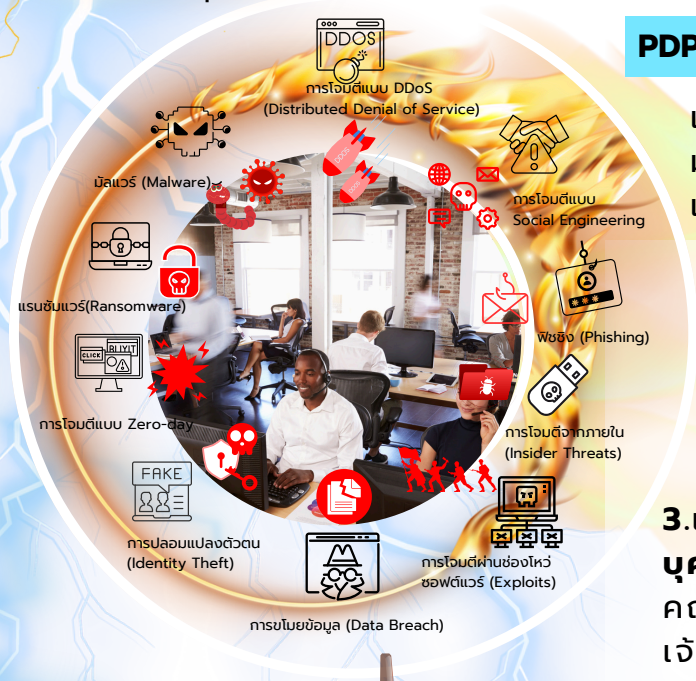
Solution PDPA to Security together

การพัฒนา PDPAกับการพัฒนาเทคโนโลยี Securityควรไปพร้อมกัน

SGC เสนอไอเดีย! การดำเนินการ PDPAและเทคโนโลยี Security ไปด้วยกัน ไม่ซับซ้อน ประหยัดเวลา มีประโยชน์มาก! โดยทั้ง2สิ่งนี้ต้องทำพร้อมกันระยะยาวตลอดเส้นทาง เพื่อการปกป้องข้อมูลให้ปลอดภัยไม่รั่วไหลและถูกกฎหมาย!

ภัย Cyber ที่หน่วยงานและองค์กรอาจเผชิญในปัจจุบันมีหลายรูปแบบ เช่น มัลแวร์ (Malware),ฟิชชิง(Phishing) ,แรนซัมแวร์ (Ransomware),การโจมตีแบบ Social Engineering เป็นต้น เหล่านี้คือภัย Cyber ที่ทุกแห่งจะต้องเจอในปัจจุบันและในอนาคตอันใกล้



PDPA หรือกฎหมายคุ้มครองข้อมูลส่วนบุคคล

เริ่มปี 2562 บังคับใช้จริงปี 2565 มีกฎหมายรองที่สำคัญออกมากว่า 15 ฉบับ สิ่งที่หน่วยงานต้องประจำตลอดไปของหน่วยงานเกี่ยวกับPDPA คือ

1.ทำประกาศแจ้งเตือนโนบายคุ้มครองข้อมูลส่วนบุคคล ทุกกิจกรรมที่เกี่ยวข้องกับข้อมูลส่วนบุคคล

2.ทำมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล

3.เมื่อมีการร้องเรียนหรือการละเมิดเกี่ยวกับข้อมูลส่วนบุคคลต้องการประเมินความเสี่ยงและทำการแจ้งต่อคณะกรรมการคุ้มครองข้อมูลส่วนหรือบุคคลและ/หรือเจ้าของข้อมูลส่วนบุคคล

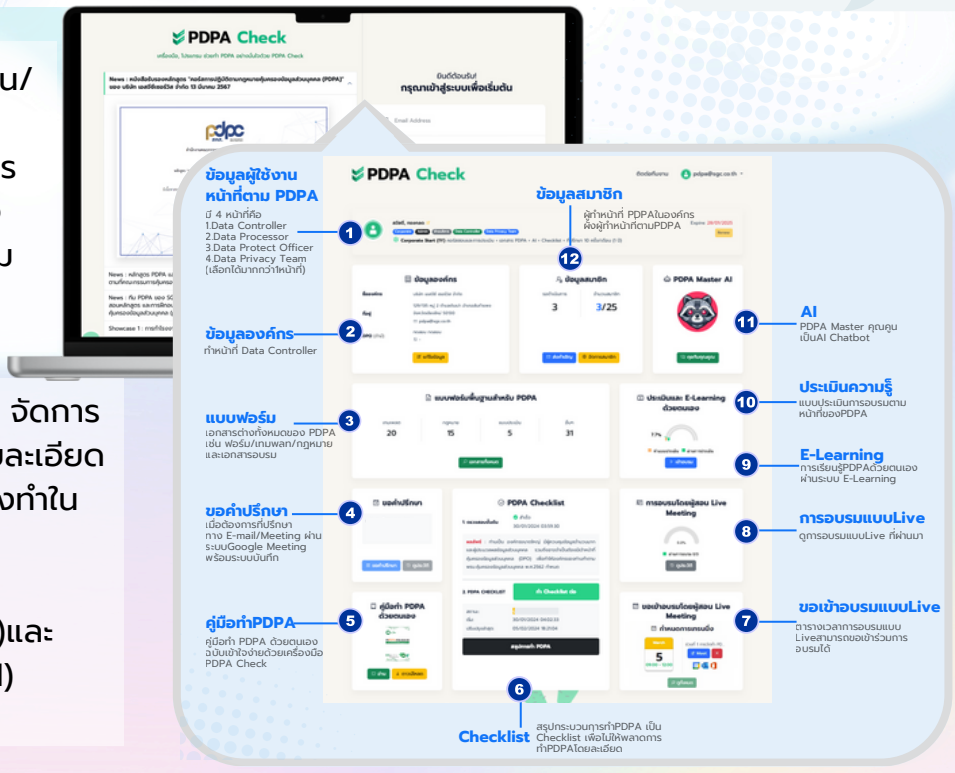
Solution นี้เหมาะกับ หน่วยงานที่มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หรือหน่วยงานที่ต้องการเครื่องมือบริหารจัดการPDPAกับระบบ Cyber Security ทำงานสอดคล้องกันโดยอัตโนมัติ

