

Argumentation Paper

NIS-2 Compliance with Log Management & SIEM



Date: 04.02.2026

Author: i-Vertix Compliance Team

PARTNER ARGUMENTATION PAPER: NIS-2 COMPLIANCE WITH LOG MANAGEMENT & SIEM

April 2026

Introduction: Turning Compliance into Opportunity

The EU NIS-2 Directive represents a major step forward in standardizing cybersecurity across member states. For organizations, compliance can appear complex due to the broad scope of requirements, but it also presents an opportunity to strengthen security, reduce operational risks, and gain stakeholder trust.

End customers need solutions that provide real-time visibility, actionable insights, and rapid incident response, all while adhering to regulatory deadlines. Partners play a critical role by guiding clients, providing tools, and ensuring effective implementation of log management and Security Information and Event Management (SIEM).

This paper provides a detailed, partner-focused guide to help convince end customers of the value of NIS-2 compliance and the benefits of robust log management and SIEM practices.

National Timelines

- Germany: NIS-2 obligations are mandatory starting 2026.
- Italy: Compliance must be achieved by October 2026.
- Other EU countries: Timelines vary; partners must help customers confirm local requirements.
- Partner argument: Early action ensures compliance, avoids fines, and strengthens cybersecurity posture.

Key Customer Benefits of NIS-2 Compliance

PGUM S.r.l

NOI Techpark
Via Ipazia 2
39100 Bolzano - Italia

Mail: info@i-vertix.com
PEC: pgumgmbh@pec.it
Web: i-vertix.com

Cod. Fisc. e P.IVA: 02923310219
REA: BZ - 216954

1. Mandatory Reporting of Security Incidents

- Failure to report significant incidents can lead to fines and reputational damage.
- Partners can implement monitoring systems and automated SIEM alerts to ensure timely reporting.

2. Consolidation of Security Measures

- NIS-2 integrates individual measures into a single framework.
- Partners provide tools and guidance to standardize security practices, making operations more predictable and auditable.

3. Operational Security & Risk Reduction

- Continuous monitoring, vulnerability scanning, and real-time alerting protect critical assets.
- SIEM correlates events across multiple systems to provide actionable insights.

DETAILED IMPLEMENTATION GUIDE FOR END CUSTOMERS

1. Asset Inventory

- Maintain a complete inventory of IT systems, endpoints, applications, and sensitive data.
- Identify critical assets to prevent untracked systems from creating vulnerabilities.
- Partner role: Offer tools and advisory services for asset discovery, classification, and ownership assignment.

2. System Monitoring & Log Management

- Implement continuous monitoring to detect vulnerabilities, anomalies, and threats.
- Collect and analyze logs systematically; configure SIEM for alerting and correlation.

PGUM S.r.l

NOI Techpark
Via Ipazia 2
39100 Bolzano - Italia

Mail: info@i-vertix.com
PEC: pgumgmbh@pec.it
Web: i-vertix.com

Cod. Fisc. e P.IVA: 02923310219
REA: BZ - 216954

- Benefit: Early threat detection reduces potential impact.
- Partner role: Deploy log management and SIEM solutions, optimize configurations, and provide ongoing support.

3. Incident Detection & Response

- Implement automated detection and response systems (EDR/NDR).
- Integrate patch management with monitoring workflows.
- Benefit: Fast, coordinated response reduces operational impact.
- Partner role: Offer managed detection and response services for clients.

4. Awareness & Policies

- Train staff on secure behavior, data handling, and incident reporting.
- Define and enforce Identity & Access Management (IAM) and incident escalation policies.
- Partner role: Provide training programs, templates, and advisory support.

5. Transparency & Risk Visibility

- Continuously monitor endpoints, networks, and applications through SIEM.
- Detect unauthorized or forgotten tools and bring them into compliance.
- Partner role: Provide dashboards, reporting, and advisory for full operational visibility.

6. Emergency & Response Planning

- Define response procedures for security incidents, including containment, reporting, and recovery.
- Ensure compliance with local timelines (Germany 2026, Italy October 2026).
- Partner role: Assist in creating, implementing, and testing incident response and disaster recovery plans.

