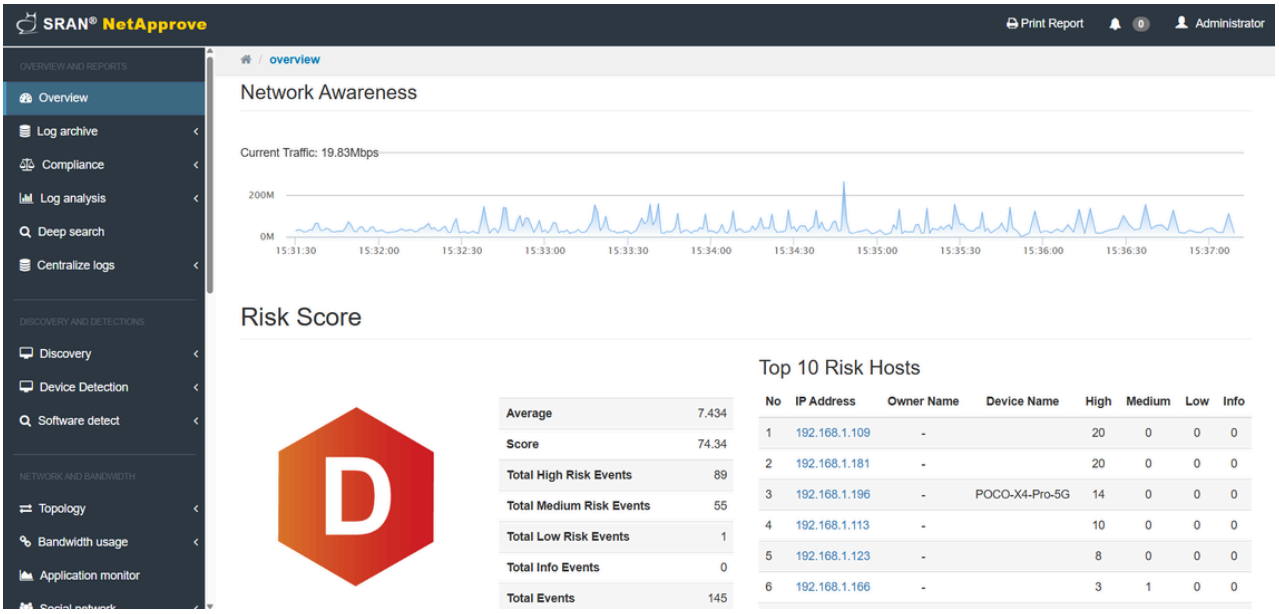
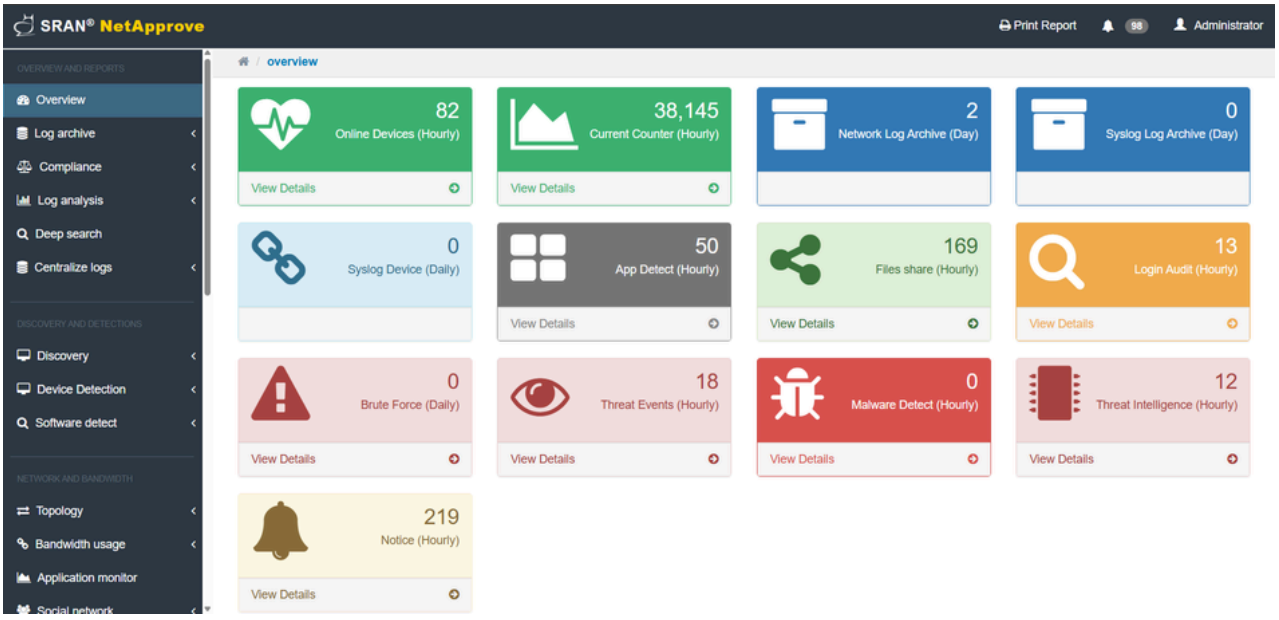
"ประสบการณ์กว่า 20 ปีที่กลั่นกรองมาเป็นผลิตภัณฑ์การจัดเก็บบันทึกข้อมูลจราจรคอมพิวเตอร์ที่คุ้มค่าที่สุดสำหรับผู้ใช้งาน" SRAN NetApprove เกิดจากการพัฒนาวิจัยอย่างต่อเนื่อง โดยนำสิ่งที่คิดว่าเป็นประโยชน์สูงสุดสำหรับผู้ใช้งาน บนนิยามว่า "Advance Centralized Log Management" เพราะเราเชื่อว่าการมองเห็นเป็นสิ่งสำคัญ ซึ่งทำให้เราประเมินสถานการณ์ต่างๆ ได้



