SRAN e-Newsletter

จดหมายข่าวออนไลน์ เพื่อความปลอดภัยทางข้อมูลสารสนเทศ ปีที่ 1 ฉบับที่ 9 ประจำเดือน ตุลาคม 2552

Editor's talk

สวัสดีค่ะคุณผู้อ่านทุกท่าน

เมื่อวันที่ 09-09-09 ที่ผ่านมา บริษัทฯ ได้เปิดตัวผลิตภัณฑ์ใหม่ "SRAN Light" อุปกรณ์ที่ช่วยฉายภาพพฤติกรรมการใช้งานไอทีภายในองค์กร รวมทั้งภัยคุกคามต่างๆ ให้เห็นแจ่มชัด เพื่อตอบโจทย์การป้องกันภัยคุกคามภายในองค์กรที่มีแนวโน้มเพิ่มสูงขึ้น จดหมายข่าวฉบับนี้จึงได้นำเสนอรายละเอียดของ SRAN Light

ปฏิวัติระบบเฝ้าระวังภัยคุกคามทางเครือข่าย

SRAN จึงได้พัฒนา "SRAN Light" ขึ้น เพื่อฉายภาพพฤติกรรมการใช้งานไอทีภายในองค์กร รวมทั้งภัยคุกคามต่างๆ ให้เห็นเด่นชัด เชื่อมงาน IT Security เข้ากับงานบริหารทรัพยากรบุคคล เสมือนมีกล้องวงจรปิดในเครือข่ายสารสนเทศ ที่บันทึกการใช้งานได้อย่างครบถ้วน และสะดวกต่อการตรวจสอบพฤติกรรมการใช้งาน โดยไม่ละเมิดสิทธิส่วนบุคคลตามนโยบายของแต่ละองค์กรได้อย่างลงตัว

การติดตั้งทำได้ 3 Mode
- In-Line >> ป้องกันภัยไซ่งลก
- Transparent >> ป้องกันภัยทั่วไป
- Passive >> ตรวจจับภัยคุกคาม

ด้วยเทคโนโลยี "HBW" หรือ Human Behavioral Warning ของ SRAN Light ที่ได้ นำเทคนิค Intrusion Detection System ในระดับ Network Base มาผนวกเข้ากับการจัดเก็บคลังข้อมูล (Inventory) จึงสามารถตรวจจับรายชื่อ พนักงาน ชื่อหน่วยงาน ค่า MAC Address นำมาเชื่อมโยงกับ IP Address (ทั้งแบบ Dynamic และ Static IP) ได้

ลักษณะการตรวจวิเคราะห์ Application Protocol ที่ SRAN Light สามารถเก็บบันทึกได้ แบ่ง เป็น 2 ส่วน คือ

ข้อมูลที่เกิดจากการใช้งานปกติ (Normal Traffic) ได้แก่ Web, Email, Messenger, File Transfer, P2P และอื่นๆ เช่น Telnet, Remote Desktop, VNC, Radius เป็นต้น

ข้อมูลที่เกิดจากการใช้งานที่ไม่ปกติ (Threat Traffic) ได้แก่

ลักษณะการแพร่กระจายสิ่งผิดปกติ เช่น Virus/worm, Backdoor, Trojan, Malware, Botnet

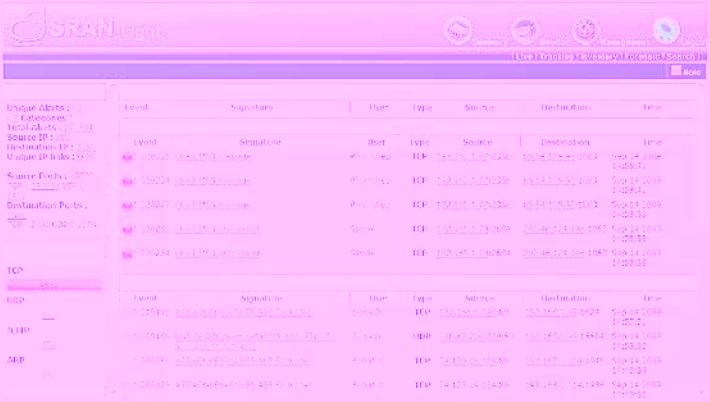
ลักษณะการโจมตีชนิดต่างๆ เช่น DDoS/ DoS , Brute

