1. ที่มาและแนวคิด SRAN

องค์ประกอบสำคัญในด้านความมั่นคงปลอดภัยทางข้อมูลสารสนเทศ คือ เทคโนโลยี คน และ กระบวนการ สิ่งที่สามารถ ควบคุมได้ง่ายที่สุดคือ เรื่องเทคโนโลยี ถึงแม้จะไม่มีเทคโนโลยีใดทที่ทำงานแทนคนได้หมด และไม่มีเทคโนโลยีใดที่ป้องกันภัยคุกคามได้สมบูรณ์แบบ หากเราควบคุมเทคโนโลยีที่นำมาใช้ได้ และรู้ทันปัญหาที่เกิดขึ้น ประหยัดงบประมาณทุน ใช้ได้อย่างคุ้มค่า เราก็สามารถนำส่วนที่ต้องลงทุนทางเทคโนโลยีที่เหลือใช้ มาอบรมเจ้าหน้าที่พนักงานให้เกิดองค์ความรู้ และ จัดหากระบวนการเพื่อสร้างมาตรฐานด้านความมั่นคงปลอดภัยทางข้อมูลสารสนเทศ ได้อย่างมีทิศทางมากขึ้น ดังนั้นในการสร้างเครือข่ายตื่นรู้จึงเป็นการ สรุปการจัดหาเทคโนโลยี มารองรับเครือข่ายคอมพิวเตอร์ จัดหาเทคโนโลยีด้านความมั่นคงปลอดภัยทางข้อมูล สมบูรณ์แบบ ที่เราสามารถระบุตัวตนของผู้ใช้งาน ระบุลักษณะการใช้งาน และบันทึกข้อมูลการใช้งานตามความเหมาะสมที่เกิดขึ้น สามารถยืนยันหลักฐานเพื่อใช้ในการสืบสวนสอบสวนหาผู้กระทำผิดทางคอมพิวเตอร์ ทั้งในองค์กร และนอกองค์กรได้อย่างมีความสะดวกมากขึ้น มีประสิทธิภาพ และมีประสิทธิผลตามมา

แนวทางการสืบหาผู้กระทำผิด (Chain of Event) ตาม พ.ร.บ. คอมพิวเตอร์

1.Who ใคร
2.What ทำอะไร
3.Where ที่ไหน
4.When เวลาใด
5.Why อย่างไร

เนื่องจากรับส่งข้อมูลผ่านเครือข่ายคอมพิวเตอร์ เป็น Real Time ไม่สามารถดูย้อนหลังได้ การที่จะสามารถดูย้อนหลังได้ ต้องมีการเก็บบันทึกข้อมูล ที่เรียกว่า Log และเพื่อเก็บรักษาข้อมูลดังกล่าว
และป้องกันไม่ให้หลักฐานข้อมูลนั้นเปลี่ยนแปลงได้ จึงควรมีการทำ Chain of Custody คือเก็บบันทึกรักษาข้อมูลจราจรขึ้น และนี้เองคือสาระสำคัญของการออกกฎหมายฉบับนี้เพื่อป้องปราบ และเก็บบันทึกหลักฐาน เพื่อสืบสวนสอบสวน หาผู้กระทำผิดมาลงโทษ ดังนั้นการจัดหาเทคโนโลยีเพื่อเก็บรักษาหลักฐานข้อมูล เป็นเรื่องที่ซับซ้อน เราจึงมีแนวคิดเพื่อจัดหาเทคโนโลยีมาแก้ไขปัญหา และลดความซับซ้อนนี้ขึ้น เรียกว่า " การสร้างเครือข่ายตื่นรู้ (Energetic Network)" ส่วนหนึ่งคือการเฝ้าระวังภัยคุกคาม (Monitoring & Analysis)

ที่มาของ SRAN

เราเชื่อว่าอนาคตโลกยุคใหม่ จะเชื่อมโยงข้อมูลผ่านระบบไอทีมากขึ้น จนเป็นส่วนหนึ่งในการใช้ชีวิตประจำวันของเราไป การที่เรามีจะป้องกันภัยคุกคามจากโลกไซเบอร์ได้นั้น เราต้องแข็งแรงในองค์ความรู้ของคนในชาติ และนวัตกรรมที่ใช้ เพื่อระบบความมั่นคงทางข้อมูล ควรเป็น เทคโนโลยีที่คนในชาติ สามารถควบคุมเองได้ จึงเกิดเป็นที่มาของการ สร้าง "SRAN" ขึ้น

SRAN ออกเสียงว่า สราญ (รมณ์) สัญลักษณ์ เป็น แมววิเชียรมาศ ซึ่งเป็นแมวลายจุดำ 9 แต้ม แมววิเชียรมาศ ที่มาของสัญลักษณ์ SRAN

SRAN เป็นคำย่อมาจาก Security Revolution Analysis Network คือ การปฏิรูปเทคโนโลยีเพื่อใช้สำหรับการเฝ้าระวังเหตุการณ์ข้อมูลจราจรบนเครือ ข่ายคอมพิวเตอร์ ซึ่งเป็น เครื่องมือทางเทคโนโลยี เพื่อใช้ทุ่นแรงสำหรับผู้ดูแลระบบ โดย สำรวจ ตรวจสอบ วิเคราะห์สาเหตุ และประเมินความเสี่ยงระบบเครือข่าย ให้เกิดความสะดวกสบายมากที่สุด

