Cybersecurity Awareness Training

1. Mitr Phol Group places great importance on raising awareness and understanding, as well as providing knowledge on methods of preventing cyberattacks and cyber threats to employees throughout the organization. The aim is to instill a sense of responsibility for maintaining cybersecurity and to enable them to handle various types of cyberattacks. This is done through the organization's online communication channels, such as email and posters, on a monthly basis, covering topics like different types of cyber threats, recognizing scams, and more. Additionally, continuous cybersecurity awareness training is provided, with national experts such as Air Marshal Amorn Chomchoey giving special lectures. He recently gave a talk on "Cybersecurity in Thailand" to senior executives to enhance their knowledge, understanding, awareness, and readiness to prevent upcoming cyber threats in 2023. Moreover, the Cybersecurity policy is communicated to all employees and necessary trainings are provided.

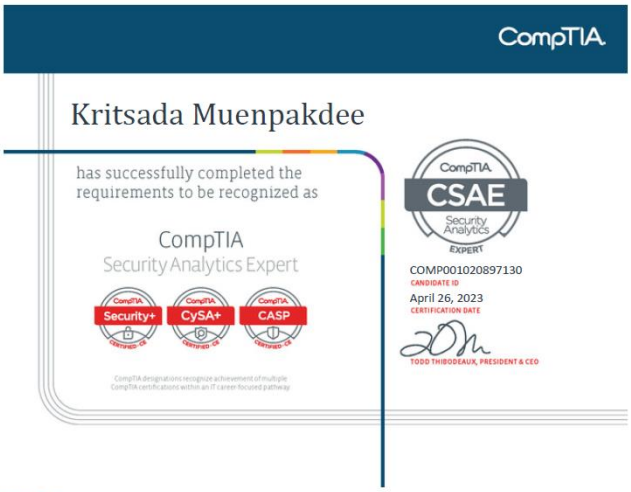
2. The activities and training sessions, which are organized both in Onsite and Online formats, can be summarized as follows:

หลักสูตร	วัตถุประสงค์	กลุ่มผู้เข้าร่วม	ระยะเวลา
1. สัมนาเรื่อง แนวโน้มภัยคุกคาม ด้านไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคล ปี 2566	สร้างการรับรู้ แนวทางของภัยไซเบอร์ในยุคปัจจุบัน เพื่อเป็นประโยชน์ต่อการวางแผนรับมือและป้องกัน	คณะกรรมการ CSC และพนักงาน	8 ก.พ. 2566
2. สื่อสารนโยบายและแนวปฏิบัติงาน ด้านความมั่นคงปลอดภัยทางไซเบอร์	สร้างการรับรู้ นโยบายและแนวปฏิบัติงาน ด้านความมั่นคงปลอดภัยทางไซเบอร์ของกลุ่มมิตรผล	DT Team	10 ส.ค. 2566
3. สื่อสารวิธีปฏิบัติงานด้านความมั่นคงปลอดภัยทางไซเบอร์	สร้างการรับรู้ และเตรียมพร้อมป้องกัน และลดความเสี่ยง ด้านความมั่นคงปลอดภัยไซเบอร์ ตามหลักมาตรฐานสากลขององค์กร	ผู้ให้บริการภายนอกที่เข้าถึงระบบสารสนเทศของกลุ่มมิตรผล	30 ส.ค. 2566
4. ทดสอบความตระหนักรู้ของบุคลากรด้วยการสุ่มทดสอบ Phishing	สร้างการรับรู้ แนวทางของภัยไซเบอร์ในยุคปัจจุบัน เพื่อเป็นประโยชน์ต่อการวางแผนรับมือและป้องกัน	พนักงาน กลุ่มมิตรผล	2 ครั้งต่อปี
5. การซ้อมแผน Cyberdrill	เตรียมความพร้อมรับมือภัยคุกคาม และปรับปรุงกระบวนการปฏิบัติงาน	DT Team DPO Team Size Up Team	2 ครั้งต่อปี
6. สัมนาเรื่อง แชร์ประสบการณ์ ด้านไซเบอร์ที่เกิดขึ้นจริง โดย พลอากาศตรี อมร ชมเชย	สร้างการรับรู้ บทเรียนจากภัยไซเบอร์ ที่เกิดขึ้นจริง เพื่อวางแผนรับมือและป้องกัน	คณะกรรมการ CSC และพนักงาน	8 ก.ย. 2566
7. ประชาสัมพันธ์สื่อสารแจ้งเตือนภัยคุกคามไซเบอร์ "Cyber Alert"	สร้างการรับรู้ และแนวทางป้องกันรับมือภัยคุกคามด้านไซเบอร์	พนักงาน กลุ่มมิตรผล	มากกว่า 12 ครั้ง เป็นประจำทุกเดือน

