TDAR Platform

Threat Detection Automation & Response Platform.

The Modern Cyber Security Operation Center (CSOC) Capability, Platform & Architecture. Managed Detection & Response Service (MDR)

Available in: Appliance, Virtual Machine, Hosted, Cloud

TDAR Platform เป็นได้มากกว่าการเก็บ Log

TDAR Platform เป็นสถาปัตยกรรมระบบเฝ้าระวังฯ ด้วยเทคโนโลยีที่ล้ำสมัย เช่น Security Information Event Management (SIEM), Machine Learning (ซึ่งทำงานในแบบ Fully Redundancy / Active-Active High Availability) , Security Orchestration Automation & Response (SOAR) และ DNS Firewall เป็นต้น ซึ่งตอบรับความต้องการครบทุกด้านเกี่ยวกับการเฝ้าระวังและตอบสนองต่อภัยคุกคามทางไซเบอร์ได้อย่างรวดเร็วและแม่นยำ ที่ได้การรับรองมาตรฐานด้านความมั่นคงปลอดภัย ISO/IEC 27001, CSA STAR Cloud Security ได้รับการทดสอบและผ่านการรับรองมาตรฐานสินค้าภายใต้เครื่องหมายผลิตภัณฑ์ FCC, CE, RoHS

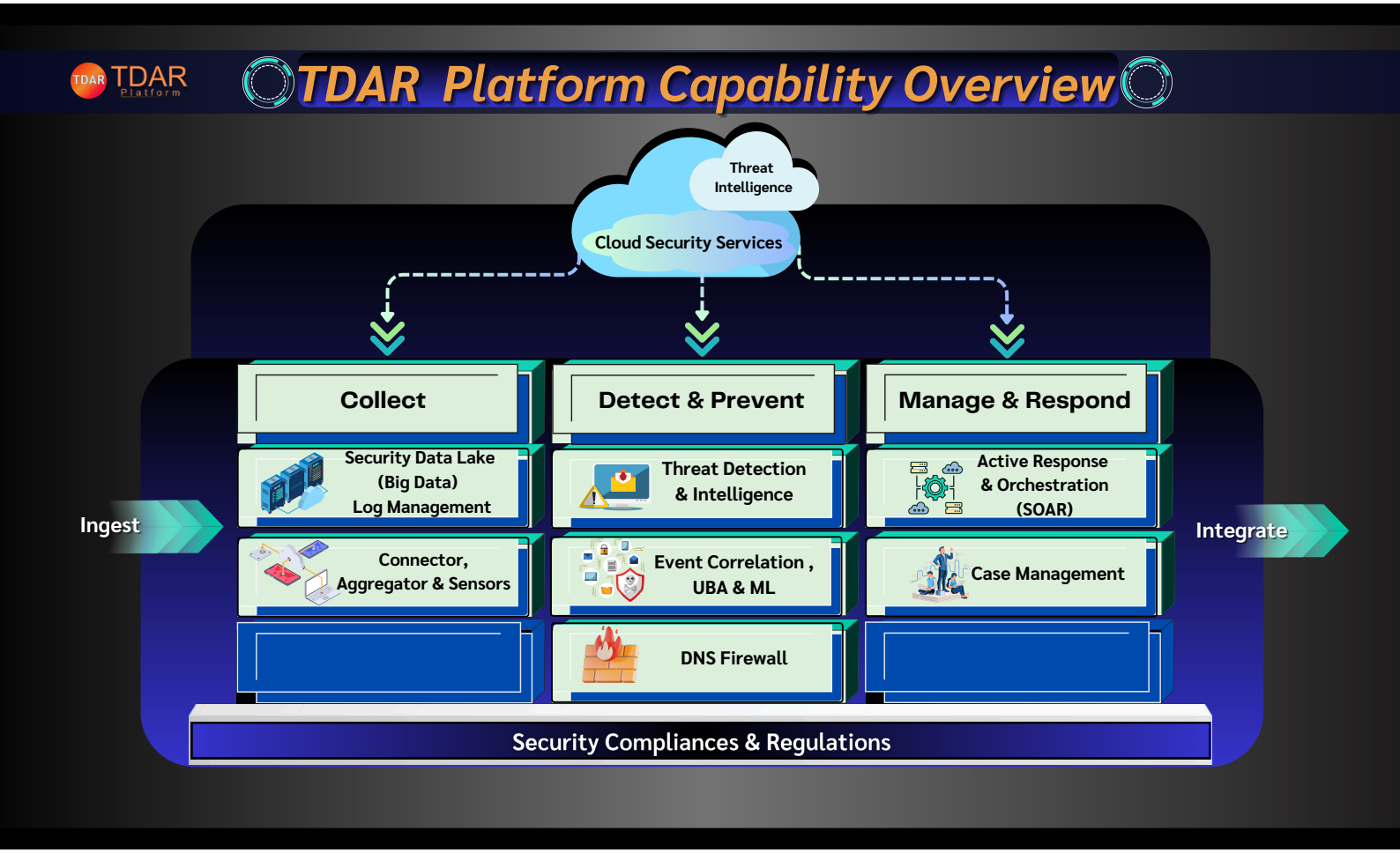
TDAR Platform เป็น ระบบบริหารจัดการข้อมูล Log File แบบศูนย์กลาง (Centralized Log)

