การไฟฟ้านครหลวง
Metropolitan Electricity Authority

ประชุมคณะทำงานพิจารณากลั่นกรองโครงการจัดหาระบบคอมพิวเตอร์ของกระทรวงมหาดไทย

ระบบเพิ่มประสิทธิภาพการตรวจจับและป้องกันภัยคุกคามบนแอปพลิเคชัน

หน่วยงาน การไฟฟ้านครหลวง ฝ่ายมั่นคงปลอดภัยไซเบอร์และธรรมาภิบาลข้อมูล

งบลงทุนปี พ.ศ ๒๕๖๕ เป้าจ่ายปี ๒๕๖๖

-วงเงินรวม(ราคากลางในเอกสาร มท.) ๓๑,๔๘๑,๗๕๔.๐๐ บาท

-วงเงินส่วนที่เป็นอุปกรณ์คอมฯ ๓๑,๑๕๐,๐๕๔.๐๐ บาท วงเงินส่วนที่เป็นอุปกรณ์อื่น ๆ ๓๓๑,๗๐๐.๐๐ บาท

วัตถุประสงค์ เป้าหมาย

วัตถุประสงค์

๑. เพื่อทดแทนระบบป้องกันการบุกรุกเว็บไซต์ (Web Application Firewall) เดิมที่ขาดฟังก์ชันในการป้องกันส่วนของ Application ซึ่ง กฟน. มีการใช้งานอยู่ ได้แก่ MEAconnext , MEASmart life , MEAe-fix เป็นต้น

๒. ~~เพื่อเพิ่มประสิทธิภาพการตรวจจับและป้องกันภัยคุกคามบนแอปพลิเคชัน เป็นระบบในการเฝ้าระวัง ตรวจสอบ และป้องกันการโจมตีทางเว็บไซต์และแอปพลิเคชัน~~

๓. เพื่อรองรับการปรับเปลี่ยนโครงสร้างระบบเครือข่ายใหม่ของ กฟน. ให้มีการป้องกันที่ครอบคลุมทั้ง Site หลัก และ Site สำรอง

๔. เพื่อเพิ่มเติมเครื่องมือในการตรวจจับและวิเคราะห์ ลักษณะภัยคุกคามทางไซเบอร์ที่คลอบคลุมรูปแบบการโจมตีเว็บไซต์และแอปพลิเคชัน และระบบที่สำคัญอื่นๆ ทั้งด้าน IT และ OT ของ กฟน.

๕. เพื่อให้ได้มาซึ่งข้อมูลในการวิเคราะห์วางแผนการบริหารความเสี่ยง ออกแบบรูปแบบในการป้องกันภัยคุกคามทางไซเบอร์แบบต่างๆ ได้อย่างทันเหตุการณ์ และเสริมศักยภาพในการรับมือเหตุภัยคุกคาม ทั้งด้าน IT และ OT ของ กฟน.

เป้าหมาย

เพื่อเพิ่มประสิทธิภาพในการเฝ้าระวัง ตรวจสอบ และป้องกันการโจมตีทางเว็บไซต์และแอปพลิเคชัน ซึ่งมักเกิดช่องโหว่ (Vulnerability) ที่ผู้ไม่ประสงค์ดีสามารถโจมตีเข้าครอบครองระบบหรือขโมยข้อมูลที่สำคัญออกไปได้ ซึ่งระบบงานนี้สามารถที่จะป้องกันการโจมตีเว็บไซต์และแอปพลิเคชันได้โดยเฉพาะ อีกทั้งยังเป็นระบบที่มีเครื่องมือในการตรวจจับและวิเคราะห์ ลักษณะภัยคุกคามทางไซเบอร์เพื่อจัดทำสถิติความมั่นคงปลอดภัยทางไซเบอร์และนำข้อมูลมาใช้ในการวิเคราะห์วางแผนการบริหารความเสี่ยงได้อย่างทันเหตุการณ์ และเสริมศักยภาพในการรับมือเหตุภัยคุกคาม ทั้งด้าน IT และ OT ของ กฟน. ให้มีความมั่นคงปลอดภัย และสามารถให้บริการประชาชนได้อย่างเต็มประสิทธิภาพและต่อเนื่อง

ขอบเขตการดำเนินงาน, วิธีการดำเนินงาน, ผู้รับผิดชอบ ผู้ใช้งาน และผู้บำรุงรักษา

ขอบเขตการดำเนินงาน

ระบบเพิ่มประสิทธิภาพการตรวจจับและป้องกันภัยคุกคามบนแอปพลิเคชัน จำนวน ๑ ระบบ พร้อมติดตั้ง ระยะเวลาดำเนินงาน ๑๘๐ วัน รับประกัน ๓ ปี

วิธีการดำเนินงาน

จัดซื้อโดยวิธีประกาศเชิญชวนทั่วไป

ผู้รับผิดชอบ ผู้ใช้งาน และผู้บำรุงรักษา

ผู้ใช้งาน วิศวกรคอมพิวเตอร์, วิศวกรสื่อสาร, นักประมวลผลข้อมูล ฝ่ายมั่นคงปลอดภัยไซเบอร์และธรรมาภิบาลข้อมูล

ผู้รับผิดชอบ ฝ่ายมั่นคงปลอดภัยไซเบอร์และธรรมาภิบาลข้อมูล

ผู้บำรุงรักษา ฝ่ายมั่นคงปลอดภัยไซเบอร์และธรรมาภิบาลข้อมูล

ประโยชน์และความคุ้มค่าของโครงการ

ประโยชน์ของโครงการ

๑. สามารถป้องกันเว็บไซต์และแอปพลิเคชันจากการโจมตีในรูปแบบต่าง ๆ เช่น cross-site forgery, cross-site-scripting (XSS), file inclusion และ SQL injection เป็นต้น

๒. สามารถตรวจจับและวิเคราะห์ ลักษณะพฤติกรรมของภัยคุกคามทางไซเบอร์ที่คลอบคลุมรูปแบบการโจมตีเว็บไซต์และแอปพลิเคชัน และระบบที่สำคัญอื่นๆ

๓. เพิ่มประสิทธิภาพการตรวจจับและป้องกันภัยคุกคามบนแอปพลิเคชัน เป็นระบบในการเฝ้าระวัง ตรวจสอบ และป้องกันการโจมตีทางเว็บไซต์และแอปพลิเคชัน ให้มีการป้องกันที่ครอบคลุมทั้ง Site หลัก และ Site สำรอง ทั้งด้าน IT และ OT ของ กฟน.

