

รายละเอียดขอบเขตของงานทั้งโครงการ (Term of Reference: TOR)
โครงการ จัดซื้อระบบบริหารจัดการเหตุการณ์และข้อมูลการรักษาความมั่นคงปลอดภัย Security
Information and Event Management (SIEM) มหาวิทยาลัยเชียงใหม่

.....

1. หลักการและเหตุผล

ภายใต้ยุทธศาสตร์ชาติ 20 ปี ยุทธศาสตร์ที่ 6 สร้างความเชื่อมั่นในการใช้เทคโนโลยีดิจิทัล และรัฐบาลได้ประกาศบังคับใช้พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ในวันที่ 28 พฤษภาคม 2562 มหาวิทยาลัยเชียงใหม่ ในฐานะมหาวิทยาลัยในการกำกับของรัฐที่มีการใช้ระบบสารสนเทศเข้ามาบูรณาการในการทำงานขององค์กรเพื่อสนับสนุนการดำเนินการตามภารกิจหลัก (Core Business) มีการจัดเก็บ การใช้ การเชื่อมโยงแลกเปลี่ยนข้อมูลที่เกี่ยวข้องกับข้อมูลส่วนบุคคล จึงจำเป็นต้องมีการจัดตั้งให้มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์หรือช่องโหว่ของทรัพย์สินด้านสารสนเทศ (Digital Assets) ซึ่งเป็นส่วนที่มีการเชื่อมต่อกับเครือข่ายภายนอกหรืออินเทอร์เน็ตทั้งนี้เพื่อให้ระบบสารสนเทศมีมาตรฐานความปลอดภัยจากภัยคุกคามทางไซเบอร์จากบุคคลที่ไม่ประสงค์ดี เกิดความเชื่อมั่นในการใช้งานระบบ และเสริมประสิทธิภาพของระบบเดิมที่มีอยู่ซึ่งระบบเดิมยังมีประสิทธิภาพไม่เพียงพอต่อการรับมือภัยคุกคามในปัจจุบัน

ดังนั้น เพื่อให้การสนับสนุนการดำเนินงานด้านการรักษาความปลอดภัยสารสนเทศ และการให้บริการของมหาวิทยาลัยมีความปลอดภัย สามารถทำการระบุ ตรวจสอบ และตอบสนองต่อภัยคุกคามต่อความปลอดภัยของระบบสารสนเทศให้เป็นไปตามกฎหมายที่เกี่ยวข้องจึงมีความต้องการระบบบริหารจัดการเหตุการณ์และข้อมูลการรักษาความมั่นคงปลอดภัย Security Information and Event Management (SIEM)

2. วัตถุประสงค์

- 2.1 เพื่อให้มีระบบในการตรวจจับภัยคุกคามด้านสารสนเทศ และเหตุละเมิดความมั่นคงปลอดภัยสารสนเทศได้อย่างมีประสิทธิภาพและทันทั่วถึง
- 2.2 เพื่อให้มีระบบในการจัดเก็บและบริหารจัดการข้อมูลจราจรคอมพิวเตอร์ (Logs) ของระบบเทคโนโลยีสารสนเทศที่มีความสำคัญต่อการให้บริการของมหาวิทยาลัยให้เป็นไปตามกฎหมายที่เกี่ยวข้อง
- 2.3 เพื่อให้มีระบบในการจัดเก็บสารสนเทศที่เกี่ยวข้องกับภัยคุกคามด้านสารสนเทศ และเหตุละเมิดความมั่นคงปลอดภัยสารสนเทศเพื่อใช้ในการวิเคราะห์ทางนิติวิทยาศาสตร์ (Forensics) อันจะนำไปสู่การป้องกันภัยคุกคามด้านสารสนเทศที่มีประสิทธิภาพมากยิ่งขึ้นในอนาคต

3. คุณสมบัติของผู้เสนอราคา

- 3.1 มีความสามารถตามกฎหมาย
- 3.2 ไม่เป็นบุคคลล้มละลาย
- 3.3 ไม่อยู่ระหว่างเลิกกิจการ

- 3.4 ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง
- 3.5 ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทำงานและได้แจ้งเวียนชื่อให้เป็นผู้ทำงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทำงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย
- 3.6 มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา
- 3.7 เป็นนิติบุคคล ผู้มีอาชีพขายพัสดุที่ประกวดราคาอิเล็กทรอนิกส์ดังกล่าว
- 3.8 ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่สำนักบริการเทคโนโลยีสารสนเทศ มหาวิทยาลัยเชียงใหม่ ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันราคาอย่างเป็นธรรมในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้
- 3.9 ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ยื่นข้อเสนอราคาได้มีคำสั่งให้สละเอกสิทธิ์ความคุ้มกันเช่นนั้น
- 3.10 ผู้ยื่นข้อเสนอต้องลงทะเบียนในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (Electronic Government Procurement: e-GP) ของกรมบัญชีกลาง
- 3.11 ผู้ยื่นข้อเสนอต้องจัดทำคุณลักษณะเฉพาะและรายละเอียดของระบบบริหารจัดการเหตุการณ์และข้อมูลการรักษาความมั่นคงปลอดภัย Security Information and Event Management (SIEM) ที่เสนอมาพร้อมกับการยื่นข้อเสนอราคาครั้งนี้ โดยทำในรูปแบบตารางเปรียบเทียบคุณลักษณะเฉพาะของสำนักฯ กำหนด และคุณลักษณะเฉพาะของผู้ยื่นข้อเสนอ (ตามข้อ 4.3)
- 3.12 ผู้ยื่นข้อเสนอจะต้องได้รับการแต่งตั้งให้เป็นตัวแทนจำหน่ายจากผู้ผลิตหรือตัวแทนจำหน่ายในประเทศไทย โดยมีหนังสือแต่งตั้งที่ไม่หมดอายุนับถึงวันที่ยื่นข้อเสนอราคา และให้ยื่นเอกสารมาพร้อมกับการยื่นเสนอราคาครั้งนี้
- 3.13 ผู้ยื่นข้อเสนอจะต้องยื่นสำเนาใบขึ้นทะเบียนผู้ประกอบการวิสาหกิจขนาดกลางและขนาดย่อม (SMEs) และต้องไม่หมดอายุ ณ วันยื่นเอกสารข้อเสนอ (ถ้ามี)
- 3.14 ผู้ยื่นข้อเสนอที่ยื่นข้อเสนอในรูปแบบของ "กิจการร่วมค้า" ต้องมีคุณสมบัติดังนี้
กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมค่างำหนดให้ผู้เข้าร่วมค้ายรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก ข้อตกลงระหว่างผู้เข้าร่วมค้าจะต้องมีการกำหนดสัดส่วนหน้าที่และความรับผิดชอบในปริมาณงาน สิ่งของหรือมูลค่าตามสัญญาของผู้เข้าร่วมค้าหลักมากกว่าผู้เข้าร่วมค้ายรายอื่นทุกราย

กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมคำกำหนดให้ผู้เข้าร่วมคำรายใดรายหนึ่งเป็นผู้เข้าร่วมคำหลัก กิจการร่วมค่านั้นต้องใช้ผลงานของผู้เข้าร่วมคำหลักรายเดียวเป็นผลงานของกิจการร่วมคำที่ยื่นข้อเสนอ

สำหรับข้อตกลงระหว่างผู้เข้าร่วมคำที่ไม่ได้กำหนดให้ผู้เข้าร่วมคำรายใดเป็นผู้เข้าร่วมคำหลัก ผู้เข้าร่วมคำทุกรายจะต้องมีคุณสมบัติครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารเชิญชวน

กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมคำกำหนดให้มีการมอบหมายผู้เข้าร่วมคำรายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอ ในนามกิจการร่วมคำ การยื่นข้อเสนอดังกล่าวไม่ต้องมีหนังสือมอบอำนาจ

สำหรับข้อตกลงระหว่างผู้เข้าร่วมคำที่ไม่ได้กำหนดให้ผู้เข้าร่วมคำรายใดเป็นผู้ยื่นข้อเสนอ ผู้เข้าร่วมคำทุกรายจะต้องลงลายมือชื่อในหนังสือมอบอำนาจให้ผู้เข้าร่วมคำรายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอในนามกิจการร่วมคำ

- 3.15 ผู้ยื่นข้อเสนอต้องมีมูลค่าสุทธิของกิจการ เป็นไปตามหนังสือคณะกรรมการวินิจฉัยปัญหาการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ ด่วนที่สุด ที่ กค(กวจ) ที่ 0405.2 /ว124 ลงวันที่ 1 มีนาคม 2566

มูลค่าสุทธิของกิจการ

(1) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยซึ่งได้จดทะเบียนเกินกว่า 1 ปี ต้องมีมูลค่าสุทธิของกิจการ จากผลต่างระหว่างสินทรัพย์สุทธิหักด้วยหนี้สินสุทธิที่ปรากฏในงบแสดงฐานะการเงินที่มีการตรวจรับรองแล้ว ซึ่งจะต้องแสดงค่าเป็นบวกติดต่อกันเป็นระยะเวลา 1 ปีสุดท้ายก่อนวันยื่นข้อเสนอ

(2) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย ซึ่งยังไม่มีงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า ให้พิจารณาการกำหนดมูลค่าของทุนจดทะเบียน โดยผู้ยื่นข้อเสนอจะต้องมีทุนจดทะเบียนที่เรียกชำระมูลค่าหุ้นแล้ว ณ วันที่ยื่นข้อเสนอ ดังนี้

- มูลค่าการจัดซื้อจัดจ้างเกิน 10 ล้านบาท แต่ไม่เกิน 20 ล้านบาท ต้องมีทุนจดทะเบียนไม่ต่ำกว่า 3 ล้านบาท

(3) สำหรับการจัดซื้อจัดจ้างครั้งหนึ่งที่มีวงเงินเกิน 500,000 บาทขึ้นไปกรณีผู้ยื่นข้อเสนอเป็นบุคคลธรรมดา ให้พิจารณาจากหนังสือรับรองบัญชีเงินฝากไม่เกิน 90 วันก่อนวันยื่นข้อเสนอโดยต้องมีเงินฝากคงเหลือในบัญชีธนาคารเป็นมูลค่า 1 ใน 4 ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง และหากเป็นผู้ชนะการจัดซื้อจัดจ้างหรือเป็นผู้ได้รับการคัดเลือกจะต้องแสดงหนังสือรับรองบัญชีเงินฝากที่มีมูลค่าดังกล่าวอีกครั้งหนึ่งในวันลงนามในสัญญา

(4) กรณีที่ผู้ยื่นข้อเสนอไม่มีมูลค่าสุทธิของกิจการหรือทุนจดทะเบียนหรือมีแต่ไม่เพียงพอที่จะเข้ายื่นข้อเสนอ ผู้ยื่นข้อเสนอสามารถของวงเงินสินเชื่อ โดยต้องมีวงเงินสินเชื่อ 1 ใน 4 ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง สินเชื่อที่ธนาคารภายในประเทศหรือบริษัทเงินทุนหรือบริษัทเงินทุนหลักทรัพย์ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจค้าประกันตาม

ประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทยแจ้งเวียนให้ทราบ โดยพิจารณาจากยอดเงินรวมของวงเงินสินเชื่อที่สำนักงานใหญ่รับรองหรือที่สำนักงานสาขารับรอง (กรณีได้รับมอบอำนาจจากสำนักงาน) ซึ่งออกให้แก่ผู้ยื่นข้อเสนอ นับถึงวันยื่นข้อเสนอไม่เกิน 90 วัน

(5) กรณีตาม (1) - (4) ยกเว้นสำหรับกรณีดังต่อไปนี้

(5.1) กรณีที่ผู้ยื่นข้อเสนอเป็นหน่วยงานของรัฐ

(5.2) นิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยที่อยู่ระหว่างการฟื้นฟูกิจการ ตามพระราชบัญญัติล้มละลาย (ฉบับที่ 10) พ.ศ. 2561

(5.3) งานก่อสร้างที่กรมบัญชีกลางได้ขึ้นทะเบียนผู้ประกอบการงานก่อสร้างแล้ว และที่หน่วยงานของรัฐได้มีการจัดทำบัญชีผู้ประกอบการงานก่อสร้างที่มีคุณสมบัติเบื้องต้นไว้แล้วก่อนวันที่ พระราชบัญญัติการจัดซื้อจัดจ้างและการบริหารพัสดุมีผลใช้บังคับ

4. การพิจารณาทางเทคนิค

4.1 มหาวิทยาลัยเชียงใหม่จะพิจารณาเปิดซองประกวดราคาเฉพาะผู้เข้าประกวดราคาที่ผ่านมาข้อเสนอทางเทคนิคและผ่านข้อกำหนดเกี่ยวกับคุณสมบัติเท่านั้น นอกจากนี้มหาวิทยาลัยเชียงใหม่ขอสงวนสิทธิ์ในการพิจารณาโปรแกรมระบบ เครื่องแม่ข่ายประมวลผลและเก็บข้อมูล เครื่องแม่ข่ายรวบรวมข้อมูล และระบบอื่นๆ ที่ผู้เข้าประกวดราคาเสนอ ซึ่งมีคุณสมบัติอื่นที่นอกเหนือไปจากคุณสมบัติที่จำเป็น และคุณสมบัติที่ควรมี และมหาวิทยาลัยสงวนสิทธิ์ที่จะพิจารณาผู้เข้าประกวดราคารายที่เสนอราคาอยู่ภายใต้กรอบงบประมาณของโครงการ และให้ประโยชน์แก่มหาวิทยาลัยมากที่สุดก่อน

4.2 ผู้เข้าประกวดราคามีหน้าที่แสดงเอกสารต่างๆ เพื่อยืนยันหรือแสดงให้เห็นถึงคุณสมบัติต่างๆ ที่จะต้องเป็นไปตามข้อกำหนดหรือมีคุณสมบัติที่ดีกว่าข้อกำหนด โดยเอกสารที่นำมาแสดงจะต้องเป็นเอกสารตัวจริงหรือเป็นเอกสารสำเนาที่เป็นทางการ สามารถเชื่อถือได้ และเป็นที่ยอมรับโดยทั่วไป ซึ่งผู้เข้าประกวดราคามีหน้าที่จะต้องเปรียบเทียบข้อกำหนดที่มหาวิทยาลัยกำหนดในแต่ละข้อกับคุณสมบัติของตนเองและของอุปกรณ์ต่างๆ ที่เสนอ โดยจะต้องระบุให้ชัดเจนว่าเอกสารที่นำมาเสนอ ข้อความในประโยคใดที่ใช้ยืนยันข้อกำหนดหมายเลขใดของมหาวิทยาลัย โดยผู้เข้าประกวดราคามีหน้าที่ทำสัญลักษณ์แสดงบนข้อความในประโยคที่ใช้ยืนยัน ได้แก่ การขีดเส้นใต้ หรือ การระบายสี พร้อมระบุหมายเลขลำดับของข้อกำหนดที่จะทำการยืนยันให้เห็นชัดเจน ซึ่งหากผู้เข้าประกวดราคาขาดเอกสารยืนยัน หรือขาดการทำสัญลักษณ์แสดงบนข้อความในประโยคที่ใช้ยืนยัน หรือแสดงเอกสารไม่ชัดเจนทำให้ขาดข้อกำหนดหนึ่งในข้อกำหนดของมหาวิทยาลัย ให้ถือว่าผู้เข้าประกวดราคาไม่ผ่านการพิจารณาทางด้านเทคนิค