ซึ่งรองรับการจัดเก็บข้อมูล Log File จากเครื่องคอมพิวเตอร์เซิร์ฟเวอร์หรืออุปกรณ์เครือข่ายต่าง ๆ สามารถจัดเก็บ Log โดยสามารถจัดเก็บผ่านทาง Protocol syslog standard ซึ่งอุปกรณ์ทุกชนิดส่วนใหญ่จะส่ง Log ผ่านทางช่องทางนี้เป็นหลัก ไม่ว่าจะเป็น Router, Switch, Firewall, System, Application เป็นต้น

TDAR Platform ตอบโจทย์การเก็บข้อมูลจราจรคอมพิวเตอร์ได้ครอบคลุมทั้งองค์กรขนาดเล็กไปจนถึงองค์กรขนาดใหญ่

โดยสามารถจัดเก็บข้อมูลการจราจรทางคอมพิวเตอร์ได้ไม่ต่ำกว่า 90 วันเป็นอย่างน้อยและกำหนดได้สูงสุด 2 ปี มีความถูกต้องครบถ้วนของข้อมูล (Data Integrity) ตรงหลักเกณฑ์การจัดเก็บข้อมูล ตาม พ.ร.บ. คอมพิวเตอร์ ปัจจุบัน TDAR Platform สามารถรองรับ EPS ได้ตั้งแต่ 2,000-200,000 EPS โดยขึ้นอยู่กับรุ่นและ Hardware ที่ใช้ติดตั้ง

TDAR Platform Capability Overview



Gartner ได้กำหนดคุณสมบัติของ Next-Generation SIEM ไว้ว่า...

ต้องมีความสามารถในการ Collect, Detect และ Response ดังนั้น TDAR Platform จึงถูกออกแบบให้มีความสามารถ (Capability) ที่ตอบโจทย์ Requirement ทั้ง 3 ด้าน คือเรื่องของ Logging, Detection และ Response

โดยความสามารถดังกล่าวทั้งหมด... ได้ถูกรวบรวมเป็นความสามารถหลักของ TDAR Platform

นอกเหนือจากเรื่อง ของ Collect, Detect และ Response แล้ว TDAR Platform ยังมีความสามารถที่เสริม Requirement ในด้าน IT Security นั้นก็คือเรื่องของการ Prevention ได้แก่ **TDAR Platform DNS Firewall** ที่เป็นโมดูล (Module) เสริมในตัว TDAR Platform อีกด้วย

Collection

TDAR Platform

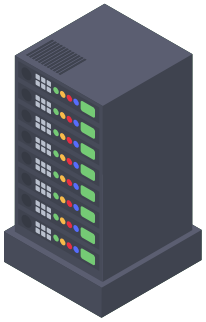
สามารถจัดเก็บ Log ได้จากหลากหลายแหล่งที่มา (Log Source) เช่น Windows, Syslog, Flow, SNMP และอื่นๆ เช่น Network Service, Azure และ รองรับ Channel อื่นๆดังนี้

Log Source Channels Support

Channel: Syslog

- **Security Devices:** Firewall, IDS/IPS, Antivirus Server, Email Security Gateway
- **Operating Systems:** Unix, Linux
- **Virtualization:** VMWare, Hyper-V

- **Applications:** Apache, IBM WebSphere, WebLogic, SSH, FTP, SFTP, SMTP, POP3, IMAP, Web Proxy
- **Network Devices:** Core Switch, Router
- **Identity Management:** TACAC+, RADIUS, LDAP
- **Databases:** Oracle DB, MySQL



Channel: Windows

- **Operating Systems:** Windows Server Events, Windows Workstation Events, WMI Data
- **Applications:** Microsoft IIS, Exchange, Apache, FTP, Custom Application Log
- **Identity Management:** Active Directory, LDAP

