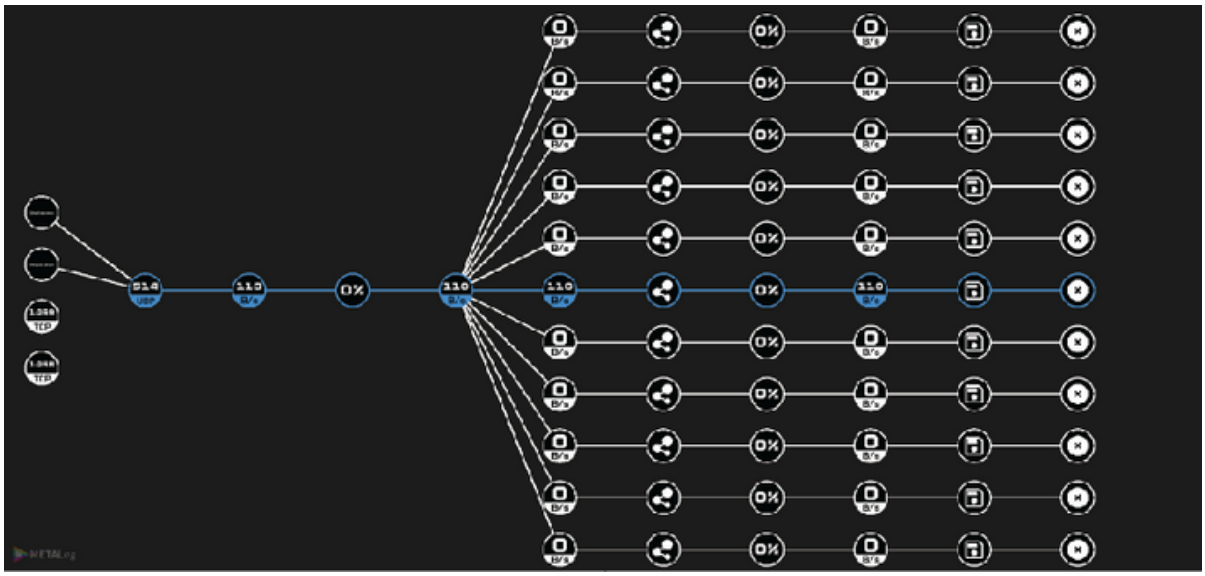
SRAN
IT Security Next Generation

SRAN Module Logger (Metalog)

HIGH PERFORMANCE LOG MANAGEMENT

ระบบจัดเก็บและรวบรวมข้อมูลจราจรทางคอมพิวเตอร์ (Log files) เก็บและค้นหาได้ในเครื่องเดียว สามารถเชื่อมการทำงานร่วมกับ SIEM ได้ รองรับทั้ง Windows และระบบปฏิบัติการ Linux



Powerfull
High Performance รองรับข้อมูล Log ขนาดใหญ่ จากหลาย Source ได้

Log Collect
รวบรวมข้อมูลจากหลาย Source ได้แก่ Network Devices Log, Endpoint Log ที่ได้จาก Windows Agent และ Linux Agent รวมถึง Application Log ทั้งในรูปแบบ Syslog ตาม RFC5424, RFC3164 และรูปแบบที่ไม่ใช่ Syslog

Log Archive
สามารถจัดเก็บข้อมูล Log files ขนาดใหญ่ โดยมีเทคโนโลยีในการบีบอัดไฟล์ ใช้การ Compressed Files แบบ LZMA และ ZSTD เพื่อลดขนาดไฟล์ดั้งเดิมได้ ลดทรัพยากรการจัดเก็บพื้นที่ฮาร์ดดิส ข้อมูลมีการเข้ารหัสด้วยความมั่นคงปลอดภัยสูง เหมาะกับการจัดเก็บข้อมูลส่วนบุคคลในองค์กรที่เป็นข้อมูล Syslog และ Non-Syslog รองรับทั้งอุปกรณ์เครือข่าย และเครื่องแม่ข่ายที่เป็น Database และ Application ที่สำคัญขององค์กร

Filter and Forward
มีความสามารถในการคัดกรอง ข้อความ เนื้อหา ฟิลด์ และเนื้อหาในไฟล์ Log เพื่อทำการส่งต่อให้กับ SIEM หรือส่งต่อไประบบ AI เพื่อวิเคราะห์ผลต่อไปได้