No	IP Address	Owner Name	Device Name	High	Medium	Low	Info
1	192.168.1.109	-		20	0	0	0
2	192.168.1.181	-		20	0	0	0
3	192.168.1.196	-	POCO-X4-Pro-5G	14	0	0	0
4	192.168.1.113	-		10	0	0	0
5	192.168.1.123	-		8	0	0	0
6	192.168.1.166	-		3	1	0	0

Average	7.434
Score	74.34
Total High Risk Events	89
Total Medium Risk Events	55
Total Low Risk Events	1
Total Info Events	0
Total Events	145

รายงานความเสี่ยงที่เกิดขึ้นภายในองค์กรโดยสามารถแสดงค่าความเสี่ยงออกมาเป็นระดับความเสี่ยงได้



ภาพรวมสถานการณ์ข้อมูลที่เกิดขึ้นบนเครือข่ายองค์กร

บนหน้าจอของ SRAN NetApprove เพียงหน้าเดียวก็ทำให้ทราบถึงเหตุการณ์และสถานการณ์ปัจจุบันที่เกิดขึ้น ทุกหน้าการแสดงผล ใน SRAN NetApprove สามารถพิมพ์เป็นรายงานเพื่อนำเสนอผู้บริหารได้ (Print to PDF Report) รองรับค่าการแสดงผลผ่าน Web GUI และการออกแบบ Responsive Web Design ที่สามารถใช้งานได้ทั้งบนเครื่องคอมพิวเตอร์ และมือถือ

SRAN NetApprove เป็นการผสม 3 เทคโนโลยีในตัวเดียว อันได้แก่

NDR (Network Detection and Response), Passive Vulnerability Assessment และ Network Log Recorder

โดยมีคุณสมบัติ

1. การสำรวจข้อมูล แบบอัตโนมัติเพื่อระบุตัวตนอุปกรณ์บนระบบเครือข่ายคอมพิวเตอร์ (Automatic Identification Device)

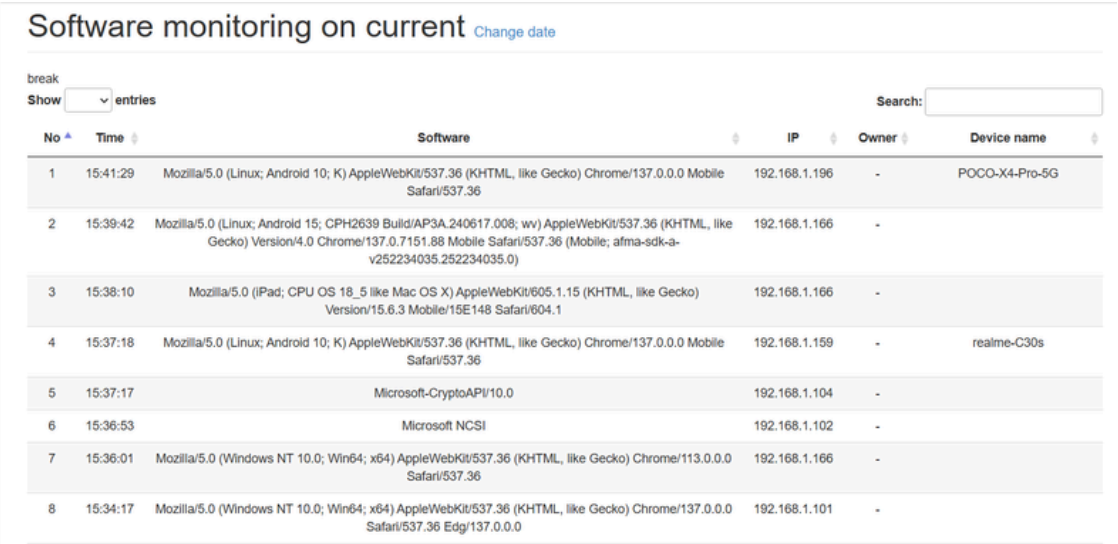
การค้นหาอุปกรณ์บนระบบเครือข่ายอย่างอัตโนมัติ เพื่อระบุอุปกรณ์ที่ใช้งาน

1.1 รายงานการคัดแยกเครื่องที่รู้จัก (Known Device) และไม่รู้จัก (Unknown Device) ได้โดยการยืนยัน (Approve) เมื่อทำการยืนยันค่าแล้วหากมีอุปกรณ์แปลกปลอมเข้าสู่ระบบเครือข่ายก็สามารถตรวจพบได้ (Rouge Detection)

1.2 รายงาน BYOD (Bring Your Own Device) แสดงค่าอุปกรณ์พกพาที่เข้าสู่ระบบเครือข่ายคอมพิวเตอร์ขององค์กรได้ซึ่งแยก Desktop (คอมพิวเตอร์พกพา เช่น โน้ตบุ๊ก) และมือถือ (Mobile) โดยรู้ว่าใครนำเครื่องพกพามาใช้งานภายในระบบเครือข่ายขององค์กร

1.3 รายงานการเก็บบันทึกเป็นค่าอุปกรณ์ (Device Inventory) โดยแยกการเก็บค่าจากอุปกรณ์ (Device) ชื่อผู้ใช้งานจากระบบ Active Directory, จาก Radius ค่าจากการ Authentication, ค่า IP Address ผู้ใช้งาน, ค่า MAC Address, แผนก (Department), ยี่ห้อรุ่นอุปกรณ์ เป็นต้น