Collection

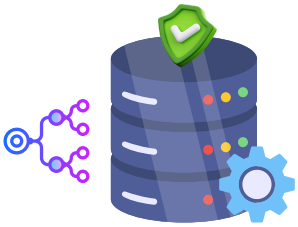
Log Source Channels Support

Channel: Windows

- **Databases:** Microsoft SQL
- **Vulnerability Assessment:** Nessus

Channel: Application

- **Applications:** Apache, IBM WebSphere, WebLogic, FTP, SMTP, POP3, IMAP, Web Proxy
- **Identity Management:** LDAP
- **Databases:** MySQL, Oracle

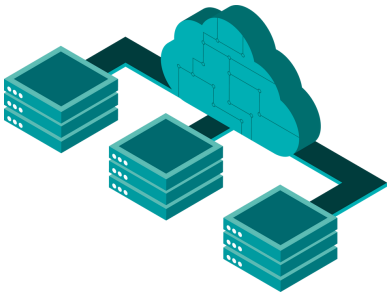


Channel: Flow

- **Network Devices:** Cisco Netflow, Juniper SFlow

Channel: SNMP

- **Network Devices:** SNMP



Channel: OPSEC

- **Security Devices:** Check Point

Channel: Network Services

- **Network Services:** DNS, DHCP, HTTP, HTTPS, SMTP, POP3, IMAP, FTP

Channel: Others

- **Cloud Services:** AWS, Azure, Google, Office 365
- **Message Brokers:** MQTT, Kafka, Redis, RabbitMQ

Collection

Logs ที่ถูกจัดเก็บจาก Log Source ต่างๆ ข้างต้น Logs เหล่านั้นสามารถนำมาใช้สร้าง Use Cases ด้าน Security Compliance ได้หลากหลาย เช่น การสร้าง Security Dashboards และ Reports สำหรับการทบทวนเหตุการณ์ด้านความมั่นคงปลอดภัยต่างตามกฎหมาย และข้อกำหนดของมาตรฐานด้านความมั่นคงปลอดภัยต่างๆ เช่น

- พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550
- พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560
- ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมเรื่องหลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2564
- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
- พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
- ISO/IEC 27001
- ISO/IEC 27002
- CSA STAR
- PCI DSS
- SOX
- FISMA
- HIPPA และอื่นๆ

- ระบบรองรับการนำเข้าข้อมูลที่ Capture มาจาก Raw Network Packet จาก Network Monitoring Tool ภายนอกได้
- รองรับการนำเข้าข้อมูลผลการตรวจสอบช่องโหว่ด้านความมั่นคงปลอดภัยสารสนเทศ (Vulnerability Assessment)
- สามารถกำหนดนโยบายป้องกันการส่ง Log มาจาก Log Source ที่ไม่ได้รับอนุญาตได้
- สามารถทำ Log Filter ตามเงื่อนไขต่างๆ เพื่อจัดกลุ่ม หรือแยก การเก็บ Log ตามหน่วยงานและแยกสิทธิ์การเข้าถึงได้
- สามารถจัดเก็บข้อมูลแบบไม่สามารถแก้ไขข้อมูล (Write Once, Read Many) และทำงานในแบบ Clustering ซึ่งต้องจัดเก็บข้อมูลไว้อย่างน้อย 2 ชุด เพื่อป้องกันข้อมูลเสียหาย

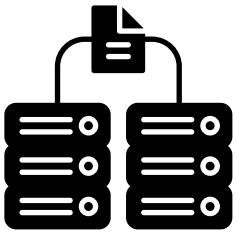
Access Control - Usage and Storage

- สามารถควบคุมหรืออนุญาตให้เข้าถึงข้อมูล Logs ที่จัดเก็บไว้บนระบบแยกตามประเภทหรือกลุ่มของ Log Source ได้ เช่น Syslog, Windows, Flow เป็นต้น
- สามารถกำหนดนโยบายควบคุมการเข้าถึงระบบในระดับเครือข่ายโดยอนุญาต หรือไม่อนุญาต ด้วย Protocol, IP Address และ Port ทั้งต้นทาง และปลายทางได้
- สามารถจำกัดการเข้าถึงที่เลเยอร์เครือข่ายด้วยกฎที่ตั้งไว้เพื่ออนุญาตหรือปฏิเสธการเข้าถึงตามโปรโตคอลเครือข่าย ที่อยู่ Source IP, Source Port, Destination IP และ Destination Port การป้องกันเลเยอร์เครือข่ายนี้สามารถใช้เพื่อป้องกันไม่ให้แหล่งบันทึกที่ไม่ได้รับอนุญาตส่งข้อมูลบันทึกไปยังแพลตฟอร์ม
- รองรับการกำหนดสิทธิ์ในการเข้าถึงข้อมูลได้หลายระดับ เช่น Admin, Analyst, Auditor, Executive ฯลฯ เป็นต้น
- สามารถให้สิทธิแก่บัญชีผู้ใช้ในการเข้าถึงแบบ Read-only เพื่อป้องกันการแก้ไขข้อมูล Log โดยไม่ตั้งใจหรือเจตนา
- สามารถจำกัดการเข้าถึงข้อมูล Log ต่อ Document, Field และ Index
- ทุก Field สามารถปิดบังข้อมูลเพื่อป้องกันข้อมูลที่ละเอียดอ่อนของในแต่ละเหตุการณ์