๔. มีข้อมูลมาใช้ในการวิเคราะห์วางแผนการบริหารความเสี่ยง และแผนการเผชิญเหตุได้อย่างทันเหตุการณ์ จัดทำสถิติความมั่นคงปลอดภัยทางไซเบอร์และเสริมศักยภาพในการรับมือเหตุภัยคุกคาม ทั้งด้าน IT และ OT ของ กฟน.

ความคุ้มค่าของโครงการ

กรณีระบบงานต่างๆ ของ กฟน. หยุดชะงักหรือไม่สามารถให้บริการแก่ประชาชนได้อันเนื่องมาจากการโจมตีทางเว็บไซต์และแอปพลิเคชัน ซึ่งมักเกิดช่องโหว่ (Vulnerability) ที่ผู้ไม่ประสงค์ดีสามารถโจมตีเข้าครอบครองระบบหรือขโมยข้อมูลที่สำคัญออกไปได้ จะส่งผลให้ทาง กฟน. ต้องใช้งบประมาณในการกู้คืนระบบงาน ระยะเวลา บุคคลกร เพื่อดำเนินงานและส่งผลต่อการให้บริการประชาชน ซึ่งการจัดซื้อในครั้งนี้สามารถที่จะป้องกันการโจมตีเว็บไซต์และเพิ่มเติมส่วนการป้องกันแอปพลิเคชันได้โดยเฉพาะ รวมทั้งวิเคราะห์ ลักษณะพฤติกรรมของภัยคุกคามทางไซเบอร์และนำข้อมูลมาใช้ในการวิเคราะห์วางแผนการบริหารความเสี่ยงได้อย่างทันเหตุการณ์ จัดทำสถิติความมั่นคงปลอดภัยทางไซเบอร์และเสริมศักยภาพในการรับมือเหตุภัยคุกคาม ทั้งด้าน IT และ OT ของ กฟน. ให้มีความมั่นคงปลอดภัยสามารถให้บริการประชาชนได้อย่างเต็มประสิทธิภาพ และต่อเนื่อง

ที่มา

เนื่องจาก กฟน. มีการปรับปรุงระบบเครือข่ายเพื่อเสริมศักยภาพในการให้บริการประชาชนของ Site หลัก และ Site สำรอง ให้สามารถทำงานได้อย่างเต็มประสิทธิภาพมากยิ่งขึ้น ซึ่งเดิมมีระบบป้องกันการบุกรุกเว็บไซต์ (Web Application Firewall) สำหรับ Site หลักเท่านั้น จึงจำต้องจัดหาระบบป้องกันการบุกรุกเว็บไซต์ (Web Application Firewall ให้คลอบคลุมระบบงานทั้ง Site หลัก และ Site สำรอง และจากการฝึกซ้อมเชิงปฏิบัติการประจำปี ๒๕๖๔ และงานทดสอบความมั่นคงปลอดภัยในส่วนแผนเผชิญเหตุและการรับมือการโจมตีทางเว็บไซต์ประจำปี ๒๕๖๔ พบว่ายังมีกระบวนการรับมือที่ไม่สามารถตอบสนองต่อภัยคุกคามได้อย่างมีประสิทธิภาพ ~~จึงเพิ่มเติมระบบดักจับผู้บุกรุกการเข้าสู่เครือข่าย (Deception) เพื่อใช้ในการตรวจจับและศึกษาวิเคราะห์ลักษณะภัยคุกคามทางไซเบอร์ที่คลอบคลุมรูปแบบการโจมตีเว็บไซต์และแอปพลิเคชัน และระบบที่สำคัญอื่นๆ ทั้งด้าน IT และ OT ของ กฟน. เพื่อนำมาจัดทำข้อมูลรูปแบบการโจมตี และปรับปรุงกระบวนงานการเผชิญเหตุภัยคุกคามให้สอดคล้องกับสามารถตอบสนองกับเหตุภัยคุกคามต่างๆได้อย่างมีประสิทธิภาพ~~

ข้อชี้แนะเพิ่มเติมจากที่ปรึกษา

การปรับปรุงกระบวนงานให้รองรับ

- ควรวางแผนทบทวนกระบวนงานของแต่ละส่วนทั้งทีมปฏิบัติการและทีมสนับสนุน ให้สังเกตกับข้อสังเกตแนะแนวทางที่ควรปฏิบัติในสถานการณ์จริง

Findings Summary

	ข้อสังเกต (Findings)
5	ควรปรับปรุงขั้นตอนการทำ Incident Response ในเอกสาร Playbook เพิ่มเติม