1.4 รายงานการเก็บบันทึกค่าซอฟต์แวร์ (Software Inventory) แยกประเภทซอฟต์แวร์ที่ใช้ได้แก่ ซอฟต์แวร์ประเภทเว็บบราวเซอร์, ซอฟต์แวร์ประเภทมัลติมีเดีย, ซอฟต์แวร์ประเภทใช้งานในออฟฟิศ และซอฟต์แวร์ที่ไม่เหมาะสม เช่นโปรแกรม Bittorrent และ พวกโปรแกรม Crypto Mining ได้



Software monitoring on current Change date

break

Show entries Search:

No	Time	Software	IP	Owner	Device name
1	15:41:29	Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/137.0.0.0 Mobile Safari/537.36	192.168.1.196	-	POCO-X4-Pro-5G
2	15:39:42	Mozilla/5.0 (Linux; Android 15; CPH2639 Build/AP3A.240617.008; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/137.0.7151.88 Mobile Safari/537.36 (Mobile; afma-sdk-a-v252234035.252234035.0)	192.168.1.166	-	
3	15:38:10	Mozilla/5.0 (iPad; CPU OS 18_5 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/15.6.3 Mobile/15E148 Safari/604.1	192.168.1.166	-	
4	15:37:18	Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/137.0.0.0 Mobile Safari/537.36	192.168.1.159	-	realme-C30s
5	15:37:17	Microsoft-CryptoAPI/10.0	192.168.1.104	-	
6	15:36:53	Microsoft NCSI	192.168.1.102	-	
7	15:36:01	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.0.0 Safari/537.36	192.168.1.166	-	
8	15:34:17	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/137.0.0.0 Safari/537.36 Edg/137.0.0.0	192.168.1.101	-	

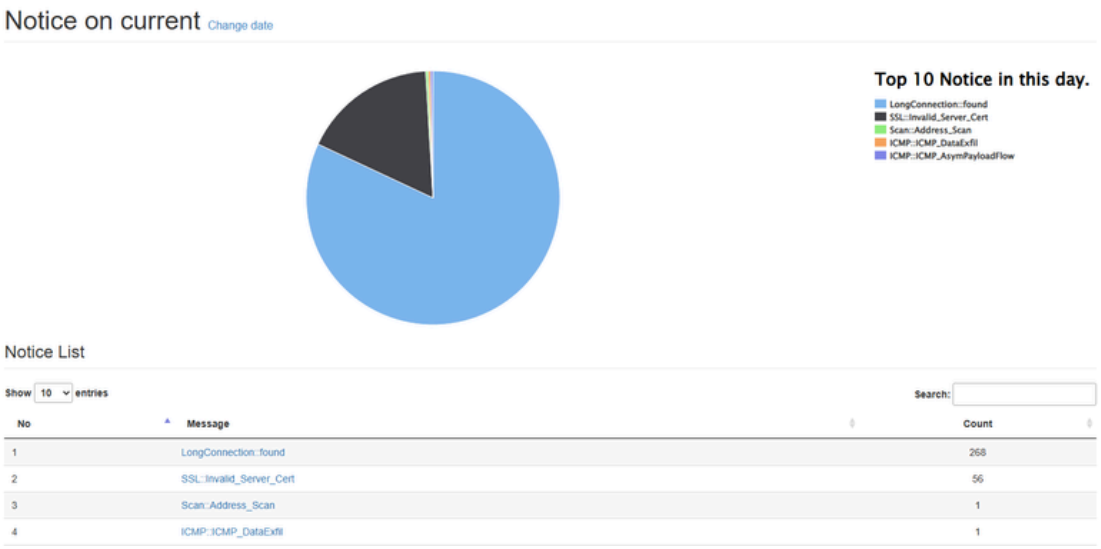
รายงานการเก็บบันทึกค่าซอฟต์แวร์ (Software Inventory)

2. การวิเคราะห์และการตรวจจับความผิดปกติข้อมูล (Detection) ประกอบด้วย

2.1 มีความสามารถตรวจจับพฤติกรรมการโจมตีระบบ ได้แก่ การ Brute Force รหัสผ่านที่เกิดขึ้นบนตัวอุปกรณ์ และเครื่องแม่ข่ายที่สำคัญ

2.2 มีความสามารถตรวจจับ มัลแวร์ / ไวรัสคอมพิวเตอร์ที่เกิดขึ้นบนระบบเครือข่าย สามารถทำการตรวจจับได้โดยไม่ต้องอาศัยการลงซอฟต์แวร์ที่เครื่องลูกข่าย (Client)

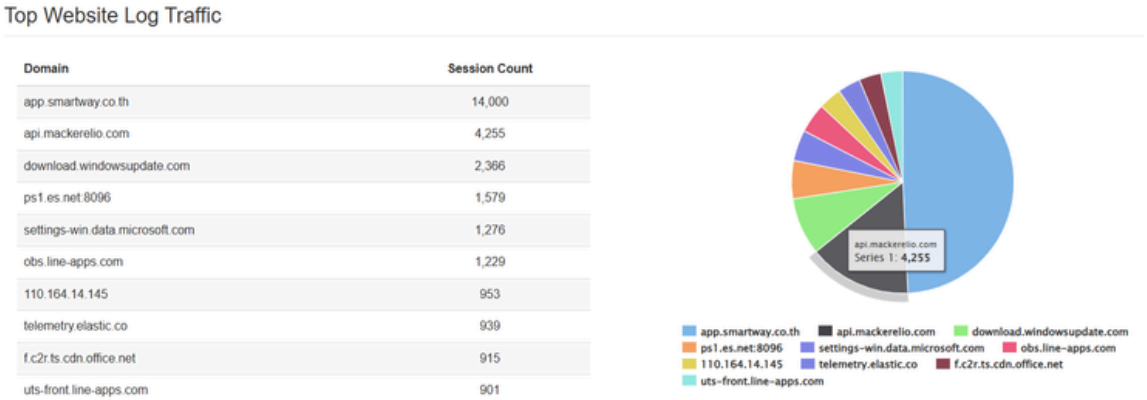
2.3 มีความสามารถตรวจพฤติกรรม Ransomware ที่อาจจะมีโอกาสเกิดขึ้นในองค์กร