- สามารถกำหนดระยะเวลาจัดเก็บข้อมูลแยกตามประเภทหรือกลุ่มของ Log Source ได้
- ระบบสามารถจัดเก็บข้อมูลชนิด Raw Data โดยแยกจัดเก็บตามชื่ออุปกรณ์ วันที่และชั่วโมงได้
- สามารถควบคุมการเข้าถึงใช้งาน และบริหารจัดการระบบในแบบ Multi Tenancy โดยที่แต่ละ Tenant อนุญาตให้แต่ละบัญชีผู้ใช้สามารถเข้าถึงข้อมูล Log ผ่าน Dashboard, Chart หรือการ Search ด้วยสิทธิของตนเอง เช่น Analyst และ Executive

Access Control - Usage and Storage

- สามารถพิสูจน์ตัวตนเข้าใช้งานระบบด้วย Multi-Factor Authentication /รองรับการยืนยันตัวตนด้วยโปรโตคอล OpenID สำหรับองค์กรเพื่อบังคับใช้เทคโนโลยีการตรวจสอบสิทธิ์แบบ Multi-Factors เช่น Google Authenticator
- รองรับการพิสูจน์ตัวตนเพื่อเข้าใช้ระบบ (User Authentication) ด้วย Users บนระบบ Active Directory และ LDAP ขององค์กรที่มีอยู่ได้โดยองค์กรสามารถกำหนดและบังคับใช้นโยบายรหัสผ่านบนระบบ Active Directory และ LDAP ตามที่องค์กรต้องการได้
- มี Audit Log เพื่อใช้ตรวจสอบการเข้าใช้งานระบบโดยผู้ดูแลระบบ
- รองรับการทำงานในแบบ HA (High Availability)
- มีกลไกการเข้ารหัสข้อมูล Raw Log (AES algorithm)



- มีกลไกการทำ Data Integrity สำหรับข้อมูล Logs ในระดับแต่ละ Record เมื่อจัดเก็บบนระบบด้วย SHA-256 และ SHA-512 ป้องกัน การเปลี่ยนแปลงแก้ไข ลบ ข้อมูล เพื่อความสมบูรณ์ของ ข้อมูลที่ถูกจัดเก็บและสอดคล้องกับข้อกฎหมายพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
- สามารถทำ Archives Log และมีการ Compression File เพื่อประหยัดพื้นที่จัดเก็บข้อมูลโดยมีอัตราส่วนได้ 13:1 เท่า ขึ้นกับชนิดและรูปแบบของข้อมูล
- ข้อมูล Log ที่เกินระยะเวลาที่กำหนด สามารถย้ายไปยังที่จัดเก็บข้อมูลภายนอกผ่านโปรโตคอล SFTP และ NFS
- รองรับการตั้งเวลา Backup Archive Log Data แยกออกไปยังอุปกรณ์อื่นผ่าน NFS Protocol ได้
- ระบบสามารถทำการสำรองข้อมูล Logs ไปไว้ยังหน่วยสำรองข้อมูล Logs ภายนอก (External Archived Storage) โดยอัตโนมัติ

Management

- สามารถบริหารจัดการระบบ (Remote Management) ผ่าน Web UI หรือ Command Line Interface ในการบริหารจัดการระบบ
- สามารถบริหารจัดการ Log แบบรวมศูนย์ได้ตามข้อกำหนด (Centralize Log Management)
- สามารถบริหารจัดการได้อย่างมั่นคงปลอดภัยด้วยมาตรการรักษาความปลอดภัย เช่น การเข้ารหัสช่องทางเชื่อมต่อด้วย HTTPS หรือ TLS 1.2 และ SSH 2.0 เป็นอย่างน้อย

