รายละเอียดคุณลักษณะเฉพาะการจัดซื้อระบบจัดเก็บข้อมูลจราจรคอมพิวเตอร์ จำนวน ๑ ระบบ

๑. รายละเอียดคุณลักษณะเฉพาะของพัสดุที่จะดำเนินการจัดซื้อ ดังนี้

รายละเอียดคุณลักษณะเฉพาะการจัดซื้อระบบจัดเก็บข้อมูลจราจรคอมพิวเตอร์ จำนวน ๑ ระบบ โดยมีรายละเอียด ดังนี้

๑. เครื่องคอมพิวเตอร์แม่ข่ายสำหรับติดตั้งระบบจัดเก็บข้อมูลจราจรคอมพิวเตอร์ จำนวน ๑ เครื่อง

๑.๑ เป็นเครื่องคอมพิวเตอร์แม่ข่ายที่ติดตั้งใน Standard Rack ๑๙" มีขนาดไม่น้อยกว่า ๒ U

๑.๒ มีหน่วยประมวลผลกลาง Processors แบบ ๑๖-Core ที่มีความเร็วสัญญาณไม่น้อยกว่า ๒.๐ GHz จำนวน ๒ หน่วย

๑.๓ มีหน่วยความจำแบบ ECC DDR-๕ ขนาด ๒๕๖ GB เป็นอย่างน้อย และรองรับการติดตั้งหน่วยความจำเพิ่มเติมได้ในอนาคตอย่างน้อย ๕๑๒ GB

๑.๔ มีช่องใส่ Hot-Plug Hard Disk แบบ ๓.๕" จำนวนไม่น้อยกว่า ๑๒ ช่อง และต้องสามารถติดตั้ง Hard disk แบบ SSD, SAS, NL-SAS หรือ NVMe ได้เป็นอย่างน้อย

๑.๕ ติดตั้งหน่วยควบคุม Hard Disk ที่สนับสนุนการทำ RAID ๐, ๑, ๕ ได้ พร้อมติดตั้ง Hard disk แบบ NL-SAS ความเร็วรอบไม่ต่ำกว่า ๗,๒๐๐ รอบต่อนาที ขนาดไม่น้อยกว่า ๑๒ TB จำนวน ๘ หน่วย และแบบ SSD ขนาดไม่น้อยกว่า ๙๖๐ GB จำนวน ๔ หน่วย

๑.๖ มี I/O Expansion Slots แบบ PCIe จำนวนไม่น้อยกว่า ๖ Slots

๑.๗ มีส่วนเชื่อมต่อกับระบบเครือข่ายแบบ ๑๐ Gbase-T จำนวนไม่น้อยกว่า ๒ Ports แบบ ๑ Gbase-T ไม่น้อยกว่า ๒ Ports

๑.๘ มีหน่วยจ่ายไฟแบบ Hot-Pluggable ขนาดไม่น้อยกว่า ๑,๔๐๐ Watts จำนวน ๒ หน่วย

๒. ซอร์ฟแวร์บริหารจัดการระบบจัดเก็บข้อมูลจราจรคอมพิวเตอร์ จำนวน ๑ ชุด

๒.๑ ต้องรองรับการทำงานร่วมกับอุปกรณ์เครือข่ายหลายประเภท เช่น Switches, Routers, Firewalls, VPN, Server เป็นต้นได้

๒.๒ ระบบที่นำเสนอต้องสามารถจัดเก็บข้อมูลบันทึกเหตุการณ์ที่จำเป็นใน พรบ. การจัดเก็บข้อมูลการจราจรคอมพิวเตอร์ได้อย่างน้อย ๒๐,๐๐๐ เหตุการณ์ต่อวินาที

๒.๓ สามารถจัดเก็บ log file ได้ถูกต้องตรงตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ฉบับที่มีผลบังคับใช้ได้เป็นอย่างน้อย

๒.๔ ระบบต้องเป็นผลิตภัณฑ์ที่มีความน่าเชื่อถือและยอมรับในระดับสากล ดังนี้

๒.๔.๑ สามารถทำงานในระดับการตรวจจับภัยคุกคามด้านไซเบอร์ (SIEM – Security Information Event Management) และรองรับการตอบสนองต่อภัยคุกคามด้านไซเบอร์ (SOAR – Security Orchestration Automation, And Response)

๒.๔.๒ ผลิตภัณฑ์ที่นำเสนอต้องมีตัวแทนจำหน่ายในประเทศไทย และมีพนักงานประจำที่ดูแลประเทศไทย

๒.๕ ระบบต้องสามารถรวบรวมบันทึกเหตุการณ์ที่ส่งมาระบบต้นทางในรูปแบบ Syslog, Event log, WMI, SNMP trap, XML, JSON, CSV หรือ Email ได้เป็นอย่างน้อย

