การพิจารณาคณะกรรมการกำหนดร่างขอบเขตของงาน (Terms of Reference : TOR)
สำหรับโครงการจัดหาระบบจัดเก็บข้อมูลจราจรคอมพิวเตอร์และวิเคราะห์ภัยคุกคามบนเครือข่ายแบบรวมศูนย์
(Security Incident Event Management: SIEM)
ต่อข้อเสนอแนะ วิจารณ์ หลังการประชาพิจารณ์ ครั้งที่ 2 (ระหว่างวันที่ 17 กุมภาพันธ์ 2565 – 24 กุมภาพันธ์ 2565)

คุณลักษณะเฉพาะที่กำหนด ในเอกสาร TOR สำหรับประชาพิจารณ์ครั้งที่ 2	**ข้อเสนอแนะ วิจารณ์ จากบริษัท** **บริษัท เบย์ คอมพิวติ้ง จำกัด**	**ความเห็นของคณะกรรมการฯ**
5.2 ระบบบริหารจัดการและตอบสนองต่อเหตุการณ์ภัยคุกคามทางคอมพิวเตอร์ (Security Orchestration, Automation and Response: SOAR)		
5.2.5 สามารถทำการกำหนดสิทธิ์ผู้ใช้งานในการเข้าถึงข้อมูล (Role-Based Access Management) เช่น Rules, Playbooks, Attachment และ Report ได้ และสามารถกำหนดสิทธิ์การ Create, Read, Update และ Delete ให้กับผู้ใช้งานระบบได้	5.2.5 สามารถทำการกำหนดสิทธิ์ผู้ใช้งานในการเข้าถึงข้อมูล (Role-Based Access Management) เช่น Rules, Playbooks, Attachment และ Report ได้ และสามารถกำหนดสิทธิ์การ Create, Read, Update “หรือ Modify” และ Delete ให้กับผู้ใช้งานระบบได้ <u>เหตุผล</u> เพื่อเป็นการเปิดกว้างในการแข่งขัน และไม่เป็นเอื้อประโยชน์แก่ผลิตภัณฑ์รายใดรายหนึ่ง	<u>ปรับแก้ไข เป็น</u> 5.2.5 สามารถทำการกำหนดสิทธิ์ผู้ใช้งานในการเข้าถึงข้อมูล (Role-Based Access Management) เช่น Rules, Playbooks, Attachment และ Report ได้ และสามารถกำหนดสิทธิ์การ Create, Read, Update หรือ Modify และ Delete ให้กับผู้ใช้งานระบบได้ <u>เหตุผล</u> เพื่อให้เปิดกว้างทางการแข่งขันและความเหมาะสมกับการใช้งาน

คุณลักษณะเฉพาะที่กำหนด ในเอกสาร TOR สำหรับประชาพิจารณ์ครั้งที่ 2	ข้อเสนอแนะ วิจารณ์ จากบริษัท บริษัท เบย์ คอมพิวติ้ง จำกัด	ความเห็นของคณะกรรมการฯ
5.2.6 สามารถกำหนดความสัมพันธ์ภายในกลุ่มของผู้ดูแลระบบ (Team Hierarchy) ในรูปแบบ Parent, Sibling และ Child ได้เป็นอย่างน้อย	ขอให้ตัดคุณสมบัติข้อนี้ <u>เหตุผล</u> เพราะผลิตภัณฑ์ที่บริษัทนำเสนอไม่สามารถยื่นข้อเสนอเข้าร่วมแข่งขันได้	ตัดทิ้ง <u>เหตุผล</u> เพื่อให้เปิดกว้างทางการแข่งขัน
5.2.18 สามารถรับข้อมูลจากรูปแบบ PDF เพื่อนำไปสร้างเป็น Indicator ให้กับระบบได้	ขอให้ตัดคุณสมบัติข้อนี้ <u>เหตุผล</u> เพราะผลิตภัณฑ์ที่บริษัทนำเสนอไม่สามารถยื่นข้อเสนอเข้าร่วมแข่งขันได้	ตัดทิ้ง <u>เหตุผล</u> เพื่อให้เปิดกว้างทางการแข่งขัน
5.2.19 ระบบสามารถรับข้อมูลจาก Indicator of Compromise (IOCs) จากแหล่งที่มีความน่าเชื่อถือและได้รับการสนับสนุนจากหน่วยงาน Cyber Threat Alliance, ICSA Labs, NSS Labs, NASA, NATO, Common Criteria และ Mitre เป็นอย่างน้อย	ขอให้ตัดคุณสมบัติข้อนี้ <u>เหตุผล</u> เพราะผลิตภัณฑ์ที่บริษัทนำเสนอไม่สามารถยื่นข้อเสนอเข้าร่วมแข่งขันได้	ตัดทิ้ง <u>เหตุผล</u> เพื่อให้เปิดกว้างทางการแข่งขัน

คุณลักษณะเฉพาะที่กำหนด ในเอกสาร TOR สำหรับประชาพิจารณ์ครั้งที่ 2	ข้อเสนอแนะ วิจารณ์ จากบริษัท บริษัท เบย์ คอมพิวติ้ง จำกัด	ความเห็นของคณะกรรมการฯ
5.3 ซอฟต์แวร์ตรวจจับและตอบสนองต่อภัยคุกคามทางไซเบอร์ (Endpoint Detection and Response: EDR)		
5.3.2 สามารถติดตั้งได้ทั้งแบบ On Cloud และ On Premise	5.3.2 สามารถติดตั้งได้ทั้งแบบ On Premise <u>เหตุผล</u> เพราะผลิตภัณฑ์ที่บริษัทนำเสนอไม่สามารถยื่นข้อเสนอเข้าร่วมแข่งขันได้	<u>ปรับแก้ไข เป็น</u> 5.3.2 สามารถติดตั้งได้ทั้งแบบ On Cloud หรือ On Premise <u>เหตุผล</u> เพื่อให้เกิดการแข่งขัน
5.3.3 รองรับการติดตั้งบนระบบปฏิบัติการต่างๆ ได้อย่างน้อยดังนี้ 1) Windows XP, 7, 8 และ 10 2) Windows Server 2003, 2008, 2012, 2016 และ 2019 3) MacOS 4) VMware Horizon 5) Red Hat Enterprise 6) CentOS 7) Ubuntu 8) Oracle	5.3.3 สามารถติดตั้งซอฟต์แวร์ Agent บนระบบปฏิบัติการ (Endpoint Operating System) ได้อย่างน้อยดังนี้ 2.1. Windows Client and Server ได้แก่ XP SP3, 7, 8.1, 10, 2003 SP2, 2008, 2008R2, 2012 และ 2016 2.2. Linux Server ได้แก่ CentOS, Ubuntu, Red Hat, Debian และ SuSE <u>เหตุผล</u> เพื่อเป็นการเปิดกว้างในการแข่งขัน และไม่เป็นเอื้อประโยชน์แก่ผลิตภัณฑ์รายใดรายหนึ่ง	<u>ปรับแก้ไข เป็น</u> 5.3.3 รองรับการติดตั้งบนระบบปฏิบัติการต่างๆ ได้อย่างน้อยดังนี้ 1) Windows XP, 7, 8 และ 10 2) Windows Server 2003, 2008, 2012, 2016 และ 2019 3) MacOS 4) Red Hat Enterprise 5) CentOS 6) Ubuntu 7) Oracle

