Analyst Program

Implementation Guide

Enabling NIS2 Directive Compliance with Fortinet for Operational Technology

Written by **Jason D. Christopher**

Originally Published September 2020
Updated March 2023

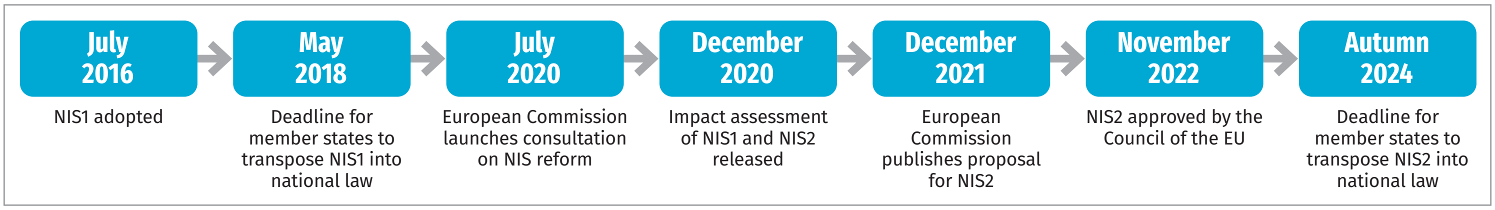
Introduction

As water and air are for our bodies, critical infrastructure sectors are the vital lifelines for our modern world. These essential services power communities, transport food, and provide medical services, among other essential functions. Each sector maintains reliable operation despite depending on network and information systems, including operational technology (OT), that face a myriad of cyber threats daily—threats with the potential to disrupt services, with a snowball effect on other businesses. This impactful nature of essential services is why the European Parliament adopted the original NIS Directive (hereafter, NIS1) in July 2016 to address the network security of critical infrastructure.[1]

Security, however, is an ever-changing field. Threats are continually on the rise, and the risks associated with cyberattacks on critical infrastructure are always increasing. Beyond these external threats, the promise of new efficiencies has inspired a wave of digital transformation, which has increased the connectivity between OT and business networks. The result is an expanded attack surface that now includes traditionally isolated industrial control systems (ICSes). These trends, combined with an analysis of the effectiveness of NIS1, led to an update of this major regulation. The NIS2 Directive (NIS2) is an improved approach to cybersecurity controls, with an expanded scope and mandatory penalties.[2]

NIS1 vs. NIS2: Why the Change?

When NIS1 was adopted in 2016, the technology and cyber threat landscape was very different than it is today. Since that time, cyber threat groups have evolved to use more tools targeting ICS/OT and to deliberately attempt to cause safety issues.[3] Meanwhile, the sharp increase in ransomware, including ICS-based ransomware families, has shifted the focus toward potential reliability and system outages for ICS/OT.[4] As cybersecurity threats evolve, so must our defenses. NIS2 considers the need for increased threat-information sharing while also focusing on cyber-risk management to proactively address the ever-evolving cyber threat landscape (see the NIS1/NIS2 timeline in Figure 1).



July 2016 — NIS1 adopted

May 2018 — Deadline for member states to transpose NIS1 into national law

July 2020 — European Commission launches consultation on NIS reform

December 2020 — Impact assessment of NIS1 and NIS2 released

December 2021 — European Commission publishes proposal for NIS2

November 2022 — NIS2 approved by the Council of the EU

Autumn 2024 — Deadline for member states to transpose NIS2 into national law

Figure 1. Timeline of NIS1 and NIS2

[1] "Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016," https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

[2] Legislation, Official Journal of the European Union, December 27, 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2022:333:FULL&from=FR

[3] "TRISIS: Analyzing Safety System Targeting Malware," December 14, 2017, www.dragos.com/resource/trisis-analyzing-safety-system-targeting-malware/

[4] "EKANS Ransomware: A Malware Targeting OT ICS System," July 1, 2020, www.fortinet.com/blog/threat-research/ekans-ransomware-targeting-ot-ics-systems

External threats were not the only considerations behind the NIS update. Modernization across digital systems has led to increased data and connectivity across traditional IT business networks and OT environments. Often referred to as the industrial internet of things (IIoT) or Industry 4.0, this digital transformation promises to provide several benefits for critical infrastructure owners and operators, as highlighted in Figure 2.

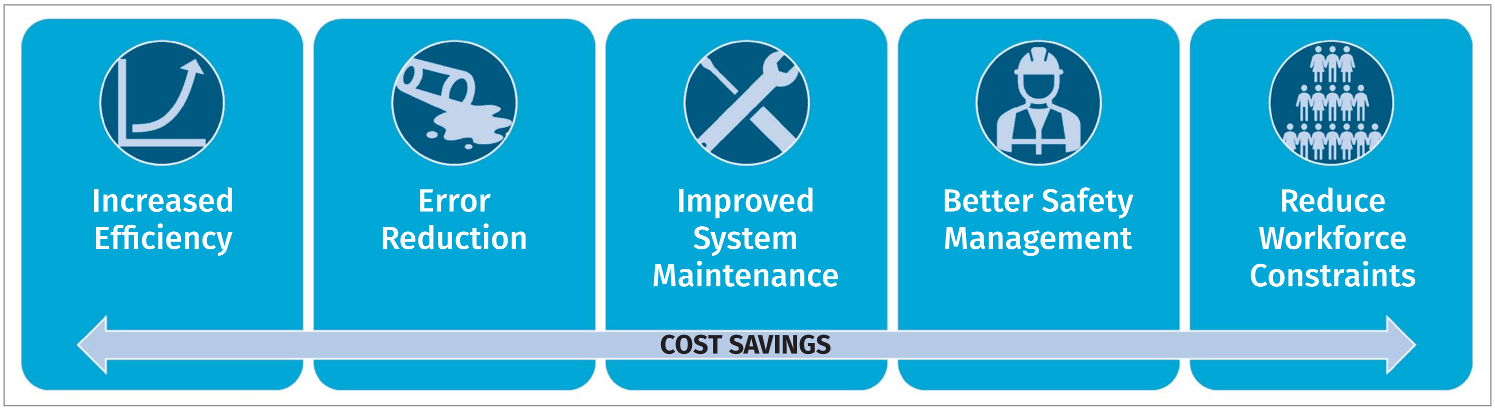


Figure 2. Digital Transformation and IIoT Benefits

This increased business need for connectivity was compounded during the quarantines and lockdowns of the COVID-19 pandemic, which spurred a large increase in remote access to manage ICS/OT. Adopting remote-access policies for these critical environments had been a multi-month or even multi-year process. But the unique business needs resulting from COVID-19 required organizations to fast-track their remote-access requirements, which led to an unprecedented explosion of new technologies being introduced in ICS/OT environments, with a proliferation of digital assets and remote connectivity. Meanwhile, as seen in Figure 3, OT-specific detection in those same environments has lagged.

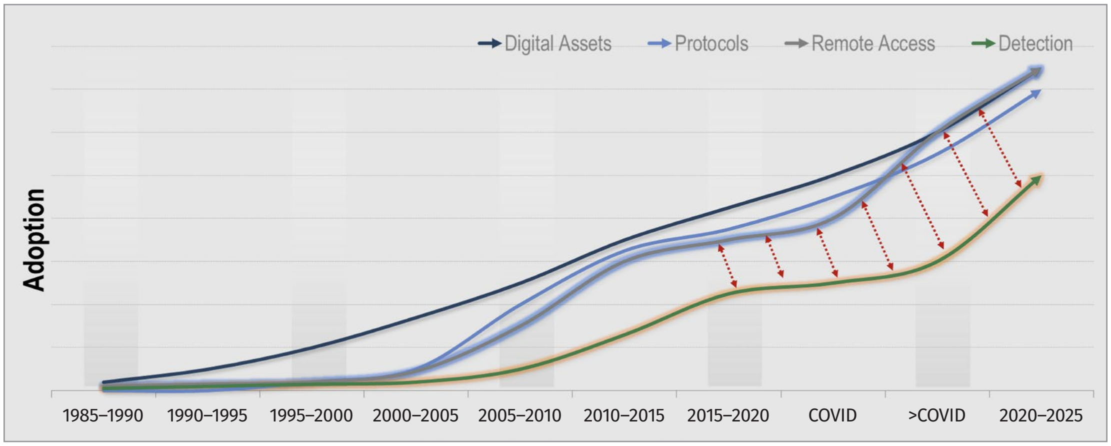


Figure 3. ICS/OT Remote Connectivity Increases Since 1985

NIS2 addresses these challenges and attempts to future-proof cybersecurity programs for organizations that must comply with the updated directive. Focusing on incident response and risk management, the security controls in NIS2 provide a foundation for creating and sustaining a comprehensive cybersecurity program. Furthermore, the expanded scope ensures that more organizations benefit from information-sharing and collaboration efforts, which ultimately strengthens the entire community.

What Is the NIS Directive?

The NIS Directive, recently updated to NIS2, establishes legal measures to increase cybersecurity capabilities within the EU and across its multiple member states and various operators by establishing a common framework to discuss both cyber-risk and cybersecurity incident response. Unlike other cybersecurity compliance programs for critical infrastructure such as North America's NERC CIP, NIS2 does not prescribe the "what to achieve" or mandatory requirements for each category; instead, each entity must examine its own cyber risks and identify steps to improve its security posture. This approach provides flexibility in designing a cybersecurity program for ICS and OT.

Compliance with any standard or framework requires a combination of a trained workforce, consistent processes, and robust technologies.[5] Compliance may be challenging in any environment, but it is even more so when OT is involved. OT, inclusive of ICSes such as SCADA systems and distributed control systems (DCSes), are defined by specialized equipment that performs real-world operations physically—opening valves, moving conveyer belts, spinning electric turbines, and so on. These systems require tailored security approaches, considering their specific communication protocols and system constraints. Traditional IT compliance approaches alone will not work as-is in production OT environments.

Many cybersecurity standards share similar areas of focus, including asset management, access control, system hardening, and incident response. NIS2 leverages many of these topics to address cyber risk for critical infrastructure.

That said, security compliance programs such as those highlighted in NIS2 are a great starting point for improving cybersecurity at certain facilities or across larger service territories. This paper will explore an approach to designing and operating ICSes to address NIS2 by:

- Utilizing the SANS ICS 410 Reference Architecture[6] as an approach to securely design and architect an environment that is in-scope for NIS2
- Examining several products within the Fortinet Security Fabric platform to implement security capabilities supporting NIS2

Security standards are useful tools for any organization. Not only do standards establish a common lexicon for discussing cyber risk, but they also provide a vetted methodology for approaching cybersecurity. When linked to appropriate incentives such as regulatory compliance, the NIS2 guidance can help with budget justifications and benchmarking security efforts. In fact, the European Commission's impact assessment of NIS2 estimates that organizations will increase their spending in cybersecurity by 22% over the next few years as a result of NIS2 compliance.[7] By leveraging an approach such as the one in this paper, asset owners and operators should be able to better align their security program with business objectives tied to NIS2 and other EU cyber-risk topics.

Additional Standards

Because NIS2 outlines objectives and practices rather than prescriptive requirements, organizations may leverage other cybersecurity standards, frameworks, and best practices that map to specific guidance in NIS2 or EU member-state regulations. By using OT-specific standards or frameworks for ICSes, organizations can ensure that their approach is tailored to their specific environment. Some useful cybersecurity standards, frameworks, and best practices include:

- **ISA/IEC 62443**
- **NIST SP 800-82**
- **NISTIR 7628**
- **NERC CIP**
- **IEC 62351**
- **API 1164**

[5] Within the context of NIS2, each EU member state will have their own laws regarding overall compliance mandates. This paper examines compliance as a tool within security programs, such as internal audit capabilities, regardless of specific member-state obligations. Each organization should ensure legal obligations with the NIS2 based on its geographic footprint and operations. The purpose of this paper is to further examine technical capabilities that internal audit teams may be able to verify and leverage.

[6] To learn more about the SANS ICS 410 Reference Architecture, download the poster at www.sans.org/posters/control-systems-are-a-target or view the video at www.youtube.com/watch?v=Ai2bxzJMuVI

[7] "Impact assessment Proposal for directive on measures for high common level of cybersecurity across the Union," December 16, 2020, https://digital-strategy.ec.europa.eu/en/library/impact-assessment-proposal-directive-measures-high-common-level-cybersecurity-across-union

From NIS1 to NIS2: Changes in Terminology and Scoping

One of the main goals of NIS2 is to provide new terms and expand concepts from NIS1 to reduce inconsistencies across EU member states and limit the interpretations around the scope of the regulations. NIS2 is mandatory regardless of any other regulatory framework already in place for organizations, including the EU's General Data Protection Regulation (GDPR), but it may be complementary in areas of incident response and reporting.

Scoping to Expand the Impact of NIS

NIS1 was scoped based on several critical infrastructure sectors, as found in Table 1 on page 6. While NIS2 maintains that original scope, it also expands the requirements to several supporting sectors, also highlighted in Figure 4.

It is important to note, however, that not all organizations in these sectors are treated equally under NIS2. Updated within NIS2 is the idea of size-capping organizations for regulatory purposes. While the previous regulatory language covered "operators of essential services (entity)," that term has since been expanded, and organizations are now either essential entities (EEs) or important entities (IEs), where criticality is designated by sector. EEs will be proactively audited for compliance, whereas IEs will be subject to reactive regulatory efforts triggered by indications of a cyber incident. All medium-sized entities (those with fewer than 250 employees and annual revenue not exceeding €50 million and/or an annual balance sheet under €43 million) and large entities will need to comply, while small entities (defined as those with fewer than 50 employees and annual revenue of less than €10 million) are generally exempt from NIS2. This allows organizations with the most critical impacts on society to invest appropriately while also not overburdening smaller organizations that, if disrupted, may not have a large consequence for any region or sector.

