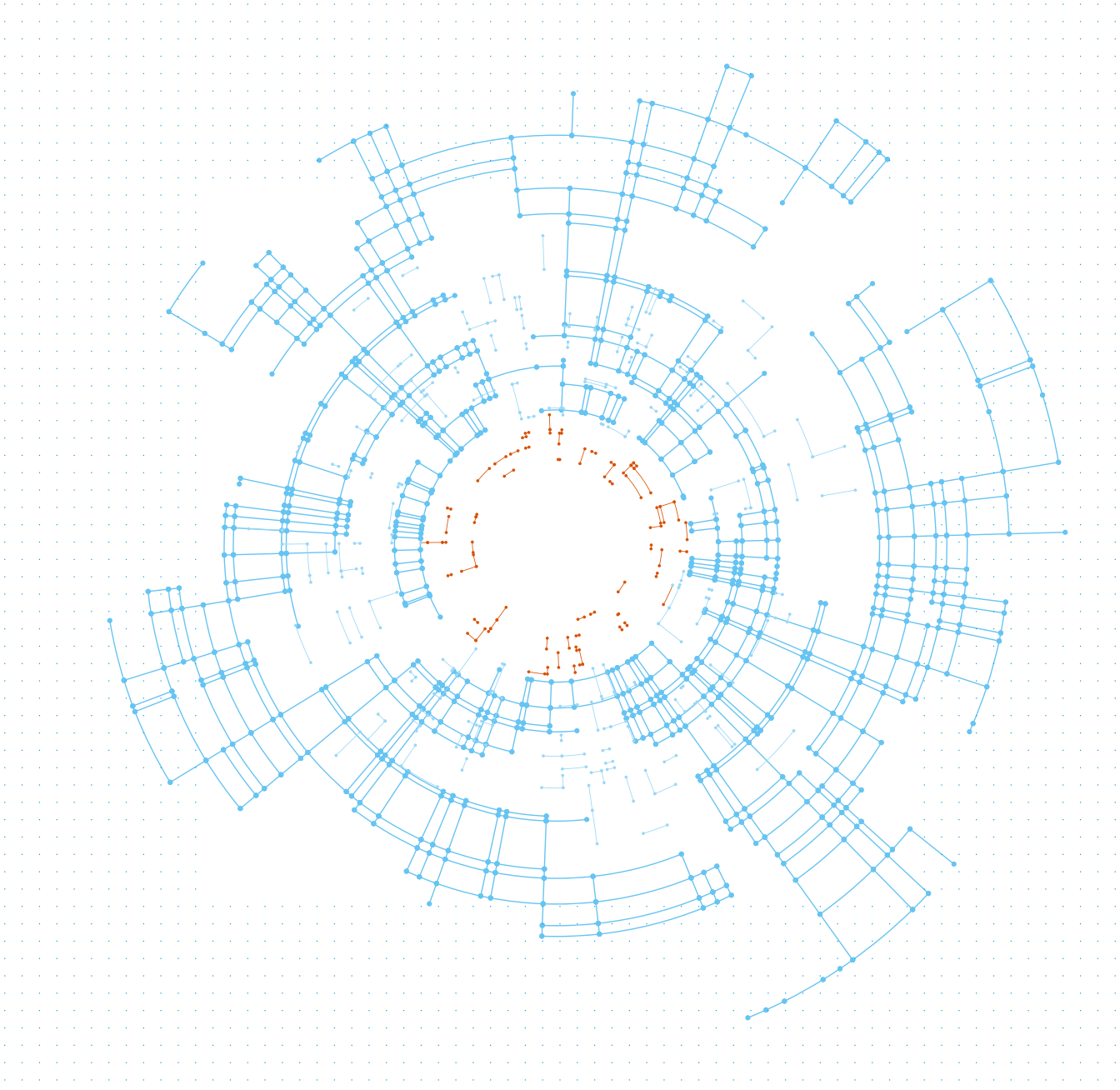
FORESCOUT

The NIS2 directive: enhancing cyber security across the EU

Forescout Mapping Guide

February 2024

Contents



Introduction

The NIS2 Directive is EU-wide legislation that aims to increase the level of cybersecurity within the European Union. One of the ways it does this is by addressing a broader range of industry sectors, mandating the implementation of cybersecurity measures and imposing strict incident reporting requirements. Currently, there is wide variation in the maturity of these issues among Member States, which this legislation seeks to align. Note that NIS2 not only requires public and private organizations to improve their cybersecurity measures, but also requires national governments to establish EU-wide programs for collaboration and vulnerability sharing.

