PHOENIX SECURITY

ACT NOW

ON RISK

FIX VULNERABILITIES

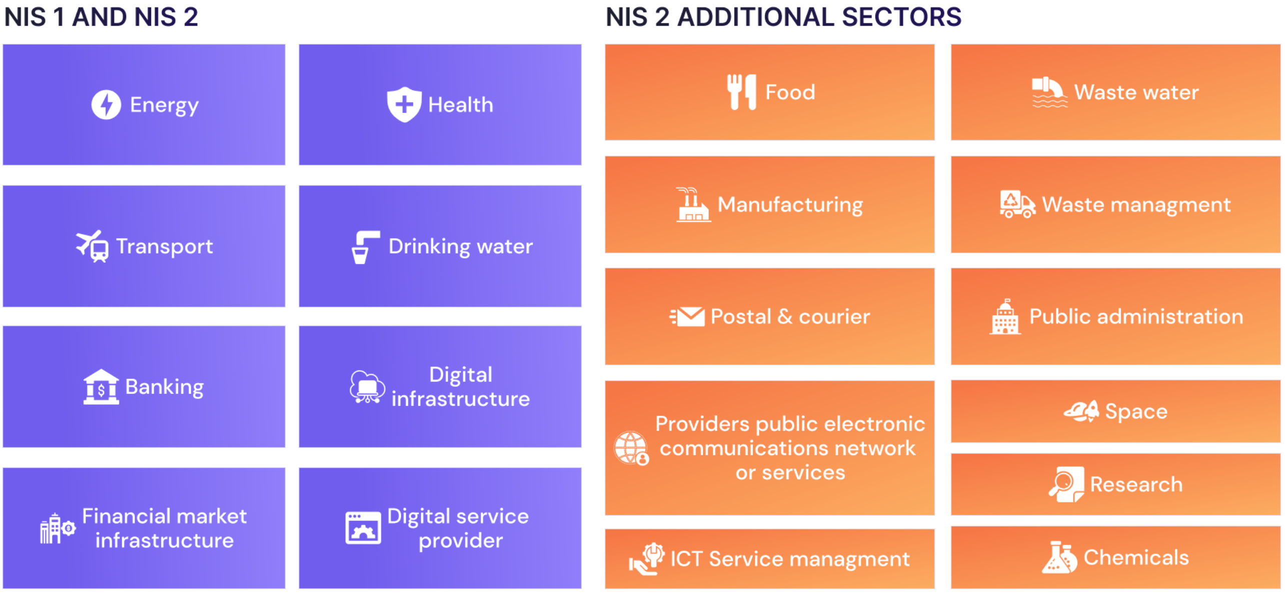
Risk Based Application & Cloud Security Posture Management

Introducing NIS 2: A new era for Cybersecurity in the EU and the impact on Vulnerability management

NIS2 Directive: https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new

The European Union has recently introduced a revised Network and Information Systems Directive, or NIS 2, which aims to improve the cybersecurity of essential services and digital service providers across the EU. This new regulation replaces the original NIS Directive, adopted in 2016.

NIS 2 applies to a wide range of operators of essential services and digital service providers, including energy, transport, banking, healthcare, and digital services such as online marketplaces and search engines. The regulation aims to establish a common level of security for these services across the EU, by requiring organizations to implement appropriate security measures and to report significant security incidents to the relevant authorities.



NIS 1 AND NIS 2

Energy	Health
Transport	Drinking water
Banking	Digital infrastructure
Financial market infrastructure	Digital service provider

NIS 2 ADDITIONAL SECTORS

Food	Waste water
Manufacturing	Waste managment
Postal & courier	Public administration
Providers public electronic communications network or services	Space Research
ICT Service managment	Chemicals

NIS2 and NIS 1 what are the differences

Scope is probably the biggest differentiator between the two regulation did have a more limited scope. One of the key differences between the NIS1 directive version 1 (NIS1) and version 2 (NIS2) is the expanded scope of NIS2. While NIS1 only applies to operators of essential services in specific sectors (such as energy, transport, healthcare, and finance).