- สามารถบันทึกเงื่อนไขในการค้นหาเพื่อทำการค้นหาข้อมูลในภายหลังได้
- มีการค้นหาที่รวดเร็วด้วย Full Text Search
- มีเทคโนโลยีการ Index ข้อมูล Log File เพื่อประสิทธิภาพในการค้นหาโดยรองรับทั้งแบบ Full Text Search และแบบกำหนด Field ในการค้นหา โดยสามารถระบุเงื่อนไขในการค้นหาได้ เช่น AND, OR, Wildcard และกำหนดช่วงเวลาหรือขอบเขตในการค้นหาได้
- มีเทคโนโลยีการค้นหาข้อมูล (Search) ได้จากทุกเนื้อความในข้อมูล Log ที่ส่งเข้ามาได้ทั้งแบบ Keyword, Field, Boolean, Expression, Regular Expression ได้
- มีความสามารถตรวจสอบสถานะของอุปกรณ์ที่ส่ง Log เข้ามาว่ายังทำงานอยู่ได้
- รองรับการส่งต่อ Log ไปยังอุปกรณ์อื่นได้
- สามารถส่งต่อ Log โดยการสร้าง Filter ตามเงื่อนไขที่ต้องการ เช่น ชื่อ Host, ชนิดของเหตุการณ์ ระดับความสำคัญ หรือ Message Keyword โดยส่งต่อไปยัง Syslog Server หรืออุปกรณ์ประเภท SIEM ผ่าน Syslog Protocol ได้โดยไม่เปลี่ยนแปลงข้อมูลต้นทาง

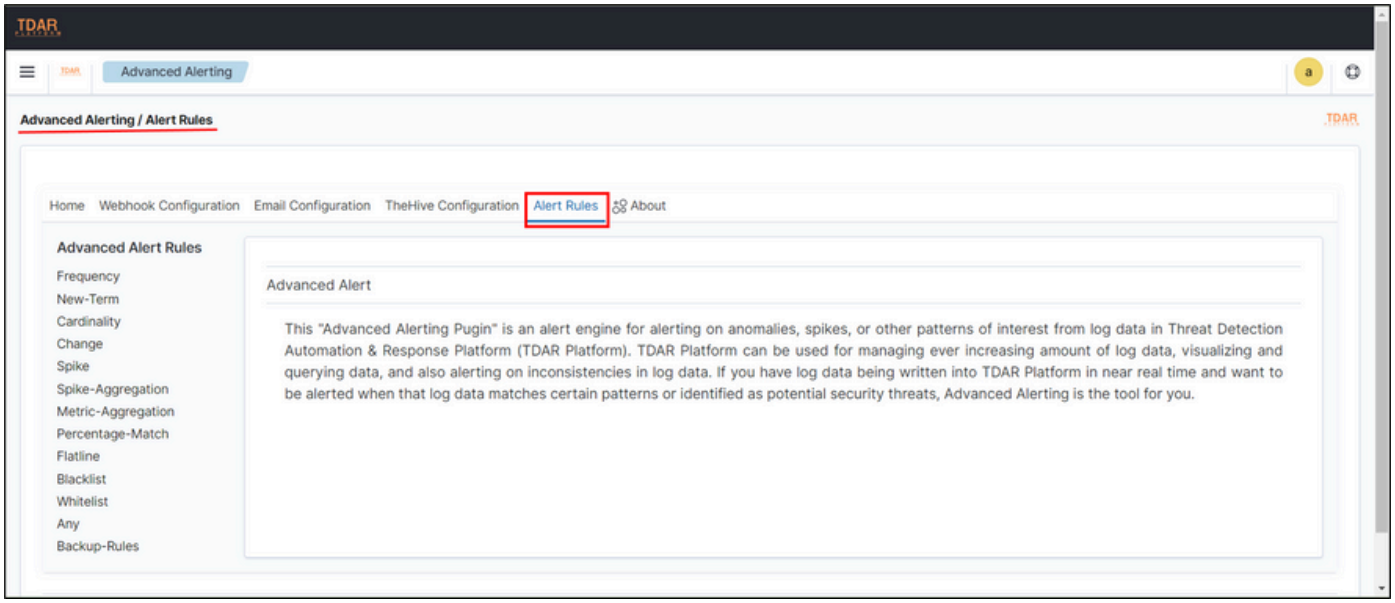
- รองรับการตั้งเวลา Time Server ผ่านโปรโตคอล NTP
- สามารถทำงานเป็น NTP Server ให้กับอุปกรณ์อื่นๆ ภายใน เครือข่ายได้* (NTP คือ network protocol ที่ใช้เทียบเวลา)