Full Text Search
สามารถทำการค้นหาข้อมูล Full Text Search Dynamic LINQ เป็น Expression Language และ Event Query Language

Fast Log Search
Log Search ค้นหาข้อมูลจากเนื้อหาในไฟล์ Log ขนาดใหญ่ได้รวดเร็ว Dashboard มีการแสดงผลเป็นแบบเรียลไทม์ และสามารถทราบสถานการณ์ปัจจุบัน ค่าจำนวน Log แต่ละ Source ภาพรวมการใช้งาน ค่า EPS ที่มีการรับและส่งข้อมูล ปริมาณค่าการใช้งานแรม และซีพียู

SRAN
IT Security Next Generation

SRAN Module Logger (Metalog)

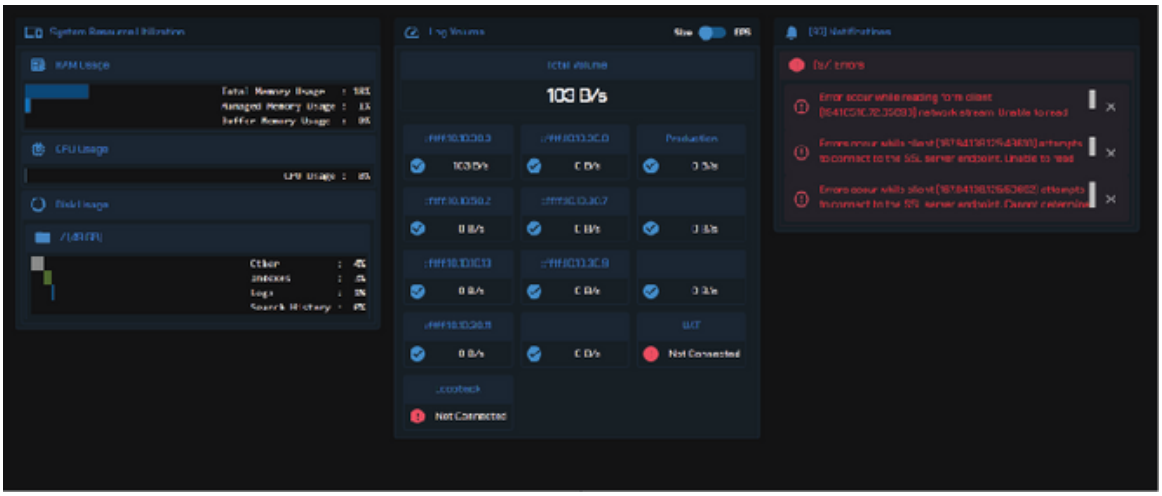
คุณสมบัติเฉพาะดังนี้

1. MEGA Traffic
รองรับปริมาณข้อมูลขนาดใหญ่ได้ เริ่มปริมาณข้อมูลตั้งแต่ 10,000 – 1,000,000 events per second (EPS) โดยสามารถเก็บบันทึก และค้นหาข้อมูล โดยรวมรวมข้อมูลจากเครือข่ายและ Host ได้

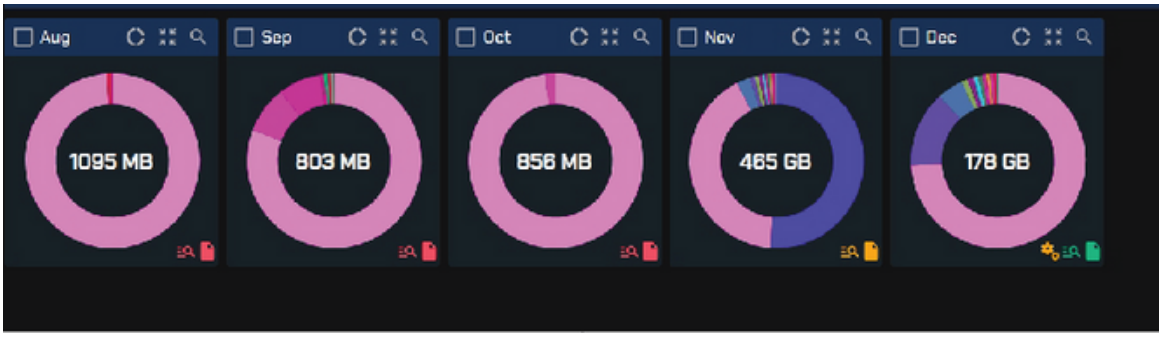
2. Intelligent Compressed
การทำ Log Archive เพื่อเก็บข้อมูลย้อนหลัง โดยใช้การผสมเทคโนโลยี Adaptive Compression Algorithm การบีบอัดข้อมูลเพื่อให้การจัดเก็บเต็มไปด้วยประสิทธิภาพ