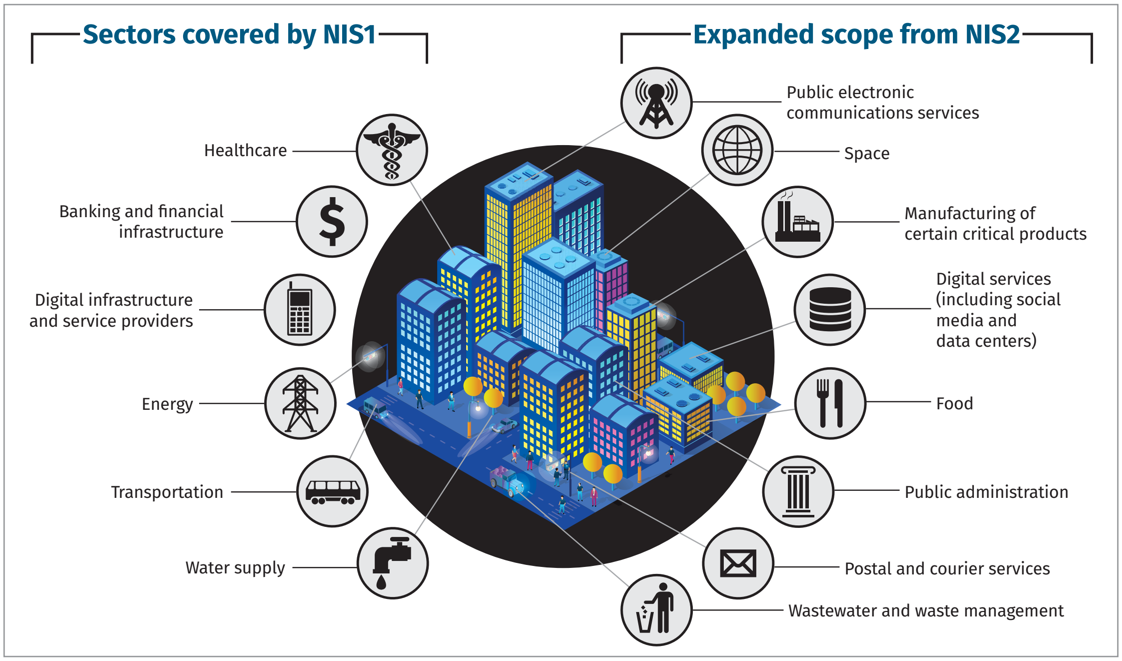

Sectors covered by NIS1
Healthcare
Banking and financial infrastructure
Digital infrastructure and service providers
Energy
Transportation
Water supply
Expanded scope from NIS2
Public electronic communications services
Space
Manufacturing of certain critical products
Digital services (including social media and data centers)
Food
Public administration
Postal and courier services
Wastewater and waste management

Figure 4. NIS2 In-Scope Sectors

Updated Objectives for NIS2

It is not just the scope of NIS2 that makes it different from its predecessor. The new directive expands on the foundation of the previous regulation by focusing on governance and creating a holistic cybersecurity program based on risks specific to each entity. This expansion requires a level of maturity around risk management and a comprehensive understanding of security controls.

Security Measures "Appropriate to the Risk Presented"

NIS2 is an accumulation of several sections and articles discussing compliance and the overall approach of the framework. Section 1 Article 18 of NIS2 dictates that EEs and IEs "shall take appropriate and proportionate technical and organizational measures to manage the risks posed to the security of network and information systems" that are used for the delivery of their services. These measures, of course, must include ICS/OT environments, because they are the production centers of critical infrastructure.

NIS2 further elaborates that the security measures must be implemented based on a level "appropriate to the risk presented." This statement implies that EEs and IEs have a thorough understanding of their cyber risks, including the potential impacts of a cyber event, the corresponding vulnerabilities, and the associated threats. Once the risks and impacts have been established, an entity must apply security controls to address the specific issues. This action is key to rolling out the required technologies and processes for an NIS2-based security program.

Section 1 Article 18 further mandates a minimum set of security controls that must be considered for compliance purposes. Table 1 provides details.

Table 1. NIS2 Directive Minimum Security Measures

NIS2 Directive, Section 1, Article 18	Description
a	Risk analysis and information system security policies
b	Incident handling (prevention, detection, and response to incidents)
c	Business continuity and crisis management
d	Supply chain security, including security-related aspects concerning the relationships between each entity and its suppliers or service providers such as providers of data storage and processing services or managed security services
e	Security in network and information systems acquisition, development, and maintenance, including vulnerability handling and disclosure
f	Policies and procedures (testing and auditing) to assess the effectiveness of cybersecurity risk management measures
g	The use of cryptography and encryption

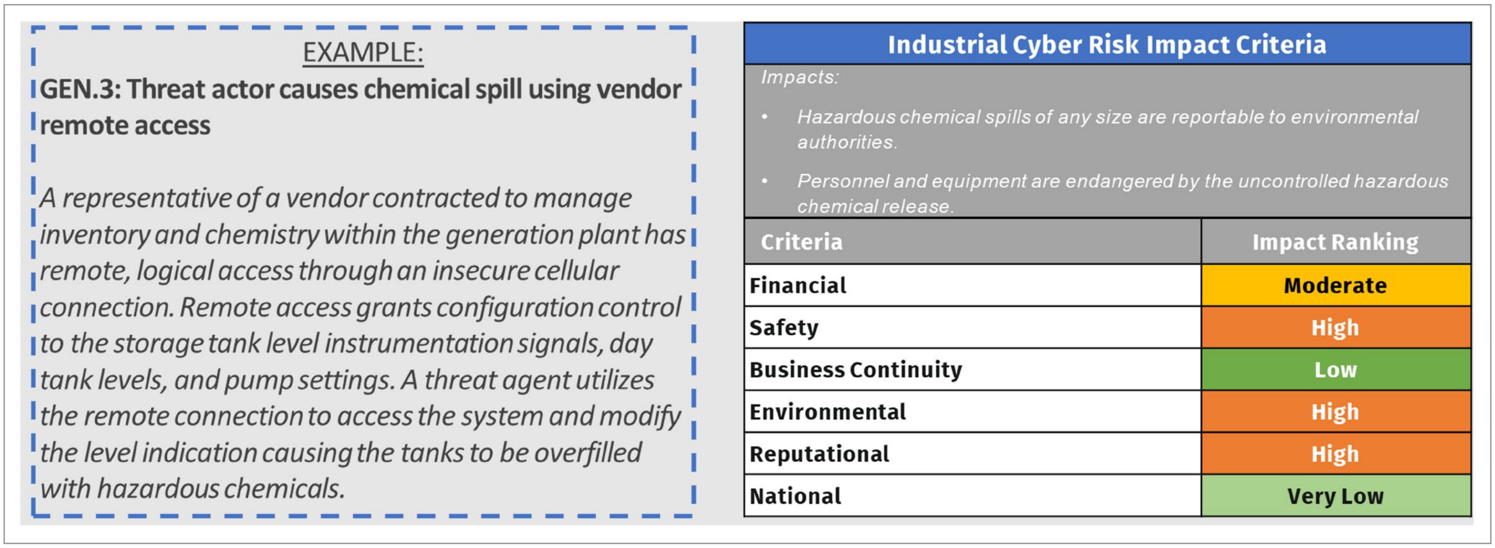
It should be noted, however, that many of these security measures require special considerations for ICS/OT because they are designed specifically for engineering processes. A few of these considerations are outlined next.

Risk Analysis and Security Policies [§I A18 2.a]

A risk analysis for ICS/OT environments moves far beyond discussion of enterprise systems that are traditional attack vectors (via methods such as phishing emails). While those incidents are important to consider, entities need to ultimately answer the question "What does a bad day look like for industrial facilities and services?" Ideally, these impacts are already quantified in engineering-based business impact criteria, which should include the following items:

- **Financial impacts—**Costs associated with recovery and property damage
- **Safety impacts—**Possibility of loss of life, limb, and eyesight at industrial sites
- **Business continuity impacts—**Measurement in hours, days, months, or years related to business interruption and associated expenses
- **Environmental impacts—**Associated areas where spills, leaks, fires, floods, or other environmental consequences may take place, with corresponding recovery timetables
- **Reputational impacts—**Gauge of public confidence, regulatory actions, and press coverage due to the cyber event
- **National-level impacts—**Collateral consequences for communities and other businesses due to the lack of services being provided

An example of an OT-centric risk analysis scenario is presented in Figure 5.



EXAMPLE:

GEN.3: Threat actor causes chemical spill using vendor remote access

A representative of a vendor contracted to manage inventory and chemistry within the generation plant has remote, logical access through an insecure cellular connection. Remote access grants configuration control to the storage tank level instrumentation signals, day tank levels, and pump settings. A threat agent utilizes the remote connection to access the system and modify the level indication causing the tanks to be overfilled with hazardous chemicals.

Industrial Cyber Risk Impact Criteria

Impacts:

- *Hazardous chemical spills of any size are reportable to environmental authorities.*
- *Personnel and equipment are endangered by the uncontrolled hazardous chemical release.*

Criteria	Impact Ranking
Financial	Moderate
Safety	High
Business Continuity	Low
Environmental	High
Reputational	High
National	Very Low

Figure 5. Example of an Industrial Cyber-Risk Analysis Scenario[8]

[8] A further breakdown of how to use threat-informed scenarios for industrial risk management was covered at the SANS ICS Summit in 2022: www.youtube.com/watch?v=5TrAICfTalk

A mature NIS2 program would then be able to rank these impacts, identify the required controls, (including a cost-benefit analysis), and list them in an appropriate risk register, similar to the one in Table 2.

Table 2. Example of an NIS2 Cyber-Risk Register[9]

ID	PRIORITY	RISK DESCRIPTION	RISK CATEGORY	FINANCIAL IMPACT	SAFETY IMPACT	BUSINESS CONTINUITY	ENVIRONMENTAL IMPACT	REPUTATIONAL IMPACT	NATIONAL IMPACT	RISK RESPONSE	COST/ BENEFIT ANALYSIS	RISK OWNER	STATUS
				INDUSTRIAL CYBER RISK EVALUATION									
1	Very High	An advanced threat activity group targets our safety systems, leading to complete plant shutdown and associated property damage.	**Cyber Incident:** Loss of Safety	$70.5M	M	M	L	M	L	Install additional OT monitoring at the plant. Increase operator training for incident response and recovery.	**$350k** for monitoring & training.	Plant Management	Open
2	Moderate	ICS vendor is compromised, resulting in malware sent to all field devices in the form of a "legitimate" software update.	**Cyber Incident:** Supply Chain Compromise	$1.2M	M	M	L	M	M	Include procurement language for supply chain risk. Add technical evaluation to all patch management cycles.	**$50k** for insurance & an additional $150k for new patch management and supply chain recommendations	OT Security Team	Open
3	Low	Operator uses infected USB to transfer project files across plant operations. Untargeted malware causes network latency issues.	**Cyber Incident:** Engineering Workstation Compromise	$750k	L	L	L	L	L	Limit ports and services across Level 3 and Level 2 assets, including physical ports. Include additional security awareness for plant personnel.	**$25k** in hourly work to create OT-based strategy for plant operations and USB protections.	Plant Management	Open

Incident Handling [§I A18 2.b] and Reporting Requirements [§I A20]

If cyber-risk analysis answers the question "What would we do during a bad day?" then incident handling addresses the actual reactive processes that entities must use to detect and respond to those bad days. It is critical, however, that entities understand that a traditional IT-centric approach to industrial incidents will not work. As the U.S. Department of Homeland Security explains, "[I]ncident response deployed in IT business systems may result in ineffective and even disastrous results when applied to ICS cyber incidents."

[9] More information about performing industrial cyber-risk analysis is available here: www.dragos.com/resource/industrial-cyber-risk-management

Instead, EEs and IEs need to consider the engineering, operations, and physics involved in their specific environments. The SANS ICS curriculum teaches students how to leverage the PICERL approach, highlighted in Figure 6.

It is critical that each stage considers how IT, security, operations, and engineering will all collaborate. For example, would an IT security technician know how to pull forensics data from a human-machine interface (HMI) in an ICS? Would an operator know how to identify a cyber event that affects service reliability? All these efforts need to be taught prior to a security incident occurring in the ICS/OT environment.[10]

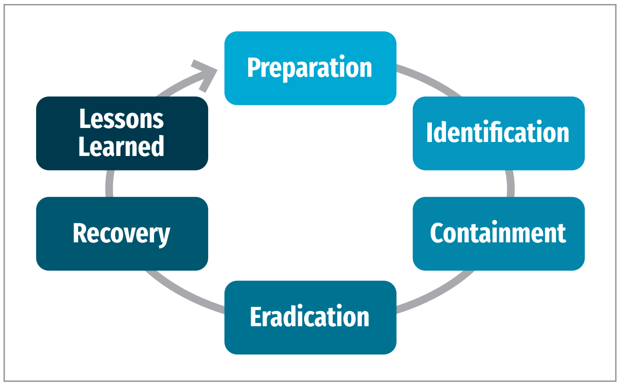


Figure 6. PICERL Approach for Incident Handling

The incident response program also needs to consider the reporting requirements within NIS2 Section 1 Article 20, which establishes a 24-hour window for an initial report, potential intermediate reports, and a final report after one month.