Expanded Scope NIS 2 Directive

- Public electronic communication services
- Digital Service
- Manufacturing
- Space
- Waste water and waste managment
- Postal & courier
- Food
- Public administration

NIS2 extends the directive's reach to include additional industries and digital service providers. This means that more organizations across the EU are subject to the requirements of the directive, including those in the water supply and distribution sector, the food supply sector, and the digital infrastructure sector. Digital service providers that offer online marketplaces, search engines, and cloud computing services are now within the directive's scope. The expansion of the scope reflects the growing importance of digital infrastructure and the need to improve the resilience of network and information systems across a broader range of sectors.

Other differentiators

Area	NIS1	NIS2
Scope	Applies only to operators of essential services in specific sectors (e.g., energy, transport, healthcare, finance)	Extends to additional sectors and digital service providers
Thresholds	No thresholds for identifying operators of essential services	New thresholds for identifying operators of essential services and digital service providers
Incident reporting	Operators of essential services must report incidents to a competent authority	New requirements for incident reporting

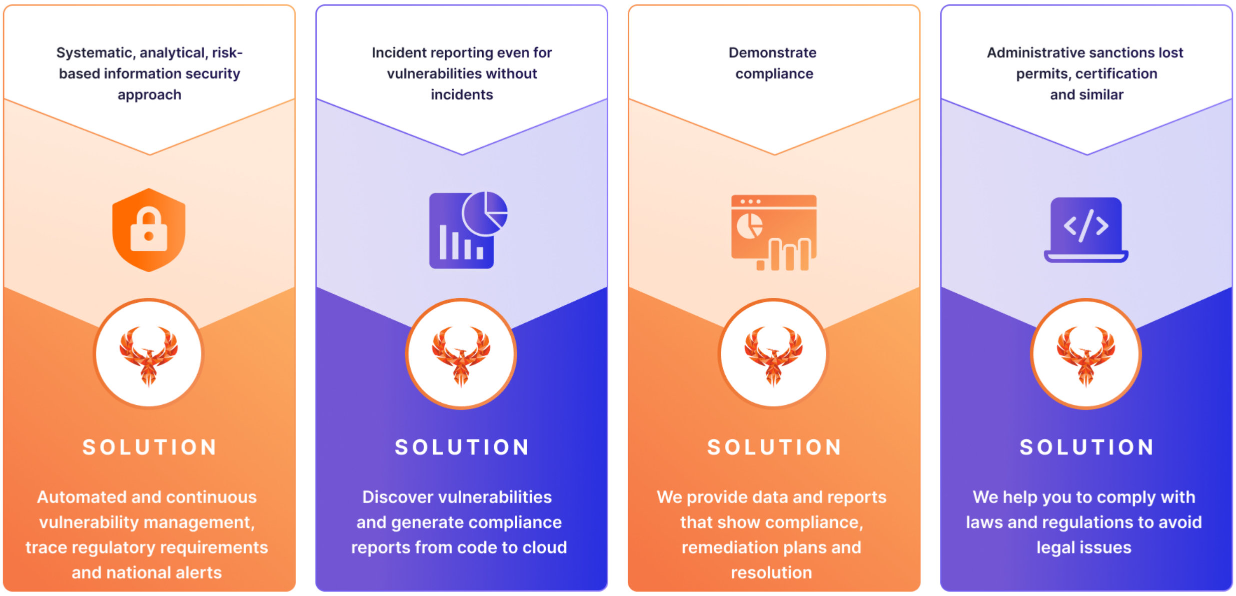
Area	NIS1	NIS2
Penalties	No specific penalties for non-compliance	Empowers national authorities to impose fines and other administrative measures
Cooperation	Emphasizes cooperation and information sharing between national authorities	Emphasizes cooperation and information sharing between national authorities and the EU Agency for Cybersecurity

Key Features of NIS2 in details:

- **Scope:** NIS 2 applies to all operators of essential services and digital service providers established in the EU and those that provide services within the EU.
- **Risk assessment:** Operators of essential services and digital service providers must conduct a risk assessment to identify and assess the risks to the security of their network and information systems.
- **Incident management:** Organizations must establish an incident management plan that outlines procedures for detecting, reporting, and responding to security incidents.
- **Security measures:** Organizations must implement appropriate technical and organizational security measures to manage the risks identified in the risk assessment. This may include access controls, encryption, monitoring and logging, and regular security updates and patches.
- **Testing and evaluation:** Organizations must regularly test and evaluate the effectiveness of their security measures, including vulnerability assessments and penetration testing.
- **Reporting:** Organizations must report significant security incidents to the relevant national authorities, as well as any relevant supervisory authorities or other stakeholders.
- **Cooperation:** Organizations must cooperate with other stakeholders, including other operators of essential services, national authorities, and other relevant bodies, to share information and coordinate responses to security incidents.