คุณลักษณะเฉพาะที่กำหนด ในเอกสาร TOR สำหรับประชาพิจารณ์ครั้งที่ 2	ข้อเสนอแนะ วิจารณ์ จากบริษัท บริษัท เบย์ คอมพิวติ้ง จำกัด	ความเห็นของคณะกรรมการฯ
		<u>เหตุผล</u> เพื่อให้เปิดกว้างทางการแข่งขันและความเหมาะสมกับการใช้งาน
5.3.4 สามารถทำ Virtual Patch ได้	ขอให้ตัดคุณสมบัติข้อนี้ <u>เหตุผล</u> เพราะผลิตภัณฑ์ที่บริษัทนำเสนอไม่สามารถยื่นข้อเสนอเข้าร่วมแข่งขันได้	<u>ไม่ปรับแก้ไข</u> <u>เหตุผล</u> เนื่องจากคุณลักษณะที่กำหนดไว้มีความจำเป็นต่อการใช้งานในปัจจุบัน
5.3.5 สามารถตรวจสอบ Application ที่ใช้งานภายในองค์กร และรายการช่องโหว่ตาม Common Vulnerability Scoring System (CVSS) ได้	5.3.5 สามารถตรวจสอบ Application ที่ใช้งานภายในองค์กร และรายการช่องโหว่ตาม Common Vulnerability Scoring System (CVSS) ได้ หรือ มีวิธีในการป้องกันและตอบสนองต่อภัยคุกคามทางด้านไซเบอร์ได้อย่างน้อยดังนี้ Scheduled Scan, Realtime Protection, Ransomware, WebShell, Brut-Force และ Advanced Threat Defense	<u>ปรับแก้ไข เป็น</u> 5.3.5 สามารถตรวจสอบ Application ที่ใช้งานภายในองค์กร และรายการช่องโหว่ตาม Common Vulnerability Scoring System (CVSS) ได้ หรือ มีวิธีในการป้องกันและตอบสนองต่อภัยคุกคามทางด้านไซเบอร์ได้อย่างน้อยดังนี้ Scheduled Scan, Realtime Protection, Ransomware, WebShell, Brut-Force และ Advanced Threat Defense <u>เหตุผล</u> เพื่อเป็นการเปิดกว้างในการแข่งขัน

คุณลักษณะเฉพาะที่กำหนด ในเอกสาร TOR สำหรับประชาพิจารณ์ครั้งที่ 2	ข้อเสนอแนะ วิจารณ์ จากบริษัท บริษัท เบย์ คอมพิวติ้ง จำกัด	ความเห็นของคณะกรรมการฯ
5.3.6 สามารถป้องกันมัลแวร์ (Malware) ด้วย Machine Learning ได้ โดยไม่ต้องติดตั้ง Agent	5.3.6 สามารถป้องกันมัลแวร์ (Malware) ด้วย Machine Learning ได้ โดยไม่ต้องติดตั้ง Agent หรือ มีระบบวิเคราะห์และตรวจจับ (Security Engines) เพื่อเพิ่มประสิทธิภาพในการป้องกันอย่างน้อยดังนี้ AI based engine, Cloud based engine, Gene engine และ Behavioral engine	ปรับแก้ไข เป็น 5.3.6 สามารถป้องกันมัลแวร์ (Malware) ด้วย Machine Learning ได้ โดยไม่ต้องติดตั้ง Agent หรือ มีระบบวิเคราะห์และตรวจจับ (Security Engines) เพื่อเพิ่มประสิทธิภาพในการป้องกันอย่างน้อยดังนี้ AI based engine, Cloud based engine, Gene engine และ Behavioral engine เหตุผล เพื่อเป็นการเปิดกว้างในการแข่งขัน
5.3.7 สามารถป้องกัน Endpoint ได้ แม้อยู่ในสถานะออฟไลน์ (Offline)	5.3.7 สามารถป้องกัน Endpoint ได้ แม้อยู่ในสถานะออฟไลน์ (Offline) หรือ มีความสามารถในการควบคุมหรือกำหนดการติดต่อสื่อสารระหว่างเครื่องคอมพิวเตอร์ (Micro-segmentation)	ไม่ปรับแก้ไข เหตุผล เนื่องจากคุณลักษณะที่กำหนดไว้มีความจำเป็นต่อการใช้งานในปัจจุบัน

คุณลักษณะเฉพาะที่กำหนด ในเอกสาร TOR สำหรับประชาพิจารณ์ครั้งที่ 2	ข้อเสนอแนะ วิจารณ์ จากบริษัท บริษัท เบย์ คอมพิวติ้ง จำกัด	ความเห็นของคณะกรรมการฯ
5.3.8 สามารถแสดงภาพกราฟตามลำดับขั้นตอนของเหตุการณ์ที่เกิดขึ้นได้	5.3.8 สามารถแสดงภาพกราฟตามลำดับขั้นตอนของเหตุการณ์ที่เกิดขึ้นได้ หรือ มีความสามารถในการค้นหาไฟล์ต้องสงสัยที่อาจจะมีอยู่ในเครื่องคอมพิวเตอร์ (Infected File Tracking)	ปรับแก้ไข เป็น 5.3.8 สามารถแสดงภาพกราฟตามลำดับขั้นตอนของเหตุการณ์ที่เกิดขึ้นได้ หรือ มีความสามารถในการค้นหาไฟล์ต้องสงสัยที่อาจจะมีอยู่ในเครื่องคอมพิวเตอร์ (Infected File Tracking) เหตุผล เพื่อเป็นการเปิดกว้างในการแข่งขัน
5.3.9 สามารถทำ Threat Hunting จาก Hash และ File name โดยกำหนดช่วงเวลาที่ต้องการค้นหาได้	5.3.9 สามารถทำ Threat Hunting จาก Hash และ File name โดยกำหนดช่วงเวลาที่ต้องการค้นหาได้ หรือ มีความสามารถในการแยกเครื่องคอมพิวเตอร์ที่มีความเสี่ยงออกมาจากระบบเครือข่าย (Endpoint Isolation)	ปรับแก้ไข เป็น 5.3.9 สามารถทำ Threat Hunting จาก Hash และ File name โดยกำหนดช่วงเวลาที่ต้องการค้นหาได้ หรือ มีความสามารถในการแยกเครื่องคอมพิวเตอร์ที่มีความเสี่ยงออกมาจากระบบเครือข่าย (Endpoint Isolation) เหตุผล เพื่อเป็นการเปิดกว้างในการแข่งขัน

