cymulate

SOLUTION BRIEF

NIS2 Directive

ACHIEVE COMPLIANCE WITH AUTOMATED EXPOSURE VALIDATION

Addressing NIS Directive Gaps

The original 2016 NIS Directive aimed to boost cybersecurity across the EU but fell short of addressing modern threats. To strengthen resilience and ensure a high level of security, the 2022 NIS2 Directive introduced stricter security requirements and expanded in-scope organizations with standardized criteria.

Cymulate simplifies NIS2 compliance by breaking down complex mandates and providing a practical, easy-to-follow approach. Cymulate helps accelerate your path to compliance.

NIS2 Non-Compliance

Organizations that fail to comply with NIS2 requirements are subject to legal and financial consequences. These could include administrative fines up to €10 million or 2% of global annual turnover, whichever is higher. Additionally, supervisory authorities may hold executives personally liable.

Why Cymulate for NIS2 Compliance?

By leveraging the Cymulate Exposure Validation Platform, organizations can accelerate their path to adherence, strengthen their overall security posture and reduce the risk of costly non-compliance penalties. Cymulate enables organizations to proactively manage cyber risk, provide audit-ready compliance evidence and continuously improve cyber resilience.

Cymulate empowers your organization to meet the following NIS2 cybersecurity compliance requirements:

- **Proactive threat cybersecurity**
- **Endpoint device security validation**
- **Automation and artificial intelligence (AI)**
- **Threat prevention and detection**
- **Increased cybersecurity awareness**
- **Risk assessments and vulnerability management**
- **Phishing training and awareness**

> **"Because we continuously track our security performance with Cymulate, I always show the platform's analytics during our compliance audits. They appreciate that I consistently have a third party evaluate my security, which gives them an unbiased perspective. Additionally, I can show them that even if an attack penetrates my defenses, I still have compensating controls to protect the organization."**
>
> – CISO, Large Industrial Organization

Solution Benefits

Proactively conduct threat validation

Comply with NIS2 by conducting automated threat validation to proactively prevent, detect, monitor and mitigate threats.

Prove ransomware resilience

Test and optimize endpoint defenses against ransomware attacks and improve awareness of device risks.

Leverage automation & AI

Utilize Cymulate AI-powered threat exposure validation to automate and streamline scoping and detection engineering processes.

Validate threat exposures

Easily convert the latest threat intelligence into assessment scenarios in minutes to quickly validate threats and identify exposures.

Elevate risk management

Prioritize and mitigate the threat gaps with the greatest risk and ensure allocation of proper risk-management resources.

Improve Threat Prevention, Detection, Monitoring & Remediation

Requirement: Utilize active cyber protection to improve the prevention, detection, monitoring, analysis and mitigation of threats.

Directive Source: Preamble (57, 105), Article 7 (2.j)

Deploy the Cymulate Exposure Validation Platform in your environment to continuously test defenses and validate security controls, monitor for cyber drift, and implement automated remediations. Quickly close security gaps and improve prevention and detection before attackers strike.

Increase Endpoint Device Security

Requirement: Enhance cybersecurity and overall awareness of device risks and develop policies to address the rise of ransomware attacks.

Directive Source: Preamble (50, 54, 89)

Cymulate increases endpoint device risk awareness and optimizes endpoint security controls by continually running endpoint threat attack simulations. Easily run comprehensive ransomware risk assessments and rapidly mitigate endpoint security risks in your environment.

Conduct Continuous Risk Assessments

Requirement: Implement a proactive risk management culture allowing for quick identification and remediation of network and information system vulnerabilities and take mitigation measures appropriate to the risks faced. In addition, conduct risk assessments and integrate technologies.

Directive Source: Preamble (58, 76, 77, 96, 97), Article 7 (2.c, 2.e), Article 21 (2.f)

The Cymulate Platform, integrated with your security technologies, empowers automated risk assessments to identify, prioritize and remediate missed threat gaps – enabling continuous validation of security controls, rapid mitigations of critical exposures and strategic allocation of risk management resources.

Why choose Cymulate?

Automated validation

More than 1000 test scenarios using thousands of known malicious file samples and behaviors to simulate real-world attacks.

Security integrations

Out-of-the-box integrations with leading SIEM, EDR and XDR platforms to validate detection, log collection and visibility to threats.

Threat prevention & detection

Actionable and automated findings to maximize threat prevention and optimize detection for the most effective threat coverage.

About Cymulate

Cymulate, the leader in exposure management and security validation, provides the single source of truth for threat exposure and the actions required to close security gaps before attackers can exploit them. More than 500 customers worldwide rely on the Cymulate platform to baseline their security posture and strengthen cyber resilience with continuous discovery, validation, prioritization, and guided remediation of security weaknesses. Cymulate automates advanced offensive security testing to validate controls, threats, and attack paths. As an open platform, Cymulate integrates with existing security and IT infrastructure and drives the workflows of the exposure management process. For more information, visit www.cymulate.com.