เอกสาร...ก.๑๑.....

โครงการเพิ่มประสิทธิภาพความปลอดภัยด้านเครือข่าย

(Security Operation Center : SOC)

การประปานครหลวง

สารบัญ

ความจำเป็นของโครงการ ๑
ความเหมาะสมของการ Design ๓
ความเหมาะสมของราคา ๕
บทสรุปให้ผู้บริหาร ๖

ความจำเป็นของโครงการ

ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๔๔ ในส่วนที่ ๑ นโยบายและแผน ของหมวดที่ ๓ การรักษาความมั่นคงปลอดภัยไซเบอร์ บัญญัติให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว

ประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามวรรคหนึ่งอย่างน้อยต้องประกอบด้วยเรื่อง ดังต่อไปนี้

(๑) แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

โดยผู้ตรวจประเมิน ผู้ตรวจสอบภายใน หรือผู้ตรวจสอบอิสระจากภายนอก อย่างน้อยปีละหนึ่งครั้ง

(๒) แผนการรับมือภัยคุกคามทางไซเบอร์

เพื่อประโยชน์ในการจัดทำประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามวรรคหนึ่ง ให้สำนักงานโดยความเห็นชอบของคณะกรรมการจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานสำหรับให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนำไปใช้เป็นแนวทางในการจัดทำหรือนำไปใช้เป็นประมวลแนวทางปฏิบัติของหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศของตน และในกรณีที่หน่วยงานดังกล่าวยังไม่มีหรือมีแต่ไม่ครบถ้วนหรือไม่สอดคล้องกับประมวลแนวทางปฏิบัติและกรอบมาตรฐาน ให้นำมาประมวลแนวทางปฏิบัติและกรอบมาตรฐานดังกล่าวไปใช้บังคับ

และมาตรา ๕๘ ในส่วนที่ ๔ การรับมือกับภัยคุกคามทางไซเบอร์ บัญญัติให้ ในกรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ต่อระบบสารสนเทศซึ่งอยู่ในความดูแลรับผิดชอบของหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศใด ให้หน่วยงานนั้นดำเนินการตรวจสอบข้อมูลที่เกี่ยวข้อง ข้อมูลคอมพิวเตอร์ และระบบคอมพิวเตอร์ของหน่วยงานนั้น รวมถึงพฤติการณ์แวดล้อมของตน เพื่อประเมินว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้นหรือไม่ หากผลการตรวจสอบปรากฏว่าเกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ขึ้น ให้ดำเนินการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานนั้น และแจ้งไปยังสำนักงานและหน่วยงานควบคุมหรือกำกับดูแลของตนโดยเร็ว

การประปานครหลวง ซึ่งเป็นหนึ่งในหน่วยงานโครงสร้างพื้นฐานสำคัญของรัฐทางด้านระบบสาธารณูปโภค และจัดเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่มีข้อมูลส่วนบุคคลของประชาชนที่เป็นผู้ใช้น้ำในครอบครอง

กองบริหารเครือข่ายสื่อสารและความมั่นคงสารสนเทศ ฝ่ายเทคโนโลยีและสื่อสารสายงานเทคโนโลยีสารสนเทศ ซึ่งมีหน้าที่รับผิดชอบภารกิจด้านความมั่นคงปลอดภัยไซเบอร์ของการประปานครหลวง จึงได้ศึกษาและจัดทำแบบประเมินความเสี่ยง ณ วันที่ ๑๕ กันยายน ๒๕๖๓

แบบระบุและประเมินความเสี่ยง ปีงบประมาณ 2564 RM 1

วัตถุประสงค์ ☒ เชิงกลยุทธ์ แผนวิสาหกิจ กปน. ฉบับที่ 5 (ปี 2563 - 2565) SO-4 : การพัฒนาเทคโนโลยีดิจิทัล และนำนวัตกรรมไปใช้อย่างเป็นระบบ เพื่อเพิ่มขีด รายงานโดย: เลขานุการคณะทำงานบริหารความเสี่ยงฯ
☐ งาน

