Neurosoft

By partnering with SOC Prime, Neurosoft has significantly improved MTTD and MTTR and cut down the false positive rate by up to 50% over the first six months of using the Platform, which has contributed to the overall quality of cybersecurity services delivered to the company's clients. By relying on the extensive library of over 11,000 behavior-based Sigma rules and tailored threat intelligence, Neurosoft obtains detection content for the latest threats in less than 24 hours, which is at least 4X faster than before leveraging SOC Prime Platform.

Industry	Region	Company Size	SIEM & XDR in Use
IT Services and IT Consulting	**Southern Europe**	**250+ employees**	**IBM QRadar, Qradar Suite, Microsoft Sentinel, Microsoft Defender for Endpoint, Carbon Black, Cisco AMP, Bitdefender, Fortiedr**

Babis Kalevrosoglou
Managed Security Services Manager

> *"Since we started partnering with SOC Prime, we have significantly increased the speed of detection algorithm delivery and improved the overall content quality. By leveraging Sigma rules from SOC Prime Platform, we have reduced the false-positive rate by up to 50% and can now seamlessly deploy detection content to our SIEM with minimum fine-tuning. With SOC Prime, we can obtain detection algorithms for emerging threats in less than 24 hours, and clients have already seen a huge improvement in our services. Our objective is to deliver high-caliber cyber defense services with the aim of fortifying the security posture of our clientele."*

Highlights

- Elevating clients' cybersecurity maturity through the improved quality of Managed Services
- Continuously reducing false positives while increasing detection content and enabling SOC analysts to focus on incident investigation rather than analyzing never-ending streams of alerts
- Streamlined threat investigation with instant access to relevant CTI and attacker TTPs linked to 11,000+ Sigma rules
- Saved time and effort on detection content development from scratch
- Ready-to-deploy detection algorithms instantly convertible to multiple SIEM, EDR, XDR, Data Lake and query language formats

Challenges

Security Risks Exceeding Detection Capabilities

The rapidly growing threat environment requires organizations to adapt their defense capabilities by switching the primary focus from compliance challenges to addressing real-world risks. Neurosoft provides a feasible solution to help its clients shift the cybersecurity strategy along with procedures and countermeasures to reduce these risks while improving the overall cybersecurity posture.

Lack of the Customers' Cybersecurity Maturity

Being one of the biggest cybersecurity companies in the Greek market and one of the top SOCs in the Greek market, Neurosoft provides a wide range of services to clients in multiple industry verticals and with disparate levels of cybersecurity maturity, which requires a personalized approach to meet the organization-specific needs.

High False-Positive Rate

Overwhelming volumes of alerts along with a lack of context pose a daunting challenge to the security systems to accurately distinguish between legitimate and potentially harmful activities while increasing the burden on SOC analysts struggling to triage alerts faster and with higher precision. To mitigate the impact of high false-positive rates, Neurosoft sought a cost-efficient solution to improve detection efficiency by fine-tuning detection algorithms with less effort and adapting them to changing behavior patterns and emerging threats.

Solution

Neurosoft established a partnership with SOC Prime to enhance their clients' cyber defense capabilities enabling them to obtain custom detection algorithms for the most critical threats in less than 24 hours. With SOC Prime, Neurosoft has managed to provide ready-to-deploy detection content tailored for dozens of SIEM, EDR, and XDR solutions while matching specific clients' needs across multiple industry sectors and accommodating both on-prem and cloud security tools. As further partnership benefits, Neurosoft can rely on SOC Prime to help its clients gain from continuously enhanced detection content quality while risk-optimizing the organization's cybersecurity posture.

In line with the company's strategy to expand the in-house security team, Neurosoft plans to engage more SOC Prime Platform capabilities to streamline its daily security operations. While it normally takes 2-3 hours for regular detection stack validation, leveraging SOC Prime's Attack Detective will enable the team to perform an automated MITRE ATT&CK® data audit at least 36 times faster, which can significantly contribute to the company's SOC efficiency.

Achievements

Saved Hours on Detection Content R&D

With access to the Threat Detection Marketplace curating over 11,000 custom Sigma rules relevant to the client's industry and covering organization-specific log sources, Neurosoft has improved its engineering team's capacity spent on threat investigation and detection content development from scratch. Freeing up this amount of time has helped the company boost detection efficiency and channel more efforts into security monitoring and threat remediation.

The Fastest Rule Feed on Emerging Threats

Leveraging SOC Prime Platform enables Neurosoft to deliver curated detection content against critical zero-days, ransomware, or the latest APT attacks within 24 hours rather than force their clients to wait for 4-5 days to address emerging threats. This also directly affects the continuous improvement of the MTTD and MTTR while boosting the overall detection content quality based on positive feedback from the company's clients.

Prime Source for Threat Intelligence

Collaboration with SOC Prime provides the leading Information and Communication Technology Integrator in the SEE region with an extensive source of tailored intelligence and cyber threat context, including CVE descriptions, PoC exploits, mitigations, and other relevant metadata easily searchable and continuously updated. Instant access to CTI integrated with Sigma rules streamlines the in-house engineering team's daily security operations and simplifies the time-intensive process of gathering intelligence from various sources.

Vendor-Agnostic Rules & Queries

SOC Prime helps Neurosoft address the challenge of providing detection content compatible with versatile SIEM, EDR, and XDR technologies and query languages. Leveraging vendor-agnostic Sigma rules reduces the workload for the company's detection engineers, as it saves them time and effort when creating and adapting content to fit the client's environment, regardless of AQL, KQL, or any other query language format in use.

Reduced False Positives

With SOC Prime, Neurosoft cut in half the number of false positives as compared to the overall detection content quality before starting the partnership. This has also contributed to bolstering the effectiveness of use cases while relying on the tools at hand and the available in-house SOC team's capacity, thus saving costs for other security investments.

About Neurosoft

Neurosoft is a leading Information and Communication Technology (ICT) Integrator delivering novelty solutions and services to enhance efficiency and security. Since 2009, the company has been publicly listed on the Italian Stock Exchange, with OPAP holding the majority of shares. Neurosoft currently employs over 250 highly skilled experts. Operating across Greece, Cyprus, and the SEE region, Neurosoft offers cutting-edge solutions and services encompassing three business areas: Cybersecurity, Infrastructure (from on-prem to multi-cloud), and the Field domain. The company covers the entire spectrum of business operations, ranging from Design and Consulting to Support and Managed Services. Rooted in dedication to excellence, Neurosoft is committed to crafting forward-looking, adaptable solutions by fusing business and technology experience.