ตารางเปรียบเทียบคุณสมบัติทางเทคนิคของระบบ Network Infrastructure and Network Security Operation Center (NSOC) จำนวน ๑ ระบบ พร้อมติดตั้ง		
รายละเอียดที่ บวท. ต้องการ	รายละเอียดของผู้ยื่นข้อเสนอ	หัวข้อบ่งชี้คุณสมบัติของผู้ยื่นข้อเสนอ
๑. คุณสมบัติผู้ยื่นข้อเสนอ ผู้ยื่นข้อเสนอต้องเป็นเจ้าของผลิตภัณฑ์หรือตัวแทนจำหน่ายที่ได้รับการแต่งตั้งจากเจ้าของผลิตภัณฑ์ หรือสาขาของเจ้าของผลิตภัณฑ์ในประเทศไทย หรือผู้แทนจำหน่ายในประเทศไทยของอุปกรณ์ข้อ ๓.๑ - ๓.๓ โดยแนบหลักฐานการแต่งตั้งดังกล่าวมาพร้อมกับการยื่นข้อเสนอ		
๒. ขอบเขตการดำเนินการ (Scope of Work) ๒.๑ ผู้ยื่นข้อเสนอต้องออกแบบระบบให้สามารถทำงานได้ตามขอบเขตงาน และสอดคล้องกับ Network Diagram แนบท้าย		
๒.๒ ผู้ยื่นข้อเสนอต้องนำส่ง Bill of Material (BOM) ของระบบอุปกรณ์ที่เสนอ พร้อม Network Design Diagram มาพร้อมในการยื่นข้อเสนอ		
๒.๓ อุปกรณ์ทั้งหมดที่เสนอต้องเป็นของแท้ ของใหม่ ไม่เคยใช้งานมาก่อน		
๒.๔ ระบบปฏิบัติการและ Software ทั้งหมดที่เสนอในโครงการ ต้องมีลิขสิทธิ์พร้อม License การใช้งานถูกต้องครบถ้วน		
๒.๕ ระบบปฏิบัติการ และ Software ทั้งหมดที่เสนอในโครงการ ต้องให้สิทธิการใช้งานแบบถาวร หรือให้สิทธิใช้งานต่อได้อย่างน้อย ๓ ปี หลังจากหมดอายุการรับประกันตามโครงการ แม้ว่าความสามารถในการ Download และ Upgrade หรือ Update ผลิตภัณฑ์จะสิ้นสุดลงเมื่อหมดอายุการรับประกันตามโครงการ ทั้งนี้ เพื่อให้เป็นไปตามอายุการใช้งานอุปกรณ์ประเภท Server Equipment ที่ บวท. กำหนดไว้ที่ ๖ ปี โดยไม่มีค่าใช้จ่ายเพิ่มเติมแต่อย่างใด		
๒.๖ ผู้ชนะการประกวดราคาต้องจัดให้มีการประชุม Kick off meeting ระหว่างผู้ชนะการประกวดราคากับคณะกรรมการตรวจรับพัสดุภายใน ๑๕ วันทำการ นับถัดจากวันลงนามสัญญา		
๒.๗ ผู้ชนะการประกวดราคาต้องนำเสนอแผนการดำเนินการให้คณะกรรมการตรวจรับพัสดุตรวจสอบความถูกต้องครบถ้วน และพิจารณาอนุมัติให้ดำเนินการ โดยนำส่งอย่างช้าไม่เกินวันที่มีการประชุม Kick off meeting ระหว่างผู้ชนะการประกวดราคากับคณะกรรมการตรวจรับพัสดุ		

๒/๒.๘ ผู้ชนะ...

รายละเอียดที่ บวท. ต้องการ	รายละเอียดของผู้ยื่นข้อเสนอ	หัวข้อบ่งชี้คุณสมบัติของผู้ยื่นข้อเสนอ
๒.๘ ผู้ชนะการประกวดราคาต้องจัดทำ Network/ Layout Diagram ของการทดสอบการทำงานพร้อมรายงานผลทดสอบ Performance ของแต่ละอุปกรณ์ให้พร้อมก่อนส่งมอบงาน		
๒.๙ ในการดำเนินการทดสอบการทำงานของแต่ละอุปกรณ์ ต้องมีเจ้าหน้าที่ของ บวท. ร่วมดำเนินการทดสอบและรับทราบด้วย		
๒.๑๐ ผู้ชนะการประกวดราคาต้องจัดหาสายสัญญาณ สายไฟฟ้า สายเชื่อมต่อต่าง ๆ และอุปกรณ์ประกอบ เพื่อใช้ในการติดตั้งให้ระบบอุปกรณ์ทำงานได้ตามข้อกำหนด		
๒.๑๑ ผู้ชนะการประกวดราคาต้องจัดทำ Label กำกับสายสัญญาณที่ติดตั้งในโครงการ ติดแสดงไว้กับสายสัญญาณทั้งต้นทางและปลายทาง โดยมีรายละเอียดตามที่คณะกรรมการตรวจรับพัสดุกำหนดให้		
๒.๑๒ ผู้ชนะการประกวดราคาต้องจัดทำ Label ที่แสดงรายละเอียดสำคัญอย่างย่อของผลิตภัณฑ์ติดแสดงไว้กับชุดผลิตภัณฑ์ที่เสนอราคา หรือตามที่คณะกรรมการตรวจรับพัสดุกำหนดให้		
๓. รายการอุปกรณ์ที่จัดหา ระบบศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบ Network Infrastructure และระบบสารสนเทศด้าน ควบคุมจราจรทางอากาศ (NSOC) จำนวน ๑ ระบบ ประกอบด้วย ๓.๑ Log Analyzer จำนวน ๑ ระบบ ๓.๒ Log Collector จำนวน ๑๒ ระบบ ๓.๓ Log Server จำนวน ๑ ระบบ		
๔. คุณสมบัติเฉพาะระบบอุปกรณ์ **๔.๑ Log Analyzer จำนวน ๑ ชุด มีคุณสมบัติอย่างน้อยดังนี้** ๔.๑.๑ ระบบที่เสนอต้องมีการติดตั้งและใช้งานจริงให้กับหน่วยงานหรือองค์กรที่ถือเป็นโครงสร้างพื้นฐานของประเทศ ตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๙ ภายในระยะเวลา ๕ ปี นับถึงวันยื่นข้อเสนอ โดยแนบเอกสารจากผู้ผลิตหรือเจ้าของผลิตภัณฑ์มาแสดงในวันยื่นข้อเสนอ		
๔.๑.๒ ระบบที่เสนอต้องเป็น Virtual Appliance ที่มีการ Hardening มาแล้วจากผู้ผลิต หรือ Software พร้อมระบบปฏิบัติการ และทำการ Hardening ตามมาตรฐานของผู้ผลิต		

๗/๔.๑.๓ ติดตั้ง...

