อยกว่า 200 GB ต่อวัน

๑.๔. ระบบบริหารและตรวจสอบการโจมตีจากภายนอกแบบอัจฉริยะ (Attack Surface Management) จำนวน ๑ ระบบ

๑.๔.๑. เป็นระบบที่ให้บริการในรูปแบบ Software as a Service (SaaS) หรือ ทำงานบนระบบคลาวด์ (Cloud-based) โดย ผู้ให้บริการต้องได้รับการรับรองมาตรฐาน ด้านความมั่นคงปลอดภัยสารสนเทศ (ISO/IEC 27001) เป็นอย่างน้อย

๑.๔.๒. ระบบที่เสนอต้องสามารถตรวจหา Asset ที่มีการสื่อสาร (Exposed) ผ่านทางอินเทอร์เน็ต รวมถึงการใช้บริการต่างๆขององค์กรผ่านระบบ Public Cloud ได้ โดยสามารถตรวจสอบและครอบคลุมปริมาณ Asset ได้ไม่น้อยกว่า 200 Asset

๑.๔.๓. ระบบต้องสามารถตรวจพบทรัพย์สินที่เกี่ยวข้องกับบริการขององค์กรบนอินเทอร์เน็ต เช่น Domain, Subdomain, IP Address, Cloud Resource, Application หรือ Service ที่เชื่อมโยงกับองค์กรโดยอัตโนมัติ

๑.๔.๔. ระบบต้องสามารถตรวจหาผลกระทบที่เกิดขึ้นจากช่องโหว่ (Vulnerabilities) โดยสามารถเชื่อมข้อมูลของช่องโหว่ เข้ากับ Asset ที่มีอยู่ของหน่วยงาน พร้อมทั้งสามารถระบุค่าความเสี่ยง เช่น CVSS, EPSS หรือ Risk Scoring ที่เทียบเท่า

๑.๔.๕. ระบบต้องสามารถจัดลำดับความสำคัญของความเสี่ยง (Risk Prioritization) โดยพิจารณาจากบริบทของทรัพย์สิน ความรุนแรงของช่องโหว่ และนโยบายความปลอดภัยขององค์กร พร้อมทั้งแนะนำแนวทางการแก้ไขหรือบรรเทาความเสี่ยง (Remediation Guidance)

๑.๔.๖. ระบบสามารถจัดทำรายงานระดับความเสี่ยงของพื้นผิวการโจมตี (Attack Surface)

๑.๔.๗. ระบบที่เสนอต้องสามารถระบุการให้บริการของ Asset ต่างๆ เช่น Services, Port ที่มีการใช้งาน , เทคโนโลยีหรือซอฟต์แวร์ที่เกี่ยวข้อง และระบุช่องโหว่ในรูปแบบ CVE ที่สัมพันธ์กับ Service หรือ Software นั้นๆได้

๑.๔.๘. ระบบต้องสามารถตรวจพบความเสี่ยงด้าน DNS เช่น Dangling DNS, Subdomain Takeover หรือ Domain Hijacking Risk เพื่อป้องกันการถูกยึดครองทราฟฟิกหรือทรัพยากรขององค์กร

๑.๔.๙. ระบบที่นำเสนอต้องสามารถตรวจสอบพื้นผิวการโจมตี (Attack Surface) ที่ครอบคลุมกับความเสี่ยงดังต่อไปนี้

๑.๔.๙.๑. การจัดการช่องโหว่ (Vulnerability Management)

๑.๔.๙.๒. ความสอดคล้องตามข้อกำหนดหรือแนวปฏิบัติ (Compliance) หรือ Best practices

๑.๔.๙.๓. ความเสี่ยงจาก SSL/TLS Certificate เช่น การหมดอายุหรือการตั้งค่าที่ไม่ปลอดภัย

