DATA SHEET

Software Version 7

INTELLIGENT LOG MANAGEMENT PLATFORM

SOFTNIX LOGGER

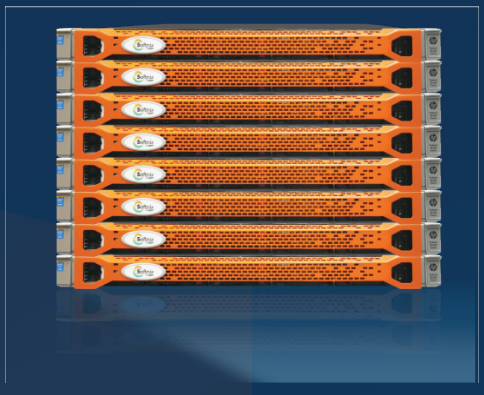
แพลตฟอร์มบริหารจัดการ Log แบบรวมศูนย์ เสริมพลังด้วย AI พร้อมรองรับ Compliance ครบวงจร

ระบบจัดเก็บและวิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์สำหรับองค์กรขนาดกลางและขนาดใหญ่ ตรวจจับภัยคุกคามแบบเรียลไทม์ วิเคราะห์อัตโนมัติด้วย AI และรองรับการจัดเก็บ Log ตาม พ.ร.บ. คอมพิวเตอร์ พ.ศ. 2560 พร้อมมาตรฐานสากล

- NTS 4003.1-2560 Certified
- AI Log Analyzer
- Security Threat Detection
- Compliance & MITRE ATT&CK

Softnix Technology Co., Ltd.

www.softnixlogger.com · sales@softnix.co.th · โทร. 02-245-4942-3



WHY SOFTNIX LOGGER

แพลตฟอร์ม Log Management อัจฉริยะ สำหรับองค์กรยุคใหม่

Softnix Logger คือระบบจัดเก็บและบริหารจัดการ Log แบบรวมศูนย์ (Centralized Log Management) ที่ออกแบบมาเพื่อรองรับการจัดเก็บข้อมูลการจราจรทางคอมพิวเตอร์ตาม **พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560** และได้รับการรับรองตามมาตรฐาน NTS 4003.1-2560 รองรับการรับส่ง Log จากอุปกรณ์หลากหลายประเภท ทั้ง Firewall, Network Devices, Operating Systems, Databases และ Applications พร้อมความสามารถด้าน AI Analytics, Real-time Monitoring, Security Threat Detection และ Compliance Dashboard ในระบบเดียว

10:1	60,000	2 ปี+	5+
อัตราบีบอัด Log สูงสุด	EPS สูงสุดต่อเครื่อง (Events/sec)	จัดเก็บ Log ตามข้อกำหนดกฎหมาย	มาตรฐาน Compliance สากล

คุณสมบัติเด่น · KEY HIGHLIGHTS

มาตรฐาน NTS 4003.1-2560

ผ่านการรับรองระบบจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ตามกฎหมายไทย