รายละเอียดที่ บวท. ต้องการ	รายละเอียดของผู้ยื่นข้อเสนอ	หัวข้อบ่งชี้คุณสมบัติของผู้ยื่นข้อเสนอ
๔.๑.๓ ติดตั้งให้มีการทำงานในรูปแบบ High Availability (HA) แบบActive/Standby ในเครื่องคอมพิวเตอร์แม่ข่ายที่เสนอมาในโครงการ		
๔.๑.๔ ระบบที่เสนอต้องเป็นแบบแยกส่วนการทำงาน (Multi Tiers Distributed Deployment)		
๔.๑.๕ ระบบสามารถจัดเก็บและประมวลผล Log จากระบบ และอุปกรณ์ต่างๆ เช่น Firewall, Network Devices, ระบบปฏิบัติการ และระบบฐานข้อมูล เป็นต้น		
๔.๑.๖ ระบบที่เสนอแต่ละส่วนมีความสามารถในการทำงานในสภาวะปกติ (Sustained Performance) ไม่น้อยกว่า 25,000 Event per Second หรือ Message per Second หรือรองรับข้อมูลรวมทุกระบบได้อย่างน้อย 500 GByte per day หรือรองรับจำนวนอุปกรณ์ทั้งหมด ไม่น้อยกว่า ๓,๐๐๐ อุปกรณ์		
๔.๑.๗ สามารถใช้งานจัดเก็บและประมวลผลข้อมูลบนระบบเครือข่าย IPv4 และ IPv6 พร้อมกันได้ เป็นอย่างน้อย		
๔.๑.๘ สามารถรับและดึงข้อมูล Log จากอุปกรณ์ต่าง ๆ (Log Source) ในรูปแบบอย่างน้อยดังนี้ ๔.๑.๘.๑ Syslog ทั้ง TCP และ UDP ๔.๑.๘.๒ WMI หรือ Windows Event Log ๔.๑.๘.๓ Database หรือ ODBC หรือ SQL ๔.๑.๘.๔ File Pull หรือ Flat File หรือ File ๔.๑.๘.๕ OPSEC หรือ LEA Protocol Transfer ๔.๑.๘.๖ Security Device Event Exchange (SDEE) Protocol		
๔.๑.๙ มีรูปแบบความสัมพันธ์ (Correlation Rules) สำหรับใช้วิเคราะห์ข้อมูลภัยคุกคามแบบ Near Real-Time หรือดีกว่า และหาความสัมพันธ์ของเหตุการณ์ต่าง ๆ (Correlation) ได้		
๔.๑.๑๐ สามารถปรับแต่งรูปแบบความสัมพันธ์ (Correlation Rules) ได้		
๔.๑.๑๑ ระบบที่เสนอต้องมีระบบฐานข้อมูลเกี่ยวกับภัยคุกคาม (Threat Intelligence) ภายใต้เครื่องหมายการค้าเดียวกัน เพื่อทำการตรวจสอบความเสี่ยงจาก IP, file, Application และ MD5 ได้เป็นอย่างน้อย		
๔.๑.๑๒ สามารถรับข้อมูล Threat Intelligence จาก Threat Intelligence Sources (Open-Source & Commercial) ได้		

๔/๔.๑.๓ สามารถ...

รายละเอียดที่ บวท. ต้องการ	รายละเอียดของผู้ยื่นข้อเสนอ	หัวข้อบ่งชี้คุณสมบัติของผู้ยื่นข้อเสนอ
๔.๑.๑๓ สามารถวิเคราะห์พฤติกรรมผู้ใช้ User behavior analytics (UBA) หรือUser and entity behavior analytics (UEBA) เพื่อใช้สำหรับวิเคราะห์ผู้ใช้งานอย่างน้อย 5,000 Users โดยมีคุณสมบัติอย่างน้อยดังนี้ ๔.๑.๑๓.๑ สามารถดึงข้อมูล User จาก Microsoft Active Directory หรือ LDAP ได้เป็นอย่างน้อย		
๔.๑.๑๓.๒ มีระบบเกณฑ์การให้คะแนนแบบอัจฉริยะ โดยกำหนดความรุนแรงจากพฤติกรรมที่เกิดขึ้นด้วย Machine Learning หรือเทียบเท่า หรือดีกว่า		
๔.๑.๑๓.๓ สามารถ drill down เพื่อดูรายละเอียดของพฤติกรรมการใช้งานของผู้ใช้จาก risk score ได้		
๔.๑.๑๔ มีรูปแบบหรือประเภทการเรียนรู้ของ machine learning เพื่อตรวจจับพฤติกรรมการใช้ของผู้ใช้ที่ผิดปกติได้อย่างน้อยดังนี้ ๔.๑.๑๔.๑ Account and Authentication ๔.๑.๑๔.๒ Browsing Behavior ๔.๑.๑๔.๓ DNS Analyzer ๔.๑.๑๔.๔ Network Traffic and Attacks ๔.๑.๑๔.๕ System Monitoring ๔.๑.๑๔.๕ Endpoint		
๔.๑.๑๕ สามารถใช้ machine learning เพื่อวิเคราะห์และตรวจจับพฤติกรรมการใช้งานของผู้ใช้ได้อย่างน้อยดังนี้ ๔.๑.๑๕.๑ Account misuse or abuse ๔.๑.๑๕.๒ Data exfiltration ๔.๑.๑๕.๓ Flow-based anomalies ๔.๑.๑๕.๔ Access at unusual times ๔.๑.๑๕.๕ Access from unusual geography ๔.๑.๑๕.๖ Sharing Credentials		
๔.๑.๑๖ สามารถแจ้งเตือนให้ผู้ดูแลระบบทราบเมื่อตรวจพบข้อมูลที่สอดคล้องกับเงื่อนไขที่ตั้งไว้ หรือเมื่อมีการตรวจพบเหตุการณ์จากผลของการทำ Correlation ตามเงื่อนไขที่กำหนด หรือเหตุการณ์ที่กำหนดไว้ผ่าน Email หรือ SMS ได้เป็นอย่างน้อย		
๔.๑.๑๗ สามารถจัดรูปแบบของ Events หรือ Logs ที่ได้รับจากอุปกรณ์ต้นทาง ให้อยู่ในรูปแบบเดียวกันเพื่อที่ระบบจะสามารถทำการวิเคราะห์ได้ (Parsed/Normalized/Transform)		

