Deloitte Brazil Customer Success Story

Deloitte Brazil's professional services augmented with outsourced SOC Operations endeavored to quickly and cost-effectively increase their end-customers' cybersecurity maturity to confront the dynamic cyber threat landscape present in the market environment. They evaluated multiple approaches to address the problem and chose SOC Prime's Detection as Code Platform. SOC Prime's solution includes a comprehensive library of behavior-based Sigma rules, enabling the delivery of curated detections 3X faster for any of the company's end-customers leveraging security tools like QRadar, Splunk, CrowdStrike SIEMs, and multiple EDRs. This allowed Deloitte Brazil to maximize available threat hunting resources while increasing the speed of threat detection operations, including a 200% increase in identification to expedite investigation and remediation.

Industry	Region	Company Size	SIEM & XDR in Use
Business Consulting and Services	**South America**	**5,500+ employees**	**QRadar, Splunk, CrowdStrike**

Eder de Abreu
Cybersecurity Partner at Deloitte Brazil

"Deloitte Brazil provides critical cyber threat intelligence and cyber threat monitoring services to multiple clients. Every day we confront the challenge of combating a continuous volume of cyber attacks launched against a demanding client base with disparate security solutions that expects excellence. With SOC Prime, we have rapidly accelerated our clients' cybersecurity maturity by delivering proactive cyber defense against pressing, prioritized, and emerging attacks."

Highlights

- Providing instant access to the extensive library of detection algorithms convertible into any end-customer's unique SIEM, EDR, or XDR environment, including QRadar, Splunk, and CrowdStrike
- Simplifying administration and accelerating the process of delivering end-customers' cybersecurity maturity
- Enhancing proactive cyber defense by expediting the detection of zero-days and other critical threats
- Increasing threat detection and hunting velocity with intelligence-driven cybersecurity solutions

Challenges

Need for Improved SOC Resource Utilization with Outsourced Threat Research and Content Development

The increasing escalation of attack volumes requires ultra-fast responsiveness from cyber defense teams. Striving to enhance cyber defense capabilities for Deloitte Brazil's customers, the company sought a scalable solution, adaptable across multiple industries, capable of increasing their end-customers' managed services security posture and responsiveness to detecting and resolving critical and emerging threats. The company considered two options to achieve this goal:

1. Significantly increase in-house engineering resources to keep pace with accelerating attack volumes. This option required substantial investments in threat hunting resources.
2. Leverage detection algorithms from a specialized threat detection content marketplace allowing the existing SOC team resources to focus on detection and mitigation rather than on content research and development.

Need for Increased Maturity and Velocity of Cybersecurity Operations

Deloitte Brazil had access to insights gleaned from a global base of client profiles across multiple industries, utilizing a myriad of SIEM, EDR, and XDR environments. This enabled the company's engineering team to seek innovative ways to dramatically improve threat detection and hunting capabilities and keep pace with evolving market demands for responsiveness and effectiveness. A primary goal was to elevate the utilization of global threat intelligence in its service delivery model. Deloitte Brazil has already started implementing the progressive cybersecurity strategy addressing these priorities, but the company's ambition was to accelerate the speed of this process.

Customers' Reliance on Disparate Security Solutions & Related Skills Shortage

As part of the global organization providing professional services, Deloitte Brazil faced the daunting challenge of matching diverse customers' demands for expert threat detection operations tailored to unique environment needs. The company realized that covering threat detection content development for all customer profiles with a diverse set of deployed technologies would require significant expansion of Deloitte Brazil's engineering team.

Solution

Deloitte Brazil pioneered SOC Prime's Detection-as-Code solution in their cybersecurity market, highlighting the company's progressive mindset and willingness to explore industry innovation to improve and accelerate the services they deliver. With SOC Prime's platform, Deloitte Brazil found both an efficient and effective solution that allowed them to amplify their professional services by outsourcing the development of context-enriched threat detection content across all stages of the attack lifecycle and translating these detections into all customers' unique security environments. This allowed Deloitte Brazil to achieve the company's core objective of increasing their customers' cybersecurity maturity. SOC Prime has enabled Deloitte Brazil to implement the proactive cybersecurity approach providing the customers with the most relevant and up-to-date detection content for critical threats.

Achievements

Ultra-Responsiveness to Most Relevant Cyber Threats

With SOC Prime's Detection as Code platform, Deloitte Brazil instantly addressed the challenge of keeping pace with the ever-evolving threat landscape without expanding their in-house security team. For instance, in the case of Log4j zero-day vulnerabilities massively exploited in the wild, the company's team was flooded with the customers' requests for related detections. These detections were already available in SOC Prime's platform the day the proof of concept (POC) was released. This proactive approach enabled Deloitte Brazil to deliver to their customers a solution that instantly addressed emerging threats while allowing the core team of Threat Hunting resources to focus on detection and remediation rather than content development.

Near Real-Time Delivery of Cross-SIEM and Industry-Specific Use Cases

Before leveraging SOC Prime's solution, Deloitte Brazil considered the need to triple the size of their engineering team to cover diverse customer demands with unique threat profiles and security environments.

SOC Prime's platform has provided the company with instant access to a broad collection of the most widely requested use cases related to brute force attacks matching the organization-specific log sources with translations available for any unique security environment. Outsourcing threat detection eliminates the skills shortage challenge that requires Detection Engineers specializing in particular SIEM or EDR since SOC Prime's platform delivers Sigma rules convertible to 25+ SIEM, EDR, and XDR solutions.

Improved Threat Coverage & Visibility with MITRE ATT&CK®

Deloitte Brazil's customers displayed multiple levels of cybersecurity maturity with their requests varying from the basic needs to more advanced services accompanied by relevant CTI. Leveraging SOC Prime's MITRE ATT&CK Coverage dashboard has enabled the company to cover multiple threat vectors relevant to particular environments, identify critical gaps, and set strategic detection objectives aligned with any organization's unique security profile and needs to reduce available attack surfaces.

About Deloitte Brazil

Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax, and related services to nearly 90% of the Fortune Global 500® and thousands of private companies. Deloitte has been recognized as the most valuable commercial services brand by Brand Finance — for the fourth year in a row and also appears in the ranking of the 10 strongest brands in 2022. Deloitte grows in scale and capabilities expanding its global team of over 345,000 seasoned professionals making an impact across 150 countries, including Brazil.

Deloitte Brazil is one of the marketing leaders connecting over 5,500 professionals on board who are recognized for integrity, competence, and capability to turn their knowledge into the best solutions for their clients. Deloitte's operations cover throughout the Brazilian territory, with offices in São Paulo, Belo Horizonte, Brasília, Campinas, Curitiba, Fortaleza, Joinville, Porto Alegre, Rio de Janeiro, Ribeirão Preto, Recife and Salvador. With a strong focus on cybersecurity, Deloitte Brazil delivers cyber threat intelligence and cyber threat monitoring services to customers from multiple industry sectors and with different maturity levels helping them to develop and implement effective cybersecurity strategies aligned with their business needs.