Digital Security Solutions

True Digital Cybersecurity บริการศูนย์กลางการตรวจสอบความปลอดภัย และเฝ้าระวังภัยคุกคามทางด้านไซเบอร์ พร้อมทั้งแจ้งเตือน (SOC-as-a-Service) ด้วยการพัฒนาเทคโนโลยีความปลอดภัยที่สอดคล้อง เพื่อสามารถตรวจจับภัยคุกคามอย่างต่อเนื่อง พร้อมการบริหารจัดการความปลอดภัยแบบมืออาชีพ

Innovated BY truedigital

มั่นใจองค์กรปลอดภัย**ในโลกไซเบอร์**

อัปเดต
เทคโนโลยี
อยู่เสมอ

บริการ
ครบวงจร

มีกระบวนการ
ได้มาตรฐาน
ตรวจสอบได้

มีผู้เชี่ยวชาญ
ดูแลตลอด
24 ชม.

บริหารจัดการ
แบบบูรณาการจากส่วนกลาง

ประเมินความเสี่ยง
พร้อมร่วมออกแบบระบบ

รับมือกับภัยคุกคาม
แบบอัตโนมัติทันที

เฝ้าระวัง

One Stop Service
ให้คำปรึกษาและออกแบบ
ระบบความปลอดภัย
ครบวงจร

ป้องกัน

ให้คำปรึกษาด้านกฎหมาย
พ.ร.บ. PDPA

แจ้งเตือน

หาสาเหตุ

แบ่งปันความรู้
เพื่อการเฝ้าระวังสูงสุด

True Digital Cybersecurity

การันตีด้วยมาตรฐานความเป็นผู้นำในการให้บริการแบบ
Secure Digital Transformation and Operation ในประเทศไทย และภูมิภาค ASEAN

CEH Certified Ethical Hacker · CGEIT · CISM · CompTIA PenTest+ · CRISC · GPEN · GCIH · GWER · OFFENSIVE SECURITY OSCP · Microsoft CERTIFIED Professional

CHFI Computer Hacking Forensic INVESTIGATOR · CISSP · COBIT 5 · ECSA · ITIL · IRCA · Microsoft CERTIFIED Systems Administrator

สอบถามบริการ โทร. 1239

Governance, Risk and Consulting Services

บริการให้คำปรึกษาในการพัฒนาระบบบริหารความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC 27001 และการออกแบบนโยบายเพื่อนำไปประยุกต์ใช้ NIST Cybersecurity Framework ขององค์กร และจัดเตรียมแผนการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Risk Treatment Plan) ที่สอดคล้องตามนโยบายและวัตถุประสงค์การบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ อีกทั้งจัดเตรียมเอกสารสรุปมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศ (Statement Of Applicability : SOA) ที่เลือกใช้ในระบบ ISMS ตามขอบเขตที่กำหนด และเอกสารขั้นตอนปฏิบัติหรือเอกสารอื่นใดที่ต้องดำเนินการให้เป็นไปตามมาตรฐาน รวมถึงคำปรึกษาในการจัดเตรียมเอกสารวิธีการวัดประสิทธิผลของระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศ (Effectiveness Measurement) พร้อมการติดตามและรายงานผลการวัดประสิทธิผลตามเกณฑ์ที่กำหนดไว้

Offensive Cybersecurity

บริการประเมินความเสี่ยงของระบบด้วยการทดสอบ
เจาะระบบและค้นหาช่องโหว่ของแอปพลิเคชันเพื่อ
ป้องกันการโจมตีที่อาจจะเกิดขึ้นในอนาคต
โดยผู้เชี่ยวชาญที่มีประสบการณ์ พร้อมทั้งออกรายงาน
ประเมินความเสี่ยง และแจ้งไปยังผู้ดูแลระบบที่เกี่ยวข้อง

Penetration Testing Service (Pen-Test)

บริการประเมินความเสี่ยงด้วยการทดสอบเจาะระบบและค้นหาช่องโหว่ ในการเข้าถึงระบบต่างๆ
เป็นการจำลองเหตุการณ์ว่ามีการโจมตีไปในระบบเพื่อค้นหาจุดอ่อนในการเข้าถึงระบบ
โดยใช้หลักการและวิธีการจากมาตรฐานการทดสอบพัฒนาโดยทีมผู้เชี่ยวชาญ
และมีการประยุกต์ใช้เทคนิคในการเจาะระบบอื่นๆ เพื่อให้เหมาะสมกับสภาพแวดล้อม
ของระบบต่างๆ โดยใช้เทคนิคดังต่อไปนี้