Copyright © SRAN Technology

SRAN

โดยใช้หลักการวิเคราะห์จากทฤษฎีดังต่อไปนี้

- วิธีการสืบหาหลักฐานจากการกระทำผิดคอมพิวเตอร์ หรือที่เรียกว่า Forensic โดยอาศัยวิธีการ Chain of Custody ใน คือพิจารณาเส้นทางลำเลียงข้อมูล และเหตุปัจจัยในการก่อให้เกิดเหตุการณ์ขึ้นตามวัน เวลา ที่ระบุตรงได้

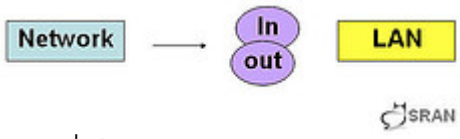
- ทฤษฎีการสร้าง Honeynet Concept ที่กล่าวถึงการทำ Data Control , Data Capture และ Data Collection ซึ่งเป็นแนวคิดที่ทางทีมพัฒนา SRAN นำมาประยุกต์เป็นผลิตภัณฑ์

- ทฤษฎี NSM (Network Security Monitoring) ที่กล่าวถึงการเฝ้าสังเกตการข้อมูลสารสนเทศที่มีความเสี่ยงต่อภัยคุกคาม อันมีผลกระทบกับเครือข่ายโดยรวม โดยแบ่งการสังเกตการตาม Full Content Data สนใจเนื้อหาของข้อมูลทั้งหมด , Session Data การพิจารณาข้อมูลการติดต่อบน Layer 3 - 7 ตาม session ของการเชื่อมต่อ ได้แก่ Network Flow , TCP Flow , UDP flow เป็นต้น

- ทฤษฎี 3 in 3 out ที่ทางผู้พัฒนา SRAN คิดค้นขึ้นเพื่ออธิบายความให้สะดวก จากพื้นฐานของ OSI 7 layer

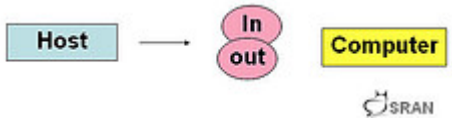
3 in 3 out คือการกำหนดลมหายใจ ของระบบเครือข่าย
เป็นเส้นทางลำเลียงข้อมูล เข้า และ ออก ไป บนการใช้งานจริงของเรา

ข้อมูล ที่เข้า และออก ในระดับ Internet เป็นข้อมูลจากโลกภายนอก ระดับ ISP (Internet Services Provider) หรือมองในระดับ WAN Technology ที่กำลังเข้าสู่ระบบเครือข่ายที่เราใช้งาน และ เป็นข้อมูลที่เราจะต้องทำการติดต่อออกไป จากภายในเครือข่ายที่เราใช้งาน เพื่อติดต่อออกไปตามเป้าหมายที่เราต้องการ ได้แก่ เราต้องการเปิด Web ไม่ว่าเป็นเว็บภายในประเทศ หรือ นอกประเทศ ก็เป็นการเชื่อมต่อแบบ HTTP port 80 ที่เป็นการติดต่อแบบ TCP การส่ง E-mail เชื่อมต่อแบบ SMTP port 25 ที่เป็น TCP เป็นต้น
ภายในระบบเครือข่ายของเรา ออกไปข้างนอก ต้องผ่านอุปกรณ์ Router จากฝั่งของเรา เพื่อไปยังจุดหมาย และเส้นทางลำเลียงข้อมูลสารสนเทศ จะดำเนินตามหลัก OSI 7 layer และ TCP/IP
พิจารณา Intrusion ภัยคุกคามทางข้อมูลที่ได้รับจากเส้นทางลำเลียงข้อมูลจาก ISP เข้าสู่ระบบเครือข่ายของเรา ส่วน Extrusion ภัยคุกคามทางข้อมูล ขา ออกเครือข่ายของเราไปยังโลกอินเตอร์เน็ท
อุปกรณ์ที่เราควรพิจารณา เส้นทางการลำเลียงข้อมูลเพื่อใช้ในการทำสืบหาการกระทำผิดทางอาชญากรรมคอมพิวเตอร์ (Network Forensics) ข้อมูลของ Log ที่เกิดขึ้นจากอุปกรณ์ Router ตามเส้นทางเดินทางของข้อมูล ทั้ง เข้า และ ออก ไปยังที่หมาย