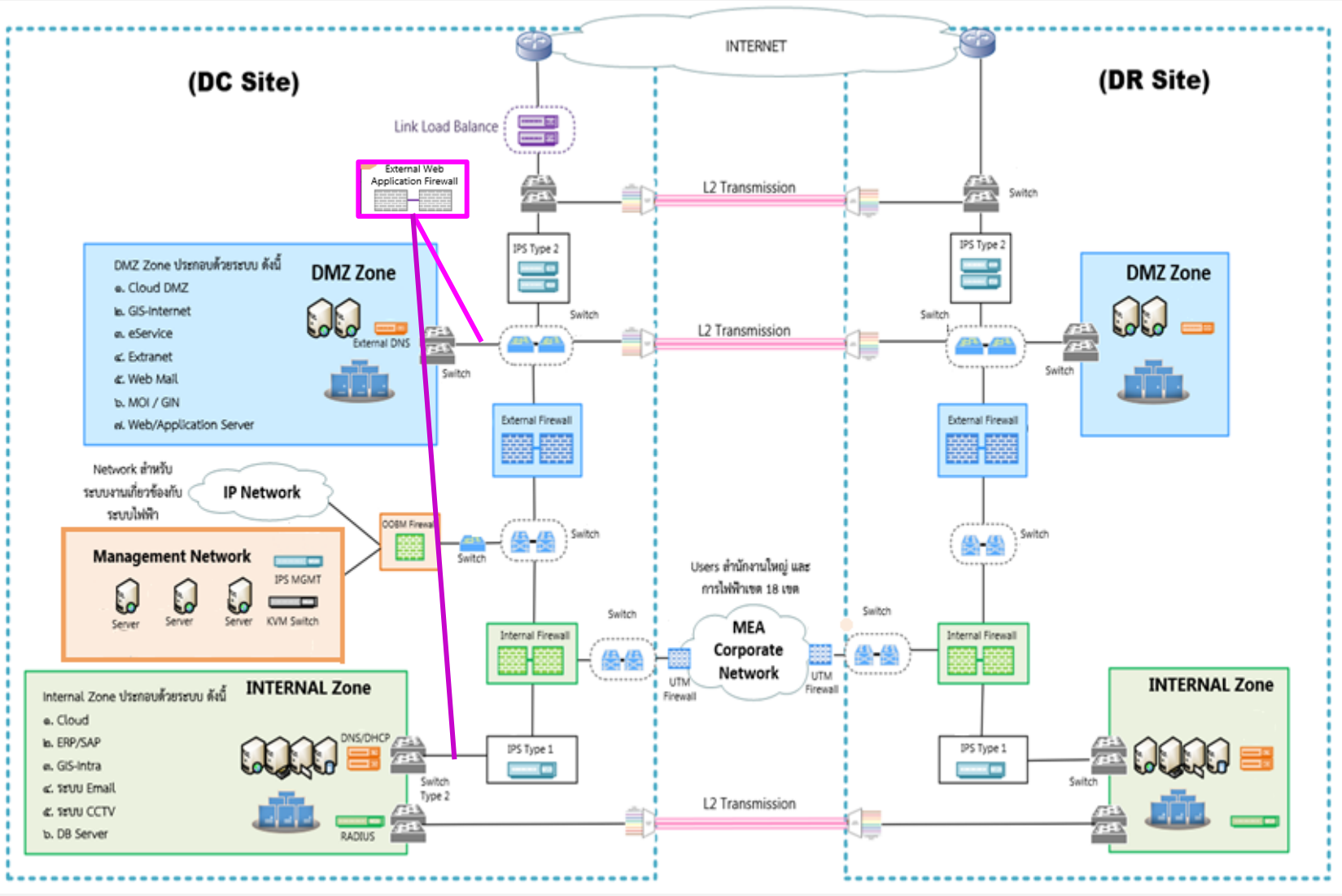
ข้อชี้แนะเพิ่มเติมจากที่ปรึกษา

ควรปรับปรุงขั้นตอนการทำ Incident Response ในเอกสาร Playbook ให้สอดคล้องกับพฤติกรรม รูปแบบ ลักษณะตามเหตุการ์ณโจมตีในปัจจุบันหรือที่พบบ่อย

การไฟฟ้านครหลวง
Metropolitan Electricity Authority

๑. ระบบป้องกันการบุกรุกเว็บไซต์ (Web Application Firewall) จำนวน ๑ ระบบ

ระบบปัจจุบัน



ข้อจำกัดของระบบปัจจุบัน ของอุปกรณ์การป้องกันการบุกรุกทางเว็บไซต์

๑. อุปกรณ์เดิมปัจจุบันป้องกันระบบ Website จำนวน ๑๓ เว็บไซต์

๒. อุปกรณ์เดิมไม่สามารถป้องกันการโจมตี Application ได้

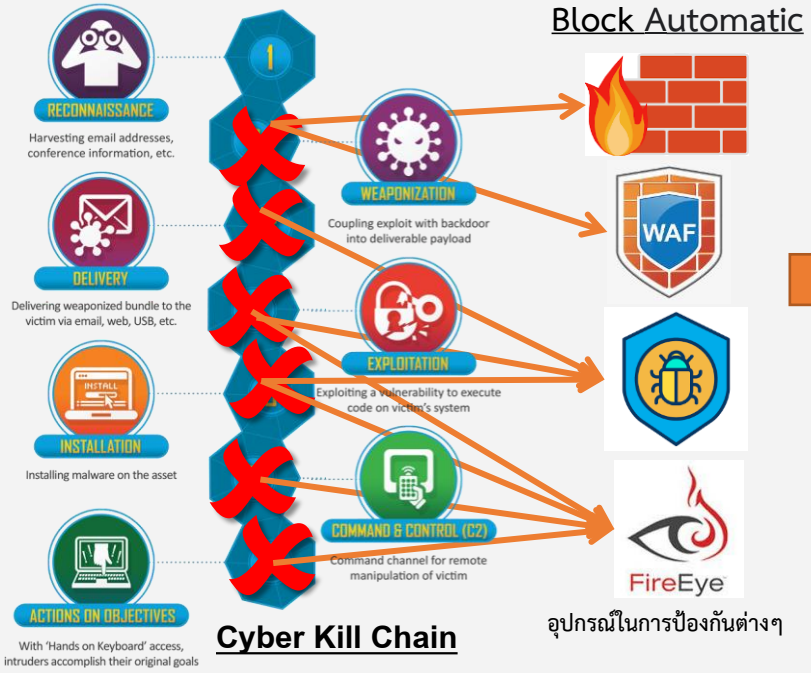
๓. อุปกรณ์เดิมมี ๒ ชุด ติดตั้งที่ Site หลักเท่านั้น เนื่องจากเครือข่ายเดิมต้องส่งผ่าน Traffic มาที่ Site หลักก่อน แต่เครือข่ายใหม่ จะทำงานแยกกันทั้ง ๒ Site