คุณสมบัติเด่นของ SRAN Light

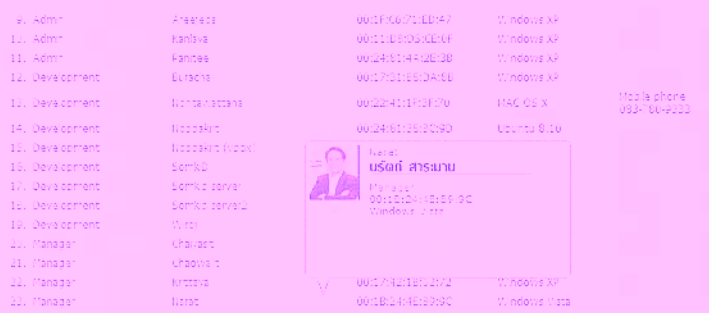
1. เก็บบันทึก Log File และจัดเปรียบเทียบให้สอดคล้องกับ พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ดังนี้

- ระบุตัวตนผู้ใช้งาน ช่วยให้ทราบพฤติกรรมการใช้ข้อมูลบนระบบไอทีในองค์กร โดยสามารถพิสูจน์ได้ว่า ใคร(who) ทำอะไร(what) ที่ไหน(where) เมื่อใด (when) อย่างไร(why/how) ได้อย่างครบถ้วน
- สามารถแยกแยะภัยคุกคามที่เกิดขึ้นในองค์กร พร้อมนำเสนอวิธีการแก้ไข
- จัดทำสถิติการใช้งานข้อมูลทั่วไป เพื่อเก็บบันทึกตามหลักเกณฑ์ การเก็บบันทึกข้อมูลจราจร

2. ตรวจจับและเฝ้าระวังภัยคุกคามทางเครือข่ายด้วยเทคโนโลยี NIDS/IPS ช่วยปกป้องเครือข่ายจากภัยคุกคามทั้งจากภายนอกสู่องค์กร (Intrusion) และภัยคุกคามจากภายในเครือข่ายออกสู่ภายนอก (Extrusion) ประมวลผลผ่านเวบบราวเซอร์ พร้อมออกรายงานผลเป็นรายวัน โดยจัดลำดับความเสี่ยงเป็น สูง กลาง ต่ำ



3. ช่วยให้ทราบถึงพฤติกรรมการใช้งานไอทีภายในองค์กร โดยเชื่อมโยง IP Address และ MAC Address เข้ากับข้อมูลรายชื่อพนักงานซึ่งสามารถเพิ่มรูปพนักงานเข้าไปในระบบได้ พร้อมเก็บประวัติการ ใช้งาน



4. สามารถจัดเก็บค่า Inventory แบบ Passive ทางระบบเครือข่าย ประกอบด้วยข้อมูลดังนี้

รายชื่อพนักงานบริษัท (Name)	ชื่อแผนก (Department)
ชื่อระบบปฏิบัติการของพนักงาน (Operating System)	ค่า IP Address และ MAC Address แต่ละเครื่องในองค์กร

5. รายงานผลการใช้งานข้อมูลสารสนเทศเป็นรายแผนก, รายบุคคลและภาพรวมของบริษัทได้ ในรูปแบบ ไฟล์ CSV, HTML ทั้งยังสามารถออกรายงานผลเพื่อ เชื่อมโยงระบบมือถือได้ผ่านช่องทาง XML

6. เฝ้าระวังพฤติกรรมการใช้งาน โดยสามารถกำหนด Rule Policy ตามนโยบายขององค์กรได้ เพื่อป้องกันการละเมิดสิทธิส่วนบุคคล ของพนักงานในองค์กร

