

Cloud Security Operation Center (CSOC) by Reply - Verified MXDR Service

Verified MXDR Security Service Offering including 24/7 Security Monitoring, Threat Detection, Incident Response, Penetration Testing

Excellence

Discover unparalleled security with Reply's Verified MXDR Service, expertly tailored to integrate and amplify your Microsoft 365 ecosystem. From initial setup to advanced operational capabilities, our 24/7 Security Monitoring, Threat Detection, Incident Response, and Penetration Testing services are the cornerstones of digital resilience.

Overview

At Reply, we deliver a comprehensive Managed Security Services ecosystem designed to fortify your operations against the spectrum of cyber threats. Central to our approach is the Reply Cloud Security Operation Center (CSOC), operating round-the-clock every day of the year to maintain vigilance over your digital landscape through Microsoft Sentinel.

Our commitment is embodied in a team of seasoned Security Analysts and Engineers based in Germany, who combine proactive threat hunting with AI-enhanced analytics to preemptively counteract emerging threats. The "Reply Content Gallery" repository enriches Microsoft Sentinel with the latest actionable intelligence, while Power BI dashboards and regular reviews ensure your security posture is continuously optimized.

Beyond vigilant surveillance and threat mitigation, Reply extends its suite to challenge system security through penetration tests, provide advisory for platform vulnerability management, and deploy on-site incident response if required—each capable of standing up to the scrutiny of legal proceedings.

Key Features

- **Direct and Expert Communication:** Immediate access to security professionals through integrated platforms like Microsoft Teams and dedicated review sessions.
- **Proactive Approach:** Regular threat hunting and strategic reviews to pre-emptively

address and mitigate potential threats.

- **24/7 Comprehensive Surveillance:** Utilizing Microsoft Sentinel and Microsoft Defender XDR Portal for continuous monitoring and threat detection.
 - **Certified Excellence:** Upholding the highest standards of quality and security management, we are proud to be ISO 27001 and ISO 9001:2015 certified, demonstrating our commitment to robust information security practices and superior quality management systems.
-

Bridging the Gap with Reply's Expertise

We understand that navigating the extensive capabilities of Microsoft 365 can be challenging. Reply bridges this gap by:

- Assisting in the configuration and optimization of Microsoft Defender within Microsoft 365 to enhance endpoint and identity protections.
 - Implementing best practices for secure collaboration and communication tools available in Microsoft 365, ensuring secure and efficient workflows.
 - Providing expert guidance to tailor Microsoft 365 security policies and governance to fit your unique organizational needs, backed by our ISO certifications.
-

Service Blocks

Analytics & Reporting

Our Analytics & Reporting service enhances the security posture of environments by perpetually improving analytic rules within our clients' repositories. Each month, detailed CSOC reports are generated, offering actionable recommendations for settings and configurations aligned with our best practice blueprints. Additionally, clients are provided with access to Power BI Reports, delivering a rich, in-depth view of their security standing to inform strategic decision-making.

Active Threat Hunting

The Active Threat Hunting service proactively searches client tenants for emerging threats and cutting-edge attack methodologies as uncovered by our dedicated threat research team. This vigilant exploration broadens the understanding of the threat environment, substantially improving the caliber of our clients' defenses.

Security Training & Awareness

Our Security Training & Awareness initiatives are designed to fortify organizations by educating their personnel on how to identify and counter cyber threats. Engaging training

modules and awareness campaigns cultivate a robust security-minded culture, diminishing risk and reinforcing the frontline of defense.

Penetration Testing Services

Penetration Testing Services from Reply methodically probe infrastructure, network, and application layers to detect and seal security gaps. Utilizing controlled cyber attack simulations, we rigorously test and affirm the resilience of clients' digital ecosystems, ensuring comprehensive readiness against potential threats.

Incident Response (SANS Framework)

Adopting the SANS framework, our Incident Response protocol is meticulously crafted to address and neutralize cyber threats efficiently. This full-spectrum service includes preparedness, prompt identification, strategic containment, and thorough eradication of threats, followed by recovery and detailed post-incident evaluations, enhancing our clients' future security strategies.

Reply's Commitment

By aligning with Reply, you gain more than just a security provider—you acquire a strategic partner that scales with you, ensuring your defenses remain robust and responsive in the face of evolving digital threats. Our suite is not only about protection; it's about enabling your business to thrive securely in the digital era.