4.3 ให้จัดทำรายละเอียดข้อเสนอด้านเทคนิคของระบบงานที่เสนอ ในรูปแบบดังต่อไปนี้

หัวข้อ	คุณลักษณะที่กำหนด	คุณลักษณะที่เสนอ	เอกสารอ้างอิง (หน้า, ข้อ)
ระบุหัวข้อให้ตรงกับที่กำหนดในเอกสารนี้	ให้ คัด ล อ ก จ า ก ข้อกำหนดที่กำหนดในเอกสารนี้	ให้ระบุความสามารถหรือคุณลักษณะเฉพาะของระบบที่เสนอ	ให้ระบุหรืออ้างอิงถึงเอกสารในข้อเสนอที่เกี่ยวข้อง และทำสัญลักษณ์แสดงข้อความในประโยคของเอกสารหรือในแคตตาล็อกนั้นให้ชัดเจน

4.4 ผู้เข้าประกวดราคาจะต้องเสนออุปกรณ์และระบบเฉพาะที่มหาวิทยาลัยได้ระบุไว้ในตารางที่ 1 เท่านั้น ซึ่งหากผู้เข้าประกวดราคาได้เสนอรายการอุปกรณ์อื่นใดที่นอกเหนือไปจากข้อกำหนดดังกล่าว มหาวิทยาลัยขอสงวนสิทธิ์ในการเปลี่ยนแปลงคุณสมบัติรายการอุปกรณ์และระบบที่เสนอดังกล่าวได้ในภายหลัง เพื่อให้ระบบสามารถใช้งานได้อย่างมีประสิทธิภาพ

4.5 ผู้เข้าประกวดราคาต้องจัดทำเอกสารสรุปแสดงรายการอุปกรณ์ต่างๆ ในแต่ละระบบ พร้อมทั้งรายละเอียดภายในอุปกรณ์ที่นำเสนอให้ครบถ้วนทุกรายการเพื่อประกอบการพิจารณา

4.6 ผู้ชนะการประกวดราคาต้องยื่นเอกสารจำแนกรายละเอียด Bill of Quantity (BOQ) ของอุปกรณ์ในรายการตามตารางที่ 1 โดยแสดงราคาต่อหน่วยของอุปกรณ์และราคารวมทั้งหมด โดยราคาต่อหน่วยนั้นได้รวมค่าใช้จ่ายของอุปกรณ์ ค่าการติดตั้ง ค่าบำรุงรักษา การรับประกัน และค่าใช้จ่ายต่าง ๆ ทั้งหมดไว้แล้ว ภายใน 15 วัน นับจากวันที่แจ้งผลการประกวดราคา

5. กำหนดระยะเวลาการติดตั้งและส่งมอบ

ผู้ชนะการประกวดราคาต้องส่งมอบระบบทั้งหมด พร้อมผลรายงานการทดสอบต่าง ๆ ภายในระยะเวลา 180 วัน หรือ 6 เดือน นับจากวันลงนามในสัญญา ซึ่งหากเกินกว่าระยะเวลาดังกล่าว ผู้ชนะการประกวดราคาต้องถูกปรับเป็นรายวันในอัตราร้อยละ 0.2 ของราคาพัสดุที่ยังไม่ได้รับมอบ

6. งบประมาณ 12,500,000 บาท (สิบสองล้านบาทถ้วน)

มหาวิทยาลัยจะทำการตรวจรับอุปกรณ์พร้อมระบบทั้งหมด และเบิกจ่ายเงินให้แก่ผู้ชนะการประกวดราคา เมื่อผู้ชนะการประกวดราคาได้ทำการติดตั้งและส่งมอบอุปกรณ์ พร้อมระบบทั้งหมด ครบถ้วนตามตารางที่ 1 ซึ่งมีรายงานครบถ้วนและระบบพร้อมใช้งานให้แก่มหาวิทยาลัยเป็นที่เรียบร้อยแล้ว

7. ข้อกำหนดการติดตั้งอุปกรณ์และระบบทั้งหมด

7.1 ผู้ชนะการประกวดราคาต้องเสนอแผนการติดตั้งของอุปกรณ์และระบบทั้งหมดอย่างละเอียด ซึ่งประกอบด้วยรายชื่อผู้รับผิดชอบโครงการ สถานที่ติดต่อ หมายเลขโทรศัพท์ ขั้นตอนการติดตั้งอุปกรณ์ในระบบต่างๆ และระยะเวลาในการดำเนินการแต่ละขั้นตอนที่แน่นอนให้กับมหาวิทยาลัยพิจารณาเห็นชอบภายใน 20 วัน นับจากวันลงนามในสัญญา

7.2 ผู้ชนะการประกวดราคาจะต้องมีบุคลากรที่มีความรู้ความสามารถในการติดตั้งและกำหนดค่า (Configuration) ให้กับระบบ SIEM ซึ่งจะต้องมีใบประกาศรับรองความรู้ความสามารถดังกล่าว (Certificate) จากบริษัทผู้ผลิต โดยมหาวิทยาลัยขอสงวนสิทธิ์ในการพิจารณาความรู้ความสามารถของบุคลากรที่จะมาติดตั้งและกำหนดค่าดังกล่าวด้วย

7.3 ก่อนที่ผู้ชนะการประกวดราคาจะเข้าดำเนินการใดๆ ผู้ชนะการประกวดราคาจะต้องทำจดหมายแจ้งให้กับมหาวิทยาลัยรับทราบก่อนจะเข้าดำเนินการอย่างน้อย 5 วันทำการ และจะต้องรอให้ได้รับการอนุมัติจากมหาวิทยาลัยก่อน จึงจะสามารถดำเนินการใดๆ ได้ ซึ่งหากผู้ชนะการประกวดราคาเข้าทำการติดตั้งระบบใดๆ โดยไม่ได้รับการอนุมัติจากมหาวิทยาลัย มหาวิทยาลัยมีสิทธิที่จะให้ผู้ชนะการประกวดราคาดำเนินการรื้อถอนระบบๆ ต่างที่ได้ติดตั้งไปแล้ว โดยให้ถือเป็นความผิดและความรับผิดชอบของผู้ชนะการประกวดราคา

7.4 ผู้ชนะการประกวดราคาจะต้องเป็นผู้จัดหาสายสัญญาณต่อเชื่อม Patch Cable สายไฟฟ้า หรือสายอื่นใดที่เกี่ยวข้องในการติดตั้ง โดยจะต้องมีการจัดทำป้ายบ่งบอก (Label) ทุกเส้น และจัดเก็บรหัสสายสัญญาณให้เรียบร้อยสวยงาม

7.5 ผู้ชนะการประกวดราคาต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น อันเนื่องจากการติดตั้ง อุปกรณ์หรือความเสียหายใดที่เกิดขึ้นจากการปฏิบัติงานของทีมงานของผู้ชนะการประกวดราคา โดยผู้ชนะการประกวดราคาจะต้องดำเนินการซ่อมแซมแก้ไขให้อยู่ในสภาพเดิมโดยเร็วและยินยอมชดเชยค่าเสียหายที่เกิดขึ้นให้กับมหาวิทยาลัย

