Data Sheet Thai

Not only PROTECTION, but LEGALIZE your business NOW!

SRAN *Light* IT Security New Generation

LOWER COST MORE SECURE

SRAN

info@gbtech●co●th

GLOBAL TECH
www.gbtech.co.th

SRAN®

SRAN Light LT50 Hybrid บัญชีรายชื่อนวัตกรรมไทย

รหัสรายชื่อบัญชีนวัตกรรมไทย หมายเลข 050001

ชื่อสามัญของผลงานนวัตกรรมไทย : อุปกรณ์เฝ้าระวังป้องกันภัยคุกคามบนระบบสารสนเทศและเก็บข้อมูลจราจรคอมพิวเตอร์

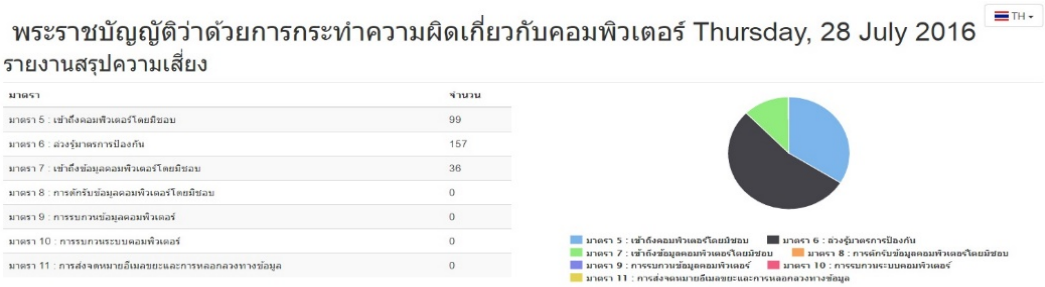
(IT Security Monitoring and Log File Collection)

ทำไมต้องมีอุปกรณ์เฝ้าระวังภัยคุกคามทางเครือข่ายสารสนเทศและจัดเก็บข้อมูลจราจรคอมพิวเตอร์ ?

มีเหตุผลหลัก 2 ประการที่หน่วยงานรัฐและเอกชนมีความจำเป็นต้องมีอุปกรณ์เฝ้าระวังภัยคุกคามทางเครือข่ายสารสนเทศและจัดเก็บข้อมูลจราจรคอมพิวเตอร์ คือ

1.1 ตามพรบ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 มาตรา 26 กำหนดให้ผู้ให้บริการ (ตามกฎหมายกำหนดให้ ผู้ให้บริการหมายถึง หน่วยงาน ห้างร้าน องค์กร ใดๆ ก็ตามที่จัดให้มีการเข้าถึงเครือข่ายอินเตอร์เน็ตให้กับคนในองค์กรนั้นหรือบุคคลอื่นทั่วไปสามารถใช้งานได้) ทำให้หน่วยงานจำเป็นต้องมีอุปกรณ์ในการจัดเก็บข้อมูลจราจรฯ และกระทรวงไอซีที โดย NECTEC ได้กำหนดมาตรฐานสำหรับอุปกรณ์จัดเก็บข้อมูลจราจรฯ คือ มาตรฐาน มศอ. 4003.1-2560 โดยมาตรฐานนี้ถูกระบุในเกณฑ์ราคากลางและคุณลักษณะพื้นฐานครุภัณฑ์คอมพิวเตอร์ ที่ประกาศโดยกระทรวงไอซีที ที่หน่วยงานรัฐหากมีการจัดซื้อ จัดจ้าง ต้องใช้เป็นเกณฑ์ในการเขียนข้อกำหนด

1.2 เนื่องจากภัยคุกคามทางไซเบอร์ (Cyber Attack) ที่ปัจจุบันเพิ่มขึ้นอย่างรวดเร็ว ด้วยหลากหลายรูปแบบและมีความซับซ้อนมากขึ้น โดยล่าสุดที่ประชุม World Economic Forum ปี 2015 ได้จัดให้ Cyber Attack เป็น 1 ใน 10 ความเสี่ยงที่มีความสำคัญของโลก รัฐบาลเองก็ให้ความสำคัญกับเรื่องนี้เป็นอย่างมาก เนื่องจากภัยคุกคามทางเครือข่ายคอมพิวเตอร์ไม่เพียงนำความซึ่งความเสียหายทางเศรษฐกิจ แต่ยังเกี่ยวข้องกับความมั่นคง และการกระทำที่อาจเกี่ยวข้องกับการกระทำความผิดตามพรบ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 ซึ่งเป็นความผิดอาญาอีกด้วย



ภาพหน้าจอแสดงรายงานผลความเสี่ยงตามมาตรา 5 - 11 ที่อาจส่งผลต่อการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

ทำไมต้องเป็น SRAN ?