Overall, NIS 2 represents a significant step forward in the EU's efforts to improve cybersecurity and protect essential services and digital services from cyber threats. By establishing a common level of security across the EU, the regulation aims to ensure that organizations are better equipped to detect and respond to security incidents and to minimize the impact of these incidents on the services they provide.

How Can Phoenix Help With NIS2 Demands



Systematic, analytical, risk-based information security approach

SOLUTION

Automated and continuous vulnerability management, trace regulatory requirements and national alerts

Incident reporting even for vulnerabilities without incidents

SOLUTION

Discover vulnerabilities and generate compliance reports from code to cloud

Demonstrate compliance

SOLUTION

We provide data and reports that show compliance, remediation plans and resolution

Administrative sanctions lost permits, certification and similar

SOLUTION

We help you to comply with laws and regulations to avoid legal issues

How does nis2 apply to you? And how does NIS2 impact vulnerability management

1. Risk assessment: Article 14(1) of the NIS 2 regulation requires operators of essential services and digital service providers to "identify and assess the risks posed to the security of their network and information systems." This includes conducting a risk assessment that considers the "likelihood and impact of a security incident."

2. Incident management: Article 14(2) of the NIS 2 regulation requires operators of essential services and digital service providers to "establish and implement appropriate and proportionate technical and organizational measures to manage the risks posed to the security of network and information systems" and to "detect and promptly respond to incidents."

3. Security measures: Article 14(3) of the NIS 2 regulation requires operators of essential services and digital service providers to "take into account state of the art" and to implement "appropriate and proportionate technical and organizational measures" to ensure the security of their network and information systems.

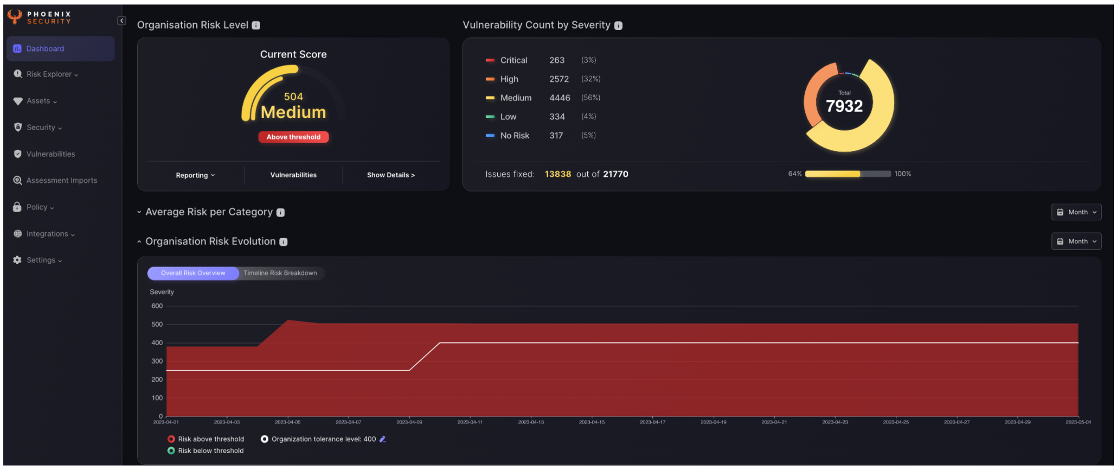
4. Testing and evaluation: Article 14(4) of the NIS 2 regulation requires operators of essential services and digital service providers to "regularly test and evaluate the effectiveness" of their security measures, including "vulnerability assessments, including penetration testing."