7.6 การติดตั้งอุปกรณ์และระบบที่ผู้ชนะการประกวดราคาได้เสนอ หรือติดตั้งอุปกรณ์และระบบอื่นใดเพิ่มเติม ซึ่งหากไม่ได้รับรู้ไว้ในข้อกำหนดของมหาวิทยาลัย ให้อยู่ในดุลยพินิจของมหาวิทยาลัย ที่จะเป็นผู้กำหนดลักษณะและรูปแบบของการติดตั้ง โดยขึ้นอยู่กับความจำเป็นและสภาพการใช้งานจริง เพื่อให้ระบบสามารถใช้งานได้อย่างมีประสิทธิภาพเป็นสำคัญ

7.7 ผู้ชนะการประกวดราคาจะต้องปฏิบัติตามนโยบายความมั่นคงปลอดภัยสารสนเทศ และกฎระเบียบต่างๆ ด้านความมั่นคงปลอดภัยสารสนเทศของสำนักฯอย่างเคร่งครัด

7.8 ผู้ชนะการประกวดราคาจะต้องปฏิบัติตามกฎหมายและข้อบังคับต่างๆ ที่เกี่ยวข้อง เช่น พรบ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พรบ.ลิขสิทธิ์ พรบ.คุ้มครองข้อมูลส่วนบุคคล เป็นต้น

7.9 ผู้ชนะการประกวดราคาจะต้องไม่เปิดเผยหรือเผยแพร่ข้อมูลที่สำคัญต่างๆ เช่น การตั้งค่าของระบบ (Configuration) รหัสผ่าน (Password) แผนผังของระบบ (Diagram) เป็นต้น ให้บุคคลอื่นทราบโดยไม่ได้รับอนุญาต อนึ่งไม่ว่าเวลาใด แม้สิ้นสุดสัญญาก็ตาม การรักษาข้อมูลที่สำคัญต่างๆ ยังคงมีผลผูกพันกับคู่สัญญาต่อไป มิฉะนั้นมหาวิทยาลัยจะดำเนินการเรียกร้องค่าเสียหาย โดยถือเป็นความผิดของผู้ชนะการประกวดราคา

8. รายการอุปกรณ์และระบบที่มหาวิทยาลัยต้องการ

มหาวิทยาลัยเชียงใหม่มีความประสงค์ที่จะประกวดราคาเพื่อจัดซื้อระบบบริหารจัดการเหตุการณ์และข้อมูลการรักษาความมั่นคงปลอดภัย Security Information and Event Management (SIEM) โดยประกอบด้วยอุปกรณ์และระบบต่างๆ ดังตารางที่ 1 ซึ่งรวมถึง การติดตั้งอุปกรณ์ การกำหนดค่าคำสั่งการทำงานอุปกรณ์ (Configuration) พร้อมทั้งทดสอบการใช้งานของระบบ ซึ่งมีความพร้อมทำงานได้ตามข้อกำหนด ซึ่งอุปกรณ์และระบบทั้งหมดประกอบไปด้วยรายการต่าง ๆ ดังต่อไปนี้ โดยกำหนดคุณสมบัติเฉพาะของอุปกรณ์และระบบทั้งหมดในภาคผนวก ก

ตารางที่ 1 : รายชื่ออุปกรณ์และระบบที่มหาวิทยาลัยต้องการ

ลำดับ	รายการ	จำนวน
1	โปรแกรมระบบ	1 ระบบ
2	เครื่องแม่ข่ายประมวลผลและเก็บข้อมูล	1 ชุด
3	เครื่องแม่ข่ายรวบรวมข้อมูล (Data Collector)	2 ชุด
4	อุปกรณ์แปลงสัญญาณเครือข่ายแบบ SFP+ Module	8 ชุด

9. การตรวจรับอุปกรณ์พร้อมระบบ และการฝึกอบรมภายหลังการติดตั้ง

9.1 ผู้ชนะการประกวดราคาต้องจัดเตรียมเอกสารต่างๆ สำหรับการส่งมอบและการตรวจรับอย่างเหมาะสมให้กับทางมหาวิทยาลัยเชียงใหม่พิจารณา โดยประกอบด้วยข้อมูลดังต่อไปนี้เป็นอย่างน้อย ได้แก่ ชื่ออุปกรณ์ รุ่นอุปกรณ์ ชนิดอุปกรณ์ ชื่อบริษัทผู้ผลิตอุปกรณ์ หมายเลขประจำตัวอุปกรณ์ (Serial No) หมายเลขประจำตัวอุปกรณ์ย่อย (ถ้ามี) ฯลฯ

9.2 ผู้ชนะการประกวดราคาต้องทำหนังสือแจ้งการส่งมอบอุปกรณ์และระบบทั้งหมดเพื่อตรวจรับให้ทางมหาวิทยาลัยเชียงใหม่ทราบก่อนวันส่งมอบอย่างน้อย 5 วันทำการ พร้อมทั้งจัดส่งเอกสารต่างๆ และไฟล์คอมพิวเตอร์ที่เกี่ยวข้องให้ครบถ้วน รวมถึงรายละเอียดอื่นใดที่จำเป็นในการตรวจรับให้แก่มหาวิทยาลัยเชียงใหม่

9.3 ผู้ชนะการเสนอราคาต้องจัดฝึกอบรมการใช้งานและดูแลระบบทั้งหมดดังกล่าว ที่ได้ทำการติดตั้งดังกล่าวให้แก่ผู้ดูแลระบบของมหาวิทยาลัยเป็นระยะเวลา 2 วัน จำนวนไม่น้อยกว่า 5 คน โดยต้องรับผิดชอบค่าใช้จ่ายที่เกิดขึ้นจากการอบรมดังกล่าวทั้งหมด เช่น ค่าวิทยากร ค่าเอกสาร ค่าเช่าห้อง ค่าเช่าอุปกรณ์ ค่าอาหารว่าง และอาหารกลางวัน ในกรณีที่ต้องมีการเดินทางไปอบรมในพื้นที่อื่น จะต้องรวมค่าเดินทางและค่าที่พักไว้ด้วยแล้ว โดยมหาวิทยาลัยขอสงวนสิทธิ์ในการพิจารณาความเหมาะสมของเนื้อหาหลักสูตรและความรู้ความสามารถของวิทยากรที่จะมาอบรมดังกล่าวด้วย

10. การดูแลรักษาและการรับประกัน

10.1 ระบบทั้งหมดที่ผู้ชนะการประกวดราคาได้เสนอให้กับมหาวิทยาลัยจะต้องรับประกันถึงความเสียหายของอุปกรณ์และระบบเป็นเวลา 5 ปี นับแต่วันที่ได้ส่งมอบการติดตั้งอุปกรณ์พร้อมระบบทั้งหมดให้มหาวิทยาลัยและคณะกรรมการตรวจรับของมหาวิทยาลัยได้ตรวจรับเป็นที่เรียบร้อยแล้ว ซึ่งหากเกิดความเสียหายใด ๆ ขึ้นกับอุปกรณ์หรือระบบ ผู้ชนะการประกวดราคาจะต้องดำเนินการแก้ไขให้กับมหาวิทยาลัยโดยไม่คิดค่าใช้จ่ายใด ๆ ในการดำเนินการ

10.2 ผู้ชนะการเสนอราคาจะต้องดูแลให้ระบบใช้งานได้ดี หากอุปกรณ์ทำงานผิดพลาด ชัดข้องหรือชำรุดเสียหายไม่ว่าจะโดยสาเหตุใด มหาวิทยาลัยสามารถแจ้งเหตุขัดข้องกับอุปกรณ์และระบบทุกรายการที่เสนอไว้ได้ตลอดเวลา ทั้งทางโทรศัพท์ โทรศัพท์เคลื่อนที่ หรือจดหมายอิเล็กทรอนิกส์ ผู้ชนะการเสนอราคาจะต้องเข้ามาให้บริการ ตรวจสอบปัญหา และแก้ไขปัญหาแบบถึงสถานที่ติดตั้ง (On-site service) ภายในระยะเวลา 24 ชั่วโมง นับจากที่ได้รับแจ้งเหตุขัดข้อง ตามวันเวลาราชการ และจะต้องรายงานถึงสาเหตุของการขัดข้องดังกล่าวให้มหาวิทยาลัยทราบภายใน 48 ชั่วโมง นับจากที่ได้รับแจ้งเหตุขัดข้อง

