CASE STUDY

Empowering Automated Investigations with Trellix, Cyberuptive, and AWS

Trellix Professional Services, in collaboration with the innovative managed detection and response Cyberuptive, embarked on a groundbreaking initiative to revolutionize the landscape of automated investigations. By synergizing the capabilities of Trellix XDR solution with advanced language models hosted on AWS Sagemaker, they achieved remarkable insights and efficiencies in security analysis. This partnership transformed operational efficiency and underscored the importance of concentrating on security research rather than the intricacies of scaling up language models.

Cyberuptive, a renowned name in the cybersecurity domain, specializes in offering outsourced managed security services and managed detection and response solutions. Armed with a team of security experts and a cutting-edge US-based Security Operations Center (SOC), Cyberuptive assists businesses of all sizes with comprehensive security advisory, compliance, and management support services. Cyberuptive aims to ease the challenges of maintaining advanced security measures in the face of cyber uncertainty.

Companies turn to Cyberuptive to relieve the burdens of day-to-day security operations and seek guidance on cost-effective technological decisions for optimal protection. The company possesses its own adept parsing team and US-based SOC analysts. When companies confront skill shortages and lack in-house specialization, Cyberuptive becomes the go-to source for bridging these gaps effectively and providing invaluable expertise.

Customer Challenge

Becoming a leading Managed Security Service Provider (MSSP) requires delivering top-tier security services with exceptional Service Level Agreements (SLAs) and support. To establish a successful MSSP program, Cyberuptive embraced Trellix XDR, built on AWS, for enhanced scalability and visibility across various security products, including endpoints, emails, networks, and the cloud.

Before adopting Trellix XDR, traditional security investigation processes, were manual and resulted in delays in threat detection and mitigating real threats. Recognizing the need for advanced automation in investigations, Cyberuptive sought ways to streamline the process and achieve quicker and more effective responses to emerging threats. The adoption of Trellix XDR into Cyberuptive's Security Operation Center(SOC) led to the exploration of cutting-edge technologies capable of automating investigative processes while maintaining accuracy.

Partner Solution

Trellix XDR seamlessly integrates all Trellix technologies, a vast ecosystem of over 1000 vendor partners, tools, and data sources, providing a cohesive SecOps experience. The collaboration between Trellix and Cyberuptive aimed to innovate the realm of automated investigations. Harnessing the power of Trellix XDR's data and investigative playbooks, they accelerated the analysis of security alerts. To complement this, they integrated large language models (LLM) running on AWS Sagemaker, enabling comprehensive. In addition, assessments of alerts with remarkable speed and accuracy.

Aligned in their vision to revolutionize security operations, Trellix and Cyberuptive worked collaboratively to seamlessly integrate their technologies, ensuring efficiency in processes and actionable outcomes. The seamless integration of Trellix XDR with third-party security applications simplified the learning curve for new analysts. Analysts can come up to speed quickly because they don't have to learn multiple ways of reading various logs since they are all the same and in the same place.

Customer Results

The collective efforts of Trellix, Cyberuptive, and AWS resulted in swift response times and accurate threat assessments. Through the automation of the investigation process, response times were reduced, incident resolution efficiency increased, and overall security posture was enhanced. The partnership with Trellix empowered Cyberuptive to deliver superior support, efficient response times, and cutting-edge threat intelligence to its customers, setting them apart in a competitive market.

Trellix XDR emerged as the driver of Cyberuptive's success as an MSSP, providing effective breach response capabilities to top enterprises. The power of Trellix Helix, designed for proactive hunting rather than being a mere log tool, enabled rapid identification of crucial data. This rapid decision-making capability is at the core of the operational efficiency achieved.

Cyberuptive can get to a resolution quickly due to the Threat Intelligence provided by Trellix XDR. With access to the finest threat intelligence in the commercial space, customers utilizing Cyberuptive's platform, integrated with Trellix XDR, gain unparalleled insight and protection against emerging threats.

Cyberuptive and Trellix were able to utilize the AWS ISV Workload Migration Program (WMP) to enhance the success of the overall project objectives, deepening each organization's operational infrastructure capabilities with Amazon Web Services (AWS)

Visit Trellix.com to learn more.

About Trellix

Trellix is a global company redefining the future of cybersecurity. The company's open and native extended detection and response (XDR) platform helps organizations confronted by today's most advanced threats gain confidence in the protection and resilience of their operations. Trellix's security experts, along with an extensive partner ecosystem, accelerate technology innovation through machine learning and automation to empower over 40,000 business and government customers.