5. Reporting: Article 16(1) of the NIS 2 regulation requires operators of essential services and digital service providers to "notify without undue delay the competent authority" of any "incident having a significant impact" on the continuity of the services they provide.Cooperation: Article 14(5) of the NIS 2 regulation requires operators of essential services and digital service providers to "cooperate with the relevant competent authorities and other relevant stakeholders" to "prevent, detect, respond to and recover from incidents."

How can Phoenix Security Help you address NIS2?

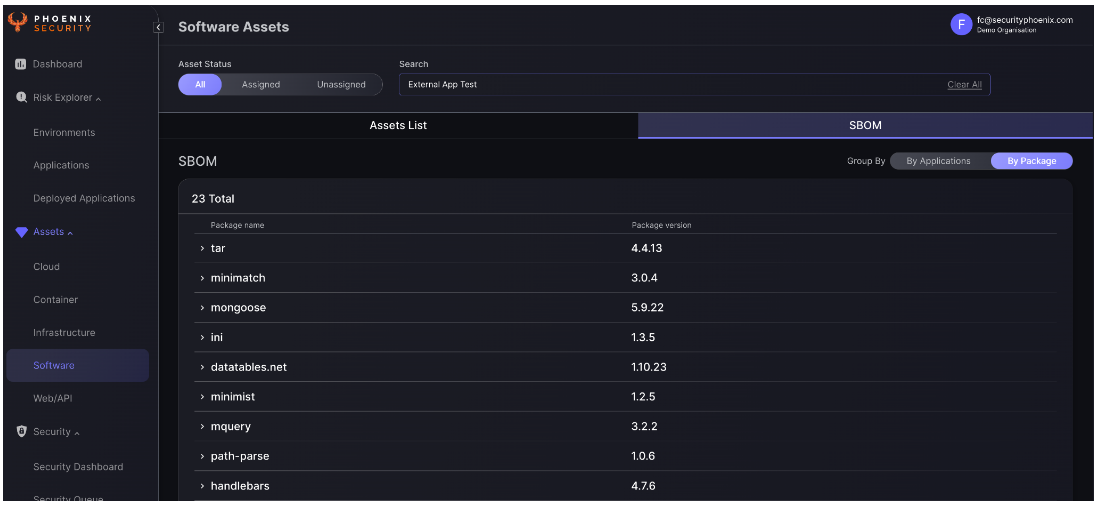
<table>
<tr><th>NIS 2
Requirements</th><th>How Phoenix Security can address the requirement</th></tr>
<tr><td><b>Risk assessment:</b>
<b>Article 14(1)</b></td><td>

Phoenix security enables real-time and systematic assessment of application security, cloud, and infrastructure risks.

