CAT cyfence

ตรวจสอบทุกช่องโหว่

ประเมินทุกความเสี่ยง ปลอดภัยทุกการใช้งาน

IT Risk Assessment Service

บริการประเมินความเสี่ยงของระบบ

บริการประเมินความเสี่ยงของระบบ สามารถช่วยป้องกันภัยที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ โดยทำการวิเคราะห์ช่องโหว่ ตรวจสอบและทดสอบความปลอดภัยของระบบ รวมถึงการให้คำปรึกษาในการ **ปิดช่องโหว่ที่เกิดขึ้นในระบบเทคโนโลยีสารสนเทศ** เพื่อป้องกันไม่ให้ผู้ไม่ประสงค์ดีเข้ามาขโมย แก้ไข หรือทำลายข้อมูลอันมีค่าขององค์กร และลดโอกาสการเกิดความเสียหายแก่ระบบเทคโนโลยีสารสนเทศภายในองค์กร ซึ่งแบ่งเป็น

Vulnerability Assessment (บริการตรวจสอบช่องโหว่ของระบบ)

เป็นบริการตรวจสอบช่องโหว่ของระบบ เช่น ช่องโหว่ในกระบวนการทำงาน ระบบเซิร์ฟเวอร์ ระบบเน็ตเวิร์ค และอุปกรณ์รักษาความปลอดภัย เป็นต้น ซึ่งหากเป็นช่องโหว่ที่ไม่ได้รับการดูแลอาจทำให้ระบบเทคโนโลยีสารสนเทศถูกบุกรุกจนถึงขั้นวิกฤตได้

Penetration Test (บริการทดสอบการบุกรุกระบบ)

ทดสอบระดับความปลอดภัยของระบบเทคโนโลยีสารสนเทศ โดยจำลองสถานการณ์การบุกรุก เพื่อทดสอบการเข้าสู่ระบบในลักษณะเดียวกับที่ผู้ไม่ประสงค์ดีใช้ในสถานการณ์จริง

CAT cyfence

IT Risk Assessment Service

Organization's network can be prone to many security threats if it is not properly protected. With IT Risk Assessment Service, CAT cyfence can help company identify weaknesses in its current network infrastructure. After that, recommendations will be given to minimize any weak spot that might exist, therefore, reducing the chance of network being attacked. CAT cyfence's IT Risk Assessment Service consists of two main services which are Vulnerability Assessment and Penetration Test.

Vulnerability Assessment

The team of security analysts and engineers will analyze existing organization's security plans, programs and processes to evaluate adequacy and identify areas that may need security improvement. CAT cyfence will also conduct network vulnerability assessment and provide summary report and recommendations regarding the current system configuration and security policy.

Penetration Test

CAT cyfence's penetration test is an advance stage of assessing the customer's IT security system. More than a simple scan, a penetration test is a multi-step process using zero knowledge, partial knowledge, and full knowledge techniques to break into the customer's system the same way a hacker would do. These steps include mapping network elements for business functions, exploiting vulnerabilities to assess effectiveness, and social engineering to test security procedures.