Business Continuity and Crisis Management [§I A18 2.c]

Disaster recovery, business continuity, and crisis management are all tasks that are routine for operations and engineering teams within industrial organizations. At any given facility, robust plans may already be in place for natural disasters, such as severe weather events. Those continuity plans should be mapped to recovery point objectives (RPOs) and recovery time objectives (RTOs) that can then be leveraged for cyber events. Because most of those plans may not consider what to do in case of a cyber incident, the following capabilities should be added to any business continuity program for OT:

- Data backups for industrial equipment, including logic for controllers, with an appropriate level of backup data for HMIs, engineering workstations, and historians
- Spare equipment for critical assets
- Knowledge of minimum operations required to run a facility, service, or business unit
- Testing of continuity plans, including any failover to backup facilities or cold sites

[10] More information about incident handling using the SANS model can be found in the SANS Incident Handler's Handbook (www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901), and specific techniques used in ICS incident response are taught in SANS ICS 515 (www.sans.org/ics515).

Supply Chain Security [§I A18 2.d]

The expanded discussion within NIS2 includes how EEs and IEs secure their suppliers and service providers, inclusive of data storage, processing services, and managed security services. Supply chain and procurement risks should likely be tracked in the same risk register as shown in Table 2 on page 8, but the treatment of the associated risks would need to include contract language and potential assurances of third-party services regarding their security posture. Important capabilities for supply chain risk management for OT should include the items on the checklist in Figure 7.

- □ Identify important suppliers, including sole-sourced contracts, original equipment manufacturers (OEMs), OT-specific vendors and integrators, and vendors linked with risk scenarios identified in the risk register.
- □ Identify suppliers and service providers with access to, control of, or custody of OT equipment.
- □ Identify risk scenarios specific to third parties.
- □ Have a defined method for evaluating and selecting a supplier, service provider, or third party. This should include consideration of cybersecurity qualifications. Where appropriate, selection criteria may include:
  - □ End-of-life and end-of-support timelines
  - □ Safeguards against counterfeit software, hardware, and services
  - □ Supply chain assurance for both hardware and software
- □ Formalize cybersecurity requirements (such as vulnerability notifications and incident-related SLA requirements) in agreements with suppliers, service providers, and other third parties.
- □ Perform acceptance testing (factory, site, and unstructured), including cybersecurity requirements.

Figure 7. Checklist for Supply Chain Risk Management

System Security Across Acquisition, Development, and Maintenance [§I A18 2.e]

Cybersecurity is never a "set it and forget it" activity. Instead, it must stretch across the entire life cycle of an entity's assets. Unlike traditional IT or enterprise assets, the life cycle of an industrial environment asset is measured in decades, not years. It is extremely common to work with assets that must run for 20, 30, or even more years. NIS2 requires EEs and IEs to consider each step of the life cycle within the security program. An example of an OT-specific life cycle for an ICS can be found in Figure 8.

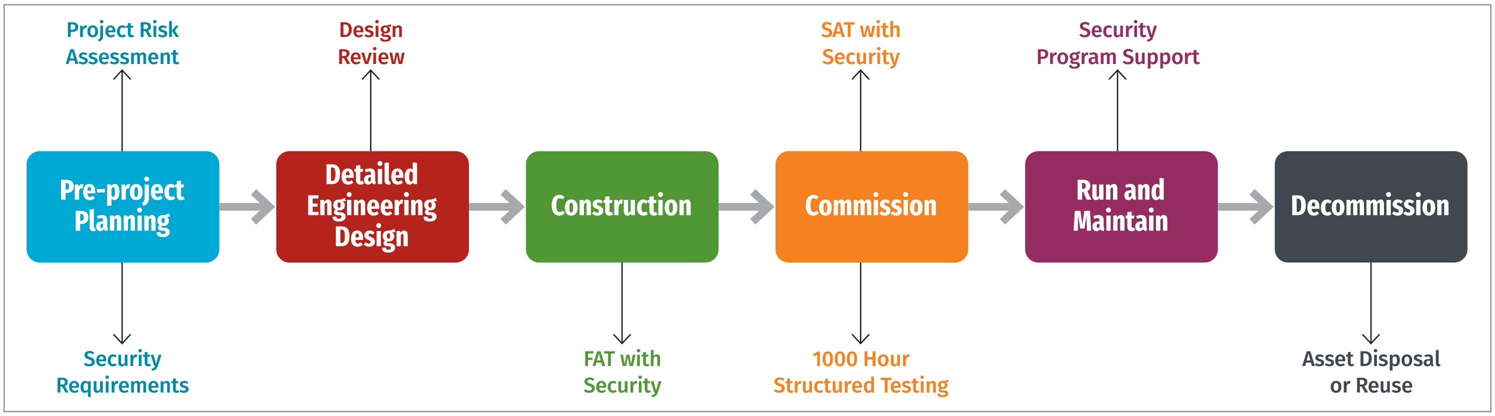


Figure 8. ICS-specific Asset Life Cycle

Each stage of Figure 8 needs to be addressed, from pre-project planning through decommissioning, and each will have its own challenges. The key for establishing a successful NIS2 program resides in exploring cyber risks (from §I A18 2.a) for each phase of the life cycle and ensuring that appropriate considerations are in place for any change in risk impacts and their associated controls.

Testing and Auditing of Security Measurements [§I A18 2.f]

Testing and auditing are routinely discussed as the third line of defense in a security program. They ensure that the governance and execution of a security program are aligned and that the overall measurements are efficient. To perform testing or auditing within an ICS/OT environment, IEs and EEs need to select technologies, procedures, and an audit partner that can not only support data retention and metrics, but also inform evidence-gathering capabilities.

Use of Cryptography and Encryption [§I A18 2.g]

While common in traditional IT and enterprise networks, cryptography and encryption should be used in only a few use cases for ICS/OT environments. Much of the data in production networks (SCADA and DCS) is real-time, with high constraints on availability and integrity, not on confidentiality. Furthermore, the production data itself may be of limited value to threat actors.

Because ICS/OT systems are deterministic in nature, there is an advantage to *not* encrypting the data communicated across Level 2 and Level 0/1 devices within ICS networks because having the data unencrypted will allow defenders to quickly identify malicious communications from threat actors. Instead, for specific ICS/OT networks, EEs and IEs should consider detection solutions, combined with strong firewall perimeters and OT-specific rules for what may be communicated across those boundaries. This topic is further explored later in this paper with a discussion on reference architectures for ICS/OT.

Cyber Program Management, Oversight, and Accountability [§I A17]

All of these security controls and measures, of course, must reside within a program with sufficient authority to implement controls across the organization. For NIS2, that authority should stretch all the way up to the board of directors. Article 17 of the NIS2 Directive directs the management bodies of essential and important entities to approve of the program outlined in the previous section.

The SANS ICS418: ICS Security Essentials for Managers course teaches overall governance of an ICS-specific security program, including establishing an industrial cyber-risk committee (outlined in Figure 9). Cyber program management and governance, when performed correctly, provides oversight and accountability for the overall implementation of the NIS2 Directive.

Working across business units and the IT-OT boundary will ensure proper coverage of security measures based on risk analysis for both enterprise-based events and operations-specific ones. This inter-business collaboration could also provide further visibility across technologies and processes that support the NIS2 implementation.

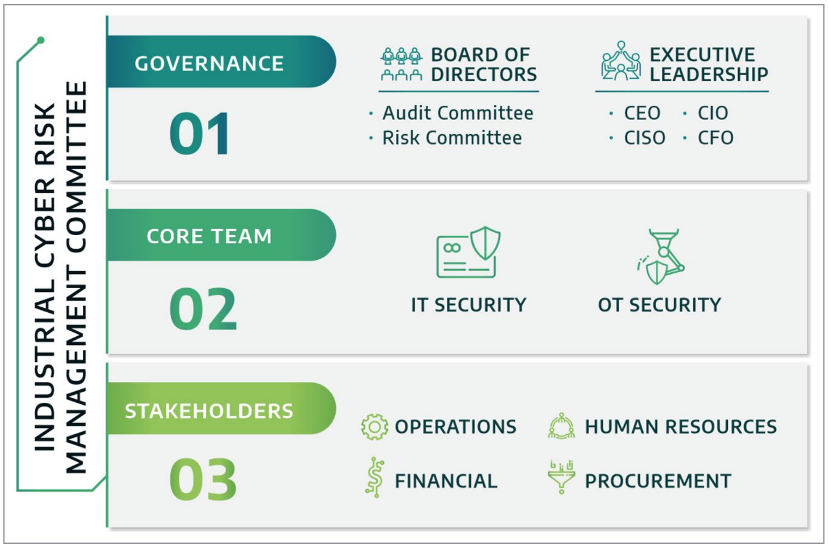


Figure 9. Industrial Cyber-Risk Management Committee Structure[11]

[11] More information about industrial cyber-risk committees can be found at www.dragos.com/resource/industrial-cyber-risk-management and overall governance practices are taught through ICS418: www.sans.org/ics418

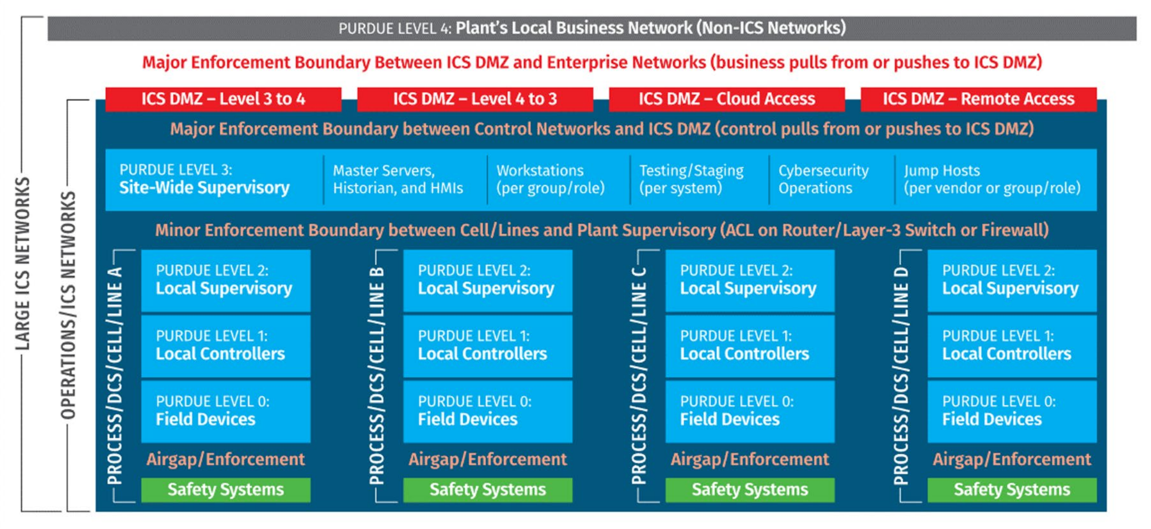
NIS Directive Compliance and IT/OT Security Architecture

The NIS2 Directive carries with it some potentially heavy penalties for noncompliance. It establishes administrative fines of up to €10 million or 2% of the entity's total turnover worldwide, whichever is higher. Also, IEs that suffer from an incident may find themselves with a more rigorous regulatory structure (similar to EEs) in response to the incident, so it is important to get the compliance program for OT right the first time.

To apply technologies correctly across your ICS environment to comply with NIS2, entities must understand their system architecture. The next section will explore how to appropriately establish boundaries for ICS/OT networks, which is a vital skill for NIS2 compliance.

Defense-in-Depth Techniques and the ICS410 Reference Model

One of the visual references used at SANS to discuss ICS security is the reference model from the ICS410: ICS/SCADA Security Essentials class. It expands on the Purdue Model for ICS Security to enhance concepts associated with segmenting OT networks (and isolating them from enterprise IT), as well as providing examples for general ICS architectures. An example of the reference model for larger industrial facilities, such as a manufacturing site, is highlighted in Figure 10.



LARGE ICS NETWORKS
OPERATIONS/ICS NETWORKS
PURDUE LEVEL 4: Plant's Local Business Network (Non-ICS Networks)
Major Enforcement Boundary Between ICS DMZ and Enterprise Networks (business pulls from or pushes to ICS DMZ)
ICS DMZ – Level 3 to 4
ICS DMZ – Level 4 to 3
ICS DMZ – Cloud Access
ICS DMZ – Remote Access
Major Enforcement Boundary between Control Networks and ICS DMZ (control pulls from or pushes to ICS DMZ)
PURDUE LEVEL 3: Site-Wide Supervisory
Master Servers, Historian, and HMIs
Workstations (per group/role)
Testing/Staging (per system)
Cybersecurity Operations
Jump Hosts (per vendor or group/role)
Minor Enforcement Boundary between Cell/Lines and Plant Supervisory (ACL on Router/Layer-3 Switch or Firewall)
PROCESS/DCS/CELL/LINE A
PROCESS/DCS/CELL/LINE B
PROCESS/DCS/CELL/LINE C
PROCESS/DCS/CELL/LINE D
PURDUE LEVEL 2: Local Supervisory
PURDUE LEVEL 1: Local Controllers
PURDUE LEVEL 0: Field Devices
Airgap/Enforcement
Safety Systems

Figure 10. ICS410 Reference Model for Large Industrial Facilities

The model in Figure 10 shows clear distinctions for different network boundaries and where specific operational *and security* functions take place.

- **Enforcement boundaries and DMZs (red)** include cybersecurity technologies to limit and monitor communications. Items typically found in this zone include firewalls, network-based intrusion detection systems, network-based intrusion prevention systems, routers (with access control lists, or ACLs), data diodes, NetFlow collectors, and full-packet collectors. A DMZ can be leveraged in any enforcement boundary. The DMZ provides a staging and inspection area to pass data between two levels, where neither side has full control. The preferred model is for one side to push data to the DMZ and the other side to pull that data when needed.

