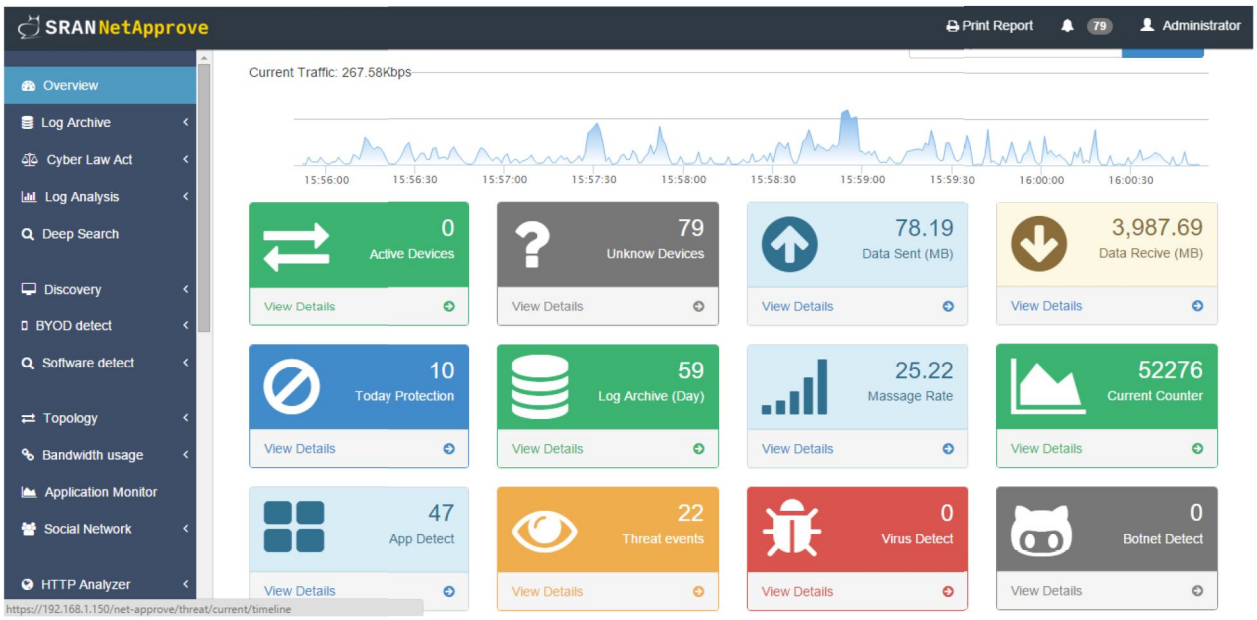
"กว่า 15 ปี SRAN ประสบการณ์ที่กลั่นกรองมาเป็นผลิตภัณฑ์การจัดเก็บบันทึกข้อมูลคอมพิวเตอร์ ที่คุ้มค่าที่สุด สำหรับผู้ใช้งาน" NetApprove เกิดจากการพัฒนาวิจัยอย่างต่อเนื่อง ยาวนานกว่า 2 ปี โดยนำสิ่งที่คิดว่าเป็นประโยชน์สูงสุดสำหรับผู้ใช้งาน บนนิยามว่า "Advance Centralized Log Management" เพราะเราเชื่อว่าการมองเห็นเป็นสิ่งสำคัญ มันจะทำให้เราประเมินสถานการณ์ต่างๆได้

ทำงานแบบ System 4 " ระบบสี่ประสาน (1) ระหว่างการเก็บ Log ที่เกิดจากระบบเครือข่าย (Network Log) (2) Log ที่มาจากอุปกรณ์และเครื่องแม่ข่ายที่สำคัญ (syslog) และ (3) การเก็บ Log ที่แกะค่า HTTPS ได้ (4) การเก็บบันทึกค่า Inventory ของเครื่องคอมพิวเตอร์ ทั้ง 4 ส่วนรวมเป็น 1 เดียวใน SRAN NetApprove



ภาพรวมสถานการณ์ข้อมูลที่เกิดขึ้นบนเครือข่ายองค์กร

บนหน้าจอของ SRAN NetApprove เพียงหน้าเดียวก็ทำให้ทราบถึงเหตุการณ์และสถานการณ์ปัจจุบันที่เกิดขึ้น ทุกหน้าการแสดงผลกว่า 100 เมนูการแสดงผล ใน SRAN NetApprove สามารถปริ้นเป็นรายงานเพื่อผู้บริหารได้ (Print to PDF Report) รองรับค่าการแสดงผลผ่าน Web GUI และการออกแบบ Responsive Web Design ที่สามารถใช้งานได้ทั้งบนเครื่องคอมพิวเตอร์ และ มือถือ

SRAN NetApprove คือการให้แบบ Full Functional Network Security and Logging Report โดยมีคุณสมบัติ

1. การสำรวจข้อมูลแบบอัตโนมัติเพื่อระบุตัวตนอุปกรณ์บนระบบเครือข่ายคอมพิวเตอร์ (Automatic Identification Device)

การค้นหาอุปกรณ์บนระบบเครือข่ายอย่างอัตโนมัติ เพื่อระบุตัวตนผู้ใช้งาน โดยไม่ต้องปรับค่าอื่นใดในอุปกรณ์ก็สามารถทำการค้นหาอุปกรณ์ที่อยู่บนระบบเครือข่ายคอมพิวเตอร์ได้

1.1 รายงานการคัดแยกเครื่องที่รู้จัก (Known Device) และ ไม่รู้จัก (Unknown Device) ได้โดยการยืนยัน (Approve) เป็นที่มาของชื่อ "NetApprove" เมื่อทำการยืนยันค่าแล้วหากมีอุปกรณ์แปลกปลอมเข้าสู่ระบบเครือข่ายก็สามารถตรวจพบได้ (Rouge Detection)