คุณลักษณะเฉพาะที่กำหนด ในเอกสาร TOR สำหรับประชาพิจารณ์ครั้งที่ 2	ข้อเสนอแนะ วิจารณ์ จากบริษัท บริษัท เบย์ คอมพิวติ้ง จำกัด	ความเห็นของคณะกรรมการฯ
5.3.10 สามารถควบคุมการใช้งานอุปกรณ์ USB ได้	5.3.10 สามารถควบคุมการใช้งานอุปกรณ์ USB ได้ หรือ มีความสามารถในการตรวจสอบความปลอดภัยขั้นพื้นฐานของเครื่องคอมพิวเตอร์ (Security & Integrity Check)	ไม่ปรับแก้ไข เหตุผล เนื่องจากคุณลักษณะที่กำหนดไว้มีความจำเป็นต่อการใช้งานในปัจจุบัน
5.3.11 สามารถป้องกันการเข้าถึงเว็บไซต์ (Website) ที่ไม่ปลอดภัยได้	5.3.11 สามารถป้องกันการเข้าถึงเว็บไซต์ (Website) ที่ไม่ปลอดภัยได้ หรือ มีความสามารถในการสแกนช่องโหว่ (Vulnerability Scan) และการอุดช่องโหว่ (Endpoint Patching)	ไม่ปรับแก้ไข เหตุผล เนื่องจากคุณลักษณะที่กำหนดไว้มีความจำเป็นต่อการใช้งานในปัจจุบัน
5.3.12 สามารถทำงานร่วมกับ Windows Security Center ได้	5.3.12 สามารถทำงานร่วมกับ Windows Security Center ได้ หรือ มีความสามารถในการแสดงบัญชีรายการของเครื่องคอมพิวเตอร์ (Inventory) อย่างน้อยดังนี้ Operating system, Applications, CPU, Memory, Disk, Motherboard, Network Adapter, Sound Card และ Graphics Card	ไม่ปรับแก้ไข เหตุผล เนื่องจากคุณลักษณะที่กำหนดไว้มีความจำเป็นต่อการใช้งานในปัจจุบัน

คุณลักษณะเฉพาะที่กำหนด ในเอกสาร TOR สำหรับประชาพิจารณ์ครั้งที่ 2	ข้อเสนอแนะ วิจารณ์ จากบริษัท บริษัท เบย์ คอมพิวติ้ง จำกัด	ความเห็นของคณะกรรมการฯ
5.3.13 สามารถแสดงผลภัยคุกคามตาม MITRE Attack Framework ได้	5.3.13 สามารถแสดงผลภัยคุกคามตาม MITRE Attack Framework ได้ หรือ มีความสามารถในการควบคุมการใช้งานอุปกรณ์ต่อพ่วง (Device Control หรือ Peripheral Control)	ตัดทิ้ง เหตุผล เพื่อเป็นการเปิดกว้างในการแข่งขัน และเป็นคุณสมบัติที่มีอยู่ในอุปกรณ์ NDR ข้อ 5.4.5 (2)
5.3.14 สามารถกำหนดเงื่อนไขในการแก้ไขปัญหาเมื่อตรวจพบมัลแวร์ (Malware) ได้อย่างน้อยดังนี้ 1) Terminate Process 2) Delete File 3) Clean Persistent Data 4) Block Address on Firewall	5.3.14 สามารถกำหนดเงื่อนไขในการแก้ไขปัญหาเมื่อตรวจพบมัลแวร์ (Malware) ได้อย่างน้อยดังนี้ 1) Terminate Process 2) Delete File 3) Clean Persistent Data 4) Block Address on Firewall หรือ มีระบบบริหารจัดกลางจากส่วนกลาง (Centralized Management) โดยระบบ มีความสามารถอย่างน้อยดังนี้ – เป็นระบบที่มีการทำงานแบบ On-Premise และสามารถเข้าบริหารจัดการระบบผ่าน WEB UI	ไม่ปรับแก้ไข เหตุผล เนื่องจากคุณลักษณะที่กำหนดไว้มีความจำเป็นต่อการใช้งานในปัจจุบัน

คุณลักษณะเฉพาะที่กำหนด ในเอกสาร TOR สำหรับประชาพิจารณ์ครั้งที่ 2	ข้อเสนอแนะ วิจารณ์ จากบริษัท บริษัท เบย์ คอมพิวติ้ง จำกัด	ความเห็นของคณะกรรมการฯ
	– สามารถ Enable, Disable, Restart และ Uninstall ซอฟต์แวร์ Agent จากส่วนกลางได้ – สามารถแสดงข้อมูลและรายละเอียดของเครื่องคอมพิวเตอร์ซึ่งประกอบด้วย Hostname, Endpoint Status Online/Offline, IP Address, MAC Address, OS Version, CPU Usage และ Memory Usage – มีหน้าจอ Dashboard สำหรับแสดงภาพรวมการตรวจจับภัยคุกคามหรือเหตุการณ์ทางด้านไซเบอร์ที่เกิดขึ้น – สามารถออกรายงาน Security Report ในรูปแบบของ PDF และสามารถตั้งค่า Schedule Report ได้แบบ Daily, Weekly และ Monthly โดยสามารถส่งผ่าน Email ได้เป็นอย่างน้อย	

คุณลักษณะเฉพาะที่กำหนด ในเอกสาร TOR สำหรับประชาพิจารณ์ครั้งที่ 2	ข้อเสนอแนะ วิจารณ์ จากบริษัท บริษัท เบย์ คอมพิวติ้ง จำกัด	ความเห็นของคณะกรรมการฯ
5.3.15 สามารถอัพเดท Threat Intelligence จากฐานข้อมูลของเจ้าของผลิตภัณฑ์ที่เสนอได้อย่างต่อเนื่องตลอดอายุสัญญา	5.3.15 สามารถอัพเดท Threat Intelligence จากฐานข้อมูลของเจ้าของผลิตภัณฑ์ที่เสนอได้อย่างต่อเนื่องตลอดอายุสัญญา หรือ สามารถทำงานร่วมกับ ระบบตรวจจับและตอบสนองต่อ ระบบเครือข่ายคอมพิวเตอร์ (Network Detection and Response) ที่นำเสนอในโครงการได้	ไม่ปรับแก้ไข เหตุผล เนื่องจากคุณลักษณะที่กำหนดไว้มีความจำเป็นต่อการใช้งานในปัจจุบัน
5.3.16 สามารถพิสูจน์ตัวตน (Authentication) ผู้ใช้งานได้ โดยรองรับฐานข้อมูลผู้ใช้แบบ Local, LDAP, SAML ได้	5.3.16 สามารถพิสูจน์ตัวตน (Authentication) ผู้ใช้งานได้ โดยรองรับฐานข้อมูลผู้ใช้แบบ Local, LDAP, SAML ได้ หรือ ผู้ขายต้องเสนอเครื่องแม่ข่ายสำหรับใช้ในการติดตั้งระบบบริหารจัดกลางจากส่วนกลาง (Centralized Management) ตามข้อกำหนดของโครงการ	ตัดทิ้ง เหตุผล ไม่ใช่คุณสมบัติหลักของอุปกรณ์ EDR และ สศค ได้มีระบบการ Authentication อยู่แล้ว จะทำให้เกิดความซ้ำซ้อนกับระบบเดิม
5.3.17 รองรับการทำงานแบบ Two Factor Authentication	ขอให้ตัดคุณสมบัติข้อนี้ เหตุผล เพราะผลิตภัณฑ์ที่บริษัทนำเสนอไม่สามารถยื่นข้อเสนอเข้าร่วมแข่งขันได้	ตัดทิ้ง เหตุผล เพื่อเป็นการเปิดกว้างในการแข่งขัน

