Softnix
DATA PLATFORM
for Security Analytics

Softnix Data Platform for Security Analytics

คือ Big Data Platform ที่ออกแบบมาสำหรับการนำเข้าและจัดเก็บข้อมูลได้หลากหลายชนิด ซึ่งได้แก่ ข้อมูลแบบโครงสร้าง (Structure Data) ข้อมูลไร้โครงสร้าง (Unstructured Data) โดยใช้ เทคโนโลยี Big Data จึงทำให้รองรับการเติบโตของข้อมูลและการขยายระบบได้ในอนาคต Softnix Data Platform มีข้อแตกต่างจาก Big Data Platform อื่นๆทั่วไป คือมี Application สำเร็จรูปที่ออกแบบมาเรียบร้อยสำหรับการจัดการกับข้อมูลในแต่ละด้านโดยเฉพาะ

SDP FOR SECURITY ANALYTICS คืออะไร ?

Softnix Data Platform for Security Analytics เรียกชื่อย่อว่า SDP for Security Analytics คือระบบวิเคราะห์เหตุการณ์ด้านความปลอดภัยในเครือข่ายคอมพิวเตอร์ โดยทำงานในลักษณะของ Security Information and Event Management หรือ SIEM โดยใช้เทคโนโลยีของ Big Data Analytics เพื่อปลดล็อคข้อจำกัดของ SIEM แบบเดิมและตอบสนองต่อปริมาณข้อมูลและความหลากหลายของรูปแบบข้อมูลในระบบ IT Infrastructure ในปัจจุบัน โดยทำการวิเคราะห์หาแนวโน้มของเหตุการณ์และตรวจสอบเหตุการณ์ด้านความปลอดภัยที่เกิดขึ้น เช่น การเข้าถึงโดยไม่ได้รับอนุญาติ ข้อมูลการเข้าถึงของผู้ใช้งาน เหตุการณ์ที่ผิดปกติ (Abnormal)

CHALLENGES

ปัจจุบันความเสี่ยง IT คือความเสี่ยงธุรกิจ อันเนื่องมากจากความสำคัญของระบบ IT ดังนั้นความปลอดภัยในระบบ IT จึงมีส่วนสำคัญมากลำดับต้นๆ ที่ผู้บริหาร IT จะต้องคำนึง

Big Data Analytics & Security Analytics

เริ่มต้นจากความต้องการพื้นฐานของ IT Security คือ ความสามารถในการตรวจพบหรือ Detection สิ่งที่ Big Data Analytic ช่วยคือการเพิ่มความสามารถในการ Detection เหตุการณ์ด้านความปลอดภัย ซึ่งเทคโนโลยีประเภท SIEM หรือ Security Information and Event Management เดิมสามารถทำได้โดยการสร้างกฎเงื่อนไข เพื่อตรวจสอบรูปแบบของข้อมูลที่ตรงตามเงื่อนไข มาในยุคของ Big Data ความซับซ้อนและปริมาณข้อมูลที่มากขึ้น เทคโนโลยีจึงต้องพัฒนาเพื่อรองรับการสร้างเงื่อนไขตามความสัมพันธ์จาก Data Source ตั้งแต่ Server และ Application Logs ไปจนถึง Network Events และ User Activity จึงเกิด Advanced Analytics ที่เหนือกว่า Rules Based ที่ผ่านมาแล้วทำงานบน Big Data Platform ที่รองรับปริมาณข้อมูลมหาศาล จึงเรียกได้ว่า Big Data Security Analytics คือ **NEXT GENERATION OF SECURITY TOOLS**

ประโยชน์ที่ได้รับ

Visibility เพิ่มความสามารถในการรับรู้ว่า มีเหตุการณ์ด้านความปลอดภัยอะไรบ้างในเครือข่าย ช่วยให้ตรวจสอบเหตุการณ์ที่ผ่านมาและนำไปกำหนดนโยบายควบคุมหรือป้องกันต่อไป

Security Monitor ตรวจสอบและติดตามเหตุการณ์ภัยคุกคามในเครือข่ายคอมพิวเตอร์ โดยสามารถกำหนดค่าการตรวจสอบเพิ่มเติมได้

Law & Compliance ปัจจุบัน LAW & Compliance ต่างๆ เช่น ISO27001, PCI-DSS, HIPAA, FISMA, Sarbanes-Oxley (SOX) หรือ กฎหมาย พ.ร.บ. คอมพิวเตอร์ พ.ศ 2560 ล้วนกำหนดให้จัดเก็บข้อมูลด้าน IT เป็นระยะเวลาเพิ่มมากขึ้น การจัดเก็บข้อมูล IT บน Big Data Platform จึงเป็นได้มากกว่าเพียงจัดเก็บ แต่ยังสามารถนำไปวิเคราะห์เพื่อใช้งานเป็นประโยชน์ในด้าน IT Operation Services ได้อีกด้วย