3. Fast Search
สามารถเปิดไฟล์ขนาดใหญ่ และค้นหาข้อความในไฟล์ขนาดใหญ่ภายในไม่กี่วินาที

4. Real Time Data Logs
มีความสามารถในการรับค่า Log files แบบ Advanced Mode โดยกำหนดค่า Initial Buffer Size, Minimum Buffer Size, Maximum Buffer Size ตั้งค่าขนาดของ Memory Buffer ขนาดของ Buffer จะปรับเปลี่ยนอัตโนมัติตามปริมาณ Traffic ของ Log ที่เข้าสู่อุปกรณ์ โดยจะเริ่มจากค่าเริ่มต้น (Initial Buffer Size) ก่อนจากนั้นขนาดของ Buffer จะเพิ่มขึ้นหรือลดลงแปลผันตรงกับขนาดของ Traffic แต่จะไม่มากกว่าค่าสูงสุด (Maximum Buffer Size) หรือน้อยกว่าขนาดต่ำสุด (Minimum Buffer Size)



5. การบริหารจัดการสิทธิ์การเข้าถึงระบบ
สามารถทำการจัดการสิทธิ์การเข้าใช้งานระบบ Role-Based Access Control (RBAC) Device Setting, User Setting, Log Inspection และ Device Statistics กำหนดการทำ Log Archive ด้วย Storage Selection Algorithm โดยเชื่อมต่อกับอุปกรณ์ภายนอกได้ มีความสามารถในการกำหนดค่า Certificate SSL เพื่อเพิ่มความปลอดภัยในการส่งข้อมูลผ่านระบบ Cloud และ ใช้ส่ง Log ข้ามระบบเครือข่ายคอมพิวเตอร์



SRAN
IT Security Next Generation

SRAN Module Logger (Metalog)

6. รองรับการติดตั้ง Agent เพื่อรับข้อมูล Log
Linux Audit Logs, Log Files, RFC5424, RFC3126, Non-Syslog, Windows Event logs

คุณสมบัติพื้นฐานดังนี้

1. เป็นอุปกรณ์ Appliance หรืออุปกรณ์คอมพิวเตอร์ที่ได้มาตรฐาน สามารถเก็บรวบรวมเหตุการณ์ (Logs of Events) ที่เกิดขึ้นในอุปกรณ์เป็น Appliance หรือ Non-Appliance เช่น Firewall, Network Devices ต่างๆ, ระบบปฏิบัติการ, ระบบ Appliance, ระบบเครือข่าย และระบบฐานข้อมูล เป็นต้น โดยสามารถแสดงผลอยู่ภายใต้แบบ (format) เดียวกันได้ไม่จำกัดจำนวนอุปกรณ์ต่อระบบ
2. สามารถรวบรวมข้อมูลจากหลาย Source ได้แก่ Network Devices Log, Endpoint Log ที่ได้จาก Windows Agent และ Linux Agent รวมถึง Application Log ทั้งในรูปแบบ Syslog ตาม RFC5424, RFC3164 และรูปแบบที่ไม่ใช่ Syslog ได้
3. สามารถจัดเก็บข้อมูลชนิด Raw Data โดยแยกจัดเก็บตามชื่ออุปกรณ์ วันที่ และชั่วโมงได้
4. สามารถทำการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ในลักษณะของ Centralized และ Forwarder Mode ได้ สามารถส่งต่อ Log Forward โดยการสร้าง Filter ตามเงื่อนไขที่ต้องการ เช่น ชื่อ Host, ชนิดของเหตุการณ์ ระดับความสำคัญ หรือ Message Keyword โดยส่งต่อไปยัง Syslog Server อื่น หรืออุปกรณ์ประเภท SIEM ผ่าน Syslog Protocol ได้ โดยที่ไม่เปลี่ยนแปลงข้อมูลต้นทาง
5. รองรับการส่งข้อมูลและรับข้อมูลผ่าน Network Protocol UDP และ TCP และสามารถใช้ TLS/SSL Certificate ที่สื่อสารกับอุปกรณ์ต้นทางแบบ Secure Protocol ได้
6. มีการแสดงผลแบบ Real-Time ที่สามารถเห็นเครื่อง Source Log ที่ส่งค่า Log จากต้นทาง ทั้งปริมาณข้อมูลจำนวน EPS, Throughput, ปริมาณ Log ที่ทำการ Forward และปริมาณข้อมูลที่ฝั่งรับ Log Destination ที่รับ Log ปลายทาง
7. มีระบบการเข้ารหัสข้อมูลเพื่อใช้ยืนยันความถูกต้องของข้อมูลที่จัดเก็บตามมาตรฐาน SHA-256
8. สามารถดาวโหลด Log Archive โดยการเลือกช่วงเวลาที่ต้องการได้ พร้อมทั้ง Log ที่ส่งออกไปสามารถกำหนดการเข้ารหัสข้อมูลได้ ไม่ว่าเป็น Zip แบบมีรหัสผ่าน และเข้ารหัส Log แบบ AES