๕/๔.๑.๑๘ สามารถ...

รายละเอียดที่ บวท. ต้องการ	รายละเอียดของผู้ยื่นข้อเสนอ	หัวข้อบ่งชี้คุณสมบัติของผู้ยื่นข้อเสนอ
๔.๑.๑๘ สามารถเก็บรักษาและส่งออก (Export) Log ในรูปแบบ Raw Log หรือ Raw Events โดยไม่มีการดัดแปลง Log ที่ส่งเข้ามาได้		
๔.๑.๑๙ สามารถเก็บรักษา Log ไว้บนระบบในรูปแบบที่สามารถสืบค้นเพื่อใช้วิเคราะห์ และทำรายงานได้ทันที (Active Log/Online Log) โดยมีพื้นที่จัดเก็บข้อมูล Logs ได้ไม่น้อยกว่า ๙๐ วัน		
๔.๑.๒๐ สามารถเก็บรักษา Log ไว้บนระบบในรูปแบบที่สามารถนำมาใช้งานภายหลัง (Archived/Compressed Log) โดยมีพื้นที่จัดเก็บข้อมูล Logs ได้ ไม่น้อยกว่า ๓๖๕ วัน		
๔.๑.๒๑ มีระบบการเก็บรักษาความลับของข้อมูลที่จัดเก็บและกำหนดชั้นความลับในการเข้าถึงข้อมูลดังกล่าวเพื่อรักษาความน่าเชื่อถือของข้อมูล และไม่ให้ผู้ดูแลระบบสามารถแก้ไขข้อมูลที่เก็บรักษาไว้เช่น การทำ Data Archiving หรือ Data Hashing หรือ Data Marking เป็นต้น		
๔.๑.๒๒ สามารถยืนยันความถูกต้องของข้อมูล Log ที่เก็บรักษาว่าไม่มีการถูกเปลี่ยนแปลงแก้ไข (Data Integrity) ด้วย Hashing Algorithm แบบ SHA-1 หรือ SHA -256 หรือเทียบเท่าหรือดีกว่า		
๔.๑.๒๓ สามารถบริหารจัดการผ่าน Web Interface หรือ GUI ได้ เป็นอย่างน้อย		
๔.๑.๒๔ สามารถแสดงภาพรวมของระบบและสถานะของการใช้งานทรัพยากรต่าง ๆ ของระบบได้		
๔.๑.๒๕ สามารถประมวลผลและวิเคราะห์ข้อมูล Log ในแบบแยกเป็นรายหน่วยงาน และรวมหลายหน่วยงานได้		
๔.๑.๒๖ สามารถกำหนดสิทธิ์การเข้าถึงระบบของผู้ดูแลระบบแต่ละคนในการเข้าถึงอุปกรณ์ที่แตกต่างกันได้ (Role - based Access Control)		
๔.๑.๒๗ สามารถทำ Compliance Monitoring และ Reporting ได้		
๔.๑.๒๘ สามารถแสดงรายงานในรูปแบบตาราง, Bar Chart, Pie Chart ได้เป็นอย่างน้อย		
๔.๑.๒๙ สามารถออกรายงานในรูปแบบ HTML หรือ PDF ได้เป็นอย่างน้อย		
๔.๑.๓๐ สามารถเปิดให้พัฒนา Application เพื่อดึงข้อมูลจากแหล่งต่าง ๆ มาประกอบในการวิเคราะห์ได้		
๔.๑.๓๑ สามารถปรับรูปแบบการแสดงผล Dashboard ให้เหมาะสมสำหรับแต่ละผู้ใช้งาน และสามารถ Customize Dashboard ได้ตามต้องการ		