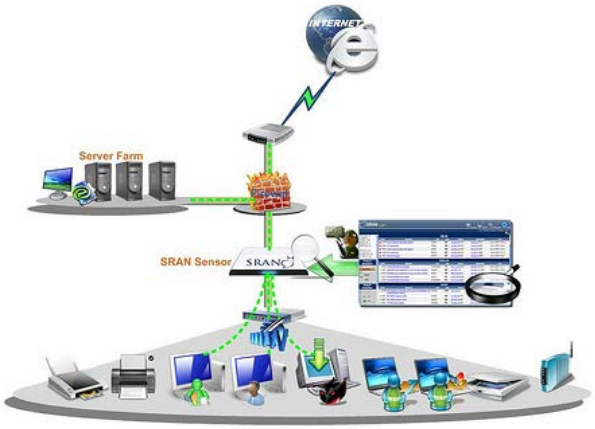
1. SRAN มีคุณสมบัติ 2 ส่วน ในอุปกรณ์เดียว คือ

1.1 สามารถจัดเก็บข้อมูลจราจรคอมพิวเตอร์ฯ ตามพรบ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 และได้รับมาตรฐาน มศอ. 4003.1-2560

1.2 สามารถเฝ้าระวังภัยคุกคาม โดยมีความสามารถหลักๆ คือ

- การสำรวจข้อมูลแบบอัตโนมัติเพื่อระบุตัวตนอุปกรณ์บนระบบเครือข่ายคอมพิวเตอร์ (Automatic Identification Device)
- การวิเคราะห์และเทคโนโลยีในการตรวจจับความผิดปกติข้อมูล (Detect and Analyzer)
- การวิเคราะห์ข้อมูลจราจรคอมพิวเตอร์(Log Analytic)
- การเฝ้าติดตามปริมาณการใช้งานข้อมูลภายในองค์กร (Bandwidth Monitoring)
- การค้นหาข้อมูลการใช้งานในเครือข่ายในเชิงลึก (Deep Search)
- การบริหารจัดการค่าการประเมินความเสี่ยง (Vulnerability Management)
- การเก็บบันทึกข้อมูลจราจรคอมพิวเตอร์และดูย้อนหลัง (Log Record and Archive)
- การเก็บบันทึกค่าสำหรับให้ IT Audit ในการตรวจสอบข้อมูลและใช้เป็นหลักฐาน (Log Audit)

2. SRAN ได้ขึ้นบัญชีนวัตกรรมไทย (ฉบับเพิ่มเติมครั้งที่ ๓) กรกฎาคม ๒๕๕๙ (http://www.bb.go.th/bbweb/?page_id=7809) โดยสิทธิประโยชน์สำหรับผลิตภัณฑ์ที่อยู่ในบัญชีนวัตกรรมไทยคือ “ส่วนงานราชการ รัฐวิสาหกิจ หน่วยงานตามกฎหมายว่าด้วยการบริหารราชการส่วนท้องถิ่น หน่วยงานอื่น ซึ่งกฎหมายบัญญัติให้มีฐานะเป็นราชการบริหารส่วนท้องถิ่น หรือหน่วยงานอื่นของรัฐ สามารถจัดซื้อจัดจ้างจากผู้ขายหรือผู้ให้บริการที่มีรายชื่อตามบัญชีนวัตกรรมไทย โดยวิธีกรณีพิเศษหรือที่เรียกชื่ออย่างอื่นซึ่งมีวิธีการทำนองเดียวกันตามระเบียบว่าด้วยการพัสดุที่หน่วยงานนั้นๆ ถือปฏิบัติ”



ภาพการออกแบบอุปกรณ์ SRAN Light LT50 Hybrid

SRAN Light LT50 Hybrid

คุณสมบัติทางเทคนิค (Feature)

1. การสำรวจข้อมูลแบบอัตโนมัติเพื่อระบุตัวตนอุปกรณ์บนระบบเครือข่ายคอมพิวเตอร์(Automatic Identification Device)

