ARMIS® servicenow®

WHITE PAPER

Overcoming the Operational Technology Blindspot

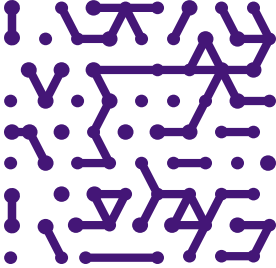
The pending cross industry regulation around NIS2 in Europe will introduce new requirements to guarantee the availability and uptime of critical services either a company or critical national infrastructure operator provides. NIS 2 was passed into law on January 16th, 2023, with a 21-month readiness window and goes live in October 2024.

NIS2 is essentially enshrining cyber security responsibility into European law for a much broader group of industry sectors which are cross market. The original industries defined in NIS were classified as 'essential' and included Healthcare, Drinking Water, Finance etc. (See table 1.1) With NIS2 we now see a new and broader category regarded as 'important' entities, which includes Postal and Courier Services, Food and Manufacturing and therefore a much broader set of industries. The law is designed to improve operational and cyber resilience of organizations and reduce the impact of cyber-attacks, especially for services for which the public and economy require to function. Currently cyber losses within the EU are estimated to be 11.3Bn Euro per annum.

Organizations subject to NIS2 will be obliged to:

"*take appropriate and proportionate technical, operational and organizational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimize the impact of incidents on recipients of their services and on other services*"

NIS2 Organizations that operate in these sectors are deemed "essential"	**NIS2 introduces a second category of "important" entities**
• Energy	• Postal & Courier Services
• Transport	• Waste Management
• Finance	• Chemicals
• Healthcare	• Food
• Drinking Water	• Manufacturing
• Wastewater	• Digital Providers
• Digital Infrastructure	• Research Organisations
• ICT Service Management	
• Public Administration	
• Space	



The difficult reality is many organizations still do not have visibility into their total asset base which underpins the critical services they will be measured against under NIS2. Another way of describing an enterprise's asset base is its cyber-attack surface, and to be able to protect assets you need to be able to see where they are and understand the health or risk posture of the assets across your entire attack surface. Most organizations have focused on building an inventory of asset classes, and this has usually started with I.T.

In many cases asset classes like Operational Technology which can be found across all industry sectors, in particular manufacturing and CNI (Critical National Infrastructure) are often not well inventoried, and the cyber risk posture of these assets can often be high as they include solutions which typically do not accept security agents or have traditionally out of scope for IT as they live in operational environments. This situation is further compounded by IoT devices which are exploding in scale across clients' environments, are often difficult to track, inherently insecure and therefore an easy target for bad actors to launch an exploit.

To compound the attack surface resilience challenges across IT, IoT and OT, the increased regulatory oversight of end-to-end services now includes third-party providers and any cyber or operational risk they may introduce, this is against a backdrop of sophisticated fraud, supply chain based cyber-attacks e.g. SolarWinds, and hostile nation state sponsored activity which has increased significantly since with the start of the war in the Ukraine.

NIS 2 also carries more onerous penalties for Enterprises and Critical National Infrastructure providers where service failure occurs, the new penalty matrix also includes critical third-party service providers should they be deemed responsible for the service or data loss, so with NIS2, outsourcing cyber services will not outsource the responsibility. Fines can reach 2% of global revenue or €10 million euros for ''Essential' entities, whereas "Important" entities in the new category face 1.4% of global revenue or up to €7 million euros. It is estimated that cyber security budgets may need to increase by 22% for the new "important' entity category to put the required controls and protection in place, whereas even the existing "important entities are looking at an increase of 12% to build in the required visibility and resilience they will require. Some international companies with headquarters outside of the European Union who have significant European operations will be subject to NIS2 compliance and penalties, hence this new regulation is becoming a global imperative.

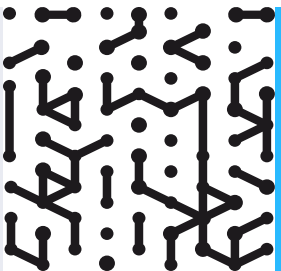
As an example, recent UK Finance research amongst members, indicated it is currently difficult for financial institutions to identify the actual IT assets which are critical in underpinning critical services. This is a good example of the challenges many organizations face in developing cyber resilience as financial institutions who typically have larger cyber security budgets than other industries and are very highly regulated. In nearly all cases 'critical services' are comprised of complex I.T. infrastructure that may span diverse logical, physical, and geographic domains across cloud, on-premises, virtual, mobile, IoT and even OT (Operational Technology) assets. We may not think of Operational Technology as being present in a bank or retail, but it is often in place for building management systems (BMS) or in retail for refrigeration or postal and courier services for materials handling. Taking a total attack surface view and considering exposure management is therefore critical.

