SRAN
IT Security New Generation

อุปกรณ์ป้องกันและตรวจจับการบุกรุก (Intrusion Prevention System) ภายใต้ชื่อ SRAN เป็นเวลากว่า 15 ปี SRAN ได้รับรางวัลด้านนวัตกรรมมีใบประกาศนียบัตรที่รับรองคุณภาพ SRAN เป็นอุปกรณ์ที่ใช้งานสะดวกโดยไม่จำเป็นต้องมีผู้เชี่ยวชาญระบบจัดเก็บข้อมูลจราจรคอมพิวเตอร์ เป็นแบบสำเร็จรูป พร้อมใช้งาน (Appliance) ทำให้กว่า 500 บริษัท/หน่วยงาน ในประเทศไทย ที่เลือกใช้ SRAN ในการเก็บบันทึกข้อมูลจราจรคอมพิวเตอร์

การติดตั้ง SRAN ทำได้สะดวกโดยไม่ต้องใช้ผู้เชี่ยวชาญทำการติดตั้งแบบ In-line ระหว่างอุปกรณ์ Firewall และ Router หรือ Firewall กับอุปกรณ์ Switch บนระบบเครือข่ายคอมพิวเตอร์ โดยเลือกรุ่นที่เหมาะสมกับองค์กร

SRAN®

(N)etShield

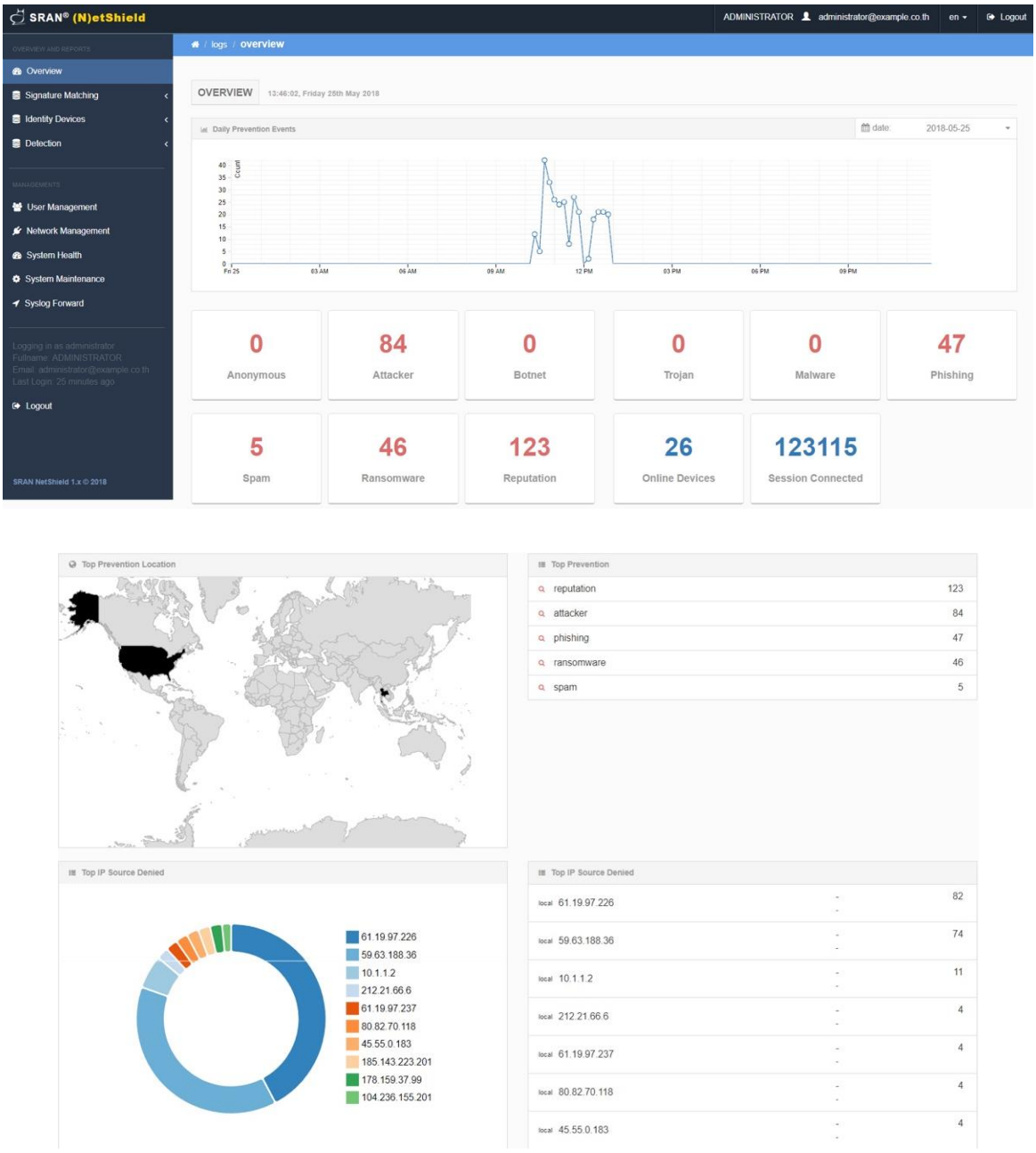
Series NIPS

“ ติด SRAN Netshield แล้วไม่จำเป็นต้องลงโปรแกรมแอนตี้ไวรัสที่เครื่องลูกข่าย (Client) ”

