การพิจารณาคณะกรรมการกำหนดร่างขอบเขตของงาน (Terms of Reference : TOR)
สำหรับโครงการจัดหาระบบจัดเก็บข้อมูลจราจรคอมพิวเตอร์และวิเคราะห์ภัยคุกคามบนเครือข่ายแบบรวมศูนย์
(Security Incident Event Management: SIEM)
ต่อข้อเสนอแนะ วิจารณ์ หลังการประชาพิจารณ์ ครั้งที่ 1 (ระหว่างวันที่ 26 มกราคม 2565 – 3 กุมภาพันธ์ 2565)

คุณลักษณะเฉพาะที่กำหนด ในเอกสาร TOR สำหรับประชาพิจารณ์ครั้งที่ 1	ข้อเสนอแนะ วิจารณ์ จากบริษัท บริษัท เบย์ คอมพิวติ้ง จำกัด	ความเห็นของคณะกรรมการฯ
5.1 อุปกรณ์วิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์ (Security Incident Event Management: SIEM)		
5.1.2 ต้องสามารถรองรับการส่งข้อมูลเหตุการณ์ได้สูงสุด 7,000 เหตุการณ์ต่อวินาที (Event Per Second) เป็นอย่างน้อย และรองรับการขยายเพิ่มเติมได้สูงสุดไม่น้อยกว่า 40,000 เหตุการณ์ต่อวินาที (Event Per Second)	5.1.2 ต้องสามารถรองรับการส่งข้อมูลเหตุการณ์ได้สูงสุด 7,000 เหตุการณ์ต่อวินาที (Event Per Second) เป็นอย่างน้อย ~~และรองรับการขยายเพิ่มเติมได้สูงสุดไม่น้อยกว่า 40,000 เหตุการณ์ต่อวินาที (Event Per Second)~~	ปรับแก้ไข เป็น 5.1.2 ต้องสามารถรองรับการส่งข้อมูลเหตุการณ์ได้สูงสุด 7,000 เหตุการณ์ต่อวินาที (Event Per Second) เป็นอย่างน้อย เหตุผล เพื่อให้เปิดกว้างในการแข่งขัน
5.1.5 ระบบต้องรองรับ log formats ในรูปแบบ Syslog, Syslog TLS, SNMP, NetFlow, OPSEC, JDBC, WMI ได้เป็นอย่างน้อย	5.1.5 รบบต้องรองรับ Log Format ในรูปแบบ Syslog, Syslog TLS, SNMP, NetFlow, OPSEC หรือ JDBC, WMI ได้เป็นอย่างน้อย	ปรับแก้ไข เป็น ระบบต้องรองรับ Log Format ในรูปแบบ Syslog, Syslog TLS, SNMP, NetFlow, OPSEC ได้เป็นอย่างน้อย

คุณลักษณะเฉพาะที่กำหนด ในเอกสาร TOR สำหรับประชาพิจารณ์ครั้งที่ 1	ข้อเสนอแนะ วิจารณ์ จากบริษัท บริษัท เบย์ คอมพิวติ้ง จำกัด	ความเห็นของคณะกรรมการฯ
		<u>เหตุผล</u> เพื่อให้เปิดกว้างในการแข่งขัน และให้เป็นไปตามคุณสมบัติเฉพาะที่ได้ผ่านการพิจารณาของคณะกรรมการคอมพิวเตอร์กระทรวงการคลังแล้ว
5.1.9 มีความสามารถในการสร้างความสัมพันธ์ (Correlation) ของข้อมูลเหตุการณ์ (Event) ได้เป็นอย่างน้อย และมี Pre - defined มาพร้อมกับระบบ 1,000 Correlation Rules เป็นอย่างน้อย	5.1.9 มีความสามารถในการสร้างความสัมพันธ์ (Correlation) ของข้อมูลเหตุการณ์ (Event) ได้เป็นอย่างน้อย <u>และมี Pre - defined มาพร้อมกับระบบ 100 Correlation Rules เป็นอย่างน้อย และ สามารถสร้าง Correlation Rules ได้ไม่จำกัด</u>	<u>ปรับแก้ไข เป็น</u> มีความสามารถในการสร้างความสัมพันธ์ (Correlation) ของข้อมูลเหตุการณ์ (Event) ได้เป็นอย่างน้อย และมี Pre - defined มาพร้อมกับระบบ 100 Correlation Rules เป็นอย่างน้อย และ สามารถสร้าง Correlation Rules ได้ไม่จำกัด <u>เหตุผล</u> เพื่อให้เปิดกว้างในการแข่งขัน
5.1.15 มีความสามารถในการสร้างรายงานสำหรับ compliance ดังต่อไปนี้ ISO, PCI-DSS, FISMA, HIPPA, NERC-CIP, SOX, GLBA, NIST, SANS, ITIL	5.1.15 มีความสามารถ ในการสร้างรายงานสำหรับ compliance ดังต่อไปนี้ ISO, PCI-DSS, FISMA, HIPPA, NERC-CIP, SOX, GLBA <u>หรือ</u> NIST, SANS, ITIL	<u>ปรับแก้ไข เป็น</u> มีความสามารถ ในการสร้างรายงานสำหรับ compliance ดังต่อไปนี้ ISO, PCI-DSS, FISMA, HIPPA, NERC-CIP, SOX, GLBA