Post COVID 19 has also compounded the challenge for many industries creating a pivot to home working and increasing additional asset complexities and additional risks to consider and mitigate. In addition, the explosion of 'unmanaged devices' across enterprise infrastructure e.g. IoT and smart devices, creates the management risk of an ever expanding cyber 'attack surface' with assets or devices which will not readily accept an endpoint security agent, so unmanaged asset visibility and management is becoming increasingly difficult for enterprises to manage which increases operational and cyber risk.

Many enterprises CMDB (Configuration Management Data Base) asset data sources are often fragmented and rely on 'point in time' scans from different sources to determine a view on IT, making it difficult to understand and track all the critical assets associated or linked with a critical service. The concept of IT, IoT and OT asset inventory being captured within the CMDB is a relatively new but gaining pace as it is an imperative to have a single system of record from which remediation and business workflows can be orchestrated, field service operations can be maintained and even third party dependencies can be tracked and monitored.

Consequently, many enterprises are now exploring asset discovery or mapping tools, in many cases these tools unfortunately do not detect all the potential assets across their environment, so often many enterprises resort to manual methods of collecting inventory data via excel spreadsheets. Some asset mapping tools also require active scanning which needs to be scheduled within a particular network segment and can be potentially disruptive to 'live' systems so are often unsuitable for sensitive Healthcare Devices or Operational Technology which could be found on a production line, or CNI. Consequently, it is difficult to achieve an 'aggregated view' of underlying asset inventory and any real-time vulnerabilities or attack scenarios that could have an impact on critical services.

In many organizations the internal risk and security, network and operational or manufacturing teams often don't have access to the same data and sometimes have disconnected goals. Auditable reporting and root cause analysis of service disruption or health can therefore be constrained by the need to query multiple data sources, involving different teams to provide a complete picture of the service composition and where the issues occurred requiring remediation. In simple terms a security team may detect an issue on the factory floor but not have the processes or know the people to get the issue fixed before it potentially impacts 'uptime' or worse. The more complex the organization and geographic distribution, the more complex this challenge can become. This new challenge is characterized as IT/OT convergence, or a complete view that is required across the 'attack surface' many organizations are now seeking solutions which enable this next level of visibility.



5 ways Armis and ServiceNow help to address the Challenges of IT/OT convergence and NIS2 Compliance.

1 Risk Analysis. See and secure all your assets.

Armis is the first step in enabling a defensible cyber maturity with regards to asset management specified in Article 21. The Armis Centrix™ platform provides a single source of truth, so you have **100% visibility into every asset** in your environment, including hardware, software, operating systems, applications, physical location, users, and more. That's IT, OT, IIOT, IoT, IoMT, virtual, and cloud—managed and unmanaged, and more. Armis powers an adaptive mature risk analysis function which can then drive CMDB enrichment with ServiceNow so downstream processes including remediation of risky assets and field service functions can be become automated and auditable thereby reducing the risk of downtime and service risk and outages.

2 Incident handling. Optimize your organization's incident response management plan.

The average enterprise has more than 50 cybersecurity-related tools. The Armis Centrix™ platform **cuts through the noise** by correlating data from across your IT, network, and security infrastructure, giving you the ability to manage and protect your entire estate. It can quickly alert security teams to anomalous device behaviour that can signal an attack. After incident response, security teams can access the platform's logs for review and forensics. ServiceNow can codify and drive the remediation workflows to reduce the overall cyber risk.

3 Classify assets and detect threats with a high degree of accuracy.

Core to the Armis Centrix™ Platform is our AI-powered **Asset Intelligence Engine**. It is a giant, crowd-sourced, cloud-based asset behavior knowledgebase—the largest in the world, tracking over 3.5 billion assets. With our Asset Intelligence Engine, Armis understands not only what the asset is and what it is doing, but what it should be doing. This is because we understand the context of each asset in its use in each environment. These asset insights enable Armis to classify assets and detect threats with a high degree of accuracy. Once detected and classified our 4 certified connectors into the ServiceNow platform enable Armis to pass all asset classes to ServiceNow in real-time along with posture status from a vulnerability and risk score perspective.

4 Focus on high-risk vulnerabilities that can cause costly disruptions.

The Armis Centrix™ for Vulnerability Prioritization and Remediation add-on module goes beyond vulnerability scanning to address the full cyber risk management lifecycle. It enables you to understand asset risk, secure vulnerable assets, and control your attack surface. These vulnerabilities can then be natively passed across in real-time to ServiceNow to drive and track the remediation activities the business requires to maintain operations.

5 Simplify security frameworks and regulatory compliance.

Frameworks like Centre and the NIST Cyber Security Framework (CSF) are the standard security blueprints for most organizations. The Armis platform provides compliance for CIS Controls as well as the NIST CSF controls across the Identify, Protect, Detect, and Respond categories for managed, unmanaged, IoT, ICS, medical devices and more. The European Commission, ENISA and the Member States should continue to foster alignments with international standards and existing industry best practices in the area of cybersecurity risk management, for example in the areas of supply chain security assessments, information sharing and vulnerability disclosure.