๒.๖ ระบบที่นำเสนอต้องสามารถรวบรวมบันทึกเหตุการณ์จากอุปกรณ์เครือข่ายในรูปแบบ NetFlow, IPFIX, sFlow, J-Flow และ NetFlow v๙ ได้

๒.๗ สามารถนำ Logs ที่จัดเก็บไว้มาสร้าง Use Cases ด้าน Security Compliance ได้หลากหลาย เช่น การสร้าง Security Dashboards และ Reports สำหรับการทบทวนเหตุการณ์ด้านความมั่นคงปลอดภัย

๒.๘ ระบบที่นำเสนอสามารถทำตามข้อกำหนดของมาตรฐานด้านความมั่นคงปลอดภัยต่างๆ ดังต่อไปนี้

๒.๘.๑ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

๒.๘.๒ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ฉบับที่ ๒ (พ.ศ. ๒๕๖๐)

๒.๘.๓ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

๒.๘.๔ ระบบต้องมีความสอดคล้องตามนโยบายพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๒.๘.๕ ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมเรื่องหลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๖๔

๒.๙ ระบบที่นำเสนอสามารถทำงานได้ตรงตามมาตรฐาน ดังต่อไปนี้

๒.๙.๑. ISO/IEC ๒๗๐๐๑

๒.๙.๒ PCI DSS

๒.๙.๓ HIPPA

๒.๑๐ ระบบที่นำเสนอต้องมีชุดตัววิเคราะห์แยกแยะบันทึกเหตุการณ์ (event parsers) แบบสำเร็จรูปพร้อมใช้งานสำหรับบันทึกเหตุการณ์จากระบบต้นทางอย่างน้อย ดังนี้

๒.๑๐.๑ DHCP Server

๒.๑๐.๒ OpenLDAP Server

๒.๑๐.๓ Next Gen Firewall

๒.๑๐.๔ Windows Server

๒.๑๐.๕ Linux Server

๒.๑๑ ระบบที่นำเสนอต้องสามารถแสดงบันทึกเหตุการณ์ในรูปแบบดิบ (RAW) ก่อนที่จะทำการวิเคราะห์แยกแยะ

๒.๑๒ ระบบที่นำเสนอต้องสามารถแสดงข้อมูลในรูปแบบบันทึกเหตุการณ์ต้นฉบับ รายการ และแผนภูมิ ได้

๒.๑๓ ระบบที่นำเสนอต้องสามารถให้ผู้ใช้งานสืบค้นข้อมูลทั้งหมดที่รวบรวมไว้ในระบบได้

๒.๑๔ ระบบที่นำเสนอต้องสามารถให้ผู้ใช้งานค้นหาข้อมูลบันทึกเหตุการณ์ที่แยกแยะแล้วโดยระบุกรองตามฟิลด์ที่แยกวิเคราะห์ไว้แล้ว

๒.๑๕ ระบบที่นำเสนอต้องสามารถให้ผู้ใช้งานสร้างรายงานจากข้อมูลใด ๆ ที่รวบรวมไว้ในระบบ โดยรายงานจะถูกสร้างขึ้นโดยอัตโนมัติ ตามช่วงเวลาที่กำหนดไว้

๒.๑๖ ระบบที่นำเสนอต้องสามารถสร้างรายงานในรูปแบบ PDF หรือ docx หรือ xlsx หรือ JPEG ได้เป็นอย่างน้อย และรองรับการเพิ่มคำอธิบายประกอบเอกสาร และโลโก้ที่ต้องการในรายงานได้

๒.๑๗ ระบบที่นำเสนอต้องมีระบบยืนยันตัวตนเข้าใช้งานระบบด้วยบัญชีผู้ใช้ร่วมกับรหัสผ่าน หรือด้วยใบรับรองเป็นอย่างน้อย

๒.๑๘ ระบบที่นำเสนอต้องสามารถรองรับการเข้ารหัสโดยใช้โปรโตคอล TLS เวอร์ชั่น ๑.๑ หรือ HTTPS หรือดีกว่า ในการสื่อสารระหว่างส่วนงานทั้งหมด

๒.๑๙ ระบบที่นำเสนอต้องสามารถรองรับการเข้ารหัสโดยใช้โปรโตคอล TLS เวอร์ชั่น ๑.๑ หรือ HTTPS หรือดีกว่า ในการสื่อสารระหว่างระบบกับเว็บเบราว์เซอร์ของผู้ใช้งาน

๒.๒๐ รองรับข้อมูลจากแหล่งข้อมูลหลายประเภท เช่น อุปกรณ์เครือข่าย ระบบปฏิบัติการ ระบบฐานข้อมูลหรือแอปพลิเคชัน

๒.๒๑ สามารถประมวลผลข้อมูลจากหลายแหล่งพร้อมกัน และสามารถทำ Event Correlation เพื่อวิเคราะห์หาความเชื่อมโยงของเหตุการณ์ที่เกิดขึ้นได้