- **Enterprise and business networks (gray)** are IT networks for business users at local sites. This level includes business workstations, local file and print servers, local phone systems, enterprise Active Directory (AD) replicas, connectivity to enterprise WAN, and possibly local internet access. No system that can influence OT processes should be in this level. Direct internet access should not extend below this level.
- **Industrial Control Systems (blue)** includes:
  - **Purdue Level 3:** Monitoring, supervisory, and operational support for an entire site or region. This level can include master servers, HMIs, alarm servers, analytic systems, or historians if scoped for an entire site or region. Level 3 can (and should) be broken into multiple subnets, grouped by function/role to simplify ACLs, enable deep packet inspection (DPI) within firewalls to inspect industrial protocols for malicious payloads and configure intrusion prevention (IPS) system features (e.g., virtual patching to mitigate exploitation of potential vulnerabilities in the legacy ICS/OT assets). If AD is needed, use a separate domain with no trust relationships. Use a subnet here for security servers such as SIEM, patching, and endpoint security.
  - **Purdue Level 2:** Monitoring and supervisory control for a single process, cell, line, or DCS solution. Isolate processes from one another, grouping by function, type, or risk. This level includes HMIs, alarm servers, process analytic systems, historians, or control room if scoped for a single process and not the site/region. Systems in this level can leverage AD in Level 3 if needed.
  - **Purdue Level 1:** Devices and systems to provide automated control of a process, cell, line, or DCS solution. Devices can include programmable logic controllers (PLCs), control processors, programmable relays, remote terminal units (RTUs), and process-specific microcontrollers. Modern ICS solutions often obscure the lines between Levels 0 and 1.
  - **Purdue Level 0:** Sensors and actuators for the cell, line, process, or DCS solution, possibly including basic sensors/actuators, smart sensors/actuators, speaking fieldbus protocols, intelligent electronic devices (IEDs), IIoT devices, communications gateways, and other field instrumentation.
- **Safety Systems (green)** are engineered for a specific protective function, attempting to prevent worst-case scenarios. This level includes all items identified in Levels 0 and 1 with a dedicated purpose of a safety control function such as acoustic monitoring, liquid chemistry monitoring, vibration monitoring, and emission monitoring. In most safety systems, a control function serves to protect the operation and personnel.

This reference model approach may cover larger service territories for EEs and IEs, such as water and power utilities, in which case both enterprise and SCADA WANs would expand the visibility and communication capabilities for essential services, as highlighted in Figure 11.

Regardless of the OT network, the ICS410 Reference Architecture can be used to describe technology implementations of NIS2, especially for organizations examining placement of security controls, which is described later in this document.

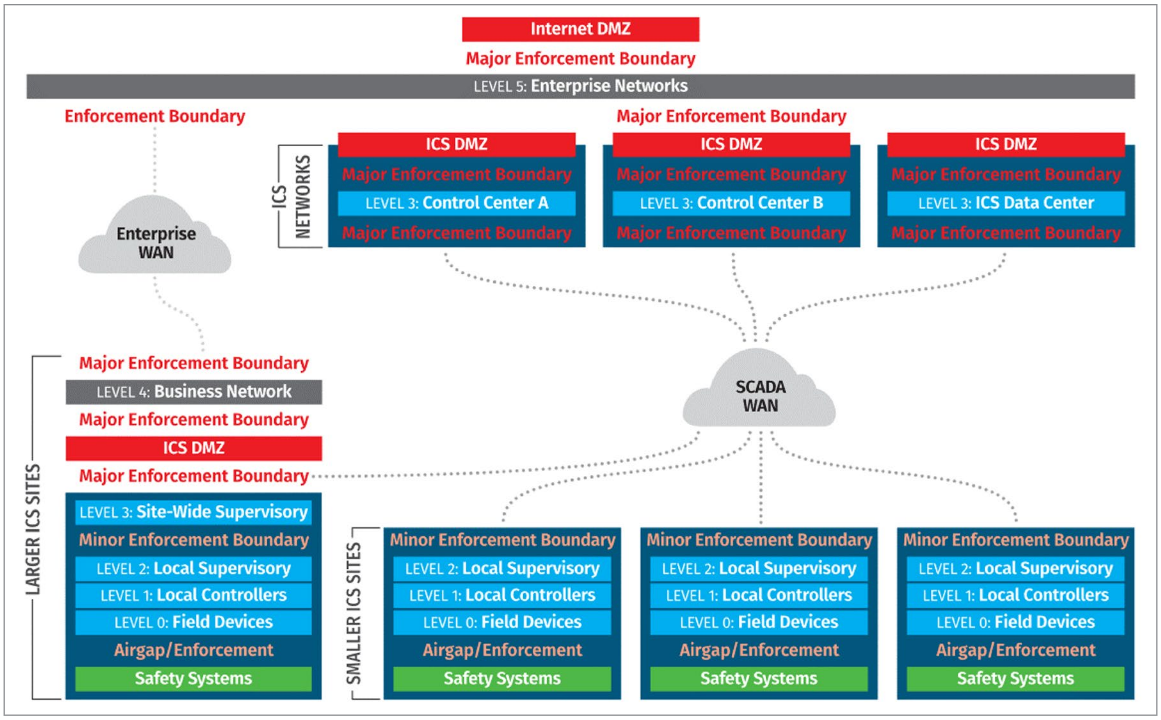

Internet DMZ
Major Enforcement Boundary
LEVEL 5: Enterprise Networks
Enforcement Boundary
Major Enforcement Boundary
ICS NETWORKS
ICS DMZ
Major Enforcement Boundary
LEVEL 3: Control Center A
Major Enforcement Boundary
ICS DMZ
Major Enforcement Boundary
LEVEL 3: Control Center B
Major Enforcement Boundary
ICS DMZ
Major Enforcement Boundary
LEVEL 3: ICS Data Center
Major Enforcement Boundary
Enterprise WAN
SCADA WAN
LARGER ICS SITES
Major Enforcement Boundary
LEVEL 4: Business Network
Major Enforcement Boundary
ICS DMZ
Major Enforcement Boundary
LEVEL 3: Site-Wide Supervisory
Minor Enforcement Boundary
LEVEL 2: Local Supervisory
LEVEL 1: Local Controllers
LEVEL 0: Field Devices
Airgap/Enforcement
Safety Systems
SMALLER ICS SITES
Minor Enforcement Boundary
LEVEL 2: Local Supervisory
LEVEL 1: Local Controllers
LEVEL 0: Field Devices
Airgap/Enforcement
Safety Systems

Figure 11. ICS410 Reference Model for SCADA over a Large Geographic Area

EU-CyCLONe and Member-State CSIRTs

As mentioned earlier, EEs and IEs have mandatory reporting requirements under NIS2 for cyber incidents. Within 24 hours, entities need to report to the member state's cybersecurity incident response team (CSIRT). The CSIRT will then provide a response and could potentially request interim reports from entities up until a final report is submitted to the CSIRT within a month of the incident first being reported.

Individual member-state CSIRTs will also collaborate with the EU cyber-crisis liaison organization network (EU-CyCLONe), a cooperative network for the national authorities in member states that are in charge of managing cyber crises. EU-CyCLONe is designed to enable timely information sharing and situational awareness across the entire EU, which could have specific benefits during systemic attacks that target multiple regions and sectors simultaneously.

Information sharing, even under regulatory contexts such as NIS2, can be a force multiplier for entities as they build OT-specific elements of their cybersecurity program. CSIRTs and the supporting EU-CyCLONe can help inform event detection, allow entities to better understand cyber events, and further enable the dissemination of intelligence to entities. In order to better facilitate incident handling and reporting, EEs and IEs should focus on the following actions:

- Identify cyber events and escalate to cyber incidents, including the criteria for what incidents should be reported to the member-state CSIRT
- Establish and maintain a relationship with the CSIRT prior to any incident
- Ensure technologies address all aspects of the ICS410 Reference Architecture and provide visibility across the IT and OT networks

Programmatic Considerations for Implementing NIS2 in OT

The updated NIS Directive provides requirements to create a cybersecurity program based on strengthening cyber-risk management and cyber-incident response. These two pillars of security address an organization's capabilities of measuring its cybersecurity posture and recovering from an incident. For OT, both of these concepts require understanding the industrial environment, protecting critical assets, and monitoring for malicious communications.

NIS2 provides governance and policies throughout. Because there is flexibility in the approach that entities are allowed to take, there is no single set of policies or prescriptive templates for organizations to use. So, to better understand the necessary components for a successful cybersecurity program, entities should evaluate the elements shown in Figure 11 within their industrial facilities and OT networks.

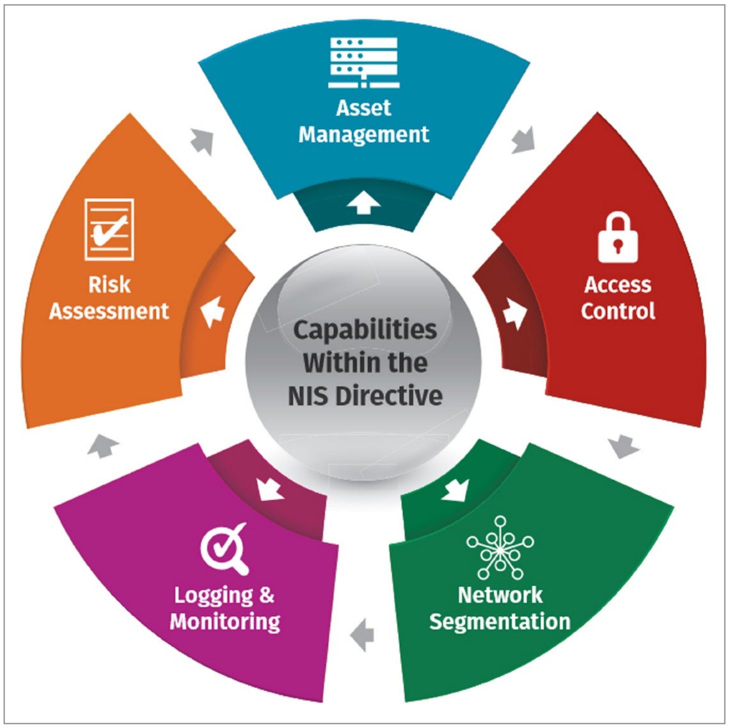


Figure 12. Capabilities Within the NIS-D

Asset Management

Simply put, asset management is the discipline of understanding the devices within a network. A robust NIS2 program has a current inventory, including important parameters for securing those devices, such as associated software and firmware versions, known security controls, and criticality of the asset itself.

Asset management is the logical starting point for any security program because it tells entities what to protect. Within risk management, asset inventories can ensure that protections are prioritized based on business and cyber risk and account for which security controls are relevant to the assets themselves. Moreover, when recovering from an incident, an up-to-date asset inventory is invaluable for incident response teams to ensure that containment, eradication, and recovery steps are used for all impacted assets during an event as covered (refer to Figure 6 on page 9).

Access Control

Once teams understand their assets and any associated criticality, access control provides context for anyone controlling the devices. This level of understanding may be difficult in the case of a variety of field devices, which do not accept usernames and passwords or other credentials. Furthermore, a variety of ICS devices have default and/or hard-coded passwords used by vendors and maintenance technicians that add complexity to any access control management program, which is an important consideration for NIS2 security policies and supply chain risk management elements.

Where possible, however, entities should examine strong access control within their control centers and across HMIs. Managing access can ensure that only approved operators, managers, and support teams may control critical assets related to the industrial process. Furthermore, appropriate logging of user activity can help identify any root causes during a cyber incident.

While access control can be challenging, it is vital that corporate networks and identities are not leveraged within the control system network. ICSes should be at a more stringent level of access and trust, as seen in the ICS 410 Reference Architecture.

Network Segmentation

System hardening around OT can be difficult. Many assets have limited cybersecurity capabilities across a longer life cycle than traditional information-centric technologies. As such, entities will need to rely on strong network perimeters by segmenting critical OT networks from corporate communications. An OT network segment should also leverage an ICS DMZ and an architecture similar to that shown in Figure 9 on page 11.

In addition to implementing network segmentation at the network perimeter, internal segmentation, also known as network microsegmentation, of the industrial networks is necessary to determine zones (according to processes controlled) and conduits (their connections) and properly address risk to each zone (as explained later in this paper). Such internal segmentation will also enable zero-trust capabilities by associating access types with each zone by determining roles, industrial protocols and applications, and associated privilege levels.

These industrial networks should be supported by both the asset management program (what devices should be in the network or in the DMZ?) and the access control capabilities (who has permission to access the network, or who can communicate across the DMZ?). All this information is extremely valuable for responding to a cybersecurity incident, but it can also *prevent* incidents with proper management of network segmentation and control.

Logging and Monitoring

Monitoring, or the active task of reviewing logs across users, assets, and networks, is a critical capability for responding to cybersecurity incidents and helping to identify what went wrong. While system logs within OT environments will vary, a proactive approach to log centralization for monitoring can help ease the burden when an incident response team attempts to identify the root cause of an event. In the context of NIS2, this approach will be important for reporting to CSIRTs.

Risk Assessment

Cyber-risk assessments and analysis, like risk analysis for safety or financial risks, should be routine for any entity. A risk assessment should evaluate the impacts associated with a potential cyber event across the myriad of attack vectors threat adversaries may use to exploit the vulnerabilities within any given system. Risk assessments effectively answer the question "What does a really bad day look like, and what is the potential of it happening based on the resilience of our OT infrastructure?" This assessment can be supplemented with an incident response tabletop exercise (TTX) that simulates or operationally tests real-world incidents specific to industrial environments. OT security teams should regularly run drills using TTXes and provide results to enterprise risk professionals for analysis. Some risk assessments may also attempt to look at the likelihood of the event or map events to known threats to examine the potential risks involved.

Within OT, risk evaluation should be based on the industrial process at each entity and the uniqueness of the system architecture. A risk assessment evaluates the assets being managed and how they can potentially be misused to cause a loss (or manipulation) of visibility or control within the ICS. This is different from information-centric systems in IT, which evaluate data breaches or loss of information systems. Benchmarking across both IT and OT could be desirable for entities that manage multiple systems, as long as the differences between each are accounted for within the risk assessment process.