3. The personnel have been divided into 8 groups based on risk levels and the necessity to acquire knowledge relevant to their work. These groups include the Board of Directors, senior executives, current employees, new employees, and front-line workers who are often at higher risk, such as those in finance, procurement, and marketing departments. It also includes those responsible for managing Cybersecurity and the Information Technology department, who require deeper knowledge than regular users. Employees responsible for Cybersecurity are required to attend specialized training, pass examinations, and obtain professional certifications to strengthen the professional management of Cybersecurity and Personal Data Protection within Mitr Phol Group, as illustrated

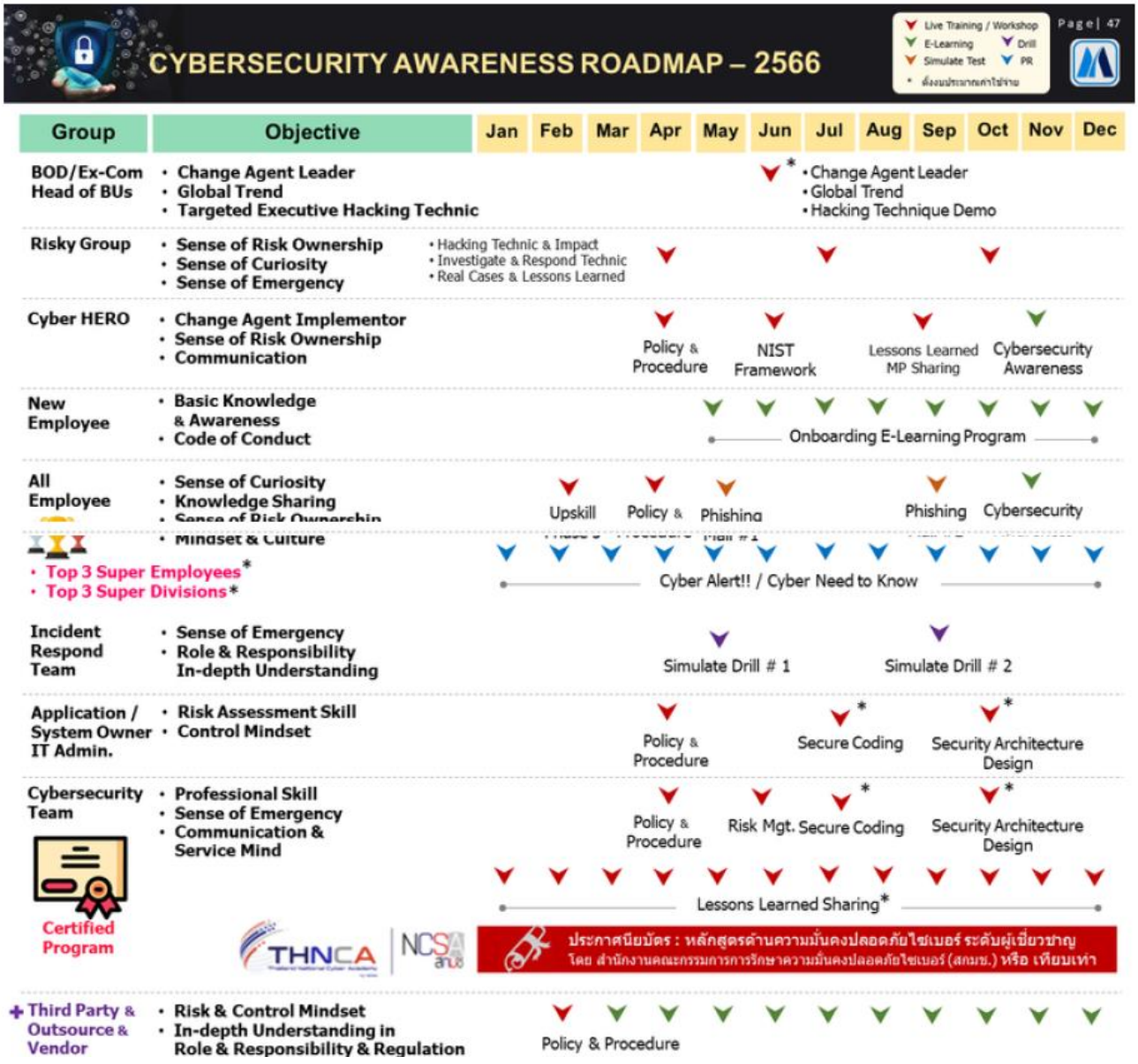
ระดับผู้เชี่ยวชาญ

Certificate to Our Cyber Security Team For successfully completing the Expert-Level Cybersecurity Training Program from The Office of the National Cybersecurity Committee



ระดับสากล

