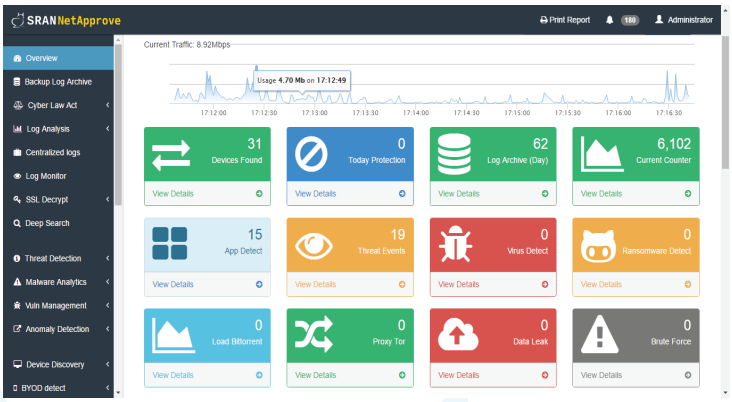
SRAN
IT Security Next Generation

Net Approve

"กว่า 20 ปี SRAN ประสบการณ์ที่กลั่นกรองมาเป็นผลิตภัณฑ์การจัดเก็บบันทึกข้อมูลคอมพิวเตอร์ ที่คุ้มค่าที่สุด สำหรับผู้ใช้งาน" NetApprove เกิดจากการพัฒนาวิจัยอย่างต่อเนื่อง โดยนำสิ่งที่คิดว่าเป็นประโยชน์สูงสุดสำหรับผู้ใช้งานบนนิยามว่า "Advance Centralized Log Management" เพราะเราเชื่อว่าการมองเห็นเป็นสิ่งสำคัญ มันจะทำให้เราประเมินสถานการณ์ต่างๆได้

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

SRAN NetApprove คือ Full Functional Network Security and Logging Report โดยมีคุณสมบัติ



ภาพรวมสถานการณ์ข้อมูลที่เกิดขึ้นบนเครือข่ายองค์กร

1. การสำรวจข้อมูล แบบอัตโนมัติเพื่อระบุตัวตนอุปกรณ์บนระบบเครือข่ายคอมพิวเตอร์ (Automatic Identification Device) การค้นหาอุปกรณ์บนระบบเครือข่ายอย่างอัตโนมัติ เพื่อระบุตัวตนผู้ใช้งาน โดยไม่ต้องปรับค่าอื่นใดในอุปกรณ์ก็สามารถทำการค้นหาอุปกรณ์ที่อยู่บนระบบเครือข่ายคอมพิวเตอร์ได้

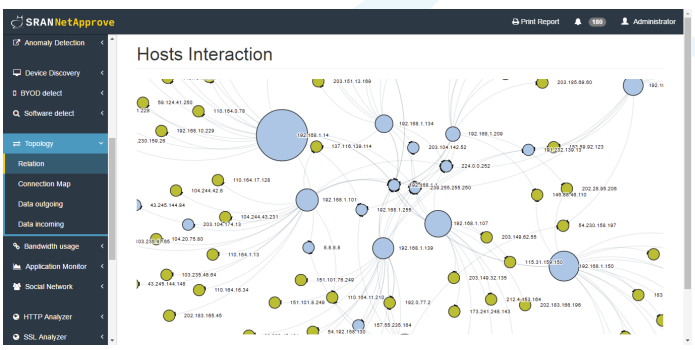
1.1 รายงานการคัดแยกเครื่องที่รู้จัก (Known Device) และไม่รู้จัก (Unknown Device) ได้โดยการยืนยัน (Approve) เป็นที่มาของชื่อ “SRAN NetApprove” เมื่อทำการยืนยันค่าแล้วหากมีอุปกรณ์แปลกปลอมเข้าสู่ระบบเครือข่ายก็สามารถตรวจพบได้ (Rouge Detection)

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) จะทำการค้นพบประเภทซอฟต์แวร์ที่ใช้ได้แก่ ซอฟต์แวร์ประเภทเว็บบราวเซอร์, ซอฟต์แวร์ประเภทมัลติมีเดีย, ซอฟต์แวร์ประเภทใช้งานในออฟฟิศ และซอฟต์แวร์ที่ไม่เหมาะสม เช่น โปรแกรม Bittorrent ก็สามารถตรวจและค้นพบได้

