ใบสั่งจ้าง

ผู้รับจ้าง บริษัท ไซเบอร์ อีลีท จำกัด
ที่อยู่ เลขที่ ๔๙๙ ถนนกำแพงเพชร ๖
แขวงลาดยาว เขตจตุจักร กรุงเทพมหานคร ๑๐๙๐๐
โทรศัพท์ ๐๒๐๑๖๕๕๕๕
เลขประจำตัวผู้เสียภาษี ๐๑๐๕๕๖๔๑๖๘๐๒๙
เลขที่บัญชีเงินฝากธนาคาร ๑๐๑๙๓๗๓๙๙๐
ชื่อบัญชี บริษัท ไซเบอร์ อีลีท จำกัด
ธนาคาร ธนาคารกรุงเทพจำกัด (มหาชน) สำนักงานใหญ่สีลม (๐๑๐๑)

ใบสั่งจ้างเลขที่ สช.๙๕/๒๕๖๘
วันที่ ๒๘ มีนาคม ๒๕๖๘
ส่วนราชการ โรงพยาบาลตำรวจ
ที่อยู่ -๔๙๒/๑ แขวงปทุมวัน เขตปทุมวัน กรุงเทพมหานคร
โทรศัพท์ -๐๒๒๐๗๖๐๖๓

ตามที่ บริษัท ไซเบอร์ อีลีท จำกัด ได้เสนอราคา ไว้ต่อ โรงพยาบาลตำรวจ ซึ่งได้รับราคาและตกลงจ้าง ตามรายการดังต่อไปนี้

ลำดับ	รายการ	จำนวน	หน่วย	ราคาต่อหน่วย (บาท)	จำนวนเงิน (บาท)
๑	วิเคราะห์ เฝ้าระวังและการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับ รพ.ตร.(ตามขอบเขตของงานที่แนบและเอกสารใบเสนอราคา เลขที่ SQ ๒๔๐๙๐๐๗๔ ลงวันที่ ๒๗ มีนาคม ๒๕๖๘) ค่าจ้างและการจ่ายเงิน แบ่งชำระ ๖ งวด งวดที่ ๑ เป็นจำนวนเงิน ๕๑,๙๘๐ บาท (ห้าหมื่นหนึ่งพันเก้าร้อยแปดสิบบาทถ้วน) (ตั้งแต่วันที่ ๑ เมษายน ๒๕๖๘- วันที่ ๓๐ เมษายน ๒๕๖๘)	๑	งาน	๓๑๑,๙๒๖.๔๐	๓๑๑,๙๒๖.๔๐

ใบสั่งจ้าง

ผู้รับจ้าง บริษัท ไซเบอร์ อีลีท จำกัด
ที่อยู่ เลขที่ ๔๙๙ ถนนกำแพงเพชร ๖
แขวงลาดยาว เขตจตุจักร กรุงเทพมหานคร ๑๐๙๐๐
โทรศัพท์ ๐๒๐๑๖๕๕๕๕
เลขประจำตัวผู้เสียภาษี ๐๑๐๕๕๖๔๑๖๘๐๒๙
เลขที่บัญชีเงินฝากธนาคาร ๑๐๑๙๓๗๓๙๙๐
ชื่อบัญชี บริษัท ไซเบอร์ อีลีท จำกัด
ธนาคาร ธนาคารกรุงเทพจำกัด (มหาชน) สำนักงานใหญ่สีลม ๐๑๐๑)

ใบสั่งจ้างเลขที่ สช. ๙๙/๒๕๖๘
วันที่ ๒๘ มีนาคม ๒๕๖๘
ส่วนราชการ โรงพยาบาลตำรวจ
ที่อยู่ -๔๙๒/๑ แขวงปทุมวัน เขตปทุมวัน กรุงเทพมหานคร
โทรศัพท์ -๐๒๒๐๗๖๐๖๓

ตามที่ บริษัท ไซเบอร์ อีลีท จำกัด ได้เสนอราคา ไว้ต่อ โรงพยาบาลตำรวจ ซึ่งได้รับราคาและตกลงจ้าง ตามรายการดังต่อไปนี้

ลำดับ	รายการ	จำนวน	หน่วย	ราคาต่อหน่วย (บาท)	จำนวนเงิน (บาท)
	งวดที่ ๒ เป็นจำนวนเงิน ๕๑,๙๘๐ บาท (ห้าหมื่นหนึ่งพันเก้าร้อยแปดสิบบาทถ้วน) (ตั้งแต่วันที่ ๑ พฤษภาคม ๒๕๖๘- วันที่ ๓๑ พฤษภาคม ๒๕๖๘) งวดที่ ๓ เป็นจำนวนเงิน ๕๑,๙๘๐ บาท (ห้าหมื่นหนึ่งพันเก้าร้อยแปดสิบบาทถ้วน) (ตั้งแต่วันที่ ๑ มิถุนายน ๒๕๖๘- วันที่ ๓๐ มิถุนายน ๒๕๖๘) งวดที่ ๔ เป็นจำนวนเงิน ๕๑,๙๘๐ บาท (ห้าหมื่นหนึ่งพันเก้าร้อยแปดสิบบาทถ้วน) (ตั้งแต่วันที่ ๑ กรกฎาคม ๒๕๖๘- วันที่ ๓๑ กรกฎาคม ๒๕๖๘)				

ใบสั่งจ้าง

ผู้รับจ้าง บริษัท ไซเบอร์ อีลีท จำกัด
ที่อยู่ เลขที่ ๔๙๙ ถนนกำแพงเพชร ๖
แขวงลาดยาว เขตจตุจักร กรุงเทพมหานคร ๑๐๙๐๐
โทรศัพท์ ๐๒๐๑๖๕๕๕๕
เลขประจำตัวผู้เสียภาษี ๐๑๐๕๕๖๔๑๖๘๐๒๙
เลขที่บัญชีเงินฝากธนาคาร ๑๐๑๙๓๗๓๙๙๐
ชื่อบัญชี บริษัท ไซเบอร์ อีลีท จำกัด
ธนาคาร ธนาคารกรุงเทพจำกัด (มหาชน) สำนักงานใหญ่สีลม (๐๑๐๑)

ใบสั่งจ้างเลขที่ สช.๗๕/๒๕๖๘
วันที่ ๒๘ มีนาคม ๒๕๖๘
ส่วนราชการ โรงพยาบาลตำรวจ
ที่อยู่ -๔๙๒/๑ แขวงปทุมวัน เขตปทุมวัน กรุงเทพมหานคร
โทรศัพท์ -๐๒๒๐๗๖๐๖๓

ตามที่ บริษัท ไซเบอร์ อีลีท จำกัด ได้เสนอราคา ไว้ต่อ โรงพยาบาลตำรวจ ซึ่งได้รับราคาและตกลงจ้าง ตามรายการดังต่อไปนี้

ลำดับ	รายการ	จำนวน	หน่วย	ราคาต่อหน่วย (บาท)	จำนวนเงิน (บาท)
	งวดที่ ๕ เป็นจำนวนเงิน ๕๑,๙๘๐ บาท (ห้าหมื่นหนึ่งพันเก้าร้อยแปดสิบบาทถ้วน) (ตั้งแต่วันที่ ๑ สิงหาคม ๒๕๖๘- วันที่ ๓๑ สิงหาคม ๒๕๖๘) งวดที่ ๖ เป็นจำนวนเงิน ๕๒,๐๒๖.๔๐ บาท (ห้าหมื่นสองพันยี่สิบหกบาทสี่สิบสตางค์) (ตั้งแต่วันที่ ๑ กันยายน ๒๕๖๘- วันที่ ๓๐ กันยายน ๒๕๖๘)				
(สามแสนหนึ่งหมื่นหนึ่งพันเก้าร้อยยี่สิบหกบาทสี่สิบสตางค์)				รวมเป็นเงิน	๒๙๑,๕๒๐.๐๐
				ภาษีมูลค่าเพิ่ม	๒๐,๔๐๖.๔๐
				รวมเป็นเงินทั้งสิ้น	๓๑๑,๙๒๖.๔๐

การสั่งจ้าง อยู่ภายใต้เงื่อนไขต่อไปนี้
๑. กำหนดส่งมอบภายใน ๑๘๓ วัน

๒. ครบกำหนดส่งมอบภายในวันที่ ๓๐ กันยายน ๒๕๖๘

๓. สถานที่ส่งมอบ ของ ฝ่ายเวชระเบียน กองบังคับการอำนวยการ โรงพยาบาลตำรวจ

๔. ระยะเวลารับประกัน -ปี

๕. สงวนสิทธิ์ค่าปรับกรณีส่งมอบเกินกำหนด โดยคิดค่าปรับเป็นรายวันในอัตราร้อยละ ๐.๑๐ ของราคางานจ้าง แต่ต้องไม่ต่ำกว่าวันละ ๑๐๐.๐๐ บาท

๖. ส่วนราชการสงวนสิทธิ์ที่จะไม่รับมอบถ้าปรากฏว่าสินค้านั้นมีลักษณะไม่ตรงตามรายการที่ระบุไว้ในใบสั่งจ้าง กรณีนี้ผู้รับจ้างจะต้องดำเนินการเปลี่ยนใหม่ให้ถูกต้องตามใบสั่งจ้างทุกประการ

๗. การจ้างช่วง ผู้รับจ้างจะต้องไม่เอางานทั้งหมดหรือแต่บางส่วนไปจ้างช่วงอีกทอดหนึ่ง เว้นแต่การจ้างช่วงงานแต่บางส่วนที่ได้รับอนุญาตเป็นหนังสือจากผู้ว่าจ้างแล้ว การที่ผู้ว่าจ้างได้อนุญาตให้จ้างช่วงงานแต่บางส่วนดังกล่าวนั้น ไม่เป็นเหตุให้ผู้รับจ้างหลุดพ้นจากความรับผิดหรือพันธะหน้าที่และผู้รับจ้างจะยังคงต้องรับผิดในความผิดและความประมาทเลินเล่อของผู้รับจ้างช่วง หรือของตัวแทนหรือลูกจ้างของผู้รับจ้างช่วงนั้นทุกประการ กรณีผู้รับจ้างไปจ้างช่วงงานแต่บางส่วน โดยฝ่าฝืนความในวรรคหนึ่ง ผู้รับจ้างต้องชำระค่าปรับให้แก่ผู้ว่าจ้างเป็นจำนวนเงินในอัตราร้อยละ ๑๐ (สิบ) ของวงเงินของงาน ที่จ้างช่วง ทั้งนี้ ไม่ตัดสิทธิผู้ว่าจ้างในการบอกเลิกสัญญา

๘. การประเมินผลการปฏิบัติงานของผู้ประกอบการ หน่วยงานของรัฐสามารถนำผลการปฏิบัติงานแล้วเสร็จตามสัญญาหรือข้อตกลงของคู่สัญญาเพื่อนำมาประเมินผลการปฏิบัติงานของผู้ประกอบการ

<u>หมายเหตุ :</u>

๑. การติดอากรแสตมป์ให้เป็นไปตามประมวลกฎหมายรัษฎากร หากต้องการให้ใบสั่งจ้างมีผลตามกฎหมาย

๒.ใบสั่งจ้างสั่งจ้างนี้อ้างอิงตามเลขที่โครงการ ๖๘๐๓๙๔๗๘๙๓๕ จ้างวิเคราะห์ เฝ้าระวังและการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับ โรงพยาบาลตำรวจ ของ ฝ่ายเวชระเบียน กองบังคับการอำนวยการ โรงพยาบาลตำรวจ โดยวิธีเฉพาะเจาะจง

ลงชื่อ.....ผู้สั่งจ้าง

(พลตำรวจตรีหญิงรชยา บุรพลพิมาน)

รองนายแพทย์ใหญ่ (สบ ๗)

ปฏิบัติราชการแทน

นายแพทย์ใหญ่ (สบ ๘)

วันที่ ๒๘ มีนาคม ๒๕๖๘

ลงชื่อ.....ผู้รับใบสั่งจ้าง

(.....)

.....

วันที่ 31 มี.ค. 2568

CYBER ELITE CO., LTD.

เลขที่โครงการ ๖๘๐๓๙๔๗๘๙๓๕

เลขคุมสัญญา ๖๘๐๓๑๔๕๑๗๘๘๙

ร่างขอบเขตของงาน (Terms of Reference: TOR)
โครงการจ้างวิเคราะห์ เฝ้าระวังและการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับโรงพยาบาลตำรวจ

๑. หลักการและเหตุผล

นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. ๒๕๖๕ – ๒๕๗๐) ได้ประกาศในราชกิจจานุเบกษา เมื่อวันที่ ๙ ธันวาคม ๒๕๖๕ และมีผลบังคับใช้เมื่อวันที่ ๑๐ ธันวาคม ๒๕๖๕ มีความสอดคล้องตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๔๓ กำหนดว่า "ให้จัดทำนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ขึ้น เพื่อเสนอคณะรัฐมนตรีให้ความเห็นชอบ โดยให้ประกาศในราชกิจจานุเบกษา และเมื่อประกาศแล้ว ให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแลและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ดำเนินการให้เป็นไปตามนโยบายและแผนดังกล่าว" ประกอบกับคณะกรรมการยุทธศาสตร์ชาติ ในการประชุม ครั้งที่ ๑/๒๕๖๖ เมื่อวันที่ ๘ กุมภาพันธ์ ๒๕๖๖ มีมติเห็นชอบแนวทางการขับเคลื่อนยุทธศาสตร์ชาติในห้วงที่ ๒ (พ.ศ. ๒๕๖๖ - ๒๕๗๐) ตามหลักวงจรบริหารงานคุณภาพ (Plan - Do-Check-Act : PDCA) โดยในส่วนของการปฏิบัติ (Do) หน่วยงานของรัฐต้องให้ความสำคัญกับการจัดทำโครงการ/แผนการดำเนินการที่สอดคล้องกับแผนแม่บทภายใต้ยุทธศาสตร์ชาติ เพื่อบรรลุเป้าหมายของยุทธศาสตร์ชาติ ตามมติคณะรัฐมนตรี เมื่อวันที่ ๕ พฤษภาคม ๒๕๖๓ และเมื่อวันที่ ๑๘ พฤษภาคม ๒๕๖๔ ซึ่งหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องปฏิบัติตามพระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ดังนี้

มาตรา ๕๖ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ต้องกำหนดให้มีกลไกหรือขั้นตอนเพื่อการเฝ้าระวังภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศของตน ตามมาตรฐานซึ่งกำหนดโดยหน่วยงานควบคุมหรือกำกับดูแล และตามประมวลแนวทางปฏิบัติ รวมถึงระบบมาตรการที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ที่คณะกรรมการกำหนด และต้องเข้าร่วมการทดสอบสถานะความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์ที่สำนักงานจัดขึ้น

มาตรา ๕๗ เมื่อมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รายงานต่อสำนักงานและหน่วยงานควบคุมหรือกำกับดูแล และปฏิบัติการรับมือกับภัยคุกคามทางไซเบอร์ตามที่กำหนดในส่วนที่ ๔ ทั้งนี้ อาจกำหนดหลักเกณฑ์และวิธีการการรายงานด้วยก็ได้

ปัจจุบันจากการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ตามแนวปฏิบัติของสำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ตรวจพบลักษณะภัยคุกคามทางไซเบอร์ ในระดับร้ายแรงในระบบสารสนเทศของโรงพยาบาลตำรวจ ซึ่งเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องปฏิบัติตามพระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ โดยฝ่ายเวชระเบียน กองบังคับการอำนวยการ โรงพยาบาลตำรวจ เป็นผู้ดูแลข้อมูลการใช้งานระบบสารสนเทศของหน่วยงานในสังกัดโรงพยาบาลตำรวจ ข้อมูลการเข้ารับการตรวจรักษาของผู้ใช้บริการ ดังนั้นเพื่อเป็นการรักษาความมั่นคงปลอดภัยไซเบอร์ ฝ่ายเวชระเบียน กองบังคับการอำนวยการ โรงพยาบาลตำรวจจึงมีความจำเป็นเร่งด่วนที่ต้องดำเนินการจัดทำโครงการจ้างวิเคราะห์ เฝ้าระวังและการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

CYBER ELITE CO.,LTD

..... ผู้รับจ้าง

..... พยาน

๒. วัตถุประสงค์

๒.๑ เพื่อให้ระบบสารสนเทศของโรงพยาบาลตำรวจมีความปลอดภัยและมีข้อมูลที่น่าเชื่อถือ

๒.๒ เพื่อเฝ้าระวังระบบที่เกี่ยวข้องและมีการแจ้งเตือนเมื่อมีเหตุการณ์ภัยคุกคามเกิดขึ้นหรือมีการโจมตีระบบที่เฝ้าระวัง พร้อมทั้งดำเนินการหาแนวทางป้องกันหรือรับมือกับภัยคุกคามเกิดขึ้นในระบบ

๒.๓ เพื่อให้สามารถรับมือกับสถานการณ์ฉุกเฉินและตอบสนองต่อป้องกันภัยคุกคามทางไซเบอร์ได้อย่างรวดเร็ว

๓. คุณสมบัติผู้ยื่นข้อเสนอ

๓.๑ มีความสามารถตามกฎหมาย

๓.๒ ไม่เป็นบุคคลล้มละลาย

๓.๓ ไม่อยู่ระหว่างเลิกกิจการ

๓.๔ ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราวเนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบ ที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