คุณลักษณะเฉพาะที่กำหนด ในเอกสาร TOR สำหรับประชาพิจารณ์ครั้งที่ 1	ข้อเสนอแนะ วิจารณ์ จากบริษัท บริษัท เบย์ คอมพิวติ้ง จำกัด	ความเห็นของคณะกรรมการฯ
		เหตุผล เพื่อให้เปิดกว้างในการแข่งขัน และให้เป็นไปตามคุณสมบัติเฉพาะที่ได้ผ่านการพิจารณาของคณะกรรมการคอมพิวเตอร์กระทรวงการคลังแล้ว
5.1.23 สามารถเฝ้าระวังการเปลี่ยนแปลง Files, Folder, Windows Registry ได้เป็นอย่างน้อย	ข้อให้ตัดคุณสมบัติข้อนี้ เนื่องจากไม่ได้เป็นคุณสมบัติของระบบ “SIEM”	ตัดทิ้ง เหตุผล เพื่อให้เปิดกว้างในการแข่งขัน
5.1.24 สามารถปกปิดข้อมูล เช่น User, Email, IP Address ด้วยวิธี Data Masking หรือ Data Obfuscation เพื่อป้องกันการละเมิดข้อมูลส่วนบุคคลได้	ข้อให้ตัดคุณสมบัติข้อนี้ เนื่องจากไม่ได้เป็นคุณสมบัติของระบบ “SIEM”	ตัดทิ้ง เหตุผล เพื่อให้เปิดกว้างในการแข่งขัน
5.1.25 สามารถพิสูจน์ตัวตน (Authentication) ผู้ใช้งานได้ โดยรองรับฐานข้อมูลผู้ใช้แบบ Local, Microsoft AD, OpenLDAP, RADIUS และ SAML ได้เป็นอย่างน้อย	5.1.25 สามารถพิสูจน์ตัวตน (Authentication) ผู้ใช้งานได้ โดยรองรับฐานข้อมูลผู้ใช้แบบ Local, Microsoft AD หรือ OpenLDAP, RADIUS และ SAML ได้เป็นอย่างน้อย	ปรับแก้ไข เป็น สามารถพิสูจน์ตัวตน (Authentication) ผู้ใช้งานได้ โดยรองรับฐานข้อมูลผู้ใช้แบบ Local, Microsoft AD ได้เป็นอย่างน้อย เหตุผล เพื่อให้เปิดกว้างในการแข่งขัน

คุณลักษณะเฉพาะที่กำหนด ในเอกสาร TOR สำหรับประชาพิจารณ์ครั้งที่ 1	ข้อเสนอแนะ วิจารณ์ จากบริษัท บริษัท เบย์ คอมพิวติ้ง จำกัด	ความเห็นของคณะกรรมการฯ
5.2 ระบบบริหารจัดการและตอบสนองต่อเหตุการณ์ภัยคุกคามทางคอมพิวเตอร์ (Security Orchestration, Automation and Response: SOAR)		
5.2.3 รองรับการทำงานแบบ Multi - tenancy ในลักษณะ Distributed Deployment และ Share Deployment ได้ โดยสามารถกำหนดการทำงานแบบอัตโนมัติ (Automation Workflow) ระบุแบ่งตาม Tenant ได้	5.2.3 รองรับการทำงานแบบ Multi - tenancy ~~ในลักษณะ Distributed Deployment และ Share Deployment~~ ได้โดยสามารถกำหนดการทำงานแบบอัตโนมัติ (Automation Workflow) ระบุแบ่งตาม Tenant ได้	ปรับแก้ไข เป็น รองรับการทำงานแบบ Multi – tenancy ได้โดยสามารถกำหนดการทำงานแบบอัตโนมัติ (Automation Workflow) ระบุแบ่งตาม Tenant ได้ เหตุผล เพื่อให้เปิดกว้างในการแข่งขัน
5.2.22 อุปกรณ์ที่เสนอต้องมีเครื่องหมายการค้าหรือผู้ผลิตหรือเจ้าของผลิตภัณฑ์เดียวกันกับอุปกรณ์วิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์ (Security Incident Event Management: SIEM) ที่เสนอในการจัดซื้อครั้งนี้	บริษัทฯ ไม่สามารถเข้าร่วมยื่นข้อเสนอได้	ปรับแก้ไข เป็น อุปกรณ์ที่เสนอต้องสามารถทำงานร่วมกับอุปกรณ์วิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์ (Security Incident Event Management: SIEM) ที่เสนอในการจัดซื้อครั้งนี้ เหตุผล เพื่อให้เปิดกว้างในการแข่งขันและความเหมาะสมกับการใช้งาน