รายละเอียดที่ บวท. ต้องการ	รายละเอียดของผู้ยื่นข้อเสนอ	หัวข้อบ่งชี้คุณสมบัติของผู้ยื่นข้อเสนอ
๔.๑.๓๒ สามารถทำ Automate Response รองรับการทำงานด้วย Programming หรือ Script หรือ Rest API		
๔.๑.๓๓ สามารถสร้างรายงานอ้างอิงตามมาตรฐานหรือ Framework ดังต่อไปนี้ได้เป็นอย่างน้อย ๔.๑.๓๓.๑ PCI-DSS ๔.๑.๓๓.๒ HIPAA ๔.๑.๓๓.๓ NERC หรือ NERC CIP ๔.๑.๓๓.๔ FISMA ๔.๑.๓๓.๕ GLBA ๔.๑.๓๓.๖ SOX ๔.๑.๓๓.๗ GPG13 ๔.๑.๓๓.๘ NIST ๔.๑.๓๓.๙ ISO27001 หรือ ISO27002		
๔.๑.๓๔ สามารถออกรายงานได้อัตโนมัติตามช่วง เวลาที่กำหนด (Scheduled Report) และส่ง Email ไปยังผู้ดูแลระบบที่กำหนดได้		
๔.๑.๓๕ ระบบที่เสนอต้องสามารถเก็บข้อมูลของ Network flow ในรูปแบบ Net flow, J-Flow, S-Flow ด้วยวิธี SPAN port หรือ network TAP บนระบบเครือข่ายได้		
๔.๑.๓๖ ระบบที่เสนอต้องสามารถรวบรวม หรือเก็บ network flow สำหรับวิเคราะห์หาสิ่งผิดปกติจากอุปกรณ์บนระบบเครือข่ายได้อย่างน้อย 25,000 flow per minute (FPM) หรือ 500 GByte per day		
๔.๑.๓๗ ระบบที่เสนอต้องสามารถตรวจจับ packet ใน network flow ซึ่งประกอบไปด้วยข้อมูลดังนี้เป็นอย่างน้อย ๔.๑.๓๗.๑ source IP address ๔.๑.๓๗.๒ destination IP address ๔.๑.๓๗.๓ source port ๔.๑.๓๗.๔ destination port ๔.๑.๓๗.๕ protocol		
๔.๑.๓๘ รองรับความสามารถในการตรวจสอบข้อมูลภัยคุกคามในระดับ Packet เชิงลึก (Deep Packet Inspection) ในรูปแบบ Real Time ภายใต้เครื่องหมายการค้าเดียวกันกับระบบ SIEM ที่เสนอในโครงการ		
๔.๑.๓๙ รองรับการทำงานเชื่อมต่อกับระบบ Cognitive หรือ AI หรือ Machine Learning เพื่อทำงานร่วมกันในการ Investigate Incident โดยนำข้อมูลจาก SIEM เช่น IP Address, hash file, URL ส่งให้ Cognitive หรือ AI หรือ Machine		

๗/Learning...

รายละเอียดที่ บวท. ต้องการ	รายละเอียดของผู้ยื่นข้อเสนอ	หัวข้อบ่งชี้คุณสมบัติของผู้ยื่นข้อเสนอ
Learning นำไปวิเคราะห์ และสามารถสั่งให้ Cognitive หรือ AI หรือ Machine Learning ทำการ Investigate Incident แบบ Manual และแบบ Automatic ได้ภายใต้เครื่องหมายการค้าเดียวกัน กับระบบ SIEM ที่เสนอในโครงการ		
๔.๒ Log Collector หรือ Log Forwarder จำนวน ๑๒ ชุด แต่ละชุดมีคุณสมบัติดังนี้ ๔.๒.๑ เป็น Virtual Appliance มีเครื่องหมายการค้าเดียวกับ Log Analyzer หรือ Software Install ที่มีเครื่องหมายการค้าเดียวกับ Log Analyzer ที่เสนอในโครงการ พร้อมระบบปฏิบัติการ โดยติดตั้งบน VM ที่ บวท. จัดหาให้		
๔.๒.๒ สามารถรับข้อมูลจากอุปกรณ์ต้นทางได้ไม่น้อยกว่า ๒,๐๐๐ เหตุการณ์ต่อวินาที (Events per Second) หรือไม่น้อยกว่า ๒,๐๐๐ ข้อความต่อวินาที (Messages per Second) หรือรองรับข้อมูลรวมทุกระบบได้อย่างน้อย 50 GB /Day		
๔.๒.๓ สามารถตรวจจับข้อมูลจราจรทางเครือข่าย (Network Packet Capture หรือ Flow Collector) แบบ Real Time ได้ สามารถนำเสนอ Virtual Appliance หรือ Software Install ที่มีเครื่องหมายการค้าเดียวกับ Log Analyzer ที่เสนอในโครงการ พร้อมระบบปฏิบัติการ		
๔.๒.๔ สามารถทำการบีบอัดข้อมูลก่อนจัดส่ง (Data Compression) และรองรับการเข้ารหัสแบบ SSL/TLS หรือ AES เป็นอย่างน้อย		
๔.๒.๕ สามารถทำ Tagging หรือ String Manager ข้อมูลด้วย Source หรือ Source Type หรือ Host ได้ เป็นอย่างน้อย		
๔.๒.๖ จัดเก็บข้อมูลชั่วคราวได้กรณีที่มีปัญหาการส่งข้อมูล (Buffering/Caching) ได้ไม่น้อยกว่า ๗ วัน โดยคำนวณจากขนาดของเหตุการณ์ หรือข้อความตามที่กำหนดในข้อ ๔.๒.๒		
๔.๒.๗ สามารถจำกัดความเร็วในการส่งข้อมูล (Bandwidth Management)		
๔.๒.๘ สามารถรับ Log จาก Protocol Syslog และ SNMP Trap ได้เป็นอย่างน้อย		
๔.๒.๙ สามารถทำงานได้ทั้ง IPv4 และ IPv6 พร้อมกัน		
๔.๓ เครื่องคอมพิวเตอร์แม่ข่าย (Log Server) จำนวน ๑ ชุด มีคุณสมบัติอย่างน้อยดังนี้ ๔.๓.๑ เป็นคอมพิวเตอร์แม่ข่ายประเภท Disaggregated Hyper-Converged Infrastructure (dHCI) หรือเทียบเท่า		
๔.๓.๒ จะต้องมีความสามารถในการทำ Deduplication และ Compression ได้ ในทุกพื้นที่ของระบบเก็บข้อมูลหลัก		

๘/Second)...