เครื่องมือช่วย

ช่วยทำ PDPA มากกว่า 12 ตัวช่วย

SGC ขอเสนอ Solution PDPA to Security together ประกอบด้วย

1.โปรแกรม PDPACheck สำหรับพนักงาน/ทุกสาขา/ทุกคนได้ใช้ เพื่อช่วยทำPDPA เช่น ระบบอบรม ระบบประเมิน ระบบเอกสาร ความรู้ PDPAทำให้พนักงานมีความรู้เข้าใจ PDPA ทำให้พนักงานทุกคนทำ PDPAเชื่อมกับระบบ Security สำนักงานใหญ่ได้



2.โปรแกรม Alltra ระบบจัดการส่วนกลาง จัดการPDPAทั้งหมดพร้อมส่งข้อมูล เงื่อนไข รายละเอียดการใช้งาน เปิดเผย ส่งออกข้อมูล สิ่งที่ต้องทำในแต่ละกิจกรรมไปใช้ในทางปฏิบัติไปให้ระบบ Security เช่น วิเคราะห์วิเคราะห์ช่องโหว่ (Vulnerability) และ ภัยคุกคาม (Threat)และ Threat and Safeguard Matrix (TaSM)

ALLTRA

จัดการ PDPA และ Log

จัดการ PDPA และช่วยทำ Security

***Alltra Log ได้รับการรับรองมาตราฐานจาก NECTEC**

ตัวอย่าง **กิจกรรม การรับสมัครงาน** -วิเคราะห์วิเคราะห์ช่องโหว่ (Vulnerability) และภัยคุกคาม (Threat)

กิจกรรม	ภัยคุกคาม (Threat)	ผลกระทบ (Impact)	ความน่าจะเป็น (Likelihood)	ระดับความเสี่ยง (Risk Level)	มาตรการป้องกัน (Safeguard)
การรับสมัครงาน	การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต (Unauthorized Access)	สูญเสียความเป็นส่วนตัว, ถูกเลือกปฏิบัติ, ข้อมูลถูกนำไปใช้ในทางที่ผิด	ปานกลาง	สูง	เข้ารหัสข้อมูล, ควบคุมการเข้าถึง, กำหนดสิทธิ์การเข้าถึง, ตรวจสอบและบันทึกกิจกรรมการเข้าถึงข้อมูล
	การเปิดเผยข้อมูลโดยไม่ได้ตั้งใจ (Accidental Dis[illegible]sure)	สูญเสียความเป็นส่วนตัว, เสียชื่อเสียง, ถูกเลือกปฏิบัติ	ต่ำ	ปานกลาง	อบรมพนักงาน, กำหนดนโยบายและขั้นตอนการจัดการข้อมูลที่ชัดเจน, ทำลายข้อมูลที่ไม่จำเป็น
	[illegible]	[illegible]	ต่ำ	[illegible]	[illegible]

ตัวอย่าง **กิจกรรม การรับสมัครงาน** - สร้างThreat and Safeguard Matrix (TaSM)