๑.๔.๙.๔. ความเสี่ยงจากการตั้งค่า DNS Record ที่ไม่เหมาะสม

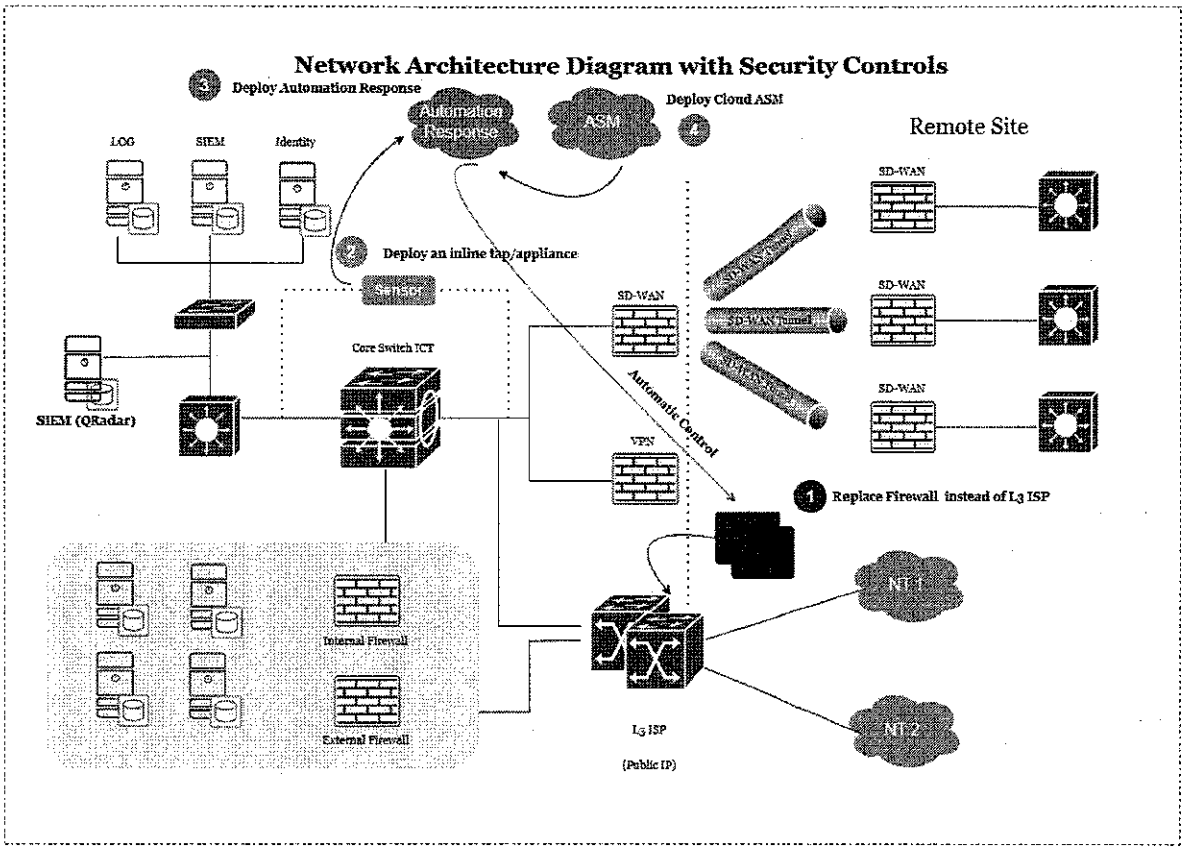
๑.๔.๑๐. ระบบต้องสามารถดำเนินการทดสอบพื้นผิวการโจมตี (Attack Surface) ได้ไม่น้อยกว่า 200 รายการ เพื่อระบุทรัพย์สินที่มีความเสี่ยงหรือมีช่องโหว่ และสามารถแสดงหลักฐานหรือเหตุผลประกอบว่าทรัพย์สินดังกล่าวมีความเป็นไปได้ในการถูกโจมตี (Exploitability Evidence)

๑.๔.๑๑. ระบบต้องสามารถบริหารจัดการรายการทรัพย์สิน (Asset Inventory) ผ่าน Web User Interface โดยต้องสามารถระบุ หน่วยงานของทรัพย์สิน, ประเภทของทรัพย์สิน ได้เป็นอย่างน้อย

๑.๔.๑๒. ระบบต้องสามารถทำการ Crawl เว็บไซต์หรือ Web Application ที่เปิดเผยต่ออินเทอร์เน็ต และแสดงข้อมูลสำคัญ เช่น URL, Technology Stack และภาพหน้าจอ (Screenshot) เพื่อใช้ประกอบการวิเคราะห์ความเสี่ยง

๑.๔.๑๓. ระบบที่เสนอสามารถ integrate workflow เข้ากับระบบการบริหารจัดการด้าน Cyber Security Workflow ได้อย่างมีประสิทธิภาพ โดยสามารถทำงานร่วมกับระบบในข้อ ๑.๓ ที่เสนอในโครงการนี้ โดยสามารถส่งข้อมูลความเสี่ยงหรือเหตุการณ์จาก Attack Surface Management เพื่อสร้างกระบวนการตอบสนองในรูปแบบอัตโนมัติ หรือกึ่งอัตโนมัติได้

๒. ผู้ขายต้องดำเนินการติดตั้งตาม รูปที่ ๑.



รูปที่ ๑. Network Architecture Diagram with Security Controls