10.3 กรณีเป็นเหตุขัดข้องและทำให้ระบบ หยุดชะงักไม่สามารถให้บริการได้ ผู้ชนะการเสนอราคาต้องรีบดำเนินการแก้ไขให้อุปกรณ์และระบบที่เสียหายนั้น กลับมาสามารถใช้งานได้ตามปกติ หรือจัดหาอุปกรณ์อื่นใดที่มีคุณสมบัติเท่าเทียมหรือดีกว่ามาทดแทน เพื่อให้ระบบสามารถใช้งานได้ตามปกติ ภายในระยะเวลา 7 วัน นับจากที่ได้รับแจ้งเหตุขัดข้อง

10.4 ผู้ชนะการเสนอราคามีหน้าที่บำรุงรักษาซ่อมแซมแก้ไขระบบบริหารจัดการเหตุการณ์ และข้อมูลการรักษาความมั่นคงปลอดภัย Security Information And Event Management (SIEM) และอุปกรณ์ที่เกี่ยวข้องให้อยู่ในสภาพใช้งานได้ดีอยู่เสมอ หากไม่ดำเนินการมหาวิทยาลัยจะปรับเป็นรายครั้ง กำหนดในอัตราร้อยละ 0.035 ของราคาตามสัญญาต่อชั่วโมง หรือใช้ตามอัตราค่าปรับที่ปรากฏตามสัญญาซื้อขายคอมพิวเตอร์

11. ข้อกำหนดอื่นๆ

ในกรณีจำเป็นมหาวิทยาลัยเชียงใหม่สามารถขอเพิ่ม ลด หรือเปลี่ยนแปลงอุปกรณ์ต่าง ๆ ให้แตกต่างจากที่ระบุไว้ในเอกสารนี้ได้ เพื่อให้อุปกรณ์และระบบต่าง ๆ ที่เสนอสามารถทำงานร่วมกับระบบเครือข่ายและระบบคอมพิวเตอร์ทั้งหมดของมหาวิทยาลัยได้อย่างมีประสิทธิภาพ โดยผู้ชนะการประกวดราคาจะต้องปฏิบัติตามที่มหาวิทยาลัยกำหนด และจะต้องเสนอมูลค่าของปริมาณงานที่เพิ่มขึ้นหรือลดลงให้มหาวิทยาลัยพิจารณาก่อนที่ผู้ชนะการประกวดราคาจะดำเนินการ ซึ่งมหาวิทยาลัยจะชำระหรือขอคืนเงินดังกล่าวให้กับผู้ชนะการประกวดราคาเมื่อมหาวิทยาลัยได้ทำการตรวจรับ และเบิกจ่ายต่อไป ทั้งนี้มหาวิทยาลัยขอสงวนสิทธิ์ที่จะพิจารณาจัดหาผู้ดำเนินการรายอื่นแทนผู้ชนะการประกวดราคาได้ หากพบว่ามูลค่าของปริมาณงานที่เพิ่มขึ้นหรือลดลงนั้น เป็นราคาที่ไม่เป็นธรรมต่อทางราชการ และอาจก่อให้เกิดความเสียหายต่อราชการได้

12. หลักเกณฑ์ในการพิจารณาคัดเลือก

ในการพิจารณาผลการยื่นข้อเสนอครั้งนี้จะพิจารณาตัดสินโดยใช้เกณฑ์ราคา

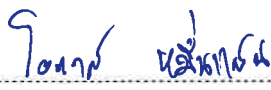
13. งานงวดงานและการจ่ายเงิน

สำนักฯ จะจ่ายค่าพัสดุซึ่งได้รวมภาษีมูลค่าเพิ่ม ตลอดจนภาษีอากรอื่น ๆ และค่าใช้จ่ายที่พึงปวงแล้วให้แก่ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกให้เป็นผู้ขาย เมื่อผู้ขายได้ส่งมอบพัสดุได้ครบถ้วนตามสัญญาหรือข้อตกลงเป็นหนังสือหรือใบสั่งซื้อ

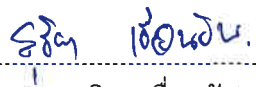
14. สถานที่ติดต่อเพื่อขอทราบข้อมูลเพิ่มเติมหรือเสนอแนะวิจารณ์หรือแสดงความคิดเห็นโดยเปิดเผยตัว

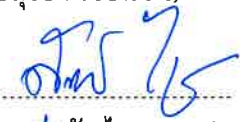
สำนักบริการเทคโนโลยีสารสนเทศ มหาวิทยาลัยเชียงใหม่
 239 ถ.ห้วยแก้ว ต.สุเทพ อ.เมือง จ.เชียงใหม่ 50200
 โทร.053-943807
 E-mail : itsc@cmu.ac.th

(ลงนาม)  ประธานกรรมการ
 (อาจารย์ ดร.ดำรงศักดิ์ นภารัตน์)

(ลงนาม)  กรรมการ
 (นายโอภาส หมิ่นแสน)

(ลงนาม)  กรรมการ
 (นายศุภวิทย์ วรรณภิละ)

(ลงนาม)  กรรมการ
 (นายสุริยา เชื้อนขัน)

(ลงนาม)  กรรมการ
 (นางสาวสุดถัย ไชยมงคล)

(ลงนาม)  เลขานุการ
 (นางสาวสุนิสา มะโนลี)

ภาคผนวก ก

คุณสมบัติเฉพาะของระบบบริหารจัดการเหตุการณ์และข้อมูลการรักษาความมั่นคงปลอดภัย
Security Information And Event Management (SIEM) จำนวน 1 ระบบ

จะต้องมีคุณสมบัติดังต่อไปนี้เป็นอย่างน้อย

1. โปรแกรมระบบ จำนวน 1 ระบบ

- 1.1. เป็นชุดของโปรแกรมสำเร็จ (Software suite หรือ Platform) เพื่อให้บริหารจัดการข้อมูลเหตุการณ์และข้อมูลด้านความปลอดภัย ซึ่งต้องประกอบด้วยส่วนย่อย ๆ อย่างน้อยดังนี้
 - 1.1.1 Log Management
 - 1.1.2 Next-Gen SIEM (ประกอบด้วย SIEM และ SOAR เป็นอย่างน้อย)
 - 1.1.3 Incident Management และ Incident Response
 - 1.1.4 Advanced Correlation
 - 1.1.5 GLBA, FISMA, GPG-13, PCI-DSS, GDPR, ISO Compliance Module
 - 1.1.6 BSI IT-Grundschutz Module, 201 CMR 17 Module, HIPPA Module, NERC-CIP Module, ASD Module, SOX Module, HiTech Module, Dodi 8500.2 Module, NRC Module, NEI Module, CCF Module, NIST CSF Module, Fraud Detection Module,
 - 1.1.7 Network Detection Response
- 1.2. สามารถเลือกการทำงานได้ทั้งแบบ Single Architecture ทุกฟังก์ชันทำงานร่วมกันภายในเครื่องเดียว หรือ Distributed Architecture ที่สามารถแยกส่วนการทำงาน Log Collector หรือ Log Management ออกมาจากส่วนประมวลผลข้อมูลและเหตุการณ์ภัยคุกคามด้านความมั่นคงปลอดภัยสารสนเทศ
- 1.3. สามารถรับข้อมูลและวิเคราะห์ข้อมูลได้ไม่น้อยกว่า 8,500 เหตุการณ์ต่อวินาที (Event per second) หรือรองรับข้อมูลรวมทุกระบบได้อย่างน้อย 5,000 GB ต่อวัน
- 1.4. สามารถรับเหตุการณ์จากอุปกรณ์เครือข่ายได้ไม่น้อยกว่า 100 อุปกรณ์
- 1.5. สามารถรับเหตุการณ์เครื่องแม่ข่าย ได้อย่างน้อย 400 เครื่อง
- 1.6. สามารถเฝ้าระวังและตรวจสอบความถูกต้องของไฟล์ข้อมูล (File Integrity Monitoring Data) ของเครื่องแม่ข่าย (Windows or Linux Server) ได้อย่างน้อย 400 เครื่อง หรือสามารถเสนออุปกรณ์อื่น ๆ ทำงานร่วมกัน เพื่อให้มีคุณสมบัติตามที่กำหนด โดยมีคุณสมบัติอย่างน้อยดังนี้
 - 1.6.1 บันทึกรายละเอียดกิจกรรมของ File หรือ Directory เช่น สร้าง (Created) และ ลบ (Deleted) ได้
 - 1.6.2 บันทึกรายละเอียดกิจกรรมของ File เช่น การแก้ไขเนื้อหา (Content modified), การแก้ไขชื่อไฟล์ (File Rename), การแก้ไขสิทธิ์ (Permission changed) และ การแก้ไขเจ้าของ (Ownership changed) เป็นต้น