NIS vs. NIS2: The extended scope of application

The NIS2 directive is intended for organizations that are classified by the EU as medium or large, those with more than 50 employees and/or that generate more than 10 million euros in revenue per year. However, the size limit does not apply to organizations in certain sectors, such as those considered critical infrastructure.

The new directive removes the distinction between operators of essential services (OES) and digital service providers (DSP) and classifies entities as essential or important based on the criticality of the service provided. The NIS2 framework requires specific categories to adopt technical and organizational measures to manage cyber security risk.

Annex I of the new directive lists the **essential** subjects: energy, transport, banks, financial market infrastructures, health, drinking water, wastewater, digital infrastructures, public administration, and space.

Annex II, by contrast, identifies the **important** subjects: postal and courier services, waste management, production and distribution of chemical products, production, processing and distribution of food, production of medical equipment, and digital suppliers (intended as online search engine providers, social network service platforms and online marketplaces).

In addition, the NIS2 Directive provides for greater coordination between organizations and Member States in disclosing new security vulnerabilities discovered across the EU. The new directive establishes a list of administrative sanctions, including penalties for cybersecurity risk management obligations. The NIS2 imposes direct obligations on management bodies to implement and monitor their organization's compliance with the directive, which can result in fines and temporary disqualification from performing managerial duties.

Among other things, the directive proposes to establish a European network of cyber crisis liaison organizations (EU-CyCLONe) to work together to prepare and implement rapid response plans for emergencies, such as large-scale cyber incidents or crises, and introduces more detailed provisions on the incident reporting process, content of reports and timing (within 24 hours of incident discovery).

How to comply with the NIS2 Directive

In response to implementation across Europe, the U.K. National Cyber Security Center (NCSC) developed the Cyber Assessment Framework (CAF) to provide a method for analyzing essential and key organizations (and their suppliers) to review and improve cybersecurity policies and procedures for the NIS2 regulation. The CAF consists of a set of 14 cybersecurity and resilience principles divided into four main objectives, plus guidance on the use and application of the principles and the CAF itself. The framework provides a systematic and comprehensive approach to assessing the extent to which risks to critical functions are being managed by the responsible organization. The CAF is intended for use by the organization itself (self-assessment) or by an independent external body, or a qualified organization acting on behalf of a regulator. The CAF defines four security objectives:

A. Managing security risk;
B. Protecting against cyber attack;
C. Detecting cyber security events; and
D. Minimizing the impact of cyber security incidents.

Objective A: Managing security risk

A1 Governance

The organization has appropriate management policies and processes in place to govern its approach to the security of network and information systems.

How Forescout can help

Forescout provides the foundational visibility necessary to accurately identify assets and effectively manage corporate and supply chain risk. Forescout's ability to see and control managed and unmanaged devices, including IT/OT/IoT and IoMT devices on a network, reduces the risk of potential attacks and remediates malicious code or high-risk devices. The Forescout Platform can continuously acquire, assess and act on new information to identify vulnerabilities, remediate noncompliant or compromised devices and minimize the window of opportunity for attackers.

Objective A: Managing security risk		
A1 Governance	*The organization has appropriate management policies and processes in place to govern its approach to the security of network and information systems.*	The Forescout platform provides comprehensive visibility into ICS devices and systems. This enables organizations to identify, understand and document cybersecurity risks and translate timely and accurate information into effective organizational practices.
A1.a Board Direction	*You have effective organizational security management that is led at the board level and articulated clearly in corresponding policies.*	
A1.b Roles and Responsibilities	*Your organization has established roles and responsibilities for the security of networks and information systems at all levels, with clear and well-understood channels for communicating and escalating risks.*	
A1.c Decision-making	*You have senior-level accountability for the security of networks and information systems, and delegate decision-making authority appropriately and effectively. Risks to network and information systems related to the operation of essential functions are considered in the context of other organizational risks.*	

A2 Risk management

The organization takes appropriate steps to identify, assess and understand security risks to the network and information systems supporting the operation of essential functions. This includes an overall organizational approach to risk management.