๓.๕ ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

๓.๖ มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

๓.๗ เป็นบุคคลธรรมดาหรือนิติบุคคล ผู้มีอาชีพขายพัสดุที่ประกวดราคาซื้อด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ดังกล่าว

๓.๘ ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่โรงพยาบาลตำรวจ สำนักงานตำรวจแห่งชาติ ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวาง การแข่งขัน อย่างเป็นธรรมในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

๓.๙ ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์ความคุ้มกันเช่นว่านั้น

๓.๑๐ ผู้ยื่นขอเสนอที่ยื่นข้อเสนอในรูปแบบของ “กิจการร่วมค้า” ต้องมีคุณสมบัติดังนี้

กรณีที่ข้อตกลงฯ กำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก ข้อตกลงฯ จะต้องมีการกำหนดสัดส่วนหน้าที่และความรับผิดชอบในปริมาณงาน สิ่งของ หรือมูลค่าตามสัญญาของผู้ร่วมค้าหลักมากกว่าผู้เข้าร่วมรายอื่นทุกราย

กรณีที่ข้อตกลงฯ กำหนดให้ผู้ร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลักกิจการร่วมค้านั้นต้องใช้ผลงานของผู้เข้าร่วมค้าหลักรายเดียวเป็นผลงานของกิจการร่วมค้าที่ยื่นข้อเสนอ

สำหรับข้อตกลงฯ ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้เข้าร่วมค้าหลัก ผู้เข้าร่วมค้าทุกรายจะต้องมีคุณสมบัติครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารเชิญชวน

กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้มีการมอบหมายผู้เข้าร่วมค้ารายใดรายหนึ่ง เป็นผู้ยื่นข้อเสนอในนามกิจการร่วมค้า การยื่นข้อเสนอดังกล่าวไม่ต้องมีหนังสือมอบอำนาจ

สำหรับข้อตกลงระหว่างผู้เข้าร่วมค้าที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้ยื่นข้อเสนอผู้เข้าร่วมค้าทุกราย จะต้องลงลายมือชื่อในหนังสือมอบอำนาจให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอในนามกิจการร่วมค้า

..... ผู้รับจ้าง

CYBER ELITE CO., LTD. ..... พยาน

๓.๑๑ ผู้ยื่นข้อเสนอต้องลงทะเบียนที่มีข้อมูลถูกต้องครบถ้วนในระบบจัดซื้อจัดจ้างภาครัฐอิเล็กทรอนิกส์ (Electronic Government Procurement: e - GP) ของกรมบัญชีกลาง

๓.๑๒ ผู้ยื่นข้อเสนอต้องมีมูลค่าสุทธิของกิจการ ดังนี้

(๑) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยซึ่งได้จดทะเบียนเกินกว่า ๑ ปี ต้องมีมูลค่าสุทธิของกิจการ จากผลต่างระหว่างสินทรัพย์สุทธิหักด้วยหนี้สินสุทธิ ที่ปรากฏในงบแสดงฐานะการเงินที่มีการตรวจรับรองแล้ว ซึ่งจะต้องแสดงค่าเป็นบวก ๑ ปีสุดท้ายก่อนวันยื่นข้อเสนอ

(๒) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย ซึ่งยังไม่มีการรายงานงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า ให้พิจารณาการกำหนดมูลค่าของทุนจดทะเบียนโดยผู้ยื่นข้อเสนอจะต้องมีทุนจดทะเบียนที่เรียกชำระมูลค่าหุ้นแล้ว ณ วันที่ยื่นข้อเสนอ ไม่ต่ำกว่า ๑ ล้านบาท

(๓) สำหรับการจัดซื้อจัดจ้างครั้งหนึ่งที่มีวงเงินเกิน ๕๐๐,๐๐๐ บาทขึ้นไป กรณีผู้ยื่นข้อเสนอเป็นบุคคลธรรมดา โดยพิจารณาจากหนังสือรับรองบัญชีเงินฝากไม่เกิน ๙๐ วัน ก่อนวันยื่นข้อเสนอ โดยต้องมีเงินฝากคงเหลือในบัญชีธนาคารเป็นมูลค่า ๑ ใน ๔ ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอ ในแต่ละครั้ง และหากเป็นผู้ชนะการจัดซื้อจัดจ้างหรือเป็นผู้ได้รับการคัดเลือกจะต้องแสดงหนังสือรับรองบัญชีเงินฝากที่มีมูลค่าดังกล่าวอีกครั้งหนึ่งในวันลงนามในสัญญา

(๔) กรณีที่ผู้ยื่นข้อเสนอไม่มีมูลค่าสุทธิของกิจการหรือทุนจดทะเบียน หรือมีแต่ไม่เพียงพอที่จะเข้ายื่นข้อเสนอ ผู้ยื่นข้อเสนอสามารถขอวงเงินสินเชื่อ โดยต้องมีวงเงินสินเชื่อ ๑ ใน ๔ ของมูลค่า งบประมาณที่ยื่นข้อเสนอในครั้งนั้น (สินเชื่อที่ธนาคารภายในประเทศหรือบริษัทเงินทุน หรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์ และประกอบธุรกิจค้ำประกันตามประกาศ ของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทยแจ้งเวียนให้ทราบ โดย พิจารณาจากยอดเงินรวมของวงเงินสินเชื่อที่สำนักงานใหญ่รับรอง หรือที่สำนักงานสาขารับรอง (กรณีได้รับ มอบอำนาจจากสำนักงานใหญ่) ซึ่งออกให้แก่ผู้ยื่นข้อเสนอ นับถึงวันยื่นข้อเสนอไม่เกิน ๙๐ วัน

(๕) กรณีตาม (๑) - (๔) ยกเว้นสำหรับกรณีดังต่อไปนี้

(๕.๑) กรณีที่ผู้ยื่นข้อเสนอเป็นหน่วยงานของรัฐ

(๕.๒) นิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยที่อยู่ระหว่างการฟื้นฟูกิจการตามพระราชบัญญัติล้มละลาย (ฉบับที่ ๑๐) พ.ศ. ๒๕๖๑

๔. ขอบเขตของงานที่จะดำเนินการจัดจ้าง

๔.๑ ผู้ยื่นข้อเสนอต้องเป็นผู้ให้บริการการบริหารจัดการระบบความปลอดภัยสารสนเทศที่มีศูนย์ปฏิบัติการเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cybersecurity Operations Center: CSOC) ตั้งอยู่ในประเทศไทย

๔.๒ ผู้ยื่นข้อเสนอต้องมีศูนย์ปฏิบัติการฯ Cybersecurity Operations Center (CSOC) ที่ได้รับมาตรฐานสากล ISO/IEC ๒๗๐๐๑ และ มาตรฐานสากล ISO/IEC ๒๗๗๐๑ และมีความพร้อมในการให้บริการเฝ้าระวังและแจ้งเตือนเหตุการณ์ภัยคุกคามตลอด ๗ วัน ๒๔ ชั่วโมง (๗ x ๒๔)

๔.๓ ระบบเฝ้าระวังความมั่นคงปลอดภัยไซเบอร์ จะต้องสามารถรองรับข้อมูลจราจรทางคอมพิวเตอร์ได้ ๑๕ GB/Day และจะต้องรองรับการทำงานหรือการเฝ้าระวัง ตามอุปกรณ์ที่ทางโรงพยาบาลตำรวจเห็นชอบ

๔.๔ ตรวจสอบความพร้อมใช้งานของระบบและอุปกรณ์ต้นกำเนิดข้อมูลจราจรทางคอมพิวเตอร์ที่จะใช้ในการเฝ้าระวังและระบุแหล่งที่มาของข้อมูลจราจรทางคอมพิวเตอร์และจัดหมวดหมู่ของอุปกรณ์ต้นกำเนิด

CYBER ELITE CO.,LTD

..... ผู้รับจ้าง

..... พยาน

๔.๕ จัดทำ Monitoring use case รวมทั้งกำหนดประเภทข้อมูลจราจรทางคอมพิวเตอร์ (Log) ที่ต้องใช้ในการวิเคราะห์

๔.๖ จัดทำ Dashboard และ Alert ให้สอดคล้องกับ Monitoring Use-case เพื่อใช้ในการแจ้งเตือนและรายงานต่างๆ

๔.๗ ระบบเฝ้าระวังต้องมีการแบ่งแยกการทำงานระหว่างระบบรับส่ง (Log collector), ระบบประมวลผล (Processor) และระบบบริหารจัดการที่ส่วนกลาง (Centralized Management) ออกจากกัน

๔.๘ ระบบเฝ้าระวังและแจ้งเตือนภัยคุกคาม จะต้องติดตั้งภายในศูนย์ Data center ที่ได้รับการรับรองระบบบริหารจัดการรักษาความมั่นคงปลอดภัยสารสนเทศตามมาตรฐานสากล ISO/IEC ๒๗๐๐๑

๔.๙ ผู้ยื่นข้อเสนอต้องให้คำแนะนำในการออกแบบระบบจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log) เพื่อจัดเก็บข้อมูล ณ ศูนย์ข้อมูลหลักให้สอดคล้องตามนโยบายหรือข้อบังคับที่ต้องปฏิบัติตาม

๔.๑๐ ผู้ยื่นข้อเสนอต้องจัดให้มีผู้เชี่ยวชาญสำหรับดำเนินการเข้าเตรียมพร้อมและส่งผ่านข้อมูลจราจรทางคอมพิวเตอร์ เพื่อใช้ในการเฝ้าระวังฯ (On-boarding process)

๔.๑๑ ผู้ยื่นข้อเสนอต้องจัดเตรียมหน่วยปฏิบัติการตอบสนองต่ออุบัติการณ์ด้านความมั่นคงปลอดภัยทางคอมพิวเตอร์ (CSIRT) พร้อมที่จะปฏิบัติหน้าที่ในการตอบสนองต่อภัยคุกคามหรือการบุกรุกระบบอย่างทันท่วงที หรือเข้าดำเนินการสืบสวนและวิเคราะห์หาสาเหตุของปัญหา ภัยคุกคามที่เกิดขึ้น รวมถึงการตรวจพิสูจน์พยานหลักฐานทาง Digital เมื่อมีการร้องขอบริการภายในระยะเวลา ๔ ชั่วโมงนับตั้งแต่ที่ร้องขอ ไม่เกินกว่า ๔ เหตุการณ์ต่ออายุสัญญา พร้อมจัดทำรายงานผลการดำเนินงานสรุปข้อมูลหลักฐานต่าง ๆ ที่ได้จากการตอบสนองต่อเหตุการณ์ภัยคุกคาม (Incident Response and Recommendations Report)

๔.๑๒ จัดเก็บข้อมูลเพื่อให้เป็นไปตาม พรบ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่๒) พ.ศ. ๒๕๖๐ เป็นระยะเวลา ๙๐ วัน ณ ศูนย์ปฏิบัติการฯ ของผู้ยื่นข้อเสนอ และทำการสืบค้นข้อมูลจราจรคอมพิวเตอร์ ตามที่ผู้ใช้บริการร้องขอโดยมี SLA ดังนี้

Log ที่ร้องขอ	**การสืบค้นข้อมูล**
น้อยกว่า ๓๐ วัน	ภายใน ๒๔ ชั่วโมง
๓๑ - ๙๐ วัน	ภายใน ๗ - ๑๐ วันทำการ

๔.๑๓ ผู้ยื่นข้อเสนอต้องแจ้งเตือนภัยคุกคามด้านความมั่นคงปลอดภัย สำหรับเหตุการณ์ที่อยู่ในขอบข่ายภัยคุกคามทางไซเบอร์ โดยจะต้องแจ้งเตือนผ่านทางอีเมลหรือทางโทรศัพท์ หรือช่องทางอื่นใดตามที่จะตกลง เพื่อให้เป็นไปตาม Severity Level Agreement (SLA) อย่างน้อยดังต่อไป ดังนี้

ระดับความรุนแรง	**แจ้งเตือน**	**ให้คำแนะนำในการแก้ไข**
วิกฤติ	๓๐ นาที	๒ ชั่วโมง
สูง	๑ ชั่วโมง	๔ ชั่วโมง
กลาง	๔ ชั่วโมง	๘ ชั่วโมง
ต่ำ	รายงานประจำเดือน	รายงานประจำเดือน

CYBER ELITE CO., LTD.

..... ผู้รับจ้าง

..... พยาน

๔.๑๔ การแจ้งเตือนจะต้องมีรายละเอียด อย่างน้อยดังนี้

๔.๑๔.๑ ระบุประเภทของภัยคุกคาม

๔.๑๔.๒ วัน-เวลา เริ่มต้นของภัยคุกคาม

๔.๑๔.๓ ระบุต้นทาง (Attacker) และปลายทาง (Target)

๔.๑๔.๔ ระบุระดับความรุนแรง (Severity)

๔.๑๔.๕ รายละเอียดเหตุการณ์และพฤติกรรม

๔.๑๔.๖ คำแนะนำและขั้นตอนการดำเนินการแก้ไขด้านเทคนิค (Action&Recommendation)

๔.๑๕ ผู้ให้บริการต้องรายงานผลการดำเนินการจัดเก็บและวิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์และสรุปผลการดำเนินการเฝ้าระวังภัยคุกคาม เหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศที่เกิดขึ้นโดยมีการวิเคราะห์ภัยคุกคาม เป็นรายเดือน (Monthly report) ซึ่งมีเนื้อหาอย่างน้อยดังนี้

๔.๑๕.๑ สรุปเหตุการณ์ตามประเภทและระดับความรุนแรง (Incident Report)

๔.๑๕.๒ สรุป ๑๐ อันดับสูงสุดของการโจมตี

๔.๑๕.๓ สรุป ๑๐ อันดับสูงสุดของเป้าหมายที่โดนโจมตี

๔.๑๕.๔ สรุป ๑๐ อันดับสูงสุดของผู้โจมตี

๔.๑๕.๕ สรุป ๑๐ อันดับสูงสุดของช่องทางที่ถูกใช้โจมตี

๔.๑๕.๖ สรุปปริมาณและสถานะการใช้งานข้อมูลจราจรทางคอมพิวเตอร์ประจำเดือน

๔.๑๖ ผู้ยื่นข้อเสนอต้องมีการแจ้งข่าวสารซึ่งเกี่ยวข้องกับระบบรักษาความปลอดภัยทางไซเบอร์ เช่น

๔.๑๖.๑ รายชื่อ และคุณลักษณะของมัลแวร์ (Malware)

๔.๑๖.๒ ช่องโหว่ใหม่ (Vulnerability) ของอุปกรณ์ในระบบเครือข่าย (Network Equipment)

๔.๑๖.๓ ช่องโหว่ใหม่ (Vulnerability) ของระบบปฏิบัติการ (Operating System)

๔.๑๖.๔ ช่องโหว่ใหม่ (Vulnerability) ของระบบฐานข้อมูลหลัก (Database)

๔.๑๗ บริการตรวจสอบช่องโหว่ของอุปกรณ์ทางไซเบอร์หรืออุปกรณ์เครื่องแม่ข่ายหรืออุปกรณ์ระบบเครือข่าย

๔.๑๗.๑ สามารถตรวจสอบช่องโหว่จำนวน ๑๐ IP Address ได้

๔.๑๗.๒ สามารถจัดลำดับความเสี่ยง และจัดทำรายงานการตรวจสอบช่องโหว่ของอุปกรณ์ทางไซเบอร์หรืออุปกรณ์เครื่องแม่ข่ายหรืออุปกรณ์ระบบเครือข่ายได้

๕. ระยะเวลาดำเนินงาน/กำหนดเวลาส่งมอบพัสดุ

กำหนดระยะเวลา ๖ เดือน (วันที่ ๑ เมษายน ๒๕๖๘ ถึงวันที่ ๓๐ กันยายน ๒๕๖๘)

๖. หลักเกณฑ์ในการพิจารณาคัดเลือกข้อเสนอ

ใช้เกณฑ์ราคา

๗. วงเงินงบประมาณ/วงเงินที่ได้รับจัดรปภสรร

เงินบำรุง โรงพยาบาลตำรวจ ประจำปี พ.ศ.๒๕๖๘ จำนวน ๓๑๑,๙๒๖.๔๐ บาท (สามแสนหนึ่งหมื่นหนึ่งพันเก้าร้อยยี่สิบหกบาทสี่สิบสตางค์)

๘. งวดงานและการจ่ายเงิน

แบ่งจ่ายเงินออกเป็น ๖ งวด โดยมีรายละเอียดดังต่อไปนี้

งวดที่ ๑ (๑-๓๐ เม.ย.๖๘) เป็นเงินจำนวน ๕๑,๙๘๐ บาท (ห้าหมื่นหนึ่งพันหกร้อยแปดสิบบาทถ้วน) เมื่อผู้รับจ้างได้ส่งมอบงาน ดังนี้

๑) รายงานการแจ้งเตือนภัยคุกคามด้านความมั่นคงปลอดภัย สำหรับเหตุการณ์ที่อยู่ในขอบข่ายภัยคุกคามทางไซเบอร์ โดยมีรายละเอียดการแจ้งเตือน ตามข้อ ๔.๑๔

