AlpenShield

AlpenShield helps organizations build a SOC/MDR-like capability in-house, often across customer environments that vary widely in telemetry, data sources, and operational maturity. To keep detection coverage strong while scaling service delivery, AlpenShield partnered with SOC Prime to accelerate detection engineering and reduce the effort required to build and maintain high-quality detection intelligence. With the SOC Prime Platform as a core foundation, AlpenShield streamlines rule development and deployment, keeps detections current as threats evolve, and scales SOC enablement with low operational overhead.

Industry	Region	Company Size	SIEM & XDR in Use
MSSP/MDR, Consultancy & Training	**Central Europe (DACH)**	**5-10 employees**	**Microsoft Sentinel, Microsoft Defender for Endpoint**

Andreas Badelt
Managing Director, AlpenShield

> *“Building high-quality SIEM analytics across diverse data sources is a challenge for every security team. SOC Prime helps us deliver detection content faster and at higher quality, backed by a responsive team that supports smooth deployment of our core service.”*

Highlights

- Instant access to behavior-based detections adaptable to each customer environment
- Rapid detection logic development and application to support SOC enablement offerings across Microsoft Security products
- Improved detection engineering efficiency across diverse data sources, with less manual effort
- Lower operational overhead by reducing time spent on research, rule coding, and maintenance

Challenges

Constantly Evolving Threat Landscape

As an expert in the Microsoft Security ecosystem, AlpenShield operates in an environment defined by increasing attack volumes and growing sophistication of adversary tooling. Supporting organizations requires addressing a wide range of threat scenarios across diverse data sources and connected Microsoft technologies.

Sustaining High-Quality Detection Coverage

Effective SOC enablement depends on behavior-based detection content that evolves alongside the emerging threats and new TTPs. Ensuring consistent coverage places constant pressure on detection rules to remain accurate, relevant, and adaptable across different environments while enabling customers to build effective SOC capabilities without slowing down operations.

Detection Engineering Complexity

Building and maintaining detection logic across Microsoft Sentinel and related Microsoft Security solutions demands deep expertise and ongoing effort. Translating threat intelligence into custom, behavior-based rules, enriching them with metadata, and tuning detection logic over time puts additional burden on security teams and drives up engineering costs.

Efficient Service Offerings Scaling
Enabling SOC capabilities quickly for multiple customers while keeping engineering effort low is difficult when every environment is different: data sources vary and detection logic must be adapted across unique configurations. Scaling SOC enablement under these conditions requires reliable access to high-quality detection content and the ability to operationalize it in accordance with customers' needs.

Solution

AlpenShield enables organizations to build SOC capabilities in-house through a combination of SaaS solutions, consulting, and hands-on training. To strengthen its SOC enablement offerings and accelerate cyber defense workflows, AlpenShield chose SOC Prime as a trusted partner. Leveraging SOC Prime's AI-Native Detection Intelligence Platform, the team gains instant access to the world's largest detection intelligence dataset and ready-to-go use cases aligned with Microsoft Sentinel and the broader Microsoft ecosystem. Active Threats feed helps the team stay focused on the emerging adversary activity, while Uncoder AI supports creating, customizing, and translating detection logic for faster, tailored deployments.

Achievements

Saved Time on Threat Research and Detection Content Development

Using SOC Prime's Threat Detection Marketplace, AlpenShield gains instant access to a broad library of high-quality, production-ready rules mapped to MITRE ATT&CK and enriched with detailed intelligence. This reduces time spent researching detection logic and maintaining analytics, which drives broader visibility and scalable services for a growing customer base.

Faster Time-to-Market for Customer-Ready Detections

AlpenShield leverages SOC Prime expertise backed by AI to rapidly develop and deploy custom detection logic, responding quickly to customer requirements and bringing new capabilities to market sooner. This shortens the path from request to deployment, including fast turnaround for new sources like Microsoft Purview.

Streamlined Detection Engineering with Uncoder AI

Uncoder AI helps AlpenShield move from detection intent to a production-ready use case faster. With SOC Prime's Uncoder, the team can instantly convert detection logic across Microsoft Sentinel, Microsoft Defender for Endpoint, and other platforms, generate AI-assisted detections from plain-language descriptions, apply automated ATT&CK mapping, and accelerate enrichment and fine-tuning while streamlining validation.

Faster Coverage for Emerging Threats

SOC Prime's AI-Native Detection Intelligence Platform helps AlpenShield strengthen and expand detection coverage as new threats emerge. AI-driven capabilities accelerate high-fidelity detection logic creation enriched with actionable context, while the Active Threats feed surfaces relevant TTPs to prioritize, supporting consistent threat detection across customer environments without increasing manual workload.

Scalable SOC Enablement Across Diverse Environments

By combining ready-to-use detection content, expert support, and AI-assisted pipelines for everything from detection to simulation, AlpenShield efficiently scales its service portfolio for the entire suite of Microsoft Security solutions, delivering enterprise-grade, SOC enablement capabilities.

About AlpenShield

AlpenShield is a recognized expert in SaaS solutions, Consultancy, and Training for Microsoft Sentinel and other Microsoft Security products. AlpenShield's SOC Guru helps organizations build their own SOC/MDR-like capability in-house without needing major investments in staff, time, or infrastructure. AlpenShield manages complex components like the Microsoft Sentinel backend, use-case development, automation, enrichment, and continuous updates, letting customers focus on their core business. The platform makes enterprise-grade SOC services accessible to organizations of any size by providing automation that enriches, contextualizes, risk-scores, and triages incidents. It generates summaries and mitigation steps for high-risk events, supports analysts via natural language copilot agents, and offers on-demand expert support to fill skill gaps.