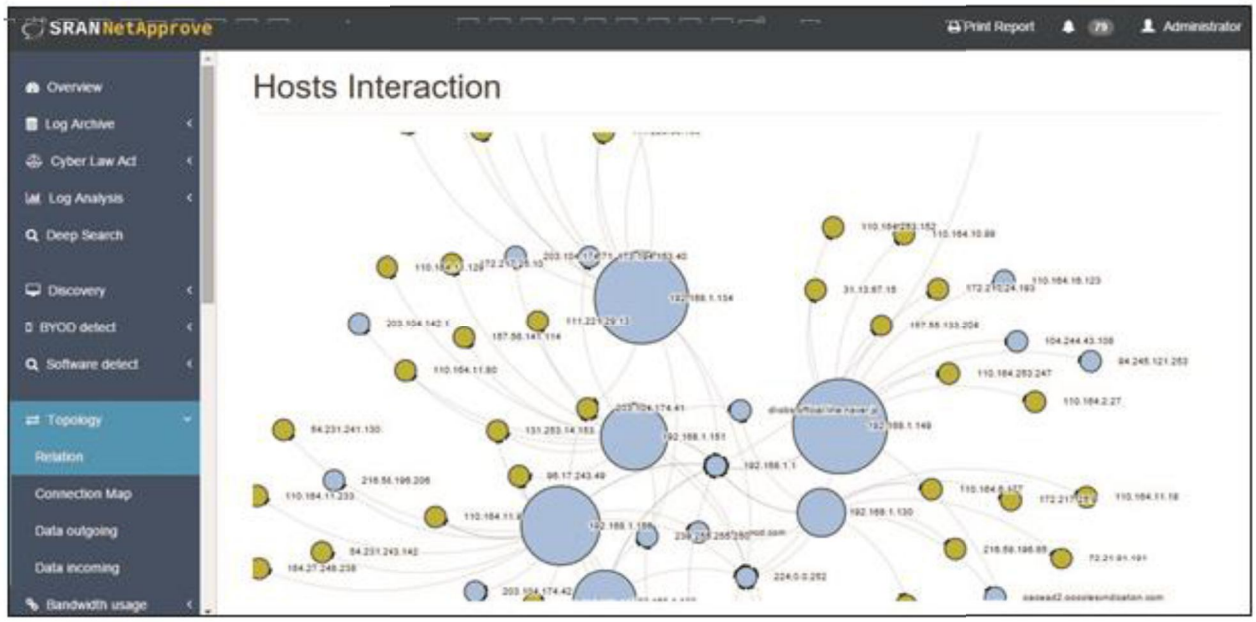
1.2 รายงาน BYOD (Bring Your Own Device) แสดงค่าอุปกรณ์พกพาที่เข้าสู่เครือข่ายคอมพิวเตอร์ขององค์กรได้โดยแยก Desktop (คอมพิวเตอร์พกพา เช่นโน้ตบุ๊ก) และมือถือ (Mobile) และรู้ว่าใครนำเครื่องพกพามาใช้งานภายในเครือข่ายองค์กร

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) ที่ใช้ซึ่งในส่วนซอฟต์แวร์จะทำการค้นพบประเภทซอฟต์แวร์ที่ใช้ได้แก่ ซอฟต์แวร์ประเภทเว็บบราวเซอร์ , ซอฟต์แวร์ประเภทมัลติมีเดีย , ซอฟต์แวร์ประเภทใช้งานในออฟฟิศ ซอฟต์แวร์ที่ไม่เหมาะสมเช่น โปรแกรม Bittorrent ก็สามารถตรวจและค้นพบได้

1.5 การวาดรูปความเชื่อมโยงระบบเครือข่าย (Topology) สร้างภาพเสมือนบนระบบเครือข่ายเป็น Network topology แบบ link chart ในการติดต่อสื่อสาร (Interconnection)

1.6 การสำรวจเครื่องที่มีโอกาสเปลี่ยนค่า Leak path เชื่อมต่อกับ gateway อื่นที่ไม่ใช่ขององค์กร



ภาพการแสดงผลการเชื่อมต่อข้อมูลบนระบบเครือข่าย

2. การวิเคราะห์และเทคโนโลยีในการตรวจจับความผิดปกติข้อมูล (Detect and Analyzer) ประกอบด้วย

2.1 Attack Detection รายงานการตรวจจับการโจมตี ที่เป็นพฤติกรรมที่ชัดเจนว่าทำการโจมตีระบบ ได้แก่การ 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) แต่ทำการตรวจผ่านการรับส่งค่าที่เกิดขึ้นบนระบบเครือข่ายคอมพิวเตอร์

