CAT cyfence

จัดการและเฝ้าระวัง
ระบบเทคโนโลยีสารสนเทศตลอด 24 ชั่วโมง
เพื่อธุรกิจดำเนินไปอย่างราบรื่น

24/7

Managed Security Service

บริการดูแลและบริหารจัดการระบบรักษาความปลอดภัยเทคโนโลยีสารสนเทศ

บริการจัดการระบบเทคโนโลยีสารสนเทศผ่านศูนย์ปฏิบัติการ Security Operation Center (SOC) ในลักษณะ**ดูแลและเฝ้าระวังการบุกรุกระบบแบบ Real-time ตลอด 24 ชั่วโมง** โดยมีนักวิเคราะห์ระบบและผู้เชี่ยวชาญด้านการรักษาความปลอดภัยปฏิบัติงานผลัดเปลี่ยนกันเพื่อดูแล ทำการแจ้งเตือนเมื่อเกิดปัญหาภัยคุกคามหรือค้นพบช่องโหว่ใหม่ๆ อย่างทันท่วงที พร้อมช่วยแก้ไขปัญหาและวิเคราะห์สถานะความปลอดภัยของระบบเทคโนโลยีสารสนเทศขององค์กร ซึ่งแบ่งออกเป็น 3 ระดับ ได้แก่

Level 1 - Security Monitoring Service

ทำการเฝ้าระวังและตอบสนองต่อปัญหาที่เกิดขึ้นที่อุปกรณ์หรือระบบเครือข่ายขององค์กรแบบ Real-time ตลอด 24 ชั่วโมง พร้อมทำการแจ้งเตือนหากเกิดเหตุการณ์ผิดปกติอย่างทันท่วงที

Level 2 - Incident Management Service

บริหารและตอบสนองต่อเหตุการณ์บุกรุก พร้อมให้ความช่วยเหลือและทำการแก้ไขปัญหา โดยทีม CAT CSIRT (Computer Security Incident Response Team) จะทำการรวบรวมข้อมูลเพื่อหาสาเหตุและแก้ไขปัญหาที่เกิดขึ้น อีกทั้งให้คำแนะนำเพื่อป้องกันการเกิดปัญหาขึ้นอีกในอนาคต

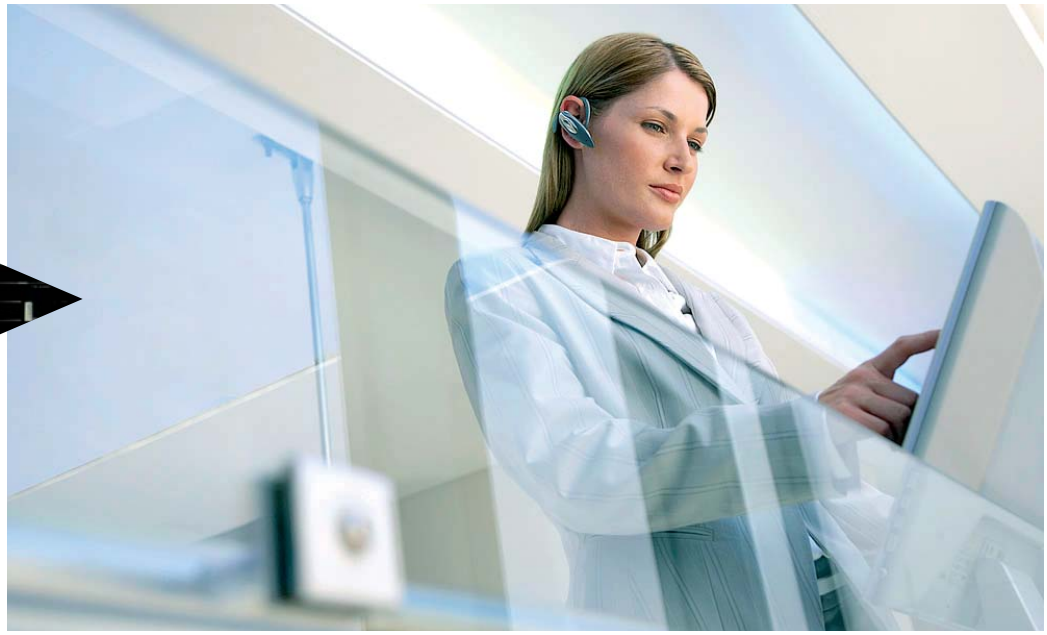
Level 3 - Configuration Management Service

บริหารจัดการระบบรักษาความปลอดภัยแบบครบวงจร โดยให้คำแนะนำในการบริหารจัดการค่าคอนฟิกของระบบและอุปกรณ์ในเครือข่าย รวมไปถึงการกำหนด แก้ไขหรือเพิ่มเติมนโยบาย (Policy) สำหรับอุปกรณ์รักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ

บริการ Managed Security Service จาก CAT cyfence ช่วยให้องค์กร

- ได้รับการเฝ้าระวังภัยคุกคามต่อระบบเทคโนโลยีสารสนเทศ แบบ Real-time ตลอด 24 ชั่วโมง
- ได้รับการแจ้งเตือนในทันทีเมื่อมีภัยคุกคามรูปแบบใหม่ๆ เกิดขึ้น (Early warning) พร้อมคำแนะนำในการแก้ไขปัญหา
- ได้รับการช่วยเหลือในการแก้ปัญหาและตอบสนองต่อเหตุการณ์บุกรุก
- ได้รับการดูแลและบริหาร Configuration พร้อมทำการปิดช่องโหว่ต่างๆ
- สามารถปฏิบัติตามกฎหมายหรือมาตรฐานการรักษาความปลอดภัยตามมาตรฐานสากลได้
- สามารถลดค่าใช้จ่ายในการลงทุนจัดหาอุปกรณ์และพัฒนาบุคลากรเพื่อดูแลระบบ

CAT cyfence



24/7

Managed Security Service

With CAT cyfence's Managed Security Service (MSS), customer's network and security devices will be monitored and managed through the Security Operation Center (SOC), where security analysts and experts are working 24 hours a day, 7 days a week throughout the year to ensure a timely response to unexpected events and to protect customer's digital assets. The security monitoring is done in real-time and, upon a risk event, an immediate notification will be delivered directly to the IT manager. In case of serious situation or severe attack, a team of IT security expert called CSIRT (Computer Security Incident Response Team) will be dispatched to help control the situation and contain the risk from spreading. The team will use IT forensic techniques to collect evidence that may lead to the cause of the problem and prepare recommendations to prevent future breakouts. Different service levels are available to suit different needs from customers.

Level 1: Security Monitoring Service

The real time monitoring can be achieved by collecting log information generated from various network devices, such as Firewall, Router, IDS/IPS and Server. Data will be securely sent to CAT's SOC then normalized and correlated for monitoring, as well as, securely stored in storage server for future reference. In case of any suspicious activity, immediate notification will be sent directly to System Administrator.

Level 2: Incident Management Service

In case of an incident or severe attack to customer's network, a team of IT security experts called CSIRT or Computer Security Incident Response Team will be dispatched to normalize the situation, as well as, collecting any information that might lead to the cause of the problem and provide recommendation to prevent similar breakout in the future.

Level 3: Configuration Management Service

With permission from customer, CAT cyfence's security experts may adjust security policy or system configuration, for example, Firewall policy or Router's ACL, to handle or manage incidents. This is done to maintain consistency, increase system performance, and strengthen security policy in order for the business to run without any interruptions.