7Layers

SOC Prime's Detection as Code platform for collective cyber defense enabled 7Layers to dramatically reduce both time and effort on searching for threat intelligence sources and their translations to multiple SIEM & XDR systems, including Microsoft Sentinel, FireEye Helix, and ArcSight. The company improved its Threat Hunting services leveraging over 9,000 behavior-based Sigma rules tailored for multiple security solutions and addressing TTPs relevant to the end-customers' threat profiles.

Industry	Region	Company Size	SIEM & XDR in Use
IT Services and IT Consulting	Southern Europe	80+ employees	Cortex XDR, FireEye Helix, Microsoft Sentinel, Microsoft 365 Defender, ArcSight

Niccolò Vascellari
System Engineer Manager at 7Layers

"With SOC Prime Platform, we managed to dramatically reduce both time and effort on searching for threat intelligence sources and their translations to multiple SIEM & XDR solutions leveraged by our customers. SOC Prime's support for the MITRE ATT&CK® framework, which is the reference beacon we're using to map and understand the various adversary techniques, has helped us significantly boost cybersecurity effectiveness and proactively hunt for threats our customers anticipate most."

Highlights

- Enriching Threat Hunting capability delivered as part of the company's Managed Security and MDR services with verified behavioral hunting queries
- Reduced number of false positives with high-quality ready-to-deploy detection algorithms
- Proactive detection of adversary TTPs matching the end-customers' threat profiles based on MITRE ATT&CK v12
- Extracting more value from SOC investments with saved hours and effort on detection content development and rule conversion to multiple SIEM & XDR solutions
- Streamlined threat investigation with access to an extensive knowledge base of Threat Hunting & Detection Engineering ideas and relevant threat intelligence

Challenges

Cyber Threat Landscape Diversity and Complexity

Cyber defenders are constantly challenged with a growing number of attack volumes, a surge in multiple APT groups, and increased sophistication of adversary tools. As an industry-leading MDR vendor, 7Layers was laser-focused on tackling their end-customers' cybersecurity risks, which involved addressing a diverse range of adversary techniques commonly intended to exfiltrate data.

Disparate Technology Toolkit

7Layers delivers Managed Security and MDR services to customers across multiple industry verticals, with diverse levels of cybersecurity maturity, and leveraging disparate SIEM and security analytics systems. Timely delivering detection content for emerging threats is already a challenge not every MDR provider can handle, not to mention migration and customization hurdles driven by the diverse environment needs of the end-customers' solutions. The company was looking for a trusted vendor curating cross-tool detection and hunting content that requires minimum fine-tuning.

Lack of Behavioral Threat Hunting Content Tailored for Customers' Environments

Having relied mainly on OSINT sources, 7Layers found the process of detection content selection, customization, and conversion to multiple SIEM & XDR systems rather time-consuming. The company was in search of a third-party SOC content provider offering high-quality behavioral threat hunting content that could minimize the number of false positives and match the environment needs of multiple end-customers.

Solution

7Layers relies on **SOC Prime's** innovation and progressive cybersecurity mindset powered by the collective cyber defense and the combination of cutting-edge technologies — Sigma language, MITRE ATT&CK, and Detection-as-Code practices. By choosing **SOC Prime's Detection as Code platform,** 7Layers has managed to address its most pressing cybersecurity challenges related to the lack of high-quality detection content, alert fatigue, and insufficient SOC team resources for threat investigation and proactive defense to keep up with an avalanche of emerging threats.

With SOC Prime, the company has accelerated its TTP-based hunting capabilities enabling end-customers to proactively search for treats that matter most. SOC Prime's support for industry-leading SIEM & XDR solutions has helped the company address one of the most common MSSP and MDR vendors' challenges of time-consuming detection content conversion to multiple technology stacks along with parsing and fine-tuning hurdles.

Achievements

Enhanced Threat Hunting Capability

With access to SOC Prime's extensive security intelligence repository, 7Layers could reach over 9,000 ideas for Threat Hunting and Detection Engineering. Leveraging a wealth of Sigma behavior-based threat hunting queries ready to deploy to multiple end-customers' environments, the company managed to enhance its Threat Hunting services and effectively tackle the false-positive challenge.

Near Real-Time Delivery of Custom Detection Rules and Hunting Queries

SOC Prime's Detection as Code platform has enabled 7Layers to proactively defend against emerging threats the company's end-customers anticipate most. The industry-leading MDR provider has managed to timely provide its customers with curated endpoint detection and cloud security rules along with verified hunting queries that are at the top list of the company's content priorities.

Improved Threat Coverage Benchmarked Against MITRE ATT&CK®

In their daily security operations, 7Layers' SOC team relies on the MITRE ATT&CK framework as the "reference beacon" to profile threat actors, adversary techniques, and tools. Leveraging the MITRE ATT&CK content visualization functionality in the SOC Prime Platform has helped 7Layers to streamline the search for detection and hunting content by particular TTPs matching the end-customers' threat profiles, address prioritization hurdles, and fill the gaps in threat detection coverage.

Saved Hours on Threat Research, Rule Coding, and Conversion to Multiple SIEM & XDR Solutions

Through a partnership with SOC Prime, 7Layers has managed to streamline threat investigation with direct access to **actionable cyber threat context** and relevant metadata, including CTI and ATT&CK references, media links, and mitigations. The company can now save hundreds of hours and reduce effort on SOC content development with access to ready-to-use detection algorithms and hunting queries tailored for 25+ SIEM and XDR technologies, including Microsoft Sentinel, FireEye Helix, and ArcSight.

About 7Layers

7Layers is one of the fastest-growing cybersecurity companies in Europe. Established in 2012, for over a decade, the company has been delivering world-class cybersecurity solutions in conjunction with Managed Detection and Response services across multiple industries, including enterprise, financial services, manufacturing, strategic asset, energy, and legal sectors. The company leverages technology coupled with human-based intelligence and internal processes to detect and combat advanced persistent threats in real time. 7Layers is a cybersecurity services company laser-focused on detecting and mitigating threats to protect its end-customers' assets, brands, and users. The company creates value by sharing its threat intelligence expertise and helping protect some of the world's famous commercial companies.

7Layers is a member of Trusted Introducer, confirming that the company is operating at a high level of process maturity and complies with a range of standards widely accepted within the global security and incident response community. The company runs Follow The Sun (FTS) operations leveraging expert cybersecurity analysts geographically distributed in three different time zones to optimize MTTD and MTTR of their end-customers. With this solution, any incident can be managed directly by an expert analyst and not by a first-level technician 24×7×365.

Explore SOC Prime's Detection as Code platform to defend against attacks easier, faster and more efficiently than ever.

EXPLORE PLATFORM