MIGRATION TO MICROSOFT SENTINEL - ESTABLISH A UNIFIED, CLOUD-NATIVE SIEM SOLUTION

What we offer

We support customers in migrating from a third-party SIEM to Microsoft Sentinel and establishing Sentinel as the primary SIEM platform for day-to-day SOC operations. The engagement follows a structured, phased approach covering Sentinel foundation, data ingestion, detection use case migration, and operational optimization.

The migration focuses on prioritized data sources and detection use cases to accelerate value realization while reducing complexity and risk. Customers benefit from Microsoft-native integration, scalable analytics, and improved visibility across their security landscape.

Microsoft Sentinel capabilities such as analytics rules, incident management, automation, and integrations with Microsoft security services are leveraged to modernize threat detection and response.

What our customers are saying

"The migration to Microsoft Sentinel significantly improved our visibility and reduced operational effort. We now operate a unified, cloud-native SIEM that enables faster detection and response across our environment."

– SOC Manager

About Reply

Reply brings together digital transformation experts and Microsoft technology enthusiasts who design and deliver high-value solutions to drive business forward. Reply has been a Microsoft Partner for over 25 years and a multiple-time "Partner of the Year" award winner. As a global Microsoft Partner, Reply currently holds all solution designations and 19 different specializations spanning Cloud & AI, AI Business Solutions, and Security.

Reply Deutschland SE
https://www.reply.com/de | microsoft.security@reply.de
See our offer on the Microsoft Commercial Marketplace

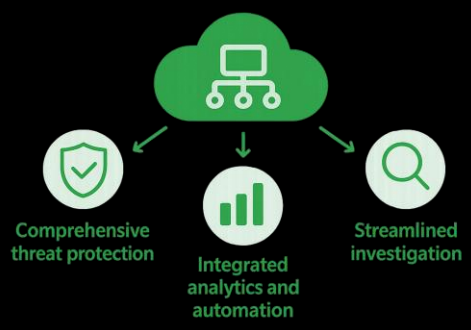
Microsoft Solutions Partner
Security

Specialist
Cloud Security
Identity and Access Management
Information Protection and Governance
Threat Protection

A STRUCTURED TRANSITION TO A MODERN SIEM PLATFORM

Why Microsoft Sentinel?

Microsoft Sentinel provides a cloud-native SIEM, integrating seamlessly with Microsoft Security services and Azure. It enables scalable threat detection, advanced analytics, and automation without the limitations of third-party SIEM platforms.



Delivery approach

- Migration scope alignment
- Data sources & use cases migrated
- SOC handover to Sentinel

Customer value

- Cloud-native SIEM visibility
- Real-time detection & response
- Reduced SIEM complexity

Engagement Details

Duration:	2+ weeks	Technologies:	Sentinel
Cost:	€ 12.000+	Company Size:	SME&C
Countries:	DACH, EU	Industry:	all

Kick-off & Scope Alignment
Migration scope, priorities, and approach confirmed.

Sentinel Foundation & Data Ingestion
Sentinel prepared and priority data sources connected.

Detection & Use Case Migration
Selected detections migrated and validated in Sentinel.

SOC Operations & Optimization
Incident workflows, SOAR automation, and operational tuning established

SOC Enablement & Handover
Knowledge transfer completed and Sentinel confirmed as primary SIEM.

Contact Reply to learn more

Peter Altheimer
Associate Partner
DE, Munich
p.altheimer@reply.de
+49 151 147 100 11

Christoph Sondermann
Head of Security
DE, Cologne
c.sondermann@reply.de
+49 174 966 7335

Reply Deutschland SE
https://www.reply.com/de | microsoft.security@reply.de
See our offer on the Microsoft Commercial Marketplace

Microsoft Solutions Partner