รายการ Website ที่อยู่ในการป้องกันของระบบ

✗	๑. App MEA Smart life Web	✓	๙. Web Sever SolarPV
✗	๒. App mea EV	✓	๑๐. Web Sever NAT MEAOR Procurement
✗	๓. App MEA e-fix	✓	๑๑. Web Sever NAT MEAORTH
✓	๔. Web Sever Meaccd	✓	๑๒. Web Sever NAT iemp
✓	๕. Web Sever MeaSAD	✓	๑๓. Web Sever CCTV
✓	๖. Web Sever SolarPV	✓	๑๔. Web Sever NAT_iotdev (Chatbot)
✓	๗. Web Sever E-Services	✓	๑๕. Web Sever NAT MEASY
✓	๘. Web Sever EVCCC	✓	๑๖. Web Server etax

ระบบปัจจุบัน

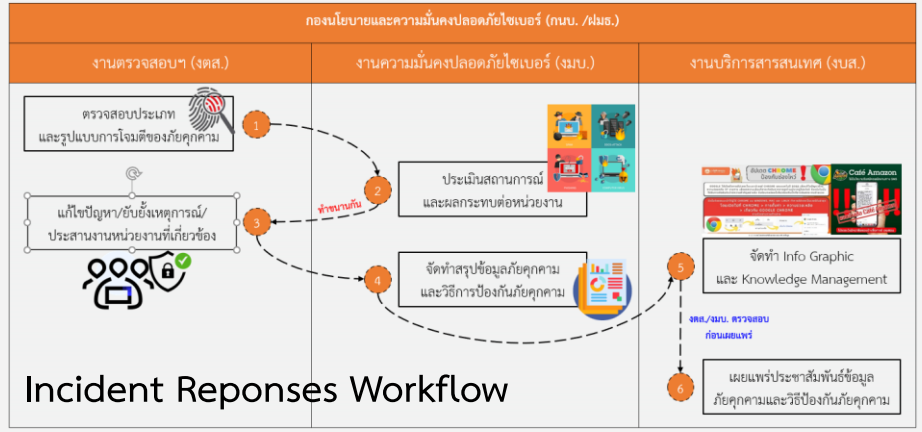
๒. ระบบดักจับการลักลอบเข้าสู่เครือข่ายเทคโนโลยีสารสนเทศ จำนวน ๑ ระบบ



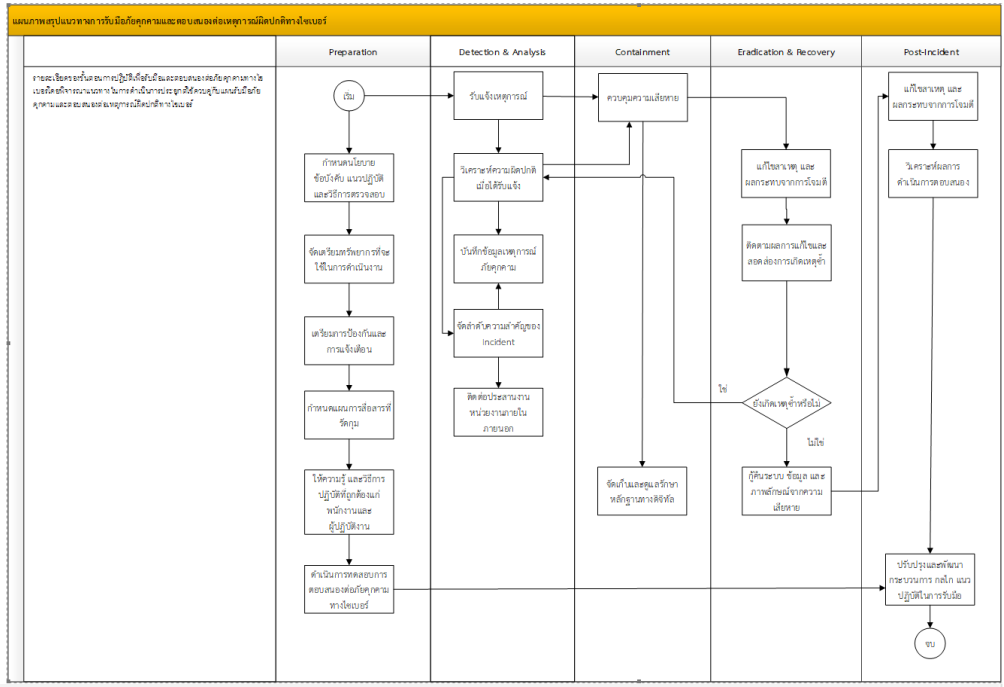
อุปกรณ์ในการป้องกันต่างๆ

Security Operations Center (SOC)

ศึกษารูปแบบพฤติกรรมจากข้อมูลอุปกรณ์และแหล่งข่าวอื่นๆ เท่าที่มีเพื่อออกแบบกระบวนงานการรับมือเหตุภัยคุกคาม



