GoSecure

SOC Prime enables GoSecure to accelerate detection workflows, improve translation accuracy, and reduce engineering overhead, reinforcing the company's position as a leading North American MXDR provider. By leveraging SOC Prime's AI-Native Detection Intelligence Platform, GoSecure cut false positives by up to 30% and doubled time-to-hunt speed. This partnership enhances MXDR coverage, lowers MTTR, boosts response effectiveness, and strengthens overall customer protection.

Industry	Region	Company Size	SIEM & XDR in Use
MSSP/MDR	North America	150+ employees	Microsoft Sentinel, Microsoft Defender for Endpoint, Carbon Black, GoSecure Countertack, Check Point Harmony, Cylerian, FortiSIEM, FortiEDR, SentinelOne

Michael Mazza
MXDR SOC Manager, GoSecure

"SOC Prime has become an essential part of our threat hunting and detection engineering workflow in Microsoft Sentinel. Its AI-assisted rule generation and cross-platform translation allow us to quickly operationalize new TTPs into validated KQL analytics and deploy them across multi-tenant Sentinel environments. This has accelerated our hunt cycles, reduced engineering overhead, and improved the overall depth of our cloud threat coverage."

Highlights

20–30% Less
False Positives

50% Reduction
In Time-to-Hunt Execution

3X Faster
Cross-Platform Content Deployment

- Rapid development and deployment of detections across the company's MXDR stack while improving customer protection and reducing MTTR
- Reduced cycle for converting detection logic into Microsoft Sentinel, Microsoft Defender for Endpoint (MDE), FortiSIEM, or Sigma
- Lower false positive rates through improved consistency and higher logic quality, leaving more time for analysts to focus on high-value investigation
- Better speed, translation accuracy, and drastically reduced engineering overhead

Challenges

Real-Time Detection Across Diverse Customer Profiles
For MSSP and MDR teams, one of the biggest challenges is ensuring consistent, high-efficacy detection content across a wide variety of customer environments. Maintaining rapid response SLAs while adapting to constantly shifting attacker TTPs spanning endpoints, cloud, network, and email requires continuous tuning and high operational maturity.

Need for Consistent & Cross-Telemetry Detections
At GoSecure, our MXDR practice covers Titan® EDR, NDR, Inbox Detection & Response (IDR), NGAV, VMaaS, SIEM+SOAR, and cloud-native Microsoft security—each with diverse data sources and versatile detection needs. The need to deliver accurate cross-platform detections across multiple data schemas and formats, including Microsoft Sentinel KQL, Defender KQL, FortiSIEM regex/CEF, and Sysmon, while supporting multi-tenant scaling and keeping pace with rapidly evolving TTPs, creates a substantial operational burden.

Diverse Security Stack Complexity & Multi-Tenant Environments
Providing round-the-clock detection, response, and expert cybersecurity services involves constantly dealing with complex and expanding customer environments. GoSecure needed a way to reduce this complexity, enhance MXDR coverage, and streamline deployment across Microsoft Sentinel, Defender, FortiSIEM, and their hosted SIEM without sacrificing speed or accuracy.

Massive Alert Volumes
Operating 24/7, the in-house engineering team processes a high volume of alerts across multiple platforms. Excess noise dilutes analyst focus, making it difficult to triage true threats quickly. High-precision detection content is critical to suppress false positives, reduce analyst fatigue, and maintain operational effectiveness.

Solution

As a North American MXDR leader delivering comprehensive defensive and offensive security services around the clock, GoSecure sought a trusted partner to accelerate threat hunting and detection engineering workflows. SOC Prime enables GoSecure to reduce environmental complexity and cut engineering overhead through a unified AI-native Detection Intelligence Platform. Leveraging Uncoder AI, MITRE ATT&CK®-mapped detection library, auto-export and integration capabilities with SIEM/XDR, AI generation of new content, and cross-platform support for Microsoft and FortiSIEM security stack enhance Titan® MXDR and GoSecure's service offerings.

Achievements

Scaling MXDR with Consistency and Precision

SOC Prime enables GoSecure to broaden its follow-the-sun defensive and offensive security services by delivering high-quality, prebuilt detections for cloud, endpoint, and SIEM environments while significantly cutting content research and development time and freeing analysts to focus on investigations. By rapidly operationalizing threat intelligence into Titan® MXDR and ensuring consistent detections across diverse customer environments, SOC Prime strengthens GoSecure's MXDR coverage and accelerates core threat response outcomes.

Stronger Threat Coverage Powered by AI-Native Detection Intel

SOC Prime's AI capabilities enhance GoSecure's service depth by generating high-fidelity detection logic for emerging threats, proactively identifying new TTPs, and enriching detection algorithms with actionable intelligence for faster analyst comprehension. A 20–30% reduction in false positives, driven by higher-quality logic, further improves operational stability, helping GoSecure maintain its leadership among North American MXDR providers.

Reduced Engineering Overhead

With SOC Prime's Uncoder AI, GoSecure can instantly convert detection logic across Microsoft Sentinel, MDE, FortiSIEM, and other platforms, generate AI-assisted detections from plain-language descriptions, apply automatic ATT&CK mapping, and accelerate enrichment and fine-tuning while streamlining validation workflows. Speed and translation accuracy deliver the most immediate value, significantly easing the burden on in-house detection engineers.

50% Faster Threat Hunting Workflows

SOC Prime boosts GoSecure's hunting efficiency by providing curated queries mapped to relevant TTPs, real-time intelligence on active threat actors and adversary campaigns, and rapid translation of hunting hypotheses into operational KQL or Sigma. With an enriched context that minimizes pre-hunt preparation, GoSecure achieves faster, more accurate, and more consistent hunts across diverse customer environments.

Higher Analyst Productivity

By leveraging SOC Prime's continuously updated detection intelligence dataset and Active Threats feed—enriched with attack flows, actionable rules, and simulation guidance—GoSecure analysts navigate the evolving threat landscape far more efficiently. SOC Prime's expertise helps accelerate research through enriched TTP context, real-world exploit insights, and AI-native detection intelligence, allowing GoSecure's analysts to spend less time correlating indicators and adversary behaviors.

Enhanced Automation Across MXDR Operations

GoSecure's heavy use of automation across Titan® MXDR and its SIEM/SOAR stack, including automated deployments, playbook-driven response, alert enrichment, triage automation, and multi-tenant rule distribution, is further amplified by SOC Prime. Machine-readable detection content, automated multi-tenant deployments, and AI-driven rule generation reduce manual workload and accelerate detection delivery, improving overall service maturity and consistency.

About GoSecure

GoSecure is a recognized cybersecurity leader and innovator, pioneering the integration of endpoint, network, and email threat detection into a single Managed Extended Detection and Response (MXDR) service. The GoSecure Titan® platform delivers predictive multi-vector detection, prevention, and response to counter modern cyber threats. GoSecure Titan® MXDR delivers rapid response and active mitigation services that directly touch the customers' network and endpoints. For over 20 years, GoSecure has been helping customers better understand their security gaps and improve their organizational risk and security maturity through MXDR and Professional Services solutions delivered by one of the most trusted and skilled teams in the industry.