2.3 Botnet Detection รายงานการตรวจบอทเน็ตภายในองค์กร และการโจมตีบอทเน็ตเข้าสู่ระบบเครือข่ายคอมพิวเตอร์ภายในองค์กร

2.4 Behavior Data Leak Detection รายงานการตรวจจับพฤติกรรมของพนักงานที่มีโอกาสสุ่มเสี่ยงในการลักลอบข้อมูลออกนอกบริษัท

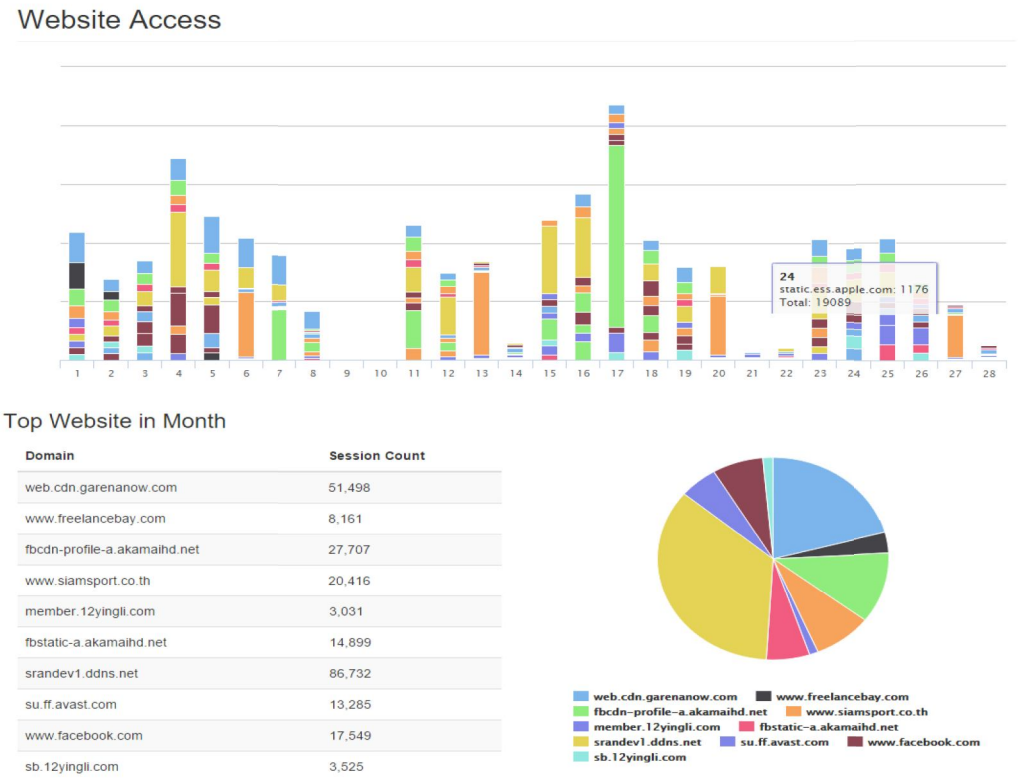
2.5 Bittorrent Detection รายงานการตรวจจับการใช้งานโปรแกรมดาวโหลดไฟล์ขนาดใหญ่ที่ส่งผลกระทบต่อการใช้งานภายรวมภายในองค์กร

2.6 Anomaly Detection รายงานการตรวจจับภัยคุกคามที่มีความผิดปกติในการติดต่อสื่อสาร

2.7 Tor/Proxy Detection รายงานการตรวจจับซอฟต์แวร์ประเภทอำพรางการสื่อสารเพื่อใช้หลบเลี่ยงการตรวจจับข้อมูลภายในระบบเครือข่ายคอมพิวเตอร์

2.8 HTTP / SSL Analyzer รายงานการตรวจวิเคราะห์การใช้งานเว็บไซต์พร้อมจัดทำสถิติการใช้งานอินเทอร์เน็ตภายในองค์กร

2.9 APT (Advanced Persistent Threat) Detection รายงานการตรวจพฤติกรรมที่มีโอกาสเป็นภัยคุกคามประเภท APT และมีความเสี่ยงต่อองค์กร



รายงานผลการใช้งานอินเทอร์เน็ตภายในองค์กร

3. การวิเคราะห์ข้อมูลจาก Log (Log Analytic)

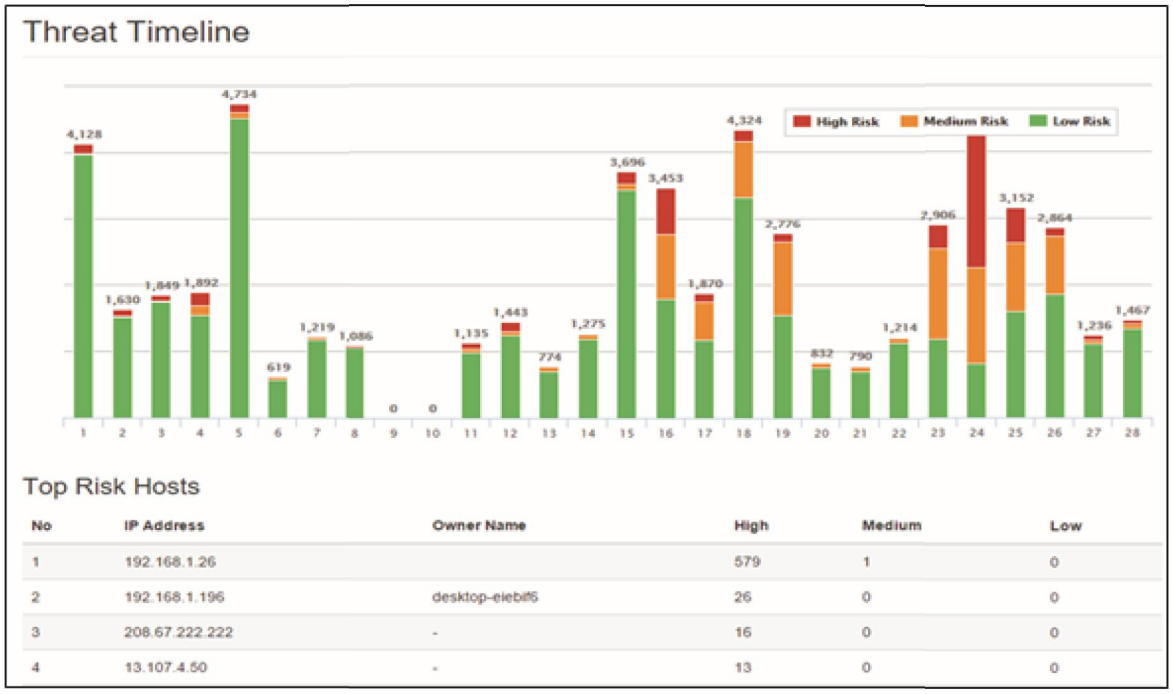
3.1 Threat event correlation รายงานการวิเคราะห์ข้อมูลจากการรวบรวมเหตุการณ์ภัยคุกคามที่เกิดขึ้นภายในระบบเครือข่ายคอมพิวเตอร์องค์กร