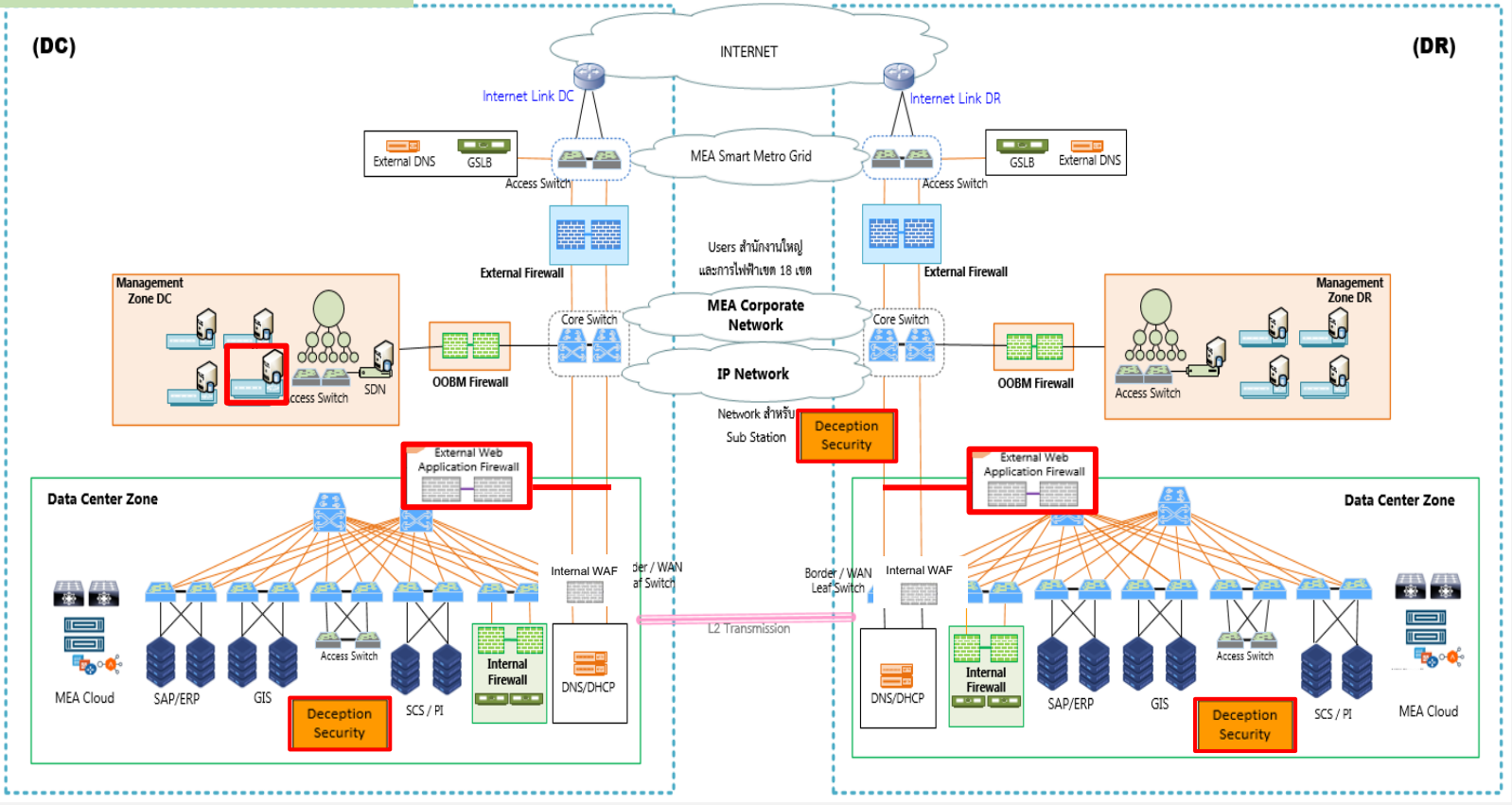
ขั้นตอนการปฏิบัติการรับมือและแก้ไขเหตุภัยคุกคามทางไซเบอร์



ปัจจุบัน กฟน. มีอุปกรณ์ในการป้องกันการโจมตีภัยคุกคามทั้งทางเว็บไซต์และการโจมตีอื่นๆ เช่น Web Firewall , Web Application Firewall , Antivirus และ End Point Protection ซึ่งมีการตรวจจับและทำการ Block Process ต้องสงสัยตั้งแต่ขั้นตอนที่ ๒ Weaponization (การวางอาวุธเพื่อโจมตี) ดังนั้นทาง Security Operations Center (SOC) จึงออกแบบกระบวนการรับมือเหตุภัยคุกคามจากข้อมูลเท่าที่อุปกรณ์มีและจากแหล่งข้อมูลต่างๆ จากการทดสอบเจาะระบบฯ ประจำปี ๒๕๖๔ เมื่อเกิดเหตุการณ์ขึ้นจริงซึ่งอุปกรณ์ต่างๆ ไม่สามารถตรวจจับและยับยั้งได้ การรับมือเหตุภัยคุกคามตามกระบวนการไม่สอดคล้องกับการปฏิบัติงานจริงทำให้การตอบสนองเหตุการณ์ไม่มีประสิทธิภาพ ล่าช้า และส่งผลให้เครื่องแม่ข่ายและเครื่องคอมพิวเตอร์ถูกโจมตีได้สำเร็จ

๑. ระบบป้องกันการบุกรุกเว็บไซต์ (Web Application Firewall) จำนวน ๑ ระบบ

ระบบที่จะจัดซื้อ



การแก้ไขข้อจำกัดของระบบปัจจุบัน

๑. เพิ่มฟังก์ชันการป้องกันการโจมตี Application ตามหัวข้อ API Security OWASP TOP 10

๒. เพิ่มจำนวนอุปกรณ์เพื่อให้รองรับระบบเครือข่าย Site สำรอง และให้ Flow Data ทำงานได้เร็วยิ่งขึ้น