รายงานผลการตรวจจับไฟล์นามสกุลที่เกี่ยวกับ Ransomware

2.4 มีความสามารถตรวจจับซอฟต์แวร์ประเภทอำพรางการสื่อสาร (Tor/Proxy) เพื่อใช้หลบเลี่ยงการตรวจจับข้อมูลภายในระบบเครือข่ายคอมพิวเตอร์

2.5 มีระบบข่าวกรองภัยคุกคามไซเบอร์ (Threat Intelligence) ระบบที่จัดการรวบรวมข้อมูลจากแหล่งข่าวโดยตรวจสอบภัยคุกคามแบบ Outside-In เทียบค่า Blacklist IP/Domain และ ค่า Hash ที่มีการโจมตีเข้าสู่ระบบภายในองค์กร และเครื่องคอมพิวเตอร์องค์กรติดต่อไปยัง C&C (Command and Control) จากภายนอก



รายงานผลการใช้งานอินเทอร์เน็ตภายในองค์กร

3. การวิเคราะห์และตรวจสอบข้อมูลตามประเภท Protocol

3.1 สามารถทำการวิเคราะห์และตรวจสอบ Protocol ที่ใช้กับ Web Application, DNS, DHCP, Active Directory, Mail, VoIP, File share

3.2 สามารถวิเคราะห์และตรวจสอบ Protocol เกี่ยวกับ Authentication อันได้แก่ NTLM, Radius, Kerberos

3.3 สามารถวิเคราะห์และตรวจสอบการสื่อสารลักษณะ Remote Access อันได้แก่ RDP และ VNC

3.4 สามารถวิเคราะห์และตรวจสอบ Protocol เกี่ยวกับ VPN อันได้แก่ SSH, OpenVPN และ WireGuard

3.5 สามารถวิเคราะห์และตรวจสอบ Protocol เกี่ยวกับการแชร์ไฟล์ในองค์กร อันได้แก่ SMB, FTP, Webdev

3.6 สามารถวิเคราะห์ Protocol จากระบบ OT (Operation Technology) อันได้แก่ Modbus, DNP3, BACNET, S7comm, COTP เป็นต้น

Live Network Log CONNECTION

ts	uid	id.orig_h	id.orig_p	id.resp_h	id.resp_p	proto	service	duration	orig_bytes	resp_bytes	conn_state	local_orig
2025-06-29 18:15:56	CETUbM3vGz1JCMGOn2	192.168.1.205	6654	35.223.142.206	8090	tcp	-	0.463807	0	0	SF	T
2025-06-29 18:15:55	CdN0Rp2Pw8NPSQ7x0l	192.168.1.205	47774	198.128.151.20	8096	tcp	http	0.781118	111	333	SF	T
2025-06-29 18:15:51	CvQhfS3lZaHn9qypE6	192.168.1.12	62988	192.168.1.1	33434	tcp	-	0.000036	0	0	REJ	T
2025-06-29 18:15:46	C3gT9k6WECm14Qv04	192.168.1.12	60296	18.172.4.54	443	tcp	-	0.010350	0	0	SF	T
2025-06-29 18:15:42	CD2kn34qGkOGQalvyl	192.168.1.51	52578	192.168.1.251	443	tcp	ssl	0.191667	2878	408	SF	T
2025-06-29 18:15:42	CAUQWM1SEZLS2McDf	192.168.1.51	52577	192.168.1.251	443	tcp	ssl	0.182616	2878	408	SF	T
2025-06-29 18:15:41	CdZUBs1C9e5mqFb5v5	192.168.1.51	52575	192.168.1.254	443	tcp	ssl	0.117185	2066	234	SF	T
2025-06-29 18:15:31	C5d1xtP7skMb1GmR7	192.168.1.73	50818	54.92.89.142	443	tcp	ssl	7.382614	5349	4939	SF	T
2025-06-29 18:15:31	CdcieM2gz5YrvGDyea	192.168.1.73	36593	192.168.1.1	53	udp	dns	0.000572	94	168	SF	T
2025-06-29 18:15:31	CPaZCt3cHL1K6LT0ab	192.168.1.73	58780	192.168.1.1	53	udp	dns	0.003872	94	72	SF	T
2025-06-29 18:15:25	CK5NxR2gnBTnSki3X	192.168.1.21	52622	192.168.1.1	53	udp	dns	0.005118	78	216	SF	T
2025-06-29 18:15:25	CMeVob2BbXgyGZi7z5	192.168.1.147	19386	192.168.1.1	53	udp	dns	0.003777	66	98	SF	T
2025-06-29 18:15:25	CeIhUs3a50Slpl1UT7	192.168.1.147	25669	192.168.1.1	53	udp	dns	0.004053	86	118	SF	T