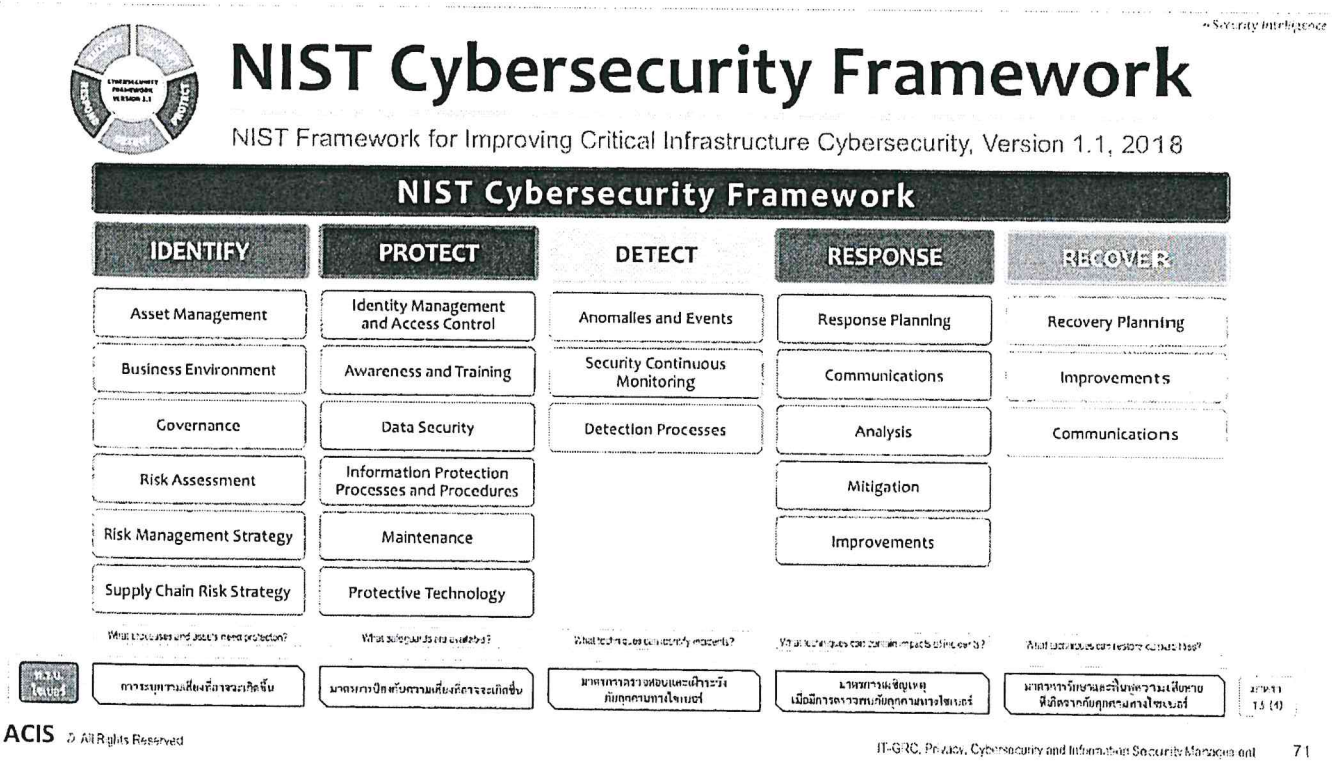
วัตถุประสงค์การบริหารความ 1) เพื่อให้เป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. 2550 และให้มีขีดความสามารถในการจัดเก็บที่เพียงพอรับรองรายงานโดย รวก.(ท)
2) เพื่อให้มีระบบบริหารจัดการและตอบสนองภัยคุกคามแบบอัตโนมัติ และจัดทำกระบวนการหรือ Playbook เพื่อตอบสนองต่อภัยคุกคามทางด้านไซเบอร์ได้อย่างมีประสิทธิภาพ
3) เพื่อให้มีระบบเฝ้าระวังและตรวจจับภัยคุกคามไซเบอร์อัจฉริยะที่นำเทคโนโลยี Artificial Intelligence และ Machine Learning มาใช้ วันที่