Each of these capabilities requires the right combination of people, processes, and technology. A well-trained workforce should understand the critical assets and systems, as well as the security controls required to protect the industrial processes for any given facility or control system. Operators who understand both cyber defenses *and* control systems are vital for cyber-risk management and incident response. They will also help build repeatable processes to ensure that NIS2 is appropriately leveraged across the entity. Processes or procedures ensure that a compliance program can build on the knowledge of the workforce and further enable technology to protect critical systems. This last piece, the technology, can automate difficult tasks as well as establish protections across IT and OT systems. The collective capabilities of people, processes, and technology shown in Figure 13 can create a powerful and defensible NIS2-based cybersecurity program for critical infrastructure protection.

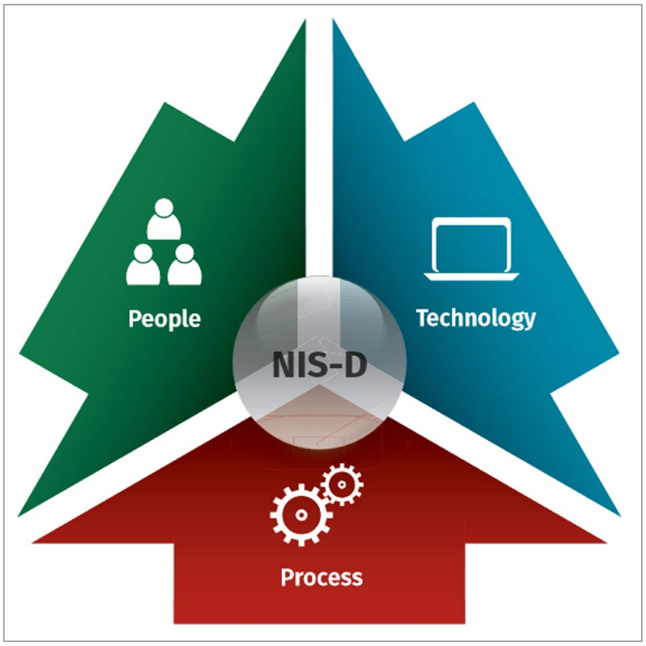


Figure 13. People, processes, and technology work together to form an NIS-based cybersecurity program.

The next section examines how Fortinet technologies can leverage the components outlined here and play a role in an NIS2 program.

Using Fortinet Security Fabric with NIS2

Fortinet maintains a large catalog of security products, which collectively provide multiple security capabilities. Fortinet offers a platform-based approach to cybersecurity through integration of these products in a unified portfolio, known as the Fortinet Security Fabric, that helps establish broad visibility, control, and automation for security operations and management across IT/OT environments. Table 3 highlights many Fortinet products.

Table 3. Fortinet Product Descriptions

Fortinet Product	Product Description
FortiEDR	FortiEDR delivers real-time automated endpoint protection with orchestrated incident response across IT and OT endpoints. A single integrated platform with flexible deployment options and a predictable operating cost, FortiEDR provides real-time proactive risk mitigation, endpoint security, pre-infection protection via a kernel-level, next-generation antivirus engine, post-infection protection, and forensics.
FortiClient FortiClient EMS	FortiClient in an endpoint agent that provides visibility and control of software and hardware inventory across the entire Fortinet Security Fabric, allowing organizations to discover, monitor and assess endpoint risks in real time. It also provides secure remote access (VPN client). FortiClient, along with the FortiClient Enterprise Management Server (EMS), is an integral part of Fortinet's zero-trust network access (ZTNA) offering. FortiClient includes the ZTNA, secure access service edge (SASE), and endpoint protection (EPP) capabilities: • ZTNA enables remote users to access their corporate applications while ensuring that strict authentication and verifiable endpoint security posture before any access is granted. • SASE ensures that remote users can securely connect to the corporate network following the same corporate security policies regardless of their location. SASE integrates seamlessly with ZTNA to deliver a transparent user experience while offering security protection for all endpoints from advanced threats. • EPP offers vulnerability detection and protection, auto-patching antivirus, application firewall, anti-ransomware, and endpoint management.
FortiSwitch	FortiSwitch is a secure access switch family that delivers outstanding performance, scalability, and manageability while allowing OT environments to extend networking and security across their network infrastructure. FortiSwitch seamlessly integrates with the Fortinet Security Fabric via FortiLink and can be managed by FortiCloud or FortiGate. The unified management of FortiSwitch via FortiGate offers complete visibility and control of users and devices in the network.
FortiAP	FortiAP is a series of Wi-Fi access points that can be managed by FortiCloud or FortiGate. These access points offer high throughput, optimal coverage, and enterprise-class 802.11ax services, and they enable security and access control policy enforcement. FortiAPs can seamlessly integrate with the Fortinet Security Fabric.
FortiExtender	FortiExtender provides a bridge between local Ethernet LANs and wireless LTE/5G WAN connections. FortiExtender can support diverse wireless applications with a high-level of backhaul redundancy using a single LTE/5G modem platform over redundant SIM cards attaching to different mobile networks. FortiExtender can be used as the LTE/5G backhaul of an on-premises FortiGate with maximum wireless LTE/5G signal strength. It can be centrally managed by FortiGate.
FortiGate	FortiGate is the flagship next-generation firewall and intrusion prevention system (NGFW/NGIPS) product family from Fortinet, delivering best-in-class security, high-speed networking, hardware-accelerated performance features using purpose-built security processors for NGFW/NGIPS, and built-in market-leading SD-WAN. FortiGate comes in different form factors and sizes, including ruggedized appliances to withstand the harsh environmental conditions often facing industrial applications.
FortiToken	FortiToken enables two-factor authentication via a one-time password (OTP) application with push notifications or a hardware time-based OTP token. FortiToken Mobile (FTM) and the hardware OTP Tokens are fully integrated with FortiClient, are secured by FortiGuard, and are available for direct management and use within the FortiGate and FortiAuthenticator security products. The FortiGate, FortiToken, and FortiAuthenticator integrated solution is easy to implement, use, and manage for multifactor authentication.
FortiAuthenticator	FortiAuthenticator offers single sign-on and user authorization for the Fortinet secured enterprise network. It identifies users, queries access permissions from third-party systems, and forwards the access requests to FortiGate to implement identity-based security policies. FortiAuthenticator supports a wide array of methods and tools for authentication and authorization, such as Active Directory, RADIUS, LDAP, SAML SP/IdP, PKI, and multifactor authentication.

Table 3. Fortinet Product Descriptions (Continued)

Fortinet Product	Product Description
FortiNAC	This network access control product enhances the Fortinet Security Fabric with visibility, control, and automated response for everything that connects to the network. FortiNAC provides protection against malicious access, extends access control to third-party devices, offers greater visibility for devices, supports dynamic network access control, and orchestrates automatic responses to a wide range of networking events.
FortiAnalyzer	FortiAnalyzer is a centralized log management, analytics, and reporting platform that provides customers with single-pane orchestration, automation, and response for simplified security operations, proactive identification, remediation of risks, and complete visibility of the entire attack surface. FortiAnalyzer can collect different types of logs and events from Fortinet products via Fortinet Security Fabric integration.
FortiManager	FortiManager provides automation-driven centralized management. IT allows end users to centrally manage FortiGate, FortiSwitch, and FortiAP devices in their network with a centralized management platform.
FortiSIEM	FortiSIEM provides unified event correlation and risk management for multivendor implementations. It enables analytics from diverse information sources including logs, performance metrics, SNMP traps, security alerts, and configuration changes. It feeds all the information into an event-based analytics engine and supports real-time searches, rules, dashboards, and ad-hoc queries. FortiSIEM offers Purdue-level classification for assets, logs, and event correlation and it also supports MITRE ATT&CK for ICS framework for log analysis. Integration with third-party OT security tools is supported out of the box.
FortiSOAR	FortiSOAR is a holistic security orchestration, automation, and response workbench that lets security operations center (SOC) teams efficiently respond to the ever-increasing influx of alerts, automate repetitive manual processes, and cope with their chronic shortage of resources. Its patented and customizable security operations platform provides, automated playbooks and incident triaging, and real-time remediation for enterprises to identify, defend, and counter attacks. FortiSOAR optimizes SOC team productivity by proving more than 3,000 actions and seamlessly integrating with over 300 security platforms. This results in faster responses, streamlined containment, and mitigation times reduced from hours to seconds. FortiSOAR includes ICS-specific capabilities, such as MITRE ATT&CK for ICS framework for asset and event correlation, IT/OT asset inventory dashboards, compliance dashboards for OT specific cybersecurity regulations and frameworks, and more.
FortiProxy	A secure web proxy that protects employees against internet-borne attacks by incorporating multiple detection techniques, such as web filtering, DNS filtering, data loss prevention, antivirus protection, intrusion prevention and advanced threat protection.
FortiWeb	A web application firewall (WAF) that secures cloud-based resources and DevOps environments by protecting against known and unknown threats, including sophisticated ones such as SQL injection, cross-site scripting, buffer overflows and DDoS attacks.
FortiDeceptor	FortiDeceptor provides honeypot and deception technology to deceive, expose, and eliminate external and internal threats early in the attack kill chain, proactively blocking these threats before any significant damage occurs. Integrated with FortiEDR and FortiGate, FortiDeceptor automates the blocking of attackers targeting IT and OT systems and devices by laying out a layer of decoys and lures designed to redirect attackers' focus while revealing their presence on the network.
FortiSandbox	FortiSandbox provides top-rated AI-powered breach protection that integrates with the Fortinet Security Fabric platform to address both rapidly evolving and targeted threats, including ransomware and crypto-malware, across a broad digital attack surface. Designed specifically for OT, FortiSandbox automates zero-day advanced malware detection and response fin order to detect in real time threats targeting OT systems and protocols.
FortiNDR	FortiNDR offers next-generation, AI-driven breach protection technology to defend against various cyber threats, including advanced persistent threats through a trained Virtual Security Analyst™. The virtual analyst helps with identifying, classifying, and responding to threats, including well-camouflaged ones. Employing deep neural networks based on advanced AI and artificial neural networks, FortiNDR provides fast security investigation (less than one second) by harnessing deep-learning technologies that assist in an automated response to remediate different types of attacks.
FortiSASE	A cloud-delivered service, FortiSASE is an architecture that combines network, security, and WAN capabilities to provide endpoints (remote users, devices, and branches) with secure access to the internet, cloud resources, and the data center network. It uses network security technologies including firewall-as-a-service (FWaaS), secure web gateway (SWG), ZTNA, and cloud access security broker (CASB). It relies on WAN technologies including SD-WAN.
FortiGuard Security Services	FortiGuard Security Services are powered by FortiGuard Labs, a global threat research and response team that leverages machine learning (ML) and AI systems around the globe to collect real-time threat intelligence. FortiGuard Security Services are offered through subscription bundles and include several advanced threat protection services for enterprise networks, web, cloud, OT, etc. The Industrial Security Service and IoT Detection Service are among the FortiGuard subscription offerings. Industrial Security Service offers more than 2,000 IPS signatures for ICS/OT applications as well as protocols that support deep packet inspection (DPI) and more than 500 IPS signatures for ICS-specific threat and vulnerability protection.
FortiCamera FortiRecorder	A suite of secure, network-based video surveillance cameras and recorders that bolster protection against cyber-physical attacks.

The previous section examined several elements of cyber-risk management and incident response capabilities that are required for a NIS2 program. Those elements can be complemented by several Fortinet products, which are reviewed next.

Asset Management

Asset management (see Figure 14) is used within the context of NIS2 to identify critical assets and systems. This helps entities establish visibility, understand the industrial network, and provide valuable information during incident response.

During our test, we looked at capabilities within the FortiGate Rugged 70F firewall, which is Fortinet's next-generation firewall and intrusion prevention system for operational technology environments. From the menu, as seen in Figure 15, operators get easy access to their connected hardware inventory, with customization for insight into where the device sits relevant to the reference model we introduced earlier, including the ICS DMZ.

