ด้านโฆษณาและเผยแพร่ : ครุภัณฑ์เพื่อการโฆษณาและเผยแพร่

รหัส : 05020001

ชื่อสามัญของผลงานนวัตกรรมไทย : อุปกรณ์เฝ้าระวังป้องกันภัยคุกคามบนระบบสารสนเทศและเก็บข้อมูลจราจรคอมพิวเตอร์ (IT Security Monitoring and Log File Collection)

ชื่อทางการค้าของผลงานนวัตกรรมไทย : SRAN Light รุ่น LT50 Hybrid

หน่วยงานที่พัฒนา : บริษัท สราญ เทคโนโลยี จำกัด

บริษัทผู้รับการถ่ายทอด : บริษัท โกลบอลเทคโนโลยีอินทิเกรเทด จำกัด

หน่วยงาน บริษัท หรือผู้ขึ้นบัญชีนวัตกรรมไทย : บริษัท โกลบอลเทคโนโลยีอินทิเกรเทด จำกัด

ช่วงเวลาที่ขึ้นทะเบียน : กรกฎาคม 2559 – กรกฎาคม 2562 (3 ปี)

คุณสมบัตินวัตกรรม:

ใช้เก็บบันทึกข้อมูลจราจรบนระบบเครือข่ายคอมพิวเตอร์ ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และใช้ดูพฤติกรรมการใช้งานอินเตอร์เน็ตของผู้ใช้งานในเครือข่าย ทั้งในส่วนของการใช้งานปกติแต่สร้างปัญหาคุณภาพการใช้งานต่อระบบเครือข่าย ตลอดจนภัยคุกคามทั้งจากผู้ใช้งานในเครือข่ายเองและภายนอกเครือข่าย โดยมีความสามารถของระบบดังต่อไปนี้

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) แสดงค่าอุปกรณ์พกพาที่พยายามติดต่อเข้าใช้งานเครือข่ายคอมพิวเตอร์ขององค์กรได้โดยแยก Desktop (คอมพิวเตอร์พกพา เช่นโน้ตบุ๊ค) 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), ยี่ห้อรุ่นอุปกรณ์ เป็นต้น

1.4 รายงานการเก็บบันทึกค่าซอฟต์แวร์ (Software Inventory) ที่ใช้ซึ่งในส่วนซอฟต์แวร์จะทำการค้นพบประเภทซอฟต์แวร์ที่ใช้ได้แก่ ซอฟต์แวร์ประเภทเว็บบราวเซอร์, ซอฟต์แวร์ประเภทมัลติมีเดีย, ซอฟต์แวร์ประเภทใช้งานในออฟฟิศ, ซอฟต์แวร์ที่ไม่เหมาะสมเช่นโปรแกรม Bittorrent 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 ได้แก่ การ 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 BittorrentDetection 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 และที่องค์กรของเราติดต่อไปยังโลกภายนอกเป็นการตรวจสอบข้อมูลวิ่งเข้าสู่องค์กร (Incoming data) และข้อมูลที่ถูกนำออกนอกองค์กร (Out going 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

4.3 Application Monitoring (Software bandwidth usage) รายงานการใช้แอพลิเคชั่นและปริมาณการใช้ข้อมูลภายในองค์กรกว่า 1,000 ชนิด ได้แก่ SAP, ERP, Orcal, Skyp, 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

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 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 systemรองรับ Protocol DNP3, Mobus (ModiconCommunication 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 หรือกรณีที่ต้องการเก็บเพิ่มก็สามารถขยายพื้นที่ในการจัดเก็บได้ โดยมีซอฟต์แวร์ SRAN Logger Module ที่ผ่านมาตรฐาน NECTEC มศอ. 4003.1 - 2552 (NECTEC STANDARD NTS 4003.1 - 2552) ระบบเก็บบันทึกข้อมูลจราจร ตาม พ.ร.บ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ ปี 2550 ให้มาด้วย

7.5 การเก็บบันทึกข้อมูลมีการยืนยันความถูกต้องข้อมูล Integrity hashing confidential files

8. การเก็บบันทึกค่าสำหรับให้ IT Audit ในการตรวจสอบข้อมูลและใช้เป็นหลักฐาน (Log Audit)

8.1 การเก็บบันทึกค่า Active Directory Login active / Login fail

8.2 การเก็บบันทึกค่า SSH Login active / Login fail

++++++++++++++++++++