3.2 Risk score รายงานการวิเคราะห์ความเสี่ยงเพื่อสร้างเป็นดัชนีชี้วัด (Indicator of Compromise) ภัยคุกคามภายในองค์กร

3.3 Risk Analyzer (High , Medium , Low) รายงานการวิเคราะห์ระดับเหตุการณ์ความเสี่ยงระดับสูง ความเสี่ยงระดับกลางและความเสี่ยงระดับต่ำ เพื่อแสดงค่าและการจัดทำรายงาน

3.4 Executive summary (Hour , Daily , Monthly) รายงานการจัดสรุปสถานการณ์ทั้งหมดให้ระดับผู้บริหารองค์กร โดยกำหนดได้ที่เป็นรายชั่วโมง รายวัน และรายเดือน

3.5 Thai Cyber Law Act รายงานความเสี่ยงที่มีโอกาสเข้าข่ายตามมาตรฐานความผิดเกี่ยวกับการใช้งานคอมพิวเตอร์ภายในองค์กร โดยแยกแยะตามมาตรา 5,6,7,8,9,10 และ 11 ซึ่งเป็นจุดเด่นสำคัญที่มีความแตกต่างกับสินค้าอื่นและช่วยให้ออกรายงานสำหรับผู้บริหารได้อย่างครบถ้วน

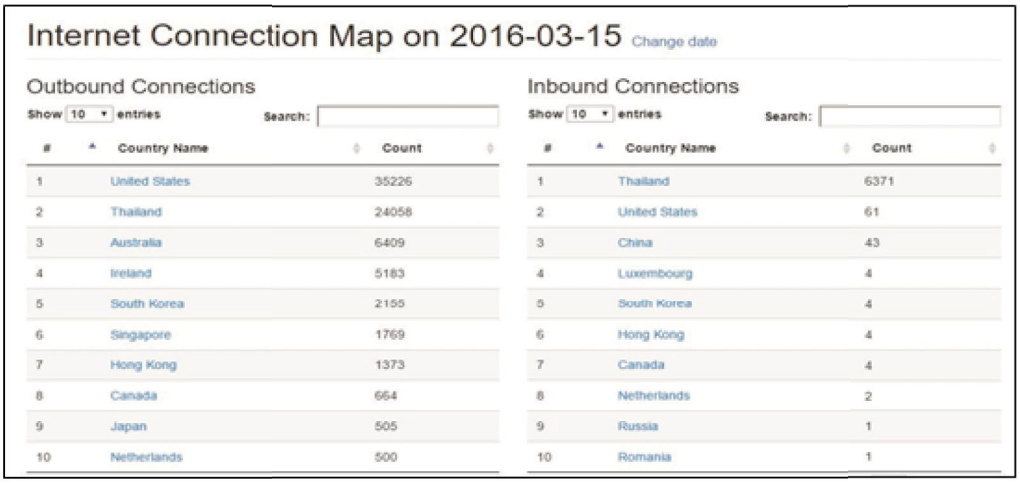


No	IP Address	Owner Name	High	Medium	Low
1	192.168.1.26		579	1	0
2	192.168.1.196	desktop-eiebif6	26	0	0
3	208.67.222.222	-	16	0	0
4	13.107.4.50	-	13	0	0

รายงานความเสี่ยงที่เกิดขึ้นภายในองค์กรที่สามารถออกรายงานได้ รายชั่วโมง รายวัน และรายเดือน

4. การเฝ้าติดตามปริมาณการใช้งานข้อมูลภายในองค์กร (Bandwidth Monitoring)

4.1 Country / City monitoring (In-out organization) รายงานผลการเฝ้าติดตามปริมาณการใช้งานข้อมูลระดับประเทศ ระดับเมือง ที่ส่งข้อมูลเข้าในองค์กรเรา และที่องค์กรของเราติดต่อไปยังโลกภายนอก เป็นการตรวจสอบข้อมูลวิ่งเข้าสู่องค์กร (Incoming data) และข้อมูลที่ถูกนำออกนอกองค์กร (Out going data) โดยผ่านเทคโนโลยี GeoData



Internet Connection Map on 2016-03-15 Change date

Outbound Connections

Show 10 entries Search:

#	Country Name	Count
1	United States	35226
2	Thailand	24058
3	Australia	6409
4	Ireland	5183
5	South Korea	2155
6	Singapore	1769
7	Hong Kong	1373
8	Canada	664
9	Japan	505
10	Netherlands	500

Inbound Connections

Show 10 entries Search:

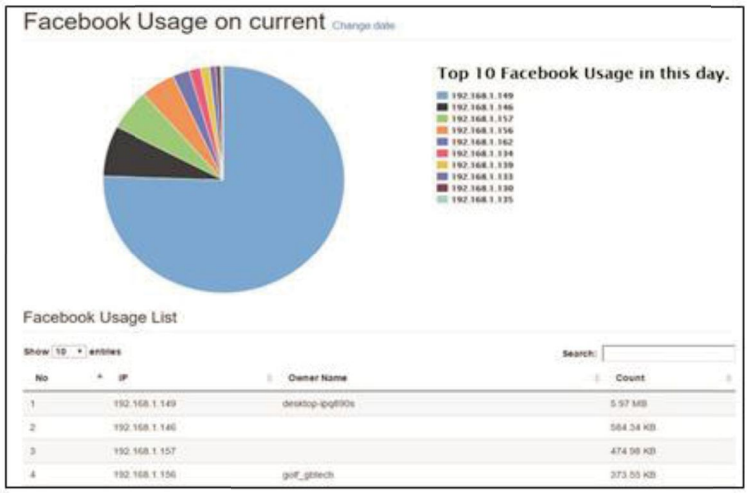
#	Country Name	Count
1	Thailand	6371
2	United States	61
3	China	43
4	Luxembourg	4
5	South Korea	4
6	Hong Kong	4
7	Canada	4
8	Netherlands	2
9	Russia	1
10	Romania	1

ภาพ SRAN ได้นำเทคโนโลยี GeoData เข้ามาเพื่อแสดงผลเหมาะสำหรับการเฝ้าระวัง
ผ่านห้อง War roomเพื่อประเมินสถานการณ์ที่เกิดขึ้นภายในองค์กร