คุณลักษณะพื้นฐาน

1. อุปกรณ์เป็นฮาร์ดแวร์ (Hardware Appliance) ที่ทำการออกแบบเพื่อป้องกันการบุกรุกทางเครือข่าย (Intrusion Prevention System)
2. มีความสามารถตรวจจับวิธีการบุกรุกและป้องกันเครือข่ายได้ดังนี้
   - 2.1) การตรวจจับผ่านระบบ Signature matching
   - 2.2) การตรวจการใช้งาน Protocol / Packet Anomalies
   - 2.3) การตรวจแบบ Statistical anomalies หรือ Application anomalies
   - 2.4) การตรวจ Buffer Overflow
   - 2.5) การตรวจการบุกรุกของ Worm, Virus, Backdoor Program, Trojan Horse, Spyware
   - 2.6) การตรวจสอบการโจมตีด้วยการ Port Scanning
   - 2.7) การตรวจ Packet Analysis
   - 2.8) การตรวจการโจมตีแบบ DDoS/DoS
3. อุปกรณ์สามารถทำงานได้อย่างต่อเนื่อง (Bypass Traffic) โดยช่องสัญญาณ In-line Mode สามารถรับส่งข้อมูลได้ตามปกติ
4. สามารถบริหารจัดการอุปกรณ์ผ่านมาตรฐาน HTTPS หรือ SSH ได้
5. รองรับการใช้งานตามมาตรฐาน IPv6

6. สามารถส่งข้อมูล Log File แบบ Syslog มีซอฟต์แวร์ในการเก็บบันทึกข้อมูลจราจรคอมพิวเตอร์ตามมาตรฐาน มศอ.4003.1-2560
7. มีระบบการกรองเนื้อหาไม่เหมาะสมจากการใช้งานอินเทอร์เน็ตรองรับที่เป็นภาษาไทยได้ จากการเข้าถึงเว็บไซต์ที่ไม่เหมาะสม การค้นหาข้อมูลอันไม่เหมาะสม ได้เป็นต้น
8. ป้องกันการมัลแวร์ เว็บไซต์หลอกลวง กว่า 5 แสนชนิด
9. เป็นอุปกรณ์ที่พร้อมใช้งานและมีเมนูรองรับภาษาไทย



หน้าจอรายงานผลภาพรวมสถานการณ์ที่เกิดขึ้นภายในองค์กรเมื่อทำการติดตั้ง SRAN Net shield

มาตรฐานที่ได้รับจากฮาร์ดแวร์อุปกรณ์ SRAN (Certification)

1. มาตรฐาน มศอ. 4003.1-2560 ระบบเก็บรักษาข้อมูลจราจรคอมพิวเตอร์ตามกฎหมายเล่ม 1 ข้อกำหนดใช้ได้ถึง 8 เมษายน 2562
2. มาตรฐาน ศอ. 2001.2-2553 วิธีการประเมินสมรรถนะ สำหรับ บริภัณฑ์คอมพิวเตอร์และส่วนประกอบเชิงหน้าที่ เล่ม 2 ความร้อนใช้ได้ถึง 8 เมษายน 2562
3. มาตรฐาน ศอ. 2006.2.1-2555 วิธีการประเมินสมรรถนะ สำหรับบริภัณฑ์คอมพิวเตอร์และส่วนประกอบเชิงหน้าที่ เล่ม 2 ส่วนที่ 1 การใช้พลังงานในภาวะใช้กำลังไฟฟ้าต่ำ ใช้ได้ถึง 8 เมษายน 2562
4. มาตรฐาน ศอ. 2006.3-2556 วิธีการประเมินสมรรถนะ สำหรับบริภัณฑ์คอมพิวเตอร์ และส่วนประกอบเชิงหน้าที่ เล่ม 3 การคำนวณและประมวลผลข้อมูล ใช้ได้ถึง 8 เมษายน 2562
5. มาตรฐาน มอก. 1956-2548 บริภัณฑ์เทคโนโลยีสารสนเทศ เฉพาะด้านความปลอดภัยข้อกำหนดทั่วไป ใช้ได้ถึง 8 เมษายน 2562
6. มาตรฐาน มอก. 1956-2553 บริภัณฑ์เทคโนโลยีสารสนเทศ ขีดจำกัดสัญญาณรบกวนวิทยุ ใช้ได้ถึง 8 เมษายน 2562
7. มาตรฐาน มอก. 1448-2544 ความเข้ากันได้ทางแม่เหล็กไฟฟ้า เล่ม 3-2 : ขีดจำกัดสำหรับสิ่งที่ส่งออกมาซึ่งเป็นกระแสฮาร์โมนิก (กระแสไฟฟ้าเข้า 16 แอมแปร์ต่อเฟส) ใช้ได้ถึง 8 เมษายน 262
8. มาตรฐาน ISO 9001:2008 จาก SGS (Thailand) ให้กับการผลิตภัณฑ์ SRAN ในการให้บริการด้านความมั่นคงปลอดภัยข้อมูลสารนเทศภายใต้ผลิตภัณฑ์ ใช้ได้ถึง 14 กันยายน 2561