Alerts, Dashboard and Report

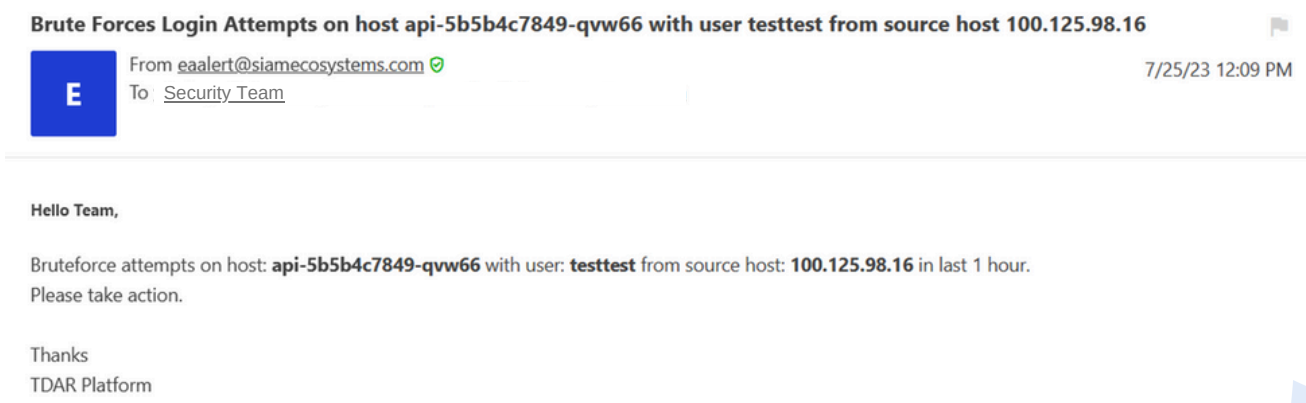
- สามารถแจ้งเตือนไปยังผู้ดูแลระบบเมื่อไม่มี log ส่งเข้ามายังระบบผ่านช่องทางต่างๆ เช่น

- Email
- Slack
- Custom Webhook
- Line Notify
- Jira
- Zabbix
- Microsoft Teams,
- TheHive,
- ServiceNow,
- PagerDuty,
- Google Chat