1.5 การวาดรูปความเชื่อมโยงระบบเครือข่าย (Topology) สร้างภาพเสมือนบนระบบเครือข่ายเป็น Network Topology แบบ Link Chart ในการติดต่อสื่อสาร (Interconnection)



ภาพการแสดงผลการเชื่อมต่อข้อมูลบนระบบเครือข่าย

2. การวิเคราะห์และเทคโนโลยีในการตรวจจับความผิดปกติข้อมูล (Detectand Analyzer) ประกอบด้วย

2.1 Attack Detection รายงานการตรวจจับพฤติกรรมการโจมตีระบบ ได้แก่ การ Brute Force รหัสผ่านที่เกิดขึ้นบนตัวอุปกรณ์ และเครื่องแม่ข่ายที่สำคัญ เช่น Active Directory, Web Server, Mail Server เป็นต้น อีกทั้งยังสามารถตรวจพบการโจมตีโดยการยิง Exploit เข้าสู่เครื่องแม่ข่ายที่สำคัญ เป็นต้น

2.2 Malware/Virus Detection รายงานการตรวจจับมัลแวร์ / ไวรัสคอมพิวเตอร์ที่เกิดขึ้นบนระบบเครือข่าย สามารถทำการตรวจจับได้โดยไม่ต้องอาศัยการลงซอฟต์แวร์ที่เครื่องลูกข่าย (Client) แต่ท าการตรวจผ่านการรับส่งค่าที่เกิดขึ้นบนระบบเครือข่ายคอมพิวเตอร์

2.3 Bittorrent Detection รายงานการตรวจจับการใช้งานโปรแกรมดาวน์โหลดไฟล์ขนาดใหญ่ที่ส่งผลกระทบต่อการใช้งานภาพรวมภายในองค์กร

2.4 Tor/Proxy Detection รายงานการตรวจจับซอฟต์แวร์ประเภทอำพรางการสื่อสารเพื่อใช้หลบเลี่ยงการตรวจจับข้อมูลภายในระบบเครือข่ายคอมพิวเตอร์

2.5 HTTP / SSL Analyzer รายงานการตรวจวิเคราะห์การใช้งานเว็บไซต์พร้อมจัดทำสถิติการใช้งานอินเทอร์เน็ตภายในองค์กร์

3. การวิเคราะห์ข้อมูลจาก Log (Log Analytic)

3.1 Threat Analyze รายงานการวิเคราะห์ข้อมูลจากการรวบรวมเหตุการณ์ภัยคุกคามที่เกิดขึ้นภายในระบบเครือข่ายคอมพิวเตอร์ขององค์กร

3.2 Risk Analyzer (High, Medium, Low) รายงานการวิเคราะห์ระดับเหตุการณ์ความเสี่ยงระดับสูง ความเสี่ยงระดับกลาง และความเสี่ยงระดับต่ำเพื่อแสดงค่าและการจัดทำรายงาน

รายงานความเสี่ยงที่เกิดขึ้นภายในองค์กรที่สามารถออกรายงานได้ รายชั่วโมง รายวัน และรายเดือน

SRAN
IT Security Next Generation

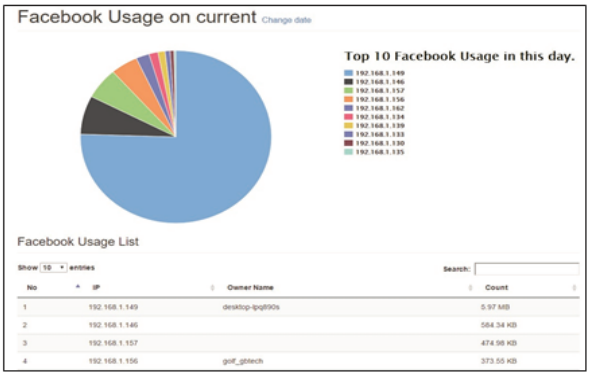
Net Approve

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

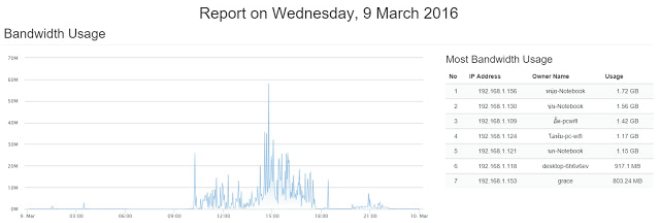
4.2 Application Monitoring รายงานการใช้แอปพลิเคชั่น และปริมาณการใช้ข้อมูลภายในองค์กร