ไม่จำกัด Device & ปริมาณข้อมูล

รองรับอุปกรณ์และปริมาณ Log ต่อวันแบบไม่จำกัดตาม License

AI Log Analyzer

วิเคราะห์และสรุปเหตุการณ์จาก Log โดยอัตโนมัติพร้อมคำแนะนำ

Security Threat Detection

ตรวจจับและแจ้งเตือนภัยคุกคามแบบเรียลไทม์พร้อม Heat Map

บีบอัด Log สูงสุด 10:1

ประหยัดพื้นที่จัดเก็บ ปรับรูปแบบการบีบอัดได้ผ่านหน้าจอ

Compliance Dashboard

PCI-DSS, GDPR, PDPA, NIS, HIPAA พร้อม MITRE ATT&CK Mapping

Real-time Monitoring & Alert

แจ้งเตือนผ่าน Email, LINE, Telegram และ Web Hook

Raw Log ปลอดภัย แก้ไขไม่ได้

ตรวจสอบความถูกต้องด้วย Hashing และเข้ารหัส AES-256

1 Log Collection & Management

เก็บรวบรวมและบริหารจัดการ Log จากทุกแหล่งในระบบเดียว

รองรับการรับส่ง Log จากอุปกรณ์และระบบที่หลากหลาย พร้อมเครื่องมือจัดการครบชุด ตั้งแต่การรับข้อมูล การบีบอัด การส่งต่อ ไปจนถึงการแยกวิเคราะห์โครงสร้าง Log ทั้งหมดกำหนดค่าได้ผ่านหน้าจอบริหารจัดการโดยไม่ต้องเขียนคำสั่ง

Syslog Protocol

รองรับ UDP, TCP และการเข้ารหัส TLS รองรับรูปแบบ BSD-syslog และ IETF syslog พร้อมกำหนด Port ได้เอง

Non-Syslog Collection

เก็บ Log จากระบบปฏิบัติการ (OS) และฐานข้อมูลผ่าน Softnix Log Agent ติดตั้งง่าย

License แบบไม่จำกัด

ไม่จำกัดจำนวน Devices และไม่จำกัดขนาดข้อมูลต่อวัน รองรับการเติบโตขององค์กร

Compression 10:1

บีบอัดข้อมูลสูงสุด 10:1 ปรับ Compression Type ได้ผ่านหน้าบริหารจัดการ

Log Forwarding

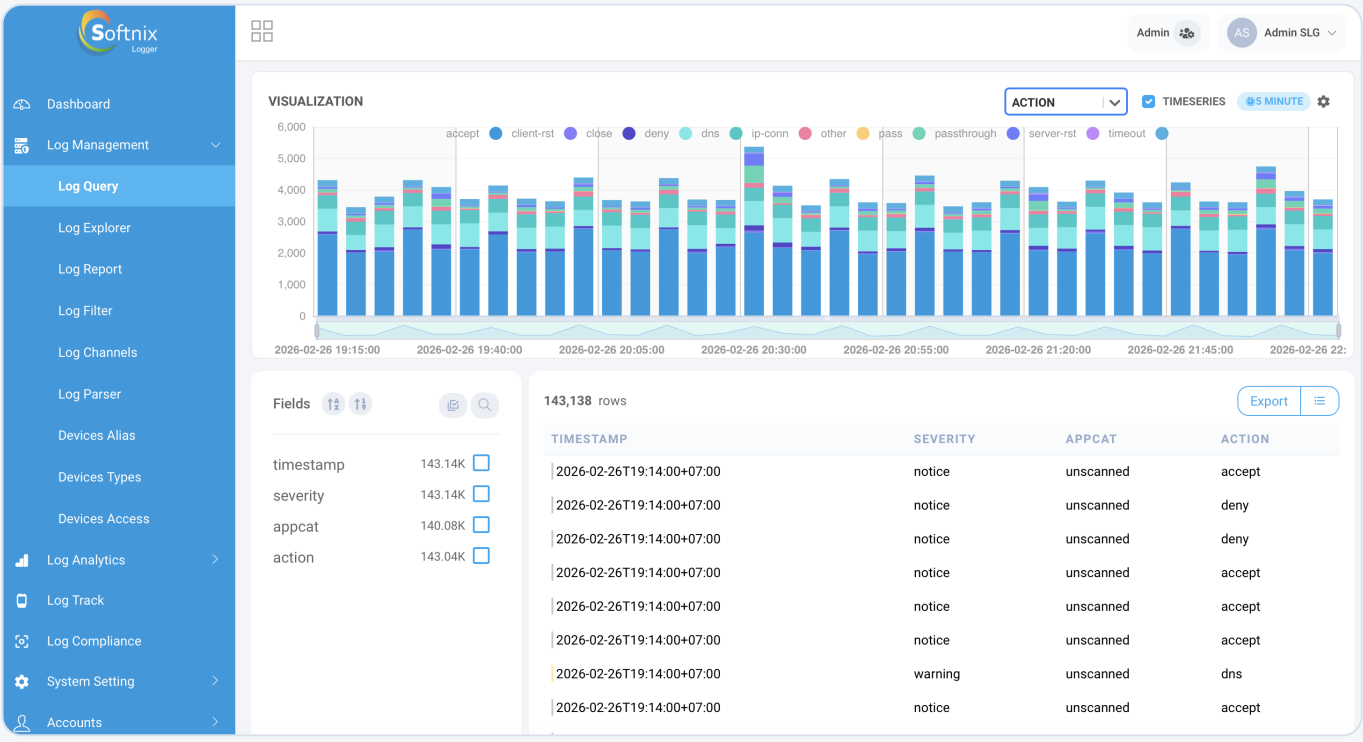
ส่งต่อ Log ไปยัง Syslog Server หรือ SIEM พร้อมกำหนด Filter ตามเงื่อนไข