..... ผู้รับจ้าง

..... พยาน

๒) รายงานผลการดำเนินการจัดเก็บและวิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์และสรุปผลการดำเนินการเฝ้าระวังภัยคุกคาม ตามข้อ ๔.๑๕

๓) รายงานข้อมูลข่าวสารซึ่งเกี่ยวข้องกับระบบรักษาความปลอดภัยทางไซเบอร์ ตามข้อ ๔.๑๖

ในรูปแบบของเอกสารและไฟล์ ภายในวันที่ ๓๐ เมษายน ๒๕๖๘ และคณะกรรมการตรวจรับพัสดุได้ตรวจรับเรียบร้อยแล้ว

งวดที่ ๒ (๑-๓๑ พ.ค.๖๘) เป็นเงินจำนวน ๕๑,๙๘๐ บาท (ห้าหมื่นหนึ่งพันหกร้อยแปดสิบบาทถ้วน) เมื่อผู้รับจ้างได้ส่งมอบงาน ดังนี้

๑) รายงานการแจ้งเตือนภัยคุกคามด้านความมั่นคงปลอดภัย สำหรับเหตุการณ์ที่อยู่ในขอบข่ายภัยคุกคามทางไซเบอร์ โดยมีรายละเอียดการแจ้งเตือน ตามข้อ ๔.๑๔

๒) รายงานผลการดำเนินการจัดเก็บและวิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์และสรุปผลการดำเนินการเฝ้าระวังภัยคุกคาม ตามข้อ ๔.๑๕

๓) รายงานข้อมูลข่าวสารซึ่งเกี่ยวข้องกับระบบรักษาความปลอดภัยทางไซเบอร์ ตามข้อ ๔.๑๖

ในรูปแบบของเอกสารและไฟล์ ภายในวันที่ ๓๑ พฤษภาคม ๒๕๖๘ และคณะกรรมการตรวจรับพัสดุได้ตรวจรับเรียบร้อยแล้ว

งวดที่ ๓ (๑-๓๐ มิ.ย.๖๘) เป็นเงินจำนวน ๕๑,๙๘๐ บาท (ห้าหมื่นหนึ่งพันหกร้อยแปดสิบบาทถ้วน) เมื่อผู้รับจ้างได้ส่งมอบงาน ดังนี้

๑) รายงานการแจ้งเตือนภัยคุกคามด้านความมั่นคงปลอดภัย สำหรับเหตุการณ์ที่อยู่ในขอบข่ายภัยคุกคามทางไซเบอร์ โดยมีรายละเอียดการแจ้งเตือน ตามข้อ ๔.๑๔

๒) รายงานผลการดำเนินการจัดเก็บและวิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์และสรุปผลการดำเนินการเฝ้าระวังภัยคุกคาม ตามข้อ ๔.๑๕

๓) รายงานข้อมูลข่าวสารซึ่งเกี่ยวข้องกับระบบรักษาความปลอดภัยทางไซเบอร์ ตามข้อ ๔.๑๖

ในรูปแบบของเอกสารและไฟล์ ภายในวันที่ ๓๐ มิถุนายน ๒๕๖๘ และคณะกรรมการตรวจรับพัสดุได้ตรวจรับเรียบร้อยแล้ว

งวดที่ ๔ (๑-๓๑ ก.ค.๖๘) เป็นเงินจำนวน ๕๑,๙๘๐ บาท (ห้าหมื่นหนึ่งพันหกร้อยแปดสิบบาทถ้วน) เมื่อผู้รับจ้างได้ส่งมอบงาน ดังนี้

๑) รายงานการแจ้งเตือนภัยคุกคามด้านความมั่นคงปลอดภัย สำหรับเหตุการณ์ที่อยู่ในขอบข่ายภัยคุกคามทางไซเบอร์ โดยมีรายละเอียดการแจ้งเตือน ตามข้อ ๔.๑๔

๒) รายงานผลการดำเนินการจัดเก็บและวิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์และสรุปผลการดำเนินการเฝ้าระวังภัยคุกคาม ตามข้อ ๔.๑๕

๓) รายงานข้อมูลข่าวสารซึ่งเกี่ยวข้องกับระบบรักษาความปลอดภัยทางไซเบอร์ ตามข้อ ๔.๑๖

ในรูปแบบของเอกสารและไฟล์ ภายในวันที่ ๓๑ กรกฎาคม ๒๕๖๘ และคณะกรรมการตรวจรับพัสดุได้ตรวจรับเรียบร้อยแล้ว

งวดที่ ๕ (๑-๓๑ ส.ค.๖๘) เป็นเงินจำนวน ๕๑,๙๘๐ บาท (ห้าหมื่นหนึ่งพันหกร้อยแปดสิบบาทถ้วน) เมื่อผู้รับจ้างได้ส่งมอบงาน ดังนี้

๑) รายงานการแจ้งเตือนภัยคุกคามด้านความมั่นคงปลอดภัย สำหรับเหตุการณ์ที่อยู่ในขอบข่ายภัยคุกคามทางไซเบอร์ โดยมีรายละเอียดการแจ้งเตือน ตามข้อ ๔.๑๔

๒) รายงานผลการดำเนินการจัดเก็บและวิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์และสรุปผลการดำเนินการเฝ้าระวังภัยคุกคาม ตามข้อ ๔.๑๕

๓) รายงานข้อมูลข่าวสารซึ่งเกี่ยวข้องกับระบบรักษาความปลอดภัยทางไซเบอร์ ตามข้อ ๔.๑๖

ในรูปแบบของเอกสารและไฟล์ ภายในวันที่ ๓๑ สิงหาคม ๒๕๖๘ และคณะกรรมการตรวจรับพัสดุได้ตรวจรับเรียบร้อยแล้ว

งวดที่ ๖ (๑-๓๐ ก.ย.๖๘) เป็นเงินจำนวน ๕๒,๐๒๖.๔๐ บาท (ห้าหมื่นสองพันยี่สิบหกบาทสี่สิบสตางค์) เมื่อผู้รับจ้างได้ส่งมอบงาน ดังนี้

๑) รายงานการแจ้งเตือนภัยคุกคามด้านความมั่นคงปลอดภัย สำหรับเหตุการณ์ที่อยู่ในขอบข่ายภัยคุกคามทางไซเบอร์ โดยมีรายละเอียดการแจ้งเตือน ตามข้อ ๔.๑๔

๒) รายงานผลการดำเนินการจัดเก็บและวิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์และสรุปผลการดำเนินการเฝ้าระวังภัยคุกคาม ตามข้อ ๔.๑๕

๓) รายงานข้อมูลข่าวสารซึ่งเกี่ยวข้องกับระบบรักษาความปลอดภัยทางไซเบอร์ ตามข้อ ๔.๑๖

ในรูปแบบของเอกสารและไฟล์ ภายในวันที่ ๓๐ กันยายน ๒๕๖๘ และคณะกรรมการตรวจรับพัสดุได้ตรวจรับเรียบร้อยแล้ว

๙. อัตราค่าปรับ

อัตราค่าปรับเป็นรายวัน ในอัตราร้อยละ ๐.๑๐ ของราคาค่าจ้าง

๑๐. การกำหนดระยะเวลารับประกันความชำรุดบกพร่อง

๑๐.๑ ระยะเวลาในการแก้ไขผลงาน/รายงาน ภายใน ๗ วัน นับถัดจากวันที่ได้รับแจ้งเป็นลายลักษณ์อักษรจากทางผู้ว่าจ้าง

๑๐.๒ ผู้ว่าจ้างสามารถขอรับคำปรึกษาด้านเทคนิคในการรับมือเหตุการณ์ภัยคุกคามที่เกิดขึ้นทางโทรศัพท์ ได้โดยไม่จำกัดจำนวนครั้งตลอด ๒๔ ชั่วโมง ตลอดระยะเวลาสัญญา

๑๐.๓ ผู้ยื่นข้อเสนอจะต้องให้บริการเฝ้าระวังภัยคุกกคามทางไซเบอร์เป็นระยะเวลา ๖ เดือน

๑๐.๔ ผู้ยื่นข้อเสนอต้องมีการแจ้งเตือนให้แก่ผู้ว่าจ้างภายในระยะเวลา ๖ ชั่วโมง เมื่อตรวจพบอุปกรณ์ต้นทางหยุดส่งข้อมูลจราจรทางคอมพิวเตอร์เป็นเวลา ๒๔ ชั่วโมงขึ้นไป

พ.ต.ท. ..... ประธานกรรมการ
(ปริญญา คำเบ้าเมือง)
รอง ผกก.วบ.บก.อก.รพ.ตร.

พ.ต.ต.หญิง ..... กรรมการ
(ดาราพร สำเร็จพร)
สว.วบ.บก.อก.รพ.ตร.

ว่าที่ ร.ต.อ. ..... กรรมการ
(เรืองวิทย์ นางแย้ม)
รอง สว.วบ.บก.อก.รพ.ตร.

CYBER ELITE CO., LTD.

..... ผู้รับจ้าง

..... พยาน

Quotation

CYBER ELITE

บริษัท ไซเบอร์ อีลีท จำกัด (สำนักงานใหญ่)
499 ตึกเบญจจินดา, ถนนกำแพงเพชร 6 ,แขวงลาดยาว, เขตจตุจักร, กรุงเทพ 10900,

ข้อมูลลูกค้า

ลูกค้า : โรงพยาบาลตำรวจ

ถึง :
บริษัท :โรงพยาบาลตำรวจ
ที่อยู่: โรงพยาบาลตำรวจ
ถนนพระราม 1 แขวงปทุมวัน เขตปทุมวัน
กรุงเทพมหานคร 10330
Email:
Mobile:

Provider Information

Quotation SQ24090074
Date: 27/03/2568
Validity: 90 days from quotation date

Salesperson: Nutthaporn Wongchansang

Email: nutthaporn.w@cyberelite.co
Mobile: 0870204500

Item	Part Number / Type of Service	Description	Quantity (Unit)	One-time Expense (THB)	Monthly Fee (THB)	Amount (THB)
1		**โครงการจ้างวิเคราะห์ เฝ้าระวังและการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับ รพ.ตร.** **บริการจ้างวิเคราะห์ เฝ้าระวังและการรักษาความมั่นคงปลอดภัยไซเบอร์ 10 GB/วัน (CSOC Service)** ระยะเวลาเริ่มต้น 1 เมษายน 2568 สิ้นสุด 30 กันยายน 2568 รายละเอียดการบริการ เก็บข้อมูล10 GB/วัน (Logger 10 GB/DAY) • เก็บข้อมูลย้อนหลัง 90 วัน (Log Retention 90 Day) • ค้นหาข้อมูลแบบออนไลน์ (Online Search 30 Day) • รายงาน รายเดือน (Monthly Report) • การเฝ้าระวังแบบ 24X7 • สรุปผล Incident Report • ข่าวด่วน Cyber Security o Unlimited Call/E-Mail for incidents o Channel Support: Call 02-016-5678 # 8 o E-Mail: csoc@cyberelite.co.th o SOC ประชุมรายเดือน รวมอุปกรณ์แม่ข่ายสำหรับเก็บข้อมูล	6		34,920.00	209,520.00
2		**บริการตรวจสอบช่องโหว่ ของระบบ จำนวน 10 IP (Vulnerability Assessment with report 10 IP)** ** scan รอบเดียวและส่ง รายงาน	1	82,000.00		82,000.00
		สามแสนหนึ่งหมื่นหนึ่งพันเก้าร้อยยี่สิบหกบาทสี่สิบสตางค์	**Total** **7% VAT** **Grand Total**			**291,520.00** **20,406.40** **311,926.40**

เงื่อนไขเฉพาะสำหรับบริการรักษาความปลอดภัย

1. ลูกค้าจะต้องไม่ก่อให้เกิดอันตรายใดๆ ต่อบุคคลที่สาม และจะต้องไม่ละเมิดพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์หรือกฎหมายอื่นๆ ที่บังคับใช้
2. บริษัทตกลงที่จะรักษาความลับของข้อมูลของลูกค้า/ผู้ใช้บริการ เว้นแต่กฎหมายกำหนดไว้
3.ใบการซื้อผลิตภัณฑ์และบริการใดๆ ที่เกี่ยวข้องกับซอฟต์แวร์และใบอนุญาต ลูกค้า/ผู้ใช้รับทราบว่าบริษัทไม่ได้เป็นเจ้าของซอฟต์แวร์/ใบอนุญาตดังกล่าว
เมื่อบริษัทดำเนินการตามคำขอบริการหรือลงทะเบียนกับเจ้าของใบอนุญาตตามใบเสนอราคา/คำขอบริการแล้ว ลูกค้า/ผู้ใช้ไม่สามารถยกเลิก เพิกถอน และ/หรือโอนสิทธิ์ให้กับหน่วยงานใดๆ
ภายใต้เงื่อนไขการให้สิทธิ์ ลูกค้า/ผู้ใช้จะต้องชำระค่าซอฟต์แวร์/สิทธิ์การใช้งานดังกล่าวเต็มจำนวน ไม่ว่าลูกค้า/ผู้ใช้จะใช้ผลิตภัณฑ์ที่ได้รับอนุญาตหรือไม่ก็ตาม

เอกสารประกอบการขอใช้บริการ
1. หนังสือรับรองของบริษัทออกให้ไม่เกิน 90 วัน
2. สำเนาบัตรประจำตัวกรรมการผู้มีอำนาจลงนาม
3. สำเนาใบทะเบียนภาษีมูลค่าเพิ่ม (ภ.พ.20)
4. หนังสือมอบอำนาจ (ถ้ามี)

Signed by company director(s) and affixed with company seal.
Signed by company director(s) and affixed with company seal (for each director)
Signed by company director(s) and affixed with company seal.
Signed by company director(s) and affixed with company seal.

Payment Terms
ตามข้อกำหนดของโครงการ

For Customer	For Service Provider
Confirm Service activation and product / Service purchase under the aforementioned pricing and conditions.	Proposed / Approver
Signed _____ Customer (.....) Position.....(Company Seal)	(Nutthaporn Wongchansang) Head Of Key Account Management Division Cyber Elite Co., Ltd. (Jirad Kachanunyanuwut) Director Of Key Account Management Department Cyber Elite Co., Ltd.

RV1/2022

RV1/2022

CYBER ELITE CO., LTD.

..... ผู้รับจ้าง

..... พยาน

CYBER ELITE CO., LTD.

ชั้นความลับ / สำหรับ โรงพยาบาลตำรวจเท่านั้น

CYBER ELITE

โครงการจ้างวิเคราะห์ เฝ้าระวังและการรักษาความมั่นคงปลอดภัย ไซเบอร์ สำหรับโรงพยาบาลตำรวจ

ข้อเสนอทางเทคนิค

(TECHNICAL PROPOSAL)

สถานะเอกสาร:	อนุมัติ
อนุมัติโดย:	นิติพัฒน์ อภิจิรวัฒน์
วันที่อนุมัติ:	๒๔ มีนาคม ๒๕๖๘
ผู้เขียน:	นาย พงศกร เจริญศรี
ครั้งที่ปรับปรุง:	๑.๐
วันที่ปรับปรุง:	๒๔ มีนาคม ๒๕๖๘

..... ผู้รับจ้าง

..... พยาน

CYBER ELITE CO.,LTD

สารบัญ

CYBER ELITE CO., LTD.

..... ผู้รับจ้าง

..... พยาน

สารบัญรูปภาพ

CYBER ELITE CO., LTD.

..... ผู้รับจ้าง

..... พยาน

ประวัติเอกสาร

วันที่ปรับปรุง	ครั้งที่ปรับปรุง	ผู้เขียน	รายละเอียด
๒๔ มี.ค. ๖๘	๑.๐A	พงศกร เจริญศรี	แบบร่างเอกสาร ครั้งที่ ๑
๒๔ มี.ค. ๖๘	๑.๐A	พงศกร เจริญศรี	ปรับปรุงแบบร่างเอกสาร ครั้งที่ ๑
๒๔ มี.ค. ๖๘	๑.๐	นิติพัฒน์ อภิจิรวัฒน์	Baseline

ข้อกำหนดทั่วไป

คำนิยามในเอกสารข้อเสนอฉบับนี้ ข้อความต่าง ๆ จะมีความหมายตามคำอธิบายดังต่อไปนี้

“บริษัทฯ”	หมายถึง	บริษัท ไซเบอร์ อีลีท จำกัด
“โรงพยาบาลฯ”	หมายถึง	โรงพยาบาลตำรวจ
“โครงการฯ”	หมายถึง	โครงการจ้างวิเคราะห์ เฝ้าระวังและการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับโรงพยาบาลตำรวจ

CYBER ELITE CO., LTD.