Creating an Alert



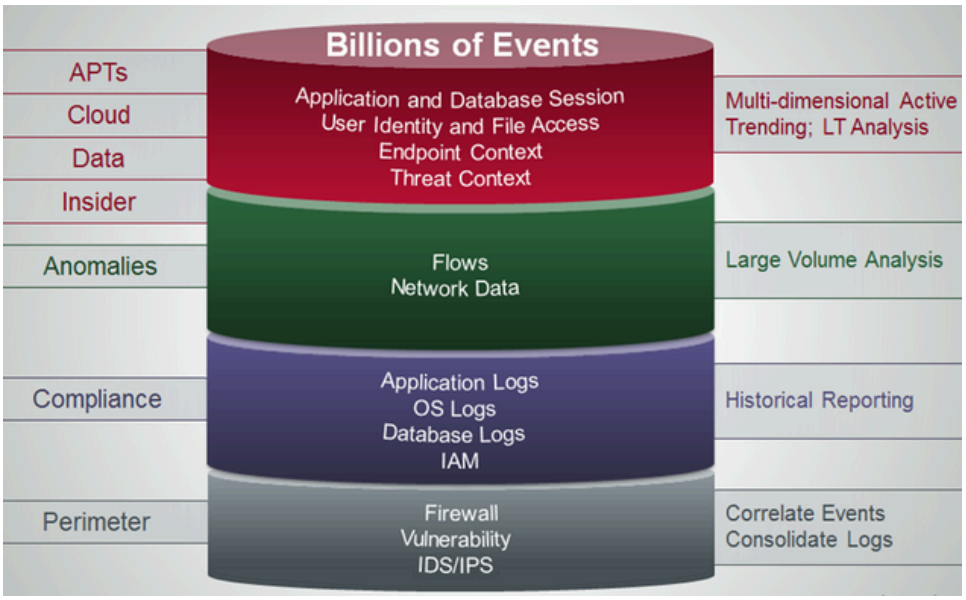
Alert Notification



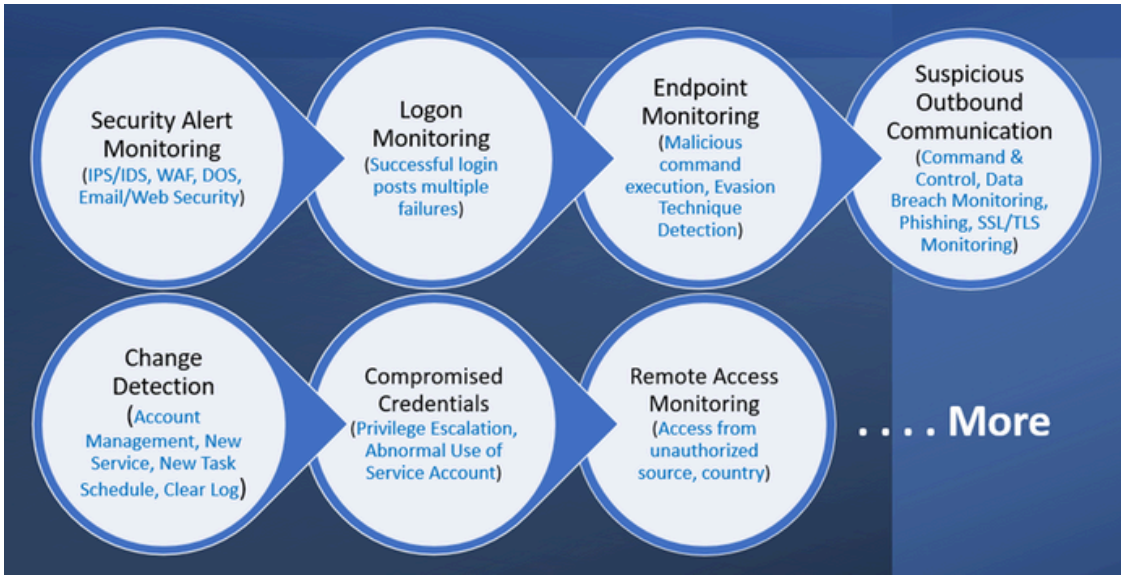
Alerts, Dashboard and Report

- สามารถส่ง Alert ผ่าน Webhook หรือ API Integration ไปยังอุปกรณ์ภายนอกได้
- สามารถนำ Logs ที่จัดเก็บไว้มาสร้าง Use Cases ด้าน Security Compliance ได้หลากหลาย เช่น การสร้าง Security Dashboards และ Reports ตามกฎหมาย และข้อกำหนดของมาตรฐานด้านความมั่นคงปลอดภัยต่างๆ