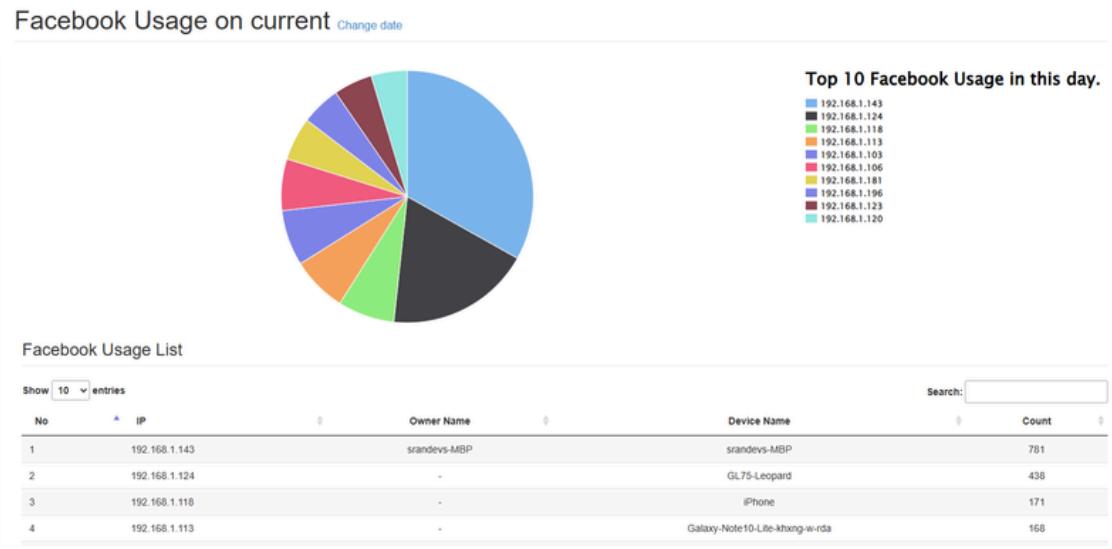
ภาพรายงานการวิเคราะห์และตรวจสอบข้อมูลตามประเภท Protocol

4. การเฝ้าติดตามปริมาณการใช้งานข้อมูลภายในองค์กร (Bandwidth Monitoring)

4.1 Protocol and Service Monitoring จะสามารถคำนวณค่าปริมาณ Bandwidth ที่เกิดขึ้นบนระบบเครือข่ายได้โดยแยก Protocol TCP, UDP, ICMP และ Service ตาม Well Know Port Service ทำให้ทราบถึงปริมาณการใช้งานข้อมูลได้อย่างละเอียด และประเมินสถานการณ์ได้อย่างแม่นยำ

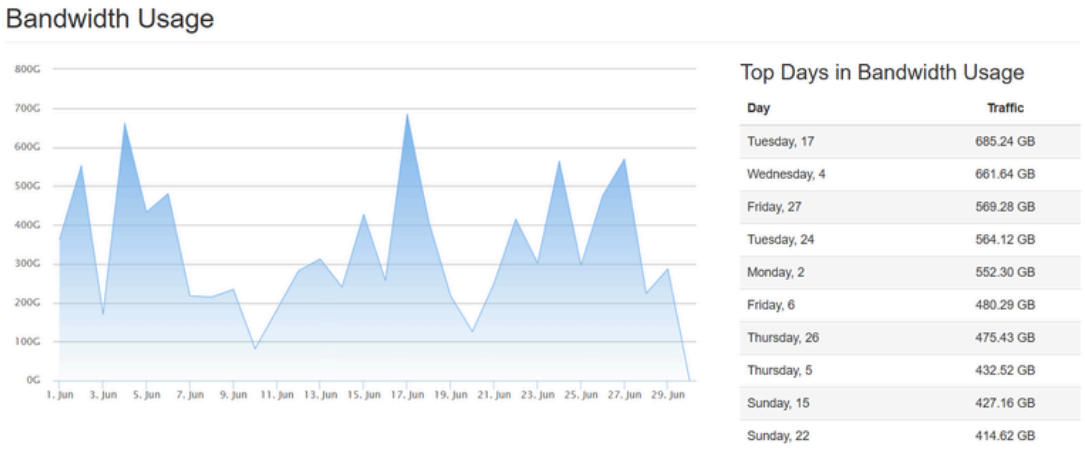
4.2 Application Monitoring รายงานการใช้แอปพลิเคชั่น และปริมาณการใช้ข้อมูลภายในองค์กร

4.3 Social Network Monitoring รายงานการใช้งานเครือข่ายสังคมออนไลน์เพื่อให้รู้ถึงปริมาณข้อมูลที่ใช้ภายในองค์กร ได้แก่ Facebook, Line, YouTube, Google Video, Twitter และ Pantip ทำให้ผู้บริหารองค์กรสามารถทราบความเคลื่อนไหว และการใช้ปริมาณข้อมูลภายในองค์กร



ภาพ Facebook Monitoring ทำให้ทราบถึงการใช้ปริมาณการใช้งานข้อมูลเครือข่ายสังคมออนไลน์

4.4 User Monitoring รายงานและจัดอันดับการใช้งาน Bandwidth ภายในองค์กร โดยจะเห็นรายชื่อผู้ใช้จากคุณสมบัติข้อ 1 ทำให้เราทราบถึงชื่อผู้ใช้งาน และค่า Bandwidth ที่สูงสุด และทำรายงานได้



รายงานปริมาณการใช้งาน Bandwidth ภายในองค์กร

5.การค้นหาข้อมูลและออกรายงาน

5.1 สามารถแบ่งประเภทการค้นหาโดยเลือกตาม Protocol Web Access, Files Access, Network Connection, SSL, Mail, Database, Syslog, VoIP, Remote Desktop, Radius และ Active Directory ซึ่งสามารถค้นหา Raw Log ที่เกิดขึ้น ทั้งแบบปัจจุบัน และย้อนหลังได้ไม่น้อยกว่า 90 วัน