PGUM S.r.l

NOI Techpark
Via Ipazia 2
39100 Bolzano - Italia

Mail: info@i-vertix.com
PEC: pgumgmbh@pec.it
Web: i-vertix.com

Cod. Fisc. e P.IVA: 02923310219
REA: BZ - 216954

7. Communication & Continuous Training

- Ensure employees are informed about security procedures and updates.
- Conduct regular refresher training sessions.
- Partner role: Provide platforms and materials for consistent communication and education.

8. Supply Chain Risk Management

- Assess risks from third parties with access to systems or applications.
- Implement Zero Trust and Multi-Factor Authentication (MFA) for all external parties.
- Partner role: Help integrate third-party monitoring and security into SIEM and log management frameworks.

NATIONAL TIMELINE AWARENESS

- Germany: Compliance mandatory from 2026
- Italy: Compliance mandatory by October 2026
- Partners should emphasize the urgency of early implementation to reduce risk and avoid fines.

SUMMARY: WHY END CUSTOMERS NEED PARTNER SUPPORT

1. Regulatory Guidance: Interpretation and application of NIS-2 requirements.
2. Technology Implementation: Deployment of log management, SIEM, and monitoring tools.
3. Process Integration: Embedding detection, response, and reporting into operations.

PGUM S.r.l

NOI Techpark
Via Ipazia 2
39100 Bolzano - Italia

Mail: info@i-vertix.com
PEC: pgumgmbh@pec.it
Web: i-vertix.com

Cod. Fisc. e P.IVA: 02923310219
REA: BZ - 216954

4. Operational Security: Proactive threat detection and risk mitigation.
5. Staff Enablement: Training on secure practices and incident handling.
6. Documentation & Compliance: Maintain evidence for audits and reporting.
7. Supply Chain Security: Secure third-party access and enforce policies.

Partner Value Proposition:

- Position as trusted advisor for compliance and cybersecurity.
- Deliver measurable security improvements.
- Enable early compliance for Germany (2026) and Italy (October 2026).
- Provide recurring managed services for log management and SIEM operations.

Strategic Benefits for End Customers

- Regulatory Assurance: Meet NIS-2 requirements across different EU member states.
- Risk Reduction: Detect threats early, minimize impact of breaches, and secure sensitive data.
- Operational Efficiency: Centralized log management and SIEM provide actionable insights and streamline response processes.
- Staff Competence: Employees understand security responsibilities and adhere to policies.
- Supply Chain Security: Third-party access is controlled and monitored, reducing indirect risk exposure.

PARTNER VALUE PROPOSITION

PGUM S.r.l

NOI Techpark
Via Ipazia 2
39100 Bolzano - Italia

Mail: info@i-vertix.com
PEC: pgumgmbh@pec.it
Web: i-vertix.com

Cod. Fisc. e P.IVA: 02923310219
REA: BZ - 216954

- **Trusted Advisor Role:** Partners guide clients through the complex regulatory landscape, delivering structured NIS-2 compliance programs.
 - **Technology Enablement:** Provide and configure log management and SIEM solutions tailored to client environments.
 - **Managed Services:** Ensure continuous monitoring, automated alerting, and rapid incident response.
 - **Revenue Growth:** Partners can expand recurring business by offering compliance, monitoring, and training services.
 - **Competitive Differentiation:** Organizations gain not only compliance but also enhanced cybersecurity posture, operational resilience, and stakeholder trust.
-

Conclusion

NIS-2 compliance is a mandatory yet transformative initiative. By focusing on log management and SIEM, organizations can achieve regulatory adherence, strengthen cybersecurity defenses, and improve operational visibility. Partners are uniquely positioned to deliver these outcomes, providing clients with the expertise, tools, and ongoing support needed to navigate the evolving cybersecurity landscape successfully.

For management, the takeaway is clear: early engagement with a knowledgeable partner ensures compliance with national timelines (Germany 2026, Italy October 2026), mitigates risk, and transforms regulatory requirements into tangible business value.

PGUM S.r.l

NOI Techpark
Via Ipazia 2
39100 Bolzano - Italia

Mail: info@i-vertix.com
PEC: pgumgmbh@pec.it
Web: i-vertix.com

Cod. Fisc. e P.IVA: 02923310219
REA: BZ - 216954