- 1.7. สามารถเชื่อมโยงเหตุการณ์จาก Source ต่างๆ เข้าด้วยกัน (Correlation) แบบ Real-time เพื่อหาต้นตอของภัยคุกคาม โดยมี Predefined Rule มาพร้อมกับระบบไม่น้อยกว่า 80 Rules และสามารถ Customize เพิ่มเติมได้
- 1.8. สามารถเลือก บีบอัดและเข้ารหัสข้อมูล log ที่ส่งผ่านกันระหว่างตัวรับ log และตัวประมวลผล/จัดเก็บ log ได้
- 1.9. สามารถแจ้งเตือนได้หากแหล่งข้อมูล log หยุดส่ง log
- 1.10. สามารถเลือกรับ หรือ กรอง (Drop) ข้อมูล log จากตัวรับ log (Log collector) ได้ โดยไม่ต้องส่ง log เข้ามาที่ตัวประมวลผล/จัดเก็บ
- 1.11. มี Predefined Dashboard มาพร้อมกับระบบ เพื่อใช้สำหรับวิเคราะห์ข้อมูลเหตุการณ์แบบ Real-time ในรูปแบบของแผนภูมิ (Chart) และตาราง (Table) และสามารถ Customize เพิ่มเติมได้
- 1.12. รองรับการแบ่งแยกกลุ่มของปุมเหตุการณ์ (Event Log) ตามแผนก สาขา ในการใช้งานระบบใหญ่ ๆ ที่มีความซับซ้อน หรือสามารถแบ่งแยกปุมเหตุการณ์ (Event Log) ตามรายชื่อลูกค้าในกรณีที่ใช้งานในลักษณะของ MSSP (Management Security Service Provider) หรือ MSP (Managed Service Provider) เพื่อความสะดวกในการตรวจสอบข้อมูล
- 1.13. รองรับการบริหารจัดการรายละเอียดของอุปกรณ์หรือระบบต้นทางของ Log (Asset Management) เช่น ประเภทของอุปกรณ์ และสถานที่ตั้ง เป็นต้น
- 1.14. สามารถพิสูจน์ตัวตน (Authentication) ผู้ใช้งานได้ โดยรองรับฐานข้อมูลผู้ใช้แบบ Local, LDAP (Microsoft AD หรือ OpenLDAP หรือ Directory Server อื่นๆ) และ SAML ได้เป็นอย่างดี
- 1.15. ตัวจัดเก็บ log (Log Collector) มีความสามารถในการจัดเก็บ log อย่างน้อย ดังนี้
 - 1.15.1. UDP/TCP Syslog protocol
 - 1.15.2. SNMP
 - 1.15.3. Open Collector (File beat, ElasticSearch)
 - 1.15.4. Cisco SDEE
 - 1.15.5. Netflow, JFlow, SFlow
 - 1.15.6. LR Universal Database Log Adapter สำหรับ log ของระบบ และ custom logs (e.g., audit, application, etc.) ที่ถูกจัดเก็บไว้ในระบบ ฐานข้อมูล (database tables) (i.e. Oracle, SQL Server, MYSQL, etc.) ผ่าน (ODBC and OLE DB protocol)
 - 1.15.7. Checkpoint OPSEC/LEA - LogExporter
 - 1.15.8. Windows Event Logs (RPC) Windows Event Logs (local)
 - 1.15.9. NetApp CIFS
 - 1.15.10. eStreamer
 - 1.15.11. Metasploit
 - 1.15.12. Nexpose

- 1.15.13. Nessus
- 1.15.14. eEye Retina
- 1.15.15. Qualys
- 1.15.16. Tripwire
- 1.15.17. API
- 1.15.18. Palo Alto networks (PAN-OS)
- 1.15.19. BIND DNS
- 1.16. สามารถจัดเก็บและสืบค้นข้อมูลระยะยาวได้ทันที โดยไม่ต้องทำการ Restore จากระบบ Archive หรือ Storage
- 1.17. ระบบจัดเก็บข้อมูล log และเหตุการณ์ต้องสามารถบริหารจัดการพื้นที่จัดเก็บข้อมูลให้สอดคล้องกับอายุของข้อมูลได้ เช่น (Hot, cold, warm Storage) และสามารถใช้อินโฟร์เมชันข้อมูลแนวโน้มการใช้พื้นที่จัดเก็บข้อมูลในระยะยาวได้
- 1.18. สามารถใช้วิธี Drill down, pivoting และ Filtering เพื่อให้การวิเคราะห์สืบสวนเหตุการณ์เพื่อหาต้นตอภัยคุกคามทำได้เร็วขึ้น และสามารถแสดงผลการค้นข้อมูลขนาดใหญ่ได้ในหน้าจอเดียว
- 1.19. มีหน้าจอแสดงความสัมพันธ์ของข้อมูลแบบ Node-link Graph analysis หรือ Tree view หรือ Hub and Spoke view ที่สามารถแสดงความสัมพันธ์ (Correlation หรือ Visual Correlation) เพื่อวิเคราะห์สืบสวนเหตุการณ์ และเห็นภาพรวมของเหตุการณ์นั้นๆ รวมถึงการ trace down ได้
- 1.20. สามารถสร้างความสัมพันธ์ของเหตุการณ์หลายๆ เหตุการณ์ เพื่อใช้วิเคราะห์หาความสัมพันธ์ของเหตุการณ์ตามช่วงเวลา
- 1.21. สามารถ โดยรับข้อมูลผ่าน Logs, performance metrics, SNMP Traps, Security Alerts และ Configuration Change เพื่อแสดงผลการวิเคราะห์ข้อมูลได้ทั้งแบบ NOC (Network Operation Center) และ SOC (Security Operation Center)
- 1.22. สามารถบันทึกข้อมูลหรือเหตุการณ์ลงบน Local Storage และเลือกบันทึกไปยัง External Storage (NFS หรือ EventDB หรือ Clickhouse หรือ Elasticsearch) ได้
- 1.23. สามารถวิเคราะห์เปรียบเทียบข้อมูลระหว่างไอพีแอดเดรส กับรายชื่อผู้ใช้งานที่ใช้งานไอพีแอดเดรสนั้น ๆ อยู่ (Identity Mapping)
- 1.24. มีระบบบริหารจัดการเหตุการณ์ (Incident Management หรือ Case Management) ในตัว โดยไม่ต้องเสนอระบบเพิ่ม และสามารถทำงานร่วมกับ (Integrate) Third Party อื่นๆ ได้
- 1.25. ระบบบริหารจัดการเหตุการณ์ (Case Management) ต้องสามารถ Share Case ใดๆ ร่วมกับผู้ร่วมงานท่านอื่นได้ ซึ่งผู้ร่วมงานสามารถเพิ่มข้อมูล หลักฐาน (Forensic Evidence) และคำอธิบายประกอบ เพื่อช่วยให้ขบวนการตรวจจับและรับมือรวดเร็วขึ้น โดยกิจกรรมทั้งหมดทั้งหมดที่เกิดขึ้นต้องถูกบันทึกไว้เป็นส่วนหนึ่งของประวัติของเคส (Case History) และการบันทึกต้องมีการป้องกันการแก้ไข (Tamper-Proof audit trail) และสามารถ Update สถานะได้ทันที (Real-Time)

