BlueZebra
Network Security

ThreatBook

เกี่ยวกับ
THREATBOOK

ThreatBook เป็นผู้ให้บริการชั้นนำด้านการตรวจจับและตอบสนองต่อภัยคุกคามทางไซเบอร์ที่ขับเคลื่อนโดย TI และ AI เราบุกเบิกแนวทางใหม่ เพื่อส่งมอบข่าวกรองด้านความปลอดภัยที่มีความเที่ยงตรงสูง ดำเนินการได้อย่างมีประสิทธิภาพ และบูรณาการความสามารถเข้ากับการตรวจจับภัยคุกคามตลอดอายุการใช้งาน ความสามารถในการตอบสนองต่อระบบและเหตุการณ์เพื่อเพิ่มพลังการป้องกันบนคลาวด์ เครือข่าย และอุปกรณ์ปลายทาง ช่วยให้องค์กรบรรลุผลสำเร็จ ประสิทธิภาพสูงในการตอบสนองต่อภัยคุกคาม ลดความซับซ้อน และปรับปรุงการดำเนินการด้านความปลอดภัย

การตรวจจับและตอบสนองเครือข่ายที่ใช้ CTI ที่ดีที่สุด

ความท้าทายที่เกิดขึ้นของการตรวจจับเครือข่าย

ยากที่จะระบุความเสี่ยงในสินทรัพย์

ยากที่จะป้องกันการโจมตี 0 วัน

ไม่มีประโยชน์ในการตรวจสอบการแจ้งเตือน

การโจมตีเป็นแบบอัตโนมัติมากขึ้น

แพลตฟอร์มการตรวจจับภัยคุกคาม-TDP THREAT DETECTION PLATFORM

TDP ใช้ประโยชน์จากข้อมูลภัยคุกคามชั้นนำของอุตสาหกรรม มอบความสามารถด้านความปลอดภัยเครือข่ายที่มีประสิทธิภาพสูงสุด การตรวจจับความเที่ยงตรงสูงในการโจมตีที่ซับซ้อนและการตอบสนองอัตโนมัติช่วยให้องค์กรต่างๆรับมือกับความท้าทายหลักในการปฏิบัติการรักษาความปลอดภัยแนวหน้า

ThreatBook

การป้องกันความเสี่ยง

การมองเห็นที่ครอบคลุม : รับการมองเห็นเครือข่ายแบบเรียลไทม์ รวมถึงพอร์ต บริการ แอปพลิเคชัน โดเมน ที่เกี่ยวข้องกับสินทรัพย์ และพฤติกรรม การวิเคราะห์ข้อมูลที่ละเอียดอ่อนและการอัพโหลดและดาวน์โหลดไฟล์

การลดพื้นผิวการโจมตี : ระบุความเสี่ยงที่สำคัญอย่างชาญฉลาดในแอปพลิเคชันที่เพิ่งเปิดตัว ทางเข้าสาธารณะ พอร์ทัลการเข้าสู่ระบบ บริการคลาวด์ และ API ความช่วยเหลือปรับนโยบายการบริหารความเสี่ยงให้เหมาะสม

การติดตามความเสี่ยงด้านสินทรัพย์ที่ปรับแต่งได้ : บรรลุการบริหารความเสี่ยงที่ยืดหยุ่นและรวมศูนย์ตามสถานการณ์ความปลอดภัยต่างๆ และความต้องการเฉพาะของทีม SecOps

การตรวจจับที่แม่นยำ

การตรวจจับภัยคุกคาม Zero-day : ตรวจจับการโจมตีแบบ Zero-day ทั่วไปอย่างแม่นยำ รวมถึงช่องโหว่แบบ Zero-day แบบไฟล์โดยใช้ประโยชน์จากเครื่องที่มีประสิทธิภาพสูง การเรียนรู้และแซนด์บ็อกซ์บนคลาวด์