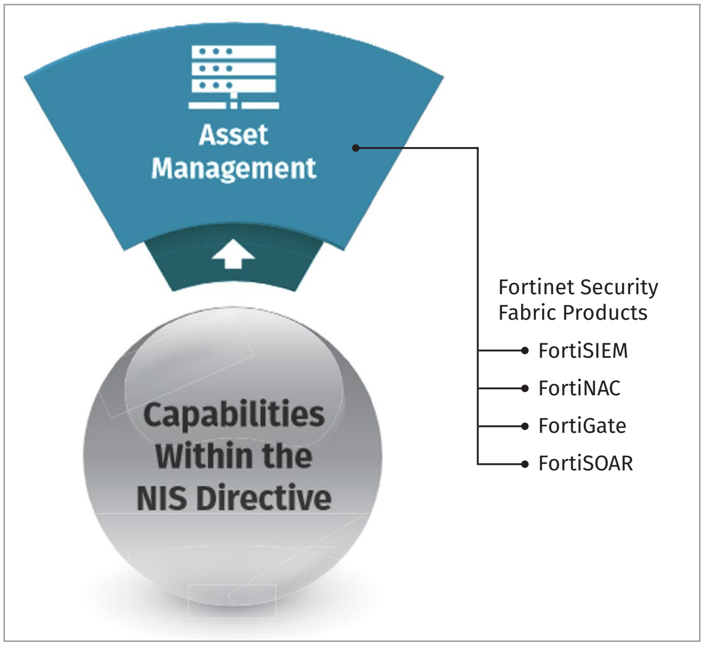
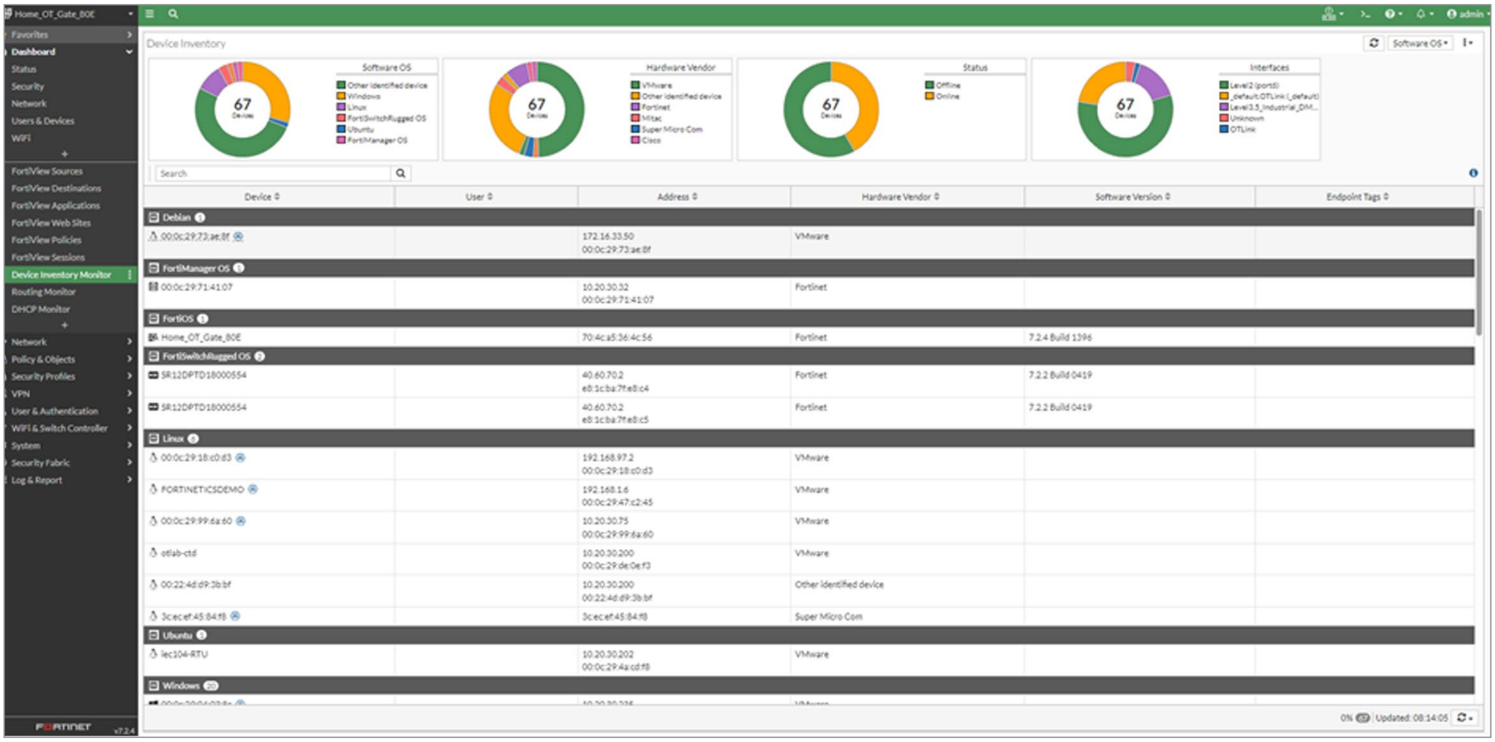


Figure 14. NIS2 Capability: Asset Management

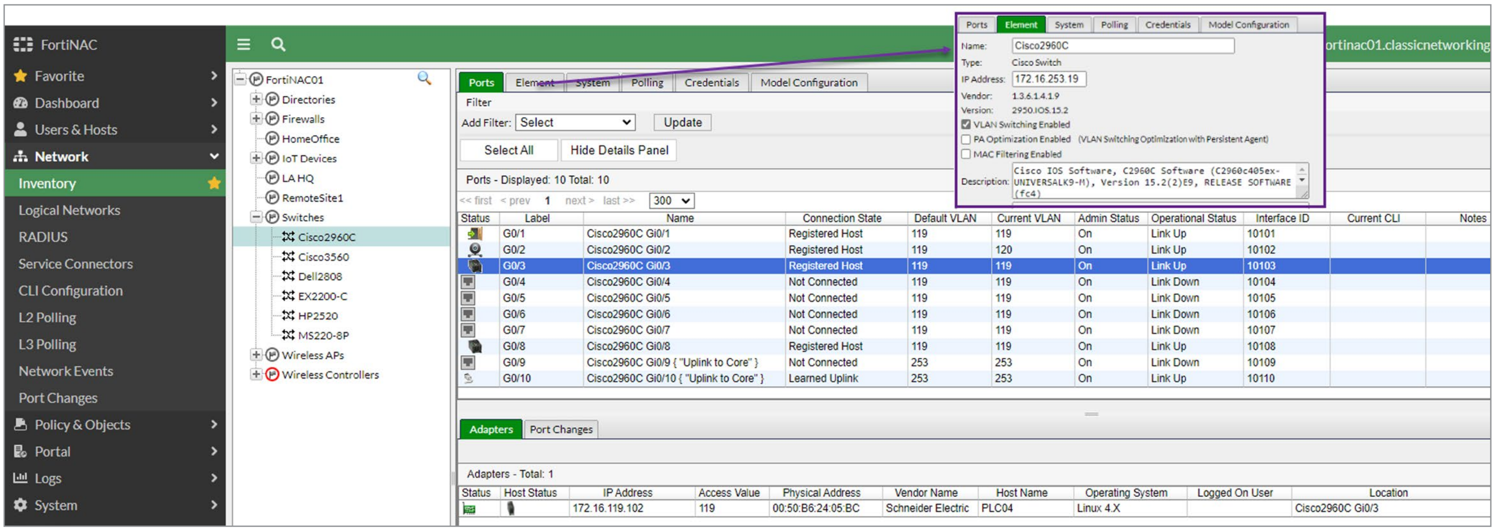


Device Inventory

Device	User	Address	Hardware Vendor	Software Version	Endpoint Tags
Debian 1					
00:0c:29:73:ae:8f		172.16.33.50 00:0c:29:73:ae:8f	VMware		
FortiManager OS 1					
00:0c:29:71:41:07		10.20.30.32 00:0c:29:71:41:07	Fortinet		
FortiOS 1					
Home_OT_Gate_80E		70:4c:a5:36:4c:56	Fortinet	7.2.4 Build 1396	
FortiSwitchRugged OS 2					
SR12DPTD18000554		40.60.70.2 e8:1c:ba:7f:e8:c4	Fortinet	7.2.2 Build 0419	
SR12DPTD18000554		40.60.70.2 e8:1c:ba:7f:e8:c5	Fortinet	7.2.2 Build 0419	
Linux 6					
00:0c:29:18:c0:d3		192.168.97.2 00:0c:29:18:c0:d3	VMware		
FORTINETICSDEMO		192.168.1.6 00:0c:29:47:c2:45	VMware		
00:0c:29:99:6a:60		10.20.30.75 00:0c:29:99:6a:60	VMware		
otlab-ctd		10.20.30.200 00:0c:29:de:0e:f3	VMware		
00:22:4d:d9:3b:bf		10.20.30.200 00:22:4d:d9:3b:bf	Other identified device		
3c:ec:ef:45:84:f8		3c:ec:ef:45:84:f8	Super Micro Com		
Ubuntu 1					
Iec104-RTU		10.20.30.202 00:0c:29:4a:cd:f8	VMware		
Windows 20					

Figure 15. FortiGate's Device Inventory View

To further help with hardware inventory, the Fortinet Security Fabric provides integration of FortiNAC and FortiSIEM, providing more information and context around the devices on the network, including non-Fortinet network devices. This information can be exported into several formats, as seen in Figure 16. Report generation and up-to-date inventories are vital for aiding sustainability across any NIS2 program.



Name: Cisco2960C
Type: Cisco Switch
IP Address: 172.16.253.19
Vendor: 1.3.6.1.4.1.9
Version: 2950.IOS.15.2
☑ VLAN Switching Enabled
☐ PA Optimization Enabled (VLAN Switching Optimization with Persistent Agent)
☐ MAC Filtering Enabled
Description: Cisco IOS Software, C2960C Software (C2960c405ex-UNIVERSALK9-M), Version 15.2(2)E9, RELEASE SOFTWARE (fc4)

Ports - Displayed: 10 Total: 10

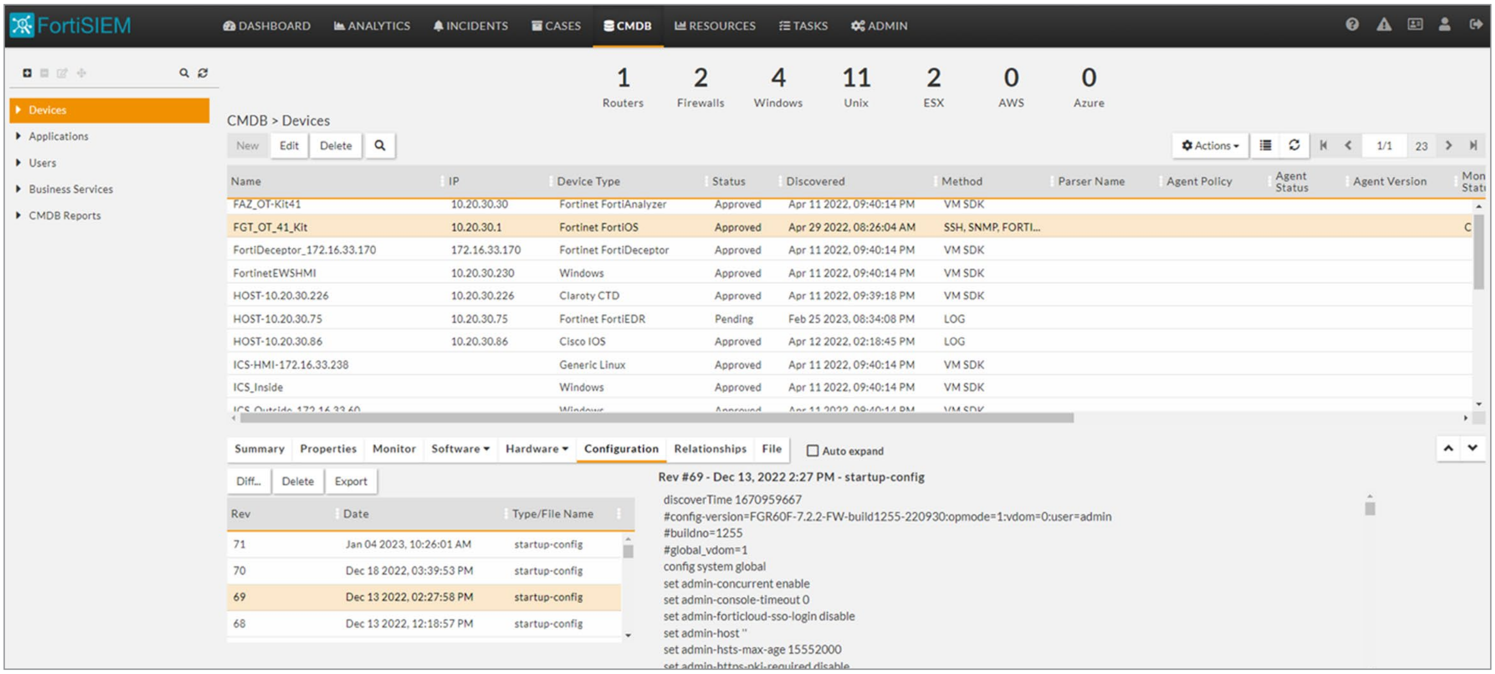
Status	Label	Name	Connection State	Default VLAN	Current VLAN	Admin Status	Operational Status	Interface ID	Current CLI	Notes
	G0/1	Cisco2960C Gi0/1	Registered Host	119	119	On	Link Up	10101		
	G0/2	Cisco2960C Gi0/2	Registered Host	119	120	On	Link Up	10102		
	G0/3	Cisco2960C Gi0/3	Registered Host	119	119	On	Link Up	10103		
	G0/4	Cisco2960C Gi0/4	Not Connected	119	119	On	Link Down	10104		
	G0/5	Cisco2960C Gi0/5	Not Connected	119	119	On	Link Down	10105		
	G0/6	Cisco2960C Gi0/6	Not Connected	119	119	On	Link Down	10106		
	G0/7	Cisco2960C Gi0/7	Not Connected	119	119	On	Link Down	10107		
	G0/8	Cisco2960C Gi0/8	Registered Host	119	119	On	Link Up	10108		
	G0/9	Cisco2960C Gi0/9 { "Uplink to Core" }	Not Connected	253	253	On	Link Down	10109		
	G0/10	Cisco2960C Gi0/10 { "Uplink to Core" }	Learned Uplink	253	253	On	Link Up	10110		

Adapters - Total: 1

Status	Host Status	IP Address	Access Value	Physical Address	Vendor Name	Host Name	Operating System	Logged On User	Location
		172.16.119.102	119	00:50:B6:24:05:BC	Schneider Electric	PLC04	Linux 4.X		Cisco2960C Gi0/3

Figure 16. FortiNAC Information View, Including Non-Fortinet Devices

Within FortiSIEM, entities can utilize a configuration management database (CMDB), which provides additional information on critical assets, including software and configuration information as well as assign criticality levels, as seen in Figure 17.