5.2 การค้นหารวดเร็ว และสามารถใช้เงื่อนไขในการค้นหา เช่น AND, OR, NOT เข้ามาเกี่ยวข้อง เพื่อให้การค้นเป็นไปอย่างมีประสิทธิภาพ

5.3 สามารถออกรายงานจากผลการค้นหาได้ สามารถออกรายงาน และตั้งค่าเป็นแบบ Line, Bar, Pie, Doughnut, Polar Area และออกรายงานเป็น CSV, Excel, PDF ได้

6. การเก็บบันทึกข้อมูลจราจรคอมพิวเตอร์และดูย้อนหลัง (Log Record and Archive)

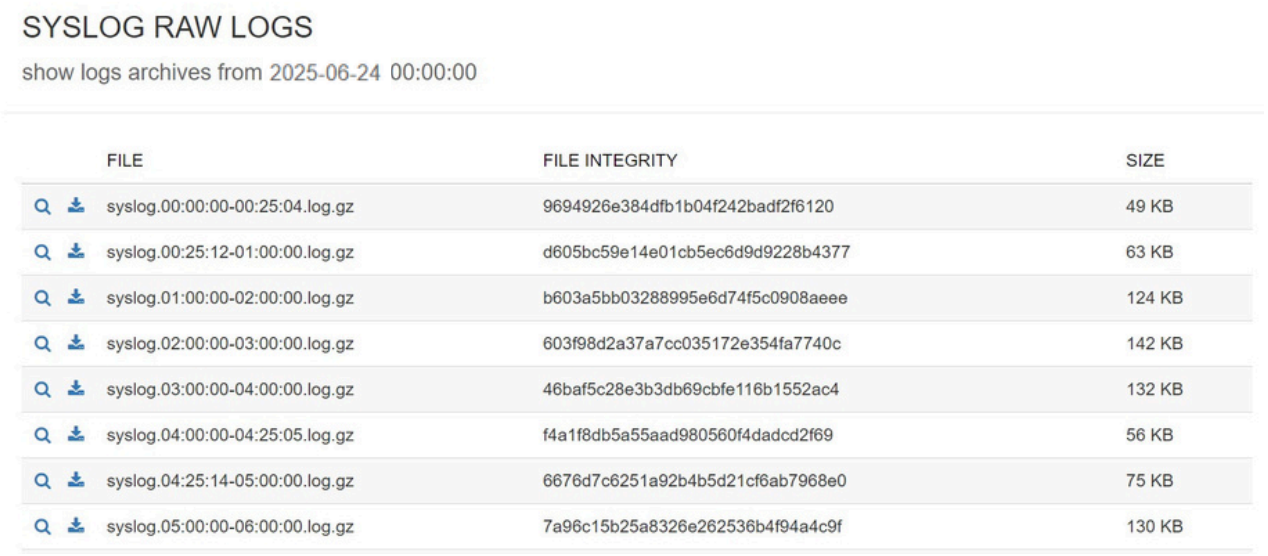
6.1 การเก็บบันทึกข้อมูลจราจรคอมพิวเตอร์ พร้อมยืนยันความถูกต้องของข้อมูลและการรักษาความปลอดภัยจากการจัดเก็บข้อมูลจราจรคอมพิวเตอร์

6.2 รองรับค่า Log จาก Active Directory, Router / Firewall/VPN, Mail Server (Exchange, Lotus Notes), DHCP, DNS, SNMP, Radius Wi-Fi Controller และทำการแยกแยะค่าการเก็บ Log โดยแบ่งเป็นหมวดให้โดยอัตโนมัติรองรับการเก็บบันทึกข้อมูลจราจรคอมพิวเตอร์ที่เกี่ยวข้องกับ Protocol ที่ใช้กับอุปกรณ์สื่อสารในโรงงานอุตสาหกรรม ประเภท Modern SCADA System รองรับ Protocol DNP3, Modbus เป็นต้น

6.3 มีความสามารถในการ Export Data เพื่อใช้ในการพิสูจน์หาหลักฐานได้

6.4 การเก็บบันทึกข้อมูลมีการยืนยันความถูกต้องข้อมูล Integrity Hashing

6.5 การเก็บบันทึกข้อมูลสามารถเก็บได้ตามที่กฎหมายกำหนด โดยมีซอฟต์แวร์ SRAN Module Logger ที่ผ่านมาตรฐาน NECTEC มศอ. ๔๐๐๓.๑ – ๒๕๖๐ (NECTEC STANDARD NTS 4003.1-2560)