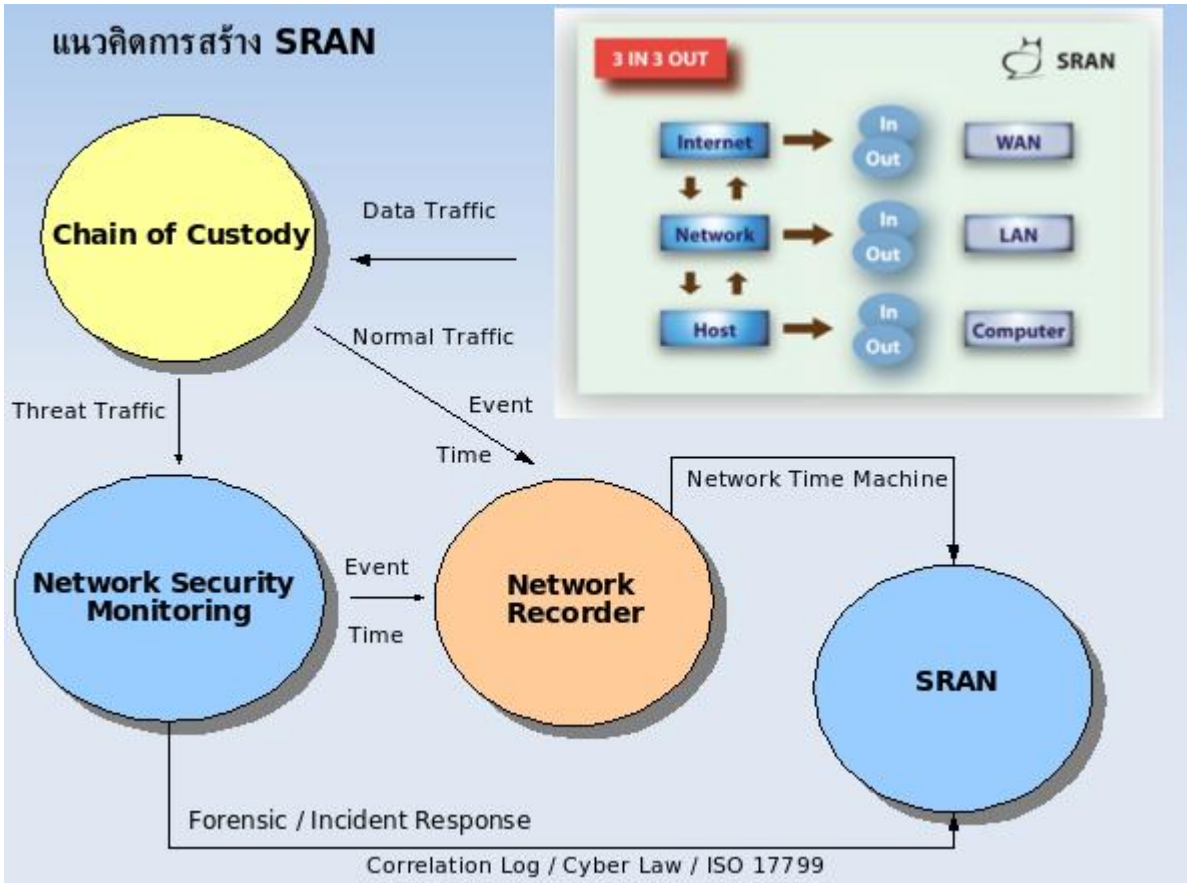
ข้อมูล ที่เข้า และออกในระดับ Network เป็นข้อมูลจากเครือข่ายที่เราอยู่ ในระดับ LAN เราจะเริ่มพิจารณา ข้อมูลที่เข้า และออกในระดับที่ ระดับชายแดนเครือข่าย (Perimeter Network) ตั้งแต่อุปกรณ์ Router ฝั่งเครือข่ายของเรา
พิจารณา Intrusion ภัยคุกคามทางข้อมูล ขา เข้าสู่ระบบเครือข่ายของเรา เป็นการเดินทางของข้อมูลจากอุปกรณ์ Router ฝั่งเครือข่ายของเรา ไปยัง Perimeter Network เข้าสู่วง LAN
พิจารณา Extrusion ภัยคุกคามทางข้อมูล ขา ออกจากระบบเครือข่ายของเรา จากวง LAN ไปสู่ Perimeter Network
อุปกรณ์ที่เราควรพิจารณา เส้นทางการลำเลียงข้อมูลเพื่อใช้ในการสืบหาการกระทำผิดทางอาชญากรรมคอมพิวเตอร์ (Network Forensics)
ทาง ขาเข้า คือ ข้อมูลของ Log ที่เกิดขึ้นจากอุปกรณ์ Internal Router , Network Firewall ,Core Switch , NIDS/IPS Access Switch , Proxy และ อุปกรณ์ Access Point (AP) เป็นต้น

Copyright © SRAN Technology



ข้อมูล ที่เข้า และออกในระดับ Host เป็นข้อมูลจากเครื่องคอมพิวเตอร์ที่ใช้งาน ในระดับ End Point ได้แก่ เครื่องแม่ข่าย (Computer Server) , เครื่องลูกข่าย (Computer Client) , Note book , PDA เป็นต้น
ข้อมูลในระดับ Internet เข้าสู่วง LAN และไปสิ้นสุดที่ End Point
พิจารณา Intrusion ภัยคุกคาม ขา เข้าสู่เครื่องคอมพิวเตอร์ของเรา (Host) เป็นการเดินทางข้อมูลจากเครือข่ายของเรา (LAN) ในจุดต่างๆ เข้าสู่เครื่องคอมพิวเตอร์ ที่อาจเป็นเครื่องแม่ข่าย , เครื่องลูกข่าย หรืออื่นๆ และแสดงผลข้อมูลผ่านระบบคอมพิวเตอร์ปลายทางที่เรียกใช้ข้อมูล
การพิจารณา Extrusion ภัยคุกคาม ขา ออกจากเครื่องคอมพิวเตอร์ของเรา (Host) ผ่านไปยังระบบเครือข่ายของเรา (LAN) ออกสู่ Perimeter Network และเดินทางไปสู่โลกอินเตอร์เน็ท (Internet)
เราควรพิจารณา เส้นทางการลำเลียงข้อมูลเพื่อใช้ในการสืบหาการกระทำผิดทางอาชญากรรมคอมพิวเตอร์ ในส่วนนี้คือ Log ที่เกิดจากอุปกรณ์ End point ได้แก่ เครื่องแม่ข่าย (Server) , เครื่องลูกข่าย (Client) , อุปกรณ์มือถือที่เชื่อมต่อเครือข่ายคอมพิวเตอร์ภายใน ออกสู่อินเตอร์เน็ทได้