Name	IP	Device Type	Status	Discovered	Method	Parser Name	Agent Policy	Agent Status	Agent Version	Mon Stat
FAZ_OT-Kit41	10.20.30.30	Fortinet FortiAnalyzer	Approved	Apr 11 2022, 09:40:14 PM	VM SDK					
FGT_OT_41_Kit	10.20.30.1	Fortinet FortiOS	Approved	Apr 29 2022, 08:26:04 AM	SSH, SNMP, FORTI...					C
FortiDeceptor_172.16.33.170	172.16.33.170	Fortinet FortiDeceptor	Approved	Apr 11 2022, 09:40:14 PM	VM SDK					
FortinetEWSHMI	10.20.30.230	Windows	Approved	Apr 11 2022, 09:40:14 PM	VM SDK					
HOST-10.20.30.226	10.20.30.226	Claroty CTD	Approved	Apr 11 2022, 09:39:18 PM	VM SDK					
HOST-10.20.30.75	10.20.30.75	Fortinet FortiEDR	Pending	Feb 25 2023, 08:34:08 PM	LOG					
HOST-10.20.30.86	10.20.30.86	Cisco IOS	Approved	Apr 12 2022, 02:18:45 PM	LOG					
ICS-HMI-172.16.33.238		Generic Linux	Approved	Apr 11 2022, 09:40:14 PM	VM SDK					
ICS_Inside		Windows	Approved	Apr 11 2022, 09:40:14 PM	VM SDK					
ICS_Outside_172.16.33.60		Windows	Approved	Apr 11 2022, 09:40:14 PM	VM SDK					

Rev	Date	Type/File Name
71	Jan 04 2023, 10:26:01 AM	startup-config
70	Dec 18 2022, 03:39:53 PM	startup-config
69	Dec 13 2022, 02:27:58 PM	startup-config
68	Dec 13 2022, 12:18:57 PM	startup-config

Rev #69 - Dec 13, 2022 2:27 PM - startup-config

```
discoverTime 1670959667
#config-version=FGR60F-7.2.2-FW-build1255-220930:opmode=1:vdom=0:user=admin
#buildno=1255
#global_vdom=1
config system global
set admin-concurrent enable
set admin-console-timeout 0
set admin-forticloud-sso-login disable
set admin-host ''
set admin-hsts-max-age 15552000
set admin-https-pki-required disable
```

Figure 17. CMDB Information from FortiSIEM

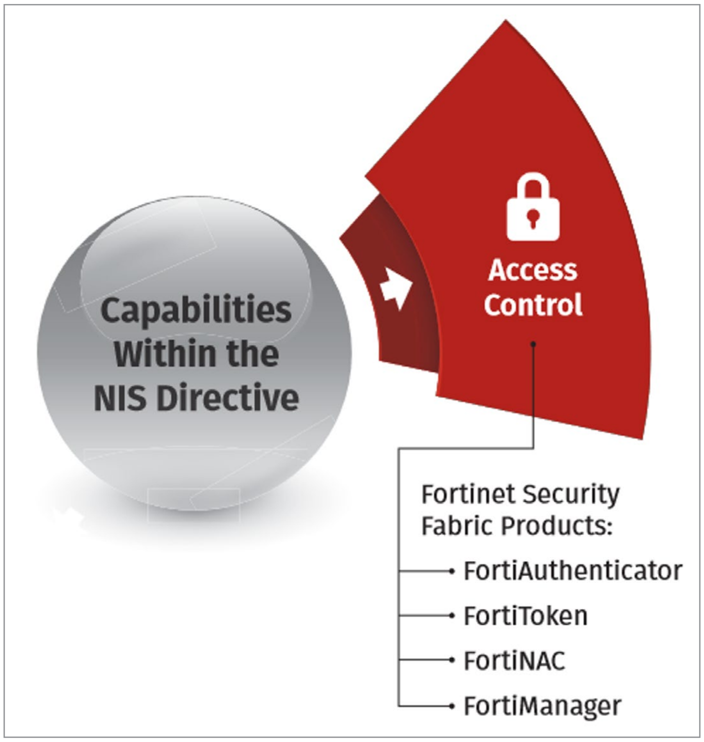
Beyond supporting risk-based mitigations covered in NIS2, the CMDB could also aid internal compliance teams evaluating the NIS2 program as outlined in Testing and Auditing of Security Measurements [§I A18 2.f].

Access Control

Access control (Figure 18) provides context regarding what persons or roles are operating and/or controlling the control system.

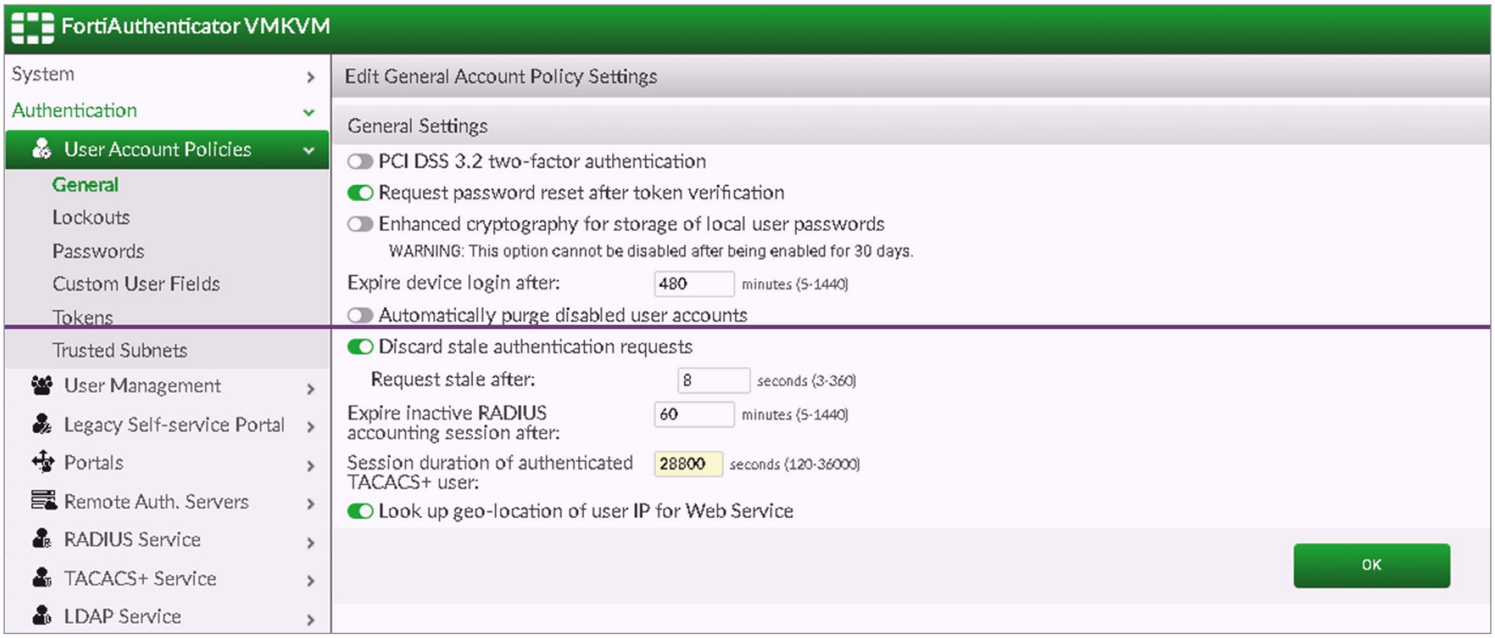
The Fortinet Security Fabric provides integrations for several Fortinet products, including FortiAuthenticator. FortiAuthenticator provides granular controls across users for access within the control network, as well as activity logging and monitoring. The users themselves can be based on identity- and role-based policies, providing profile building. See Figure 19.

FortiAuthenticator also has the capability to manage certificates, creating additional options for managing access across multiple control network devices. Certain environments will favor certificate management over individual user credentials, and the flexibility to manage those certificates at a system-level can provide additional security controls.



Capabilities Within the NIS Directive
Access Control
Fortinet Security Fabric Products:
FortiAuthenticator
FortiToken
FortiNAC
FortiManager

Figure 18. NIS2 Capability: Access Control



Edit General Account Policy Settings

General Settings

○ PCI DSS 3.2 two-factor authentication

● Request password reset after token verification

○ Enhanced cryptography for storage of local user passwords

WARNING: This option cannot be disabled after being enabled for 30 days.

Expire device login after: 480 minutes (5-1440)

○ Automatically purge disabled user accounts

● Discard stale authentication requests

Request stale after: 8 seconds (3-360)

Expire inactive RADIUS accounting session after: 60 minutes (5-1440)

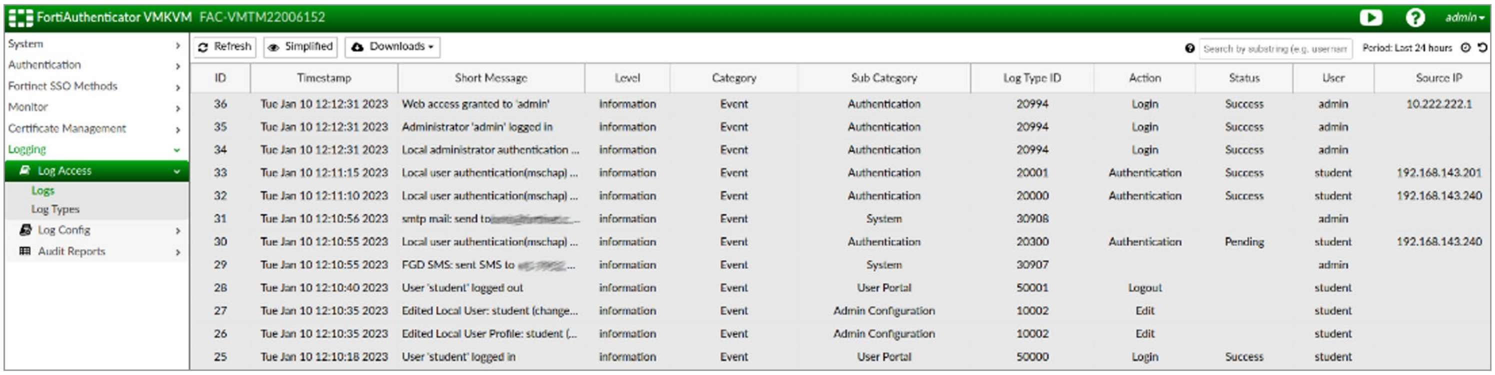
Session duration of authenticated TACACS+ user: 28800 seconds (120-36000)

● Look up geo-location of user IP for Web Service

Figure 19. User Account Policies View in FortiAuthenticator

FortiAuthenticator provides access governance to networks by establishing user identification (linkable to AD), authentication, and authorization (even temporarily closing timed-out connections automatically). The system connects users with networks and allows the addition of context tags to the networks for the necessary coordination with OT. Even guest management can be provided, which is especially welcome when urgent interventions require external access to keep processes transparent and traceable without slowing operations.

FortiToken, which was not accessible during this evaluation, can add two-factor authentication to FortiAuthenticator. While many corporate networks can deploy cloud-based solutions for two-factor authentication, the same is not true for control networks, which should be isolated and segmented from internet-facing authentication schemes or corporate AD instances. Two-factor authentication is a powerful security access control for higher-risk accounts, such as administrative access or remote access granted to third parties for maintenance within the control network. Event logs such as those in Figure 20 are invaluable for incident response and may be used in reporting for CSIRT-mandated incident handling reports. FortiToken resides within the Fortinet Security Fabric and can provide a potential solution locally for these concerns.



ID	Timestamp	Short Message	Level	Category	Sub Category	Log Type ID	Action	Status	User	Source IP
36	Tue Jan 10 12:12:31 2023	Web access granted to 'admin'	information	Event	Authentication	20994	Login	Success	admin	10.222.222.1
35	Tue Jan 10 12:12:31 2023	Administrator 'admin' logged in	information	Event	Authentication	20994	Login	Success	admin	
34	Tue Jan 10 12:12:31 2023	Local administrator authentication ...	information	Event	Authentication	20994	Login	Success	admin	
33	Tue Jan 10 12:11:15 2023	Local user authentication(mschap) ...	information	Event	Authentication	20001	Authentication	Success	student	192.168.143.201
32	Tue Jan 10 12:11:10 2023	Local user authentication(mschap) ...	information	Event	Authentication	20000	Authentication	Success	student	192.168.143.240
31	Tue Jan 10 12:10:56 2023	smtp mail: send to[redacted]...	information	Event	System	30908			admin	
30	Tue Jan 10 12:10:55 2023	Local user authentication(mschap) ...	information	Event	Authentication	20300	Authentication	Pending	student	192.168.143.240
29	Tue Jan 10 12:10:55 2023	FGD SMS: sent SMS to [redacted]...	information	Event	System	30907			admin	
28	Tue Jan 10 12:10:40 2023	User 'student' logged out	information	Event	User Portal	50001	Logout		student	
27	Tue Jan 10 12:10:35 2023	Edited Local User: student (change...	information	Event	Admin Configuration	10002	Edit		student	
26	Tue Jan 10 12:10:35 2023	Edited Local User Profile: student (...	information	Event	Admin Configuration	10002	Edit		student	
25	Tue Jan 10 12:10:18 2023	User 'student' logged in	information	Event	User Portal	50000	Login	Success	student	

Figure 20. Authentication Event Logs in FortiAuthenticator

Network Segmentation

OT networks are often described as following an M&M candy model: They have a hard outer shell and a soft center. Many of the devices within an ICS are difficult to harden, and operators have historically relied on strong perimeters to protect their critical assets, both physical and electronic.

Within the ICS410 Reference Architecture, these strong perimeters are major enforcement boundaries, protecting the higher-trust zones within supervisory control from the less-trustworthy corporate networks, with a DMZ in between. Minor enforcement boundaries are also placed between supervisory control (Level 3 devices) and local control (Level 2 and its corresponding Level 0/1 devices). When examining technology options for network segmentation (shown in Figure 21) to enforce these boundaries, the firewalls must have knowledge of industrial protocols. The FortiGate Rugged 70F, with FortiGuard Industrial Security Service, provides a robust list of industrial protocols that may be used in ICS networks, as seen in Figure 22 on the next page.