Add on

RealScan การตรวจสอบและประเมินความเสี่ยงระบบสารสนเทศภายในองค์กร

Compitak การป้องกันการเข้าถึงเว็บไซต์ไม่เหมาะสม ป้องกันไวรัสคอมพิวเตอร์ ป้องกันการเข้าถึงเว็บไซต์หลอกลวง และการค้นหาข้อมูลที่รองรับภาษาไทย

คุณสมบัติอย่างละเอียดในแต่ละรุ่น SRAN NetShield

ลำดับ	คุณสมบัติ	NS50	NS500	NS3000X
1	อุปกรณ์เป็นฮาร์ดแวร์ (Hardware Appliance) ที่ทำการออกแบบเพื่อป้องกันการบุกรุกทางเครือข่าย (Intrusion Prevention System)	✓	✓	✓
2	รองรับการทำงานได้จำนวน Segment	1	3	Custom
3	ความเร็วในการตรวจจับ (Throughput)	600 Mbps	1 Gbps	Custom
4	รองรับ Power Supply แบบ Redundant (Hot Swap)	1	2	2
5	มีความสามารถตรวจจับวิธีการบุกรุกและป้องกันเครือข่ายได้ดังนี้ 1) การตรวจจับผ่านระบบ Signature matching 2) การตรวจการใช้งาน Protocol / Packet Anomalies 3) การตรวจแบบ Statistical anomalies หรือ Application anomalies 4) การตรวจการบุกรุกของ Worm , Virus, Backdoor Program, Trojan Horse , Spyware, Buffer Overflow , DDoS/DoS , Port Scanning	✓	✓	✓
6	อุปกรณ์สามารถทำงานได้อย่างต่อเนื่อง (Bypass Traffic) โดยช่องสัญญาณ In-line Mode สามารถรับส่งข้อมูลได้ตามปกติ		✓	✓
7	สามารถบริหารจัดการอุปกรณ์ผ่านมาตรฐาน HTTPS หรือ SSH ได้	✓	✓	✓
8	รองรับการใช้งานตามมาตรฐาน IPv6	✓	✓	✓
9	สามารถส่งข้อมูล Log File แบบ Syslog มีซอฟต์แวร์ในการเก็บบันทึกข้อมูลจราจรคอมพิวเตอร์ตามมาตรฐาน มศอ.4003.1-2560	✓	✓	✓
10	มีระบบการกรองเนื้อหาไม่เหมาะสมจากการใช้งานอินเทอร์เน็ตรองรับที่เป็นภาษาไทยได้ จากการเข้าถึงเว็บไซต์ที่ไม่เหมาะสม การค้นหาข้อมูลอันไม่เหมาะสม ได้เป็นต้น	✓	✓	✓
11	ป้องกันการมัลแวร์ เว็บไซต์หลอกลวง กว่า 5 แสนชนิด และสามารถป้องกันการค้นหาคำไทยที่ไม่เหมาะสมจากโปรแกรม Search engine ได้	✓	✓	✓
12	ตรวจสอบเครื่องคอมพิวเตอร์หรืออุปกรณ์สื่อสารแบบพกพาแบบอัตโนมัติ เพื่อที่รายงานผลช่องโหว่ (Vulnerability) และอาจจะสร้างความเสียหายให้แก่ระบบเครือข่ายคอมพิวเตอร์	✓	✓	✓
13	รายงานการตรวจสอบโดยทำการสแกนหาความเสี่ยงได้รับผลการตรวจสอบจากค่ามาตรฐานสากลดังนี้ ค่า CVE ค่าดัชนีชี้วัดความเสี่ยง CVSS เวอร์ชั่น 3 , ค่าความไม่ปลอดภัยของซอฟต์แวร์ CWE , ค่า CAPEC	✓	✓	✓
14	รับประกันการอัพเดทฐานข้อมูลเพื่อรู้เท่าทันภัยคุกคามรูปแบบที่ทันสมัย	1 Years	1 Years	1 Years