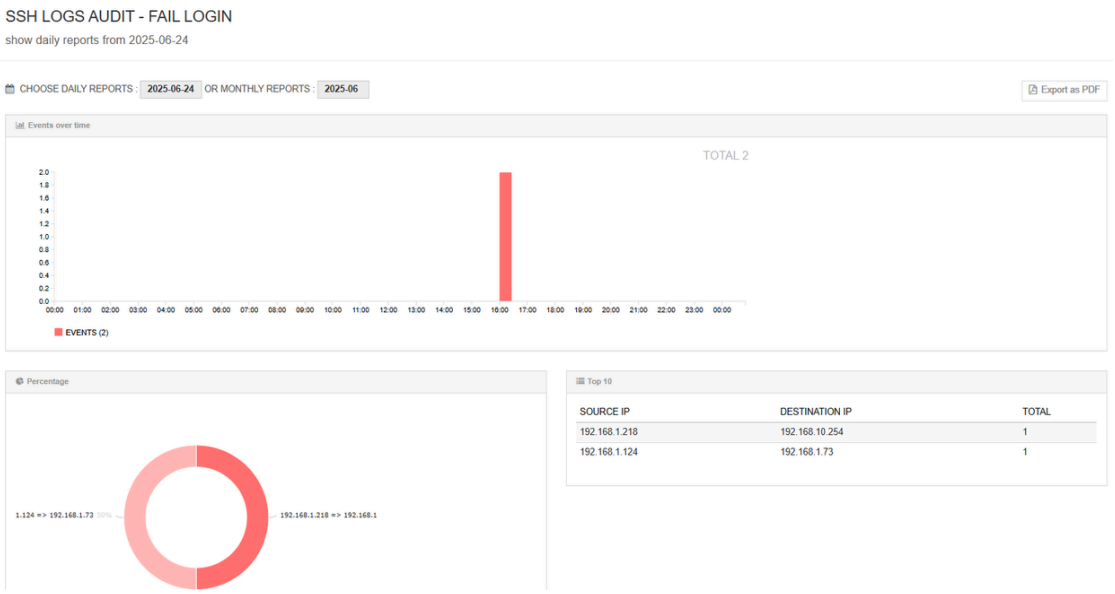


ภาพการเก็บบันทึกข้อมูลจาก Syslog มีการทำ File Integrity เพื่อยืนยันความถูกต้องของข้อมูล
(ผู้ที่เข้าถึงไฟล์ได้ต้องเป็นระดับ Data Keeper ที่องค์กรได้มอบหมายรับผิดชอบในส่วนนี้)

7. การเก็บบันทึกค่าสำหรับให้ IT Audit ในการตรวจสอบข้อมูลและใช้เป็นหลักฐาน (Log Audit)

7.1 การเก็บบันทึกค่า Active Directory Login Success / Login Fail

7.2 การเก็บบันทึกค่า SSH Login Success / Login Fail



รายงานการ Login ผิดพลาดที่เกิดขึ้น

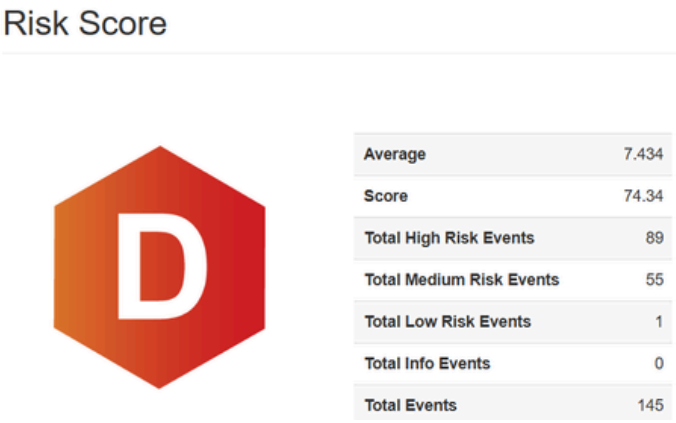
7.3 Files Audit มีความสามารถในการตรวจสอบการแก้ไขไฟล์ผ่าน Protocol การแชร์ไฟล์ ซึ่งสามารถทำให้รู้ถึงการแก้ไขไฟล์ (Modify) หรือแก้ไขชื่อ (Rename) การเปิดไฟล์ (Open Files) และการลบไฟล์ (Delete Files) โดยไม่ต้องลงซอฟต์แวร์อื่นเสริม

7.4 Login Audit มีความสามารถในการตรวจสอบการ Login เข้าสู่ระบบว่ามีการ Login ผิด Login ถูก และออกรายงานผลการ Login ของผู้ใช้งานได้

8. การเฝ้าระวังและประเมินความเสี่ยงและผลกระทบด้านไซเบอร์ (Vulnerability Assessment)

8.1 สามารถทำการวิเคราะห์ข้อมูลจากการรวบรวมเหตุการณ์ภัยคุกคามที่เกิดขึ้นภายในระบบเครือข่ายคอมพิวเตอร์ขององค์กร โดยแบ่งระดับความเสี่ยงสูง กลาง และต่ำได้

8.2 สามารถออกผลการประเมินความเสี่ยงเป็นแบบ Score คะแนน และเป็นเกรดการให้คะแนนของระบบที่ประเมินความเสี่ยงได้เป็นเกรด A ถึง F ทำให้ทราบถึงภาพรวมของภัยคุกคามในองค์กร ได้อย่างทันท่วงที



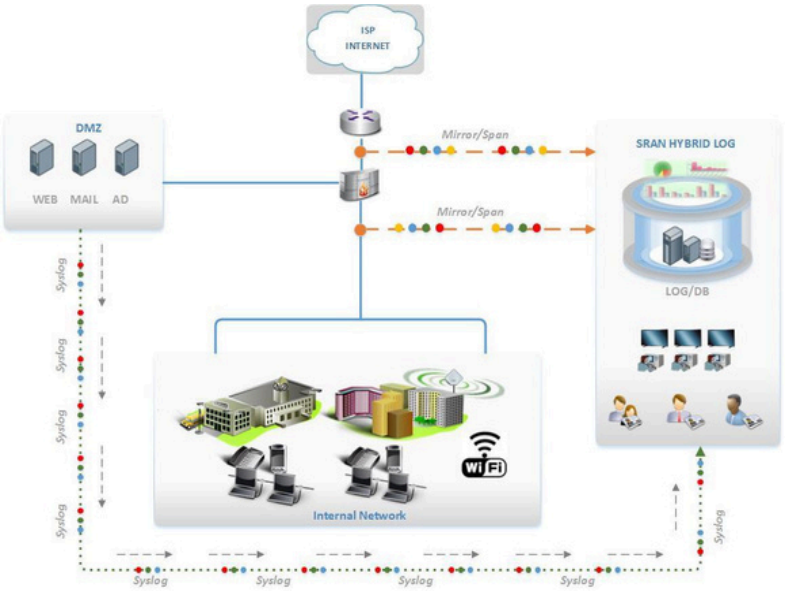
ภาพผลการประเมินความเสี่ยง (Risk Score)