เลขที่ความเสี่ยง	ประเภทความเสี่ยง	ความเสี่ยง (Risk)	สาเหตุของความเสี่ยง (Risk Driver)	การควบคุมความเสี่ยงที่มีอยู่เดิม (Existing Risk Response)	ประเมินความเสี่ยงปัจจุบัน ณ วันที่ 15 กันยายน 2563 โอกาส	ผลกระทบ	ระดับความเสี่ยง	แผนรองรับความเสี่ยงที่ต้องทำเพิ่มเติม (Required Risk Response)	กำหนดเวลาสิ้นสุดแผน	ผู้รับผิดชอบแผนบริหารความเสี่ยง	ประเมินความเสี่ยงหลังทำแผนเพิ่มเติม ณ วันที่ 30 กันยายน 2565 โอกาส	ผลกระทบ	ระดับความเสี่ยง
	ด้าน IT	ระบบสารสนเทศของ กปน. โดนโจมตี ทำให้เกิดความเสียหาย / สูญหาย / รั่วไหล ของข้อมูล รวมไปถึงการหยุดชะงักของระบบงาน และการให้บริการต่าง ๆ ของ กปน.	1) ยังไม่มีระบบบริหารจัดการความปลอดภัยสำหรับเครื่องที่เข้าถึงระบบงานจากภายนอกองค์กร เช่น Work From Home อันเป็นช่องทางนำพาภัยคุกคามเข้าสู่องค์กรโดยตรง 2) ยังไม่มีกระบวนการรับมือการโจมตีที่ทันต่อสถานการณ์ เช่นระบบ AI , ML , EDR และ Playbook 3) บุคลากรไม่เพียงพอต่อภารกิจการเฝ้าระวัง และตอบสนองต่ออาชญากรรมทางไซเบอร์ที่มีความซับซ้อนสูงมากในปัจจุบัน	ระบบป้องกันเดิม ได้แก่ DDoS , Gateway IPS , Gateway Firewall , Branch Firewall , WiFi Security , DNS Security , Web Proxy , RADIUS Proxy , Active Directory , Web Application Firewall , Service Gateway , AntiVirus	3	4	สูง	1) จัดหาระบบ VDI (Virtual Desktop Infrastructure) 2) จัดหาระบบ SOC (Security Operation Center) 3) ประสานงานกับ HR เพื่อจัดหาบุคลากรเพิ่มขึ้น	30 กย 64 30 กย 65 30 กย 64	ฝยส.	2	3	ปานกลาง

รวมถึงแผนฉุกเฉินกรณีการถูกโจมตีระบบเทคโนโลยีสารสนเทศทางไซเบอร์ อันเป็นส่วนหนึ่งของแผนบริหารความตอเนื่องทาง. ธุรกิจ (Business Continuity Plan: BCP) และยกขึ้นเป็นส่วนหนึ่งของแผนรัฐวิสาหกิจการประปานครหลวงฉบับที่ ๕ โดยการจัดทำโครงการเพิ่มประสิทธิภาพความปลอดภัยด้านเครือข่าย (Security Operation Center : SOC) ขึ้น

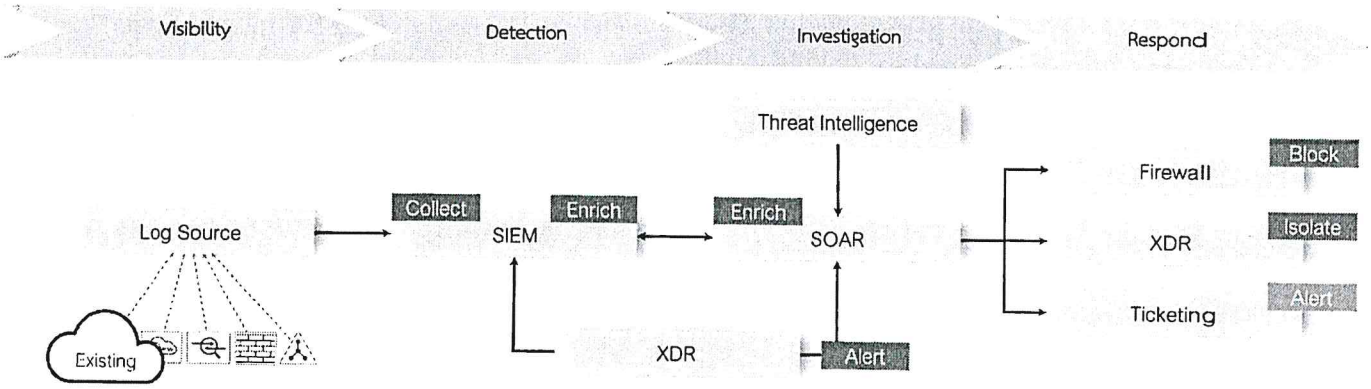
ความเหมาะสมของการ Design

การออกแบบระบบในโครงการเพิ่มประสิทธิภาพความปลอดภัยด้านเครือข่าย (Security Operation Center : SOC) การประปานครหลวง ออกแบบโดยอ้างอิงสถาปัตยกรรมความมั่นคงปลอดภัยไซเบอร์ ที่ถอดแบบมาจากกรอบการทำงานด้านความมั่นคงปลอดภัยไซเบอร์ (NIST Cybersecurity Framework) ของสถาบันมาตรฐานและเทคโนโลยีแห่งชาติประเทศสหรัฐอเมริกา (National Institute of Standards and Technology)