4.2 Protocol and Service Bandwidth monitor จะสามารถคำนวณค่าปริมาณ Bandwidth ที่เกิดขึ้นบนระบบเครือข่ายได้โดยแยก Protocol TCP, UDP,ICMP และ Service ตาม well know port service จะทำให้ทราบถึงปริมาณการใช้งานข้อมูลได้อย่างละเอียดและประเมินสถานการณ์ได้อย่างแม่นยำ

4.3 Application Monitoring (Software bandwidth usage) รายงานการใช้แอปพลิเคชั่นและปริมาณการใช้ข้อมูลภายในองค์กรกว่า 1,000 ชนิด ได้แก่ SAP , ERP , Orcal , Skyp, Microsoft และ Enterprise แอปพลิเคชั่น SRAN รู้จักทำการเฝ้าติดตามและรายงานผ่านหน้าจอเพื่อดูปริมาณการใช้งานที่มีผลกระทบต่อองค์กร

4.4 Social Network Monitoring (Facebook , Line ,Youtube , Google Video , Twitter , Pantip) รายงานการใช้งานเครือข่ายสังคมออนไลน์เพื่อให้รู้ถึงปริมาณข้อมูลที่ใช้ภายในองค์กร ได้แก่ Facebook , Line , Youtube , Google Video , Twitter และ Pantip ทำให้ผู้บริหารองค์กรสามารถทราบความเคลื่อนไหวและการใช้ปริมาณข้อมูลภายในองค์กร



Facebook Usage on current Change date

Top 10 Facebook Usage in this day.

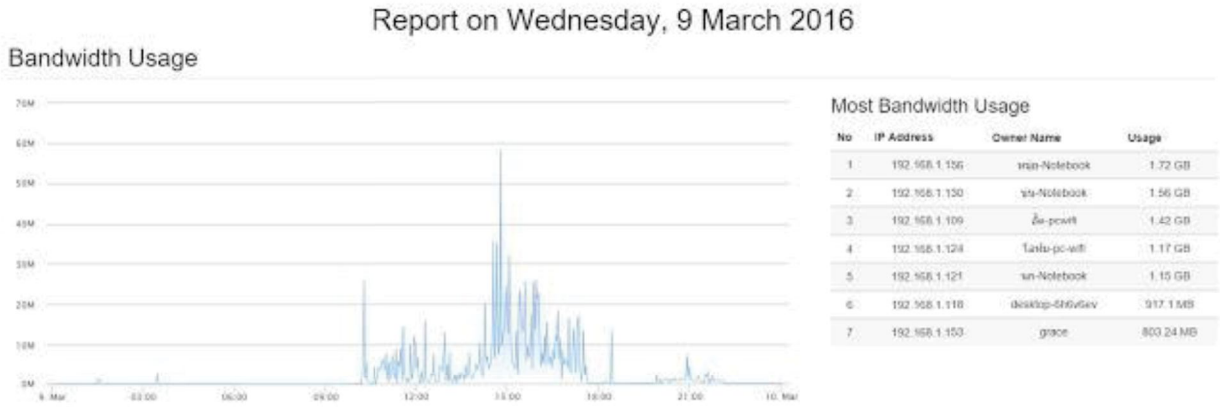
Facebook Usage List

Show 10 entries Search:

No	IP	Owner Name	Count
1	192.168.1.149	desktop-ipq890s	5.97 MB
2	192.168.1.146		584.34 KB
3	192.168.1.157		474.98 KB
4	192.168.1.156	golf_gbtech	373.55 KB

ภาพ Facebook Monitoring ทำให้ทราบถึงการใช้ปริมาณการใช้งานข้อมูลเครือข่ายสังคมออนไลน์

4.5 User Monitoring รายงานและจัดอันดับการใช้งาน Bandwidth ภายในองค์กร โดยจะเห็นรายชื่อผู้ใช้จากคุณสมบัติข้อ 1 ทำให้เราทราบถึงชื่อผู้ใช้งานและค่า Bandwidth ที่สูงสุดและทำเป็นรายงานผลได้เป็นรายชั่วโมง รายวัน และรายเดือน



รายงานปริมาณการใช้งาน Bandwidth ภายในองค์กร

5. การค้นหาข้อมูลในเชิงลึก (Deep Search)

5.1 การพิสูจน์หลักฐานทางข้อมูลสารสนเทศ (Network Forensic Evident data) ค้นหาเหตุการณ์ที่เกิดขึ้น แบ่งตามเนื้อหา (content search) ดังนี้ Web Access , Files Access , Network connection , SSL , Mail , Data Base , Syslog , VoIP , Remote Desktop , Radius และ Active Directory เหล่านี้สามารถค้นหา RAW Log ที่เกิดขึ้นได้ ทั้งแบบปัจจุบัน และ ย้อนหลังตามกฎหมาย

5.2 การค้นหาข้อมูลเชิงลึกสำหรับผู้บริหารและทรัพยากรบุคคล (HR /Top Manager query sensitivity data) การค้นหาเชิงลึกสำหรับผู้บริหารระดับสูง ที่ระบุถึงพฤติกรรมการใช้งานและการสื่อสารผ่านระบบอินเทอร์เน็ตและเครือข่ายคอมพิวเตอร์ภายในองค์กร

5.3 การค้นหารวดเร็ว และสามารถใช้เงื่อนไขในการค้นหา เช่น AND OR NOT เข้ามาเกี่ยวข้องเพื่อให้การค้นเป็นไปอย่างมีประสิทธิภาพที่สุด

6. การบริหารจัดการค่าการประเมินความเสี่ยง (Vulnerability Management)