8.3 ทำการประเมินความเสี่ยงแบบต่อเนื่องโดยใช้เทคนิค Passive Vulnerability Assessment และสามารถตรวจสอบดูผลการประเมินความเสี่ยงย้อนหลังได้

8.4 เมื่อพบระดับความเสี่ยงสูง สามารถตั้งค่า Alert เพื่อแจ้งเตือนผ่าน Line ได้

คุณสมบัติเพิ่มเติมของ SRAN NetApprove

1. เป็นอุปกรณ์ Appliance ที่ได้รับการปรับปรุง Firmware เพื่อปิดช่องโหว่ (Hardened) เป็นที่เรียบร้อยแล้ว หรืออุปกรณ์คอมพิวเตอร์ที่ได้มาตรฐาน สามารถเก็บรวบรวมเหตุการณ์ (Logs or Events) ที่เกิดขึ้นในอุปกรณ์ที่เป็น Appliances และ Non-Appliances เช่น Firewall, Network Devices ต่าง ๆ ระบบปฏิบัติการ ระบบ Appliances ระบบเครือข่าย และระบบฐานข้อมูล เป็นต้น ได้อย่างน้อย 3, 10, 15 อุปกรณ์ต่อระบบ โดยสามารถแสดงผลอยู่ภายใต้รูปแบบ (Format) เดียวกันได้
2. มีระบบการเข้ารหัสข้อมูลเพื่อใช้ยืนยันความถูกต้องของข้อมูลที่จัดเก็บตามมาตรฐาน SHA-256
3. สามารถเก็บ Log File ในรูปแบบ Syslog ของอุปกรณ์ เช่น Router, Switch, Firewall, VPN, Server ได้
4. สามารถบริหารจัดการอุปกรณ์ผ่านมาตรฐาน HTTPS, Command Line Interface และ SSH ได้
5. สามารถกำหนดสิทธิ์ในการเข้าถึงข้อมูล Role Based Access Control ได้
6. สามารถจัดเก็บ Log File ได้ถูกต้อง ตรงตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ ฉบับที่มีผลบังคับใช้ โดยได้รับรองมาตรฐานการจัดเก็บและรักษาความปลอดภัยของ Log File ที่ได้มาตรฐานของศูนย์อิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (มศอ. 4003.1-2560)
7. สามารถทำการสำรองข้อมูล (Data Backup) ไปยังอุปกรณ์จัดเก็บข้อมูลภายนอก เช่น Tape หรือ DVD หรือ External Storage เป็นต้นได้



ภาพแสดงการออกแบบเป็นระบบ Hybrid ที่สามารถรับค่า Log จาก Syslog ได้

SRAN
IT Security Next Generation

SPECIFICATIONS

Model	NG50	NG100	NG200
Capacity and Performance			
Normal Log Rate (Event/Second) ***	1,000	10,000	20,000
Feature			
1. Automatic Identification Device - Know Device/Unknown Device - Approve device/Rogue Detection - BYOD: Desktop/Mobile - Inventory: Device	✓	✓	✓
2. Detection - Attack Detection (Brute Force, Exploit) - Malware/Virus Detection - Detect Software - Bittorrent Detection - Tor/Proxy Detection	✓	✓	✓
3. Log Analysis: Security Information Event Management - Threat Analysis - Risk Analyzer (High, Medium, Low)	✓	✓	✓
4. Bandwidth Monitoring - Protocol and Bandwidth Usage - Application Monitoring (Software Bandwidth Usage) - Social Network Monitoring (Facebook, Line, Youtube, Pantip) - User Monitoring	✓	✓	✓
5. Deep Search - Network Forensic Evident Data - Conditional Search	✓	✓	✓
6. Log Archive - Raw Full Data - Export Data - Integrity Hashing	✓	✓	✓
7. Log Auditor - Active Directory Login Success/Login Fail, SSH Login Success/Login Fail	✓	✓	✓
8. Report - Executive Summary - Compliance Thai Cyber Law Log Correlation Report - HTTP/SSL Analyzer	✓	✓	✓
Hardware Specification			
CPU***	Quad Core	Quad Core	12 Core
Memory***	8 GB	32 GB	64 GB
Network***	4 Port (10/100/1000)	4 Port (10/100/1000)	4 Port (10/100/1000)
Storage Capacity***	1 TB	1 TB	2x1.92 TB
Log Capacity***	~800 GB	~800 GB	~1.8 TB
Raid Support	-	-	Raid 1/5/10
Default Raid***	-	-	1
HDD (Hot Swap)	-	-	Yes
Hot Swap Power Supply	-	-	Yes
Device License			
Mirror Mode	Unlimited	Unlimited	Unlimited
Syslog Mode	Unlimited	Unlimited	Unlimited
Recommendation			
Dual Mode (Mirror/Syslog) **	~50 Client / 5 Device	~100 Client / 10 Device	~200 Client / 15 Device

**กรณีติดตั้งเพื่อจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ทั้ง 2 รูปแบบ (Mirror/Syslog) ในขณะเดียวกัน

***สามารถรองรับการปรับแต่งอุปกรณ์ได้

บริษัท โกลบอลเทคโนโลยี อินทิเกรเทด จำกัด 48/6 ซอยแจ้งวัฒนะ 14 ทุ่งสองห้อง หลักสี่ กรุงเทพฯ 10210
โทรศัพท์ : +66 2 982 5454 โทรสาร: +66 2 982 4004 อีเมล์: info@gbtech.co.th