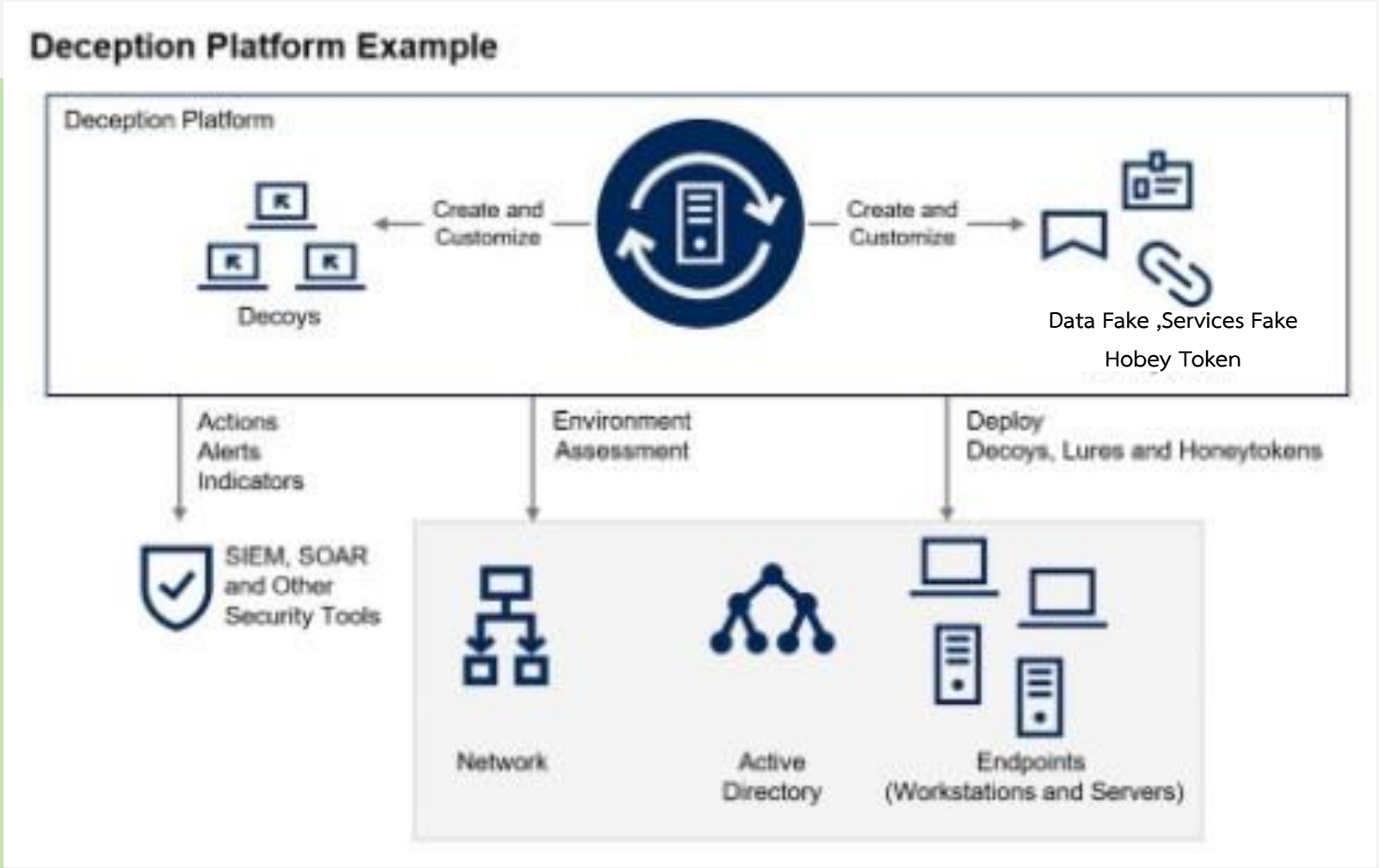
๓. เพิ่มประสิทธิภาพการป้องกันของอุปกรณ์ เช่น Memory ,Hard disk ,ความเร็วการประมวลผลข้อมูล เพื่อรองรับการป้องกันเว็บไซต์ของ กฟน. อีก ๒๓ ระบบงาน รวมเป็น ๓๖ ระบบงานในปี พ.ศ.๒๕๖๖

รายการ Website ที่อยู่ในการป้องกันของระบบในปี พ.ศ. ๒๕๖๖			
1.	App MEA Smart life Web	19.	Web Sever MEA Mdox
2.	App mea ev	20.	Web Server NAT SmartMetro
3.	App MEA e-fix	21.	Web Sever NAT TRD
4.	Web Sever Meaccd	22.	Web Server EDoc
5.	Web Sever MeaSAD	23.	Web Sever MEA 1130 _Web Server
6.	Web Sever SolarPV	24.	NAT_MedAppointment(ระบบนัดหมาย)
7.	Web Sever E-Services	25.	Web Sever MEA Login
8.	Web Sever EVCCC	26.	Web Sever NAT_sems-pcdweb
9.	Web Sever SolarPV	27.	Web Sever NAT_BIIS_WebSVR
10.	Web Sever NAT MEAOR Procurement	28.	Web Sever NAT_SCS_Production
11.	Web Sever NAT MEAORTH	29.	Web Sever NAT_smartgrid-iot
12.	Web Sever NAT iemp	30.	Web Sever NAT_smartdiagram
13.	Web Sever CCTV	31.	Web Sever NAT_iTimeSheet
14.	Web Sever NAT_iotdev (Chatbot)	32.	Web Sever NAT_BEMS BEMS (ระบบบริหารจัดการพลังงานในอาคาร)
15.	Web Sever NAT MEASY	33.	Web Sever NAT_iotdev ระบบ Cloud Smart Grid โปรเจค iot ในวง DMZ
16.	Web Server etax	34.	Web Server NAT_ictsub
17.	Web Sever GIS	35.	MEA testmeaor.mea.or.th
18.	Web Sever MEA_wms	36.	Web Sever NAT KMPubilc