..... ผู้รับจ้าง

..... พยาน

๑. ข้อมูลเบื้องต้นของบริษัท ไซเบอร์ อีลีท จำกัด (CYBER ELITE)

บริษัท ไซเบอร์ อีลีท จำกัด (CYBER ELITE) เป็นบริษัทฯ ที่มีประสบการณ์ทางด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ซึ่งได้รวบรวมผู้ที่มีประสบการณ์ด้านต่าง ๆ ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์รวมกัน โดยบุคลากรของบริษัทฯ มีประสบการณ์ทั้งในด้านของ Consultants, Implementers, Advisors, Instructors, Researchers รวมถึง Service Providers ด้วย

โดยบริษัทฯ อยู่ภายใต้กลุ่มเบญจจินดา ซึ่งเป็นกลุ่มบริษัท ที่ดำเนินธุรกิจให้บริการสื่อสารโทรคมนาคม เทคโนโลยีสารสนเทศภายใต้การบริหารและดำเนินงานโดยทีมงานที่มีประสบการณ์ในธุรกิจมายาวนานกว่า ๗๐ ปี ด้วยปณิธานมุ่งมั่นที่จะใช้ประสบการณ์ในการบริหารพัฒนาธุรกิจต่าง ๆ ให้มีประสิทธิภาพและเติบโตควบคู่ไปกับความก้าวหน้าของประเทศ และในปี พ.ศ. ๒๕๕๑ **บริษัท เบญจจินดา โฮลดิ้ง จำกัด** ได้บรรลุเกียรติยศสูงสุดได้รับพระราชทานแต่งตั้ง (ตราครุฑ) โดยได้รับพระบรมราชานุญาตจากพระบาทสมเด็จพระเจ้าอยู่หัว (รัชกาลที่ ๙) โดยธุรกิจของกลุ่มมีทั้งหมด ๔ ธุรกิจ ดังนี้

๑. กลุ่มธุรกิจ DIGITAL INFRASTRUCTURE AND DIGITAL SOLUTION SI BUSINESS ประกอบด้วยบริษัท

- **บริษัท ไซเบอร์ อีลีท จำกัด (CYBER ELITE)**
- บริษัท ยูไนเต็ด เทเลคอม เซลส์ แอนด์ เซอร์วิสเซส จำกัด (UTEL)
- บริษัท เบรนเนอร์จี้ จำกัด (Brainergy)
- บริษัท ยูไนเต็ด เทคโนโลยี เอ็นเตอร์ไพรส์ จำกัด (UTE)
- บริษัท ยูไนเต็ด อินฟอร์เมชั่น ไฮเวย์ จำกัด (UIH)
- บริษัท คลาวด์ เอชเอ็ม จำกัด (Cloud HM)
- บริษัท บีบี เทคโนโลยี จำกัด (BBTEC)

๒. กลุ่มธุรกิจ DISTRIBUTION AND FULFILLMENT SERVICE ประกอบด้วยบริษัท

- บริษัท วายเอ เซลส์ แอนด์ เซอร์วิสเซส จำกัด (YAS)
- บริษัท ยูไนเต็ด ดิสทริบิวชั่น บิซซิเนส จำกัด (UD)

๓. กลุ่มธุรกิจ CONTENT BUSINESS ประกอบด้วยบริษัท

- บริษัท สำนักข่าว ไอ.เอ็น.เอ็น.จำกัด (INN)
- บริษัท รักบ้านเกิด จำกัด (Rakbankerd)

๔. กลุ่มธุรกิจ INVESTMENT BUSINESS ประกอบด้วยบริษัท

- บริษัท บีซีเอช เวนเจอร์ส จำกัด (BCH VENTURES)

..... ผู้รับจ้าง

..... พยาน

CYBER ELITE CO., LTD.

ด้านบุคลากร

ในด้านบุคลากร บริษัทฯ มีนโยบายมุ่งส่งเสริมให้บุคลากรของบริษัทฯ ได้เข้ารับการอบรม เพื่อพัฒนาศักยภาพ, ความรู้ความสามารถ และเข้าร่วมการทดสอบด้านความปลอดภัยสารสนเทศ (Information Security) โดยในปัจจุบัน บริษัทฯ มีบุคลากรซึ่งได้รับการรับรองมาตรฐานความรู้ความสามารถทางด้านระบบเครือข่าย และความปลอดภัยคอมพิวเตอร์ โดยหน่วยงานในระดับสากล เช่น CISSP, CSSLP, CISA, CISM, CDPSE, CDPO, CCISO, GIAC GWAPT, ECSA, CEH, CHFI, ECES, ENSA, CSCU, CEI, CSIE, CSAE, CASP+, CySA+, Security+, Pentest+, Network+, CTT+, CNVP, CSAP, CNSP, IRCA ISO๒๗๐๐๑ PA, PECB ISO ๒๗๐๐๑ SLI, PECB ISO๒๗๐๐๑ LI, PECB ISO๒๒๓๐๑ PI, PECB ISO๓๑๐๐๐ RM, ITILv๓ Foundation เป็นต้น นอกจากนี้บริษัทฯ มีศูนย์ Cybersecurity Operation Center (CSOC) ที่ได้รับการรับรองมาตรฐาน ISO/IEC ๒๗๐๐๑ Information security management systems และ ISO/IEC ๒๗๗๐๑ Privacy Information Management รวมถึงทางบริษัทฯ ได้การรับรองมาตรฐาน ISO/IEC ๒๙๑๑๐ - Software Development Process Standard ให้มีการบริหารจัดการคุณภาพและบริการด้านซอฟต์แวร์ที่มีประสิทธิภาพและมีศักยภาพ

OUR ELITE TEAM

Our team has over 20 years of experience in cybersecurity as consultants, implementers, advisors, instructors, researchers, and service providers in various industries.

Financial	Telecom	Insurance
Retail	Healthcare	Government
Energy	Defense	National CERT
Leasing	Manufacuring	Entertainment

OUR CERTIFICATIONS

CISSP | CSSLP | CISA | CISM | CDPSE | CDPO | CCISO | GIAC GWAPT | ECSA | CEH | CHFI | ECES | ENSA | CSCU | CEI | CSIE | CSAE | CASP+ | CySA+ | Security+ | Pentest+ | Network+ | CTT+ | CNVP | CSAP | CNSP | IRCA ISO27001 PA | PECB ISO27001 SLI | PECB ISO27001 LI | PECB ISO22301 PI | PECB ISO31000 RM | ITILv3 Foundation

ISO 29110 Certified

Our Cybersecurity Operations Center (CSOC) is 27001 and 27701 certified

รูปที่ 0-1 บุคลากรซึ่งได้รับการรับรองมาตรฐานโดยหน่วยงานในระดับสากล

..... ผู้รับจ้าง

..... พยาน

๒. ข้อมูลการติดต่อกับบริษัทฯ

ในกรณีที่ “โรงพยาบาลตำรวจ” มีความประสงค์ต้องการสอบถาม หรือทราบข้อมูลเพิ่มเติมเกี่ยวกับการดำเนินงานตามข้อเสนอโครงการ “โครงการจ้างวิเคราะห์ เฝ้าระวังและการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับโรงพยาบาลตำรวจ” สามารถติดต่อกับบริษัทฯ ได้โดยใช้ข้อมูลสำหรับการติดต่อ ดังนี้

บริษัท ไซเบอร์ อีลีท จำกัด
เลขที่ ๔๙๙ อาคารเบญจจินดา ถนนกำแพงเพชร ๖ แขวงลาดยาว เขตจตุจักร กรุงเทพมหานคร
โทรศัพท์ ๐๒-๐๑๖-๕๑๔๓
www.cyberelite.co.th

ผู้ประสานงานโครงการ (Contact Point)
คุณ ณัฐพร วงค์จันทร์แสง
โทรศัพท์เคลื่อนที่: ๐๘๗-๐๒๐-๔๕๐๐
อีเมล: nutthaporn_w@cyberelite.co

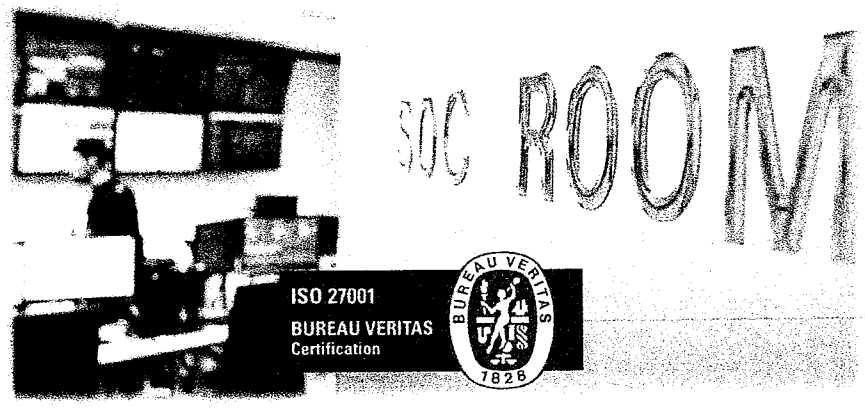
หน่วยงานให้ข้อมูลและคำแนะนำเบื้องต้น (SOC Helpdesk Support)
โทรศัพท์: ๐๒-๐๑๖๕๖๗๘ # ๘
อีเมล: csoc@cyberelite.co.th

..... ผู้รับจ้าง
..... พยาน

๓. รายละเอียดข้อเสนอ (PROPOSED SOLUTION)

ทางบริษัท ไซเบอร์ อีลีท จำกัด มีบุคลากรประจำศูนย์ CSOC ที่ได้รับการฝึกอบรม เพื่อพัฒนาศักยภาพ ความรู้ความสามารถ สำหรับการตรวจสอบ เฝ้าระวังภัยคุกคาม รวมถึงการรับมือภัยคุกคามทางไซเบอร์ (Incident Response) เผื่อยับยั้งภัยคุกคามทางไซเบอร์ในรูปแบบต่าง ๆ ที่เกิดขึ้น ในปัจจุบัน บริษัทฯ มีบุคลากรซึ่งได้รับการรับรองมาตรฐานความรู้ความสามารถทางด้านระบบเครือข่าย และความปลอดภัยคอมพิวเตอร์ โดยหน่วยงานในระดับสากลโดยนำเสนอบริการและโซลูชัน (Solutions) สำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยมีศูนย์ปฏิบัติการ Cyber Security Operations Center (CSOC) ดูแลตลอด ๒๔ ชั่วโมง ซึ่งเมื่อใดที่มีการตรวจพบเจอสิ่งผิดปกติ ทางศูนย์ CSOC ก็จะส่งการแจ้งเตือนดังกล่าว เพื่อให้สามารถแก้ไขปัญหาได้ทันท่วงที พร้อมด้วยความหลากหลายของบริการด้าน Security ที่มีให้เลือกตามความต้องการให้เหมาะสมกับแต่ละธุรกิจ

บริการจัดเก็บและบริหารจัดการข้อมูลจราจรทางคอมพิวเตอร์แบบรวมศูนย์ หรือระบบ Centralized Log Management ที่ได้มาตรฐาน เป็นระยะเวลา ๙๐ วัน การจัดเก็บข้อมูล Log ไว้ที่ระบบศูนย์กลางจะทำให้การดูแล และตรวจสอบเป็นไปได้ง่ายยิ่งขึ้น โดยมีระบบ Backup เพื่อป้องกัน Log สูญหาย และเสริมความปลอดภัยอีกขั้นด้วยระบบป้องกันการเปลี่ยนแปลงข้อมูล Log หรือการพยายามลบ Log ทิ้งโดยผู้ไม่หวังดีที่ต้องการบิดเบือนข้อมูล พร้อมรองรับปริมาณข้อมูลจราจรทางคอมพิวเตอร์โดยไม่จำกัดจำนวนอุปกรณ์กำเนิดข้อมูลจราจรทางคอมพิวเตอร์ (Log Source) และทางบริษัทฯ ได้รับรองมาตรฐาน ISO/IEC ๒๗๐๐๑ ตามภาคผนวก ก. เอกสารรับรองมาตรฐานสากลและมีความพร้อมในการให้บริการเฝ้าระวังและแจ้งเตือนเหตุการณ์ภัยคุกคามให้แก่ทาง โรงพยาบาลฯ ตลอด ๗ วัน ๒๔ ชั่วโมง (๗ x ๒๔)



รูปที่ ๓-1 ศูนย์ปฏิบัติการความมั่นคงปลอดภัย

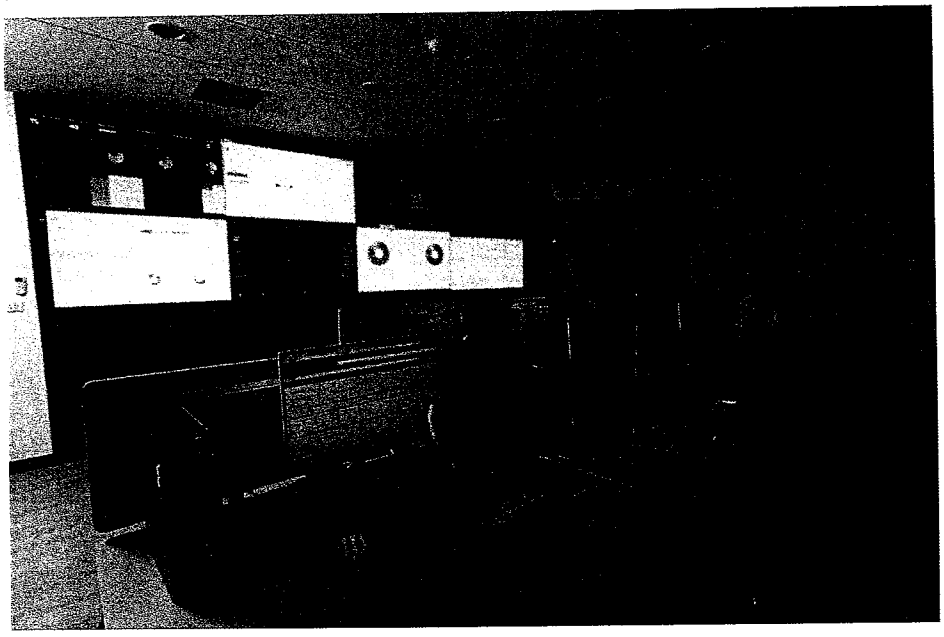
..... ผู้รับจ้าง

..... พยาน

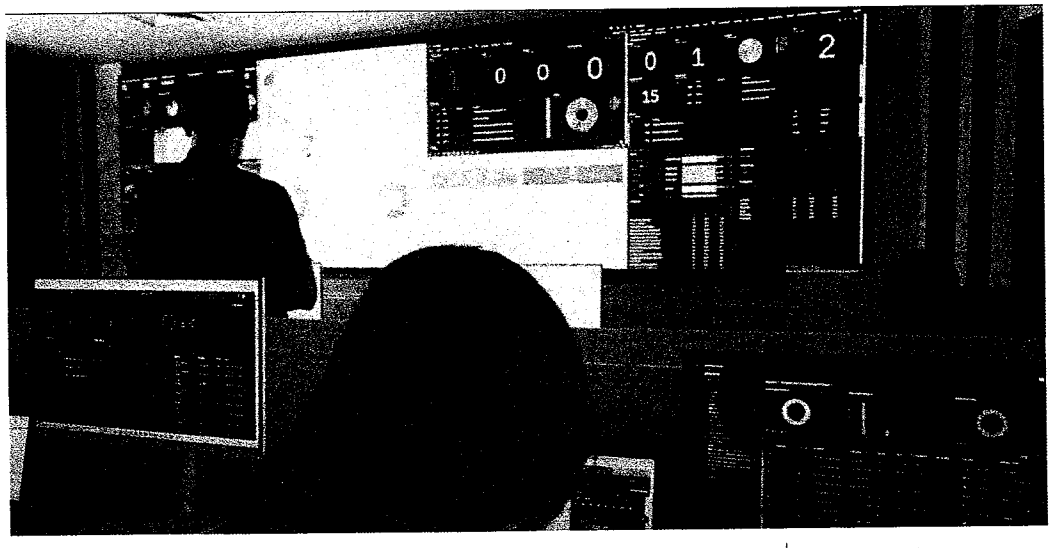
CYBER ELITE CO., LTD

๓.๑ ข้อมูลทั่วไปของ Cyber Elite Cybersecurity Operations Center (CSOC)

ศูนย์ Cybersecurity Operations Center (CSOC) ของบริษัทฯ ตั้งอยู่ในประเทศไทย และมีศูนย์ปฏิบัติการสำรองอีกหนึ่งแห่ง จึงมั่นใจได้ว่าข้อมูลสำคัญของทาง โรงพยาบาลฯ จะไม่ถูกส่งออกนอกประเทศ และการบริหารจัดการรักษาความปลอดภัยของระบบสามารถดำเนินการเฝ้าระวังภัยคุกคามทางไซเบอร์เป็นไปอย่างต่อเนื่อง