การตรวจจับโฮสต์ที่ถูกบุกรุก : ระบุโฮสต์ที่ถูกบุกรุกอย่างแม่นยำโดยรวมการวิเคราะห์ตามกฎเข้ากับข่าวกรอง IOC ที่มีความเที่ยงตรงสูง

เสียงการแจ้งเตือนที่จำเป็น : เปิดเผยภัยคุกคามที่สำคัญที่สุดด้วยการวิเคราะห์ที่มีประสิทธิภาพของการโจมตีที่กำลังดำเนินอยู่ ซึ่งได้รับการปรับปรุงด้วยบริบทเพื่อปรับปรุงความแม่นยำของการแจ้งเตือน

การวิเคราะห์แบบเรียลไทม์

การวิเคราะห์เส้นทางการโจมตี : รวบรวมเหตุการณ์ในไทม์ไลน์อย่างชาญฉลาดเพื่อแยกแยะเส้นทางการโจมตีของแฮ็กเกอร์และวิถีกิจกรรมอย่างชัดเจน ทำให้การวิเคราะห์ความสัมพันธ์ง่ายขึ้น

การวิเคราะห์หลายมิติ : ดำเนินการวิเคราะห์ภัยคุกคามที่ครอบคลุมจากมุมมองของผู้โจมตี กองหลัง และผู้แจ้งเตือน พร้อมด้วยการวิเคราะห์ด้วยภาพ ท่าทางการรักษาความปลอดภัย

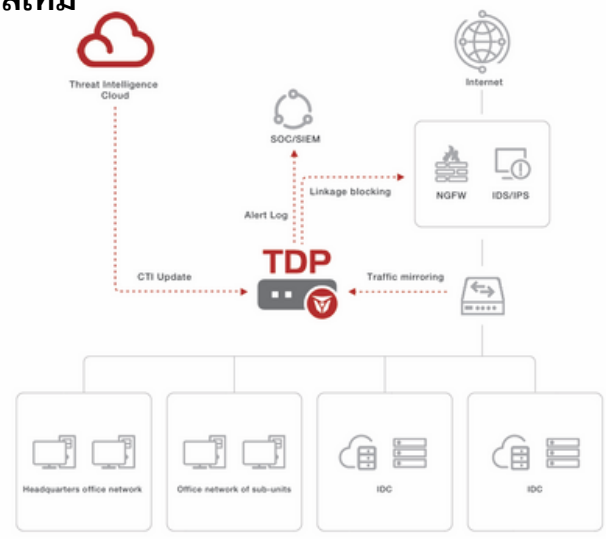
การทำโปรไฟล์ผู้โจมตี : วิเคราะห์และแยกรูปแบบพฤติกรรมการโจมตีโดยอัตโนมัติเพื่อสร้างโปรไฟล์ผู้โจมตี

การตอบสนองอัตโนมัติ

การบล็อกและรีเซ็ต TCP : รับรู้อัตราการบล็อกการรีเซ็ต TCP สูงโดยใช้กลไกเซสชัน TCP เพื่อส่งแพ็กเก็ตการรีเซ็ตไปยัง IP ที่ถูกโจมตีและโฮสต์ภายในพร้อมกัน

การสืบสวนอัตโนมัติ : ตรวจพิสูจน์หลักฐานอัตโนมัติเพื่อระบุโปรแกรมที่เป็นอันตรายและกระบวนการมัลแวร์ที่ทำงานอยู่ผ่าน TDP Agent

การบล็อกไฟร์วอลล์ : ผสานรวมกับไฟร์วอลล์ได้อย่างราบรื่น กำหนดค่านโยบายการบล็อกไฟร์วอลล์ผ่าน TDP แบบเรียลไทม์



More than 1,500 enterprises choose TDP for NDR

<0.003%	<3%	>81%	99%
FALSE POSITIVE RATE	UNDERREPORTING RATE	ZERO-DAY DETECTION RATE	TCP RESET BLOCKING RATE

Gartner Peer Insights. A Strong Performer in Gartner Peer Insights™

sales@bluezebra.co.th www.bluezebra.co.th