SRAN
IT Security Next Generation

SRAN Module Logger (Metalog)

9. สามารถจัดเก็บ Log file ในรูปแบบ Syslog ของอุปกรณ์ เช่น Router, Switch, Firewall, VPN, Server ได้
10. สามารถบริหารจัดการอุปกรณ์ผ่านมาตรฐาน HTTPS, Command Line Interface และ SSH ได้
11. สามารถจัดเก็บฐานข้อมูลในรูปแบบ NOSQL เพื่อความรวดเร็วในการจัดเก็บและค้นหาได้
12. สามารถทำการค้นหาข้อมูล Full Text Search Dynamic LINQ เป็น Expression Language และ Event Query Language ได้
13. มีเทคโนโลยีการ Index ข้อมูล Log File เพื่อประสิทธิภาพในการค้นหา โดยรองรับทั้งแบบ Full Text Search และแบบกำหนด Field ในการค้นหา โดยสามารถระบุเงื่อนไขในการค้นหาได้ เช่น AND, OR, Wildcard Expression, Regular Expression และกำหนดช่วงเวลาหรือขอบเขตในการค้นหาได้
14. สามารถจัดเก็บ Log file ได้ถูกต้อง ตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ โดยมีซอฟต์แวร์ SRAN Module Logger ที่ผ่านมาตรฐานของศูนย์อิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ NECTEC มศอ. 4003.1-2560 (NECTEC STANDARD NTS 4003.1-2560) และหนังสือรับรอง MiT (Made in Thailand) จาก สภาอุตสาหกรรม (ซอฟต์แวร์เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์)
15. สามารถจัดเก็บข้อมูล Log files ขนาดใหญ่ โดยมีเทคโนโลยีในการบีบอัดไฟล์ ใช้การ Compressed Files แบบ LZMA และ ZSTD เพื่อลดขนาดไฟล์ดังเดิมได้ (สามารถบีบอัดข้อมูลบนพื้นที่จัดเก็บได้ 15:1) ลดทรัพยากรการจัดเก็บพื้นที่ฮาร์ดดิส ข้อมูลมีการเข้ารหัสด้วยความมั่นคงปลอดภัยสูง เหมาะกับการจัดเก็บข้อมูลส่วนบุคคลในองค์กรที่เป็นข้อมูล Syslog และ Non-Syslog รองรับทั้งอุปกรณ์เครือข่าย และเครื่องแม่ข่ายที่เป็น Database และ Application ที่สำคัญขององค์กรได้
16. สามารถทำการสำรองข้อมูล (Data Backup) ไปยังอุปกรณ์จัดเก็บข้อมูลภายนอก เช่น Tape หรือ External Storage ได้
17. สามารถรับปริมาณข้อมูลจาก Log files ที่ส่งมาจาก Source ต่างๆจำนวนมากได้โดยวิธีการสร้าง Load Balancer ในการจัดคิวของข้อมูลแบบอัตโนมัติ