6.1 Passive Vulnerability scanner : เป็นการทำงานต่อเนื่องเพื่อตรวจสอบและประเมินความเสี่ยงโดยทำการตรวจสอบจากค่า CVE (Common Vulnerabilities and Exposures) การค่า SSL Heartbleed Poodle, Shellsock ที่พบเครื่องแม่ข่ายและลูกข่ายภายในองค์กรที่มีโอกาสเกิดความเสี่ยงจากช่องโหว่นี้, การตรวจสอบการรับใบ Certification ที่ไม่ถูกต้อง ที่อาจตกเป็นเหยื่อการทำ MITM (Man in The Middle Attack) การตรวจสอบการรับใบ Certification ที่หมดอายุ expired date SSL certification) การตรวจสอบการรับส่งไฟล์ขนาดใหญ่ที่เกิดขึ้นในองค์กร , การตรวจสอบ backdoor และการสื่อสารที่ผิดวิธีจากมาตรฐาน และทำการแจ้งเตือนผ่าน Incident response notices

6.2 Active Vulnerability scanner : การตรวจสอบโดยตั้งค่า ตรวจสอบความปลอดภัยให้กับเครื่องแม่ข่ายที่ใช้ทำเป็น Active Directory การตรวจสอบรายชื่อผู้ใช้งาน ค่าความปลอดภัย รวมถึงการตรวจสอบเครื่องที่มีโอกาสติดเชื้อและมีช่องโหว่ตาม CVE

6.3 IPv6 checklist : การตรวจสอบค่า IPv6 โดยทำการส่งค่าตรวจสอบแบบ Broadcast เพื่อสำรวจเครือข่ายว่าอุปกรณ์ไหนที่รองรับค่า IPv6 และจัดทำรายงานการสำรวจ

7. การเก็บบันทึกข้อมูลจราจรคอมพิวเตอร์และดูย้อนหลัง (Log Record and Archive)

7.1 การเก็บบันทึกข้อมูลแบบ Raw Full data การเก็บข้อมูลที่เป็นประโยชน์ในการสืบสวนสอบสวนและการหาผู้กระทำความผิด ด้วยการเก็บบันทึกที่สามารถทำได้แบบ Hybrid ซึ่ง SRAN เป็นต้นฉบับของการทำวิธีนี้ คือการรับข้อมูลจราจรคอมพิวเตอร์แบบ Passive mode และ รับค่าจากอุปกรณ์อื่นได้

7.2 รองรับค่า Log จาก AD (Active Directory) , Router / Firewall / VPN ,Mail Server (Support Exchange , Lotus note) , DHCP , DNS, SNMP , Radius Wi-Fi Controller และทำการแยกแยะค่าการเก็บ Log โดยแบ่งเป็นหมวดให้ได้โดยอัตโนมัติ รองรับการเก็บบันทึกข้อมูลจราจรคอมพิวเตอร์ที่เกี่ยวข้องกับ Protocol ที่ใช้กับอุปกรณ์สื่อสารในโรงงานอุตสาหกรรม ประเภท Modern SCADA system รองรับ Protocol DNP3, Mobus (Modicon Communication Bus) เป็นต้น

7.3 รองรับ SCP , sFTP และการ mount files log จากเครื่องอื่นมาเก็บแบบรวมศูนย์ (Centralization Log) และมีความสามารถใน Export Data ออกเพื่อใช้ในการพิสูจน์หาหลักฐาน การ Export ข้อมูลเรียงตามชั่วโมง วันและเดือนปี

7.4 การเก็บบันทึกข้อมูลสามารถเก็บได้ยาวนายกว่า 90 วันตามกฎหมายกำหนด มีซอฟต์แวร์ SRAN Logger Module รวมอยู่ในอุปกรณ์ ผ่านมาตรฐาน NECTEC มศอ.๔๐๐๓.๑ - ๒๕๕๒ (NECTEC STANDARD NTS 4003.1-2552) ระบบเก็บบันทึกข้อมูลจราจร ตาม พ.ร.บ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ ปี 2550

7.5 การเก็บบันทึกข้อมูลมีการยืนยันความถูกต้องข้อมูล Integrity hashing confidential files

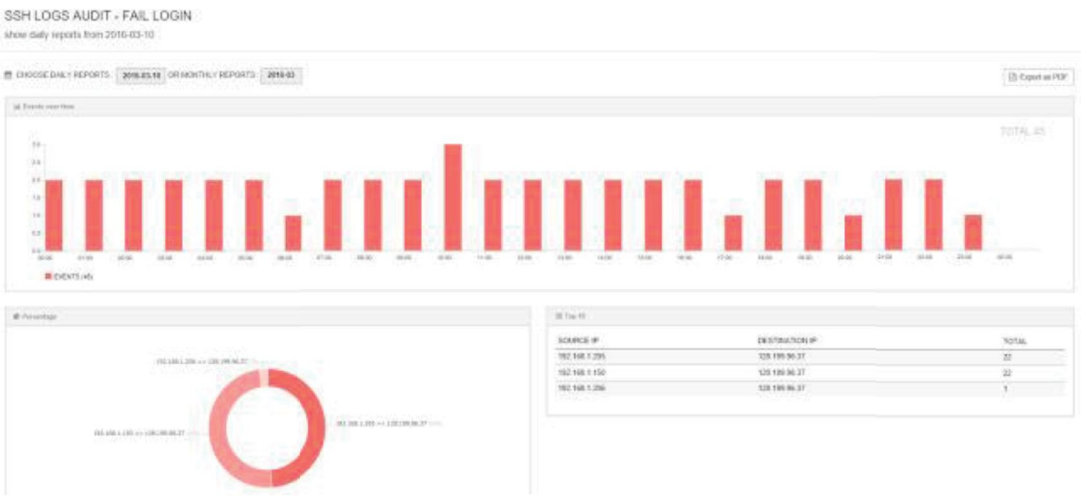
ภาพการเก็บบันทึกข้อมูลจาก Syslog มีการทำ File integrity เพื่อยืนยันความถูกต้องข้อมูล
ผู้ที่เข้าถึงไฟล์ได้ต้องเป็นระดับ Data Keeper ที่องค์กรได้มอบหมายรับผิดชอบในส่วนนี้