ซึ่ง NIST Cybersecurity Framework เป็นกรอบการทำงานที่ได้รับการยอมรับและถูกอ้างอิงถึงมากที่สุดในปัจจุบัน ทั้งจากสำนักตรวจสอบและที่ปรึกษาด้านความมั่นคงปลอดภัยไซเบอร์ระดับชาติและทั่วโลก

ซึ่งจากกรอบการทำงานข้างต้น ทางคณะทำงานได้ศึกษาเพิ่มเติมถึงแนวปฏิบัติที่เหมาะสม จากแหล่งข้อมูลต่าง ๆ และจากเจ้าตัวแทนบริษัทเจ้าของผลิตภัณฑ์ชั้นนำในท้องตลาดในแต่ละส่วนที่เกี่ยวข้อง จนสามารถสรุปออกมาเป็นรูปแบบมาตรฐานที่นิยมใช้กันในขณะนี้ ตาม Logical Diagram นี้



Log Source จะหมายถึงอุปกรณ์ Security ต่าง ๆ ทั้ง Network , Endpoint และอื่น ๆ เช่น Firewall , IPS , Proxy , Antivirus , Active Directory ซึ่งเป็นแหล่งกำเนิดของข้อมูลบันทึกการทำงานต่าง ๆ (Raw Log)

XDR (Extended Detection and Response) คือระบบที่รวมการทำงานของ EDR กับ NTA เข้าด้วยกัน เฝ้าดูพฤติกรรมการใช้งานในระบบเครือข่าย โดยจะเก็บข้อมูลไว้ใน Cloud และทำการวิเคราะห์เพื่อตรวจจับ แจ้งเตือน และตอบสนองเหตุการณ์ภัยคุกคามได้อย่างอัตโนมัติ

EDR (Endpoint Detection and Response) คือระบบการตรวจจับ เก็บหลักฐาน และตอบสนองต่อภัยคุกคามไซเบอร์บนเครื่อง Endpoint ต่าง ๆ

NTA (Network Traffic Analysis) คือระบบการตรวจจับ เก็บหลักฐาน และตอบสนองต่อภัยคุกคามไซเบอร์ในระดับเครือข่าย

SIEM (Security Information and Event Management) คือระบบจัดเก็บและวิเคราะห์ข้อมูลความปลอดภัยของระบบเครือข่ายขององค์กร โดยใช้ข้อมูล Log จากอุปกรณ์รักษาความปลอดภัยเครือข่าย, อุปกรณ์เครือข่าย, ระบบงาน และ Application ต่างๆ

SOAR (Security Orchestration, Automation และ Response) คือแพลตฟอร์มด้านความปลอดภัย ที่ผสานการทำงานร่วมกัน และตอบสนองต่อภัยคุกคามที่เกิดขึ้นได้โดยอัตโนมัติแบบเรียลไทม์ ด้วยการจัดการ Threat Intelligence แบบองค์รวม

Threat Intelligence คือข้อมูลวิเคราะห์เชิงลึก อันเป็นองค์ประกอบหลักสำคัญของระบบนิเวศน์ไซเบอร์ซีเคียวริตี้ทุกระบบ (Cybersecurity Ecosystem) โดย Gartner ได้นิยามข้อมูลเชิงลึกเช่นนี้ว่าเป็นองค์ความรู้เชิงหลักฐานประจักษ์ (Evidence-Based Knowledge)

ความเหมาะสมของราคา

การประปานครหลวงมีกระบวนการกำหนดกรอบวงเงินงบประมาณในโครงการสำคัญต่าง ๆ ที่มีความสำคัญและความซับซ้อนสูง ซึ่งโครงการเพิ่มประสิทธิภาพความปลอดภัยด้านเครือข่าย (Security Operation Center : SOC) ของการประปานครหลวงก็เช่นเดียวกัน คณะทำงานได้เริ่มต้นจากการประเมินความเสี่ยงสำคัญต่าง ๆ ขององค์กร สำหรับความเสี่ยงในด้านความมั่นคงไซเบอร์ คณะทำงานได้ระบุปัจจัยต่าง ๆ ที่ส่งผลต่อความเสี่ยงองค์กร วางแนวกลยุทธ์ในการบริหารจัดการความเสี่ยง ศึกษาแนวปฏิบัติ และระบุวิธีการที่เหมาะสมกับสภาพแวดล้อมการทำงานเฉพาะตัวของการประปานครหลวงขึ้น