การพิจารณาเส้นทางลำเลียงข้อมูลของระบบ SRAN จึงอาศัยหลักการ 3 in 3 out เป็นหลัก



ภาพแสดงแนวคิดการสร้าง SRAN จากทฤษฎี Honeynet Concept , NSM Theory , 3 in 3 Out ตลอดจนการทำ Chain of Custody แบบฉบับการ Forensics ผ่านระบบเครือข่ายคอมพิวเตอร์ SRAN ถูกออกแบบมาจากทฤษฎีเหล่านี้ ประโยชน์เพื่อเฝ้าระวัง และเก็บบันทึกข้อมูลจราจร รวมถึง ย้อนเวลากลับสู่เหตุการณ์ต้องการได้ (Network Time Machine) ภาพนี้จึงเป็นต้นกำเนิดการทำอุปกรณ์ SRAN ในปัจจุบัน

ซึ่งระบบ SRAN จะอยู่บนพื้นฐานองค์ประกอบการเฝ้าสังเกต เฝ้าระวัง พฤติกรรมการใช้งานบนระบบเครือข่าย แบ่งเป็น 3 องค์ประกอบได้ดังนี้
- การเฝ้าระวังข้อมูลที่ไม่ปกติ (Threat Data Traffic)
- การเฝ้าระวังข้อมูลที่ปกติ (Normal Data Traffic)
- การเก็บบันทึกข้อมูล (Recorder)

Copyright © SRAN Technology

1.1 การเฝ้าระวังข้อมูลที่ไม่ปกติ (Threat Data Traffic) ซึ่งเป็นข้อมูลไม่พึงประสงค์ ได้แก่ ข้อมูลที่มีการติดเชื้อไวรัสคอมพิวเตอร์ ข้อมูลที่มีการระบาดของไวรัสคอมพิวเตอร์ หรือที่เรียกว่า Worm ข้อมูลที่มีผลกระทบกับธุรกิจ และการก่อการร้าย (Hacking) การโจรกรรมข้อมูลภายในองค์กร และภายนอกองค์กร การทำลายข้อมูล การดักข้อมูล หรือการแก้ไขข้อมูลให้มีความคลาดเคลื่อนจากความเป็นจริง ซึ่งทั้งหมดนี้ต้องมีระบบวิเคราะห์ภัยคุกคาม และออกรายงานผลให้รับทราบ เพื่อทำแผนรองรับเพื่อแก้ไขสถานะการณ์ฉุกเฉินดังกล่าว

1.2 การเฝ้าระวังการใช้อย่างปกติ (Normal Data Traffic) การใช้งานปกติสามารถแบ่งประเภทได้ดังนี้
การตรวจสภาวะการใช้งานอุปกรณ์ เครื่องแม่ข่าย แล้วมีการแสดงผลลัพธ์ที่บ่งบอกถึง ระดับการใช้ข้อมูลตาม Bandwidth , Protocol (HTTP , SMTP ,POP3 ,IMAP ,P2P ,IM เป็นอย่างน้อย)
การแจ้งผลเตือนระดับการใช้งาน เช่น แจ้งค่าตาม Flow Network / Collector จาก Protocol ICMP , SNMP ได้แก่ ค่า CPU , RAM และ Response Time
การใช้งานตาม Application Protocol ที่สำคัญ ได้แก่

- การใช้งานอินเตอร์เน็ทโดยการเปิดเว็บบราวเซอร์ ผ่าน Protocol HTTP ต้องมีระบบเฝ้าระวัง และวิเคราะห์ เพื่อตรวจสอบลักษณะการใช้งาน ตาม Source / Destination IP หรือ Domain วันที่ เวลาที่ใช้งานงาน รูปแบบการติดต่อว่าเป็นแบบ GET หรือ POST และ Path ที่เปิดเว็บนั้น
- การใช้งานอินเตอร์เน็ทโดยการใช้บริการอีเมลล์ ผ่าน Protocol SMTP , POP3 , IMAP ต้องมีระบบเฝ้าระวังและวิเคราะห์ เพื่อตรวจสอบลักษณะการใช้งาน ตาม Source / Destination IP หรือ Domain วันที่ เวลาที่ใช้งาน รูปแบบการติดต่อว่าเป็นแบบ รับ หรือ ส่ง อีเมลล์ ชื่อหัวเรื่องอีเมลล์ ชื่อเอกสารไฟล์ที่แนบมากับอีเมลล์
- การใช้งานอินเตอร์เน็ทโดยใช้บริการสนทนาออนไลท์ ผ่าน Protocol IM ชนิดต่างๆ ต้องมีระบบเฝ้าระวัง และวิเคราะห์ เพื่อตรวจสอบลักษณะการใช้งาน ตาม Source / Destination IP หรือ Domain วันที่ เวลาที่ใช้งาน รูปแบบการติดต่อ จากโปรแกรมชนิดใด เช่น Yahoo , MSN , ICQ , IRC เป็นต้น
- การใช้งานอินเตอร์เน็ทโดยใช้บริการอื่นๆ ได้แก่ ลักษณะการใช้ VoIP และ P2P ต้องมีระบบเฝ้าระวังและวิเคราะห์ เพื่อตรวจสอบลักษณะการใช้งาน ตาม Source / Destination IP หรือ Domain ระบุวันที่ เวลาที่ใช้ รูปแบบการติดต่อ จากโปรแกรมชนิดใด เช่น SkyP , P2P Program เป็นต้น