รายละเอียดที่ บวท. ต้องการ	รายละเอียดของผู้ยื่นข้อเสนอ	หัวข้อบ่งชี้คุณสมบัติของผู้ยื่นข้อเสนอ
๔.๓.๓ ต้องมีสถาปัตยกรรมแบบ Scale-out ทั้ง Compute และ Storage Node โดยสามารถเพิ่มขยายได้ โดยไม่ต้องหยุดการทำงานของระบบ		
๔.๓.๔ มีเครื่องคอมพิวเตอร์แม่ข่าย Hyper-Converged Node หรือ Computer Node จำนวน 3 Node แต่ละ Node มีคุณสมบัติดังนี้		
๔.๓.๔.๑ มีหน่วยประมวลผลกลางแบบ Intel Xeon แบบ 12 Core CPU Processor หรือดีกว่า โดยจะต้องมีความเร็ว ไม่น้อยกว่า 2.7 GHz จำนวนไม่น้อยกว่า ๒ หน่วยต่อ Node		
๔.๓.๔.๒ มีหน่วยความจำแบบ DDR4 LRDIMM หรือ RDIMM หรือดีกว่า ขนาดไม่น้อยกว่า 512 GB โดยระบบจะต้องสามารถเพิ่มความจุได้ในอนาคต		
๔.๓.๔.๓ มีหน่วยจัดเก็บข้อมูล SSD แบบ SATA Hot - Plug ชนิด 2.5" ขนาดความจุไม่น้อยกว่า 240 GB จำนวน ๒ หน่วย รองรับการใส่สูงสุดไม่น้อยกว่า ๘ หน่วย		
๔.๓.๔.๔ มี I/O Expansion Slot แบบ PCI-e 3.0 หรือดีกว่า จำนวนอย่างน้อย 3 Slot		
๔.๓.๔.๕ มีอุปกรณ์เชื่อมต่อระบบเครือข่ายแบบ 10 GBase SFP+ จำนวนไม่น้อยกว่า 4 Ports หรือดีกว่า		
๔.๓.๔.๖ มี AC Redundancy Power Supply ขนาดไม่น้อยกว่า 800 W สามารถถอดเปลี่ยนหากเกิดความเสียหายได้โดยไม่ต้องหยุดระบบ		
๔.๓.๔.๗ มีระบบ Remote Management Port แบบ 1 GbE RJ-45 จำนวน 1 Port ต่อ Node สามารถบริหารจัดการ remote console, power off, power on และ monitor สถานะของ Server ผ่านทาง HTTP หรือ HTTPS ได้ พร้อม license แบบถาวร		
๔.๓.๔.๘ ได้รับการรับรองมาตรฐาน FCC หรือ UL หรือ CE เป็นอย่างน้อย		
๔.๓.๕ มีระบบจัดเก็บข้อมูลหลัก (Storage Node) จำนวน ๑ ชุด มีคุณสมบัติดังนี้ ๔.๓.๕.๑ มีส่วนควบคุมอุปกรณ์ (Controller) แบบ Redundant ในแต่ละ Controller จะต้องมี Storage Front End Ports แบบ 10 GBase SFP+ จำนวนไม่น้อยกว่า 4 ports		
๔.๓.๕.๒ ต้องรองรับการขยายได้ทั้งแบบ Scale-Up เพิ่มจำนวนดิสก์และ Scale-Out เพิ่มจำนวน Storage Node ได้สูงสุดไม่น้อยกว่า ๔ ชุด		

๙/๔.๓.๕.๓ ระบบ...

รายละเอียดที่ บวท. ต้องการ	รายละเอียดของผู้ยื่นข้อเสนอ	หัวข้อบ่งชี้คุณสมบัติของผู้ยื่นข้อเสนอ
๔.๓.๕.๓ ระบบเก็บข้อมูลหลักจะต้องมีดิสก์แบบ NL-SAS หรือ SATA โดยมี ความจุไม่น้อยกว่า 250 TB สำหรับใช้งาน (Usable Capacity)		
๔.๓.๕.๔ ระบบเก็บข้อมูลหลักจะต้องมีดิสก์ SSD Cache Tier จำนวนไม่น้อยกว่า 25 TB		
๔.๓.๕.๕ ระบบเก็บข้อมูลหลักต้องรองรับการเสียหายของหน่วยจัดเก็บข้อมูลได้ทั้งหมด ๓ หน่วย แบบไม่ระบุตำแหน่งและไม่ส่งผลกระทบให้ข้อมูลสูญหาย		
๔.๓.๖ Software Virtualization Management จำนวน ๑ ระบบ มีคุณสมบัติดังนี้ ๔.๓.๖.๑ สามารถทำ High Availability (HA) โดยทำการ Restart คอมพิวเตอร์เสมือนได้โดยอัตโนมัติ ในกรณีที่ Hardware หรือ Operating System มีปัญหา		
๔.๓.๖.๒ สามารถทำการย้ายคอมพิวเตอร์เสมือนข้ามไปมาระหว่าง Server ได้ โดยไม่กระทบการทำงานของผู้ใช้งาน		
๔.๓.๖.๓ รองรับการทำงานแบบ Fault Tolerance เพื่อให้ Application ทำงานต่อเนื่องในกรณีที่ Hardware ของ Server มีปัญหา โดยรองรับการทำงาน (Workload) ที่ 2 Virtual CPUs		
๔.๓.๖.๔ สามารถย้ายไฟล์ดิสก์ของคอมพิวเตอร์เสมือนข้ามไปมาระหว่าง storage ได้ โดยไม่มีผลกระทบกับผู้ใช้งาน		
๔.๓.๗ มี Top of Rack Ethernet Switch จำนวน ๒ ตัว แต่ละตัวมีคุณสมบัติดังนี้ ๔.๓.๗.๑ มีลักษณะการทำงานไม่น้อยกว่า Layer 3 ของ OSI Model		
๔.๓.๗.๒ มีช่องเชื่อมต่อระบบเครือข่าย 10 GBase SFP+ จำนวนอย่างน้อย 24 Ports พร้อม SFP+ Module ยี่ห้อเดียวกับ Top of Rack Ethernet Switch จำนวน 22 Module มีช่องเชื่อมต่อแบบ 10 GbE จำนวนอย่างน้อย 2 Ports และมีช่องเชื่อมต่อแบบ 40 Gbps หรือดีกว่า จำนวนไม่น้อยกว่า 2 Ports และมี Port Stack จำนวนไม่น้อยกว่า 2 Port ที่มี Stacking Bandwidth ไม่น้อยกว่า 40 Gbps พร้อมสาย Stack		
๔.๓.๗.๓ มี Out of Band Management แบบ UTP Ethernet RJ-45 จำนวน 1 Port		
๔.๓.๗.๔ มี Switching Capacity 1.8 Tbps หรือสูงกว่า		
๔.๓.๗.๕ มี Processing Capacity or Forwarding Rate 1.5 Bpps หรือสูงกว่า		

๑๐/๔.๓.๗.๖ มี Switching...