Log Parser (No-Code)

รองรับ KV, CSV, GROK, JSON ผ่าน UI โดยไม่ต้องใช้ Command Line

Log Filter & Devices Alias

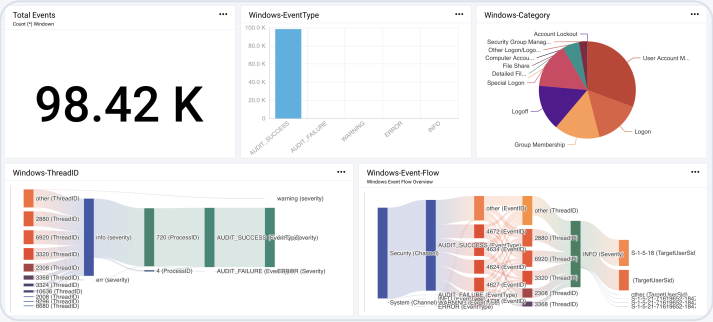
กำหนดเงื่อนไขตาม Host, Facility, Severity, Keyword และ Hashtag พร้อมตั้งชื่อ Alias ให้อุปกรณ์ที่ส่ง Log เข้ามาเพื่อให้เข้าใจง่าย



หน้าจอ Log Query — ค้นหาและแสดงผล Log พร้อม Visualization แบบเรียลไทม์

2 Log Query, Analytics & Visualization

ค้นหา วิเคราะห์ และเปลี่ยนข้อมูล Log จำนวนมากให้เป็นภาพที่เข้าใจง่าย



Log Analytics Dashboard — กราฟหลากหลายรูปแบบ Near Real-time

- **ค้นหาทรงพลัง ยืดหยุ่น** รองรับทั้ง Real-time และ On-Demand ค้นหาจาก Log Archive อัตโนมัติ ไม่ต้องแยกการค้นหา
- รองรับ Operation: Equal, Not Equal, AND, OR พร้อม **Auto Suggestion** และปรับแต่ง Field ได้ตามต้องการ
- บันทึกคำสั่งค้นหาเพื่อใช้ในอนาคต และเปิด/ปิดการประมวลผลแบบ Real-time เพื่อประหยัดทรัพยากร
- ส่งออกรายงานเป็น **PDF, CSV และ JSON**

รูปแบบกราฟที่รองรับ

Bar, Pie, Donut, Polar, Line, Area, Table, Metric, Radar, Bar Label, Bar Stack และ **Sankey Flow** รองรับ Near Real-time, Drill Down, Filter, Search และ Full Screen

ส่งออก: JPEG · PNG · PDF · SVG · TIF · DOCX · ODT · HTML · XHTML

Log Report สำเร็จรูป

Total Events, Total Bandwidth, Total Log Usage, Top 10 Total Event / EPS / Log Usage, Total Event per Minute, EPM Channel/Host, Facility และ Severity พร้อมสรุประยะเวลาจัดเก็บและปริมาณข้อมูล