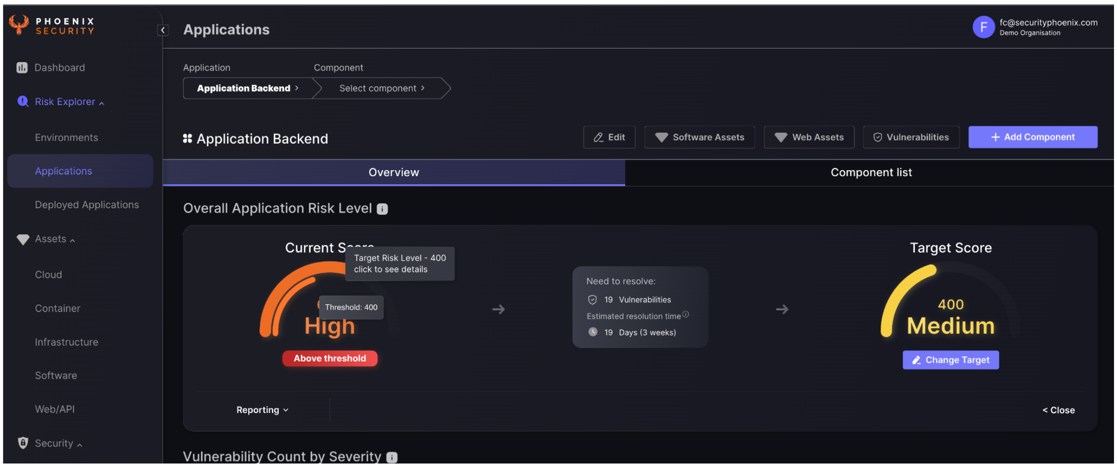


</td></tr>
</table>

<table>
<tr><th>NIS 2
Requirements</th><th>How Phoenix Security can address the requirement</th></tr>
<tr><td><b>Incident management: Article 14(2)</b></td><td>
Phoenix security enables the reconstruction of incident data by leveraging contextual searches and providing vulnerability information in real-time. It allows easy assessment and scheduling of upgrades and searches all systems and teams affected with just one click.



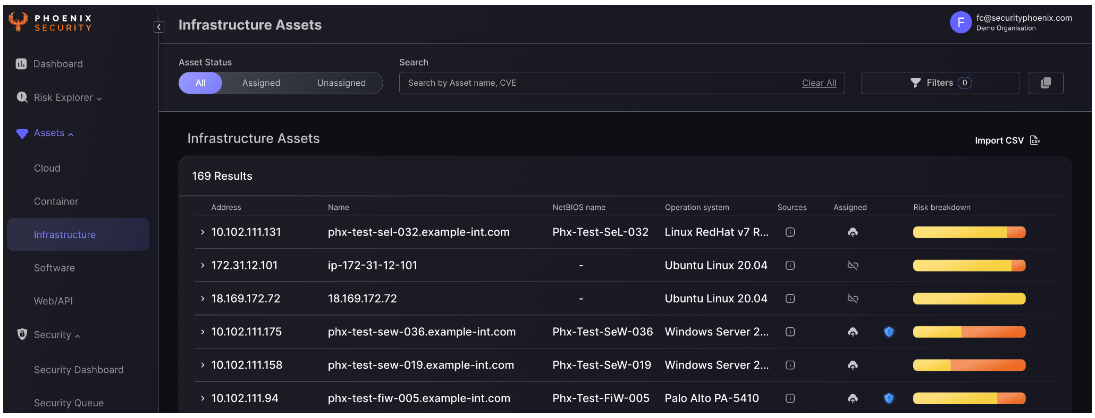
Software Assets
fc@securityphoenix.com
Demo Organisation
Asset Status: All
Search: External App Test
SBOM
Group By: By Package
23 Total
<table>
<tr><th>Package name</th><th>Package version</th></tr>
<tr><td>tar</td><td>4.4.13</td></tr>
<tr><td>minimatch</td><td>3.0.4</td></tr>
<tr><td>mongoose</td><td>5.9.22</td></tr>
<tr><td>ini</td><td>1.3.5</td></tr>
<tr><td>datatables.net</td><td>1.10.23</td></tr>
<tr><td>minimist</td><td>1.2.5</td></tr>
<tr><td>mquery</td><td>3.2.2</td></tr>
<tr><td>path-parse</td><td>1.0.6</td></tr>
<tr><td>handlebars</td><td>4.7.6</td></tr>
</table>
</td></tr>
<tr><td><b>Security measures and demonstrating compliance</b></td><td>
Phoenix security enables assessment of the real risk of specific applications and controls and specifies which compensating controls apply to specific applications or environments to ensure compliance.