8. การเก็บบันทึกค่าสำหรับให้ IT Audit ในการตรวจสอบข้อมูลและใช้เป็นหลักฐาน (Log Audit)

8.1 การเก็บบันทึกค่า Active Directory Login active / Login fail

8.2 การเก็บบันทึกค่า SSH Login active / Login fail

*8.3 การเก็บบันทึกค่า Active Directory user security check ตาม AAA Authentication เพื่อตรวจสอบรายชื่อพนักงาน รหัสผ่านที่ยังไม่ได้ทำการแก้ไข และอายุระยะเวลาของรายชื่อ (Account) , Authorization สิทธิในการเข้าถึงข้อมูล



รายงานการ Login ผิดพลาดที่เกิดขึ้นจากการใช้

9. การวิเคราะห์ไฟล์ที่ติดเชื้อจากการติดต่อสื่อสารบนระบบเครือข่ายคอมพิวเตอร์ (Malware Analytic)

9.1 Files Integrity monitoring การตรวจสอบค่าความถูกต้องจากการสื่อสาร โดยสามารถมองเห็นประเภทของไฟล์ที่เกิดขึ้นบนระบบเครือข่าย ไฟล์ประเภทเอกสาร (pdf,doc,docx,xls ,ppt เป็นต้น) , ไฟล์ประเภทมัลติมีเดีย (mp3,mp4 เป็นต้น) , ไฟล์ประเภทบีบอัดข้อมูล (zip , rar เป็นต้น) , ไฟล์ประเภททำงานได้ในตัว (exe ,dll เป็นต้น), ไฟล์เกี่ยวกับภาพ (jpg,png,gif เป็นต้น)

*9.2 นำค่าการตรวจพบในข้อ 9.1 เข้ามาทำการวิเคราะห์เพื่อหามัลแวร์ (Malware Analytic file with virustotal) โดยใช้การตรวจสอบไฟล์ผ่านโปรแกรมแอนตี้ไวรัสกว่า 50 ชนิด ผ่าน API Virustotal

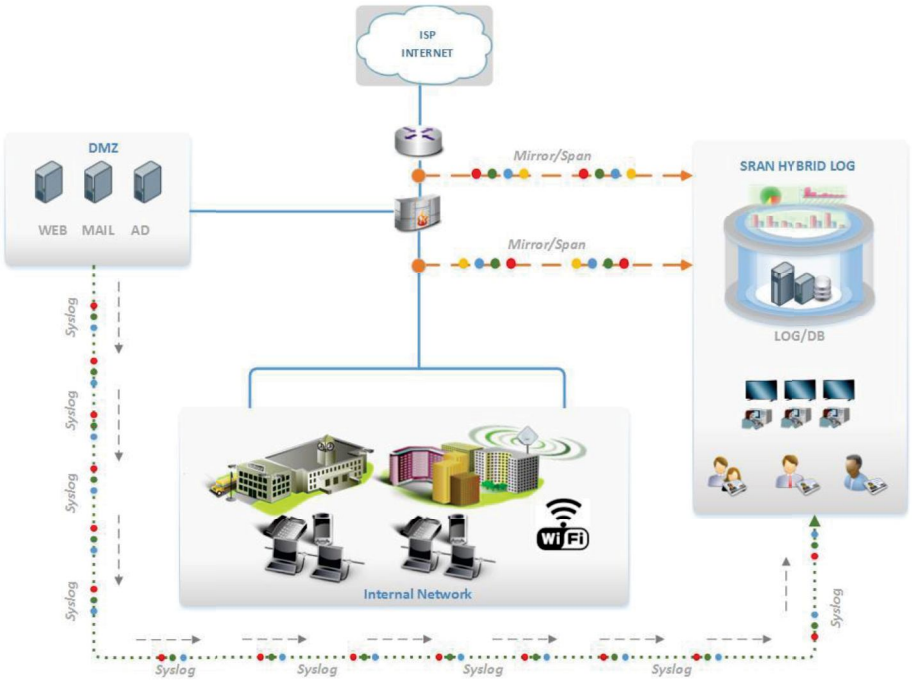
10. ระบบ Alert System รองรับการแจ้งเตือนผ่าน E-mail ไปยังผู้ดูแลระบบเมื่อมีเหตุการณ์ความเสี่ยงในระดับสูง เช่น ไวรัสคอมพิวเตอร์เข้าสู่ระบบ หรือมีการโจมตีทางไซเบอร์ (Cyber Attack) ที่สร้างความเสียหายให้แก่องค์กร

คุณสมบัติพิเศษ * การมองเห็นและเก็บบันทึกเหตุการณ์ที่ผ่านการเข้ารหัส (SSL log Decryption)

การมองเห็นเป็นสิ่งสำคัญ ในยุคปัจจุบันจะพบว่าทุกการสื่อสารจะมีการผ่านช่องทางเรียกว่า SSL บนเว็บไซต์จะผ่าน HTTPS ซึ่งจะทำให้เราไม่สามารถมองเห็นเหตุการณ์ที่เกิดขึ้นได้ ในตัว Net Approve สามารถมองเห็น ค่าภายใน SSL โดยจะทำได้ในรุ่น NG-100 ขึ้นไป เพื่อตรวจการกระทำที่มีโอกาสเสี่ยงในการกระทำความผิดทางกฎหมาย และใช้ Log อ้างอิงได้ในชั้นศาล

ทั้ง 10 ข้อที่กล่าวมาบรรจุลงบนเครื่อง SRAN Appliance ที่พร้อมใช้งาน สามารถติดตั้งและเห็นผลภายใน 30 นาที เห็นผลไม่จำเป็นต้องใช้ผู้เชี่ยวชาญก็สามารถติดตั้งได้ และเมื่อใช้อุปกรณ์ SRAN NetApprove ก็เปรียบเสมือนกับมีผู้เชี่ยวชาญระดับมืออาชีพทำงานให้เรา ทำงานรายงานผลสรุปให้ผู้บริหาร เฝ้าระวังและคุ้มครองให้องค์กรและหน่วยงานเรามีความมั่นคง
และปลอดภัยทางข้อมูล 24 x 7 โดยไม่มีวันเหนื่อยล้า