๒. ระบบดักจับการลักลอบเข้าสู่เครือข่ายเทคโนโลยีสารสนเทศ จำนวน 1 ระบบ

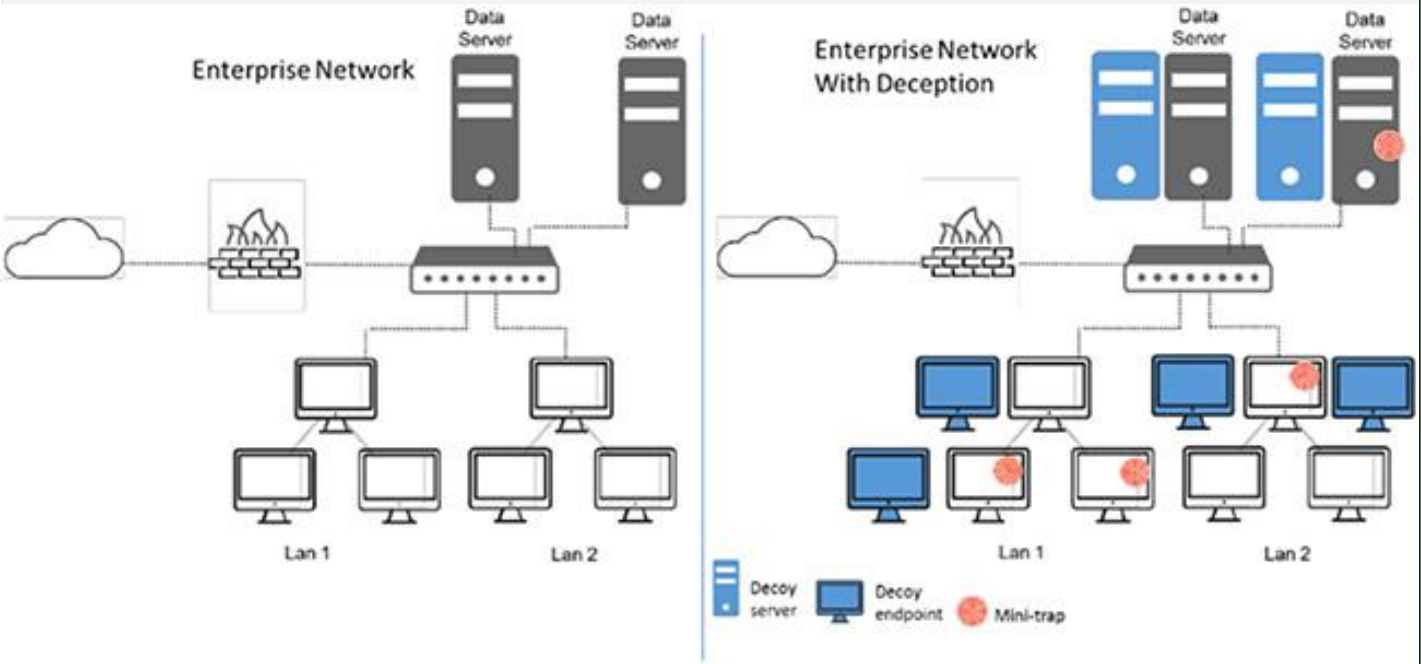
ระบบที่จะจัดซื้อ

Deception Solution คือการใช้เหยื่อล่อ นกต่อ หรือเล่ห์เหลี่ยมที่ถูกออกแบบมาเพื่อขัดขวาง หรือหลบหนีจากกระบวนการทางความเข้าใจของแฮ็คเกอร์ ขัดขวางเครื่องมือที่แฮ็คเกอร์ใช้โจมตีอัตโนมัติ ยืดเวลาที่แฮ็คเกอร์ต้องใช้โจมตีออกไป หรือตรวจจับการโจมตี การวางเทคโนโลยี Deception ไว้ด้านหลัง Firewall ทำให้องค์กรสามารถตรวจจับการเจาะระบบป้องกันได้อย่างแม่นยำมากขึ้นและนำข้อมูลมาวิเคราะห์เพื่อทำ Playbook เพื่อการป้องกันแบบเชิงรุก



การไฟฟ้านครหลวง
Metropolitan Electricity Authority

๒. ระบบดักจับการลักลอบเข้าสู่เครือข่ายเทคโนโลยีสารสนเทศ จำนวน 1 ระบบ



โซนการติดตั้ง

1. Data Center DMZ Zone
2. Data Center Internal Zone
3. Corporate Network
4. IP Network (link to SCADA system)

- สร้างเหยื่อล่อในระบบ Network ได้จำนวนไม่น้อยกว่า 500 Decoys IP Address และอย่างน้อย 50 VLANs
  สร้างเหยื่อล่อบน Endpoint หรือ Breadcrumbs จำนวนไม่น้อยกว่า 500 Endpoints
- มี Virtual Machine สำหรับสร้างกับดักล่อในรูปแบบ Real-OS Decoys ได้ไม่น้อยกว่า 12 VMs
  - Microsoft Windows 2 VMs
  - Microsoft Server 4 VMs
  - linux , MAC OS และอื่นๆ 6 VMs

การไฟฟ้านครหลวง
Metropolitan Electricity Authority

รายการอุปกรณ์คอมพิวเตอร์ที่ขออนุมัติ

รายการ		
๑.	ระบบป้องกันการบุกรุกเว็บไซต์ (Web Application Firewall)	๑ ระบบ
	๑.๑ อุปกรณ์ป้องกันการบุกรุกเว็บไซต์ (Web Application Firewall)	๔ ชุด
	๑.๒ ระบบบริหารจัดการอุปกรณ์ป้องกันการบุกรุกเว็บไซต์ (Web Application Firewall Management)	๑ ระบบ
๒.	ระบบดักจับการลักลอบเข้าสู่เครือข่ายเทคโนโลยีสารสนเทศ	๑ ระบบ

หลักสูตรการอบรม

รายการ		
๑.	หลักสูตรสำหรับผู้ดูแลอุปกรณ์ป้องกันการบุกรุกเว็บไซต์ (Web Application Firewall) จำนวน ๑ รุ่น รุ่นละ ๒ วัน	๕ คน
๒.	หลักสูตรสำหรับผู้แลระบบบริหารจัดการอุปกรณ์ป้องกันการบุกรุกเว็บไซต์ (Web Application Firewall Management) จำนวน ๑ รุ่น รุ่นละ ๒ วัน	๕ คน
๓.	หลักสูตรสำหรับผู้แลระบบดักจับผู้บุกรุกการเข้าสู่เครือข่าย (Deception) จำนวน ๑ รุ่น รุ่นละ ๒ วัน	๕ คน

แบบ คกก.มท. ๐๑

แบบ คกก.มท. ๐๑ (ปรับปรุง ก.ค. ๖๐)

แบบรายงานสรุปโครงการเพื่อพิจารณาความเหมาะสมของคุณลักษณะเฉพาะและราคา (ก่อนการจัดหา)

☐ เสนอคณะกรรมการฯ ของ มท. เพื่อพิจารณาให้ความเห็นชอบในหลักการ

☐ เสนอคณะกรรมการฯ ของ มท. เพื่อทราบ (ได้รับความเห็นชอบในหลักการจากคณะกรรมการของ.....(ระบุ).....ในการประชุมครั้งที่.....เมื่อวันที่.....)