3 AI Log Analyzer

เทคโนโลยี AI ที่เปลี่ยน Data ให้เป็น Insight โดยอัตโนมัติ

เทคโนโลยี AI ที่วิเคราะห์และสรุปรายงานเหตุการณ์จาก Log โดยอัตโนมัติ ช่วยให้ผู้ดูแลระบบเข้าใจสถานการณ์ ได้อย่างรวดเร็ว ลดเวลาในการสอบสวนเหตุการณ์ และตัดสินใจตอบสนองภัยคุกคามได้ทันท่วงที

AI Analyze

รายงานการวิเคราะห์ความปลอดภัยและประสิทธิภาพของเครือข่าย

สรุปสำหรับผู้บริหาร

ภาพรวม: รายงานนี้เป็นการวิเคราะห์ข้อมูลบันทึก (log data) ณ วันที่ 2026-02-27 การวิเคราะห์พบกิจกรรมเครือข่ายที่ผิดปกติหลายรายการและเหตุการณ์ที่อาจเป็นภัยคุกคามความปลอดภัย โดยเฉพาะการเชื่อมต่อขาออกจากเครื่องคอมพิวเตอร์ที่ใช้ระบบปฏิบัติการที่ล้าสมัยไปยัง IP ในต่างประเทศจำนวนมาก

ข้อกังวลหลัก:

- **การเชื่อมต่อที่น่าสงสัยจากเครื่อง Win7-PC**: เครื่องคอมพิวเตอร์ win7-PC (192.168.10.7) ซึ่งใช้ระบบปฏิบัติการ Windows 7 ที่หมดระยะเวลาการสนับสนุนแล้ว (End-of-Life) มีการเชื่อมต่อขาออกไปยังหลายประเทศ (เช่น จีน, รัสเซีย, อาร์เจนตินา) บนพอร์ต UDP ที่ไม่เป็นมาตรฐานจำนวนมาก ซึ่งเป็นสัญญาณบ่งชี้ว่าอาจมีการติดมัลแวร์หรือเป็นส่วนหนึ่งของเครือข่าย Botnet
- **ความเสี่ยงจากซอฟต์แวร์ที่ล้าสมัย**: การใช้ระบบปฏิบัติการที่ไม่ได้รับการอัปเดตความปลอดภัยทำให้องค์กรมีความเสี่ยงสูงต่อการถูกโจมตีผ่านช่องโหว่ที่รู้จักกันดี
- **นโยบายการเชื่อมต่อขาออกที่หละหลวม**: นโยบายไฟร์วอลล์อาจอนุญาตให้มีการเชื่อมต่อขาออกจากเครือข่ายภายในไปยังอินเทอร์เน็ตมากเกินความจำเป็น ซึ่งเพิ่มความเสี่ยงในการสื่อสารของมัลแวร์ไปยังเซิร์ฟเวอร์ควบคุม (Command and Control)

ข้อเสนอแนะ:

- **แยกและตรวจสอบเครื่องที่น่าสงสัย**: แยกเครื่อง win7-PC (192.168.10

AI Log Analyzer — รายงานวิเคราะห์อัตโนมัติพร้อมข้อเสนอแนะการแก้ไข

DATA ข้อมูล Log ดิบ → **AI LOG ANALYZER** ประมวลผลด้วย AI → **INSIGHT** ข้อสรุปที่นำไปใช้ได้