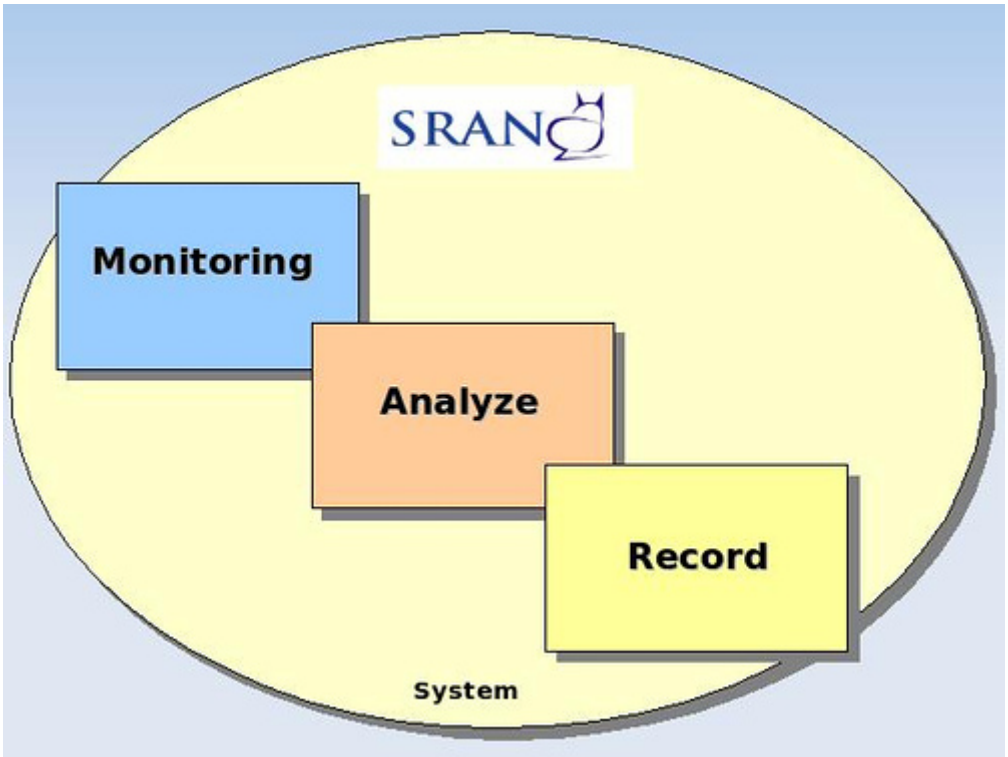
SRAN

หลัก พิจารณา	การใช้เว็บ Web / HTTP / HTTPS	การใช้เมลล์ (E-mail) SMTP / POP3/ IMAP	การสนทนา (IM) Yahoo / MSN / ICQ	FTP	VoIP, P2P
Who	Source / Destination / Domain	Source / Destination / Domain	Source / Destination / Domain	Source / Destination / Domain	Source / Destination / Domain
What	GET or POST	Send or Receive	Chat	Upload / Download	Chat / Upload / Download
Where	URL / IP / Domain	IP / Domain	MSN/Yahoo ICQ/IRC	IP / Domain	IP / Domain
When	Time / Date	Time / Date	Time / Date	Time / Date	Time / Date

1.3 การเก็บบันทึกข้อมูล (Recorder) เพื่อเก็บบันทึกข้อมูลทั้งที่เป็นข้อมูลจราจรที่ปกติ (Normal Data Traffic) และ ข้อมูลจราจรที่ไม่ปกติ (Threat Data Traffic) ที่เป็นรูปของ Raw Data หรือลักษณะที่สามารถดูข้อมูลที่เก็บบันทึกได้ ผ่านทาง Data Base เทคโนโลยี หรือจะเป็น Text files ก็ได้ ในการเก็บบันทึกควรมีการแสดงค่ายืนยันว่ามีความถูกต้อง และแก้ไขไม่ได้นั้น มีกระบวนการเก็บผ่านนโยบายขององค์กร (Security Policy) วิธีปฏิบัติของผู้ปฏิบัติงาน (Operation Security) และมีค่ายืนยันความไม่เปลี่ยนเปลี่ยน (Check sum) เพื่อยืนยันว่า file นั้นไม่มีการแก้ไขหรือเปลี่ยนแปลงได้ (Integrity)

Copyright © SRAN Technology

2. คำนิยามอุปกรณ์ SRAN Security Center คือ USM (Unified Security Monitoring) นั้นคือการเฝ้าระวัง (Monitoring) วิเคราะห์ข้อมูล (Analysis) และ เก็บบันทึกข้อมูล (Record)เหตุการณ์ทั้งปกติ และ ทั้งที่เป็นภัยคุกคามที่เกิดขึ้นบนเครือข่าย