รูปที่ ๓-๒ ภาพระหว่างการทำงานภายในศูนย์ปฏิบัติการความมั่นคงปลอดภัย



รูปที่ ๓-๓ ภาพระหว่างการทำงานภายในศูนย์ปฏิบัติการความมั่นคงปลอดภัย

..... ผู้รับจ้าง

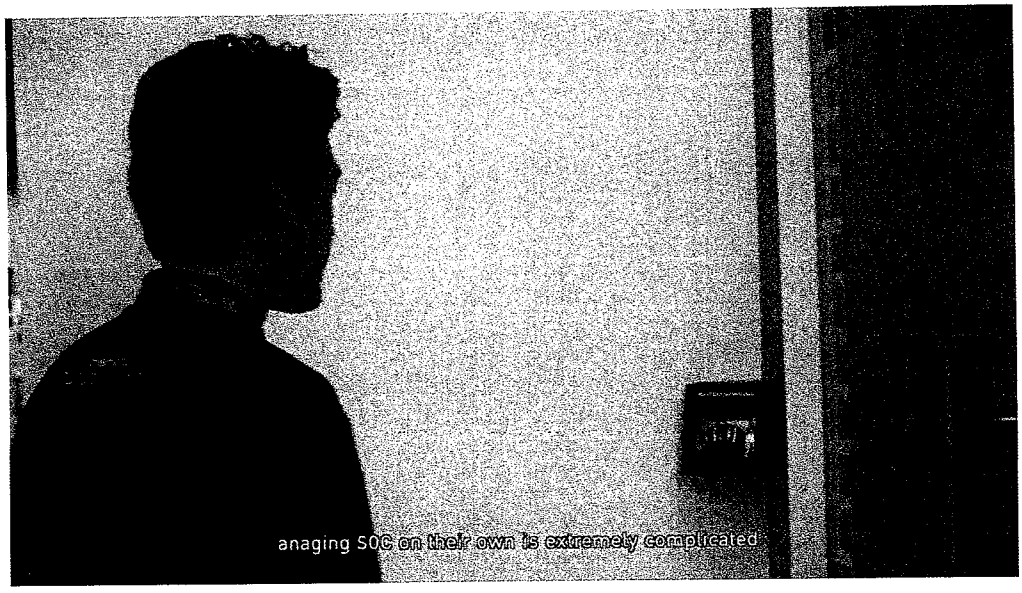
..... พยาน

๓.๒ คุณสมบัติด้านเทคนิคของศูนย์ปฏิบัติการ CSOC

๓.๒.๑ มีศูนย์ปฏิบัติการ CSOC สามารถดำเนินงานได้ตลอด ๒๔ ชั่วโมง ๗ วันต่อสัปดาห์โดยมีผู้เชี่ยวชาญปฏิบัติงานประจำตลอด ๒๔ ชั่วโมง

๓.๒.๒ ศูนย์ปฏิบัติการ CSOC ได้รับมาตรฐาน ISO ๒๗๐๐๑ และ ISO ๒๗๗๐๑ สำหรับศูนย์ปฏิบัติการเฝ้าระวังภัยคุกคามระบบเทคโนโลยีสารสนเทศ (Security Operations Centre: SOC)

๓.๒.๓ ศูนย์ปฏิบัติการ CSOC มีระบบควบคุมการเข้าถึง รูปแบบการยืนยันตัวด้วยข้อมูลชีวภาพ (Biometric Access control)

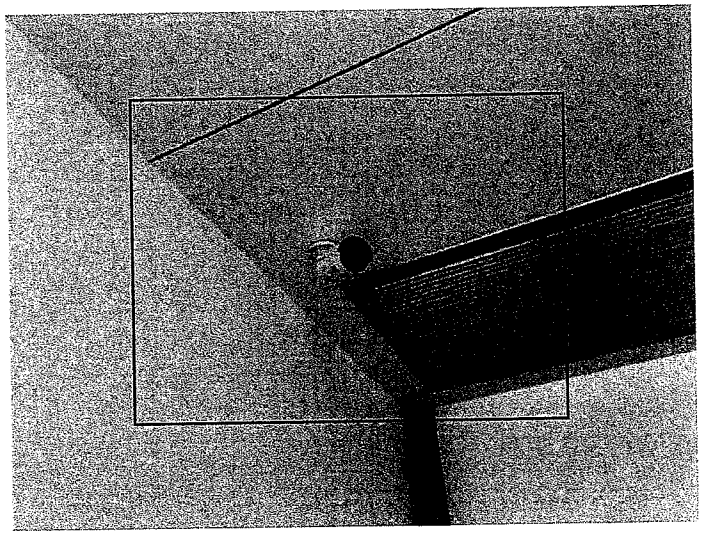


รูปที่ ๓-๔ ระบบควบคุมการเข้าถึง รูปแบบการยืนยันตัวด้วยข้อมูลชีวภาพ (Biometric Access control)

๓.๒.๔ มีระบบกล้องวงจรปิด CCTV สำหรับตรวจสอบการปฏิบัติงานและสามารถดูภาพย้อนหลังได้ โดยจัดเก็บข้อมูลไม่น้อยกว่า ๙๐ วันนับตั้งแต่วันที่ข้อมูลเข้าสู่ระบบคอมพิวเตอร์

ผู้รับจ้าง

พยาน



รูปที่ ๓-๕ ระบบกล้องวงจรปิด CCTV ของศูนย์ปฏิบัติการความมั่นคงปลอดภัย

๓.๒.๕ มีแผนความต่อเนื่องธุรกิจ (Business Continuity plan) และมีศูนย์ปฏิบัติการสำรองที่สามารถทำงานทดแทนได้ทันทีในกรณีที่ศูนย์ปฏิบัติการหลักไม่สามารถทำงานได้ตามเอกสารแผนฉุกเฉินเพื่อบริหารความต่อเนื่องทางธุรกิจ ศูนย์ปฏิบัติการความมั่นคงปลอดภัย (Security Operation Center - SOC) ของบริษัท ไซเบอร์ อีลีท (Cyber Elite) จำกัด

หมายเหตุ : บริษัทฯ ขอสงวนสิทธิ์สำหรับการขอข้อมูลการเข้าถึง Access Control และภาพย้อนหลังของการปฏิบัติการสำหรับการเฝ้าระวังภัยคุกคามทางไซเบอร์ของศูนย์ปฏิบัติการความมั่นคงปลอดภัย (Security Operation Center - SOC)

๓.๓ รายละเอียดของ Cyber Elite Cybersecurity Operations Center (CSOC)

๓.๓.๑ มีศูนย์ปฏิบัติการสำรองหรือ Disaster Recovery Site ที่มีระยะห่างไม่น้อยกว่า ๑๐ กิโลเมตร

๓.๓.๑ มีระบบไฟฟ้าสำรองฉุกเฉิน (UPS) เพื่อให้การทำงานของระบบเป็นไปตามปกติ ในกรณีที่เกิดไฟฟ้าขัดข้อง

๓.๔ คุณสมบัติด้านเทคนิคของระบบที่ใช้ในศูนย์ปฏิบัติการ CSOC

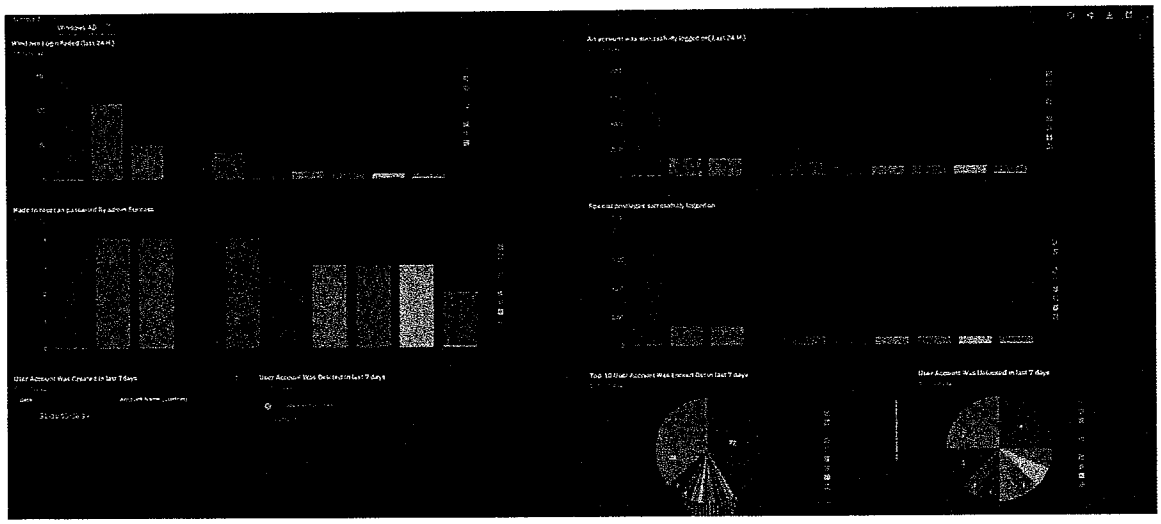
๓.๔.๑ มีศูนย์ปฏิบัติการ CSOC สามารถดำเนินงานได้ตลอด ๒๔ ชั่วโมง ๗ วันต่อสัปดาห์โดยมีผู้เชี่ยวชาญปฏิบัติงานประจำตลอด ๒๔ ชั่วโมง

ผู้รับจ้าง

พยาน

๓.๔.๒ ได้รับมาตรฐาน ISO ๒๗๐๐๑: ๒๐๑๓ และ ISO ๒๗๗๐๑ สำหรับศูนย์ปฏิบัติการเฝ้าระวังภัยคุกคามระบบเทคโนโลยีสารสนเทศ (Security Operations Center: SOC)

๓.๔.๓ มีหน้าจอแสดงผลแบบ Real-time ที่สามารถแสดงผลรายละเอียดเหตุการณ์ภัยคุกคามไซเบอร์ที่เกิดขึ้นในระบบได้พร้อมกันหลายหน้าจอ



รูปที่ ๓-๖ ตัวอย่างหน้าจอแสดงผลที่สามารถแสดงผลรายละเอียดเหตุการณ์ภัยคุกคามไซเบอร์

๓.๔.๔ สามารถตรวจสอบสถานะการทำงานของอุปกรณ์ในการส่งข้อมูลจราจรทางคอมพิวเตอร์มาเชื่อมความสัมพันธ์ (Correlation) ได้

๓.๔.๕ สามารถทำการวิเคราะห์เหตุการณ์ โดยแสดงผลแบบ Real Time เพื่อบอกลำดับเหตุการณ์ต่างๆที่เกี่ยวกับความปลอดภัย (Incidents) โดยสามารถจำแนกระดับของความรุนแรง Critical และ Non-critical ได้

๓.๔.๖ สามารถทำการแจ้งเตือนเมื่อมีเหตุการณ์เสี่ยงภัยหรือเหตุการณ์การบุกรุกระบบที่มีระดับความสำคัญหรือความรุนแรงสูง ผ่านทางอีเมล์ หรือทาง โทรศัพท์

๓.๔.๗ สามารถแสดงสถานะการให้บริการและผลจากการวิเคราะห์เหตุการณ์ที่เกิดขึ้นในระบบจำแนกตามผู้ใช้งานหรือกลุ่มผู้ใช้งานโดยมีข้อมูลอย่างน้อยดังต่อไปนี้

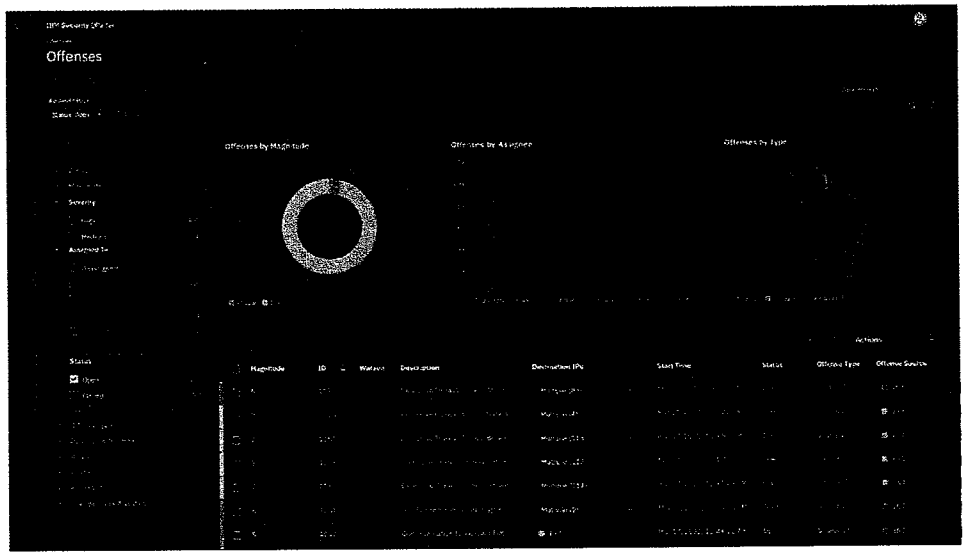
๓.๔.๗.๑ สถานะของการเปิดและปิด tickets

๓.๔.๗.๒ สถานะของ Incidents ที่เกิดขึ้น

๓.๔.๗.๓ ระดับความรุนแรงของ Incidents

ผู้รับจ้าง

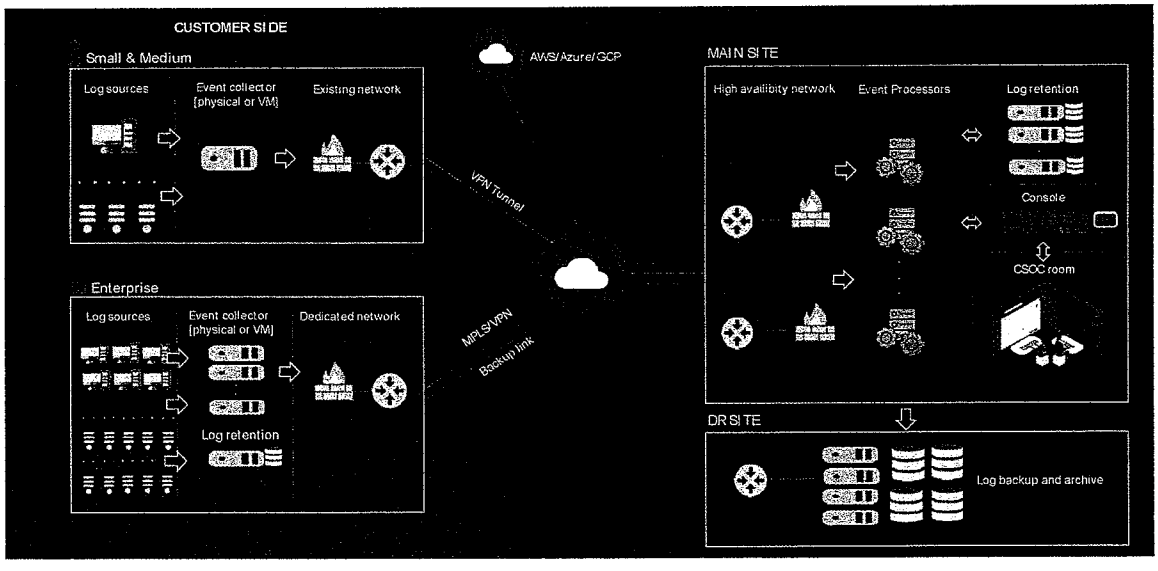
พยาน



รูปที่ ๓-๗ สถานะการให้บริการและผลจากการวิเคราะห์เหตุการณ์

ส่วนที่ ๑ การเตรียมระบบ

๓.๕ บริษัทฯ จัดเตรียมผังการติดตั้งและ Diagram สำหรับการเชื่อมต่อการเฝ้าระวังความมั่นคงปลอดภัยไซเบอร์



รูปที่ ๓-๘ รูปภาพ Diagram แสดงการเชื่อมต่อการเฝ้าระวังความมั่นคงปลอดภัยไซเบอร์

๓.๖ บริษัทฯ จัดเตรียมระบบเฝ้าระวังความมั่นคงปลอดภัยไซเบอร์ที่มีประสิทธิภาพ ซึ่งสามารถจัดเก็บและวิเคราะห์ข้อมูลความปลอดภัยของระบบเครือข่ายขององค์กร ระบบ SIEM ยี่ห้อ IBM QRadar ที่นำเสนอประกอบด้วยการทำงาน ดังต่อไปนี้

ผู้รับจ้าง .....

พยาน .....