Certificate of Completion for Specialized Knowledge Training and Passing the Examination



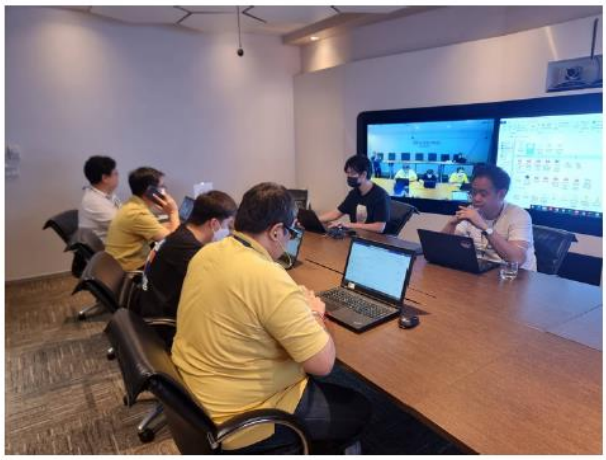
In addition, a Cybersecurity training plan has been developed in various formats, carefully selecting the content of courses and awareness-building activities to ensure they are appropriate and aligned with the different groups of personnel within Mitr Phol Group. The implementation of this plan is closely monitored, and knowledge is

continuously tested. The main objective is to establish a culture of cybersecurity awareness, ensuring that Mitr Phol employees are informed, aware, and able to apply this knowledge correctly in their daily work, as illustrated. In addition, KPIs of cybersecurity are assigned to relevant employees and that it is part of their annual performance review.

4. Cyber Alert Channels for Employees and Stakeholders (Cyber Alert!!)

5. Cyber Incident Response Drill (Cyber Drill)

The Company has conducted incident response plan, at least semi-annually as seen in the two sets of picture below.