How Forescout can help

Forescout provides detailed device visibility for ICS environments, enabling effective management of operational and cyber risks in real time. The Forescout platform leverages multi-factor risk scoring to support organizational efforts in assessing and managing cyber assets with comprehensive risk profiles. Forescout's goal is to create a single point of control that leverages automation to help eliminate or mitigate the organization's greatest risks.

Objective A: Managing security risk Objective A: Managing security risk		
A2 Risk Management	*The organization takes appropriate steps to identify, assess and understand security risks to the network and information systems supporting the operation of essential functions. This includes an overall organizational approach to risk management.*	The Forescout platform uses multifactor threat detection and individual data points to assign a single security and operational risk score to each network asset. These risk scores provide a consistent method for identifying and prioritizing remediation actions and reducing overall risk exposure. The solution supports various risk and compliance frameworks, and the risk formula can be further customized to fit the organization's risk management model.
A2.a Risk Management Process	*Your organization has effective internal processes for managing risks to the security of network and information systems related to the operation of essential functions and communicating associated activities.*	
A2.b Assurance	*You have gained confidence in the effectiveness of the security of your technology, people and processes relevant to essential functions.*	

A3 Common asset management

Everything required to deliver, maintain or support networks and information systems necessary for the operation of essential functions is determined and understood. This includes data, people and systems as well as any supporting infrastructure (I.e., power, cooling, etc.).

How Forescout can help

Forescout helps asset owners make smart, up-to-date security and business decisions and meet compliance requirements by providing real-time asset inventory and asset management for every connected device in the ICS environment. The Forescout platform helps eliminate blind spots and removes the manual processes to collect instant asset intelligence and maintain accurate asset inventories and lifecycle management for each device as soon as it is connected to the network.

Objective A: Managing security risk		
A3 Common Asset Management	*Everything required to deliver, maintain or support networks and information systems necessary for the operation of essential functions is determined and understood. This includes data, people and systems as well as any supporting infrastructure (such as power or cooling).*	The Forescout platform enables organizations to gain a real-time asset inventory across all physical and virtual devices - IoT, IoMT, OT, BAS, mobile and network infrastructure - across campus, data center, cloud, and OT networks. Forescout identifies the control system role and service dependencies for each device on the network and provides asset inventory information such as model number, firmware version, serial number, etc. The solution helps security teams share contextual data with security operations, help desk personnel and third-party asset management tools.
A3.a Asset Management		

A4 Supply chain

The organization understands and manages security risks to networks and information systems supporting the operation of essential functions that arise because of dependencies on external suppliers. This includes ensuring that appropriate measures are employed where third-party services are used.

How Forescout can help

With Forescout's enhanced visibility, organizations can monitor various aspects of the supply chain, from interactions with third-party services (e.g., contractors) to the use of remote applications (e.g., the cloud). Whether the owning organization or a third party is running the function, the Forescout platform can monitor network and resource access, compliance with security requirements and policies, device configuration, vulnerabilities, and potential threats to ICS system security.

Objective A: Managing security risk		
A4 Supply Chain	*The organization understands and manages security risks to networks and information systems supporting the operation of essential functions that arise because of dependencies on external suppliers. This includes ensuring that appropriate measures are employed where third party services are used.*	Forescout combines patented deep packet inspection (DPI) and anomalous system behavior analysis designed specifically for OT/ICS environments with a library of thousands of ICS-specific threat checks and indicators of potential supply chain compromise.
A4.a Supply Chain		

Objective B: Protect against cyber attacks

B1 Service protection policies and processes

The organization defines, implements, communicates, and enforces appropriate policies and processes that direct its overall approach to securing systems and data that support operation of essential functions.