๓.๖.๑ ระบบสามารถวิเคราะห์และหาความสัมพันธ์ของข้อมูล เพื่อหาเหตุการณ์ผิดปกติได้

๓.๖.๒ ระบบสามารถปรับแต่งรูปแบบความสัมพันธ์หรือเงื่อนไข (Custom Rule, Playbook) ได้

๓.๖.๓ ระบบสามารถแจ้งเตือนให้ผู้ดูแลระบบทราบ เมื่อตรวจพบข้อมูลที่สอดคล้องกับเงื่อนไขที่ได้ตั้งไว้

๓.๖.๔ ระบบสามารถจัดทำรายงาน หรือสรุปรายงานประจำเดือนได้

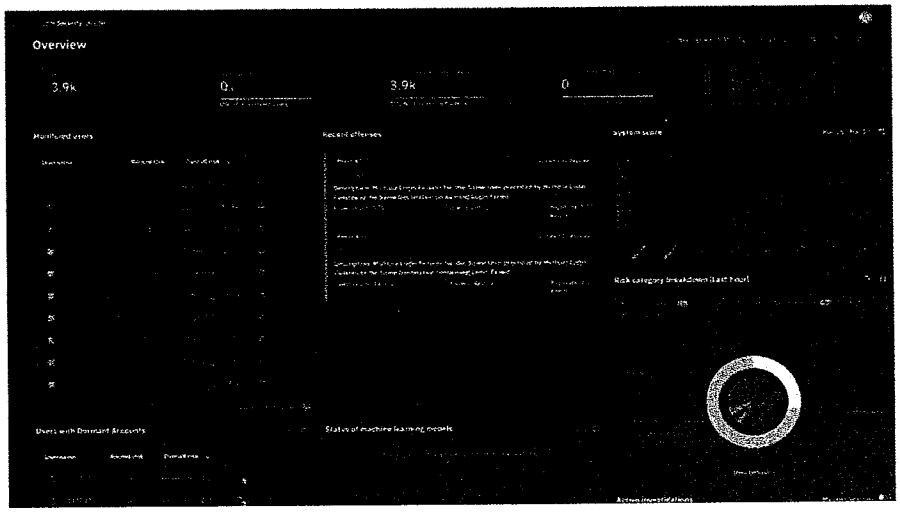
๓.๖.๕ ระบบสามารถบริการจัดการผ่าน Web Interface หรือ GUI ได้เป็นอย่างน้อย

๓.๖.๖ ระบบสามารถกำหนดสิทธิ์การเข้าถึงระบบ ตามระดับสิทธิ์การเข้าถึงได้ (Role Base Access Control)

๓.๖.๗ ระบบเฝ้าระวังมีการแบ่งแยกการทำงานระหว่างระบบรับส่ง (Log collector), ระบบประมวลผล (Processor) และระบบบริหารจัดการที่ส่วนกลาง (Centralized Management) ออกจากกัน

๓.๖.๘ สามารถรับ Feed ข้อมูลจาก Threat Intelligence Source (Opensource & Commercial) และนำมาทำ Threat Collections กับ Log ที่จัดเก็บมาได้โดยอัตโนมัติ

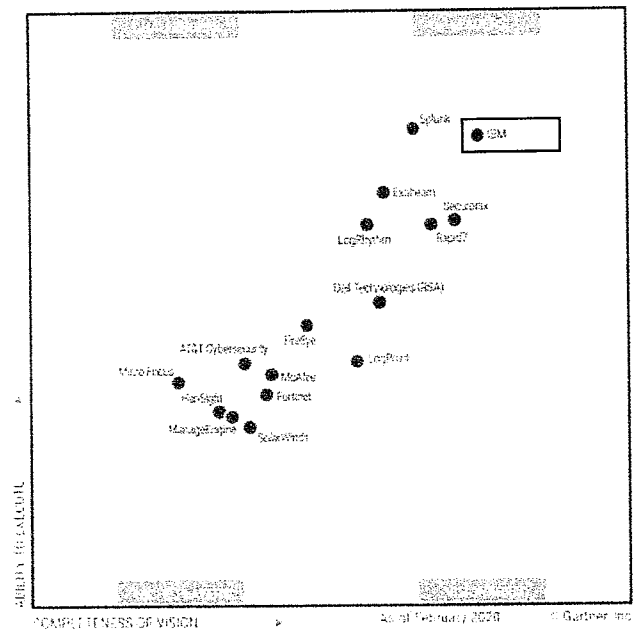
๓.๖.๙ สามารถวิเคราะห์พฤติกรรมผู้ใช้ User Entity behaviour analytics (UEBA) โดยกำหนดความรุนแรงจากพฤติกรรมที่เกิดขึ้นด้วยความสามารถของ Machine leaning ในการวิเคราะห์พฤติกรรม โดยสามารถวิเคราะห์พฤติกรรมที่เป็นภัยคุกคามได้



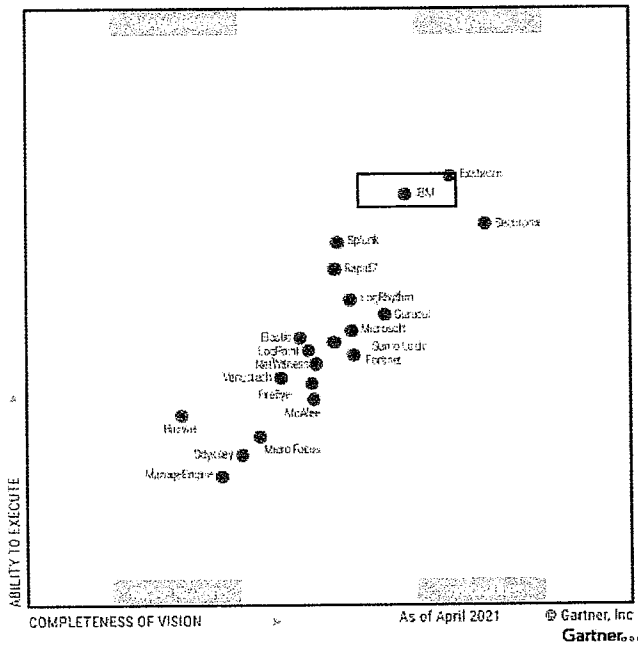
รูปที่ ๓-๙ วิเคราะห์พฤติกรรมผู้ใช้ User behavior analytic (UEBA)

๓.๖.๑๐ ระบบ SIEM ยี่ห้อ IBM Qradar ที่ทางบริษัทฯ เสนอนั้นอยู่ในกลุ่ม Leaders บน Gartner Magic Quadrant for SIEM ตลอด ๓ ปีติดต่อกันตั้งแต่ปี ๒๐๒๐ เป็นต้นมาจนถึงปัจจุบัน ๒๐๒๒

Figure 1. Magic Quadrant for Security Information and Event Management



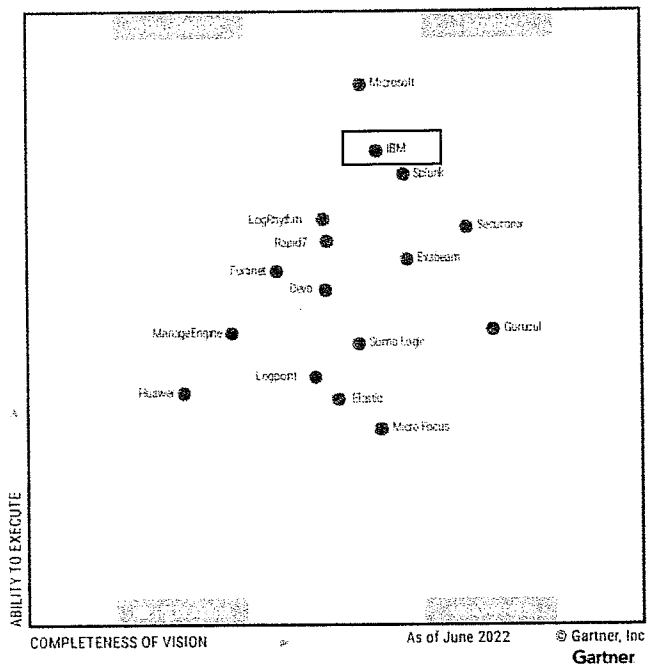
รูปที่ ๓-๑๐ Gartner Magic Quadrant for SIEM ๒๐๒๐



รูปที่ ๓-๑๑ Gartner Magic Quadrant for SIEM ๒๐๒๑

ผู้รับจ้าง

พยาน



รูปที่ ๓-๑๒ Gartner Magic Quadrant for SIEM ๒๐๒๒

๓.๗ ระบบเฝ้าระวังความมั่นคงปลอดภัยไซเบอร์ สามารถรองรับข้อมูลจราจรทางคอมพิวเตอร์ (Log File) ของอุปกรณ์ความปลอดภัยทางด้านเครือข่าย ตามรายการระบบที่ใช้งานอยู่ในปัจจุบัน โดยสามารถรองรับข้อมูล ๑๕ GB/Day และรองรับการเฝ้าระวังตามอุปกรณ์ต่างๆที่ต้องการเฝ้าระวังความมั่งคงปลอดภัยทางไซเบอร์ของทาง โรงพยาบาลฯ ได้

๓.๘ บริษัทฯ ดำเนินการติดตั้งอุปกรณ์จัดเก็บข้อมูล Log (Log Collector) โดยทางบริษัทฯ เป็นผู้จัดหาฮาร์ดแวร์ที่มีประสิทธิภาพและความจุเพียงพอสำหรับรองรับปริมาณข้อมูลจราจรทางคอมพิวเตอร์ โดยมีคุณสมบัติดังต่อไปนี้

๓.๘.๑ ทำหน้าที่รับข้อมูลจราจรจากเครื่องต้นทางมายัง Log Collector ได้

๓.๘.๒ ทำหน้าที่ในการเก็บข้อมูลจราจรคอมพิวเตอร์บนอุปกรณ์ ในกรณีที่เครือข่ายเชื่อมโยงไม่สามารถใช้งานได้ หรือข้อมูลจราจรไม่สามารถส่งไปที่ศูนย์ปฏิบัติการได้ เป็นเวลา ๑ วัน นับจากเวลาที่ไม่สามารถส่งไปที่ศูนย์ปฏิบัติการได้

๓.๘.๓ ทำหน้าที่ในการแจ้งเตือนในกรณีที่ข้อมูลจราจรไม่ส่งมายังตัวอุปกรณ์ได้เพื่อแจ้งไปยังทาง โรงพยาบาลฯ ถัดไป

๓.๘.๔ สามารถติดตั้งบนระบบ Virtual Machine (VMware) ได้

ผู้รับจ้าง

พยาน

๓.๙ บริษัทฯ จัดให้มีผู้เชี่ยวชาญเข้าทำกระบวนการเตรียมพร้อมและส่งผ่านข้อมูลจราจรทางคอมพิวเตอร์เพื่อใช้ในการเฝ้าระวังฯ (On-boarding process) ดังนี้

๓.๙.๑ ตรวจสอบความพร้อมใช้ของระบบและอุปกรณ์ต้นกำเนิดข้อมูลจราจรทางคอมพิวเตอร์ที่จะใช้ในการเฝ้าระวังร่วมกับเจ้าหน้าที่ของ โรงพยาบาลฯ และให้คำแนะนำในการตั้งค่าอุปกรณ์เพื่อให้สามารถส่งข้อมูลจราจรทางคอมพิวเตอร์จากอุปกรณ์ต้นทางไม่ว่าจะเป็น Server, Network, Security และ System อื่นๆ ซึ่งติดตั้งใช้งานที่ศูนย์คอมพิวเตอร์ (Data Center) ได้

๓.๙.๒ ระบุแหล่งที่มาของข้อมูลจราจรทางคอมพิวเตอร์และจัดหมวดหมู่ของอุปกรณ์ต้นกำเนิดและระบุและวิเคราะห์ความเสี่ยง และจัดระดับของผลกระทบต่อระบบของทางโรงพยาบาลฯ รวมทั้งกำหนดประเภทข้อมูลจราจรทางคอมพิวเตอร์ (Log) ที่ต้องใช้ในการวิเคราะห์ร่วมกับทาง โรงพยาบาลฯ

๓.๙.๓ ระบุและวิเคราะห์ความเสี่ยง และจัดระดับของผลกระทบต่อระบบของทาง โรงพยาบาลฯ รวมทั้งกำหนดประเภทข้อมูลจราจรทางคอมพิวเตอร์ (Log) ที่ต้องใช้ในการวิเคราะห์ร่วมกับทาง โรงพยาบาลฯ

๓.๙.๔ จัดทำ Monitoring Use case ให้สอดคล้องกับระบบที่ใช้เฝ้าระวังฯ

๓.๙.๕ จัดทำ Dashboard และ Alert ให้สอดคล้องกับ Monitoring Use case เพื่อใช้ในการแจ้งเตือนและรายงานต่างๆ

๓.๑๐ บริษัทฯเตรียมความพร้อมและจัดเตรียมทีมงานผู้เชี่ยวชาญเพื่อให้คำแนะนำในการออกแบบระบบจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log) เพื่อจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ ณ ศูนย์ข้อมูลหลักของ โรงพยาบาลฯ ให้สอดคล้องตามนโยบายหรือข้อบังคับที่ทาง โรงพยาบาลฯ ต้องปฏิบัติตาม

๓.๑๑ กระบวนการจัดการและการดำเนินงานเมื่อมี Incident เกิดขึ้น

๑) เมื่อระบบ SIEM ทำการตรวจสอบพบสิ่งผิดปกติที่เข้าข่ายภัยคุกคามทางไซเบอร์จะทำการแจ้ง Alert และ ทำการสร้าง incident ticket แล้วส่งข้อมูล incident ticket ไปยังระบบ Ticketing Management

๒) ระบบ Ticketing Management ทำการบันทึก Incident แล้วดำเนินการส่งข้อมูลไปให้ Tier ๑ ทำการแจ้งไปยัง โรงพยาบาลฯ ผ่านช่องทาง E-Mail และ โทรศัพท์ เพื่อให้ทาง โรงพยาบาลฯ ทำการแก้ไข Incident ดังกล่าว เมื่อดำเนินการแก้ไขปัญหาเสร็จเรียบร้อยแล้วแจ้งกลับมายัง Tier ๑ เพื่อทำการแก้ไขปัญหา

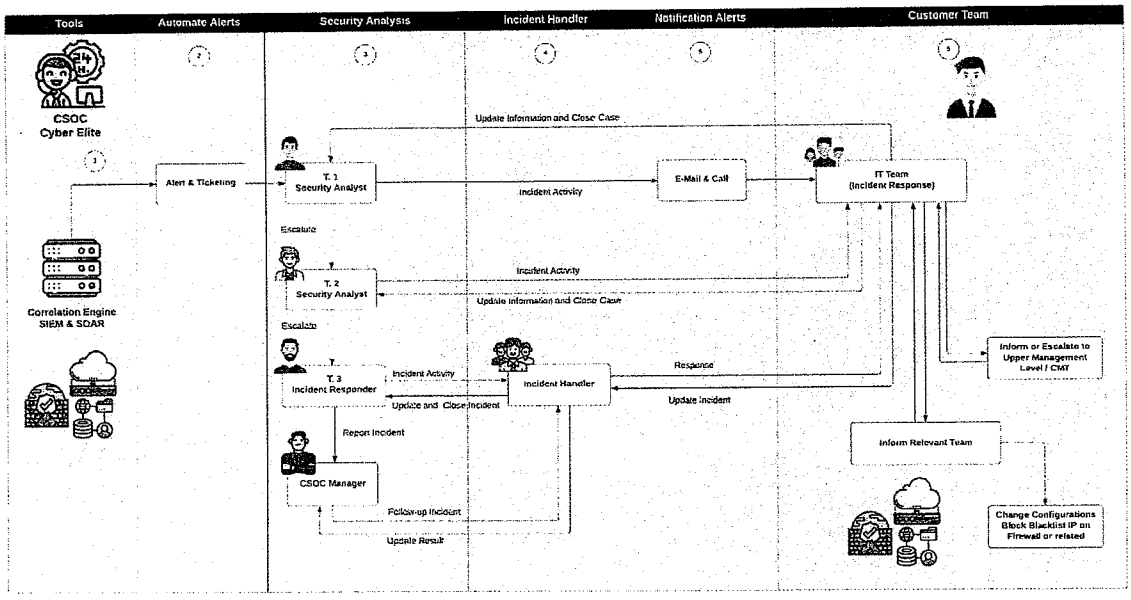
..... ผู้รับจ้าง

.....

