HWG Sababa NOVOMATIC ITALIA

Novomatic Italia Strengthens Cyber Resilience in a Highly Regulated Environment with HyperSOC™



Executive Summary

Novomatic Italia, part of the Novomatic Group – a global gaming technology company operating in over 50 countries with more than 4,200 employees – is a leading operator in the gaming and payment services sector. The company operates in a highly regulated environment where cybersecurity is directly tied to business continuity and compliance.

To strengthen detection and response capabilities across its complex, predominantly on-premise infrastructure, Novomatic Italia partnered with HWG Sababa. By implementing HyperSOC™ managed security operations, the company improved visibility, reduced false positives, and established a more efficient and resilient security model.

The collaboration enabled Novomatic to move from alert-driven monitoring to an outcome-driven security model, improving detection accuracy, reducing operational noise, and strengthening resilience against real-world attack scenarios – including the successful prevention of a lateral movement attempt toward core systems.

Key Results

- **~60% reduction in alert volume through continuous tuning and contextualization**
- **Significant reduction in false positives and manual investigation effort**
- **Improved prioritization of high-risk events through contextualized detection**
- **Structured and efficient SOC-to-internal team collaboration model**
- **Proven ability to detect and contain real-world threats before business impact**

Company Background

Novomatic Italia is the Italian branch of Novomatic Group, a global leader in gaming technology and services, operating in over 50 countries and serving more than 150 markets worldwide. In Italy, Novomatic employs over 4,200 people across its headquarters in Rome, its production hub in Rimini, multiple operational sites, and around 300 gaming venues nationwide.

The company operates in the gaming, betting, and payment services sector, managing multiple legal entities under strict regulatory frameworks. Its infrastructure is complex, largely on-premise, and tightly integrated with business operations, including retail gaming, online platforms, and digital payment services.

The organization operates in a multi-regulated environment, including:
- NIS2 directive
- ISO 27001 certification
- PSD2 and financial regulations
- National gaming authority requirements

In this context, cybersecurity is not only a technical function but a critical business enabler, directly linked to operational continuity, regulatory compliance, and the protection of a highly distributed and transaction-intensive ecosystem.

Key Challenges

Novomatic Italia faced several challenges typical of large, regulated, and infrastructure-heavy organizations.

Highly Regulated Environment
Compliance is essential to maintain operating licenses. Cybersecurity must align with multiple overlapping regulations, requiring structured governance and continuous monitoring.

Complex On-Premise Infrastructure
The company operates a predominantly on-premise architecture, with high volumes of data and strong internal technical capabilities. This increases complexity in monitoring and limits the adoption of cloud models.

Focused Cybersecurity Team
In a complex environment, the internal team is purpose-built and operates with strong coordination, leveraging specialized external partners to ensure continuous coverage and high-quality monitoring.

SOC service experience with a continuous improvement approach
Experience with the previous SOC provider highlighted key areas for optimization and provided a baseline to strengthen the service model. In this context, targeted initiatives were launched to improve monitoring quality, response timeliness, and alignment with operational and security requirements, within a structured continuous improvement approach.

“Despite good visibility, operational effectiveness was limited: the high volume of alerts did not translate into corresponding operational value, impacting the perceived reliability of the service.”
– Marcello David, Cybersecurity Manager at Novomatic Italia

The Solution: Continuous and Context-Aware Security Operations

To address these challenges, Novomatic Italia selected HWG Sababa as its SOC partner, implementing HyperSOC™ as the central platform for detection and monitoring.

The approach focused on:
- Replacing legacy detection logic
- Introducing structured collaboration between SOC and internal teams
- Enabling continuous improvement of detection capabilities

Unlike traditional SOC models focused on tool-centric monitoring, HyperSOC™ operates as a continuous optimization layer – combining detection, contextualization, and feedback loops to progressively improve accuracy and reduce noise within the specific operational environment.

"What really changed with HWG Sababa was the quality of the alerts. Instead of noise, we started receiving meaningful signals we could actually act on."
– Marcello David, Cybersecurity Manager at Novomatic Italia

Implemented Capabilities

Managed Security Operations through HyperSOC™
Deployment of continuous monitoring and detection capabilities, with centralized log collection and SIEM-based correlation. HWG Sababa SOC provides first- and second-level analysis, filtering the majority of alerts and escalating only relevant events.

Detection Optimization and Continuous Improvement
Initial correlation rules were replaced with HWG Sababa's baseline and continuously refined based on Novomatic's operational context. This continuous feedback loop enabled progressive reduction of noise, improved detection accuracy, and alignment of alerts with real business-relevant events.

Structured Incident Handling
A clear escalation model was established to ensure rapid response while maintaining control over remediation actions:
- SOC performs L1/L2 analysis
- Internal team handles L3 validation and response
- Critical incidents trigger immediate escalation

Post-Attack Security Enhancements
Following an attempted lateral attack targeting Novomatic Italia, the activity was promptly detected by HyperSOC™, enabling the threat to be contained before any impact on critical systems.

As a result, Novomatic expanded its security posture, with all capabilities managed and monitored through HyperSOC™, by:

- Implementing Secure DNS to detect malicious queries across the network
- Extending API security controls
- Improving visibility across infrastructure components

The Results: From Noise to Effective Security Operations

The implementation of HyperSOC™ transformed Novomatic's security operations from high-volume alert monitoring to a focused, outcome-driven model centered on detection accuracy and operational relevance.

Operational Outcomes

- Significant reduction in false positives and alert volume (~60%)
- Improved efficiency in internal security operations
- Faster identification and prioritization of relevant threats
- Effective collaboration between SOC and internal teams

Incident Response Validation

A real-world attack scenario validated the effectiveness of the model, demonstrating the ability to detect and stop threats before they could impact business-critical operations:

- Rapid detection and escalation
- Containment of impact to non-critical systems
- Coordinated response and recovery
- Support for forensic analysis and regulatory reporting

Strategic Impact

The initiative elevated cybersecurity from a monitoring function to a core component of business risk management. Rather than focusing on alert volumes, Novomatic shifted toward measuring real outcomes – incident impact, response effectiveness, and overall resilience. Cybersecurity is now:

- Integrated into enterprise risk management
- Based on structured processes and systematic approaches
- Focused on continuous improvement and operational resilience

The collaboration enabled Novomatic to move from alert-driven monitoring to an outcome-driven security model, improving detection accuracy, reducing operational noise, and strengthening resilience against real-world attack scenarios – including the successful prevention of a lateral movement attempt toward core systems.

Future Outlook

Novomatic continues to evolve its cybersecurity roadmap, focusing on:

- Further optimization of detection capabilities
- Selective automation (starting from endpoint protection)
- Evaluation of next-generation SIEM technologies, enhanced with AI capabilities for advanced threat analysis

The company maintains a hybrid approach, combining internal expertise with external SOC capabilities to ensure both operational control and access to broader threat intelligence.

This approach reflects a broader shift in how Novomatic views cybersecurity:

"Cybersecurity cannot be managed in isolation. Internal teams provide context, but external partners bring visibility across the threat landscape. Both are essential to build resilience."

– Marcello David, Cybersecurity Manager at Novomatic Italia