Nozomi Networks Platform

แพลตฟอร์มเดียว ที่ช่วยให้คุณมองเห็นและดูแลความปลอดภัยของระบบ OT และ IoT ทั้งหมดได้ในที่เดียว

โซลูชันความปลอดภัยทางไซเบอร์ของ Nozomi Networks ถูกออกแบบมาเพื่อปกป้องระบบที่มีความสำคัญสูงสุดในทุกกลุ่มอุตสาหกรรม ไม่ว่าจะเป็นระบบ OT หรือ IoT ที่ใช้ในการทำงานในปัจจุบัน

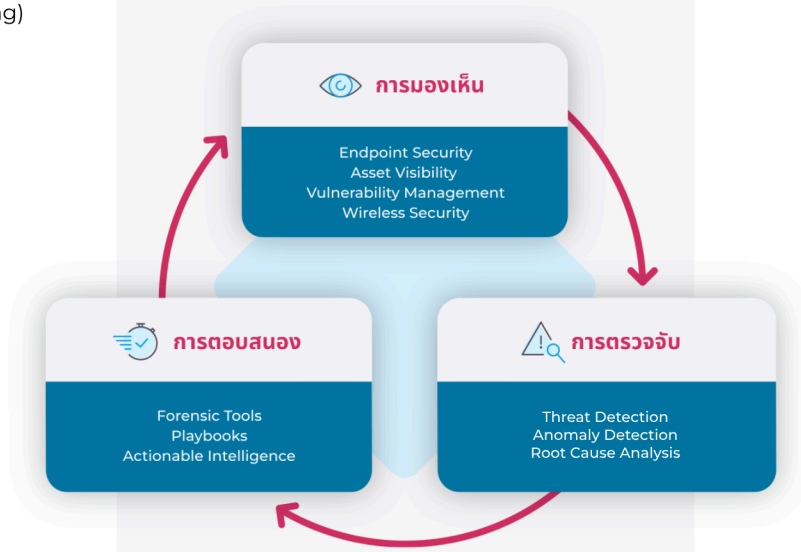
เราโดดเด่นด้วยการรวมความสามารถในการมองเห็นทั้งระบบเครือข่าย (แบบใช้สายและไร้สาย) เข้ากับระบบดูแลความปลอดภัยที่ตัวอุปกรณ์ (Endpoint) พร้อมระบบตรวจจับภัยคุกคามและการวิเคราะห์ด้วย AI เพื่อให้คุณสามารถตอบโต้ภัยไซเบอร์ได้อย่างรวดเร็วและมีประสิทธิภาพมากกว่าที่เคย

ประโยชน์ที่ลูกค้าจะได้จากเราคือ:

- การรวมศูนย์ข้อมูลเพื่อให้คุณมองเห็น (Visibility) และเฝ้าระวัง (Monitoring) ทั้งอุปกรณ์ในระบบเครือข่ายและอุปกรณ์ปลายทาง (Endpoint) ภายในสภาพแวดล้อม OT และ IoT ของคุณได้แบบเบ็ดเสร็จในที่เดียว
- ความสามารถในการรองรับ Protocol ต่างๆ ที่มากกว่าพร้อมการวิเคราะห์ที่ครอบคลุมและแม่นยำ ไม่ว่าจะเป็น Protocol ในฝั่ง OT, IoT หรือ IT ที่มีรูปแบบให้เลือกหลากหลาย
- การใช้ข้อมูลเชิงลึกจาก AI (AI-driven insights) และการวิเคราะห์หาสาเหตุที่แท้จริง (Root cause analysis) จะช่วยเป็นแนวทางให้คุณแก้ไขปัญหา (Remediation) ได้อย่างตรงจุดและแม่นยำ
- มีการพิสูจน์การใช้งานจริงมาแล้วจากสภาพแวดล้อมของลูกค้าที่ใหญ่และซับซ้อนที่สุดมาแล้วทั่วโลก
- การเชื่อมต่อการทำงานร่วมกับระบบ SIEM และ SOC ได้อย่างราบรื่น (Seamless Integration) เพื่อช่วยอุดช่องว่างในการมองเห็นสถานะการทำงานและปิดช่องโหว่ด้านความปลอดภัยของระบบให้สมบูรณ์
- การวิเคราะห์เชิงลึกทางนิติวิทยาศาสตร์ทางดิจิทัล (Forensic Analysis) อย่างละเอียด เพื่อใช้ในการรับมือเหตุการณ์ภัยคุกคาม (Incident Response) และช่วยให้คุณได้รับข้อมูลเชิงลึกที่แม่นยำยิ่งขึ้น
- เครือข่ายพันธมิตรระดับโลก (Global Partner Ecosystem) ที่พร้อมสนับสนุนทุกความต้องการ ทั้งด้านการจัดซื้อสินค้าและการให้บริการครอบคลุมทั่วทุกภูมิภาค