จากผลการศึกษา คณะทำงานจึงได้เลือกกรอบการทำงานด้านความมั่นคงปลอดภัยไซเบอร์ของ NIST Cybersecurity Framework ตามที่กล่าวไปแล้วข้างต้นในเรื่องความเหมาะสมของการ Design มาเป็นแนวคิดตั้งต้น แล้วติดต่อไปยังตัวแทนเจ้าของผลิตภัณฑ์ต่าง ๆ ที่เกี่ยวข้องกับกรอบการทำงานดังกล่าว โดยคัดเลือกเฉพาะผลิตภัณฑ์ชั้นนำในท้องตลาดซึ่งอ้างอิงตามรายงานของสำนักวิจัยตลาดที่ได้รับการยอมรับในระดับสากล เช่น Gartner Magic Quadrant และ Forrester Wave Report เป็นต้น แล้วเชิญตัวแทนเจ้าของผลิตภัณฑ์เหล่านั้นเข้าให้ข้อมูลเกี่ยวกับผลิตภัณฑ์ (Product Presentation) และดำเนินการทดสอบการทำงานของผลิตภัณฑ์ (Solution Demo - PoC) เพื่อรวบรวมข้อมูลขีดความสามารถและความเข้ากันได้กับสภาพแวดล้อมการทำงานของการประปานครหลวง

เมื่อสามารถระบุผลิตภัณฑ์ที่เหมาะสมได้แล้ว คณะทำงานจึงติดต่อกลับไปยังตัวแทนจำหน่ายของผลิตภัณฑ์แต่ละรายที่เข้าเกณฑ์เพื่อขอราคาในขั้นต้นมาใช้เปรียบเทียบมูลค่ากับขอบเขตความสามารถของผลิตภัณฑ์ที่นำเสนอ และคณะทำงานก็ได้ทำการต่อรองราคาและขอบเขตความสามารถของผลิตภัณฑ์ยี่ห้อต่าง ๆ อีกหลายครั้ง จนสามารถระบุกรอบวงเงินงบประมาณที่สามารถผ่านกระบวนการคัดกรองและได้รับความเห็นชอบจากคณะกรรมการบริหารทุกคณะของการประปานครหลวงได้ทั้งหมด ทั้งด้านความเสี่ยงองค์กร ด้านงบประมาณ และด้านไอที จึงได้จัดทำโครงการเพิ่มประสิทธิภาพความปลอดภัยด้านเครือข่าย (Security Operation Center : SOC) นี้ขึ้น

บทสรุปให้ผู้บริหาร

เนื่องด้วยการประปานครหลวงอันเป็นหนึ่งในหน่วยงานโครงสร้างพื้นฐานสำคัญของรัฐด้านระบบสาธารณูปโภค และจัดเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่มีข้อมูลส่วนบุคคลของประชาชนที่เป็นผู้ใช้น้ำในครอบครอง อันจำเป็นต้องมีกระบวนการกำกับดูแลมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ที่รัดกุมและเป็นไปตามมาตรฐานสากล ประกอบกับการบังคับใช้พระราชบัญญัติและกฎหมายต่าง ๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ที่มีเพิ่มขึ้นอย่างมาก รวมไปถึงระดับความเสี่ยงจากการโจมตีและเข้ายึดครองระบบสารสนเทศของอาชญากรไซเบอร์ข้ามชาติและการก่อวินาศกรรมทางเทคโนโลยีสารสนเทศที่ทวีความรุนแรงมากขึ้นทั่วโลกในปัจจุบัน

ด้วยกระบวนการบริหารจัดการความเสี่ยงองค์กร การประปานครหลวงได้ตระหนักถึงความสำคัญในการปกป้องระบบสารสนเทศขององค์กรให้มีความมั่นคง ปลอดจากภัยคุกคามทางไซเบอร์ การประปานครหลวงจึงได้กำหนดแผนจัดตั้งศูนย์ Security Operation Center ขึ้นเป็นกลยุทธ์หนึ่งของยุทธศาสตร์องค์กร โดยมีกระบวนการกลั่นกรองการใช้งบประมาณภายใน ซึ่งได้มีมติเห็นชอบแล้วให้ดำเนินการจัดตั้งศูนย์ Security Operation Center ขึ้นอย่างเร่งด่วน ภายใต้กรอบวงเงินงบประมาณที่ได้รับการจัดสรรตามกระบวนการที่รัดกุมแล้วนั้น การประปานครหลวงจึงได้จัดทำโครงการเพิ่มประสิทธิภาพความปลอดภัยด้านเครือข่าย (Security Operation Center : SOC) ขึ้น โดยมีรายละเอียดตามที่ได้นำเสนอไปแล้ว