แบ่งรูปแบบได้เป็น 4 ระบบ

1. ระบบ Infrastructure ตรวจหาช่องโหว่ที่ระบบเครือข่าย และระบบปฏิบัติการภายในองค์กร
2. ระบบเครือข่ายทางด้าน Network and WiFi เพื่อตรวจหาช่องโหว่ของระบบเครือข่าย
3. ระบบ Web Application ตรวจหาช่องโหว่ที่เว็บแอปพลิเคชันที่ถูกพัฒนาขึ้นมาทั้งก่อนและหลังใช้งาน
4. ระบบ Mobile Application ตรวจหาช่องโหว่ที่แอพพลิเคชันบนโทรศัพท์มือถือทั้งระบบ iOS และ Android

- **ได้ทราบผลกระทบของช่องโหว่ในระบบเครือข่ายภายในองค์กรเพื่อแก้ไขปรับปรุงได้ทันที**
- **ประเมินความเสี่ยงเพื่อเตรียมการป้องกันในการเกิดภัยคุกคามของระบบ**
- **ผู้ใช้งานภายในองค์กรได้ตระหนักถึงภัยคุกคามที่อาจเกิดขึ้นได้**
- **เข้าใจแนวทางการป้องกันความมั่นคงปลอดภัยทางสารสนเทศ**
- **สามารถบริหารจัดการความปลอดภัยได้อย่างมีประสิทธิภาพ**

Black Box Testing
การทดสอบเจาะระบบผ่านมุมมองของบุคคลทั่วไป หรือ Hacker ภายนอก โดยผู้ที่ต้องการทดสอบไม่ต้องจัดเตรียมข้อมูลระบบใดๆ

Gray Box Testing
การทดสอบเจาะระบบโดยผู้ที่ต้องการทดสอบให้ข้อมูลระบบบางส่วน

White Box Testing
การทดสอบเจาะระบบโดยผู้ที่ต้องการทดสอบให้ข้อมูลครบถ้วนเสมือนกับผู้ทดสอบเป็นพนักงานภายในองค์กร

Managed Detection and Response Services

บริการศูนย์ปฏิบัติเฝ้าระวัง และการรักษาความปลอดภัยเพื่อตรวจสอบ ตรวจจับ ป้องกัน และตอบสนองต่อเหตุการณ์ ภัยคุกคามทางไซเบอร์ที่อาจจะเกิดขึ้น (SOC)

Security Operation Center (SOC) Service

บริการศูนย์กลางการตรวจสอบความปลอดภัยและเฝ้าระวังภัยคุกคามทางด้านไซเบอร์ภายในเครือข่ายขององค์กร ดูแลและตรวจสอบการเข้าถึงระบบ ที่จะมาเฝ้าระวัง อุดช่องโหว่ และตรวจสอบภัยคุกคามแอบแฝง เพื่อการป้องกันการโจมตีแบบเรียลไทม์ พร้อมเก็บข้อมูลเพื่อตรวจหาช่องทางที่อาชญากรบุกรุกเข้ามาได้อย่างแม่นยำ ตอบโจทย์ธุรกิจด้วยเทคโนโลยีที่ทันสมัยมีความพร้อมใช้งานสูง รองรับบริการต่างๆ ที่เพิ่มขึ้นในอนาคต มั่นใจกับทีมผู้เชี่ยวชาญพร้อมเหล่าพันธมิตรจากทุกภาคส่วน ไม่พลาดทุกข้อมูลความเสี่ยง เพราะมีการมอนิเตอร์พร้อมอัปเดตภัยคุกคามใหม่ๆ และ ประเมินความเสี่ยงอยู่เสมอ

- บริการดูแลระบบ ตรวจจับ แจ้งเตือน และทำรายงานสรุปภัยคุกคาม
- บริการให้คำปรึกษา พร้อมแนวทางการป้องกัน วิเคราะห์พฤติกรรมของผู้ใช้งานเชิงลึก และวิเคราะห์ภัยคุกคามแบบล่วงหน้า
- บริการจัดเก็บ Log ตามพระราชบัญญัติ (พ.ร.บ.) ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560
- ครบด้วยระบบความปลอดภัยสูงสุด ผ่านการรับรองมาตรฐานสากล
- ผู้เชี่ยวชาญบริการระบบรักษาความปลอดภัยทางไซเบอร์แบบครบวงจร ที่มากด้วยประสบการณ์มากกว่า 10 ปี
- บริการตรวจสอบและเฝ้าระวัง ตลอด 24 ชม.