คุณลักษณะเฉพาะที่กำหนด ในเอกสาร TOR สำหรับประชาพิจารณ์ครั้งที่ 2	ข้อเสนอแนะ วิจารณ์ จากบริษัท บริษัท เบย์ คอมพิวติ้ง จำกัด	ความเห็นของคณะกรรมการฯ
5.3.18 รองรับการทำงานร่วมกับระบบความปลอดภัยอื่นๆ (Connector) เช่น Firewall และ Sandbox	ขอให้ตัดคุณสมบัติข้อนี้ เหตุผล เพราะผลิตภัณฑ์ที่บริษัทนำเสนอไม่สามารถยื่นข้อเสนอเข้าร่วมแข่งขันได้	ตัดทิ้ง เหตุผล เพื่อเป็นการเปิดกว้างในการแข่งขัน
5.3.19 สามารถกำหนด Action ได้อัตโนมัติผ่าน Playbook Policy	ขอให้ตัดคุณสมบัติข้อนี้ เหตุผล เพราะผลิตภัณฑ์ที่บริษัทนำเสนอไม่สามารถยื่นข้อเสนอเข้าร่วมแข่งขันได้	ตัดทิ้ง เหตุผล เพื่อเป็นการเปิดกว้างในการแข่งขัน
5.3.20 รองรับการทำงานร่วมกับ Event Management Tool เช่น Jira หรือ ServiceNow	ขอให้ตัดคุณสมบัติข้อนี้ เหตุผล เพราะผลิตภัณฑ์ที่บริษัทนำเสนอไม่สามารถยื่นข้อเสนอเข้าร่วมแข่งขันได้	ตัดทิ้ง เหตุผล เพื่อเป็นการเปิดกว้างในการแข่งขัน
5.3.21 สามารถส่ง Log แบบ Syslog ได้	ขอให้ตัดคุณสมบัติข้อนี้ เหตุผล เพราะผลิตภัณฑ์ที่บริษัทนำเสนอไม่สามารถยื่นข้อเสนอเข้าร่วมแข่งขันได้	ไม่ปรับแก้ไข เหตุผล เนื่องจากคุณลักษณะที่กำหนดไว้มีความจำเป็นต่อการใช้งานในปัจจุบัน

คุณลักษณะเฉพาะที่กำหนด ในเอกสาร TOR สำหรับประชาพิจารณ์ครั้งที่ 2	ข้อเสนอแนะ วิจารณ์ จากบริษัท บริษัท เบย์ คอมพิวติ้ง จำกัด	ความเห็นของคณะกรรมการฯ
5.3.22 สามารถค้นหาเหตุการณ์ด้วยเงื่อนไขต่างๆ ได้อย่างน้อยดังนี้ 1) User 2) Operating System 3) Device Name 4) Device Group 5) Policy 6) Playbook Action 7) Process Path 8) Event Action	ขอให้ตัดคุณสมบัติข้อนี้ <u>เหตุผล</u> เพราะผลิตภัณฑ์ที่บริษัทนำเสนอไม่สามารถยื่นข้อเสนอเข้าร่วมแข่งขันได้	<u>ตัดทิ้ง</u> <u>เหตุผล</u> เพื่อเป็นการเปิดกว้างในการแข่งขัน
5.3.23 สามารถแจ้งเตือนผู้ดูแลระบบเมื่อตรวจพบมัลแวร์ (Malware) ผ่าน Email ได้เป็นอย่างน้อย	ขอให้ตัดคุณสมบัติข้อนี้ <u>เหตุผล</u> เพราะผลิตภัณฑ์ที่บริษัทนำเสนอไม่สามารถยื่นข้อเสนอเข้าร่วมแข่งขันได้	<u>ไม่ปรับแก้ไข</u> <u>เหตุผล</u> เนื่องจากคุณลักษณะที่กำหนดไว้มีความจำเป็นต่อการใช้งานในปัจจุบัน

คุณลักษณะเฉพาะที่กำหนด ในเอกสาร TOR สำหรับประชาพิจารณ์ครั้งที่ 2	ข้อเสนอแนะ วิจารณ์ จากบริษัท บริษัท เบย์ คอมพิวติ้ง จำกัด	ความเห็นของคณะกรรมการฯ
5.3.24 สามารถแสดงผลรายงานแบบ PDF ได้เป็นอย่างน้อย	ขอให้ตัดคุณสมบัติข้อนี้ <u>เหตุผล</u> เพราะผลิตภัณฑ์ที่บริษัทนำเสนอไม่สามารถยื่นข้อเสนอเข้าร่วมแข่งขันได้	<u>ไม่ปรับแก้ไข</u> <u>เหตุผล</u> เนื่องจากคุณลักษณะที่กำหนดไว้มีความจำเป็นต่อการใช้งานในปัจจุบัน
5.4 ระบบตรวจจับและตอบสนองต่อระบบเครือข่ายคอมพิวเตอร์ (Network Detection and Response: NDR)		
5.4.1 มีอุปกรณ์ Hardware Appliance จำนวนอย่างน้อย 1 ชุด โดยมีคุณลักษณะอย่างน้อยดังนี้ 1) มีช่องเชื่อมต่อเครือข่าย 10 Gigabit Ethernet SFP+ จำนวนไม่น้อยกว่า 2 พอร์ต พร้อมติดตั้ง Transceiver 10G SR จำนวนไม่น้อยกว่า 2 พอร์ต 2) มีช่องเชื่อมต่อเครือข่าย 10/100/1000Base-T จำนวนไม่น้อยกว่า 2 พอร์ต 3) มี SSD ขนาดไม่น้อยกว่า 128 Gb จำนวน 1 หน่วย 4) มี Harddisk ขนาดไม่น้อยกว่า 1.2 TB จำนวนไม่น้อยกว่า 4 หน่วย	5.4.1 มีอุปกรณ์ Hardware Appliance จำนวนอย่างน้อย 1 ชุด โดยมีคุณลักษณะอย่างน้อยดังนี้ 1) มีช่องเชื่อมต่อเครือข่าย 10 Gigabit Ethernet SFP+ จำนวนไม่น้อยกว่า 2 พอร์ต พร้อมติดตั้ง Transceiver 10G SR จำนวนไม่น้อยกว่า 2 พอร์ต 2) มีช่องเชื่อมต่อเครือข่าย 10/100/1000Base-T จำนวนไม่น้อยกว่า 2 พอร์ต 3) มี SSD ขนาดไม่น้อยกว่า 128 Gb จำนวน 1 หน่วย 4) มี Harddisk ขนาดไม่น้อยกว่า 1.2 TB จำนวนไม่น้อยกว่า 4 หน่วย	<u>ปรับแก้ไข</u> 5.4.1 มีอุปกรณ์ Hardware Appliance จำนวนอย่างน้อย 1 ชุด โดยมีคุณลักษณะอย่างน้อยดังนี้ 1) มีช่องเชื่อมต่อเครือข่าย 10 Gigabit Ethernet SFP+ จำนวนไม่น้อยกว่า 2 พอร์ต พร้อมติดตั้ง Transceiver 10G SR จำนวนไม่น้อยกว่า 2 พอร์ต 2) มีช่องเชื่อมต่อเครือข่าย 10/100/1000Base-T จำนวนไม่น้อยกว่า 2 พอร์ต 3) มี SSD ขนาดไม่น้อยกว่า 128 Gb จำนวน 1 หน่วย