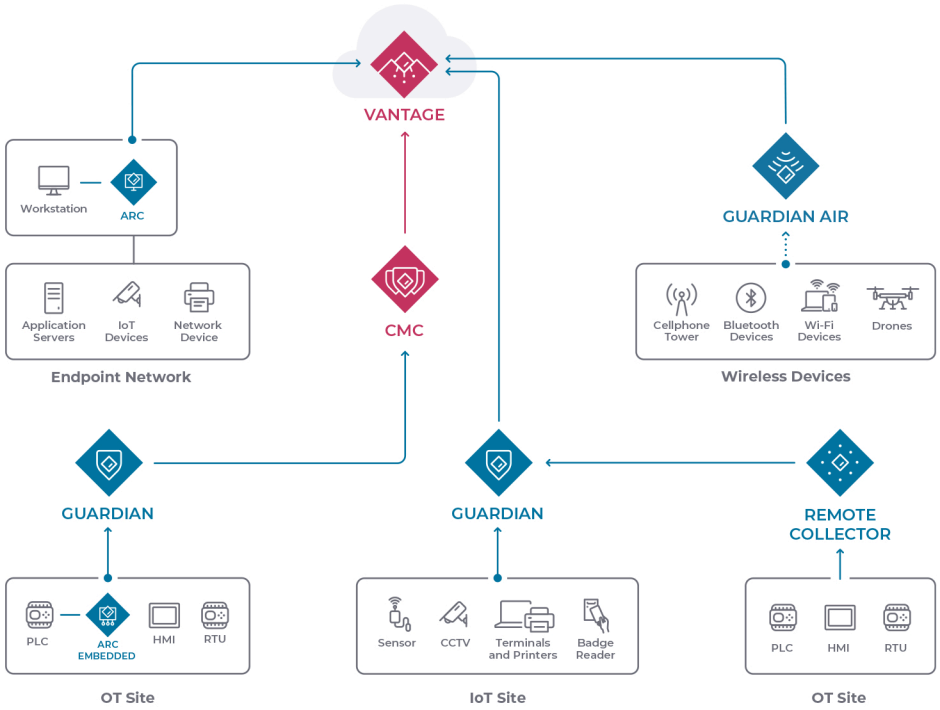
การทำงานของแพลตฟอร์ม Nozomi Networks ถูกออกแบบมาโดยอ้างอิงตามแผนการรับมือเหตุการณ์ภัยคุกคาม (Incident Response Lifecycle) ซึ่งประกอบด้วย 3 ระยะสำคัญ คือ การมองเห็น (Visibility), การ ตรวจจับ (Detection) และการตอบโต้ (Response)

แพลตฟอร์มของเรามาพร้อมฟีเจอร์สำคัญที่รองรับการทำงานครอบคลุมทั้งด้านการบริหารจัดการ (Admin), ด้านความปลอดภัย (Security) และด้านการจัดการระบบเครือข่าย (Networking) โดยแบ่งฟังก์ชันการใช้งานออก ตามระยะต่างๆ (Phases) ดังที่อธิบายไว้ ด้านล่างนี้



ออกแบบโซลูชันที่เหมาะกับคุณ

แพลตฟอร์มของ Nozomi มีองค์ประกอบ (Components) และรูปแบบการติดตั้ง (Form factors) ที่หลากหลายทำให้คุณสามารถเลือกติดตั้งและขยายระบบ (Scale) ได้อย่างยืดหยุ่น ทั้งในรูปแบบ On-premises (ติดตั้งในพื้นที่ของตัวเอง) หรือบน Cloud เพื่อให้ครอบคลุมทุกสภาพแวดล้อม ทั้งในส่วนของโรงงานอุตสาหกรรม และระบบเครือข่ายขององค์กร



MANAGEMENT

VANTAGE

โซลูชันรูปแบบ SaaS ที่ช่วยรวบรวมการตรวจสอบความปลอดภัย (Security Monitoring) และการจัดการความเสี่ยง (Risk Management) ทั้งหมดมาไว้ในที่เดียว

FIPS COMPLIANT

CENTRAL MANAGEMENT CONSOLE

การรวมศูนย์ข้อมูลเพื่อให้คุณสามารถมองเห็น (Visibility) และบริหารจัดการ (Management) การทำงานของ Guardian Sensors ที่ติดตั้งอยู่ตามสาขาหรือพื้นที่ต่างๆ (Distributed Sites) ได้จากจุดเดียว