วิเคราะห์ความปลอดภัยและประสิทธิภาพเครือข่าย

ประเมินสุขภาพและความเสี่ยงของเครือข่ายจากพฤติกรรมใน Log

ภาพรวมเหตุการณ์สำคัญที่เกิดขึ้น

สรุปเหตุการณ์เด่นในช่วงเวลาที่เลือกอย่างกระชับ

ข้อกังวลหลักและคำแนะนำการแก้ไข

ระบุประเด็นเสี่ยง เช่น การเชื่อมต่อขาออกที่น่าสงสัย พร้อมแนวทางจัดการ

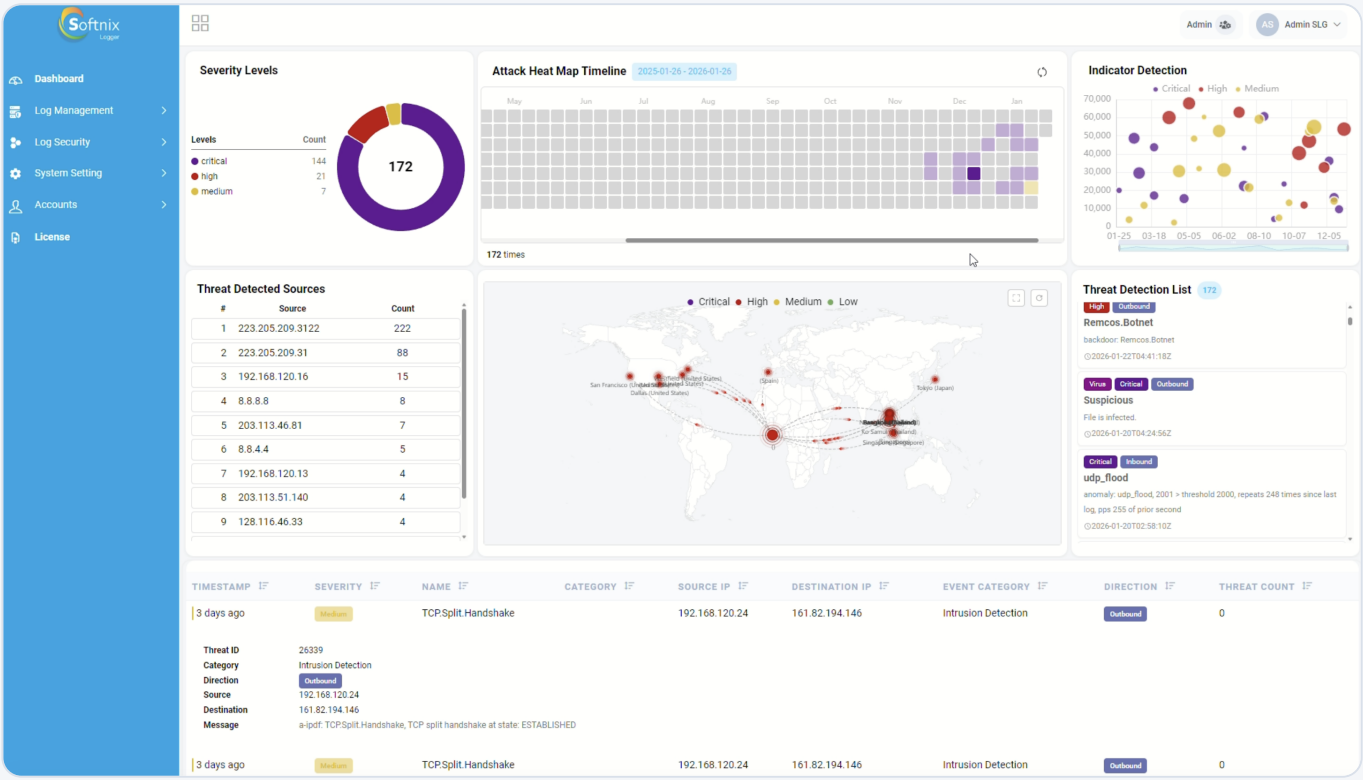
ผลการวิเคราะห์โดยละเอียด

รายงานเชิงลึกที่ส่งออกเป็น PDF / DOCX เพื่อรายงานผู้บริหาร

4 Security Threat Detection

ตรวจจับและแจ้งเตือนภัยคุกคามด้านความปลอดภัยแบบครบวงจร

Softnix Logger ไม่ได้เป็นเพียงระบบจัดเก็บ Log แต่ยังตรวจจับและแจ้งเตือนภัยคุกคามได้แบบครบวงจร เหมาะกับองค์กรขนาดกลางและใหญ่ที่ใช้เครือข่ายและข้อมูลจำนวนมาก รวมถึงหน่วยงานที่เก็บข้อมูลส่วนบุคคลหรือข้อมูลลับ ช่วยลดความเสี่ยงจากการสูญเสียข้อมูล ตอบสนองต่อภัยคุกคามได้อย่างรวดเร็ว และวิเคราะห์แนวโน้มเพื่อวางแผนการป้องกันเชิงรุก