คุณลักษณะเฉพาะที่กำหนด ในเอกสาร TOR สำหรับประชาพิจารณ์ครั้งที่ 2	ข้อเสนอแนะ วิจารณ์ จากบริษัท บริษัท เบย์ คอมพิวติ้ง จำกัด	ความเห็นของคณะกรรมการฯ
5) มี Performance แบบ Mix Mode (Brand และ Sensor) ไม่น้อยกว่า 8 Gbps หากอุปกรณ์ไม่สามารถทำงานในแบบ Mix Mode ได้ให้เสนออุปกรณ์ภายนอกที่ทำหน้าที่เป็น Sensor โดยอุปกรณ์ภายนอกที่เสนอต้องมี Throughput ไม่น้อยกว่า 8 Gbps	5) มี Performance แบบ Mix Mode (Brand และ Sensor) ไม่น้อยกว่า 8 Gbps หากอุปกรณ์ไม่สามารถทำงานในแบบ Mix Mode ได้ให้เสนออุปกรณ์ภายนอกที่ทำหน้าที่เป็น Sensor โดยอุปกรณ์ภายนอกที่เสนอต้องมี Throughput ไม่น้อยกว่า 8 Gbps หรือ ซอฟต์แวร์รวบรวมข้อมูลภายในระบบเครือข่าย (Sensor) จำนวน 1 ชุด โดยมีคุณสมบัติต่อชุดดังนี้ — สามารถติดตั้งบนระบบ Virtualization — ใช้ทรัพยากรหน่วยประมวลผลกลางแบบเสมือน (vCPU) 8 Core — ใช้ทรัพยากรหน่วยความจำหลักแบบเสมือน (Virtual RAM) 8 GB — ใช้ทรัพยากรหน่วยความจำสำรองแบบเสมือน (Virtual Disk) ไม่ต่ำกว่า 128 GB	4) มี Harddisk ขนาดไม่น้อยกว่า 1.2 TB จำนวนไม่น้อยกว่า 4 หน่วย 5) มี Performance แบบ Mix Mode (Brand และ Sensor) ไม่น้อยกว่า 8 Gbps หากอุปกรณ์ไม่สามารถทำงานในแบบ Mix Mode ได้ให้เสนออุปกรณ์ภายนอกที่ทำหน้าที่เป็น Sensor โดยอุปกรณ์ภายนอกที่เสนอต้องมี Throughput ไม่น้อยกว่า 8 Gbps หรือมีซอฟต์แวร์รวบรวมข้อมูลภายในระบบเครือข่าย (Sensor) จำนวน 1 ชุด พร้อมซอฟต์แวร์สำหรับการตรวจจับและตอบสนองต่อภัยคุกคามทางด้านไซเบอร์ (security detection and response) จำนวน 1 ชุด โดยมีคุณสมบัติต่อชุดดังนี้ 1) ซอฟต์แวร์รวบรวมข้อมูลภายในระบบเครือข่าย (Sensor) มีคุณสมบัติต่อชุดดังนี้

คุณลักษณะเฉพาะที่กำหนด ในเอกสาร TOR สำหรับประชาพิจารณ์ครั้งที่ 2	ข้อเสนอแนะ วิจารณ์ จากบริษัท บริษัท เบย์ คอมพิวติ้ง จำกัด	ความเห็นของคณะกรรมการฯ
	– สามารถรวบรวมข้อมูลภายในระบบเครือข่ายด้วยวิธีการ SPAN หรือ Mirrored Traffic จากอุปกรณ์ Switch หรือ Virtual Switch ได้ – สามารถรับ Traffic Throughput ได้อย่างน้อย 1 Gbps	• สามารถติดตั้งบนระบบ Virtualization • ใช้ทรัพยากรหน่วยประมวลผลกลางแบบเสมือน (vCPU) 8 Core • ใช้ทรัพยากรหน่วยความจำหลักแบบเสมือน (Virtual RAM) 8 GB • ใช้ทรัพยากรหน่วยความจำสำรองแบบเสมือน (Virtual Disk) ไม่ต่ำกว่า 128 GB • สามารถรวบรวมข้อมูลภายในระบบเครือข่ายด้วยวิธีการ SPAN หรือ Mirrored Traffic จากอุปกรณ์ Switch หรือ Virtual Switch ได้ 2) ซอฟต์แวร์สำหรับการตรวจจับและตอบสนองต่อภัยคุกคามทางด้านไซเบอร์ (security detection and response)มีคุณสมบัติต่อชุดดังนี้

คุณลักษณะเฉพาะที่กำหนด ในเอกสาร TOR สำหรับประชาพิจารณ์ครั้งที่ 2	ข้อเสนอแนะ วิจารณ์ จากบริษัท บริษัท เบย์ คอมพิวติ้ง จำกัด	ความเห็นของคณะกรรมการฯ
		• สามารถติดตั้งบนระบบ Virtualization ใช้ทรัพยากรหน่วยประมวลผลกลางแบบเสมือน (vCPU) 8 Core • ใช้ทรัพยากรหน่วยความจำหลักแบบเสมือน (Virtual RAM) 64 GB • ใช้ทรัพยากรหน่วยความจำสำรองแบบเสมือน (Virtual Disk) 2 TB • สามารถรับ Traffic Throughput ได้อย่างน้อย 2 Gbps • สามารถทำการรวบรวมข้อมูลจากซอฟต์แวร์รวบรวมข้อมูลภายในระบบเครือข่าย (Sensor) ที่นำเสนอได้ <u>เหตุผล</u> เพื่อเป็นการเปิดกว้างในการแข่งขัน