3. หน้าที่อุปกรณ์ SRAN Security Center คือ สำรวจ ตรวจสอบ วิเคราะห์ ประเมินความเสี่ยง ทั้งหมดเพื่อทำการเก็บบันทึกข้อมูล

3.1 สำรวจเครือข่าย โดยเทคโนโลยี Passive Scan เพื่อตรวจดูการใช้งาน Bandwidth ที่ใช้งาน , การใช้งานตาม Protocol ต่างๆ ได้แก่ HTTP (web) , SMTP/POP3 (mail) , Chat , FTP , DNS , DHCP , P2P เป็นต้น

3.2 ตรวจสอบ การใช้งานที่ผิดปกติ (Threat Data Traffic) ซึ่งอาจส่งผลต่อภัยคุกคาม ที่อาจจะเกิดขึ้นบนระบบเครือข่าย ตรวจสอบการใช้งานที่ปกติ (Normal Data Traffic) ที่ใช้งานทั่วไป ได้แก่ การใช้งานเว็บผ่านอินเตอร์เน็ท การใช้งานอีเมลล์ผ่านอินเตอร์เน็ท การเล่นสนทนา Online เป็นต้น

3.3 วิเคราะห์ เมื่อทำการตรวจสอบแล้ว ระบบจะนำผลที่ได้รับมาวิเคราะห์ข้อมูลที่พบบนระบบเครือข่าย เพื่อทำการจับเปรียบเทียบตามฐานข้อมูลที่มีอยู่

Copyright © SRAN Technology

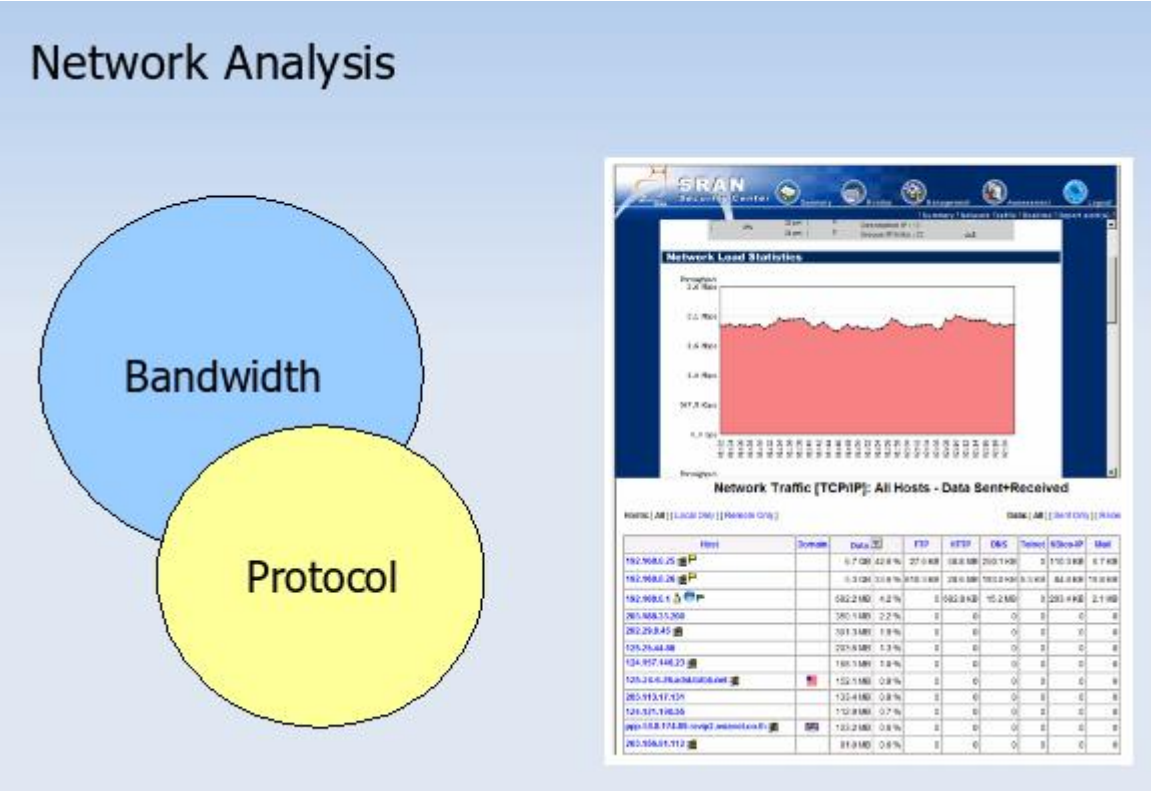
3.4 ประเมินความเสี่ยง หลังจากขั้นตอนการวิเคราะห์ข้อมูล ระบบจะทำการประเมินความเสี่ยงข้อมูลที่ผิดปกติ (Threat Data Traffic) นั้นจัดลำดับความรุนแรง สูง กลาง ต่ำ ทั้งนี้ยังประเมินความเสี่ยง อุปกรณ์เครือข่าย (Devices) เครื่องแม่ข่าย (Server) และ โปรแกรมมิ่งที่ใช้งาน (Application) พร้อมออกรายงานผลให้รับทราบอย่างอัตโนมัติ

3.5 เก็บบันทึกข้อมูล (Data Traffic Recored) ทำการเก็บบันทึกทั้งข้อมูลปกติ และไม่มีปกติ เพื่อทำการดูย้อนหลังตามวัน เวลา ที่ระบุได้ อย่างสะดวกในการสืบหาหลักฐานต่อไปในอนาคต