Security Threat Detection Dashboard — ตรวจจับภัยคุกคามพร้อมแผนที่แหล่งโจมตีทั่วโลก

องค์ประกอบของ Threat Detection Dashboard

- **Severity Levels** — แสดงระดับความรุนแรง Critical, High, Medium, Low
- **Attack Heat Map Timeline** — แสดงเหตุการณ์การโจมตีตามช่วงเวลา
- **Indicator Detection** — ตรวจจับสัญญาณบ่งชี้ภัยคุกคาม
- **Threat Detected Sources** — แสดงแหล่งที่มาของการโจมตีบนแผนที่โลก
- **Threat Detection List** — รายละเอียดเหตุการณ์แต่ละรายการพร้อมประเภทการโจมตี

ตอบสนองได้รวดเร็ว

ลดเวลาในการตรวจพบและตอบสนองต่อภัยคุกคาม ช่วยจำกัดความเสียหายก่อนลุกลาม

วิเคราะห์แนวโน้มเชิงรุก

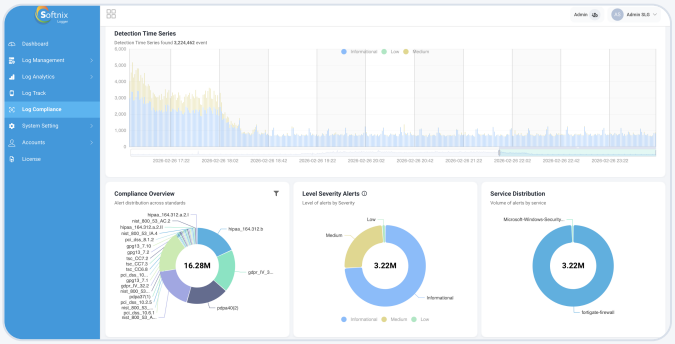
มองเห็นรูปแบบและแนวโน้มการโจมตี เพื่อวางแผนป้องกันล่วงหน้าอย่างมีประสิทธิภาพ

5 Compliance Dashboard & MITRE ATT&CK

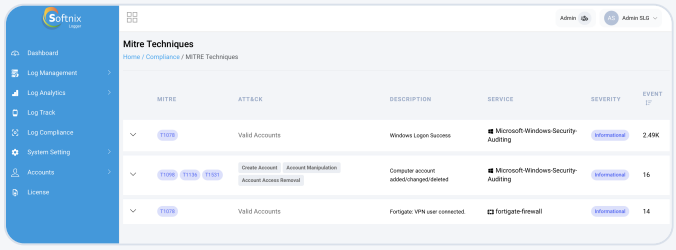
มองเห็นสถานะการปฏิบัติตามข้อกำหนดและเทคนิคการโจมตีในที่เดียว

PDPA | GDPR | PCI-DSS | NIS | HIPAA

Compliance Dashboard แสดงข้อมูลอย่างน้อย: Detection Time Series, Compliance Overview, Level Severity Alerts, Sources/IP, Service Distribution, Alert Descriptions พร้อม MITRE Techniques และ Tactics ตามมาตรฐาน **MITRE ATT&CK** ช่วยให้ทีมความปลอดภัยเชื่อมโยงเหตุการณ์เข้ากับเทคนิคการโจมตีที่รู้จัก และประเมินความสอดคล้องกับมาตรฐานได้ทันที