- 1.26. มี Predefined Report มาพร้อมกับระบบไม่น้อยกว่า 500 รูปแบบ และสามารถ Customize เพิ่มเติมได้
- 1.27. สามารถแจ้งเตือนแบบ Real-time เมื่อมีเหตุการณ์ตรงตามเงื่อนไขที่สร้างไว้ และ เหตุการณ์ผิดปกติของตัวอุปกรณ์ผ่าน Email ได้เป็นอย่างน้อย กรณีตรวจจับค่าต่าง ๆ แล้วมีค่าเกินกว่าที่กำหนด (threshold)
- 1.28. สามารถแสดงผลของเหตุการณ์ที่ถูกตรวจจับโดยแยกตามหมวดหมู่ของ MITRE ATT&CK ได้
- 1.29. สามารถทำการวิเคราะห์เปรียบเทียบข้อมูลระหว่าง IP address กับรายชื่อผู้ใช้งาน และทำการแสดงผลออกมาเป็นชื่อผู้ใช้งานรายนั้นได้ทันที
- 1.30. สามารถหาข้อมูลเกี่ยวกับเครื่องคอมพิวเตอร์ที่อยู่บน Internet เช่น Who is หรือ Ping ได้
- 1.31. มีระบบการจัดเก็บองค์ความรู้เพื่อให้คำแนะนำในการแก้ปัญหาต่าง ๆ และสามารถศึกษาย้อนหลังได้มี Predefined Report มาพร้อมกับระบบ และสามารถปรับแต่งเพิ่มเติมได้ โดยสามารถ Export รายงานในรูปแบบไฟล์ PDF, CSV, XML ได้เป็นอย่างน้อย
- 1.32. สามารถบริหารจัดการระบบผ่าน Web Interface ที่มีการเข้ารหัส เช่น HTTPS หรือสามารถบริหารจัดการผ่าน Software Console ได้
- 1.33. สามารถจัดทำรายงานแบบ Customized ได้ และรองรับการทำรายงานที่เกี่ยวข้องกับมาตรฐาน ISO27001, SAN หรือ SOX, NIST และอื่นๆ ไม่น้อยกว่า 5 รูปแบบมาตรฐาน
- 1.34. สามารถปิดบังข้อมูลบางส่วน เช่น User, Email, IP Address ด้วยวิธี Data Masking หรือ Data Obfuscation เพื่อป้องกันการละเมิดข้อมูลส่วนบุคคลได้
- 1.35. รองรับคุณสมบัติ UEBA เพื่อช่วยในการตรวจสอบพฤติกรรมของผู้ใช้ในระบบได้
- 1.36. สามารถตรวจจับเหตุการณ์ผิดปกติที่สอดคล้องกับสิ่งบ่งชี้ภัยคุกคาม (Indicator of Compromise: IoC) เทียบกับฐานข้อมูลของเจ้าของผลิตภัณฑ์ โดยประกอบด้วย Domain, IP, URL และ Hash เป็นอย่างน้อย
- 1.37. มีระบบ SOAR (Security Orchestration, Automation and Response) หรือ SAO (Security Automation & Orchestration) มาพร้อมกับตัวระบบด้วย สามารถใช้งานร่วมกับระบบทั้งหมดได้โดยไม่จำกัดและไม่คิด license เพิ่มเติม
- 1.38. ระบบ SOAR ต้องสามารถทำงานร่วมกันกับระบบ SIEM ที่นำเสนอในโครงการได้อย่างมีประสิทธิภาพ เพื่อให้สามารถทำงานร่วมกันได้โดยสมบูรณ์
- 1.39. ระบบ SOAR ต้องไม่จำกัดจำนวน SOC analysts หรือ playbook templates ที่จะนำมาใช้งานได้
- 1.40. ระบบ SOAR ต้องมีความสามารถอย่างน้อยดังนี้
 - 1.40.1. Disable AD user account
 - 1.40.2. Quarantine an infected machine
 - 1.40.3. Add IP to Firewall block list
 - 1.40.4. ชัดขวาง (Prevent) user จากการเรียกใช้ (Run) non-authorized process หรือ application
 - 1.40.5. บังคับ/ควบคุม service ให้ start, stop หรือ disabled

- 1.40.6. Add/Remove item to a watch list
- 1.40.7. Disable local user account
- 1.40.8. Enforce the user to be logged off from a machine
- 1.40.9. Extract the PCAP file and open the leaked attachment
- 1.40.10. Execute remote command
- 1.40.11. ลบ File
- 1.40.12. Take memory dump
- 1.41. ระบบ SOAR ต้องอนุญาตให้ผู้ใช้งาน (IR หรือ SOC Teams) เลือกทางเลือกในการสั่งการอย่างน้อยดังนี้
 - 1.41.1. Automatic Execution: สามารถทำงานตอบสนองแบบอัตโนมัติทั้งหมด เมื่อพบภัยคุกคามที่มีความเสี่ยงสูงที่เกิดขึ้นซ้ำ ๆ
 - 1.41.2. Approval-Based Execution: สามารถทำงานตอบสนองหลังจากได้รับอนุมัติให้ดำเนินการ โดยการอนุมัติสามารถตั้งให้เป็นการอนุมัติผู้เดียว หรือเป็นแบบ hierarchical chain
 - 1.41.3. Analyst-Triggered Execution: ทำงานตอบสนองเป็นครั้งๆ หลังจากได้รับคำสั่งให้ดำเนินการ จาก Web UI.
 - 1.41.4. Remote Execution: ควบคุมสั่งการระยะไกลจากศูนย์กลาง (Centralized manage)
- 1.42. ระบบ SOAR ต้องมีชุดคำสั่งปฏิบัติการสำเร็จรูป เพื่อช่วยลดเวลาการตอบสนองเหตุให้กับ IR/SOC Teams โดยมีอย่างน้อยดังนี้
 - 1.42.1. Endpoint Quarantine: Disable the port/device ของเครื่องที่ต้องสงสัย
 - 1.42.2. Suspend Users: ถ้ามี account ที่ต้องสงสัยว่าจะเป็น account ที่รั่วไหลหรือเป็นต้นเหตุ
 - 1.42.3. Collect Machine Data: เก็บรวบรวมข้อมูลภายในเครื่อง ใช้ในกรณีของ malware
 - 1.42.4. Suspend Network Access: ถ้าพบมีการรั่วไหลหรือโอนย้ายข้อมูล สามารถปิดการเชื่อมต่อ connection นั้นๆได้โดย update ใน ACL ของระบบที่เกี่ยวข้อง หรือวิธีการอื่นที่เทียบเท่า
 - 1.42.5. Kill Processes: ถ้าสามารถ Terminate process ที่นักวิเคราะห์พบว่า เป็น process ต้องห้าม หรือไม่รู้จักได้
- 1.43. ระบบ SOAR Playbook ต้องอนุญาตให้นักวิเคราะห์ (Analyst) สามารถสร้าง incident response procedure / Playbook เพิ่มขึ้นเองได้ และติดตามได้ผ่าน Web UI
- 1.44. สามารถทำงานร่วมกับ Endpoint Security Software เช่น Kaspersky, ESET หรืออื่นๆ เพื่อเพิ่มประสิทธิภาพในการค้นหา จัดทำรายงาน และแจ้งเตือน เมื่อติด Malware หรือมีเหตุการณ์ที่ผิดปกติได้
- 1.45. สามารถกำหนดค่า Triggers การแจ้งเตือน (Alarms) และสามารถทำ Filters ตามช่วงเวลาได้