4. เทคโนโลยี บน SRAN Security Center

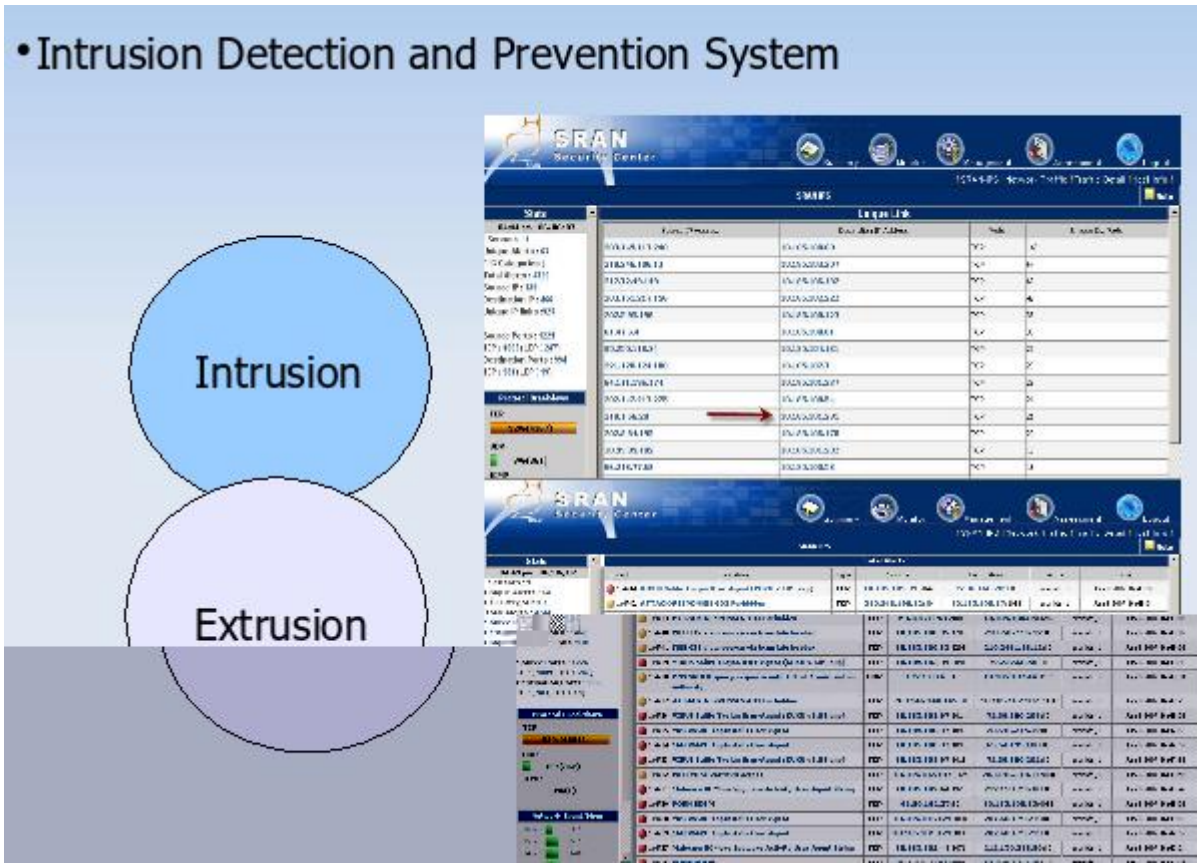
มีคุณสมบัติดังนี้

4.1 เทคโนโลยีการทำ Network Analysis ที่ดูข้อมูล การเข้า และ ออกบนระบบเครือข่าย โดยพิจาณาจาก Bandwidth และ Protocol ที่ใช้งาน