4.3 Social Network Monitoring รายงานการใช้งานเครือข่ายสังคมออนไลน์เพื่อให้รู้ถึงปริมาณข้อมูลที่ใช้ภายในองค์กร ได้แก่Facebook, Line, YouTube, Google Video, Twitter และ Pantip ทำให้ผู้บริหารองค์กรสามารถทราบความเคลื่อนไหวและการใช้ปริมาณข้อมูลภายในองค์กร



ภาพ Facebook Monitoring ทำให้ทราบถึงการใช้ปริมาณการใช้งานข้อมูลเครือข่ายสังคมออนไลน์

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



รายงานปริมาณการใช้งาน Bandwidth ภายในองค์กร

5.การค้นหาข้อมูลในเชิงลึก (Deep Search)

5.1 การพิสูจน์หลักฐานทางข้อมูลสารสนเทศ (Network Forensic Evidence Data) ค้นหาเหตุการณ์ที่เกิดขึ้น โดยแบ่งตามเนื้อหา (Content Search) ดังนี้ Web Access, Files Access, Network Connection, SSL, Mail, Database, Syslog, VoIP, Remote Desktop, Radius และ Active Directory ซึ่งสามารถค้นหา Raw Log ที่เกิดขึ้น ทั้งแบบปัจจุบัน และย้อนหลังได้

5.2 การค้นหารวดเร็ว และสามารถใช้เงื่อนไขในการค้นหา เช่น AND, OR, NOT เข้ามาเกี่ยวข้อง เพื่อให้การค้นเป็นไปอย่างมีประสิทธิภาพ

6. การเก็บบันทึกข้อมูลจราจรคอมพิวเตอร์และดูย้อนหลัง (Log Record and Archive)

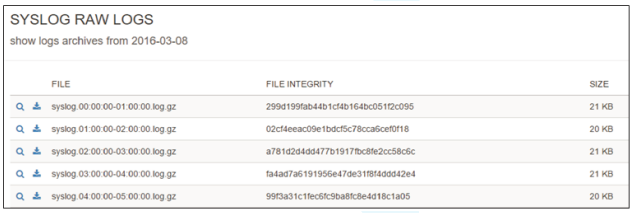
6.1 การเก็บบันทึกข้อมูลแบบ Raw Full Data เพื่อเป็นประโยชน์ในการสืบสวนสอบสวน และการหาผู้กระทำความผิด ด้วยการเก็บบันทึกที่สามารถทำได้แบบ Hybrid ซึ่ง SRAN NetApprove เป็นต้นฉบับของการทำวิธีนี้ คือ การรับข้อมูลจราจรคอมพิวเตอร์แบบ Passive modeและรับค่าจากอุปกรณ์อื่นได้ (Syslog)

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 (Modicon Communication Bus) 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

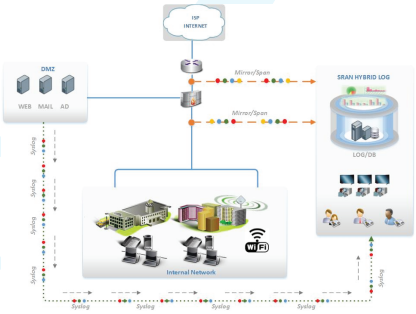
7.3 Files Audit มีความสามารถในการตรวจสอบการแก้ไขไฟล์ผ่าน Protocol การแชร์ไฟล์ ซึ่งสามารถทำให้รู้ถึงการแก้ไขไฟล์ (Modify) หรือแก้ไขชื่อ (Rename) การเปิดไฟล์ (Open Files) และการลบไฟล์ (Delete Files) โดยไม่ต้องลงซอฟต์แวร์อื่นเสริม

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

8. การออกรายงาน (Report)

8.1 Executive Summary รายงานสรุปสถานการณ์ทั้งหมดสำหรับผู้บริหาร

8.2 รองรับกฎหมายประเทศไทย ทั้งกฎหมายคุ้มครองข้อมูลส่วนบุคคล พ.ร.บ ความมั่นคงปลอดภัยทางไซเบอร์ ฯ และ กฎหมาย พ.ร.บ ว่าด้วยการกระทำความผิดทางคอมพิวเตอร์



ภาพแสดงการออกแบบเป็นระบบ Hybrid ที่สามารถรับค่า Log จาก Syslog ได้

GLOBAL TECH www.gbtech.co.th SGS UKAS FC CE UL RoHS

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