๓) หาก Tier ๑ ไม่สามารถทำการวิเคราะห์ปัญหาดังกล่าวได้ จะทำการยกระดับไปยัง Tier ๒ โดย Tier ๒ จะทำการติดต่อประสานงานในการแนะนำแนวทางแก้ไขปัญหาให้กับ โรงพยาบาลฯ

๔) เมื่อ โรงพยาบาลฯ ดำเนินการแก้ไขปัญหาเสร็จเรียบร้อยแล้ว แจ้งกลับมายัง Tier ๒ เพื่อดำเนินการปิดเคสดังกล่าว

๕) หาก Tier ๒ ไม่สามารถทำการวิเคราะห์ปัญหาหรือแนวทางในการแก้ไขหรือต้นเหตุของปัญหาที่เกิดขึ้นได้ จะทำการยกระดับไปยัง Tier ๓ เพื่อดำเนินการแก้ไขปัญหาดังกล่าว จะมีทีม Incident Handler เข้ามาช่วยในการแก้ไขปัญหาจนจบสิ้นกระบวนการ โดยมี CSOC Manager ติดตามอย่างใกล้ชิด



รูปที่ ๓-๑๗ ภาพแสดงการทำงานร่วมกันในกระบวนการ Incident & Ticket Management

๓.๑๒ บริการจัดเก็บและสืบค้นข้อมูลจราจรคอมพิวเตอร์ (Log Management)

๓.๑๒.๑ จัดเก็บข้อมูลจราจรคอมพิวเตอร์ ให้เป็นไปตาม พ.ร.บ. ว่าด้วยการกระทาความผิดเกี่ยว กับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ เป็นระยะเวลา ๙๐ วัน ณ ศูนย์ปฏิบัติการเฝ้าระวังฯ ของทางบริษัทฯ และทำการสืบค้นข้อมูลจราจรคอมพิวเตอร์ตามที่ โรงพยาบาลฯ ร้องขอ โดยมี SLA ดังนี้

Log ที่ร้องขอ	การสืบค้นข้อมูล
น้อยกว่า ๓๐ วัน	ภายใน ๒๔ ชั่วโมง
๓๐ - ๙๐ วัน	ภายใน ๗ - ๑๐ วันทำการ

ผู้รับจ้าง

พยาน

๓.๑๒.๒ บริการตรวจสอบสถานะการส่งข้อมูลจราจรทางคอมพิวเตอร์ พร้อมแจ้งเตือนไปยังเจ้าหน้าที่ที่เกี่ยวข้องของทาง โรงพยาบาลฯ ผ่านทางระบบอีเมล์หรือช่องทางที่ติดต่อได้ หากพบว่าอุปกรณ์ทั้งหมดของ โรงพยาบาลฯ ไม่ส่งข้อมูลมายังสถานที่จัดเก็บข้อมูลของบริษัทฯ

๓.๑๓ ดำเนินงานเฝ้าระวังความมั่นคงปลอดภัยไซเบอร์ วิเคราะห์เหตุการณ์ และแจ้งเตือนภัยคุกคามทางไซเบอร์ให้แก่ โรงพยาบาลฯ ณ ศูนย์ปฏิบัติการ โดยให้บริการแบบตลอดเวลา ๒๔ ชั่วโมงของทุกวัน ไม่มีวันหยุด (๗ x ๒๔) ตลอดระยะเวลาของสัญญา

๓.๑๔ ทางบริษัทฯ แจ้งเตือนภัยคุกคามด้านความมั่นคงปลอดภัย สำหรับเหตุการณ์ที่อยู่ในขอบข่ายภัยคุกคามทางไซเบอร์ โดยจะต้องแจ้งเตือนผ่านทาง Email หรือทางโทรศัพท์ หรือระบบ Ticket Management หรือช่องทางอื่นใด ตามที่ตกลงร่วมกันกับ โรงพยาบาลฯ โดยเป็นไปตาม Service Level Agreement (SLA) อย่างน้อยดังต่อไปนี้

ระดับความรุนแรง	แจ้งเตือนผู้รับบริการ	ให้คำแนะนำในการแก้ไข
วิกฤต	๓๐ นาที	๒ ชั่วโมง
สูง	๑ ชั่วโมง	๔ ชั่วโมง
ตลาง	๔ ชั่วโมง	๘ ชั่วโมง
ต่ำ	รายงานประจำเดือน	รายงานประจำเดือน

๓.๑๕ บริษัทฯ จะทำการการแจ้งเตือนให้กับ โรงพยาบาลฯ มีรายละเอียดดังนี้

๓.๑๕.๑ ระบุประเภทของภัยคุกคาม

๓.๑๕.๒ วัน-เวลา เริ่มต้นของภัยคุกคาม

๓.๑๕.๓ ระบุต้นทาง (Attacker) และปลายทาง (Target)

๓.๑๕.๔ ระบุระดับความรุนแรง (Severity)

๓.๑๕.๕ รายละเอียดเหตุการณ์และพฤติกรรมทั้งหมด

๓.๑๕.๖ คำแนะนำและขั้นตอนการดำเนินการแก้ไขด้านเทคนิค Action & Recommendation

๓.๑๖ บริษัทฯ สามารถวิเคราะห์รูปแบบการตรวจจับเหตุการณ์การคุกคามครอบคลุมในเรื่องดังนี้

๓.๑๖.๑ Unauthorized Access

..... ผู้รับจ้าง

..... พยาน

๓.๑๖.๒ Inappropriate usage

๓.๑๖.๓ Denial of service

๓.๑๖.๔ Information Gathering

๓.๑๖.๕ Malware

๓.๑๖.๖ Suspicious Traffic

๓.๑๖.๗ Vulnerability Scan

๓.๑๖.๘ Lateral movement

๓.๑๗ บริษัทฯ มีทีมงานให้บริการสำหรับการรวบรวมข้อมูลภัยคุกคามทางไซเบอร์ที่มีการปรับปรุงให้ทันสมัยอยู่เสมอจากแหล่งต่างๆ จากทั่วทุกมุมโลก (Threat Intelligence) เพื่อการวิเคราะห์ข้อมูลภัยคุกคามร่วมกับระบบ SIEM หรือ CSOC Technology เพิ่มเติม เพื่อให้ทาง โรงพยาบาลฯ สามารถรับมือกับภัยคุกคามไซเบอร์ได้ อย่างมีประสิทธิภาพมากยิ่งขึ้น

๓.๑๘ บริษัทฯ รายงานผลการดำเนินการจัดเก็บและวิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์และสรุปผลการดำเนินการเฝ้าระวังภัยคุกคามเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศที่เกิดขึ้นโดยมีการวิเคราะห์ ภัยคุกคาม เป็นรายเดือน (Monthly report) ซึ่งมีเนื้อหาดังนี้

๓.๑๘.๑ สรุปเหตุการณ์ตามประเภทและระดับความรุนแรง (Incident Report)

๓.๑๘.๒ รายงานสถิติของการโจมตี

๓.๑๘.๓ รายงานสถิติของเป้าหมายที่โดนโจมตี

๓.๑๘.๔ รายงานสถิติของผู้โจมตี

๓.๑๘.๕ รายงานสถิติของช่องทางที่ถูกใช้โจมตี

๓.๑๘.๖ สรุปปริมาณและสถานะการใช้งานข้อมูลจราจรทางคอมพิวเตอร์ประจำเดือน

๓.๑๙ บริษัทฯ จัดให้มีบริการแจ้งข่าวสารให้กับทาง โรงพยาบาลฯ ที่เกี่ยวข้องกับระบบรักษาความมั่นคงปลอดภัย ระบบคอมพิวเตอร์และระบบเครือข่ายที่เกิดขึ้นผ่านทางอีเมล์ เช่น

๓.๑๙.๑ รายชื่อและคุณลักษณะของมัลแวร์ (Malware)

๓.๑๙.๒ ช่องโหว่ใหม่ (Vulnerability) ของอุปกรณ์ในระบบเครือข่าย (Network Equipment)

๓.๑๙.๓ ช่องโหว่ใหม่ (Vulnerability) ของระบบปฏิบัติการ (Operating System)

๓.๒๐.๔ ช่องโหว่ใหม่ (Vulnerability) ของระบบฐานข้อมูลหลัก (Database)

..... ผู้รับจ้าง

..... พยาน

๓.๒๐ บริษัทฯ จัดเตรียมหน่วยปฏิบัติการตอบสนองต่ออุบัติการณ์ด้านความมั่นคงปลอดภัยทางคอมพิวเตอร์ (CSIRT) พร้อมที่จะปฏิบัติหน้าที่ในการตอบสนองต่อภัยคุกคามหรือการบุกรุกระบบอย่างทันท่วงที เพื่อเข้าดำเนินการสืบสวนและวิเคราะห์หาสาเหตุของปัญหาภัยคุกคามที่เกิดขึ้น รวมถึงการตรวจพิสูจน์พยานหลักฐานทาง Digital เมื่อมีการร้องขอบริการจากทาง โรงพยาบาลฯ ภายในระยะเวลา ๔ ชั่วโมง จำนวนไม่เกินกว่า ๔ เหตุการณ์ต่ออายุสัญญาตามที่ โรงพยาบาลฯ ร้องขอ พร้อมจัดทำรายงานผลการดำเนินงานสรุปข้อมูลหลักฐานต่างๆ ที่ได้จากการตอบสนองต่อเหตุการณ์ภัยคุกคาม รวมถึงแนวทางในการป้องกันการเกิดซ้ำในอนาคต (Incident Response and Recommendations Report)

การตอบสนองต่อเหตุการณ์ภัยคุกคามทางไซเบอร์ โดยการช่วย โรงพยาบาลฯ และประสานงานและให้ความร่วมมือกับทาง ผู้ให้บริการผลิตภัณฑ์ software (Third-party Vendors) หรือเจ้าของผลิตภัณฑ์ (Vendors) เพื่อทำการวิเคราะห์อย่างละเอียดถึงลักษณะที่สำคัญของภัยคุกคามเพื่อให้สามารถแก้ไขสถานการณ์ได้อย่างถูกต้อง และลดความเสี่ยงและผลกระทบที่อาจจะเกิดขึ้นจากการโจมตี รวมถึงทำการหยุดยั้งภัยคุกคามดังกล่าวโดยเร็วที่สุด การทำ Incident Management ที่มีประสิทธิภาพนั้นจะต้องทำการสรุปผลจากเหตุการณ์ต่างๆ ที่ตรวจพบจากหลายแหล่งข้อมูล วิเคราะห์สาเหตุของภัยคุกคาม จัดลำดับความสำคัญของภัยคุกคามจากผลกระทบที่เกิดขึ้นกับ โรงพยาบาลฯ ติดตามเหตุการณ์ของภัยคุกคามจนเสร็จสิ้น และจัดทำวิธีปฏิบัติที่ถูกต้องให้กับ โรงพยาบาลฯเพื่อป้องกันการเกิดซ้ำของเหตุการณ์ การตอบสนองต่อเหตุการณ์ภัยคุกคามของทีม CSIRT แบ่งเป็น ๔ ขั้นตอนคือ

๓.๒๐.๑ Containment: จำกัดพื้นที่ที่เสี่ยงต่อการบุกรุกและจำกัดความรุนแรงของภัยคุกคาม

๓.๒๐.๒ Eradication: กำจัดต้นเหตุของภัยคุกคามรวมถึงปิดกั้นช่องทางของภัยคุกคาม

๓.๒๐.๓ Recovery: แก้ไขระบบที่ถูกภัยคุกคามให้สามารถทำงานได้อย่างปกติ

๓.๒๐.๔ Follow-Up: บันทึกผลกระทบของเหตุการณ์และแนะนำวิธีปฏิบัติเพื่อป้องกันการเกิดซ้ำของเหตุการณ์

๓.๒๑ บริษัทฯจัดเตรียมบริการตรวจสอบช่องโหว่ของอุปกรณ์ทางไซเบอร์หรืออุปกรณ์เครื่องแม่ข่ายหรืออุปกรณ์ระบบเครือข่ายโดยมีรายละเอียดดังนี้

๓.๒๑.๑ ดำเนินการตรวจสอบช่องโหว่จำนวน ๑๐ IP Address

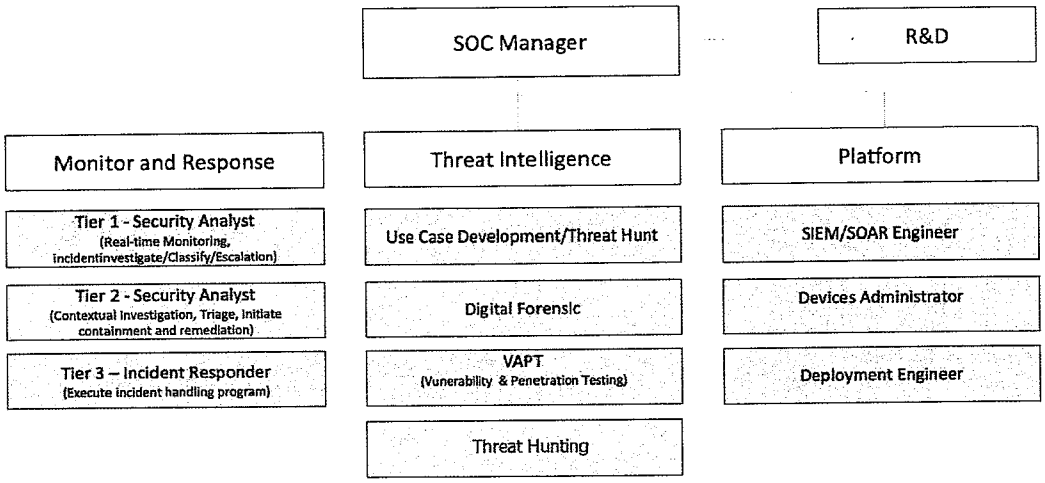
๓.๒๑.๒ จัดลำดับความเสี่ยง และจัดทำรายงานการตรวจสอบช่องโหว่ของอุปกรณ์ทางไซเบอร์หรืออุปกรณ์เครื่องแม่ข่ายหรืออุปกรณ์ระบบบเครือข่ายให้กับทางโรงพยาบาลฯ

..... ผู้รับจ้าง

..... พยาน

๔. บุคลากรในการดำเนินโครงการ

บริษัทฯ มีผู้เชี่ยวชาญและเจ้าหน้าที่ที่ปฏิบัติงานในศูนย์เฝ้าระวังความมั่นคงปลอดภัยไซเบอร์ (พนักงานประจำ ที่มีประสบการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ ที่ได้รับการรับรองความรู้ความสามารถ)



รูปที่ ๔-๑ โครงสร้างทีม CSOC ของบริษัทฯ

จากภาพโครงสร้างทีม CSOC ของ บริษัท ไซเบอร์ อีลีท จำกัด จะพบว่ามีทีมงานที่ทำหน้าที่ปฏิบัติงานที่ศูนย์ปฏิบัติการ แบ่งออกเป็น ๓ กลุ่มใหญ่ๆ ซึ่งประกอบด้วยเจ้าหน้าที่ที่มีความรู้ความสามารถและผ่านการรับรองความรู้ความสามารถจากสถาบันชั้นนำและเป็นพนักงานที่พร้อมปฏิบัติงานให้กับทาง โรงพยาบาลฯ ซึ่งมีรายละเอียดดังต่อไปนี้

๔.๑ Monitor and Response Team ประกอบด้วย

๔.๑.๑ Tier ๑ – Security Analyst ประกอบด้วยทีมงานที่มีประสบการณ์เพื่อรับแจ้งเหตุด้านความมั่นคงปลอดภัยไซเบอร์เฝ้าระวังเหตุบุกรุก และแจ้งเตือนเหตุบุกรุก ระดับรุนแรง และระดับไม่รุนแรงตลอด ๒๔ ชั่วโมง โดยจะเน้นการเฝ้าระวังและแจ้งเตือนเหตุการณ์ที่ผิดปกติต่างๆ ในเบื้องต้น

๔.๑.๒ Tier ๒ – Security Analyst ประกอบด้วยทีมงานที่มีประสบการณ์ในการระบุปัญหาด้านความปลอดภัยของระบบขึ้นอยู่กับการวิเคราะห์ความเสี่ยง มีการวิเคราะห์เหตุการณ์ที่เกิดขึ้นได้อย่างเป็นระบบและสามารถที่จะสร้างเป็นแผนผังของเหตุการณ์ที่เกิดขึ้น

ผู้รับจ้าง .....

พยาน .....

CYBER ELITE CO.,LTD

๔.๑.๓ Tier ๓ – Incident Responder ประกอบด้วยทีมงานที่มีประสบการณ์ตรงในการรับมือกับอุบัติการณ์ ศึกษาและวิจัยเกี่ยวกับภัยคุกคามอย่างต่อเนื่องเพื่อเสริมให้ศูนย์ปฏิบัติการฯ สามารถเฝ้าระวังและแจ้งเตือนภัยคุกคามได้อย่างทันท่วงที

Threat Intelligence Team ประกอบด้วย

๔.๒.๑ Use Case Development/Threat Hunt ประกอบด้วยทีมงานที่มีประสบการณ์ตรงสำหรับการสร้าง Use Case จากข้อมูลภัยคุกคามล่าสุดที่ได้มาจากระบบ Threat Intelligence จากนั้นนำไปสร้าง Rule บนระบบ SIEM ซึ่งเป็นศูนย์กลางของศูนย์ปฏิบัติการด้านความมั่นคงปลอดภัยจึงทำให้ โรงพยาบาลฯ สามารถค้นพบความผิดปกติหรือเหตุการณ์ต้องสงสัยว่าเกี่ยวข้องกับภัยคุกคามไซเบอร์ได้อย่างทันท่วงทีและกักกันความเสียหายไม่ให้ลุกลามได้อย่างรวดเร็ว

๔.๒.๒ Digital Forensic ประกอบด้วยทีมงานเก็บหลักฐานการบุกรุก ระบุเก็บรวบรวมตรวจสอบและเก็บรักษาหลักฐานโดยใช้เทคนิคการวิเคราะห์และการสืบสวนที่มีการควบคุมและเอกสาร ค้นหาสาเหตุของการถูกบุกรุก (Root Cause Analysis) ดำเนินการตรวจสอบเชิงลึกเกี่ยวกับอาชญากรรมบนคอมพิวเตอร์ที่สร้างหลักฐานทางเอกสารหรือหลักฐานทางกายภาพรวมถึงสื่อดิจิทัลและบันทึกที่เกี่ยวข้องกับเหตุการณ์การบุกรุกในโลกไซเบอร์

๔.๒.๓ VAPT ทีมงานผู้เชี่ยวชาญด้านทักษะด้านการสแกนช่องโหว่ (VA Scan), มีทักษะด้านการประเมินช่องโหว่, มีทักษะด้านการทดสอบการเจาะระบบ (Penetration Test)

๔.๒.๔ ทีมงานค้นหาภัยคุกคามเชิงรุก (Threat Hunting) มีทักษะด้านการตรวจสอบภัยคุกคามในเชิงรุก คอยค้นหาและยับยั้งภัยคุกคามต่างๆที่จะเกิดขึ้นภายในระบบโดยใช้ข้อมูลจากระบบ Threat Intelligence เพื่อเพิ่มประสิทธิภาพในการดำเนินงาน

๔.๓ Platform Team ประกอบด้วย

๔.๓.๑ SIEM/SOAR Engineer ทีมงานผู้เชี่ยวชาญด้านการรับผิดชอบในการติดตั้งระบบ SIEM ประเมินประสิทธิภาพของการควบคุมความปลอดภัย ประเมินกระบวนการจัดการการกำหนดค่าทั้งหมด (เปลี่ยนแปลงการกำหนดค่า) พัฒนาขั้นตอนและทดสอบระบบ SIEM