๒.๒๒ ระบบที่นำเสนอต้องสามารถกำหนดชุดกฎ Correlation Rules ได้อย่างน้อย ดังนี้

๒.๒๒.๑ สามารถสร้างชุดกฎ (Correlation Rules) ที่กำหนดไว้ล่วงหน้าไม่น้อยกว่า ๒๐ รายการ

๒.๒๒.๒ สามารถสร้างและปรับแต่งกฎใหม่ได้ตามความต้องการของผู้ใช้งาน

๒.๒๒.๓ สามารถสร้างเงื่อนไขในการตรวจจับข้อความ (Keyword) ใดๆ ในเนื้อหาภายในข้อมูล Log ได้

๒.๒๒.๔ สามารถแจ้งการพบหรือไม่พบค่าของ Field ที่ต้องการได้

๒.๒๒.๕ สามารถสร้างเงื่อนไขการตรวจจับเหตุการณ์ที่เกิดขึ้นตามจำนวนครั้งหรือความถี่ได้

๒.๒๒.๖ สามารถค้นหาและแสดงผลเหตุการณ์หรือเหตุการณ์ผิดปกติที่เกิดขึ้นจากกฎการวิเคราะห์ที่ตั้งไว้

๒.๒๒.๗ สามารถนำผลการค้นหามาใช้สร้างกฎเพิ่มเติมได้

๒.๒๒.๘ สามารถรวบรวมผลลัพธ์จากการค้นหาหลายรายการเพื่อวิเคราะห์ร่วมกัน

๒.๒๒.๙ สามารถจัดระดับความรุนแรงของเหตุการณ์ที่ตรวจพบได้ และสามารถปรับระดับความรุนแรงตามความเหมาะสมของกฎแต่ละรายการได้

๒.๒๓ ระบบที่นำเสนอต้องสามารถแสดงตำแหน่งทางภูมิศาสตร์ของ IP Address ที่เกี่ยวข้องกับเหตุการณ์ด้านข้อมูลภัยคุกคามได้

๒.๒๔ ระบบที่นำเสนอต้องสามารถรวบรวมและจัดการบันทึกเหตุการณ์แบบรวมศูนย์ผ่าน Web Browser เช่น Firefox, Chrome, Microsoft Edge ได้

๒.๒๕ ระบบที่นำเสนอสามารถให้เจ้าหน้าที่ตรวจสอบความถูกต้องสมบูรณ์ (Data Integrity) ของ Log ที่จัดเก็บไว้บนระบบ Centralized Log ด้วยอัลกอลิทึมที่ใช้ตรวจสอบความถูกต้องคือ MD๕ หรือ SHA๑ หรือ SHA ๒๕๖ ได้เป็นอย่างน้อย

๒.๒๖ สามารถนำเสนออุปกรณ์ได้มากกว่าหนึ่งผลิตภัณฑ์ แต่ระบบทั้งหมดต้องใช้งานร่วมกันได้

๓. โทรทัศน์แอล อี ดี (LED TV) แบบ Smart TV ระดับความละเอียดจอภาพ ๓๘๔๐x๒๑๖๐ พิกเซล ขนาด ๖๕ นิ้ว จำนวน ๑ เครื่อง

๓.๑ ระดับความละเอียด เป็นความละเอียดของจอภาพ (Resolution) (พิกเซล)

๓.๒ ขนาดที่กำหนดเป็นขนาดจอภาพ ๖๕ นิ้ว

๓.๓ แสดงภาพด้วยหลอดไฟแบ็คไลท์ LED TV

๓.๔ สามารถเชื่อมต่ออินเตอร์เน็ตได้ (Smart TV)

๓.๕ เป็นระบบปฏิบัติการ Android Tizen VIDAA U webOS หรืออื่นๆ

๓.๖ ช่องต่อ HDMI ไม่น้อยกว่า ๒ ช่อง เพื่อการเชื่อมต่อสัญญาณภาพและเสียง

๓.๗ ช่อง USB ไม่น้อยกว่า ๑ ช่อง รองรับไฟล์ภาพ เพลง และภาพยนตร์

๓.๘ มีตัวรับสัญญาณดิจิทัล (Digital) ในตัว

ผู้เสนอราคาต้องทำตารางการเปรียบเทียบคุณลักษณะระหว่างซอฟต์แวร์ที่เสนอกับข้อกำหนดคุณลักษณะที่มหาวิทยาลัยฯ กำหนดไว้ และมีเอกสารอ้างอิง **ณ วันยื่นเสนอราคา**