How Forescout can help

Forescout can help organizations to implement security policies and processes by continuously monitoring authorized and unauthorized access to the network, creating policies to automatically isolate rogue access points and notifying personnel of discoveries. By helping to ensure that real-time vulnerability scans are performed and that relevant third-party protection software is installed, correctly configured and operational, Forescout addresses the outcome of ensuring resilient networks and systems.

The Forescout platform identifies users attempting to access information which they are not authorized to access by their Active Directory group. The platform provides device- and role-based network authentication and authorization, allowing individuals and their devices to obtain their identified network access determined by VLANs or ACLs. The platform enables automated segmentation of network access by user, device classification and/or posture, regardless of how that device is connecting to the network—wired, wireless or VPN. Devices may be mobile, servers, virtual machines, OT, or other IoT devices. Network segregation strategies can be deployed centrally via the Forescout platform.

Objective B: Protect against cyber attacks		
B1 Service Protection Policies and Processes	*The organization defines, implements, communicates, and enforces appropriate policies and processes that direct its overall approach to securing systems and data that support operation of essential functions.*	Forescout simplifies policy enforcement, audits, assessments, and analytics with customizable compliance thresholds and compliance-audit-focused reporting. Regardless of device type or location, the Forescout platform can enforce network access control based on corporate policy to effectively manage risk and meet regulatory requirements.
B1.a Policy and Process Development	*You have successfully implemented your security policies and processes and can demonstrate the security benefits achieved.*	

B2 Identity and access control

The organization understands, documents and manages access to networks and information systems supporting the operation of essential functions. Users (or automated functions) that can access data or systems are appropriately verified, authenticated, and authorized.

How can Forescout help?

The Forescout platform identifies users attempting to access information for which they are not authorized by their Active Directory group. It provides device- and role-based network authentication and authorization so that individuals and their devices have network access determined by VLANs or ACLs.

Objective B: Protect against cyber attacks		
B2 Identity and Access Control	*The organization understands, documents and manages access to networks and information systems supporting the operation of essential functions. Users (or automated functions) that can access data or systems are appropriately verified, authenticated and authorized.*	The Forescout platform helps you set up trusted and untrusted zones to protect financial data through network segmentation and network access control. It can automate security segment assignment and create access enforcement using policy-based assignment and enforcement of ACLs and VLANs. The platform provides real-time visibility into devices as they connect to the network to automate and enforce policy-based network access control, endpoint compliance and mobile device security. The platform can integrate with a variety of third-party authentication systems (IdAM) to validate a unique identity and users before granting role-based network access.
B2.a Identity Verification, Authentication and Authorization	*You robustly verify, authenticate and authorize access to the networks and information systems supporting your essential functions.*	
B2.b Device Management	*You fully know, and have trust in, the devices that are used to access your networks, information systems and data that support your essential functions.*	
B2.c Privileged User Management	*You closely manage privileged user access to networks and information systems supporting the essential functions.*	
B2.d Identity and Access Management (IdAM)	*You closely manage and maintain identity and access control for users, devices and systems accessing the networks and information systems supporting the essential function.*	

B3 Data security

Data stored or transmitted electronically is protected from actions such as unauthorized access, modification or deletion that may cause an adverse impact on essential functions. Such protection extends to how authorized users, devices and systems access critical data necessary for the operation of essential functions. It also covers information that would assist an attacker, such as the design details of networks and information systems.

How Forescout can help

The Forescout platform is a key component in many organizations' data security strategies because it is such an effective tool for strengthening data privacy and security, reducing overall risk, and demonstrating compliance. The platform can help detect unauthorized access to sensitive information, including operational data, network traffic and configurations, and monitor access to data according to the risks to essential functions posed by compromising data integrity and/or availability.