การออกแบบเป็นระบบ Hybrid ที่สามารถรับค่า Log จาก syslog , SCP/sFTP ได้ อย่างอัตโนมัติ



หมายเหตุ ค่า * คือเป็น Feature ที่ทดลองใช้งานจริง

คุณสมบัติเพิ่มเติมของ SRAN NetApprove

1. เป็นอุปกรณ์ Appliance หรืออุปกรณ์คอมพิวเตอร์ที่ได้มาตรฐาน สามารถเก็บรวบรวมเหตุการณ์ (logs or Events) ที่เกิดขึ้นในอุปกรณ์ที่เป็น appliances และ non-appliances เช่น Firewall, Network Devices ต่าง ๆ ระบบปฏิบัติการ ระบบ appliances ระบบเครือข่าย และระบบฐานข้อมูล เป็นต้น ได้อย่างน้อย 10, 15 อุปกรณ์ต่อระบบ โดยสามารถแสดงผลอยู่ภายใต้รูปแบบ (format) เดียวกันได้
2. มีระบบการเข้ารหัสข้อมูลเพื่อใช้ยืนยันความถูกต้องของข้อมูลที่จัดเก็บตามมาตรฐาน SHA-1
3. สามารถเก็บ Log File ในรูปแบบ Syslog ของอุปกรณ์ เช่น Router, Switch, Firewall, VPN, Serverได้
4. สามารถบริหารจัดการอุปกรณ์ผ่านมาตรฐาน HTTPS, Command Line Interface และ SSH ได้
5. สามารถจัดเก็บ log file ได้ถูกต้อง ตรงตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ ฉบับที่มีผลบังคับใช้ โดยได้รับรองมาตรฐานการจัดเก็บและรักษาความปลอดภัยของ log file ที่ได้มาตรฐานของศูนย์อิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (มศอ. 4003.1-2552)
6. สามารถทำการสำรองข้อมูล (Data Backup) ไปยังอุปกรณ์จัดเก็บข้อมูลภายนอก เช่น Tape หรือ DVD หรือ External Storage เป็นต้น ได้

NetApprove	NG100	NG200	NG300X
Capacity and Performance			*Custom depend on customer
Logs Capacity per Day	5GB	10GB	by Request
Current Counter (Session/Hour)	2,200,000	3,500,000	by Request
Normal Log Rate (Event/Second)	7,000	20,000	by Request
Feature			
1. Automatic Identification Device 1.1 Know Device / Unknown device 1.2 Approve device / Rogue Detection 1.3 BYOD : Desktop / Mobile 1.4 Inventory : Device / Software	✔	✔	✔
2. Detect and Analyzer 2.1 Attack Detection (Brute force, exploit) 2.2 Malware/Virus Detection 2.3 Botnet Detection 2.4 Behavior Data Leak Detection 2.5 Bittorent Detection 2.6 Anomaly Detection 2.7 Tor/Proxy Detection 2.8 HTTP / SSL Analyzer 2.9 APT (Advanced Persistent Threat) Detection	✔	✔	✔
3. Log Analysis : Security Information Event Management 3.1 Threat intelligent correlation 3.2 Risk score 3.3 Risk Analyzer (High , Medium , Low) 3.4 Executive summary (Hour, Daily, Week, Monthly) 3.5 Compliance Thai Cyber law log correlation report (Hour, Daily,Week, Monthly)	✔	✔	✔
4. Bandwidth Monitoring 4.1 Country / City monitoring (In-out organization) 4.2 Application Monitoring (Software bandwidth usage) 4.3 Social Network Monitoring (Facebook , Line ,Youtube , Pantip) 4.4 User Monitoring	✔	✔	✔
5. Deep Search 5.1 Network Forensic Evident data 5.2 HR /Top Manager query sensitivity data	✔	✔	✔
6. Vulnerability Management 6.1 Passive Vulnerability scanner (CVE check,SSL Heartbleed , Shellsock check invalid cert MITM ,expired date SSL certification) 6.2 Active Vulnerability scanner (Malware , Sniffer , Broadcast) 6.3 IPv6 checklist	✔	✔	✔
7. Log Archive 7.1 Raw full data 7.2 Support AD (Active Directory) 7.3 Router / Firewall / VPN , Mail Server (Support Exchange ,Lotus note) , DHCP , DNS , SNMP , Radius Wi-Fi Controller	✔	✔	✔

NetApprove	NG100	NG200	NG300X
Feature			
8. Log Auditor 8.1 Active Directory Login active / Login fail, SSH Login active / Login fail, Active Directory - user security check	✔	✔	✔
9. Protection 9.1 Passive internet blocking 9.2 Blacklist blocking	✔	✔	✔
10. Malware Analytic 10.1 Files Integrity monitoring 10.2 Analytic file with virustotal	✔	✔	✔
11. Alert System : Email Alert (High Risk)	✔	✔	✔
Hardware Specification			
Form Factor	1U	2U	2U
Total Interfaces	8x1GbE	4x1GbE	4x1GbE
Storage Capacity	1TB	2TB	4TB
Removable Hard Drives	No	Yes	Yes
RAID Levels Supported	None	RAID 0/1	RAID 5/1
Default RAID Level	-	1	5
Redundant Hot Swap Power Supply	No	YES	YES
Compliance			
Safety Certifications	CE, FCC, UL	CE, FCC, UL	CE, FCC, UL

Planet Communications Asia PLC.
157 Soi Ramindra 34, Ramindra Rd., Tarang, Bangkhen, Bangkok 10230
Tel: +66 2 792 2400 I Fax: +66 2 792 2499, +66 2 943 5771
E-mail: sales@planetcomm.com