HWG Sababa NOVOMATIC ITALIA

Novomatic Italia rafforza la cyber resilience in un contesto altamente regolamentato con HyperSOC™



Executive Summary

Novomatic Italia, parte del Gruppo Novomatic – multinazionale attiva nel settore delle tecnologie per il gaming, presente in oltre 50 Paesi e con più di 4.200 dipendenti – è uno dei principali operatori nei settori del gaming e dei servizi di pagamento. L'azienda opera in un contesto altamente regolamentato, in cui la cybersecurity è direttamente collegata alla continuità operativa e alla conformità normativa.

Per rafforzare le capacità di detection e risposta all'interno di un'infrastruttura complessa, prevalentemente on-premise, Novomatic Italia ha scelto di collaborare con HWG Sababa. Attraverso l'implementazione di servizi di sicurezza gestita basati su HyperSOC™, l'azienda ha migliorato la visibilità, ridotto i falsi positivi e introdotto un modello di sicurezza più efficiente e resiliente.

La collaborazione ha consentito a Novomatic di passare da un monitoraggio basato sugli alert a un modello di sicurezza orientato ai risultati, migliorando l'accuratezza della detection, riducendo il rumore operativo e rafforzando la resilienza rispetto a scenari di attacco reali, fino a bloccare con successo un tentativo di movimento laterale verso sistemi core.

Risultati principali

- **Riduzione del volume di alert di circa il 60%, grazie a tuning continuo e contestualizzazione**
- **Riduzione significativa dei falsi positivi e dello sforzo manuale richiesto per le analisi**
- **Miglior prioritizzazione degli eventi critici grazie a una detection contestualizzata**
- **Modello strutturato ed efficiente di collaborazione tra SOC e team interno**
- **Capacità comprovata di rilevare e contenere minacce reali prima che generino impatti sul business**

Profilo dell'azienda

Novomatic Italia è la filiale italiana del Gruppo Novomatic, leader globale nelle tecnologie e nei servizi per il gaming, presente in oltre 50 Paesi e attivo in più di 150 mercati a livello mondiale. In Italia, Novomatic conta oltre 4.200 dipendenti distribuiti tra la sede centrale di Roma, lo stabilimento di Rimini, numerose sedi operative e circa 300 luoghi di gioco sul territorio nazionale.

L'azienda opera nei settori del gaming, delle scommesse e dei servizi di pagamento, gestendo più entità legali all'interno di un contesto fortemente regolamentato. La sua infrastruttura è complessa, prevalentemente on-premise e strettamente integrata con le operazioni di business, che includono il retail gaming, le piattaforme online e i servizi di pagamento digitale.

L'organizzazione opera in un ambiente multi-regolamentato, che comprende:
- Direttiva NIS2
- Certificazione ISO 27001
- PSD2 e normative finanziarie
- Requisiti delle autorità di regolazione del gaming

In questo contesto, la cybersecurity non è solo una funzione tecnica, ma un abilitatore critico del business, direttamente collegato alla continuità operativa, alla conformità normativa e alla protezione di un ecosistema altamente distribuito e ad alta intensità transazionale.

Le principali sfide

Novomatic Italia si trovava ad affrontare diverse sfide tipiche di organizzazioni complesse e fortemente regolamentate.

Contesto altamente regolamentato
La compliance è fondamentale per mantenere le licenze operative. La cybersecurity deve quindi allinearsi a molteplici normative, richiedendo governance strutturata e monitoraggio continuo.

Infrastruttura on-premise complessa
L'azienda opera su un'architettura prevalentemente on-premise, con elevati volumi di dati e competenze tecniche interne. Questo aumenta la complessità del monitoraggio e circoscrive l'adozione di modelli cloud.

Team cybersecurity mirato
A fronte di un contesto complesso, il team interno è dimensionato in modo mirato e opera con forte coordinamento, facendo leva su partner esterni specializzati per garantire copertura continua e qualità del monitoraggio.

Esperienze del servizio SOC in ottica di miglioramento continuo
L'esperienza maturata con i precedenti fornitori SOC ha rappresentato una base utile per identificare aree di ottimizzazione e rafforzare progressivamente il modello di servizio. In quest'ottica, sono stati avviati interventi mirati a migliorare la qualità del monitoraggio, la tempestività nella gestione degli eventi e l'allineamento ai requisiti operativi e di sicurezza, in un percorso strutturato di continuous improvement.

"A fronte di una buona visibilità, l'efficacia operativa risultava limitata: l'elevato volume di alert non si traduceva in un corrispondente valore operativo, incidendo sulla piena affidabilità percepita del servizio."
– Marcello David, Cybersecurity Manager, Novomatic Italia

La Soluzione: sicurezza continua e contestualizzata

Per rispondere a queste sfide, Novomatic Italia ha selezionato HWG Sababa come partner SOC, implementando HyperSOC™ come piattaforma centrale per detection e monitoraggio.