คุณลักษณะเฉพาะที่กำหนด ในเอกสาร TOR สำหรับประชาพิจารณ์ครั้งที่ 2	ข้อเสนอแนะ วิจารณ์ จากบริษัท บริษัท เบย์ คอมพิวติ้ง จำกัด	ความเห็นของคณะกรรมการฯ
5.4.2 ระบบที่เสนอต้องเป็นระบบทางด้าน Network Detection and Response (NDR) และใช้ข้อมูล Raw Network Packet เพื่อนำมาใช้ในการตรวจจับ และวิเคราะห์ภัยคุกคามขั้นสูงได้	5.4.2 ระบบที่เสนอต้องเป็นระบบทางด้าน Network Detection and Response (NDR) และใช้ข้อมูล Raw Network Packet เพื่อนำมาใช้ในการตรวจจับ และวิเคราะห์ภัยคุกคามขั้นสูงได้ หรือ ซอฟต์แวร์สำหรับการตรวจจับและตอบสนองต่อภัยคุกคามทางด้านไซเบอร์ (security detection and response) จำนวน 1 ชุด โดยมีคุณสมบัติต่อชุดดังนี้ — สามารถติดตั้งบนระบบ Virtualization — ใช้ทรัพยากรหน่วยประมวลผลกลางแบบเสมือน (vCPU) 8 Core — ใช้ทรัพยากรหน่วยความจำหลักแบบเสมือน (Virtual RAM) 64 GB — ใช้ทรัพยากรหน่วยความจำสำรองแบบเสมือน (Virtual Disk) 2 TB — สามารถรับ Traffic Throughput ได้อย่างน้อย 2 Gbps	ไม่ปรับแก้ไข เหตุผล เนื่องจากคุณลักษณะที่กำหนดไว้มีความจำเป็นต่อการใช้งานในปัจจุบัน

คุณลักษณะเฉพาะที่กำหนด ในเอกสาร TOR สำหรับประชาพิจารณ์ครั้งที่ 2	ข้อเสนอแนะ วิจารณ์ จากบริษัท บริษัท เบย์ คอมพิวติ้ง จำกัด	ความเห็นของคณะกรรมการฯ
	– สามารถทำการรวบรวมข้อมูลจากซอฟต์แวร์รวบรวมข้อมูลภายในระบบเครือข่าย (Sensor) ที่นำเสนอได้	
5.4.3 ต้องมีความสามารถประมวลผลและวิเคราะห์ข้อมูลได้ในรูปแบบ On-Premise	5.4.3 ต้องมีความสามารถประมวลผลและวิเคราะห์ข้อมูลได้ในรูปแบบ On-Premise หรือ มีระบบวิเคราะห์ (Security Engines) เพื่อเพิ่มประสิทธิภาพในการตรวจจับ อย่างน้อยดังนี้ – Artificial intelligence (AI) – Threat Intelligence – User and Entity Behavioral Analytics (UEBA)	<u>ไม่ปรับแก้ไข</u> <u>เหตุผล</u> เนื่องจากคุณลักษณะที่กำหนดไว้มีความจำเป็นต่อการใช้งานในปัจจุบัน
5.4.4 ระบบที่เสนอต้องสามารถในการวิเคราะห์และตรวจจับภัยคุกคามขั้นสูงด้วยวิธีการดังต่อไปนี้ 1) ต้องมีการใช้ Behavioral Techniques (Non-Signature-Based Detection) โดยการใช้ Machine Learning ในการตรวจวิเคราะห์ และต้องมีการใช้	5.4.4 ระบบที่เสนอต้องสามารถในการวิเคราะห์และตรวจจับภัยคุกคามขั้นสูงด้วยวิธีการดังต่อไปนี้ 1) ต้องมีการใช้ Behavioral Techniques (Non-Signature-Based Detection) โดยการใช้ Machine Learning ในการตรวจวิเคราะห์ และต้องมีการใช้	<u>ไม่ปรับแก้ไข</u> <u>เหตุผล</u> เนื่องจากคุณลักษณะที่กำหนดไว้มีความจำเป็นต่อการใช้งานในปัจจุบัน

คุณลักษณะเฉพาะที่กำหนด ในเอกสาร TOR สำหรับประชาพิจารณ์ครั้งที่ 2	ข้อเสนอแนะ วิจารณ์ จากบริษัท บริษัท เบย์ คอมพิวติ้ง จำกัด	ความเห็นของคณะกรรมการฯ
Unsupervised Learning เป็นอย่างน้อย เพื่อสามารถตรวจจับ Network Traffic ที่ผิดปกติ (Anomaly Network Traffic) ได้ 2) ต้องมีความสามารถในการใช้ Supervised Learning ในการสร้าง Model เพื่อใช้ในการตรวจจับภัยคุกคามทางด้าน Network ที่ใช้เทคนิคขั้นสูงได้ 3) มีความสามารถในการปรับปรุงประสิทธิภาพ (Fine-tune) ในด้านความถูกต้องแม่นยำในการตรวจจับ (Accuracy of Detection) 4) ต้องสามารถวิเคราะห์ Network Packets ในรูปแบบ Encrypted Traffic และ Decrypted Traffic โดยสำหรับ Encrypted Traffic ต้องสามารถวิเคราะห์ด้วยวิธี JA3 Fingerprint และ JA3S Fingerprint	Unsupervised Learning เป็นอย่างน้อย เพื่อสามารถตรวจจับ Network Traffic ที่ผิดปกติ (Anomaly Network Traffic) ได้ 2) ต้องมีความสามารถในการใช้ Supervised Learning ในการสร้าง Model เพื่อใช้ในการตรวจจับภัยคุกคามทางด้าน Network ที่ใช้เทคนิคขั้นสูงได้ 3) มีความสามารถในการปรับปรุงประสิทธิภาพ (Fine-tune) ในด้านความถูกต้องแม่นยำในการตรวจจับ (Accuracy of Detection) 4) ต้องสามารถวิเคราะห์ Network Packets ในรูปแบบ Encrypted Traffic และ Decrypted Traffic โดยสำหรับ Encrypted Traffic ต้องสามารถวิเคราะห์ด้วยวิธี JA3 Fingerprint และ JA3S Fingerprint	

คุณลักษณะเฉพาะที่กำหนด ในเอกสาร TOR สำหรับประชาพิจารณ์ครั้งที่ 2	ข้อเสนอแนะ วิจารณ์ จากบริษัท บริษัท เบย์ คอมพิวติ้ง จำกัด	ความเห็นของคณะกรรมการฯ
	หรือ มีความสามารถในการตรวจจับภัยคุกคามทางด้านไซเบอร์ (Threat Detection) อย่างน้อยดังนี้ – ภัยคุกคามหรือการโจมตีที่เข้ามายังระบบเครือข่ายภายในผ่านช่องทางอินเตอร์เน็ต (Inbound Threats) – ภัยคุกคามหรือการโจมตีที่มีการเชื่อมต่อหรือโจมตีออกไปยังอินเตอร์เน็ต (Outbound Threats) – ภัยคุกคามหรือการโจมตีที่เกิดขึ้นในระบบเครือข่ายภายใน (Lateral Threats)	
5.4.5 ระบบที่เสนอต้องมีความสามารถในการแสดงผลและสนับสนุนด้านการตอบสนองภัยคุกคามแบบ Manual Response หรือแบบ Automatic Response ได้ ดังต่อไปนี้	5.4.5 ระบบที่เสนอต้องมีความสามารถในการแสดงผลและสนับสนุนด้านการตอบสนองภัยคุกคามแบบ Manual Response หรือแบบ Automatic Response ได้ ดังต่อไปนี้	<u>ปรับแก้ไข เป็น</u> 5.4.5 ระบบที่เสนอต้องมีความสามารถในการแสดงผลและสนับสนุนด้านการตอบสนองภัยคุกคามแบบ Manual Response หรือแบบ Automatic Response ได้ ดังต่อไปนี้