ประเภทของ Log Source ที่สามารถรับเข้ามาเฝ้าระวังฯ

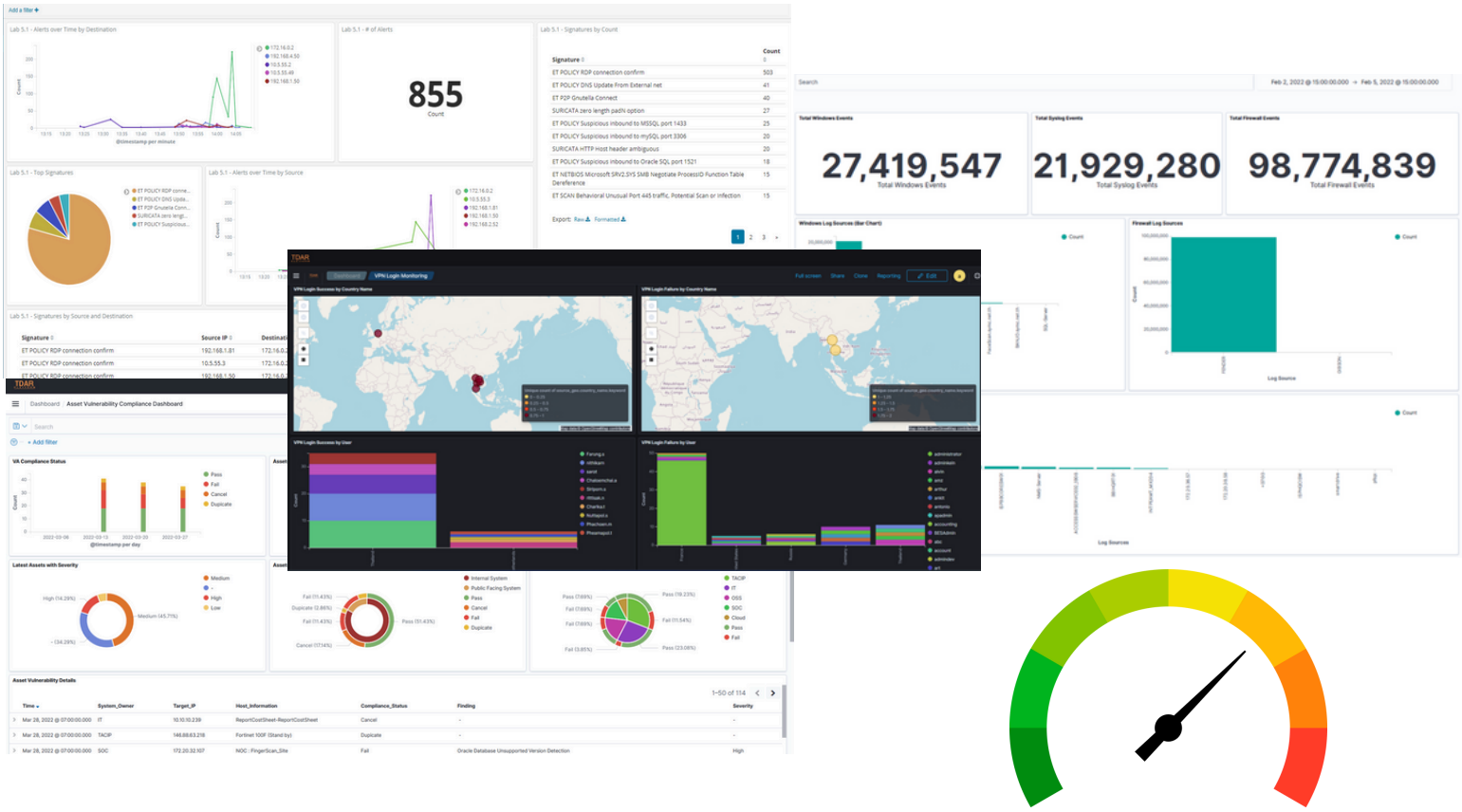


Security Compliance Use Cases



Alerts, Dashboard and Report

- สามารถออกรายงานเป็นรายครั้ง รายวัน รายสัปดาห์ และรายเดือน ได้ทันที (On-demand) ตามที่ผู้ใช้งานต้องการ และสามารถตั้ง Schedule ให้สร้างรายงานตามวันเวลาที่กำหนดได้
- มี Dashboard ที่สรุปข้อมูล Top Source, Top Destinations, Top Applications, Top Websites, Top Threats, System Event และ Resource Usage ได้เป็นอย่างน้อย



- สามารถแสดงข้อมูล Log เช่น Date, Time, Source IP, User, Destination IP และ Services ได้เป็นอย่างน้อย
- สามารถสร้างรายงานที่เกิดจาก Dashboard, Search และ Chart ได้
- สามารถสร้างรายงานในรูปแบบไฟล์ PDF, PNG และ CSV ได้เป็นอย่างน้อย
- ระบบมีส่วนสรุปของข้อมูลรายงาน รายการ Host หรือ อุปกรณ์ที่ส่ง Log เข้ามาจัดเก็บ โดยระบุข้อมูลได้อย่างน้อย ดังนี้ ชื่อ Host, ปริมาณเหตุการณ์, ปริมาณข้อมูล Log โดยสามารถส่งออกข้อมูลได้ทั้งแบบ PDF,CSV

JUST SOME OF THE FEATURES...

Specific Abilities

- มีความสามารถวิเคราะห์เหตุการณ์ภัยคุกคามด้วย AI หรือ Machine Learning สำหรับใช้จัดทำ Use Case ประเภท Anomaly Detection ที่ต้องการได้
- รองรับการทำหน้าที่เป็น DNS Firewall บนตัวระบบได้ เพื่อป้องกันภัยคุกคามทางไซเบอร์ เช่น Phishing และ Malware ที่เกิดจากการใช้งานอินเตอร์เน็ตของเครื่องผู้ใช้งานภายในองค์กร (Prevention)
- มี Use Case สำหรับการวิเคราะห์ภัยคุกคามทางไซเบอร์ (Threat Detection) อย่างน้อย 15 Use Case เช่น
  - Abnormal Login Monitoring
  - New Service Monitoring
  - Unauthorized Change Monitoring
  - Privilege Escalation Monitoring
  - Compromised Host Monitoring
  - Command and Control Monitoring
  - Malware Monitoring
  - Unauthorized System Monitoring
  - Phishing Attack Monitoring
  - DNS Tunneling Attack Monitoring
  - SSL/HTTPS Abnormal Behavior Analysis
  - Powershell Evasion Attack Analysis
  - Frequency Analysis of Domain Name, Service Name, Hostname
  - Top 1 Million Domain Analysis
  - Abnormal VPN Access Monitoring