Compliance Dashboard — ภาพรวมเหตุการณ์ด้าน Compliance



MITRE ATT&CK — Mapping เทคนิคการโจมตีเข้ากับเหตุการณ์จริง

Detection Time Series

ไทม์ไลน์เหตุการณ์ตรวจจับแยกตามระดับความรุนแรง

Tactic & Technique Mapping

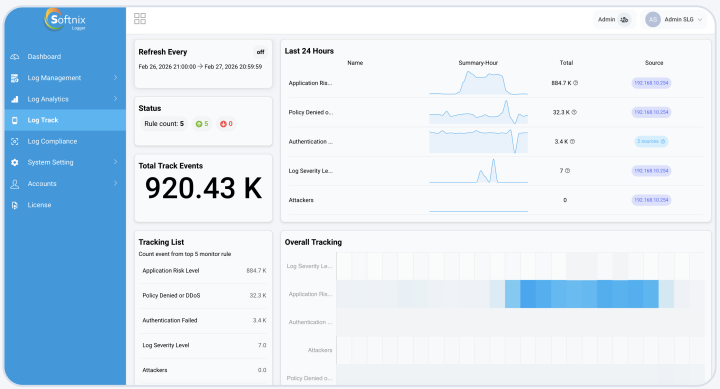
จับคู่เหตุการณ์กับ MITRE Techniques เช่น T1078 Valid Accounts

Severity Alert Analysis

วิเคราะห์การแจ้งเตือนตามระดับ Informational ถึง Critical

6 Log Tracking, Monitoring & Log Integrity

ติดตามเหตุการณ์สำคัญเรียลไทม์ และรักษาความถูกต้องของ Log ตามกฎหมาย



Log Tracking Dashboard — ติดตามเหตุการณ์แบบเรียลไทม์

- สร้างเงื่อนไขการติดตามได้ **ไม่จำกัด** พร้อม Template สำเร็จรูปและสร้าง Template เพิ่มได้เอง
- มีคุณสมบัติ **Time Suppression** และแจ้งเตือนหากไม่มี Log ส่งเข้ามาเกินเวลาที่กำหนด
- Dashboard แสดง Total Track Events, Top 5 Monitor Rules และ Overall Tracking

ช่องทางแจ้งเตือน

Email · LINE App · Telegram · Web Hook

7 มาตรฐานและความถูกต้องของ Log

พ.ร.บ. คอมพิวเตอร์ พ.ศ. 2560 & NTS

จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ครบถ้วน ผ่านการรับรอง NTS 4003.1-2560 เก็บ Log Archive ไม่น้อยกว่า 2 ปี

Raw Log ที่แก้ไขไม่ได้

ตรวจสอบความถูกต้องด้วย Hashing (MD5, SHA256) พร้อมเข้ารหัสส่งออก AES-256/192/128 และ DES

Timestamp ที่เชื่อถือได้

ซิงค์เวลากับ NTP Server พร้อมแสดง Clock Stratum Status

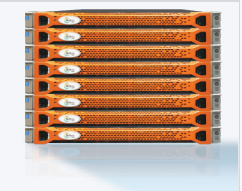
Authentication & Audit Trail

Local Users, LDAP, Active Directory พร้อม Two-Factor Authentication และบันทึกการเข้าถึงระบบของผู้ดูแล

PRODUCTS EDITION

เลือกรุ่นที่ใช่ ครอบคลุมทุกขนาดองค์กร

ยืดหยุ่นครบทุกความต้องการ ตั้งแต่ Enterprise ขนาดกลาง องค์กรขนาดใหญ่ ไป จนถึง Telco/ISP และรุ่น Virtual Machine