คุณลักษณะเฉพาะที่กำหนด ในเอกสาร TOR สำหรับประชาพิจารณ์ครั้งที่ 2	ข้อเสนอแนะ วิจารณ์ จากบริษัท บริษัท เบย์ คอมพิวติ้ง จำกัด	ความเห็นของคณะกรรมการฯ
1. ต้องสามารถเรียกดูข้อมูลบนระบบที่ให้บริการอย่างน้อยดังต่อไปนี้ ย้อนหลังได้ไม่น้อยกว่า 90 วัน ● หน้า dashboard แสดงการใช้งาน Network ที่ผิดปกติที่ระบบสามารถตรวจจับได้ (All Alerts / Detections) ● ประเภทของการใช้งาน Network ผิดปกติที่ระบบสามารถตรวจจับได้ (Security Category) ● ระดับความรุนแรง (Severity) หรือค่าความเสี่ยง (Risk Score) ของการใช้งาน Network ผิดปกติที่ระบบสามารถตรวจจับได้ ● ข้อมูลของ host ต่างๆ โดยสามารถดู detail และ Detection ได้	1 ต้องสามารถเรียกดูข้อมูลบนระบบที่ให้บริการอย่างน้อยดังต่อไปนี้ ย้อนหลังได้ไม่น้อยกว่า 90 วัน ● หน้า dashboard แสดงการใช้งาน Network ที่ผิดปกติที่ระบบสามารถตรวจจับได้ (All Alerts / Detections) ● ประเภทของการใช้งาน Network ผิดปกติที่ระบบสามารถตรวจจับได้ (Security Category) ● ระดับความรุนแรง (Severity) หรือค่าความเสี่ยง (Risk Score) ของการใช้งาน Network ผิดปกติที่ระบบสามารถตรวจจับได้ ● ข้อมูลของ host ต่างๆ โดยสามารถดู detail และ Detection ได้หรือมีความสามารถในการตรวจจับภัยคุกคามทางด้านไซเบอร์แบบเชิงรุก	1 ต้องสามารถเรียกดูข้อมูลบนระบบที่ให้บริการอย่างน้อยดังต่อไปนี้ ย้อนหลังได้ไม่น้อยกว่า 90 วัน ● หน้า dashboard แสดงการใช้งาน Network ที่ผิดปกติที่ระบบสามารถตรวจจับได้ (All Alerts / Detections) ● ประเภทของการใช้งาน Network ผิดปกติที่ระบบสามารถตรวจจับได้ (Security Category) ● ระดับความรุนแรง (Severity) หรือค่าความเสี่ยง (Risk Score) ของการใช้งาน Network ผิดปกติที่ระบบสามารถตรวจจับได้ ● ข้อมูลของ host ต่างๆ โดยสามารถดู detail และ Detection ได้หรือมีความสามารถในการตรวจจับภัยคุกคามทางด้านไซเบอร์แบบเชิงรุก

คุณลักษณะเฉพาะที่กำหนด ในเอกสาร TOR สำหรับประชาพิจารณ์ครั้งที่ 2	ข้อเสนอแนะ วิจารณ์ จากบริษัท บริษัท เบย์ คอมพิวติ้ง จำกัด	ความเห็นของคณะกรรมการฯ
	(Threat Hunting) โดยมีความสามารถดังนี้ – สามารถวิเคราะห์และตรวจจับแหล่งที่มาของภัยคุกคาม (patient zero หรือ Entry Point) – สามารถเชื่อมโยงการแพร่กระจายหรือการโจมตีของภัยคุกคามที่เกิดขึ้นภายในระบบเครือข่ายได้	(Threat Hunting) โดยมีความสามารถดังนี้ – สามารถวิเคราะห์และตรวจจับแหล่งที่มาของภัยคุกคาม (patient zero หรือ Entry Point) – สามารถเชื่อมโยงการแพร่กระจายหรือการโจมตีของภัยคุกคามที่เกิดขึ้นภายในระบบเครือข่ายได้ <u>เหตุผล</u> เพื่อเป็นการเปิดกว้างในการแข่งขัน
2. ต้องมีความสามารถ Correlate Security Events เพื่อให้ทราบว่าภัยคุกคามดังกล่าวมีความสัมพันธ์เชื่อมโยง ● แสดงผลความเชื่อมโยงระหว่างเครือข่าย Network Lateral Movement ได้	2 ต้องมีความสามารถ Correlate Security Events เพื่อให้ทราบว่าภัยคุกคามดังกล่าวมีความสัมพันธ์เชื่อมโยง ● แสดงผลความเชื่อมโยงระหว่างเครือข่าย Network Lateral Movement ได้	<u>ไม่ปรับแก้ไข</u> <u>เหตุผล</u> เนื่องจากคุณลักษณะที่กำหนดไว้มีความจำเป็นต่อการใช้งานในปัจจุบัน

คุณลักษณะเฉพาะที่กำหนด ในเอกสาร TOR สำหรับประชาพิจารณ์ครั้งที่ 2	ข้อเสนอแนะ วิจารณ์ จากบริษัท บริษัท เบย์ คอมพิวติ้ง จำกัด	ความเห็นของคณะกรรมการฯ
• สามารถ Map Security Events กับ MITRE Framework หรือ Cyber Kill Chain เพื่อให้ทราบว่าภัยคุกคามดังกล่าวเป็นภัยคุกคามประเภทใด และอยู่ใน Attack Phase ใดได้	• สามารถ Map Security Events กับ MITRE Framework หรือ Cyber Kill Chain เพื่อให้ทราบว่าภัยคุกคามดังกล่าวเป็นภัยคุกคามประเภทใด และอยู่ใน Attack Phase ใดได้ หรือ มีความสามารถในการค้นหาอุปกรณ์ที่เชื่อมต่อเข้ามาภายในระบบเครือข่ายด้วยวิธีการ automatically discovered เพื่อใช้ในการสร้าง Asset Management ได้	
3. ต้องสามารถนำข้อมูลที่เป็น Network Packet มาแสดงผล และสามารถ Export PCAP เพื่อนำไปทำ Network Forensics ได้	3 ต้องสามารถนำข้อมูลที่เป็น Network Packet มาแสดงผล และสามารถ Export PCAP เพื่อนำไปทำ Network Forensics ได้หรือ มีความสามารถในการตอบสนองต่อภัยคุกคามทางด้านไซเบอร์ที่ตรวจพบ (Response)	<u>ไม่ปรับแก้ไข</u> <u>เหตุผล</u> เนื่องจากคุณลักษณะที่กำหนดไว้มีความจำเป็นต่อการใช้งานในปัจจุบัน

