SOLUTION BRIEF

Unpacking NIS2: Ensuring compliance by leveraging Tanium

The landscape of cybersecurity has been continually evolving in response to an increasingly interconnected world. One of the more recent developments is the European Union's Network and Information Systems (NIS) Directive, which has been updated to NIS2 in order to address the growing challenges faced by modern organizations. NIS2 will come into force in 2024 – so it's time to prepare.

What is NIS2?

NIS2 is the revised and updated version of the European Union's (EU) first major cybersecurity regulation, the NIS Directive. Implemented in 2016, the NIS Directive aimed to bolster the security of critical infrastructure and essential services across the EU. NIS2, officially known as the 'Directive on measures for a high common level of cybersecurity across the Union', expands and strengthens the original directive, providing a more comprehensive framework for managing cybersecurity risks and incidents.

The main goals of NIS2 are to:

- Increase the security and resilience of essential services and critical infrastructure.
- Improve the overall cybersecurity posture of EU member states.
- Enhance cooperation and information sharing among member states.
- Raise awareness of cybersecurity risks and promote a culture of risk management.

Why do companies need to be compliant with NIS2?

NIS2 compliance is crucial for organizations for several reasons:

- **Legal obligations:** Companies operating within the EU or providing services to EU citizens must adhere to NIS2 regulations. Non-compliance may result in significant fines and legal repercussions.
- **Reputation:** Demonstrating a strong commitment to cybersecurity can help build trust with customers, IT partners, and stakeholders, while non-compliance can tarnish an organization's image.
- **Competitive advantage:** Companies that are proactive in their cybersecurity efforts and compliant with NIS2 are more likely to gain a competitive edge in the market, as they can demonstrate a higher level of security to clients and investors.
- **Risk mitigation:** Compliance with NIS2 means that organizations are taking the necessary steps to protect their networks and information systems, thus reducing the likelihood of costly cyber incidents.
- **Managing third-party risk:** Contrary to the previous directive, NIS2 cybersecurity rules apply not only to the organizations that fall under its expanded definition of 'critical' but also to the subcontractors and service providers that assist such organizations.
- **Incident reporting:** NIS2 establishes more stringent requirements for incident reporting. Major security incidents must now be reported to critical entities within 24 hours of their discovery. Organizations must provide a preliminary analysis of the incident within 72 hours of its discovery and submit a thorough final report within a month of detection.

Why organizations should turn to Tanium to achieve NIS2 compliance.

Tanium is the industry's only provider of converged endpoint management (XEM). Applying XEM dramatically improves the management of complex security and technology environments. Only Tanium protects every team, endpoint, and workflow from cyber threats by integrating IT, Compliance, Security, and Risk into a single platform that delivers comprehensive visibility across devices, a unified set of controls, and a common taxonomy for a single shared purpose: to protect critical information and infrastructure at scale. This makes Tanium uniquely positioned to assist organizations within the EU to become compliant with NIS2.

Tanium helps in several ways:

Centralized management

Many companies have deployed a diverse set of networking and security tools over the years. These usually do not work well with each other, so breaches may not be detected in time, and it is difficult to get a complete overview of all the assets the company is held responsible for. Tanium solves that with its Converged Endpoint Management (XEM): from a central location, the entire endpoint infrastructure can be managed. That helps streamline compliance efforts and reduces the time and resources required to achieve compliance.

Real-time visibility

Tanium's platform provides organizations with real-time visibility into all their digital assets, thus allowing them to identify and assess risks and remediate across their digital infrastructure, any place, any time, and in seconds – not hours, days, or weeks.

Real-time prioritization

Risk prioritization can help IT teams evaluate the IT infrastructure beyond data vulnerabilities to help determine which vulnerabilities to patch and assess an endpoint's security level – which can dramatically change the risk level. By prioritizing risks, security teams can more effectively allocate their already limited resources to focus on mission-critical tasks.

Real-time and automated compliance checks

Tanium ensures real time and automated compliance checks by continuously monitoring endpoints on their data, users, configurations, and software (Bill of Material). It employs advanced algorithms to compare this data against predefined compliance policies, generating alerts and remedial actions when violations are detected, thus enabling swift and proactive compliance management.

Real-time risk mitigation/remediation

Leveraging its comprehensive endpoint visibility and control platform, Tanium swiftly identifies vulnerabilities, assesses risks, and initiates immediate response actions across all endpoints. This proactive approach ensures rapid threat detection, containment, and remediation, thus minimizing potential damage and enhancing one's overall security posture.

Real-time incident response

Tanium continuously monitors and collects data from endpoints, providing instant visibility into security incidents. With its rapid query and response capabilities, Tanium enables organizations to quickly investigate and remediate threats, thus minimizing the impact of security incidents.

Improve cyber hygiene

Tanium's continuous monitoring capabilities help to improve cyber hygiene by ensuring that all endpoints are up to date with patches, software updates, and security configurations.

Simplify compliance reporting

Tanium can simplify compliance reporting by generating comprehensive reports that demonstrate compliance with NIS2 regulations and provide evidence of due diligence.

Why work with Tanium?

Organizations that fall under the NIS2 directive need to collaborate with Tanium for compliance with NIS2 because of the huge amount of work that needs to be done to comply. IT departments need to be able to easily automate and scale their activities and processes and Tanium is the only technology that can do that reliably and resiliently across all assets with a single platform. Tanium provides instant visibility into their IT infrastructure, empowering real-time monitoring, and threat detection. Its extensive control capabilities allow efficient management of assets, configurations, and vulnerabilities.

Tanium's unparalleled speed enables rapid response to security incidents and compliance requirements. Its platform technology and multiple integrations with well-established vendors facilitate streamlined process operations. By partnering with Tanium, organizations gain a comprehensive solution that addresses their compliance needs with efficiency, agility, and enhanced security.

Tanium works closely with a portfolio of partners who can assist organizations in advising on NIS2, and implement the solutions required.

SEE TANIUM IN ACTION

See, control and remediate every endpoint in real time on the industry's only converged endpoint management (XEM) platform.

SEE DEMO