ประโยชน์ที่ได้รับจาก SRAN Light

1. ประหยัดงบประมาณ ด้วยการรวมทุกคุณสมบั ไว้ในอุปกรณ์เดียว และไม่ต้องอาศัยอุปกรณ์เสริม
2. ติดตั้งง่าย ไม่ส่งผลต่อการเชื่อมต่อเครือข่ายเดิม
3. เฝ้าระวังภัยคุกคามเครือข่ายองค์กร ทั้งจากภาย ในและภายนอกเครือข่าย
4. เก็บบันทึก Log File สอดคล้องตาม พ.ร.บ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
5. ทราบพฤติกรรมการใช้งานไอทีภายในองค์ก อย่างชัดเจน แสดงผลด้วยภาพพนักงาน ทำให้ทราบ พนักงานมีพฤติกรรมการใช้งานเครือ-ข่ายอย่างไม่เหมาะ ม เช่น ดาวน์โหลดหนัง, เพลง เป็นเหตุให้การใช้งา เครือข่ายโดยรวมช้าลงหรือไม่ เป็นต้น
6. รู้เท่าทันปัญหาการฉ้อโกงภายในองค์กร (Intern Fraud) เช่น การลักลอบขโมยข้อมูลภายในองค์ก พร้อมหลักฐานประกอบรูปคดี
7. แสดงสถิติการใช้งานเป็นรายแผนก รายบุคค ช่วยให้การพยากรณ์การลงทุนระบบไอทีในองค์กร ประสิทธิภาพยิ่งขึ้น
8. สรุปผลรายงานได้เองตามความต้องการ จา ไฟล์ CSV

SRAN *Light*

รุ่นของผลิตภัณฑ์

LT50
- Storage Disk 250 GB
- Interface 4 Port GbE (10/100/1000)
- Maximum Devices
  - * Passive/Transparent Mode = 50
  - * In-line Mode = 20

LT100
- Storage Disk 500 GB
- Interface 4 Port GbE (10/100/1000), Bypass mode support
- Maximum Devices
  - * Passive/Transparent Mode = 100
  - * In-line Mode = 80

LT500
- Storage Disk 1024 GB Raid 1/5
- Interface 8 Port GbE (10/100/1000), Bypass mode support
- Maximum Devices
  - * Passive/Transparent Mode = 500
  - * In-line Mode = 150

FAQ for SRAN Security Center

Q: ไม่สามารถเข้าไป Monitor SRAN ผ่านหน้าเว็บได้ เกิดจากสาเหตุใด?

A: <u>จากภายในองค์กร</u> อาจเกิดได้จากหลายสาเหตุ ดังนี้

- ไม่ได้เปิดเครื่อง SRAN
- ไม่ได้ใช้ Protocol “HTTPS”
- ใส่ IP ผิด
- ไม่ได้ต่อสายที่ Port Manage เข้ากับเครื่องคอม หรือเข้ากับ Switch ในวง Network เดียวกัน
- ในกรณีที่ต่อตรงเข้ากับคอมพิวเตอร์เครื่องเดียวให้ใช้สาย Cross ดีที่สุด
- สายที่นำมาใช้ต่อเข้ากับ Port Manage มีการชำรุดหรือขาด
- ตอน Set IP ใช้วิธี Set ผ่าน Port Console ซึ่งการ Set IP แบบนี้ต้องเข้ามา SAVE ผ่านหน้าเว็บด้วยทุกครั้งในหน้า Management –> TCP/IP Configuration ตรวจสอบ IP ให้ถูกต้อง แล้วกด Save Config
- ถ้าในกรณีที่เปิดเครื่องแล้วยังไม่สามารถ Monitor SRAN ผ่านหน้าเว็บได้ ให้รอสักครู่ เนื่องจากบางทีเครื่อง SRAN อาจกำลังทำการ Scan Disk อยู่ ซึ่งจะสามารถเห็นได้ถ้าเปิดผ่านหน้า HyperTerminal โดยการต่อที่ Port Console

<u>จากภายนอกองค์กร</u>

- Firewall ขององค์กรที่ติดตั้ง SRAN ไม่ได้ฟอร์เวิร์ด Port 443 ของ SRAN ออกมาให้หรือ Config Rules Firewall ไม่ผ่าน

ดูข้อมูล FAQ เพิ่มเติมได้ที่
http://www.gbtech.co.th/th/contacts/faq