Objective B: Protect against cyber attacks		
B3 Data Security	*Data stored or transmitted electronically is protected from actions such as unauthorized access, modification or deletion that may adversely impact essential functions. Such protection extends to how authorized users, devices and systems access critical data necessary for the operation of essential functions.*	In addition to effective data access control measures, Forescout can help protect the organization's data by detecting attacks to the confidentiality, integrity and availability of device, network and data. The Forescout platform reports any undesired network communication and activity, helping to ensure that network integrity and segregation is preserved.
B3.a Understanding Data	*You have a good understanding of data important to the operation of the essential function, where it is stored, where it travels, and how unavailability or unauthorized access, modification or deletion would adversely impact the essential function.*	
B3.b Data in Transit	*You have protected the transit of data important to the operation of the essential function. This includes the transfer of data to third parties.*	
B3.c Stored Data	*You have protected stored data important to the operation of the essential function.*	
B3.d Mobile Data	*You have protected data important to the operation of the essential function on mobile devices.*	
B3.e Media Equipment Sanitization	*You appropriately sanitize media and equipment holding data important to the operation of the essential function.*	

B4 System security

Network and information systems and technology critical for the operation of essential functions are protected from cyberattacks. An organizational understanding of risk to essential functions informs the use of robust and reliable protective security measures to effectively limit opportunities for attackers to compromise networks and systems.

How Forescout can help

Forescout can help minimize the likelihood of a successful attack by detecting and managing known vulnerabilities commonly exploited by attackers and monitoring device configuration, compliance, network data flow, system access, etc. The platform can detect both security and operational threats and prioritize them based on urgency and potential impact on the organization's essential functions.

Objective B: Protect against cyber attacks		
B4 System Security	*Network and information systems and technology critical for the operation of essential functions are protected from cyberattacks. An organizational understanding of risk to essential functions informs the use of robust and reliable protective security measures to effectively limit opportunities for attackers to compromise networks and systems.*	The Forescout platform performs continuous monitoring of devices for policy compliance and vulnerabilities as well as continuous analysis of network communications (format and content) to detect vulnerabilities, changes to the network or device configurations in real time, including new devices, infrastructure changes and irregular operational activity. Forescout can also enforce segmentation policies at the network level across heterogeneous infrastructures (e.g., switches, next-generation firewalls or software-defined networks) to segregate the most critical services and systems.
B4.a Secure by Design	*You design security into the network and information systems that support the operation of essential functions. You minimize their attack surface and ensure that the operation of the essential function should not be impacted by the exploitation of any single vulnerability.*	
B4.b Secure Configuration	*You securely configure the network and information systems that support the operation of essential functions.*	
B4.c Secure Management	*You manage your organization's network and information systems that support the operation of essential functions to enable and maintain security.*	
B4.d. Vulnerability Management	*You manage known vulnerabilities in your network and information systems to prevent adverse impact on the essential function.*	

B5 Resilient network and systems

The organization builds resilience against cyberattacks into the design, implementation, operation, and management of systems that support the operation of essential functions.

How Forescout can help

Forescout can help organizations reduce the likelihood of an outage or attack by monitoring the networks and systems that support essential functions. The platform ensures that critical resources are separated from other business and external systems and detects unexpected events. Forescout also makes it possible to deploy appropriate policies to protect supporting utilities such as power, fuel, heating, ventilation, and air conditioning.

Objective B: Protect against cyberattacks		
B5 Resilient Network and Systems	*The organization builds resilience against cyberattacks and system failure into the design, implementation, operation, and management of systems that support the operation of essential functions.*	The Forescout platform enforces flexible remediation, from modest to severe, so that even vulnerable OT/ICS systems can continue to operate securely. The platform provides a comprehensive asset map and history, allowing you to perform quick and detailed forensic analysis or examine past network topologies and analyze alerts to enable fast and informed recoveries from cybersecurity events. In addition, the system can ensure that replaced or recovered assets meet the configuration, policies and criteria that have been established.
B5.a Resilience Preparation	*You are prepared to restore the operation of your essential functions following adverse impact.*	
B5.b Design for Resilience	*You design the network and information systems supporting your essential functions to be resilient to cyber security incidents. Systems are appropriately segregated, and resource limitations are mitigated.*	
B5.c Backups	*You hold accessible and secured current backups of data and information needed to recover operation of your essential functions.*	

B6 Staff awareness and training governance

Staff have appropriate awareness, knowledge and skills to carry out their organizational roles effectively in relation to the security of network and information systems supporting the operation of essential functions.