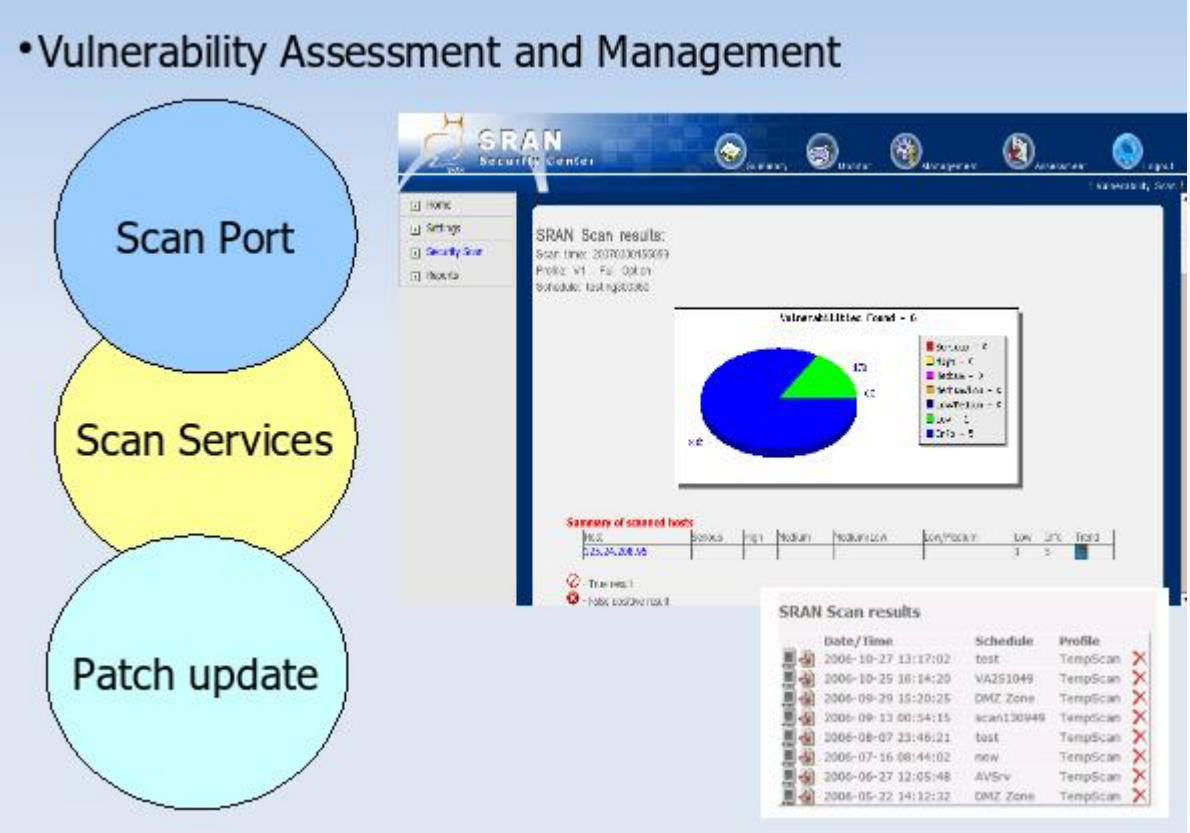
4.2 เทคโนโลยี IDS/IPS (Intrusion Detection / Prevention System) ใช้ในหน้าที่วิเคราะห์ข้อมูลที่ผิดปกติ (Threat Data Traffic) และปกติ (Normal Data Traffic) เพื่อทำการเปรียบเทียบกับฐานข้อมูลที่มีอยู่ ที่วิเคราะห์ว่าเป็นภัยคุกคามชนิดที่เป็นภัยคุกคามจากภายนอกสู่ภายใน (In trusion) และภัยคุกคามจะภายในสู่ภายนอกที่เรียก (Extrusion) ซึ่งในที่จะสามารถทำให้ทราบถึง ภัยคุกคามต่างๆ เช่น Virus/worm , Spam , Spyware , Phishing และภัยคุกคามจากการโจมตีระบบ เช่น DDoS/DoS, Remote Exploit , Brute Fore Password เป็นต้น หากนำอุปกรณ์ SRAN Security Center ติดตั้งแบบ In-line จะสามารถป้องกันภัยคุกคามต่างๆ จะกลายเป็น IPS ในตัวทันที หากนำ SRAN Security Center ติดตั้งแบบดักข้อมูล โดยใช้ความสามารถของอุปกรณ์ Switch มาช่วยก็จะกลายเป็น IDS ตามที่กล่าวมา

Copyright © SRAN Technology



4.3 เทคโนโลยีการเประเมินความเสี่ยง (VA / VM) Vulnerability Assessment & Management ระบบจะสามารถประเมินความเสี่ยงโดยการ Scan Port , Scan Services และ รายงานผลควร Update Patch ได้ ทั้งจะประเมินความเสี่ยงจาก อุปกรณ์ (Devices) , เครื่องแม่ข่าย (Server) และ Application เป็นต้น

Copyright © SRAN Technology



4.4 เทคโนโลยีการเก็บบันทึกข้อมูล (Log Archive) ระบบ SRAN จะสามารถเก็บบันทึกข้อมูล ทั้งที่เป็นข้อมูลไม่ปกติ (Threat Data Traffic) และ ข้อมูลปกติ (Normal Data Traffic)

ส่วนที่เป็นข้อมูลไม่ปกติ (Threat Data Traffic) จะลำดับเหตุการณ์ปัจจุบัน แล้วทำการ Correlation Log ให้สอดคล้องตาม ISO17799 และ พรบ. ว่าด้วยการกระทำผิดทางคอมพิวเตอร์ และเก็บบันทึกเพื่อทำการดูย้อนหลังสืบหาต้นต่อของปัญหาต่อไป

ส่วนที่เป็นข้อมูลปกติ (Normal Data Traffic) จะทำการบันทึกข้อมูลการใช้งานอินเตอร์เน็ท ประกอบด้วย

- การเก็บบันทึกข้อมูลจราจรเกี่ยวกับเว็บ (Internet Web Recorder)
- การเก็บบันทึกข้อมูลจราจรเกี่ยวกับเมล (Internet Mail Recorder)
- การเก็บบันทึกข้อมูลจราจรเกี่ยวกับสนทนา (Internet Chat Recorder)
- การเก็บบันทึกข้อมูลจราจรเกี่ยวกับ FTP (Internet FTP Recorder)
- การเก็บบันทึกข้อมูลจราจรเกี่ยวกับ P2P (Internet P2P Recorder) ซึ่งส่วนนี้จะประกอบด้วยการใช้ VoIP ในบาง Application เช่น Skyp เป็นต้น

ทั้งหมดที่กล่าวนี้ บรรจุไว้ใน **Box เครื่องเดียว ที่เรียกว่า "SRAN Security Center"**

Copyright © SRAN Technology