ภัยคุกคาม (Threats)	Identify (ระบุ)	Protect (ป้องกัน)	Detect (ตรวจจับ)	Respond (ตอบสนอง)	Recover (กู้คืน)
• Server Attack: การโจมตีเซิร์ฟเวอร์ที่เก็บข้อมูลในสมัครงาน อาจทำให้ข้อมูลสูญหายหรือถูกขโมยได้ • Web App Attack: การโจมตีเว็บแอปพลิเคชันที่ใช้รับใบสมัครงาน อาจทำให้ข้อมูลรั่วไหลหรือระบบขัดข้องได้ • Phishing: การหลอกลวงผู้สมัครให้กรอกข้อมูลส่วนตัวในเว็บไซต์ปลอม อาจ[illegible]	• Application Security Tools: ใช้เครื่องมือตรวจสอบความปลอดภัยของเว็บแอปพลิเคชัน • Breach & Attack Simulation: จำลองการโจมตีเพื่อทดสอบระบบ [illegible]etration Tests:	• API Security Tools: ใช้เครื่องมือป้องกันการโจมตี API • CASB: ใช้ Cloud Access Security Broker เพื่อควบคุมการเข้าถึงระบบคลาวด์ • Data Masking: ปกปิดข้อมูลสำคัญในใบสมัคร[illegible] • DLP: ใช้ Data [illegible]	• Deception Technology: สร้างระบบล่อเพื่อดักจับผู้โจมตี • [illegible]ewall (Layer 3): ใช้[illegible]อลล์เพื่อป้องกันการเข้าถึง[illegible]ยไม่[illegible]ญาต • [illegible]etection System เพื่อตรวจจับการบุกรุก • Si[illegible]: ใช้ Security In[illegible]ation [illegible]Eve[illegible] [illegible]Management[illegible]	• Deception Technology: สร้างระบบล่อเพื่อดักจับผู้โจมตี • Firewall (Layer 3): ใช้ไฟร์วอลล์เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต • IDS: ใช้ Intrusion Detection System เพื่อตรวจจับการบุกรุก [illegible]M/XDR: ใช้ Security [illegible]ation and[illegible]ent [illegible]Extended [illegible]Response	• Audit/Evaluate Controls: ตรวจสอบและประเมินมาตรการควบคุมความปลอดภัย • Backups: กู้คืนข้อมูลในสมัครงานจากข้อมูลสำรอง • BCP: ใช้ Business Continuity Plan เพื่อให้ระบบสามารถทำงานต่อได้ในการณ์ที่[illegible]การณ์ไม่

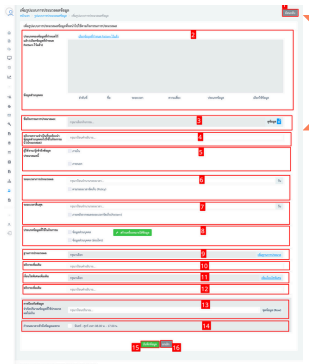
3.ระบบจัดการกิจกรรมการประมวลผลกับอุปกรณ์รักษาความปลอดภัย โดยสามารถนำข้อมูล PDPA มาเชื่อมกับระบบ Security เดิม และ/หรือเสนอทางเลือกสำหรับระบบ Security ที่เหมาะสมกับความเสี่ยงและกิจกรรม

ตัวอย่าง **กิจกรรม การรับสมัครงาน** การทำงานร่วมระหว่าง Microsoft Defender for Endpoint ร่วมกับ Alltra มีการจัดเก็บ ใช้งาน fileข้อมูลส่วนบุคคลอ่อนไหวชื่อ Quarantine ต้องการแจ้งเตือนเมื่อมีผู้เข้าใช้งาน

ALLTRA User ทั่วไปของ Alltra ทำตามระเบียบปฏิบัติกฎหมาย PDPA คือ บันทึกกิจกรรมประมวลผล file Quarantine

ALLTRA ระบบจะสร้างกฎ Automated Investigation and Remediation (AIR) ใน Microsoft Defender for Endpoint สามารถทำได้ผ่าน Microsoft 365 Defender portal และ/หรือAPI

Microsoft Defender for Endpoint



ข้อ 11 เลือกแจ้งเตือน
เมื่อมีผู้เข้าไปใช้งาน file Quarantine

```
POST
https://api.security.microsoft.com/api/machines/{id}
/startInvestigation
Authorization: Bearer <access_token>
Content-Type: application/json
{
    "Comment": "Quarantine suspicious files",
    "TriggerType": "Alert",
    "Conditions": {
        "AlertSeverity": "High",
        "AlertTitleContains": "Suspicious file detected"
    },
    "Actions": [
        {
            "ActionType": "QuarantineFile"
        },
        {
            "ActionType": "NotifyUser",
            "UserMessage": "A suspicious file has
been quarantined."
        }
    ]
}
```

ชื่อกฎ: Quarantine suspicious files ประเภททริกเกอร์: Alert
เงื่อนไข:
- Alert severity: High
- Alert title contains: "Suspicious file detected"

การดำเนินการ:
- Quarantine file
- Notify security team

คำอธิบาย: กฎนี้จะทำงานเมื่อมีการแจ้งเตือน (Alert) ระดับความรุนแรงสูงที่มีชื่อว่า "Suspicious file detected" ระบบจะทำการกักกันไฟล์ที่น่าสงสัยและแจ้งเตือนทีมรักษาความปลอดภัย

ติดต่อเรา

SGC SERVICE CO.,LTD 090-9192898 PDPA@SGC.CO.TH SGC.CO.TH PDPACHECK.COM