How Forescout can help

Forescout can help organizations gain the knowledge and skills they need to use the Forescout platform to support the security of networks and industrial control systems.

Objective B: Protect against cyberattacks		
B6 Staff Awareness and Training Governance	*Staff have appropriate awareness, knowledge and skills to carry out their organizational roles effectively in relation to the security of network and information systems supporting the operation of essential functions.*	Forescout provides training and certification to help partners and customers get the most out of the Forescout platform and gain access to up-to-date knowledge and expertise for security best practices.
B6.a Cybersecurity Culture	*You develop and pursue a positive cybersecurity culture.*	
B6.b Cybersecurity Training	*The people who support the operation of your essential function are appropriately trained in cybersecurity. A range of approaches to cybersecurity training, awareness and communications are employed.*	

Objective C: Security monitoring

C1 Security monitoring

The organization monitors the security status of the networks and systems supporting the essential functions to detect potential security problems and track the ongoing effectiveness of protective security measures.

How Forescout can help

Forescout can help organizations identify events or activities that adversely impact the operational networks, assets and systems that support critical functions. The Forescout platform enables threat detection (of both known and unknown threats), log collection and aggregation and alerts analysis. It leverages Forescout's Vedere Labs threat intelligence to investigate complex operational and security events.

Objective C: Security monitoring		
C1 Security Monitoring	*The organization monitors the security status of the networks and systems supporting the operation of essential functions to detect potential security problems and track the ongoing effectiveness of protective security measures.*	The Forescout platform protects industrial networks from a wide range of threats. It combines patented anomaly detection and deep packet inspection (DPI) with an ever-growing library of thousands of ICS-specific behavior checks and IoCs to protect asset owners from advanced cyberattacks, network misconfigurations and operational failures. The platform integrates with existing enterprise tools to automate workflows, such as correlating and responding to incidents in a SIEM/SOC, synchronizing assets with a CMDB or creating tickets in the ITSM system. Forescout enables security teams to detect and prioritize events based on the unique environment of the organization, industry or specific ICS resources and systems. You can continuously improve the model using threat intelligence to assess the organization's coverage against real-world scenarios.
C1.a Monitoring Coverage	*The data sources that you include in your monitoring allow for timely identification of security events that may affect the operation of your essential functions.*	
C1.b Securing Logs	*You hold logging data securely and grant read access only to accounts with business need. No employee should ever need to modify or delete logging data within an agreed retention period, after which it should be deleted.*	
C1.c Generating Alerts	*Evidence of potential security incidents contained in your monitoring data is reliably identified and triggers alerts.*	
C1.d Identifying Security Incidents	*You contextualize alerts with knowledge of the threats and your systems to identify those security incidents that require some form of response.*	
C1.e Monitoring Tools and Skills	*The skills, tools and roles of monitoring staff, including anything that is sourced, should reflect governance and reporting requirements, expected threats and complexities of the network or system data which they need to use.*	

C2 Proactive security event discovery

The organization detects, within networks and information systems, malicious activity affecting or having the potential to affect, the operation of essential functions, even when the activity evades standard signature-based security prevent/detect solutions (or when standard solutions are not deployable).

How Forescout can help

Forescout can automatically establish network and system baselines for ICS environments and constantly monitors devices and communications to detect anomalous behavior and deviations from the baselines. The platform supports proactive detection of security events and monitors deviations from normal interaction with systems, unusual patterns of network traffic, and other indicators of compromise to detect adversaries' tactics and techniques.

Objective C: Security monitoring		
C2 Proactive Security Event Discovery	*The organization detects, within networks and information systems, malicious activity affecting, or with the potential to affect, the operation of essential functions, even when the activity evades standard signature-based security prevent/detect solutions (or when standard solutions are not deployable).*	The Forescout platform continuously monitors network traffic and alerts in real time for any threat to the network and its components. The platform features over 2.500 built-in, ICS-specific signatures and checks, combining them with powerful anomaly detection engines to help ensure that both known and unknown threats are identified at the earliest stage possible. Such threats include the use of insecure protocols and configurations, network reconnaissance activity, possible data breach, known and unknown malware and exploits, plus error and malfunction indicators of ICS devices and other undesired process operations that can put operational continuity at risk.
C2.a System Abnormalities for Attack Detection	*You define examples of abnormalities in system behavior that provide practical ways of detecting malicious activity that is otherwise hard to identify.*	
C2.b Proactive Attack Discovery	*You use an informed understanding of more sophisticated attack methods and normal system behavior to proactively monitor for malicious activity.*	