- 1.46. สามารถวิเคราะห์ข้อมูลต่าง ๆ ได้ เช่น Remote Location, Conversation, Packet Flow, Node Detail, Protocols หรือ Sub-protocols เป็นต้น
- 1.47. มี Rules หรือ Classification สำหรับการวิเคราะห์เหตุการณ์สำเร็จรูปมาพร้อมกับระบบ
- 1.48. มี Use Cases สำเร็จรูปพร้อมใช้งานมาพร้อมกับระบบ ไม่น้อยกว่า 1,000 Use Cases และมี Report พร้อมใช้งานไม่น้อยกว่า 1250 Reports (คืออะไร)
- 1.49. ระบบต้องมี Metrics และ reports ด้าน Mean Time To Detect (MTTD) และ Mean Time To Respond (MTTR) เพื่อเป็นเครื่องมือวัด (KPI) ด้านประสิทธิภาพของทีมที่ปฏิบัติงานได้
- 1.50. มีระบบ AI หรือ Machine Learning หรือระบบที่ช่วยในการสร้าง Model สำหรับการวิเคราะห์ และสามารถนำไปใช้กับข้อมูลเหตุการณ์ เพื่อวิเคราะห์ถึงความเสี่ยงหรือทำนายผลลัพธ์ที่จะเกิดขึ้นในอนาคตของข้อมูลได้
- 1.51. สามารถแสดงผลในรูปแบบ Chart และ Performance Metric ได้เป็นอย่างดี
- 1.52. สามารถบริหารจัดการวิกฤตเหตุการณ์ (Incident War Room) เพื่อมอบหมาย ติดตามและจัดระเบียบการสืบสวน โดยทำงานร่วมกับเครื่องมือภายนอกเช่น MS Team, Slack หรือ Zoom ได้เป็นอย่างดี
- 1.53. มีการรับประกัน (Warranty) ระบบ เป็นระยะเวลาไม่น้อยกว่า 5 ปี
- 1.54. ระบบที่นำเสนอต้องอยู่ใน Gartner Magic Quadrant for SIEM (Security Information and Event Management) 2024 หรือใหม่กว่า

2. เครื่องแม่ข่ายประมวลผลและเก็บข้อมูล จำนวน 1 ชุด

- 2.1. มีหน่วยประมวลผลกลาง (CPU) ความเร็วพื้นฐาน 2.9 GHz 24 Core 60 MB Cache รองรับ DDR5-5200 เป็นอย่างน้อย จำนวน 2 หน่วย
- 2.2. หน่วยความจำ DDR5-5200 หรือดีกว่า ขนาดต่อชิ้นไม่น้อยกว่า 32GB ความจุรวมไม่น้อยกว่า 512GB
- 2.3. หน่วยบันทึกข้อมูลแบบ SSD ขนาดไม่น้อยกว่า 800GB จำนวน 2 หน่วย
- 2.4. หน่วยบันทึกข้อมูลแบบ NVMe ขนาดพื้นที่หลังทำ RAID 6 รวมไม่น้อยกว่า 40 TB พร้อม RAID Controller ที่มีหน่วยความจำไม่น้อยกว่า 8GB
- 2.5. ส่วนเชื่อมต่อเครือข่ายความเร็ว 10/25Gb Ethernet จำนวน 4 ช่อง มี interface แบบ OCP3.0 หรือดีกว่า พร้อมทั้ง Module เชื่อมต่อระบบเครือข่าย.....
- 2.6. ส่วนเชื่อมต่อเครือข่ายความเร็ว 1000BASE-T Ethernet จำนวน 2 ช่อง หรือดีกว่า
- 2.7. ภาคจ่ายไฟแบบ Redundant Power Supply และ Hot-Plug จำนวน 2 หน่วย
- 2.8. มีระบบบริหารจัดการเครื่องแม่ข่ายจากระยะไกล สามารถแสดงจอภาพ และ ควบคุม Keyboard/ Mouse จากระยะไกลได้ พร้อมช่องเชื่อมต่อเครือข่ายแบบ 1000BASE-T Ethernet และ Micro USB อย่างละ 1 ช่อง
- 2.9. รับประกันอย่างน้อย 5 ปี ให้บริการซ่อมถึงสถานที่ติดตั้ง ภายใน 24 ชั่วโมงหลังจากได้รับแจ้ง และตรวจสอบปัญหาเรียบร้อยแล้ว

3. เครื่องแม่ข่ายรวบรวมข้อมูล (Data Collector) จำนวน 2 ชุด

1. มีหน่วยประมวลผลกลาง (CPU) ความเร็วพื้นฐาน 3.2 GHz 8 Core 12 MB Cache รองรับ DDR5-4800 เป็นอย่างน้อย จำนวน 1 หน่วย
2. หน่วยความจำ DDR5-4800 หรือดีกว่า ขนาดต่อชิ้นไม่น้อยกว่า 16GB ความจุรวมไม่น้อยกว่า 32GB
3. หน่วยบันทึกข้อมูลแบบ SSD ขนาดไม่น้อยกว่า 800GB จำนวน 2 หน่วย
4. ส่วนเชื่อมต่อเครือข่ายความเร็ว 10Gb Ethernet จำนวน 2 ช่อง พร้อมทั้ง Module เชื่อมต่อระบบเครือข่าย
5. ส่วนเชื่อมต่อเครือข่ายความเร็ว 1000BASE-T Ethernet จำนวน 2 ช่อง หรือดีกว่า
6. ภาคจ่ายไฟแบบ Redundant Power Supply และ Hot-Plug จำนวน 2 หน่วย
7. มีระบบบริหารจัดการเครื่องแม่ข่ายจากระยะไกล สามารถแสดงจอภาพ และ ควบคุม Keyboard/ Mouse จากระยะไกลได้ พร้อมช่องเชื่อมต่อเครือข่ายแบบ 1000BASE-T Ethernet และ Micro USB อย่างละ 1 ช่อง
8. รับประกันอย่างน้อย 5 ปี ให้บริการซ่อมถึงสถานที่ติดตั้ง ภายใน 24 ชั่วโมงหลังจากได้รับแจ้งและตรวจสอบปัญหาเรียบร้อยแล้ว

4. อุปกรณ์แปลงสัญญาณเครือข่ายแบบ SFP+ Module จำนวน 8 ชุด

1. เป็นชนิด 10 GBASE-LR
2. มีหัวเชื่อมต่อ (Connector Type) แบบ LC
3. อุปกรณ์ SFP+ สามารถใช้กับสายแบบ Fiber Optic ชนิด Single Mode
4. รองรับมาตรฐาน IEEE802.3z
5. สามารถใช้ร่วมกับเครื่องแม่ข่ายที่นำเสนอทั้งหมดได้
6. สามารถใช้ร่วมกับอุปกรณ์เครือข่ายหลักของมหาวิทยาลัยที่ต้องเชื่อมต่อไปยังเครื่องแม่ข่ายที่นำเสนอได้