รายละเอียดที่ บวท. ต้องการ	รายละเอียดของผู้ยื่นข้อเสนอ	หัวข้อบ่งชี้คุณสมบัติของผู้ยื่นข้อเสนอ
๔.๓.๗.๖ มี Switching Latency ไม่เกิน 300 ns		
๔.๓.๗.๗ สามารถใช้งาน Link Aggregation Group โดยสามารถสร้าง Link Aggregation Group ข้าม Node ได้		
๔.๓.๗.๘ สามารถใช้งาน VLAN หรือ 802.1Q ได้		
๔.๓.๗.๙ รองรับการใช้งานกับ OpenFlow หรือ sFlow ได้		
๔.๓.๗.๑๐ สามารถบริหารจัดการผ่านทาง CLI และ Web GUI ได้		
๔.๓.๗.๑๑ มี AC Redundancy Power Supply สามารถถอดเปลี่ยนหากเกิดความเสียหายได้ โดยไม่ต้องหยุดระบบ		
๔.๓.๘ มีอุปกรณ์จัดเก็บข้อมูลภายนอกชนิด NAS Storage จำนวน ๑ ชุด มีคุณสมบัติดังนี้ ๔.๓.๘.๑ หน่วยประมวลผลความเร็วไม่น้อยกว่า 2.1 GHz มีจำนวน Core ไม่น้อยกว่า 8 cores		
๔.๓.๘.๒ หน่วยความจำขนาดไม่น้อยกว่า 32 GB		
๔.๓.๘.๓ มีขนาดพื้นที่ใช้งานไม่น้อยกว่า 200 TB (Usable Capacity)		
๔.๓.๘.๔ มีอุปกรณ์จัดเก็บข้อมูลประเภท Hard disk SAS 12G Midline หรือ Nearline ความเร็วไม่น้อยกว่า ๗,๒๐๐ รอบต่อนาที		
๔.๓.๘.๕ มี Interface ประเภท 10 GBase SFP+ ไม่น้อยกว่า 4 Ports		
๔.๓.๘.๖ รองรับการใช้งานได้ทั้ง CIFS/SMB, NFS และ iSCSI protocol		
๔.๓.๘.๗ มี AC Redundancy Power Supply สามารถถอดเปลี่ยนหากเกิดความเสียหายได้ โดยไม่ต้องหยุดระบบ		
๔.๓.๙ มีระบบบริหารจัดการและควบคุมการใช้งานบัญชีของผู้จัดการระบบ (Privileged Account Management : PAM) จำนวน ๑ ระบบ มีคุณสมบัติอย่างน้อยดังนี้ ๔.๓.๙.๑ ระบบที่นำเสนอต้องถูกออกแบบมาเพื่อเป็นระบบ Privileged Account Management โดยเฉพาะเท่านั้น		
๔.๓.๙.๒ ระบบที่เสนอต้องเป็น Virtual Appliance ที่มีการ Hardening มาแล้วจากผู้ผลิต หรือ Software พร้อมระบบปฏิบัติการ และทำการ Hardening ตามมาตรฐานของผู้ผลิต		
๔.๓.๙.๓ ต้องติดตั้งในเครื่องคอมพิวเตอร์แม่ข่ายที่เสนอมาในโครงการ โดยติดตั้งให้มีการทำงานในรูปแบบ High Availability (HA) แบบ Active/Standby		
๔.๓.๙.๔ ระบบที่นำเสนอต้องสามารถทำการบริหารจัดการอุปกรณ์ได้ไม่น้อยกว่า ๑๐๐๐ อุปกรณ์ และสามารถมีผู้ใช้งานได้ไม่น้อยกว่า 100 User		

รายละเอียดที่ บวท. ต้องการ	รายละเอียดของผู้ยื่นข้อเสนอ	หัวข้อบ่งชี้คุณสมบัติของผู้ยื่นข้อเสนอ
๔.๓.๙.๕ สามารถบริหารจัดการผ่านทาง Web Browser ในช่องทาง HTTPS		
๔.๓.๙.๖ สามารถบริหารจัดการได้โดยไม่จำเป็นต้องมีการติดตั้ง Software Agent ที่อุปกรณ์ปลายทาง (Agentless)		
๔.๓.๙.๗ สามารถรองรับระบบการ Authentication ผ่านระบบ Active Directory, Radius หรือ Local user ได้		
๔.๓.๙.๘ สามารถบริหารจัดการ Privileged Account กับอุปกรณ์อย่างน้อยดังนี้ ๔.๓.๙.๘.๑ Operating System เช่น Windows Server, Linux, AIX, HP-UX, AS400		
๔.๓.๙.๘.๒ Database Account เช่น SQL Server, Oracle, MySQL, Sybase		
๔.๓.๙.๘.๓ Network/Security Appliances เช่น Check Point, Juniper, Cisco, Palo Alto, Fortinet, F5		
๔.๓.๙.๙ สามารถกำหนดสิทธิ์ของผู้ใช้งานในการเข้าใช้งานระบบได้อย่างน้อยดังนี้ ๔.๓.๙.๙.๑ ผู้ร้องขอ (Requestor) ๔.๓.๙.๙.๒ ผู้อนุมัติ (Approver) ๔.๓.๙.๙.๓ ผู้ร้องขอและผู้อนุมัติ (Approver/Requestor) ๔.๓.๙.๙.๔ ผู้ดูแลด้าน IS (ISA : Information Security Administrator) ๔.๓.๙.๙.๕ ผู้ตรวจสอบ (Auditor)		
๔.๓.๙.๑๐ สามารถควบคุมการขอใช้และกำหนดนโยบายการเปลี่ยนรหัสผ่านได้อย่างน้อยดังนี้ ๔.๓.๙.๑๐.๑ สามารถเปลี่ยนรหัสผ่านเมื่อถึงระยะเวลาที่กำหนดทุก ๆ ๓๐ วัน ๔.๓.๙.๑๐.๒ สามารถเปลี่ยนรหัสผ่านทุกครั้งที่มีการขอใช้งาน ๔.๓.๙.๑๐.๓ สามารถตรวจสอบและปรับปรุงรหัสผ่านให้ถูกต้องแบบอัตโนมัติ ในกรณีที่รหัสผ่านในอุปกรณ์ไม่ตรงกับที่เก็บบันทึกอยู่ในระบบ ๔.๓.๙.๑๐.๔ สามารถกำหนดเวลาที่ต้องการให้ทำการเปลี่ยนรหัสผ่านได้		
๔.๓.๙.๑๑ สามารถกำหนดให้มี Workflow ในลักษณะ Request-Approve ได้		
๔.๓.๙.๑๒ สามารถกำหนดจำนวนผู้อนุมัติ (Approver) ขั้นต่ำได้		

๑๒/....