การเก็บข้อมูล log จาก source device หรือ platform ต่างๆ ในองค์กรของลูกค้า ที่มีข้อมูลบ่งชี้การตรวจจับและเฝ้าระวัง

ระบบ SOC platform พร้อมกับทีมงานผู้เชี่ยวชาญ คอยดูแล ตรวจสอบ เฝ้าระวังภัยคุกคาม และแจ้งเตือนพร้อมให้คำแนะนำ

เมื่อตรวจพบเจอภัยคุกคาม จะแจ้งเตือนพร้อมหลักฐานและคำแนะนำ เพื่อช่วยให้ลูกค้าสามารถรับมือกับเหตุการณ์นั้นได้อย่างเหมาะสม และเข้าไปดูแลทันที นำไปสู่การแก้ไขปัญหาภัยคุกคามที่เกิดขึ้น

Managed Security Services

บริการด้านบริหารจัดการและดูแลปรับปรุงระบบความปลอดภัยแบบครบวงจรจากภัยคุกคามทางไซเบอร์แบบศูนย์กลางที่มีการบริหารจัดการและการตอบสนองต่อการปรับปรุงแก้ไข เปลี่ยนแปลงนโยบายให้มีความปลอดภัยเพิ่มมากยิ่งขึ้น ตั้งแต่การเปลี่ยนแปลงการตั้งค่า (Managed Policy) การตรวจสอบและอัปเดต (Update and Upgrade) รวมถึงการปรับปรุงให้การป้องกันการโจมตีใหม่ (Enhance Policy) เข้ากับสภาพแวดล้อมขององค์กรมากยิ่งขึ้น ด้วยบุคลากรของทาง True Digital Cybersecurity ที่มีความเชี่ยวชาญเฉพาะด้านในระบบความปลอดภัยนั้นๆ อีกทั้งยังสามารถให้คำช่วยเหลือและคำปรึกษาด้านการเชื่อมต่อแบบบูรณาการ (Solution Integration) ครบวงจรตลอด 24 ชม.

บริการมาตรการการรักษาความปลอดภัยอย่างมีประสิทธิภาพ (Security Operation Efficiency) ประกอบไปด้วย

1. **บริการป้องกันการโจมตี เวปแอปพลิเคชัน (Managed Service Web Application Firewall : WAF)**
2. **บริการตรวจจับและตอบสนองต่อภัยคุกคามอย่างรวดเร็ว (Managed Service Endpoint Detection and Response : EDR)**
3. **บริหารจัดการสิทธิ์การเข้าถึงระบบในองค์กร (Managed Service Privileged Access Management : PAM)**
4. **บริการค้นหาความผิดพลาด และนำ Source Code มาสแกนเพื่อหาช่องโหว่และประเด็นที่สามารถปรับปรุงได้ (Managed Service Static Source Code Scan : SAST)**
5. **บริการตรวจสอบอย่างเป็นระบบในการหาช่องโหว่และแนะนำอุดช่องโหว่แบบตรงจุด (Managed Service Vulnerability Management : VM)**
6. **บริการศูนย์กลางการเชื่อมต่อระบบคลาวด์และอินเทอร์เน็ตเพื่อการเข้าถึงระบบภายในองค์กร (Managed Service Secure Access Service Edge : SASE)**

PDPA and Data Protection Services

บริการให้คำปรึกษากฎหมาย พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล 2562 (Personal Data Protection Act: PDPA) หรือนโยบายข้อมูลความเป็นส่วนตัว Data Privacy Policy ตั้งแต่การเตรียมความพร้อมเพื่อปฏิบัติตามเงื่อนไขใน พ.ร.บ. รวมทั้งการออกแบบและพัฒนานโยบายการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าและพันธมิตรทางการค้าเพื่อให้สอดคล้องกับรูปแบบการดำเนินธุรกิจ โดยเฉพาะอย่างยิ่ง องค์กรต่างๆ ดังนี้

- **องค์กรที่มีการเก็บข้อมูลส่วนบุคคลและนำข้อมูลเหล่านั้นมาใช้งาน**
- **องค์กรที่เป็นตัวกลางคอยเก็บข้อมูลและประมวลผลข้อมูลของลูกค้า**
- **องค์กรที่เสนอขายสินค้าต่างๆ และเก็บข้อมูลลูกค้าภายในประเทศไทย**

- **ป้องกันการนำข้อมูลส่วนบุคคลไปใช้งานโดยมิชอบหรือไม่ได้รับความยินยอมจากเจ้าของข้อมูล**
- **มีแผนการทำงาน และกระบวนการที่ชัดเจนในการคุ้มครองข้อมูลส่วนบุคคลสอดคล้องกับ PDPA**
- **ครบวงจรด้วยทีมที่ปรึกษาเกี่ยวกับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล 2562 (PDPA)**
- **ลดโอกาสได้รับโทษทางกฎหมายในกรณีเกิดปัญหาการละเมิดข้อมูลส่วนบุคคลโดยสามารถอ้างอิงได้จากกระบวนการบริหารจัดการ PDPA ที่ได้ทำเรียบร้อยแล้ว**

กฎหมาย PDPA (Personal Data Protection Act) เป็น พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล 2562

ถูกกำหนดขึ้นเพื่อใช้ในการคุ้มครองข้อมูลส่วนบุคคล ไม่ให้ถูกจัดเก็บหรือนำไปใช้โดยไม่ได้แจ้งให้เราทราบ และ/หรือได้รับความยินยอมจากเราในฐานะเจ้าของข้อมูลก่อน