NETWORK SENSORS

GUARDIAN

เซนเซอร์ที่ถูกออกแบบมาเพื่อให้มองเห็นทุกอย่างที่เกิดขึ้นในระบบเครือข่ายได้อย่างครอบคลุม

ANSSI-CERTIFIED | FIPS COMPLIANT

GUARDIAN AIR

เซนเซอร์แบบ Plug and Play ที่ติดตั้งง่ายและใช้งานได้ทันที เพื่อช่วยเพิ่มความสามารถในการมองเห็น (Visibility) และเฝ้าระวัง (Monitoring) อุปกรณ์ต่างๆ ที่เชื่อมต่อผ่านระบบไร้สาย

REMOTE COLLECTOR

เซนเซอร์ที่ใช้พลังงานต่ำ (Low-resource) สำหรับติดตั้งในพื้นที่ห่างไกล นอกชายฝั่ง (Offshore) หรือพื้นที่ที่มีการกระจายตัวสูง

ENDPOINT SENSORS

ARC

เพิ่มประสิทธิภาพการเก็บข้อมูลและการมองเห็นทุกจุดเสี่ยงบนอุปกรณ์ต่างๆ ได้ครอบคลุมทุกการโจมตีบนอุปกรณ์ปลายทาง (Endpoint Attack Surfaces)

ARC EMBEDDED

ยกระดับความปลอดภัยและการมองเห็น (Visibility) ของระบบ OT/IoT ให้เหนือชั้นกว่าเดิมด้วยเซนเซอร์ตรวจจับความปลอดภัยตัวแรกของโลกที่ฝังตัวลึกเข้าไปถึงระดับล่างสุดของเครือข่ายระบบควบคุมอุตสาหกรรม (ICS)

ANALYSIS & INTELLIGENCE

VANTAGE IQ

การวิเคราะห์ข้อมูลด้วยเทคโนโลยี AI ที่ช่วยให้ทีม Security สามารถปิดช่องโหว่ด้านความปลอดภัยและตอบโต้ภัยคุกคามได้อย่างรวดเร็ว

THREAT INTELLIGENCE

ตรวจจับภัยคุกคามและช่องโหว่ใหม่ๆที่เกิดขึ้นในระบบ OT และ IoT พร้อมรองรับการใช้งานร่วมกับแพลตฟอร์มอื่นๆ

SMART POLLING

การทำ Active Polling เพื่อระบุตัวตนของอุปกรณ์ ที่ไม่มีการเคลื่อนไหว (Non-communicating assets) และตรวจหาอุปกรณ์แปลกปลอม (Rogue devices) ที่แอบเข้ามาเชื่อมต่อในระบบ

TI EXPANSION PACK

POWERED BY MANDIANT

ยกระดับการป้องกันด้วยการรวมข้อมูลภัยคุกคามจาก Mandiant เพื่อให้คุณได้รับข้อมูลเชิงลึกแบบเรียลไทม์ เกี่ยวกับภัยคุกคามที่เกิดขึ้นกับระบบ IT, OT และอุปกรณ์ IoT

ASSET INTELLIGENCE

ค่อยอัปเดตข้อมูลล่าสุดเกี่ยวกับอุปกรณ์ต่างๆ (Assets) ในระบบ และตรวจจับความผิดปกติ (Anomalies) ที่เกิดขึ้นอยู่เสมอ

หากต้องการข้อมูลเพิ่มเติม สามารถเข้าไปดูรายละเอียดได้ที่
nozominetworks.com/products

Nozomi Networks ช่วยปกป้องระบบโครงสร้างพื้นฐานสำคัญระดับโลกจากภัยคุกคามทางไซเบอร์ โดยเป็นแพลตฟอร์มที่มีความโดดเด่นในการรวมความสามารถด้านการมองเห็นทั้งในส่วนของ Network และ Endpoint เข้าด้วยกัน พร้อมระบบตรวจจับภัยคุกคามและการวิเคราะห์ด้วย AI ที่ช่วยให้การตอบสนองต่อเหตุการณ์ต่างๆ ทำได้รวดเร็วและมีประสิทธิภาพมากขึ้น ลูกค้าทั่วโลกจึงไว้วางใจให้เราช่วยลดความเสี่ยงและความยุ่งยากในการดูแลระบบ พร้อมกับช่วยเสริมสร้างความแข็งแกร่งให้ธุรกิจสามารถดำเนินต่อไปได้อย่างต่อเนื่อง (Operational Resilience) โดยไม่สะดุด

NOZOMI NETWORKS

nozominetworks.com