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

1.2 รายงาน BYOD (Bring Your Own Device) แสดงค่าอุปกรณ์พกพาที่พยายามติดต่อเข้าใช้งานเครือข่ายคอมพิวเตอร์ขององค์กร ได้โดยแยก Desktop (คอมพิวเตอร์พกพา เช่นโน้ตบุ๊ก) และมือถือ (Mobile) และรู้ว่าใครนำเครื่องพกพามาใช้งานภายในเครือข่าย

1.3 รายงานการเก็บบันทึกเป็นค่าอุปกรณ์ (Device Inventory) โดยแยกการเก็บค่าจากอุปกรณ์ (Device) ชื่อผู้ใช้งานจากระบบ Active Directory , จาก Radius ค่าจากการ Authentication , ค่า IP Address ผู้ใช้งาน , ค่า MAC Address , แผนก (Department) , ยี่ห้อ รุ่นอุปกรณ์ เป็นต้น

1.4 รายงานการเก็บบันทึกค่าซอฟต์แวร์ (Software Inventory) ที่ใช้ ซึ่งในส่วนซอฟต์แวร์จะทำการค้นพบประเภทซอฟต์แวร์ที่ใช้ได้แก่ ซอฟต์แวร์ประเภทเว็บบราวเซอร์ , ซอฟต์แวร์ประเภทมัลติมีเดีย , ซอฟต์แวร์ประเภทใช้งานในออฟฟิศ ซอฟต์แวร์ที่ไม่เหมาะสมเช่น โปรแกรม Bitorrent ก็สามารถตรวจและค้นพบได้

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

1.6 การสำรวจเครื่องที่มีโอกาสเปลี่ยนค่า Leak path เชื่อมต่อกับ gateway อื่นที่ไม่ใช่ขององค์กร

2. การวิเคราะห์และเทคโนโลยีในการตรวจจับความผิดปกติข้อมูล(Detect and Analyzer)

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 รายงานการตรวจจับการใช้งานโปรแกรมดาวโหลดไฟล์ขนาดใหญ่ที่ส่งผลกระทบต่อประสิทธิภาพการใช้งานโดยรวมภายในองค์กร

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

3. การวิเคราะห์ข้อมูลจราจรคอมพิวเตอร์ (Log Analytic)

3.1 Threat event correlation รายงานการวิเคราะห์ข้อมูลจากการรวบรวมเหตุการณ์ภัยคุกคามที่เกิดขึ้นภายในระบบเครือข่ายคอมพิวเตอร์องค์กร

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

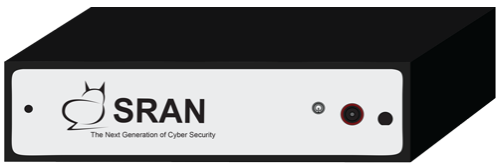
3.3 Executive summary (Hour, Daily, Monthly) รายงานการจัดสรุปสถานการณ์ทั้งหมดให้ระดับผู้บริหารองค์กร โดยกำหนดได้ที่เป็นรายชั่วโมง รายวัน และรายเดือน

3.4 Thai Cyber Law Act รายงานความเสี่ยงที่มีโอกาสเข้าข่ายตามมาตรฐานความผิดเกี่ยวกับการใช้งานคอมพิวเตอร์ภายในองค์กร ซึ่งเป็นจุดเด่นสำคัญที่มีความแตกต่างกับสินค้าอื่นและช่วยให้ออกรายงานสำหรับผู้บริหารได้อย่างครบถ้วน

4. การเฝ้าติดตามปริมาณการใช้งานข้อมูลภายในองค์กร (Bandwidth Monitoring)

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

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



ภาพอุปกรณ์ฮาร์ดแวร์ระบบเฝ้าระวังภัยคุกคามข้อมูลสารสนเทศและการ เก็บบันทึกข้อมูลจราจรคอมพิวเตอร์ที่ได้รายชื่อบัญชีนวัตกรรมไทยจาก สำนักงบประมาณ

4.3 Application Monitoring (Software bandwidth usage) รายงานการใช้แอพพลิเคชั่นและปริมาณการใช้ข้อมูลภายในองค์กรกว่า 1,000 ชนิด ได้แก่ SAP , ERP , Orcal , Skype, Microsoft และ Enterprise แอพพลิเคชั่น 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

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

5. การค้นหาข้อมูลการใช้งานในเครือข่ายในเชิงลึก (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