L'approccio si è concentrato su:
- Sostituzione della logica di detection legacy
- Introduzione di una collaborazione strutturata tra SOC e team interno
- Miglioramento continuo delle capacità di rilevamento

A differenza dei modelli tradizionali, HyperSOC™ introduce un livello di ottimizzazione continua, combinando detection, contestualizzazione e feedback loop per migliorare progressivamente l'accuratezza e ridurre il rumore nel contesto operativo specifico.

"Ciò che è cambiato davvero con HWG Sababa è stata la qualità degli alert. Da semplice rumore, siamo passati a segnali significativi su cui potevamo realmente agire."
– Marcello David, Cybersecurity Manager, Novomatic Italia

Capacità implementate

Managed Security Operations con HyperSOC™
Implementazione di capacità di monitoraggio continuo e detection, con centralizzazione dei log e correlazione tramite SIEM. Il SOC di HWG Sababa gestisce le analisi di primo e secondo livello, filtrando la maggior parte degli alert e scalando solo gli eventi rilevanti.

Ottimizzazione della Detection e miglioramento continuo
Le regole di correlazione iniziali sono state sostituite con il baseline HWG Sababa e continuamente ottimizzate in base al contesto operativo. Questo ciclo continuo ha ridotto il rumore e migliorato l'allineamento degli alert agli eventi realmente rilevanti per il business.

Gestione strutturata degli incidenti
È stato definito un modello chiaro di escalation:
- Il SOC gestisce L1/L2
- Il team interno gestisce L3 e risposta
- Gli incidenti critici attivano escalation immediata

Evoluzione della sicurezza post-attacco
A seguito di un tentativo di attacco laterale verso Novomatic Italia, l'attività è stata rilevata tempestivamente da HyperSOC™, consentendo di bloccare la minaccia prima di qualsiasi impatto sui sistemi critici.

Di conseguenza, Novomatic ha rafforzato la propria postura di sicurezza, facendo leva su HyperSOC™ come layer centrale e introducendo:
- Secure DNS per il rilevamento di query malevole sulla rete
- Estensione dei controlli di sicurezza API
- Maggiore visibilità sui componenti infrastrutturali

Risultati: dal rumore a operazioni di sicurezza efficaci

L'adozione di HyperSOC™ ha trasformato le operazioni di sicurezza da un monitoraggio ad alto volume di alert a un modello focalizzato sull'efficacia e sulla rilevanza operativa.

Risultati operativi

- Riduzione significativa dei falsi positivi e del volume di alert (~60%)
- Maggiore efficienza del team interno
- Identificazione e prioritizzazione più rapida delle minacce rilevanti
- Collaborazione efficace tra SOC e team interno

Validazione in scenario reale

Uno scenario di attacco reale ha validato l'efficacia del modello, dimostrando la capacità di rilevare e bloccare le minacce prima che potessero impattare le operazioni critiche di business:

- Rilevamento ed escalation rapidi
- Contenimento senza impatto su sistemi critici
- Risposta coordinata
- Supporto nelle attività forensi e di reporting

Risultati operativi

L'iniziativa ha portato la cybersecurity da una funzione di monitoraggio a una componente centrale della gestione del rischio aziendale.

Anziché concentrarsi sul volume degli alert, Novomatic ha orientato il proprio approccio verso la misurazione di risultati concreti – impatto degli incidenti, efficacia della risposta e resilienza complessiva. La cybersecurity è ora:

- Integrata nella gestione del rischio aziendale
- Basata su processi strutturati e approcci sistematici
- Orientata al miglioramento continuo e alla resilienza operativa

La collaborazione ha consentito a Novomatic di passare a un modello di sicurezza orientato ai risultati, migliorando l'accuratezza della detection, riducendo il rumore operativo e rafforzando la resilienza rispetto a scenari di attacco reali.

Prospettive Future

- Novomatic continua a evolvere la propria strategia di cybersecurity, con focus su:
- Ulteriore ottimizzazione delle capacità di detection
- Automazione selettiva (a partire dagli endpoint)
- Valutazione di tecnologie SIEM di nuova generazione, potenziate da funzionalità di intelligenza artificiale per l'analisi avanzata delle minacce

L'azienda mantiene un modello ibrido, combinando competenze interne e servizi SOC esterni per garantire controllo operativo e visibilità sul panorama delle minacce.

Questo approccio riflette un cambiamento più ampio nel modo in cui Novomatic interpreta la cybersecurity:

"La cybersecurity non può essere gestita come un dominio isolato. I team interni assicurano una profonda comprensione del contesto aziendale, mentre i partner esterni offrono visibilità sul panorama delle minacce. Entrambi sono essenziali per costruire resilienza."

– Marcello David, Cybersecurity Manager, Novomatic Italia