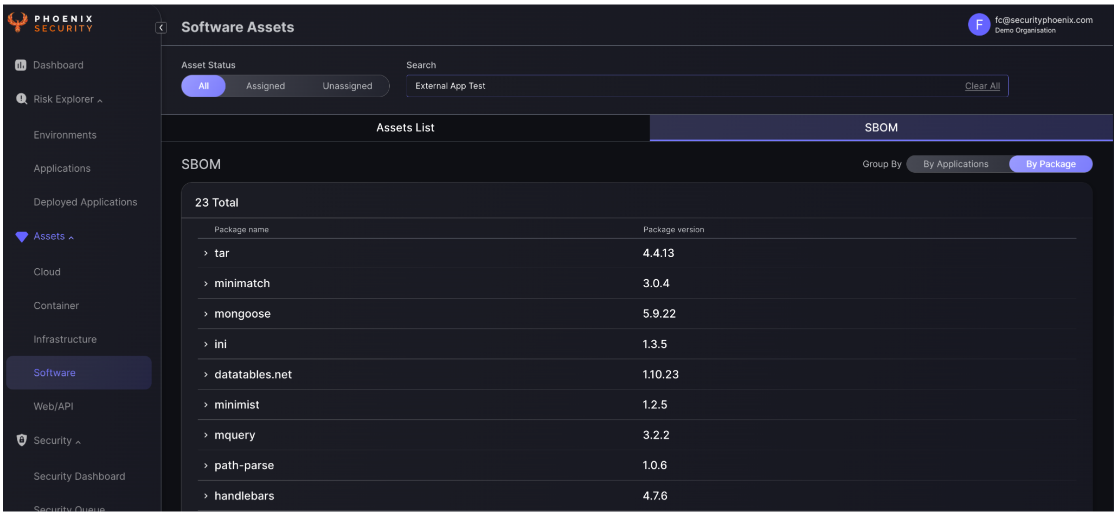
Applications
fc@securityphoenix.com
Demo Organisation
Application: Application Backend
Component: Select component
Application Backend
Overall Application Risk Level
Current Score
Target Risk Level - 400
click to see details
Threshold: 400
High
Above threshold
Need to resolve:
19 Vulnerabilities
Estimated resolution time
19 Days (3 weeks)
Target Score
400
Medium
Vulnerability Count by Severity
</td></tr>
</table>

<table>
<tr><th>NIS 2

Requirements</th><th>How Phoenix Security can address the requirement</th></tr>
<tr><td><b>Early identification of nation-state alerts and critical action</b></td><td>Phoenix security ingests nation-state and critical alerts, enabling quick action on the most critical assets.



Infrastructure Assets
Asset Status: All
Search: Search by Asset name, CVE
Infrastructure Assets
169 Results
<table>
<tr><th>Address</th><th>Name</th><th>NetBIOS name</th><th>Operation system</th><th>Sources</th><th>Assigned</th><th>Risk breakdown</th></tr>
<tr><td>10.102.111.131</td><td>phx-test-sel-032.example-int.com</td><td>Phx-Test-SeL-032</td><td>Linux RedHat v7 R...</td><td></td><td></td><td></td></tr>
<tr><td>172.31.12.101</td><td>ip-172-31-12-101</td><td>-</td><td>Ubuntu Linux 20.04</td><td></td><td></td><td></td></tr>
<tr><td>18.169.172.72</td><td>18.169.172.72</td><td>-</td><td>Ubuntu Linux 20.04</td><td></td><td></td><td></td></tr>
<tr><td>10.102.111.175</td><td>phx-test-sew-036.example-int.com</td><td>Phx-Test-SeW-036</td><td>Windows Server 2...</td><td></td><td></td><td></td></tr>
<tr><td>10.102.111.158</td><td>phx-test-sew-019.example-int.com</td><td>Phx-Test-SeW-019</td><td>Windows Server 2...</td><td></td><td></td><td></td></tr>
<tr><td>10.102.111.94</td><td>phx-test-fiw-005.example-int.com</td><td>Phx-Test-FiW-005</td><td>Palo Alto PA-5410</td><td></td><td></td><td></td></tr>
</table>
</td></tr>
<tr><td><b>Reporting</b></td><td>Phoenix security enables reporting on the risk posture of each product, including the number of issues that have been fixed and the expected time to fix them.



Software Assets
Asset Status: All
Search: External App Test
SBOM
23 Total
<table>
<tr><th>Package name</th><th>Package version</th></tr>
<tr><td>tar</td><td>4.4.13</td></tr>
<tr><td>minimatch</td><td>3.0.4</td></tr>
<tr><td>mongoose</td><td>5.9.22</td></tr>
<tr><td>ini</td><td>1.3.5</td></tr>
<tr><td>datatables.net</td><td>1.10.23</td></tr>
<tr><td>minimist</td><td>1.2.5</td></tr>
<tr><td>mquery</td><td>3.2.2</td></tr>
<tr><td>path-parse</td><td>1.0.6</td></tr>
<tr><td>handlebars</td><td>4.7.6</td></tr>
</table>
</td></tr>
</table>