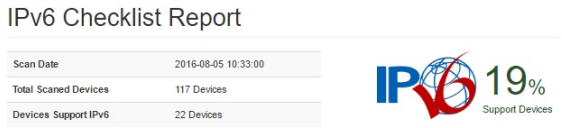
ภาพช่องรับสัญญาณข้อมูลที่ผ่านระบบเครือข่ายคอมพิวเตอร์

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



ภาพการรายงานผลการประเมินอุปกรณ์ภายในองค์กรที่รองรับ IPv6 ตามข้อกำหนดของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารที่ให้ภาครัฐตรวจสอบอุปกรณ์ที่รองรับค่า IPv6 ซึ่งจะทำให้หน่วยงานที่ใช้ SRAN ได้คุณสมบัติในการตรวจสอบเป็นรายงานทำให้สะดวกและลดค่าใช้จ่ายภายในองค์กรโดยไม่จำเป็นต้องจ้างผู้เชี่ยวชาญเข้ามาประเมิน

7. การเก็บบันทึกข้อมูลจราจรคอมพิวเตอร์และดูย้อนหลัง (Log Record and Archive)

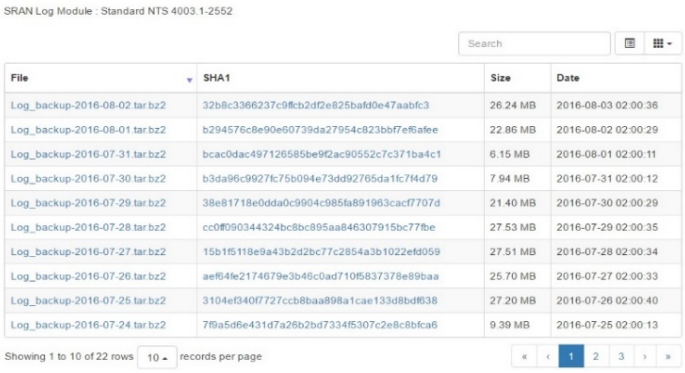
7.1 การเก็บบันทึกข้อมูลแบบ Raw data การเก็บข้อมูลที่เป็นประโยชน์ในการสืบสวนสอบสวนและการหาผู้กระทำความผิด ด้วยการเก็บบันทึกที่สามารถทำได้แบบ Hybrid ซึ่ง SRAN เป็นต้นฉบับของการทำวิธีนี้ คือการรับข้อมูลจราจรคอมพิวเตอร์แบบ Passive mode และ รับค่าจากอุปกรณ์อื่นได้

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 การเก็บบันทึกข้อมูลสามารถเก็บได้ตามจำนวนวันที่กฎหมายกำหนด หรือกรณีที่ต้องการเก็บเพิ่มก็สามารถขยายพื้นที่ในการจัดเก็บได้โดยมีซอฟต์แวร์SRAN Logger Module ที่ผ่านมาตรฐาน NECTEC มศอ.๔๐๐๓.๑ – ๒๕๖๐ (NECTEC STANDARD NTS 4003.1-2560) ระบบเก็บบันทึกข้อมูลจราจร ตาม พ.ร.บ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ ปี 2560 ให้มาด้วย

7.5 การเก็บบันทึกข้อมูลมีการยืนยันความถูกต้องข้อมูล Integrity hashing confidential files



หน้าแสดงค่า Log file ที่ถูกต้องตามมาตรฐาน มศอ. และสามารถไปใช้ในชั้นศาลได้

8. การเก็บบันทึกค่าสำหรับให้ IT Audit ในการตรวจสอบข้อมูลและใช้เป็นหลักฐาน (Log Audit)