Objective D: Response and recovery planning

D1 Response and recovery planning

There are well-defined and tested incident management processes in place that aim to ensure continuity of essential functions in the event of system or service failure. Mitigation activities designed to contain or limit the impact of compromise are also in place.

How Forescout can help

Forescout can enhance an organization's incident response strategy by improving threat detection, analysis, containment, and recovery. The Forescout platform enables a holistic, ICS-specific cybersecurity strategy, from detection to response, by leveraging state-of-the-art detection technologies, linking them to community knowledge in the form of TTPs and integrating them with existing security tools to reduce mean time to respond (MTTR).

Objective D: Response and recovery planning		
D1 Response and Recovery Planning	*There are well-defined and tested incident management processes in place that aim to ensure continuity of essential functions in the event of system or service failure. Mitigation activities designed to contain or limit the impact of compromise are also in place.*	The Forescout platform can enhance an organization's incident response strategy by improving threat detection and response and containing or limiting the impact of an attack. Integration with third-party security tools enables automation of basic tasks. The platform's alerts provide rich contextual information about the source, type and target of threats, as well as key inputs for analysis (including captured packets related to the threat). You can visually locate each threat and its propagation on the interactive network map. The system network and device baselines can be used in recovery situations to ensure that devices and applications are functioning as expected. Forescout also provides threat hunting, risk identification and incident response services for organizations that do not have the internal resources and visibility to protect against or respond to cyberattacks, including ransomware and advanced persistent threats.
D1.a Response Plan	*You have an up-to-date incident response plan that is grounded in a thorough risk assessment that takes account of your essential functions and covers a range of incident scenarios.*	
D1.b Response and Recovery Capability	*You have the capability to enact your incident response plan, including effective limitation of impact on the operation of your essential functions. During an incident, you have access to timely information on which to base your response decisions.*	
D1.c Testing and Exercising	*Your organization carries out exercises to test response plans, using past incidents that affected your (and other) organization and scenarios that draw on threat intelligence and your risk assessment.*	

D2 Lesson learned

When an incident occurs, steps must be taken to understand its root causes and ensure appropriate remediating action is taken.

