TDAR Platform

www.tdarplatform.com

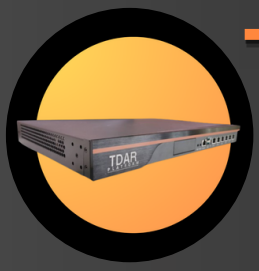
Threat Detection Automation & Response Platform

The Modern Cyber Security Operations Center

Capability:

- Platform & Architecture
- Managed Detection & Response Service

THREAT DETECTION AUTOMATION AND RESPONSE PLATFORM



TDAR Platform
Next-Generation **SIEM**

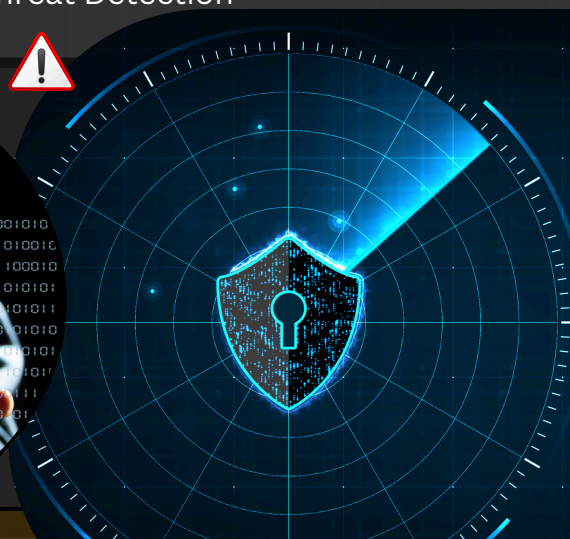
- Log Collection
- Threat Detection
- Automation Response

Collection (Logging)

- TDAR Platform มีความสามารถในการรับข้อมูล Log จากหลายแหล่งที่มา (Log source) โดยมีการเชื่อมต่อกับ Log Source ผ่าน Connector และ Sensor เพื่อเก็บข้อมูล Log จากอุปกรณ์ต่างๆ เช่น อุปกรณ์ Security, Operating System, Network Service, Application หรือ IOT Device Sensor
- TDAR Platform มี Module ที่ทำหน้าที่เก็บรวบรวมและจัดการ Log ที่เรียกว่า Log Management หรือ Security Data Lake ซึ่งเป็นถังเก็บ Log ขนาดใหญ่ โดยใช้เทคโนโลยี Big Data ในการจัดเก็บข้อมูล การเชื่อมต่อกับ Log Source ต่างๆสามารถทำได้ทั้งในรูปแบบ Agent-less และ Agent-based รวมถึงการใช้ Network Sensor เพื่อรวบรวมข้อมูล Log ของ Network Service

Detection & Prevention

- TDAR Platform ทำงานด้าน Detection & Prevention โดยอาศัยการวิเคราะห์ข้อมูลจาก Log Source ที่รวบรวมเข้ามา (Collection) ผนวกกับฐานข้อมูล Threat Intelligence ในการตรวจจับภัยคุกคาม (Detection) และ DNS Firewall ในการป้องกันการเข้าถึงเว็บไซต์หรือบริการที่เป็นอันตราย (Prevention) * โดยอาศัยการทำงานแบบ Proxy ของ DNS Firewall ในการ Block ไม่ให้มีการเข้าถึง Domain ที่อยู่ใน Block List (ต้องมีการ Setup เพิ่มเติมในระบบ Network)
- TDAR Platform มีฐานข้อมูล Threat Intelligence ที่ครอบคลุมทั้ง Commercial feed Threat Intelligence และ Open-Source สามารถอัปเดตฐานข้อมูล Threat Intelligence และ Block list ได้ตามต้องการ หากพบว่า IP, Domain, URL, File Hash ที่เป็นส่วนหนึ่งของภัยคุกคามที่ตรวจพบโดย Threat Detection หรือ Security Tools อื่นๆ ที่องค์กรใช้งานอยู่



THREAT DETECTION AUTOMATION AND RESPONSE PLATFORM

Managed & Respond

TDAR Platform เป็นแพลตฟอร์มที่มีโมดูล (Module)
ในการทำเรื่อง Active Response and Orchestration
“Security Orchestration Automation Response" (SOAR)
โดยมี Tools ที่ใช้จัดการเรียกว่า Case Management

Active Response and Orchestration

- สร้าง Workflow เพื่อตอบสนองต่อเหตุการณ์ที่เกิดขึ้นช่วยในการตรวจสอบ Source IP ที่เข้ามา เช่น การ Brute Force Attack เป็นต้น
- Integrate กับอุปกรณ์ Security หรือ Third Party Platform เพื่อใช้ Response และเปิดเคส เช่น Ticketing System
- มีกลไกในการทำการตอบสนองโดยอัตโนมัติ (Automated Response) ตาม Alert ที่ระบบ Detect และตรวจสอบกับ Alert Rule Verify ข้อมูลจาก Alert โดยใช้ Cloud Service เช่น Virus Total เพื่อยืนยันความเสี่ยง และทำการ Response ต่อไป
- Run Playbook เพื่อ Block Source IP หรือ Destination Domain Name ที่ Contact กับ Malicious สามารถเปิด Case เก็บหลักฐานต่างๆ และข้อมูลที่เกี่ยวข้อง ใน Case Management Module สำหรับใช้เป็น Knowledge Base เพื่อเรียนรู้ภายในองค์กร

TDAR Platform DNS Firewall

อีกหนึ่งโมดูลที่เสริมการทำงานของ
กระบวนการป้องกันการโจมตีแบบฟิชชิง
ทำหน้าที่ในการกรองข้อมูลและปิดกั้น
ต้นเหตุของการแพร่กระจายมัลแวร์
และแรนซัมแวร์...