รายละเอียดที่ บวท. ต้องการ	รายละเอียดของผู้ยื่นข้อเสนอ	หัวข้อบ่งชี้คุณสมบัติของผู้ยื่นข้อเสนอ
๔.๓.๙.๑๓ สามารถทำการแจ้งเตือนทางอีเมล์ในกระบวนการร้องขอ (Request)		
๔.๓.๙.๑๔ สามารถกำหนดลักษณะและนโยบายของ Password เช่น ความยาว		
๔.๓.๙.๑๕ สามารถกำหนดระยะเวลาสำหรับการขอใช้งานรหัสผ่านได้สูงสุด ๓๖๕ วัน		
๔.๓.๙.๑๖ สามารถทำการ Reset Windows Service Account พร้อมเปลี่ยนรหัสผ่านให้แก่ Service Account ที่ถูกบริหารจัดการโดยระบบ Privileged Account Management ได้		
๔.๓.๙.๑๗ สามารถกำหนดนโยบายการขอเข้าใช้งาน Privileged Account ให้แตกต่างกันตามช่วงระยะเวลา วัน และ Network Zone ได้		
๔.๓.๙.๑๘ ผู้ร้องขอ (Requester) สามารถกำหนดนโยบายในการเข้าใช้งานได้อย่างน้อยดังนี้ ๔.๓.๙.๑๘.๑ ช่วงวันที่ต้องการเข้าใช้งาน ๔.๓.๙.๑๘.๒ ระยะเวลาในการขอใช้งาน ๔.๓.๙.๑๘.๓ ระบบ หรืออุปกรณ์ที่ต้องการเข้าใช้งาน		
๔.๓.๙.๑๙ สามารถทำงานในรูปแบบ Session Proxy หรือ Session Management ได้ ไม่น้อยกว่า 250 sessions		
๔.๓.๙.๒๐ สามารถเปิด Session RDP และ SSH ได้ โดยไม่จำเป็นต้องมีการติดตั้ง Java ที่เครื่องต้นทาง		
๔.๓.๙.๒๑ สามารถทำการ Monitor Session ที่กำลังถูกใช้งานอยู่ได้แบบ Real- time (Live Session Monitoring)		
๔.๓.๙.๒๒ สามารถทำการควบคุม Session ที่ถูกเปิดใช้งานได้อย่างน้อยดังต่อไปนี้ ๔.๓.๙.๒๒.๑ Lock Screen ๔.๓.๙.๒๒.๒ Terminate Session ๔.๓.๙.๒๒.๓ Terminate Session and Cancel Request		
๔.๓.๙.๒๓ สามารถทำ Black-Listing สำหรับ SSH Commands เพื่อป้องกันการรันคำสั่งที่ไม่อนุญาตบนระบบที่ควบคุม		
๔.๓.๙.๒๔ สามารถบันทึกหน้าจอในทุกการกระทำที่เปิดใช้งานผ่าน Session Management โดยสามารถดูย้อนหลังในรูปแบบของ Video ได้		
๔.๓.๙.๒๕ สามารถบันทึกการพิมพ์ของ Session ที่เปิดใช้งานได้ (Key Stroke Logger)		

๑๓/...

รายละเอียดที่ บวท. ต้องการ	รายละเอียดของผู้ยื่นข้อเสนอ	หัวข้อบ่งชี้คุณสมบัติของผู้ยื่นข้อเสนอ
๔.๓.๙.๒๖ สามารถค้นหา Session จากคำสั่งที่พิมพ์และชื่อผู้ใช้งานได้เป็นอย่างน้อย		
๔.๓.๙.๒๗ อุปกรณ์ที่นำเสนอต้องสามารถทำงานร่วมกับ Windows Terminal Service โดยสามารถกำหนด Windows application ที่จะถูกเปิดใช้งาน พร้อมทำการ login ให้โดยอัตโนมัติได้		
๔.๓.๙.๒๘ สามารถออกรายงานในรูปแบบของการแสดงผลแบบรูปภาพ (Dashboard) ได้		
๔.๓.๙.๒๙ สามารถออกรายงานเป็น Schedule Report และรองรับการส่ง Mail ผลรายงานได้		
๔.๓.๙.๓๐ สามารถบันทึกรายงานในรูปแบบของ PDF และ CSV ได้		
๔.๓.๙.๓๑ จัดให้มี Jump Host จำนวน ๑๒ ชุด แต่ละชุดมีคุณสมบัติดังนี้ ๔.๓.๙.๓๑.๑ เป็น Virtual Appliance หรือ Software Install พร้อมระบบปฏิบัติการ Windows โดยติดตั้งบน VM ที่ บวท. จัดหาให้		
๔.๓.๙.๓๑.๒ สามารถรับการ Remote เข้าใช้งานจากระบบ PAM ได้จากผู้ใช้งานพร้อมกัน 5 User เป็นอย่างน้อย		
๕. การติดตั้ง ๕.๑ ผู้ชนะการประกวดราคาจะต้องติดตั้งอุปกรณ์สำหรับระบบ NSOC และทดสอบการใช้งาน ณ สถานที่ติดตั้งของ บวท. ทาง บวท. จะจัดเตรียมสถานที่สำหรับการติดตั้ง และเชื่อมต่อส่วนต่าง ๆ ของระบบ NSOC ไว้ให้ โดยผู้ชนะการประกวดราคาจะต้องเดินสายสัญญาณให้ระบบพร้อมใช้งาน		
๕.๒ ดำเนินการตั้งค่าระบบฯ ให้รองรับการทำงานในรูปแบบ High Availability แบบ Active/Standby ในส่วนของระบบ NSOC ที่ส่วน Console และส่วนจัดเก็บและวิเคราะห์ Event Processor		
๕.๓ ดำเนินการจัดเก็บรวบรวมข้อมูล log ของอุปกรณ์เข้ามายังระบบจำนวนสูงสุดไม่เกิน ๑,๐๐๐ เครื่อง		
๕.๔ ดำเนินการปรับแต่งระบบเพื่อให้สามารถทำงานกับอุปกรณ์ที่มี log แบบ non-standard ของ บวท. ที่ใช้อยู่ได้จำนวนสูงสุดไม่เกิน 100 Log sources		
๕.๕ ดำเนินการจัดทำ Use Cases และต้องปรับปรุงเงื่อนไขตรวจจับพฤติกรรมและเหตุการณ์ผิดปกติเชิงลึกของแต่ละ Use Cases ดังนี้ ๕.๕.๑ Critical Host Logon Failed		