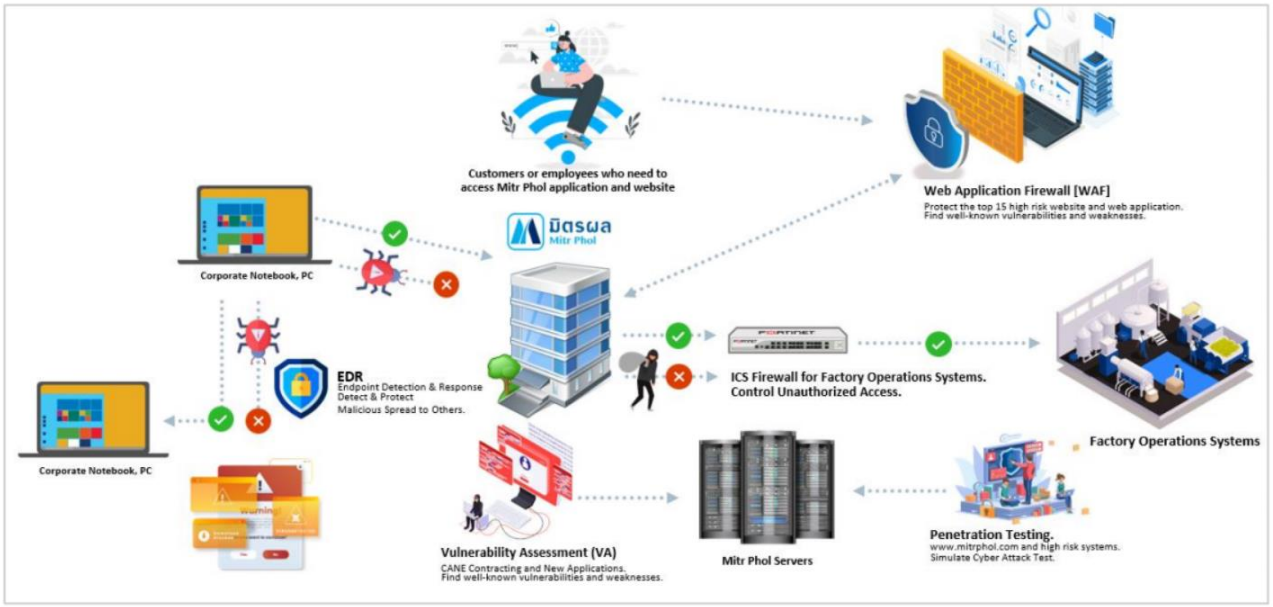


Cyber Incident Response Drill (Tabletop Exercise)

Overview of Cybersecurity and Personal Data Protection Technologies in 2023

This figure presents a comprehensive overview of the technologies and systems implemented by Mitr Phol Group in 2023 to enhance cybersecurity and protect personal data. The focus includes:

- Advanced Cybersecurity Technologies: Deployment of cutting-edge solutions such as firewalls, intrusion detection systems (IDS), and encryption protocols to protect against evolving cyber threats.
- Data Privacy Measures: Implementation of data protection technologies that align with regulations like PDPA (Personal Data Protection Act) to safeguard personal information and ensure compliance with global standards.
- Automation and AI: Utilization of AI and machine learning to detect anomalies, automate threat response, and predict potential security risks.
- Cyber Incident Management: Tools like JIRA Service Management for tracking and managing cyber incidents efficiently.
- Employee Awareness Programs: Continuous education and awareness training programs tailored to different roles within the organization to foster a culture of cybersecurity.



In terms of technology, Mitr Phol Group has considered the adoption of various technologies, focusing on the balance between maintaining security and flexibility to ensure business goals are met. The following key areas have been implemented:

- **Multi-Factor Authentication (MFA)**: A multi-step authentication process where users enter a password and a verification code from another device (e.g., mobile phone) to enhance security for accessing critical systems.
- **Cloud Management Gateway (CMG) and System Center Configuration Manager (SCCM)**: These tools allow centralized control over software installation and updates on computers and critical systems, ensuring that software is always up to date.
- **BYOD (Bring Your Own Devices)**: Employees are permitted to use personal devices for work while maintaining data security. Unauthorized individuals are denied access to the company's systems.
- **Data Labeling**: Documents are assigned confidentiality levels, allowing access, editing, and sharing permissions based on the sensitivity of the information.
- **Data Loss Prevention (DLP)**: This system prevents the loss or leakage of important or sensitive data through email or file-sharing platforms.
- **Network Access Control (NAC)**: Only authorized devices are allowed to connect to the company's network, enhancing network security.
- **Security Operation Center (SOC)**: This center collects and analyzes computer traffic data to detect potential abnormalities. Traffic data is sent to the operations center for real-time monitoring and anomaly detection.
- **Database Encryption**: Critical database information is encrypted, making it unreadable to unauthorized users.
- **Industrial Control Systems (ICS) Firewall**: This firewall protects factory networks from external attacks.

- **USB Blocker**: This feature prevents unauthorized copying of sensitive data to external storage devices.
- **Vulnerability Assessment (VA) & Penetration Testing**: These tools check for vulnerabilities and simulate cyberattacks on Mitr Phol's internal systems to evaluate and improve the security of the company's infrastructure, focusing on external attack scenarios and security readiness.

These technologies are designed to protect Mitr Phol Group's systems and data while ensuring operational efficiency.