คุณสมบัติ	SLG-SA2-DS	SLG-SA3-DS	SLG-SA4-DS	SLG-SA2-LG	SLG-SA3-LG	SLG-SA4-LG	SLG-VM
User Environment	Medium Enterprise	Large Enterprise	Telco / ISP	Medium Enterprise	Large Enterprise	Telco / ISP	Flexible
Log Analytic	Support	Support	Support	N/A	N/A	N/A	Option
Processor	4C / 8T	8C / 16T	1–2 Socket 10C/ 20T	4C / 8T	8C / 16T	10C / 20T	CPU Multi-core
Device Support	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited
EPS	15,000	30,000	60,000	15,000	30,000	60,000	–
Memory	16 GB	32–64 GB	64–96 GB	16 GB	16–64 GB	64 GB	Min 16 GB
Network	2× 1GbE	2× 1GbE	4× 10GBase-T	2× 1GbE	2× 1GbE	4× 10GBase-T	1 GbE LAN
Internal Storage (Hot Swap)	1.92TB SSD	2–8TB SSD	10–20TB SATA + 3.84TB SSD	1TB SATA	2–8TB SATA	10–20TB SATA	Custom
Standard	FCC, CE	FCC, CE, RoHS, UL	FCC, CE, RoHS, UL	FCC, CE	FCC, CE, RoHS, UL	FCC, CE, RoHS, UL	N/A
Redundant Power	N/A	Support	Support	N/A	Support	Support	N/A
Maintenance	1 Year Support (รวมติดตั้ง) · On-Site 3 ครั้ง/ปี (กทม.) · 9:00–18:00 (8×5) · Support On-call, Email & Remote						

** SLG-VM รองรับ Software version 7.x เท่านั้น · สเปกอาจปรับเปลี่ยนตามความเหมาะสม โปรดตรวจสอบกับทีมขาย

แนวทางการเลือกรุ่นให้เหมาะกับองค์กร

ควรประเมินปริมาณ Log (EPS) ปัจจุบันและแนวโน้มการเติบโตในอนาคต พร้อมพิจารณาความต้องการด้าน Compliance และ Log Security Monitoring หากองค์กรเข้มงวดด้าน Compliance ควรเลือกรุ่นประสิทธิภาพสูงที่มี **Redundant Power** และรองรับ Dashboard, Alert และ AI-Based Monitoring ต่อเนื่อง เลือก **SSD/DS Edition** เมื่อเน้นประสิทธิภาพประมวลผล หรือ **SATA/LG Edition** เมื่อเน้นความคุ้มค่าในการเก็บข้อมูล แนะนำให้เลือกรุ่นที่รองรับมากกว่าปริมาณใช้งานจริง **20–30%** เพื่อความพร้อมด้าน Performance และ Security ในอนาคต ส่วน **VM Edition** ตอบโจทย์ความยืดหยุ่นโดยไม่ต้องเพิ่มฮาร์ดแวร์

SUMMARY OF CAPABILITIES

สรุปคุณสมบัติโดยรวม

Log Collection
Syslog UDP/TCP/TLS · Log Agent · Forwarding · Compression 10:1

Log Parser
KV / CSV / GROK / JSON · UI Config · Auto Field Extraction

Visualization
Bar/Pie/Donut/Line/Sankey · Near Real-time · Drill Down

AI Log Analyzer
AI-Powered Analysis · Anomaly Detection · Automated Insights

Threat Detection
Critical→Low Alerts · Attack Heat Map · Real-time Dashboard

Compliance
PCI-DSS/GDPR/PDPA/NIS/HIPAA · MITRE ATT&CK Mapping

Raw Log Integrity
MD5 / SHA256 · AES-256/192/128 · Tamper-proof Storage

User & System
LDAP/AD · 2FA · HTTPS/SSH · CPU/RAM/Storage Monitoring

มาตรฐานและการรับรอง

- ผ่านการรับรอง **NTS 4003.1-2560** ระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์
- รองรับ **พ.ร.บ. คอมพิวเตอร์ พ.ศ. 2560** จัดเก็บข้อมูลครบถ้วน
- Raw Log แก้ไขไม่ได้ พร้อม Audit Trail และ Timestamp ซิงค์ NTP
- Compliance: PCI-DSS, GDPR, PDPA, NIS, HIPAA, MITRE ATT&CK

พร้อมยกระดับความปลอดภัยองค์กรของคุณ

Softnix Technology Co., Ltd.
เว็บไซต์ www.softnixlogger.com
อีเมล sales@softnix.co.th
โทรศัพท์ 02-245-4942-3

ติดต่อขอ Demo & ประเมินความต้องการ