Entelgy Innotec Security

Through partnership with SOC Prime, Entelgy Innotec Security has managed to save up to 600 hours per year on the development of cross-SIEM use cases tailored to the needs of the company's customers.

Industry
Information Technology & Services

Region
Southern Europe

Company Size
450+ employees

SIEM & XDR in Use
Microsoft Sentinel, Splunk, Elastic Stack, QRadar

Alfonso Cid Pertierra
Project Manager Officer at Entelgy Innotec Security

"The decision for establishing partnership with SOC Prime was taken firstly due to the extensive, curated and constantly updated catalog of detection content, which is surely the best on the market and the most complete. What's more, another point that drove us to choose SOC Prime was the ability to obtain use cases for proactive incident detection."

Highlights

- Fast-track delivery of custom use cases based on the log source product filtering tailored to the customers' business needs and environment
- Content search and management via automation based on the SIEM and XDR tools in use and ATT&CK parameters
- Availability of critical detections within 48 hours after threat discovery
- Threat-centric selection of detection content using the MITRE ATT&CK framework
- Fast and easy content translation to multiple SIEM & XDR formats using the generic Sigma language

Challenges

Lack of Custom Content Tailored to the Organization-Specific Threats and Environment. As a Managed Security Service Provider (MSSP), Entelgy Innotec Security has long been struggling to find a flexible approach that will allow treating each company's customer in an individual way considering the level of security maturity, company size, and technologies in use. Developing curated use cases matching the specific customers' needs posed a challenge when considering an extensive number of parameters, including ever-changing attack vectors, the industry-specific threat landscape, and a versatile security toolkit. Leveraging custom SOC content that goes beyond what is offered by SIEM vendors with the high scalability potential has been anticipated by Entelgy Innotec Security as key to this common MSSP challenge.

Sufficient SOC Team Hours Spent on Proactive Threat Detection and Incident Prevention. Following the cutting-edge threat detection practices, Entelgy Innotec Security was primarily looking for ways to obtain SOC use cases that would allow proactively defending against threats rather than implementing a reactive cyber defense strategy. This required sufficient effort on the company's SOC team and stressed the need for automated capabilities to streamline regular SOC operations, including threat discovery and hunting, content search and management.

Need for Prompt Response to Emerging Threats. Providing Managed Security services to over 250 organizations requires being highly responsive to the customers' needs. New threats are emerging at an ever-increasing pace and obtaining detection content to address them is a daunting challenge for MSSPs, since clients are often in dire need of the SOC content just a few hours after the vulnerability disclosure. Facing this challenge, Entelgy Innotec Security was in search of a third-party content provider that would be able to deliver detection and response algorithms at the earliest stages of attack lifecycle.

Solution

Backed by a holistic approach to cyber defense, Entelgy Innotec Security was looking for a third-party vendor that would help the company deliver full-scale security protection of their customers' infrastructure. The SOC Prime's world's first platform for collaborative cyber defense, threat hunting and threat discovery has become a universal solution capable of addressing the custom security needs of the company's clients who leverage different types of content for TTP-based or IOC-based threat hunting, threat investigation and tailored to 20+ SIEM & XDR solutions. The extensive catalogue of detection rules, queries and parsers set for exponential growth has become a key reason why SOC Prime has been given preference over other content providers on the market. Content alignment with the latest version of the MITRE ATT&CK framework has helped Entelgy Innotec Security boost their customers' cybersecurity posture providing continuous visibility into threats relevant to the organization's threat profile.

Achievements

Use Case Parameterization

With access to the world's largest Threat Detection Marketplace, Entelgy Innotec Security has found a highly flexible solution matching a wide range of the customers' environments, content types, and industry-driven threat profiles. Depending on the organization-specific parameters and security needs, Entelgy Innotec Security can now easily find and deploy G Suite-based detections, SIEM-native content, like Elastic Watcher and ElastAlert, Microsoft Sentinel analytics rules and hunting queries, on-premises and cloud detection algorithms, including content for QRadar and Splunk.

Enrichment and Automation

Driven to accelerate the content search and deployment operations, Entelgy Innotec Security has taken advantage of the SOC Prime's integrated automation feature with the Threat Detection Marketplace content repository. The automated capabilities of the SOC Prime's Detection as Code platform has enabled Entelgy Innotec Security to reduce manual effort on the company's SOC team involving custom content selection across multiple SIEM systems and ATT&CK techniques, tools, or APT groups. Entelgy Innotec Security is also planning to try out the Continuous Content Management module as a long-term solution for adapting cyber defense capabilities to the latest threats the company's customers anticipate most.

Proactive Exploit Detection

Struggling to keep up with the dynamic pace of the evolving threat landscape, Entelgy Innotec Security has come up with the SOC Prime's Detection as Code platform, which is constantly updated to provide content for detection of the latest threats. Leveraging the SOC Prime's platform, Entelgy Innotec Security can now help their customers proactively deploy detections for critical vulnerabilities within a period of 48 hours. In the case of the PrintNightmare RCE vulnerability, the company's customers required a solution at the exact time of content publication to the SOC Prime Threat Detection Marketplace, which allowed Entelgy Innotec Security to address this content request without delay.

Urgent Response to Customers' Needs and Progress Tracking

With SOC Prime, Entelgy Innotec Security has managed to promptly respond to any threat detection use cases challenges arising on the customers' side, like deployment issues with Elastic Watcher and other SIEM-related needs. What's more, regular meetings with the SOC Prime's Customer Success Team has helped Entelgy Innotec Security assess the platform threat detection and hunting capabilities in terms of their value for the company's customers, as well as receive guided support on the new and existing functionality.

About Entelgy Innotec Security

Entelgy Innotec Security belongs to the Entelgy Group as a wholly owned division aimed to protect the company's infrastructure and customers' businesses from digital attacks and security breaches. Leveraging the Advanced Security Operations Center (SmartSOC), Entelgy Innotec Security delivers world-class cybersecurity services to 250+ customers, including major public organizations and industry-leading companies in Spain and Latin America. Backed by flexibility, technological independence, and the certified standard of excellence, Entelgy Innotec Security tailors a wide range of provided cybersecurity services to the organization-specific business needs, including Blue Team and Red Team Services, Cybersecurity Strategy Consulting, Managed Security Services, Security Monitoring & Incident Response.