๑๔/๕.๕.๒ High...

รายละเอียดที่ บวท. ต้องการ	รายละเอียดของผู้ยื่นข้อเสนอ	หัวข้อบ่งชี้คุณสมบัติของผู้ยื่นข้อเสนอ
๕.๕.๒ High Privilege login Success non-Working Times ๕.๕.๓ Possible Brute Force Attack ๕.๕.๔ Critical System Changes or Object Access ๕.๕.๕ SSH Brute Force User Name Authentication Fail ๕.๕.๖ High Privilege User Admin Account Guessing ๕.๕.๗ Remote Desktop Login from Internet ๕.๕.๘ SSH Login from Internet ๕.๕.๙ Unusual Protocol Usage ๕.๕.๑๐ Unauthorized Account Administration ๕.๕.๑๑ Log Devices Absent ๕.๕.๑๒ Malware Outbreak ๕.๕.๑๓ Suspected Malware Detection ๕.๕.๑๔ Web Defacement Detection ๕.๕.๑๕ Unusual Bandwidth Usage		
๕.๖ ดำเนินการจัดทำเอกสารกระบวนการรองรับเหตุการณ์/ภัยคุกคามทางไซเบอร์ (Playbook) จำนวนสูงสุดไม่เกิน ๑๕ เหตุการณ์		
๕.๗ ดำเนินการกำหนดรูปแบบการตรวจสอบและการแจ้งเตือนผ่านทางหน้าจอ เพื่อสำหรับบริหารจัดการเหตุการณ์ผิดปกติ จำนวนไม่น้อยกว่า ๕ หัวข้อ		
๕.๘ ดำเนินการตั้งค่าระบบเพื่อทำรายงานสรุป (Report) แบบรายวัน รายสัปดาห์ และรายเดือน จำนวนไม่น้อยกว่า ๑๐ หัวข้อ		
๕.๙ ดำเนินการติดตั้งและปรับแต่งระบบบริหารจัดการบัญชีการเข้าถึงระบบ (Privileged Account Management)		
๖. การฝึกอบรม ๖.๑ ผู้ชนะการประกวดราคาต้องจัดอบรมหลักสูตรการจัดการภัยคุกคามของศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยให้กับเจ้าหน้าที่ของ บวท. จำนวนไม่เกิน ๑๕ คน มีระยะเวลาฝึกอบรมไม่น้อยกว่า ๕ วันทำการ โดยมีเนื้อหาอย่างน้อยดังต่อไปนี้ ๖.๑.๑ Attack Methodology ๖.๑.๒ Cyber Kill Chain ๖.๑.๓ Need of Log Management ๖.๑.๔ SOC Concepts ๖.๑.๕ SIEM ๖.๑.๖ Log Analysis & Investigation		

๑๕/๖.๑.๗ Incident...

รายละเอียดที่ บวท. ต้องการ	รายละเอียดของผู้ยื่นข้อเสนอ	หัวข้อบ่งชี้คุณสมบัติของผู้ยื่นข้อเสนอ
๖.๑.๗ Incident Response ๖.๑.๘ Effective use of Threat Intelligence		
๖.๒ ผู้ชนะการประกวดราคาจะต้องจัดอบรมการใช้งานระบบ Network Infrastructure and Network Security Operation Center (NSOC) ให้กับเจ้าหน้าที่ของ บวท. จำนวนไม่เกิน ๑๕ คน มีระยะเวลาฝึกอบรมไม่น้อยกว่า ๕ วันทำการ		
๖.๓ จัดให้มีการถ่ายทอดความรู้และประสบการณ์ด้านการบริหาร Security Operation Center (SOC) ในรูปแบบการฝึกงาน (On the Job Training) ให้กับเจ้าหน้าที่ของ บวท. จำนวนไม่เกิน ๑๕ คน เป็นระยะเวลาไม่น้อยกว่า ๒ วันทำการ โดยมีเนื้อหาอย่างน้อยดังนี้ ๖.๓.๑ SOC Overview ๖.๓.๒ Defensible Network Concepts ๖.๓.๓ Event, Alerts, Anomalies, and Incidents ๖.๓.๔ Incident Management ๖.๓.๕ Automation and Orchestration ๖.๓.๖ Continuous Improvement, Analytics, and Automation		
๖.๔ ผู้ชนะการประกวดราคาต้องรับผิดชอบในการจัดหาสถานที่ในการอบรมในเขตกรุงเทพมหานคร หรือปริมณฑล เอกสารและอุปกรณ์ต่าง ๆ ในการฝึกอบรมให้ครบถ้วนตามจำนวนผู้เข้ารับการฝึกอบรม		
๖.๕ ผู้ชนะการประกวดราคาต้องทำการบันทึก VDO การอบรมตามข้อ ๖.๑ และ ๖.๒ นำส่งให้ บวท. จำนวนไม่น้อยกว่า ๒ ชุด		
๖.๖ ผู้ชนะการประกวดราคาต้องรับผิดชอบค่าใช้จ่ายเกี่ยวกับการฝึกอบรมทั้งหมด <u>ยกเว้น</u> ค่าที่พัก ค่าเดินทาง และค่าเบี้ยเลี้ยง		