คุณลักษณะเฉพาะที่กำหนด ในเอกสาร TOR สำหรับประชาพิจารณ์ครั้งที่ 2	ข้อเสนอแนะ วิจารณ์ จากบริษัท บริษัท เบย์ คอมพิวติ้ง จำกัด	ความเห็นของคณะกรรมการฯ
	– สามารถระบุระดับความรุนแรงของภัยคุกคามหรือเหตุการณ์ที่เกิดขึ้นได้ (Severity/Prioritized based) – สามารถแสดงความสัมพันธ์ของสถานะการณ์และผลกระทบที่เกิดขึ้นได้ (Stage of Attack/Attack chain) – สามารถแสดงรายละเอียดย้อนหลัง (Traceback) เพื่อทำให้ทราบจุดเริ่มต้น (Entry points) และระยะเวลาที่เกิดเหตุการณ์หรือความสัมพันธ์ได้ (Timeline) – สามารถให้คำแนะนำเพื่อใช้ในการตอบสนองหรือแก้ไขปัญหาที่เกิดจากภัยคุกคามที่ตรวจพบได้ (Suggestions)	

คุณลักษณะเฉพาะที่กำหนด ในเอกสาร TOR สำหรับประชาพิจารณ์ครั้งที่ 2	ข้อเสนอแนะ วิจารณ์ จากบริษัท บริษัท เบย์ คอมพิวติ้ง จำกัด	ความเห็นของคณะกรรมการฯ
4. ระบบรองรับการทำงานร่วมกับอุปกรณ์ด้านความมั่นคงปลอดภัย (Security Products) เช่น SIEM, Firewall, EDR ได้	4 ระบบรองรับการทำงานร่วมกับอุปกรณ์ด้านความมั่นคงปลอดภัย (Security Products) เช่น SIEM, Firewall, EDR ได้ หรือ มีหน้าจอที่ใช้แสดงภาพเหตุการณ์หรือภัยคุกคามทางด้านไซเบอร์ที่เกิดขึ้น (Visualization) อย่างน้อยดังนี้ — แสดงภัยคุกคามหรือการโจมตีที่เข้ามายังระบบเครือข่ายภายในผ่านช่องทางอินเตอร์เน็ต (Inbound Threats) — แสดงภัยคุกคามหรือการโจมตีที่มีการเชื่อมต่อหรือโจมตีออกไปยังอินเตอร์เน็ต (Outbound Threats) — แสดงภัยคุกคามหรือการโจมตีที่เกิดขึ้นในระบบเครือข่ายภายใน (Lateral Threats) — แสดงความสัมพันธ์ของสถานะการณ์และผลกระทบที่เกิดขึ้นได้ (Stage of Attack/Attack chain)	ตัดทิ้ง เหตุผล เพื่อเป็นการเปิดกว้างในการแข่งขัน

คุณลักษณะเฉพาะที่กำหนด ในเอกสาร TOR สำหรับประชาพิจารณ์ครั้งที่ 2	ข้อเสนอแนะ วิจารณ์ จากบริษัท บริษัท เบย์ คอมพิวติ้ง จำกัด	ความเห็นของคณะกรรมการฯ
5. ระบบสามารถทำงานร่วมกับ AD โดยสามารถ manual หรือ automate ในการตัด connection บัญชีผู้ใช้ (disabling accounts) โดยการทำ Account Lockdown บน platform ได้	5 ระบบสามารถทำงานร่วมกับ AD โดยสามารถ manual หรือ automate ในการตัด connection บัญชีผู้ใช้ (disabling accounts) โดยการทำ Account Lockdown บน platform ได้ หรือ สามารถออกรายงาน (Security Risk Reports) และแจ้งเตือน (Security Alarms) ผ่าน Email ได้เป็นอย่างน้อย	ตัดทิ้ง เหตุผล เพื่อเป็นการเปิดกว้างในการแข่งขัน และเป็นคุณสมบัติที่มีอยู่ในอุปกรณ์ SOAR ข้อ 5.2.13
6. สามารถทำงานร่วมกับอุปกรณ์วิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์ (Security Incident Event Management: SIEM) และระบบบริหารจัดการและตอบสนองต่อเหตุการณ์ภัยคุกคามทางคอมพิวเตอร์ (Security Orchestration, Automation and Response: SOAR) ที่เสนอในโครงการนี้ได้	6 สามารถทำงานร่วมกับอุปกรณ์วิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์ (Security Incident Event Management: SIEM) และระบบบริหารจัดการและตอบสนองต่อเหตุการณ์ภัยคุกคามทางคอมพิวเตอร์ (Security Orchestration, Automation and Response: SOAR) ที่เสนอในโครงการนี้ได้ หรือ สามารถทำการแชร์ข้อมูลทางด้านไซเบอร์ (Data sharing) ให้กับอุปกรณ์หรือระบบรักษาความปลอดภัยทางด้านไซเบอร์ที่มีอยู่	ปรับแก้ไข เป็น สามารถทำงานร่วมกับอุปกรณ์วิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์ (Security Incident Event Management: SIEM เหตุผล เพื่อเป็นการเปิดกว้างในการแข่งขัน

คุณลักษณะเฉพาะที่กำหนด ในเอกสาร TOR สำหรับประชาพิจารณ์ครั้งที่ 2	ข้อเสนอแนะ วิจารณ์ จากบริษัท บริษัท เบย์ คอมพิวติ้ง จำกัด	ความเห็นของคณะกรรมการฯ
	ภายในหน่วยงานผ่านช่องทาง RESTful API หรือ Syslog ได้เป็นอย่างน้อย	
	ขอเพิ่ม มีความสามารถในการทำงานร่วมกับระบบป้องกันและตอบสนองต่อภัยคุกคามทางด้านไซเบอร์สำหรับเครื่องคอมพิวเตอร์ (Endpoint Protection and Response) ที่นำเสนอในโครงการได้ ดังนี้ – สามารถทำการรวบรวมข้อมูลจากระบบ Endpoint Protection and Response ได้ – สามารถส่งคำสั่งไปยังระบบ (Response Policies) เพื่อทำ Host Isolation และ Threat Scan ได้	<u>ไม่ปรับแก้ไข</u> <u>เหตุผล</u> คุณสมบัติเดิมของ NDR มีความเหมาะสมกับการใช้งาน

คุณลักษณะเฉพาะที่กำหนด ในเอกสาร TOR สำหรับประชาพิจารณ์ครั้งที่ 2	ข้อเสนอแนะ วิจารณ์ จากบริษัท บริษัท เบย์ คอมพิวติ้ง จำกัด	ความเห็นของคณะกรรมการฯ
	ผู้ขายต้องมีหนังสือสนับสนุนทางด้านเทคนิคและการให้บริการจากบริษัทสาขาเจ้าของผลิตภัณฑ์ในประเทศไทยโดยตรงในการนำเสนองานครั้งนี้เพื่อรับรองว่าผู้สามารถให้คำปรึกษาทางด้านเทคนิครวมถึงการติดตั้งให้เป็นไปตามวัตถุประสงค์ของโครงการและการให้บริการอย่างมีประสิทธิภาพตลอดระยะเวลารับประกัน	ไม่ปรับแก้ไข เหตุผล เนื่องจากเป็นคุณสมบัติของผู้ยื่นข้อเสนอ ในข้อที่ 3.1