๒. กำหนดเวลาส่งมอบพัสดุ

กำหนดส่งมอบระบบจัดเก็บข้อมูลจราจรคอมพิวเตอร์ จำนวน ๑ ระบบ ภายใน ๑๘๐ วัน นับถัดจากวันที่ลงนามในสัญญา และต้องทำการติดตั้งและทดสอบการทำงานให้สามารถทำงานร่วมกันได้ก่อนการส่งมอบไม่น้อยกว่า ๑๕ วัน

๓. หลักเกณฑ์การพิจารณาคัดเลือกข้อเสนอ

- พิจารณาคัดเลือกข้อเสนอโดยใช้เกณฑ์ราคา

๔. วงเงินงบประมาณ/วงเงินที่ได้รับจัดสรร

๔.๑ งบประมาณรายจ่ายจากรายได้ฯ ประจำปีงบประมาณ พ.ศ. ๒๕๖๘ สถาบันคอมพิวเตอร์ แผนงานบริหารมหาวิทยาลัย กองทุนสินทรัพย์ถาวร งบลงทุน ค่าครุภัณฑ์ เป็นเงิน ๔,๐๐๐,๐๐๐.๐๐ บาท (สี่ล้านบาทถ้วน)

๔.๒ ราคากลาง เป็นเงิน ๔,๐๐๓,๒๖๖.๖๖ บาท (สี่ล้านสามพันสองร้อยหกสิบหกบาทหกสิบหกสตางค์)

๕. งวดงานและการจ่ายเงิน

งวดเดียว ชำระเงินเมื่อผู้ขายได้ส่งมอบงานแล้วเสร็จ และคณะกรรมการตรวจรับพัสดุได้ตรวจรับพัสดุเรียบร้อยแล้ว

๖. อัตราค่าปรับ

อัตราค่าปรับ ร้อยละ ๐.๒๐ (ศูนย์จุดสองศูนย์) ของวงเงินที่ตกลงซื้อตามสัญญา

๗. การกำหนดระยะเวลารับประกันความชำรุดบกพร่อง

๑. รายการที่ ๑ ต้องมีการรับประกันแบบ ๗x๒๔x๔ เป็นระยะเวลา ๕ ปี โดยต้องทำการเปลี่ยนอุปกรณ์ที่ชำรุด ๔ ชั่วโมง หลังจากได้รับแจ้งจากทางมหาวิทยาลัยฯ

๒. รายการที่ ๒ ต้องมีใบอนุญาตลิขสิทธิ์ซอฟต์แวร์แบบถาวร และมีการรับประกันอย่างน้อย ๓ ปี

๓. รายการที่ ๒ ต้องมีการรับประกันบริการแบบออนไซด์ ๒๔x๗x๔ ระยะเวลาอย่างน้อย ๓ ปี โดยเมื่อเกิดปัญหาเกี่ยวกับการทำงานของระบบฯ ต้องมีผู้เชี่ยวชาญเข้ามาดำเนินการแก้ไขให้ระบบใช้งานได้ภายใน ๔ ชั่วโมง หลังจากได้รับแจ้งจากทางมหาวิทยาลัยฯ

๔. รายการที่ ๓ ต้องมีการรับประกัน ๑ ปี

๘. การกำหนดตัวถ่วง

๑. จำนวนชั่วโมงที่ขัดข้องในขณะใดขณะหนึ่งเท่ากับค่าสูงสุดของจำนวนชั่วโมงที่ขัดข้องในขณะนั้นของอุปกรณ์คูณด้วยค่าตัวถ่วง

จำนวนชั่วโมง = ค่าสูงสุด (ชั่วโมงที่ขัดข้อง x ค่าตัวถ่วง)

เศษของชั่วโมงนับเป็น ๑ ชั่วโมง

๒. ค่าปรับ = ๐.๐๓๕ x (ผลรวมจำนวนชั่วโมง - ๒๔) x ราคาอุปกรณ์ที่ขัดข้อง

๓. กำหนดค่าตัวถ่วงของคอมพิวเตอร์

อุปกรณ์ที่ขัดข้อง	ค่าถ่วง
๑. เครื่องคอมพิวเตอร์แม่ข่ายสำหรับติดตั้งระบบจัดเก็บข้อมูลจราจรคอมพิวเตอร์	๑
๒. ซอร์ฟแวร์บริหารจัดการระบบจัดเก็บข้อมูลจราจรคอมพิวเตอร์	๑

ลงชื่อ.....ประธานกรรมการ
(นายขจรฤทธิ์ พุ่มพฤกษ์)

ลงชื่อ.....กรรมการ
(นายภาสกร พรเจริญนพ)

ลงชื่อ.....กรรมการ
(นายจิรศักดิ์ พรอัครพันธุ์)

ลงชื่อ.....กรรมการ
(นายนิพพิชฌน์ อ่อนหิรัญ)

ลงชื่อ.....กรรมการและเลขานุการ
(นางศิริพร อำพันทอง)