LOGPOINT

BlueZebra Network Security

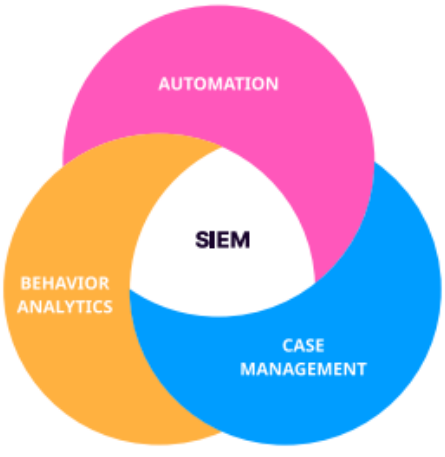
LOGPOINT SIEM

Security analysts สามารถเปลี่ยน SIEM เข้าสู่แพลตฟอร์มการป้องกันทางไซเบอร์โดยการรวม SIEM, SOAR และ UEBA เข้าด้วยกันความสามารถ Logpoint SIEM เป็นแพลตฟอร์มการจัดการกิจกรรมการรักษาความปลอดภัยแบบครบวงจรสำหรับองค์กรและ MSSP เร่งการตรวจจับภัยคุกคาม การสืบสวน และการตอบสนองด้วยส่วนเสริมที่ง่ายดาย แทนที่จะใช้แบบสแตนด์อโลนต่างๆ ผลิตภัณฑ์ต่างๆ ทีมงาน SOC จะรวมชุดข้อมูลจากแหล่งที่มาที่แตกต่างกันมาไว้ในแพลตฟอร์มที่รวมเข้าด้วยกันและได้รับการมองเห็นอย่างเต็มรูปแบบผ่านโครงสร้างพื้นฐานด้านไอที

ระบบ SIEM ของ Logpoint – วิธีการทำงาน

SIEM ซึ่งย่อมาจาก Security Information and Event Management คือกระบวนการนำเข้าข้อมูลบันทึกจากระบบที่แตกต่างกัน จากนั้นเชื่อมโยงข้อมูลนั้นเพื่อพยายามค้นหาตัวบ่งชี้ของการประนีประนอม/การโจมตี หรือรูปแบบของพฤติกรรม ปัญหาเดียวของแนวทางนี้คือลักษณะการใช้งานทางเทคนิคขั้นสูง ซึ่งนำไปสู่บริษัทจำนวนมากที่ละทิ้งเครื่องมือรักษาความปลอดภัยเครือข่ายที่มีการจัดการที่สำคัญ

ระบบ SIEM ของ Logpoint ได้รับการออกแบบตั้งแต่ต้นจนจบให้เรียบง่าย ยืดหยุ่น และปรับขนาดได้ โดยมอบเครื่องมือการออกแบบ การใช้งาน และการรวมที่มีประสิทธิภาพ เพื่อเปิดการใช้งานเครื่องมือรักษาความปลอดภัยเครือข่ายให้กับทุกธุรกิจ ซึ่งหมายความว่าสถาปัตยกรรมสามารถขยายได้อย่างต่อเนื่องด้วยฟังก์ชันเพิ่มเติมโดยไม่จำเป็นต้องออกรุ่นใหญ่เต็มรูปแบบ เพื่อรองรับความต้องการที่เพิ่มขึ้นและเปลี่ยนแปลงของธุรกิจของคุณต่อไป



ระบบ Logpoint สร้างขึ้นจากกลุ่มผู้เช่าเฉพาะ:

ไม่มีบริษัทใดควรถูกจำกัดด้วยปริมาณข้อมูลที่สามารถนำเข้าสู่ระบบ SIEM ได้ หลักการทางสถาปัตยกรรมที่เรียบง่ายเพื่อให้สามารถใช้งานซอฟต์แวร์ได้รวดเร็วและมีประสิทธิภาพยิ่งขึ้น การสนับสนุนระดับโลกพร้อมให้บริการทุกวันตลอด 24 ชั่วโมง เพื่อช่วยให้ลูกค้าได้รับประโยชน์สูงสุดจากระบบ SIEM

Logpoint Architecture

ซอฟต์แวร์ Logpoint SIEM สำหรับการรักษาความปลอดภัยเครือข่ายที่ได้รับการจัดการสามารถแบ่งออกเป็นสามโมดูลหลักที่ให้ฟังก์ชันการทำงานที่คาดหวังจากระบบ SIEM โดยทั่วไป ส่วนประกอบเหล่านี้สามารถจัดส่งได้ภายในอุปกรณ์ทางกายภาพเครื่องเดียว หรือแยกออกเป็นเซิร์ฟเวอร์ทางกายภาพ/เสมือนได้มากเท่าที่เหมาะสมกับความต้องการทางธุรกิจ

องค์ประกอบหลักสามประการของแพลตฟอร์ม Logpoint ได้แก่:

-LogPoint Collectors Collectors มีหน้าที่รับผิดชอบในการนำเข้า การทำให้เป็นมาตรฐาน และการเพิ่มคุณค่าของข้อมูลบันทึกจากแหล่งบันทึกที่แตกต่างกันเข้าสู่แพลตฟอร์ม LogPoint ซึ่งสามารถทำได้ด้วยอนุกรมวิธานเดี่ยวของ LogPoint และปลั๊กอินที่คอมไพล์แล้ว ซึ่งจะทำให้ไฟล์บันทึกใดๆ เป็นมาตรฐานในรูปแบบคู่คีย์/ค่ามาตรฐานของ LogPoint เพื่อการจัดเก็บข้อมูลระยะยาว ด้วยการทำให้ข้อมูลบันทึกเป็นมาตรฐานเมื่อมีการนำเข้า (แทนที่จะทำการค้นหา) LogPoint สามารถเร่งกระบวนการค้นหาและความสัมพันธ์ได้

-LogPoint Backend แบ็กเอนด์ของระบบ LogPoint เป็นโซลูชันการจัดเก็บข้อมูลที่ใช้ NOSQL ซึ่งหมายความว่าข้อมูลทั้งหมดจะถูกจัดเก็บไว้ในไฟล์แบบแฟลต ทำให้สามารถค้นหาได้ในเวลาไม่กี่วินาที จากนั้นสถาปัตยกรรมนี้จะถูกแบ่งออกเป็นพื้นที่เก็บข้อมูลแต่ละแห่งตามที่ลูกค้ากำหนด ตามความเหมาะสมกับความต้องการทางธุรกิจมากที่สุด ที่เก็บข้อมูล (repos) เหล่านี้สามารถจัดการนโยบายการเก็บรักษาได้เป็นรายบุคคล ซึ่งหมายความว่าการใช้ repos อย่างสมเหตุสมผลสามารถช่วยให้ธุรกิจประหยัดได้มหาศาลบนโครงสร้างพื้นฐานการจัดเก็บข้อมูล แพลตฟอร์ม LogPoint ยังช่วยให้คุณสามารถย้ายข้อมูลภายใน repo ไปยังชั้นพื้นที่จัดเก็บข้อมูลที่แตกต่างกันได้โดยอัตโนมัติเมื่อข้อมูลมีอายุมากขึ้น จนกระทั่งถึงเวลาที่ข้อมูลนั้นไม่จำเป็นอีกต่อไป เมื่อข้อมูลดังกล่าวสามารถถูกลบได้โดยอัตโนมัติ

-LogPoint Search head การค้นหาเป็นที่ที่ลูกค้าจะพัฒนาเนื้อหาแบบกำหนดเองที่แยกค่าจากข้อมูลบันทึกดิบและมาตรฐานนั้น กลไก การวิเคราะห์บันทึกในตัวจะใช้เนื้อหานี้เพื่อตรวจจับและแจ้งเตือนเหตุการณ์สำคัญในระบบของคุณโดยอัตโนมัติ เหตุการณ์ที่ได้รับการตรวจสอบสามารถมีความหลากหลายมาก และอาจรวมถึงการโจมตีที่กำลังดำเนินอยู่ ระบบที่ถูกบุกรุก กิจกรรมภายในที่เป็นอันตราย ประสิทธิภาพการทำงานที่ลดลง และอื่นๆ อีกมากมาย

In Logpoint SIEM, the alerts are mapped to the MITRE ATT&CK framework

Key benefits

-ง่ายต่อการปรับใช้: ในฐานะแพลตฟอร์ม SaaS การเตรียมความพร้อมและการใช้งานเป็นกระบวนการที่เรียบง่าย ทำให้ LogpointSIEM พร้อมให้บริการโดยมีระยะเวลารอคอยสินค้าน้อยที่สุด

-ใช้งานง่าย: การจัดส่งบนคลาวด์จะลบไฟล์ความยุ่งยากในการบำรุงรักษาและอัพเดตระบบช่วยให้คุณเพื่อเน้นเรื่องความปลอดภัย

-แพลตฟอร์มแบบครบวงจร: โดยการเพิ่มข้อมูลภัยคุกคามทางธุรกิจบริบทและความเสี่ยงด้านเอนทิตี การแจ้งเตือนที่อ่อนแอกลายเป็นสิ่งที่มีความหมายการสอบสวนและการตอบสนองที่รวดเร็ว

-การปรับปรุงผลิตภัณฑ์อย่างต่อเนื่อง: ทีมงานเฉพาะของนักวิจัยด้านความปลอดภัยจะอัปเดตผลิตภัณฑ์เป็นประจำความสามารถในการตรวจจับและการตอบสนอง เพิ่มความคล่องตัวของคุณเพื่อจัดการกับภูมิทัศน์ภัยคุกคามที่กำลังเกิดขึ้น

-เครื่องมือเดียวรักษาความปลอดภัยทุกด้านของธุรกิจ: Logpoint SIEM รวมและทำให้การตรวจจับเหตุการณ์เป็นแบบอัตโนมัติการสืบสวนและกระบวนการตอบสนองอย่างมากปรับปรุงประสิทธิภาพ SOC และลดความเสี่ยงในการปฏิบัติตามข้อกำหนด

Endpoint Sensor

Threat Intelligence

Single Taxonomy

Log sources & Integrations