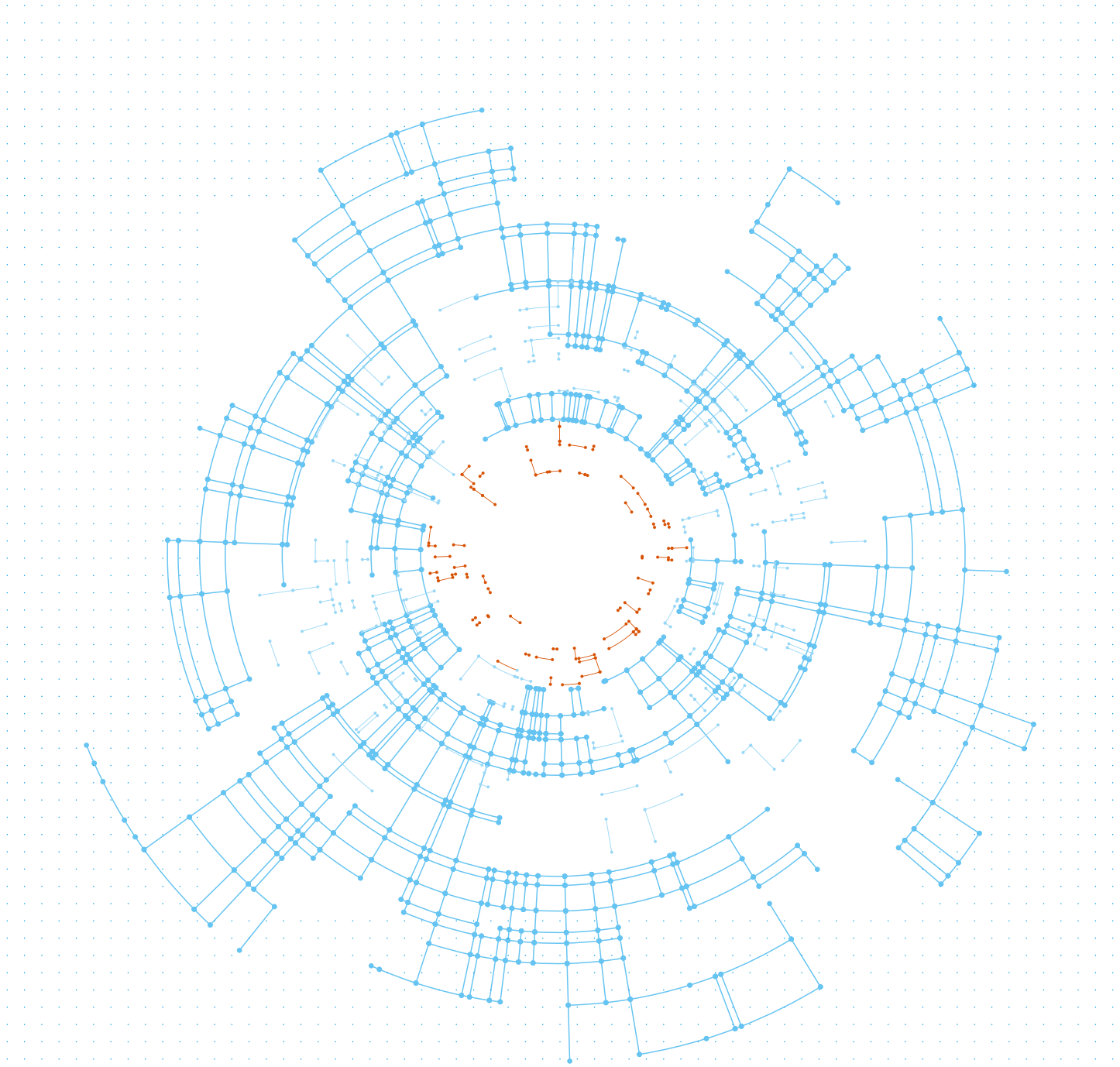
How Forescout can help?

Forescout can help organizations improve the resilience of critical functions by providing all the information needed to analyze incidents and take all necessary steps to prevent the problem from recurring. The platform enables security teams to improve the quality and timeliness of detection and to take remediation actions to reduce the likelihood of such incidents reoccurring.

Objective D: Response and recovery planning		
D2 Lesson Learned	*When an incident occurs, steps are taken to understand its root causes and to ensure appropriate remediating action is taken to protect against future incidents.*	The Forescout platform supports incident follow-up to verify the effectiveness and efficiency of incident-handling workflows. The platform can capture packets and other critical information in response to alerts before and after the time of the alert, automatically documenting the cybersecurity event for detailed forensic analysis and continuous operational improvement. This includes initial root cause, response execution issues, lack of policies and procedures, and inadequate infrastructure segmentation. Visual network analytics enable incident responders to perform forensic analysis of both real-time and historical network activity.
D2.a Incident Root Cause Analysis	*When an incident occurs, steps must be taken to understand its root causes and ensure appropriate remediating action is taken.*	
D2.b Using Incidents to Drive Improvements	*Your organization uses lessons learned from incidents to improve your security measures.*	

Conclusion

Compliance with the NIS2 Directive as it applies in each Member State is an urgent requirement for any organization operating an ICS network in Europe. Failure to comply with the directive's requirements represents a serious business risk that can cost millions. Existing best practices are a good starting point for meeting the requirements of NIS2. However, optimized, non-intrusive network monitoring and a situational awareness platform for industrial networks provide a best-practice approach to meeting the key security principles of the NIS2 Directive.



FORESCOUT®

Forescout Technologies, Inc.
Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591
Learn more at Forescout.com