SECURITY LOG ที่รองรับในการวิเคราะห์

Anti-malware solution, Intrusion Detection system (IDS), Intrustion prevention system (IPS), Anti-DDos solution, Web application firewall (WAF), Data loss prevention system (DLP), Endpoint security (AV/EDR), Next generation firewall (NGFW), Unified Threat Management system (UTM) และนอกจากนั้นยังรองรับ Audit Event Log และ Authentication Log จาก Operating System (OS) อีกด้วย

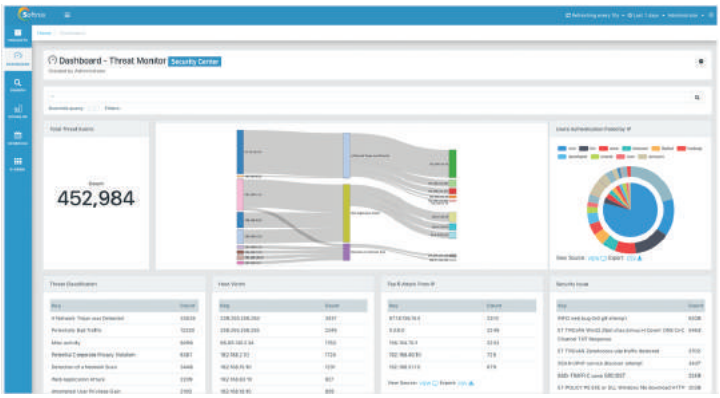
www.softnix.co.th
sales@softnix.co.th

KEY FEATURES

คุณสมบัติทางเทคนิค

Management System

Web based management ผ่านช่องทางเข้ารหัส SSL โดยรองรับการ Authentication ผ่าน Local System ได้ พร้อมทั้งการกำหนดอนุญาติสิทธิ์ในแบบ Role Based Access Control



Aggregation

รองรับการรวบรวมและสรุปผลข้อมูลเพื่อให้ทราบถึงจำนวนเหตุการณ์ที่เกิดขึ้น รวมทั้งลดปริมาณข้อมูลที่เหมือนกันด้วย

Normalization

รองรับการจัดรูปแบบข้อมูลเหตุการณ์ให้อยู่ในรูปแบบเดียวกัน เพื่อเป็นมาตรฐานเดียวกันและง่ายต่อการค้นหาโดยระบุตาม Field ที่ต้องการโดยเฉพาะ

Distributed Search

ระบบ SEARCH ENGINE รองรับการค้นหาได้ทั้งแบบ Simple Search คือการระบุเพียง Keyword ที่ต้องการ หรือ Complex Search คือการกำหนดเงื่อนไข เช่น AND OR NOT เพื่อค้นหา Log ได้อย่างแม่นยำ พร้อมกับการแสดงกราฟแผนภูมิเหตุการณ์ตามช่วงเวลาจากการค้นหาทันที

Predefined Report

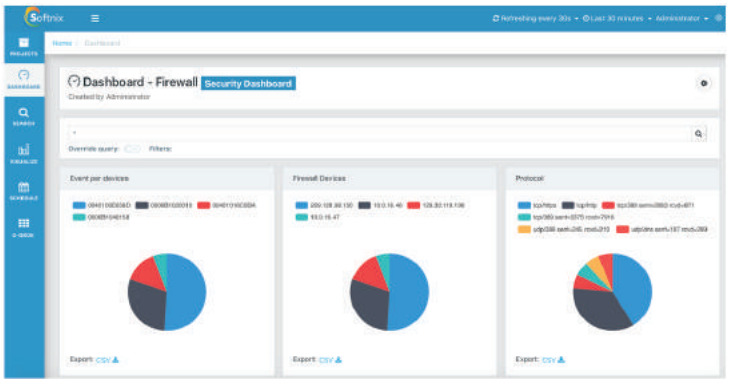
รองรับการสร้างรายงานที่กำหนดรูปแบบไว้หรือสามารถปรับแต่งเพิ่มเติมได้ตามต้องการ โดยรองรับการส่งออกในรูปแบบ PDF, CSV หรือการส่งแบบ HTML ไปยังอีเมล์ที่ต้องการโดยการกำหนดเวลาล่วงหน้า

Event Alert

รองรับการกำหนดค่าแจ้งเตือนเหตุการณ์ตามเงื่อนไขที่กำหนดไปยังผู้ดูแลความปลอดภัย ผ่าน Email, SNMP Trap และ Syslog ได้

Client Agent

รองรับการทำงานร่วมกับ Softnix Agent และ Softnix Logger ซึ่งเป็น Centralized Log Server โดยทำการรวบรวมและส่งต่อเหตุการณ์สำคัญเข้ามาวิเคราะห์ด้านความปลอดภัย อีกทั้งกระบวนการส่งข้อมูลยังรองรับการทำ Event Caching เพื่อป้องกันข้อมูลสูญหายระหว่างทางและ Bandwidth Management เพื่อประหยัด Traffic ในการส่งข้อมูลอีกด้วย



www.softnix.co.th
sales@softnix.co.th