8.1 การเก็บบันทึกค่า Active Directory Login active / Login fail

8.2 การเก็บบันทึกค่า SSH Login active / Login fail

คุณสมบัติเพิ่มเติม SRAN Light LT50 Hybrid

1. เป็นอุปกรณ์ Appliance หรืออุปกรณ์คอมพิวเตอร์ที่ได้มาตรฐาน สามารถเก็บรวบรวมเหตุการณ์ (logs or Events) ที่เกิดขึ้นในอุปกรณ์ที่เป็น appliances และ non-appliances เช่น Firewall, Network Devices ต่างๆ ระบบปฏิบัติการ ระบบ appliances ระบบเครือข่าย และระบบฐานข้อมูล เป็นต้น ได้อย่างน้อย 3 อุปกรณ์ต่อระบบ โดยสามารถแสดงผลอยู่ภายใต้รูปแบบ (format) เดียวกันได้
2. มีระบบการเข้ารหัสข้อมูลเพื่อใช้ยืนยันความถูกต้องของข้อมูลที่จัดเก็บตามมาตรฐาน SHA-1
3. สามารถเก็บ Log File ในรูปแบบ Syslog ของอุปกรณ์ เช่น Router, Switch, Firewall, VPN, Server ได้
4. สามารถบริหารจัดการอุปกรณ์ผ่านมาตรฐาน HTTPS, Command Line Interface และ SSH ได้
5. สามารถจัดเก็บ log file ได้ถูกต้อง ตรงตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ ฉบับที่มีผลบังคับใช้ โดยได้รับรองมาตรฐานการจัดเก็บและรักษาความปลอดภัยของ log file ที่ได้มาตรฐานของศูนย์อิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (มศอ. 4003.1-2560)
6. สามารถทำการสำรองข้อมูล (Data Backup) ไปยังอุปกรณ์จัดเก็บข้อมูลภายนอก เช่น Tape หรือ DVD หรือ External Storage เป็นต้น ได้
7. มีระบบ Alert System รองรับการแจ้งเตือนผ่าน E-mail ไปยังผู้ดูแลระบบเมื่อมีเหตุการณ์ความเสี่ยงในระดับสูง เช่น ไวรัสคอมพิวเตอร์เข้าสู่ระบบ หรือมีการโจมตีทางไซเบอร์ (Cyber Attack) ที่สร้างความเสียหายให้แก่องค์กร

มาตรฐานที่ได้รับจากฮาร์ดแวร์อุปกรณ์ SRAN และขั้นตอนในผลิตภัณฑ์ (Certification)

1. มาตรฐาน มศอ. 4003.1-2552 ระบบเก็บรักษาข้อมูลจราจรคอมพิวเตอร์ตามกฎหมายเล่ม 1 ข้อกำหนดใช้ได้ถึง 8 เมษายน 2562
2. มาตรฐาน ศอ. 2001.2-2553 วิธีการประเมินสมรรถนะ สำหรับบริภัณฑ์คอมพิวเตอร์และส่วนประกอบเชิงหน้าที่ เล่ม 2 ความร้อน ใช้ได้ถึง 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 ในการให้บริการด้านความมั่นคง ปลอดภัยข้อมูลสารสนเทศภายใต้ผลิตภัณฑ์ ใช้ได้ถึง 14 กันยายน 2561

สิทธิประโยชน์

ส่วนราชการ รัฐวิสาหกิจ หน่วยงานตามกฎหมายว่าด้วยการบริหารราชการส่วนท้องถิ่น หน่วยงานอื่น ซึ่งมีกฎหมายบัญญัติให้มีฐานะเป็นราชการบริหารส่วนท้องถิ่น หรือหน่วยงานอื่นของรัฐ **สามารถจัดซื้อจัดจ้างจากผู้ขายหรือผู้ให้บริการที่มีรายชื่อตามบัญชีนวัตกรรมไทย โดยวิธีกรณีพิเศษที่เรียกชื่ออย่างอื่นซึ่งมีวิธีการทำนองเดียวกันตามระเบียบว่าด้วยการพัสดุที่หน่วยงานนั้น ๆ ถือปฏิบัติ**

อ้างอิงสิทธิประโยชน์จากเอกสาร บัญชีรายชื่อนวัตกรรมไทยฉบับเดือนมกราคม 2559 หน้าที่ 5

คุณสมบัติ SRAN Light LT50 Hybrid

Product	LT50
Capacity and Performance	**Custom depend on customer*
Logs Capacity per Day	1GB
Current Counter (Session/Hour)	950,000
Normal Log Rate (Event/Second)	1,000
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	✔

คุณสมบัติ SRAN Light LT50 Hybrid

Product	LT50
Feature	
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 7.4 Log Archive more 90 Day 7.5 Integrity hashing confidential files	✔
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	Desktop
Total Interfaces	4x1 GbE
Storage Capacity	250 GB
Compliance	
Safety Certifications	CE, FCC

GLOBAL TECH
www.gbtech.co.th

บริษัท โกลบอลเทคโนโลยี อินทิเกรเทด จำกัด
48/6 ซอยแจ้งวัฒนะ 14 ทุ่งสองห้อง หลักสี่ กรุงเทพฯ 10210
โทรศัพท์ : +66 2 982 5454 โทรสาร: +66 2 982 4004 อีเมล์: info@gbtech.co.th