CYDERES

By choosing SOC Prime's CaaS platform as the primary source of detection content for its Managed Detection and Response (MDR) services, CYDERES has been able to improve MTTR to critical threats, ensuring cutting-edge cybersecurity for their customers' data and systems.

Industry
Security & Investigations (MSSP)

Region
USA

Company Size
250+ employees

SIEM & XDR in Use
Cloud Native Analytics Platform powered by Google Cloud's Chronicle

Eric Foster
Co-Founder and President of CYDERES

"This partnership enables CYDERES CNAP to provide advanced detection content without increasing our human capital, helping us deliver on the vision of "legendary service at a fair price" that's been so instrumental in helping us disrupt the legacy MSSP industry. More importantly, with this incredible baseline of rules, we can repurpose our detection engineering team on creating highly customized content to optimize security protection for each of our clients."

Highlights

- Delivery of curated and verified detection content along with continuous support for the CYDERES Cloud Native Analytics Platform (CNAP) and Managed Detection & Response (MDR) services
- Proactive response to the most critical and constantly emerging threats in real time
- Continuous threat coverage and content alignment with the MITRE ATT&CK® framework
- Seamless integration with Chronicle Security powered by Google Cloud and 20+ supported SIEM, EDR, and NTDR security solutions

Challenges

Custom Behavior-Based SOC Content. To deliver advanced cybersecurity services tailored to the threat profile and client's environment, it is important to obtain the source of qualified, cross-vendor, and cross-tool threat detection content covering critical threats and matching the relevant XDR stack. Business is looking for tailored solutions able to ensure streamlined and full CI/CD threat detection workflow. With SOC Prime's detection content as an engine, CYDERES can provide state-of-the-art services to help their clients create an integrated cloud-native infrastructure and maximize the value of their security investments.

Talent Shortage and Content Scalability Issues. Increasing the in-house engineering team requires not only significant financial investments for MSSP organizations but also raises a common problem on the cybersecurity market, which involves a pressing talent shortage. Moreover, detection content crafted by the individual in-house Content Developers and Threat Hunters is not always fully scalable to match versatile business needs and a wealth of technologies the company's customers expect to obtain when ordering the MSSP services.

Mass Content Migration from On-Premise SIEM to Cloud. Extensive on-premise SIEM integration within a complex business environment might be time-consuming, hard to maintain, and demanding in terms of specific expertise. Such stumbling blocks may result in wasted organizational resources, business process downtime, and significantly decreased ROI for MSSP clients. Furthermore, manual SIEM migration to the cloud is a daunting issue demanding in-depth expertise and extensive resources, which drove CYDERES to look for a reliable source of qualified cloud-native content to power the migration to Chronicle Security.

Lots of SOC Team Hours on Content Development to Cover the Latest Threats. In view of the continuously increasing amount of security alerts, Security Operations (SecOps) teams need to collect and process impressive amounts of data. Although security practitioners struggle to cover critical threats with relevant detection content, a high percentage of red flags is missing due to a lack of proper threat context and prioritization. As a result, a large amount of effort applied does not correlate with the final outcome, allowing adversaries to pass the protections unnoticed.

Enrichment and Automation. A lot of MSSPs in the IT sector are looking for ways to accelerate their daily SOC procedures to save SOC team hours on threat detection and incident prevention. SOC automation is vital for proper management of security alerts and helps keep SIEMs in proper shape to withstand the avalanche of emerging threats. Gaining from automated capabilities allows reducing manual efforts on content development, deployment, and fine-tuning of detection and response algorithms. With this in mind, CYDERES was in search of a third-party vendor that could help streamline the process of content development by enabling automated delivery, deployment, and customization of the latest detections along with accelerated migration possibilities tailored to the customers' SIEM and XDR stack.

Solution

While looking for a reliable cross-tool detection content provider that could deliver custom use cases for their clients, CYDERES found the SOC Prime Threat Detection Marketplace as a key to the fast-track, curated content delivery and support. By establishing a long-term partnership with SOC Prime, CYDERES has managed to boost their cyber defense services without adding additional engineering resources.

Threat Detection Marketplace enables community collaboration, integration, and continuous support of the detection content. Obtaining cross-tool content to detect the latest threats at the right time along with rich threat context has helped CYDERES satisfy the content needs of the company's customers in various industries. Gaining access to the massive library of Premium SOC content enriched with the complete threat context has enabled CYDERES to bring their customers to the next level of security detection and response.

Achievements

Extensive Threat Coverage

CYDERES CNAP powered by the cutting-edge content from Threat Detection Marketplace helps customers to be constantly updated on the latest threats and get custom detections within 48 after the threat discovery. This ensures enhanced security protection for CYDERES clients and saves hours on content development.

Smooth Migration to Cloud

Partnership with SOC Prime enables CYDERES to seamlessly transition custom use cases from the legacy and on-premise SIEMs and other security tools in use to the cloud-native Chronicle Security format at a Google speed saving hundreds of SOC team hours.

Continuous Security Intelligence

Continuous access to qualified, cross-vendor, and cross-tool threat detection content allows CYDERES customers to master their security infrastructure to run like clockwork. Complete threat context fuels retrospective hunt, which in turn, enables enhanced proactive threat detection for CYDERES clients.

Automation of Threat Hunting Procedures

Automated capabilities of the Threat Detection Marketplace allow CYDERES to accelerate SOC content development by obtaining on-the-fly translations to the Chronicle Security language format and other cloud-native solutions leveraged by the company's customers. Gaining from the API integration tool adds to the streamlined detection search and significantly boosts threat hunting operations.

About CYDERES

CYDERES, a global Top 25 MSSP, is the 24/7 human-led and machine-driven Security-as-a-Service division of Fishtech Group, the leading current generation cybersecurity solutions provider for enabling secure and successful business transformation. CY(ber) DE(fense&) (RES)ponse supplies the people, process, and technology to help organizations manage cybersecurity risks, detect threats, and respond to security incidents in real time. Learn more at https://fishtech.group/cyderes/.