..... ผู้รับจ้าง

..... พยาน

๔.๓.๑ Devices Administrator ทีมงานผู้เชี่ยวชาญด้านการบริหารจัดการอุปกรณ์ต่าง ๆ ภายในศูนย์ปฏิบัติการ

๔.๓.๓ Deployment Engineer ทีมงานผู้เชี่ยวชาญด้านการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) และบริหารจัดการเทคโนโลยีในศูนย์ปฏิบัติการฯ ซึ่งมีประสบการณ์ตรงในสายงาน

๔.๔ SOC Manager ทำหน้าที่ในการบริหารจัดการและรับผิดชอบบริการทั้งหมดของศูนย์ปฏิบัติการฯ ภายใต้ขอบเขตโครงการ ซึ่งมีประสบการณ์ตรงในการบริหารจัดการศูนย์ปฏิบัติการฯ โดยบริหารโครงการด้านการเฝ้าระวังและการรับมือภัยคุกคามด้านความมั่นคงปลอดภัยสารสนเทศมาแล้วมากมาย ไม่ว่าจะเป็นภาครัฐ การเงิน การไฟฟ้า องค์กรเอกชนขนาดใหญ่ โดยทำงานด้านนี้มามากกว่า ๑๐ ปี

๔.๕ R/D Team ซึ่งทำหน้าที่พัฒนาระบบเพื่อให้การบริการจากศูนย์ปฏิบัติการฯ มีประสิทธิภาพต่อผู้ใช้บริการอย่างที่สุด

ผู้รับจ้าง

พยาน

๕. แผนการดำเนินงาน

๕.๑ บริษัทฯ ขอนำเสนอแผนการดำเนินงานสำหรับการติดตั้งของโครงการ

No.	กิจกรรม (Activities)	M๑				M๒				M๓			
		W๑	W๒	W๓	W๔	W๑	W๒	W๓	W๔	W๑	W๒	W๓	W๔
๑	Kick-off Installation • Get requirement. • Scope and project team responsibility. • Prepare log and datasource.												
๒	Installation and configuration • Log Collector installation. • Log Collector configuration • Check connection between Centralize and Log Collector • Log Collector deployment to centralize												
๓	On-Boarding Process • Prepare and check log source. • Log parsing and normalization (optional) • Datasource grouping. • Analysis Cyber Attack and prepare impact of cyber attack. • Develop use-case. • Develop virtualize and dashboard. • Develop report. • Develop incident management procedure. • Recommendation and improve incident response process												

No	กิจกรรม (Activities)	M๑				M๒				M๓			
		W๑	W๒	W๓	W๔	W๕	W๖	W๗	W๘	W๙	W๑๐	W๑๑	W๑๒
๔	Documentation • Admin Guide • Installation detail and Network Diagram • Log source summary • System Detail & Diagram			■	■								
๕	Go-live to monitor					■	■	■	■	■	■	■	■

รูปที่ ๕-๑ แสดงระยะเวลาในการดำเนินโครงการ

หมายเหตุ: แผนการดำเนินงานสามารถปรับเปลี่ยนได้ตามความเหมาะสม

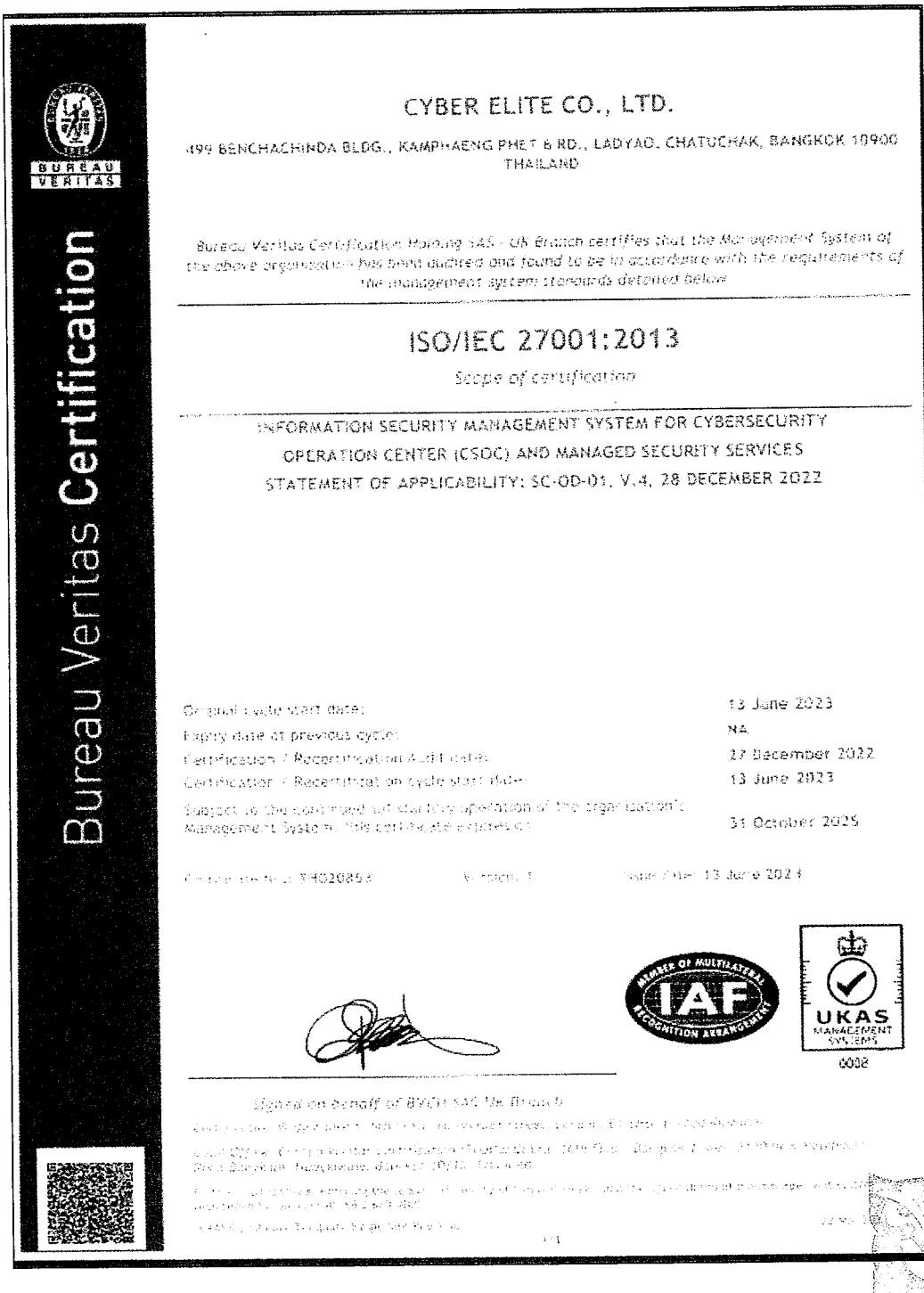
๕.๒ แผนการดำเนินงานการให้บริการเฝ้าระวังความมั่นคงปลอดภัยไซเบอร์ ในปี พ.ศ. ๒๕๖๘

No	กิจกรรม (Activities)	JAN				FEB				MAR				APL				MAY				JUN				JUL				AUG				SEP				OCT				NOV				DEC			
		w ๑	w ๒	w ๓	w ๔	w ๕	w ๖	w ๗	w ๘	w ๙	w ๑๐	w ๑๑	w ๑๒	w ๑๓	w ๑๔	w ๑๕	w ๑๖	w ๑๗	w ๑๘	w ๑๙	w ๒๐	w ๒๑	w ๒๒	w ๒๓	w ๒๔	w ๒๕	w ๒๖	w ๒๗	w ๒๘	w ๒๙	w ๓๐	w ๓๑	w ๓๒	w ๓๓	w ๓๔	w ๓๕	w ๓๖	w ๓๗	w ๓๘	w ๓๙	w ๔๐	w ๔๑	w ๔๒	w ๔๓	w ๔๔	w ๔๕	w ๔๖	w ๔๗	w ๔๘
๑	Security Monitoring ๒๔ x ๗													■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■										
๒	Monthly report															■				■				■				■				■				■													
๓	Monthly Cyber Security Trend update															■				■				■				■				■				■													
๔	Vulnerabilities Assessment ๑๐ IP addresses																									■																						
๕	CSIRT response ๔ hours within ๔ time / contract (by request)																																														

รูปที่ ๕-๒ แผนการดำเนินงานการให้บริการเฝ้าระวังความมั่นคงปลอดภัยไซเบอร์ ปี พ.ศ. ๒๕๖๘

หมายเหตุ: แผนการดำเนินงานสามารถปรับเปลี่ยนได้ตามความเหมาะสม

๖. ภาคผนวก ก. เอกสารรับรองมาตรฐานสากล



BUREAU VERITAS

Bureau Veritas Certification

CYBER ELITE CO., LTD.

499 BENCHACHINDA BLDG., KAMPHAENG PHET 6 RD., LADYAO, CHATUCHAK, BANGKOK 10900 THAILAND

Bureau Veritas Certification Holding SAS - UK Branch certifies that the Management System of the above organisation has been audited and found to be in accordance with the requirements of the management system standards detailed below

ISO/IEC 27001:2013

Scope of certification

INFORMATION SECURITY MANAGEMENT SYSTEM FOR CYBERSECURITY OPERATION CENTER (CSOC) AND MANAGED SECURITY SERVICES STATEMENT OF APPLICABILITY: SC-OD-01, V.4, 28 DECEMBER 2022

Original cycle start date:	13 June 2023
Expiry date of previous cycle:	NA
Certification / Recertification Audit date:	27 December 2022
Certification / Recertification cycle start date:	13 June 2023
Subject to the continued satisfactory operation of the organization's Management System, this certificate expires on:	31 October 2025

Certificate No.: FM020853 Version: 1 Issue Date: 13 June 2023

MEMBER OF MULTILATERAL RECOGNITION ARRANGEMENT IAF

UKAS MANAGEMENT SYSTEMS 0032

Signed on behalf of BVCH SAS UK Branch

CYBER ELITE CO., LTD

..... ผู้รับจ้าง

..... พยาน

BUREAU VERITAS

Bureau Veritas Certification

CYBER ELITE CO., LTD.

499 BENCHACHINDA BLDG., KAMPHAENG PHET 6 RD., LADYAO, CHATUCHAK, BANGKOK 10900, THAILAND

Bureau Veritas Certification certify that the Management System of the above organisation has been audited and found to be in accordance with the requirements of the management system standards detailed below

ISO/IEC 27701:2019

Scope of certification

PRIVACY INFORMATION MANAGEMENT SYSTEM FOR CYBERSECURITY OPERATION CENTER (CSOC) AND MANAGED SECURITY SERVICES STATEMENT OF APPLICABILITY: SC-OD-01, V.4, 28 DECEMBER 2022

Original cycle start date:	**21 April 2023**
Expiry Date of Previous Cycle:	**N/A**
Certification / Recertification Audit date:	**N/A**
Certification / Recertification cycle start date:	**21 April 2023**
Subject to the continued satisfactory operation of the organisation's Management System, this certificate expires on:	**20 April 2026**

Certificate no.: **TH020700** Version: 1 Issue Date: **21 April 2023**

Certification Authority

Local office: Bureau Veritas Certification (Thailand) Ltd. 16th Floor, Bangkok Tower, 2170 New Petchburi Road, Bangkapi, Huaykwang, Bangkok 10310, Thailand

Further clarifications regarding the scope of this certificate and the applicability of the management system requirements may be obtained by consulting the organisation.
To check this certificate validity please call: +662 670 4800

1/1

CYBER ELITE CO., LTD.

ผู้รับจ้าง

พยาน

๗. การกำหนดระยะเวลารับประกันความชำรุดบกพร่อง (ถ้ามี)

๑. บริษัทฯ มีระยะเวลาในการแก้ไข ผลงานหรือรายงาน ภายใน ๗ วัน นับถัดจากวันที่ได้รับแจ้งเป็นลายลักษณ์อักษรจากทางผู้ว่าจ้าง

๒. ทางโรงพยาบาลฯ สามารถขอรับคำปรึกษาด้านเทคนิคในการรับมือเหตุการณ์ภัยคุกคามที่เกิดขึ้นทางโทรศัพท์ ได้โดยไม่จำกัดจำนวนครั้งตลอด ๒๔ ชั่วโมง ตลอดระยะเวลาสัญญา

๓. บริษัทฯ ให้บริการเฝ้าระวังภัยคุกกคามทางไซเบอร์เป็นระยะเวลา ๖ เดือน

๔. บริษัทมีการแจ้งเตือนให้แก่ทางโรงพยาบาลภายในระยะเวลา ๖ ชั่วโมง เมื่อตรวจพบอุปกรณ์ต้นทางหยุดส่งข้อมูลจราจรทางคอมพิวเตอร์เป็นเวลา ๒๔ ชั่วโมงขึ้นไป

CYBER ELITE CO., LTD.

..... ผู้รับจ้าง

..... พยาน

close the account in accordance with the Bank's regulations.

สาขา 0101
Branch สำนักงานใหญ่สีลม

บัญชีเลขที่
Account No. 101-9-37399-0

101 937399 0

ชื่อบัญชี Account Name 戶口名稱

บริษัท ไซเบอร์ อีลิท จำกัด

SCT3200199

ลายเซ็นชื่อผู้มีอำนาจ
Authorized Signature

3200199

ผู้รับจ้าง

พยาน

CYBER ELITE CO., LTD.

รายละเอียดการขอเสียอากรแสตมป์เป็นตัวเงินสำหรับตราสารอิเล็กทรอนิกส์

รหัสรับรองการเสียอากรแสตมป์ 80296804095638747874

เลือกยื่นตราสาร ☑ ตราสารอิเล็กทรอนิกส์ ☐ ตราสารกระดาษ

ผู้ขอเสียอากรแสตมป์

เลขประจำตัวผู้เสียภาษีอากร 0 1055 64168 02 9

สาขาที่ 0

ชื่อผู้ขอเสียอากรแสตมป์ บริษัท ไซเบอร์ อีลีท จำกัด

ในฐานะ ผู้รับจ้าง

คู่สัญญา

เลขประจำตัวผู้เสียภาษีอากร 0 9940 00165 33 1

สาขาที่

ชื่อคู่สัญญา โรงพยาบาล โรงพยาบาลตำรวจ

รายละเอียดเกี่ยวกับสัญญา

ลักษณะแห่งตราสาร ตราสาร 4 จ้างทำของ

สัญญาเลขที่ สช.98/2568 ลงวันที่ 28/03/2568

วัน เดือน ปี ที่เริ่มสัญญา 01/04/2568

วัน เดือน ปี ที่สิ้นสุดสัญญา 30/09/2568

หมายเลขอ้างอิงตราสารอิเล็กทรอนิกส์ 0994000165331

มูลค่าในตราสาร (ไม่รวมภาษีมูลค่าเพิ่ม) 291,520.00

วันที่ได้รับตราสารอิเล็กทรอนิกส์

รายละเอียดเพิ่มเติมเกี่ยวกับตราสารอิเล็กทรอนิกส์

งานที่รับจ้าง โครงการจ้างวิเคราะห์เฝ้าระวังและการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับโรงพยาบาลตำรวจ

จำนวนงวดงาน 6

จำนวนเงินค้ำประกันตามสัญญา บาท

รายละเอียดการชำระเงิน

จำนวนเงินค่าอากรแสตมป์ 292.00

เงินเพิ่มอากร 0.00

รวมจำนวนเงินค่าอากรแสตมป์ และเงินเพิ่มอากร 292.00

เลขที่ใบเสร็จรับเงิน 68120552206

วันที่ชำระเงิน 09/04/2568

กรณียื่นแบบเพิ่มเติม (สำหรับตราสาร 1, 2, 3, 4, 5, 11(2), 14, 17, 18 และ 21)

หมายเลขอ้างอิงตราสารอิเล็กทรอนิกส์ (ฉบับเดิม)

สัญญาเลขที่ (ฉบับเดิม)

ลงวันที่ (ฉบับเดิม)

Digitally Signed
By the Revenue Department (EPA)
Date :2025-04-09 13:33:47

ใบเสร็จรับเงิน

หน่วยรับชำระ กองบริหารการคลังและรายได้ กรมสรรพากร	**วันชำระเงิน/วันนำส่ง** 09/04/2568
ผู้ชำระภาษีอากร บริษัท ไชเบอร์ อีลีท จำกัด	**เดือน/ปีภาษี**
เลขประจำตัวผู้เสียภาษีอากร/เลขประจำตัวประชาชน 0-1055-64168-02-9	**ประเภทการชำระ** อากรแสตมป์

หมายเลขอ้างอิงการยื่นแบบ	เลขที่ใบเสร็จรับเงิน	จำนวนเงิน (บาท)
P090031652251	68120552206	**********292.00
จำนวนเงินเป็นตัวอักษร (สองร้อยเก้าสิบสองบาทถ้วน)		292.00

อ.ส.9

ผู้รับเงิน

(นางสาวจิตรา พงษ์พานิช)

ผู้อำนวยการกองบริหารการคลังและรายได้/ผู้รับมอบอำนาจ

Digitally Signed
By the Revenue Department (EPA)
Date :2025-04-09 13:33:46