ชื่อโครงการ ระบบเพิ่มประสิทธิภาพการตรวจจับและป้องกันภัยคุกคามบนแอปพลิเคชัน งบประมาณลงทุนประจำปี พ.ศ. ๒๕๖๕

รวมวงเงินโครงการ จำนวนเงิน ๓๑,๔๘๑,๗๕๔.๐๐ บาท (สามสิบเอ็ดล้านสี่แสนแปดหมื่นหนึ่งพันเจ็ดร้อยห้าสิบสี่บาทถ้วน) รวมภาษีมูลค่าเพิ่ม ๗ เปอร์เซ็นต์

ส่วนที่เป็นอุปกรณ์คอมพิวเตอร์ จำนวนเงิน ๓๑,๑๕๐,๐๕๔.๐๐ บาท (สามสิบเอ็ดล้านหนึ่งแสนห้าหมื่นห้าสิบสี่บาทถ้วน) รวมภาษีมูลค่าเพิ่ม ๗ เปอร์เซ็นต์

ฝ่ายมั่นคงปลอดภัยไซเบอร์และธรรมาภิบาลข้อมูล การไฟฟ้านครหลวง

ส่วนที่เป็นอุปกรณ์คอมพิวเตอร์

กรณีตรงตามเกณฑ์ของกระทรวงดิจิทัลฯ หรือเกณฑ์ที่ส่วนราชการอื่นประกาศกำหนด

ลำดับ	รายการ	ข้อตามเกณฑ์ (ชื่อเกณฑ์/ชื่อหน่วยงานที่ประกาศกำหนดเกณฑ์)	ราคาตามเกณฑ์	ราคาอ้างอิง	จำนวน	วงเงินรวม
๑	ไม่มีรายการ	-	-	-	-	
	รวมจำนวนเงินตามเกณฑ์					

กรณีไม่มีราคาตามเกณฑ์ของกระทรวงดิจิทัลฯ หรือเกณฑ์ที่ส่วนราชการอื่นประกาศกำหนด

ลำดับ	รายการ	การสืบราคาจากท้องตลาดรวมทั้งเว็บไซต์ต่าง ๆ (เปรียบเทียบอย่างน้อย ๓ ราย / ๓ ยี่ห้อ รวมทั้งเว็บไซต์อย่างน้อย ๑ เว็บไซต์)				ราคาอ้างอิง	จำนวน	วงเงินรวม	หมายเหตุ
		บริษัท เอ็ม เอฟ อี ซี จำกัด (มหาชน)	บริษัท ฟูจิตสึ (ประเทศไทย) จำกัด	บริษัท จัสทวาล คอม มิวนิเคชั่นซีสเต็ม จำกัด	เว็บไซต์				
1	ระบบเพิ่มประสิทธิภาพการตรวจจับและป้องกันภัยคุกคามบนแอปพลิเคชัน								

การไฟฟ้านครหลวง
Metropolitan Electricity Authority

แบบ คกก.มท. ๐๑

๑.๑	อุปกรณ์ป้องกันการบุกรุกเว็บไซต์ (Web Application Firewall)	ยี่ห้อ F5 รุ่น R5800	ยี่ห้อ Impreva รุ่น X8520	ยี่ห้อ Radware รุ่น Alteon D-7612SL	https://www.f5.com/solutions/application-security				มีเว็บไซต์ แต่ไม่ปรากฏราคาบนหน้าเว็บไซต์
		๓,๒๓๐,๐๐๐.๐๐	๓,๓๒๗,๗๐๐.๐๐	๓,๗๔๕,๐๐๐.๐๐	-	๓,๒๓๐,๐๐๐.๐๐	๕	๑๒,๘๔๐,๐๐๐.๐๐	
๑.๒	ระบบบริหารจัดการอุปกรณ์ป้องกันการบุกรุกเว็บไซต์ (Web Application Firewall Management)	ยี่ห้อ F5 รุ่น BIG-IQ	ยี่ห้อ Impreva รุ่น M170	ยี่ห้อ Radware รุ่น APsolute Vision ODS-VL2	https://www.f5.com/products/automation-and-orchestration/big-iq				มีเว็บไซต์ แต่ไม่ปรากฏราคาบนหน้าเว็บไซต์
		๑,๘๕๒,๗๕๐.๐๐	๑,๘๗๗,๕๐๐.๐๐	๒,๓๔๐,๐๐๐.๐๐	-	๑,๘๕๒,๗๕๐.๐๐	๑	๑,๘๕๒,๗๕๐.๐๐	
๒	ระบบตักจับผู้บุกรุกการเข้าสู่เครือข่าย (Deception)	ยี่ห้อ Acalvio รุ่น ShdowPlex	ยี่ห้อ Attivo รุ่น ABS-5500-SUB	ยี่ห้อ TrapX รุ่น 50 V-LANS	https://www.acalvio.com/product/#				มีเว็บไซต์ แต่ไม่ปรากฏราคาบนหน้าเว็บไซต์
		๑๖,๓๕๗,๓๐๕.๐๐	๑๖,๕๒๔,๕๐๐.๐๐	๑๗,๓๓๕,๐๐๐.๐๐	-	๑๖,๓๕๗,๓๐๕.๐๐	๓	๑๖,๓๕๗,๓๐๕.๐๐	
					รวมจำนวนเงินกรณีไม่มีราคาตามเกณฑ์			๓๑,๓๕๐,๐๕๔.๐๐	
					รวมจำนวนเงินส่วนที่เป็นอุปกรณ์คอมพิวเตอร์			๓๑,๓๕๐,๐๕๔.๐๐	

ส่วนที่เป็นอุปกรณ์อื่น ๆ

ลำดับ	รายการ						จำนวนเงิน	จำนวน	จำนวนเงินรวม
๑	ค่าติดตั้ง						๒๖๗,๕๐๐.๐๐	๑	๒๖๗,๕๐๐.๐๐
๒	ค่าฝึกอบรม						๖๔,๒๐๐.๐๐	๑	๖๔,๒๐๐.๐๐
					รวมจำนวนเงินส่วนที่เป็นอุปกรณ์อื่น ๆ				๓๓๑,๗๐๐.๐๐
					รวมวงเงินโครงการ				๓๑,๔๘๑,๗๕๔.๐๐

จึงเรียนมาเพื่อโปรดพิจารณา