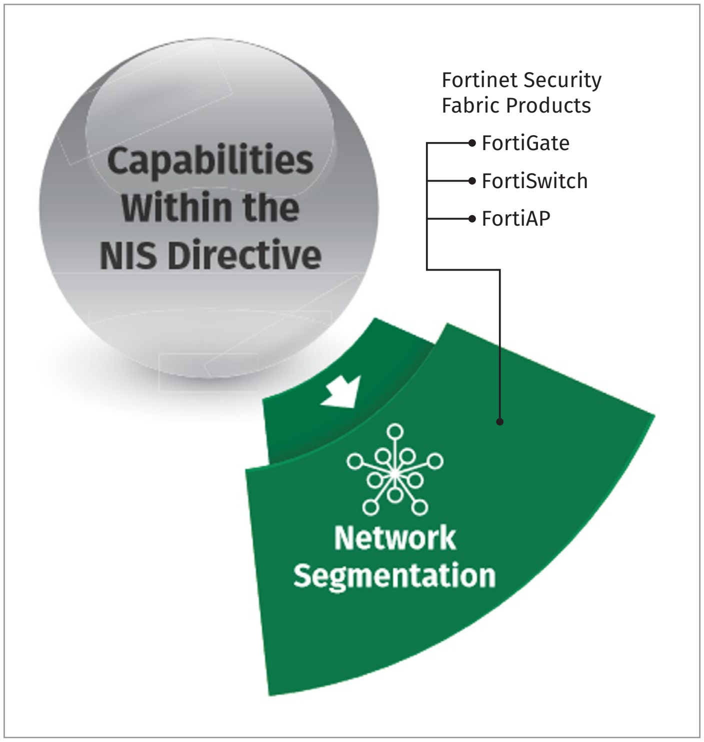
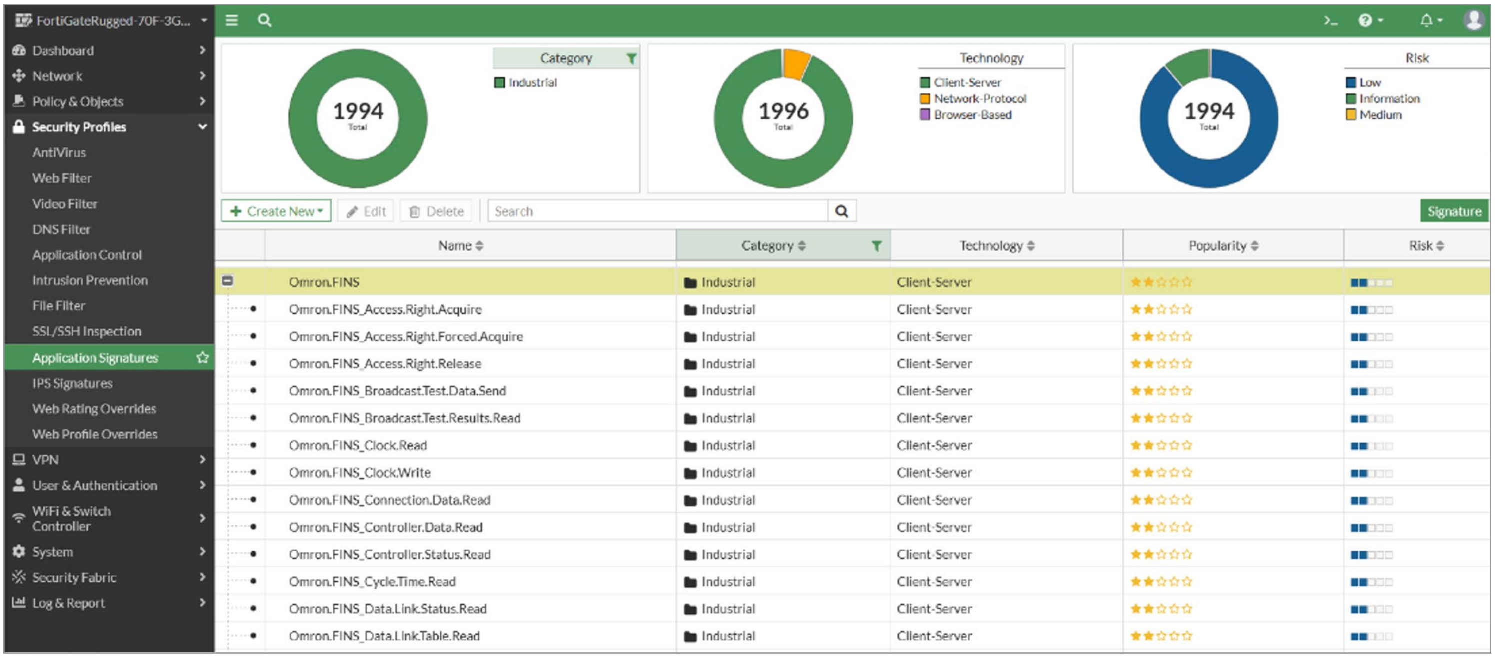

Capabilities Within the NIS Directive
Fortinet Security Fabric Products
FortiGate
FortiSwitch
FortiAP
Network Segmentation

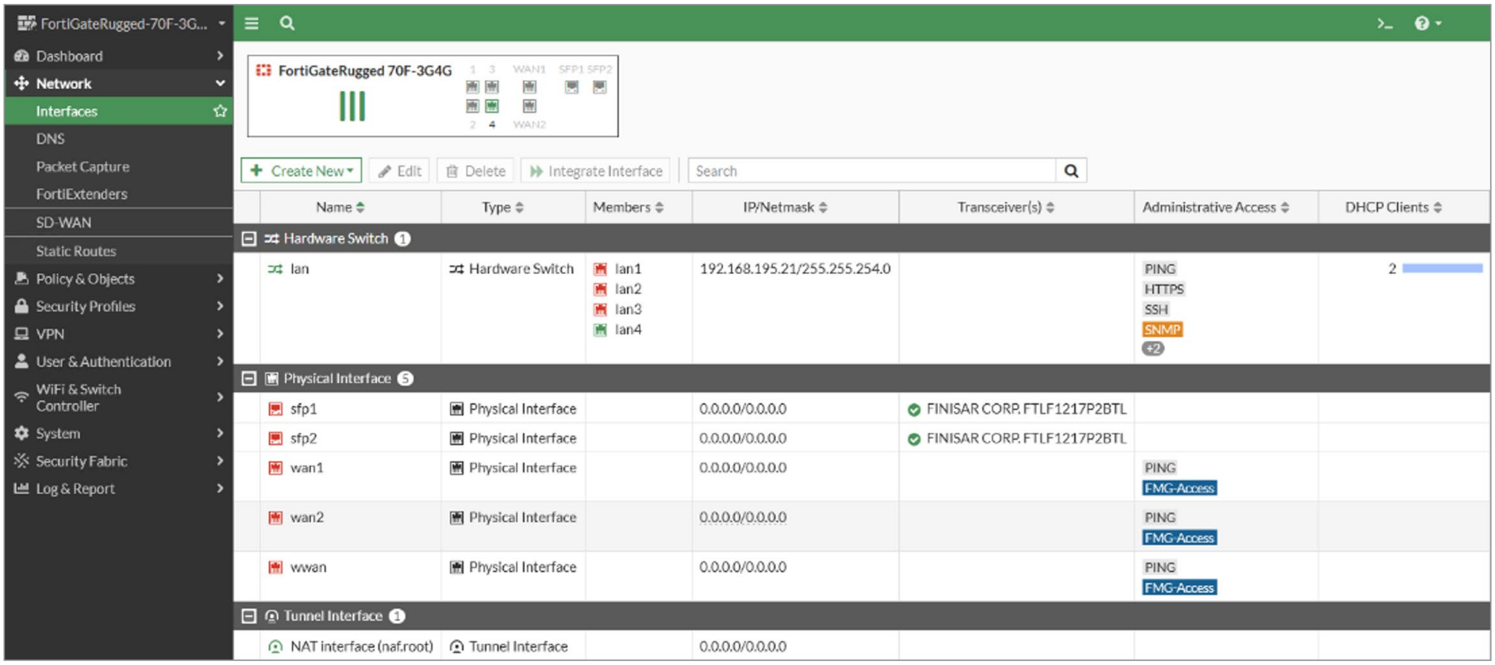
Figure 21. NIS2 Capability: Network Segmentation



Name	Category	Technology	Popularity	Risk
Omron.FINS	Industrial	Client-Server	★★☆☆☆	■■□□□
Omron.FINS_Access.Right.Acquire	Industrial	Client-Server	★★☆☆☆	■■□□□
Omron.FINS_Access.Right.Forced.Acquire	Industrial	Client-Server	★★☆☆☆	■■□□□
Omron.FINS_Access.Right.Release	Industrial	Client-Server	★★☆☆☆	■■□□□
Omron.FINS_Broadcast.Test.Data.Send	Industrial	Client-Server	★★☆☆☆	■■□□□
Omron.FINS_Broadcast.Test.Results.Read	Industrial	Client-Server	★★☆☆☆	■■□□□
Omron.FINS_Clock.Read	Industrial	Client-Server	★★☆☆☆	■■□□□
Omron.FINS_Clock.Write	Industrial	Client-Server	★★☆☆☆	■■□□□
Omron.FINS_Connection.Data.Read	Industrial	Client-Server	★★☆☆☆	■■□□□
Omron.FINS_Controller.Data.Read	Industrial	Client-Server	★★☆☆☆	■■□□□
Omron.FINS_Controller.Status.Read	Industrial	Client-Server	★★☆☆☆	■■□□□
Omron.FINS_Cycle.Time.Read	Industrial	Client-Server	★★☆☆☆	■■□□□
Omron.FINS_Data.Link.Status.Read	Industrial	Client-Server	★★☆☆☆	■■□□□
Omron.FINS_Data.Link.Table.Read	Industrial	Client-Server	★★☆☆☆	■■□□□

Figure 22. FortiGate Rugged 70F View of Supported Industrial Protocols

FortiGate also provides policy enablement, which can establish rules for network segmentation and also provide a system for controlled access to data within the ICS DMZ or the different process subnets where segmentation has been applied, as highlighted in Figure 23.



Name	Type	Members	IP/Netmask	Transceiver(s)	Administrative Access	DHCP Clients
Hardware Switch 1						
lan	Hardware Switch	lan1 lan2 lan3 lan4	192.168.195.21/255.255.254.0		PING HTTPS SSH SNMP +2	2
Physical Interface 5						
sfp1	Physical Interface		0.0.0.0/0.0.0.0	✓ FINISAR CORP. FTLF1217P2BTL		
sfp2	Physical Interface		0.0.0.0/0.0.0.0	✓ FINISAR CORP. FTLF1217P2BTL		
wan1	Physical Interface		0.0.0.0/0.0.0.0		PING FMG-Access	
wan2	Physical Interface		0.0.0.0/0.0.0.0		PING FMG-Access	
wwan	Physical Interface		0.0.0.0/0.0.0.0		PING FMG-Access	
Tunnel Interface 1						
NAT interface (naf.root)	Tunnel Interface		0.0.0.0/0.0.0.0			

Figure 23. FortiGate Interface View

Any NIS2 program should invest in strong boundaries between IT and OT environments based on the associated risks of traffic traversing corporate networks and into the more sensitive ICS operations. It should also address the internal network segmentation based on asset criticality derived from the same risk management. Evidence of firewall rules will therefore be critical for testing and auditing of security measurements [§I A18 2.f] in any NIS2-based program.

There are many possible instances where ICS information may be required to leave the higher-trust zone. That data can be placed in the DMZ through the policy rules described in this paper, where access controls into the DMZ can be logged and monitored. The DMZ should be leveraged to control how information is sent to enterprise systems, as described in the ICS410 Reference Architecture. By implementing strong firewall controls aligned with an ICS-specific architecture, entities can help prevent security events and gather data to boost cyber-risk management and incident response capabilities aligned to NIS2.

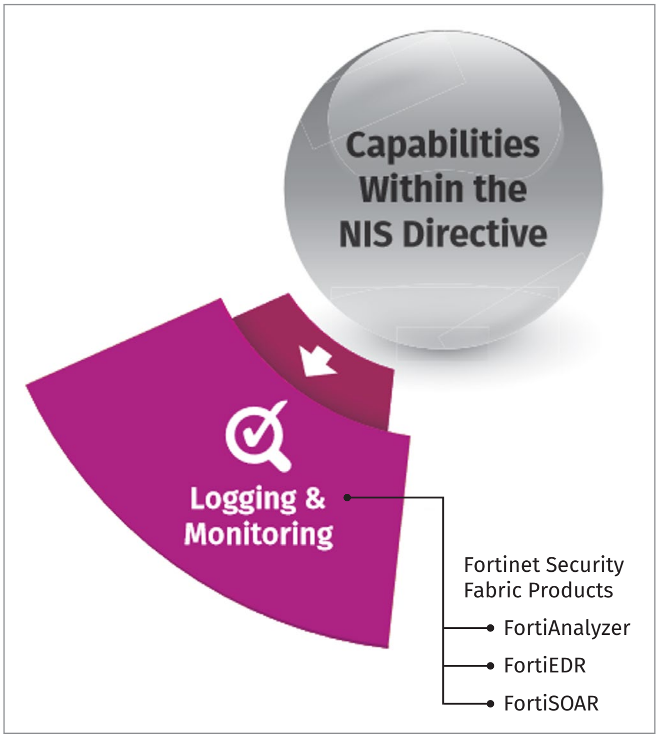

Capabilities Within the NIS Directive
Logging & Monitoring
Fortinet Security Fabric Products
FortiAnalyzer
FortiEDR
FortiSOAR

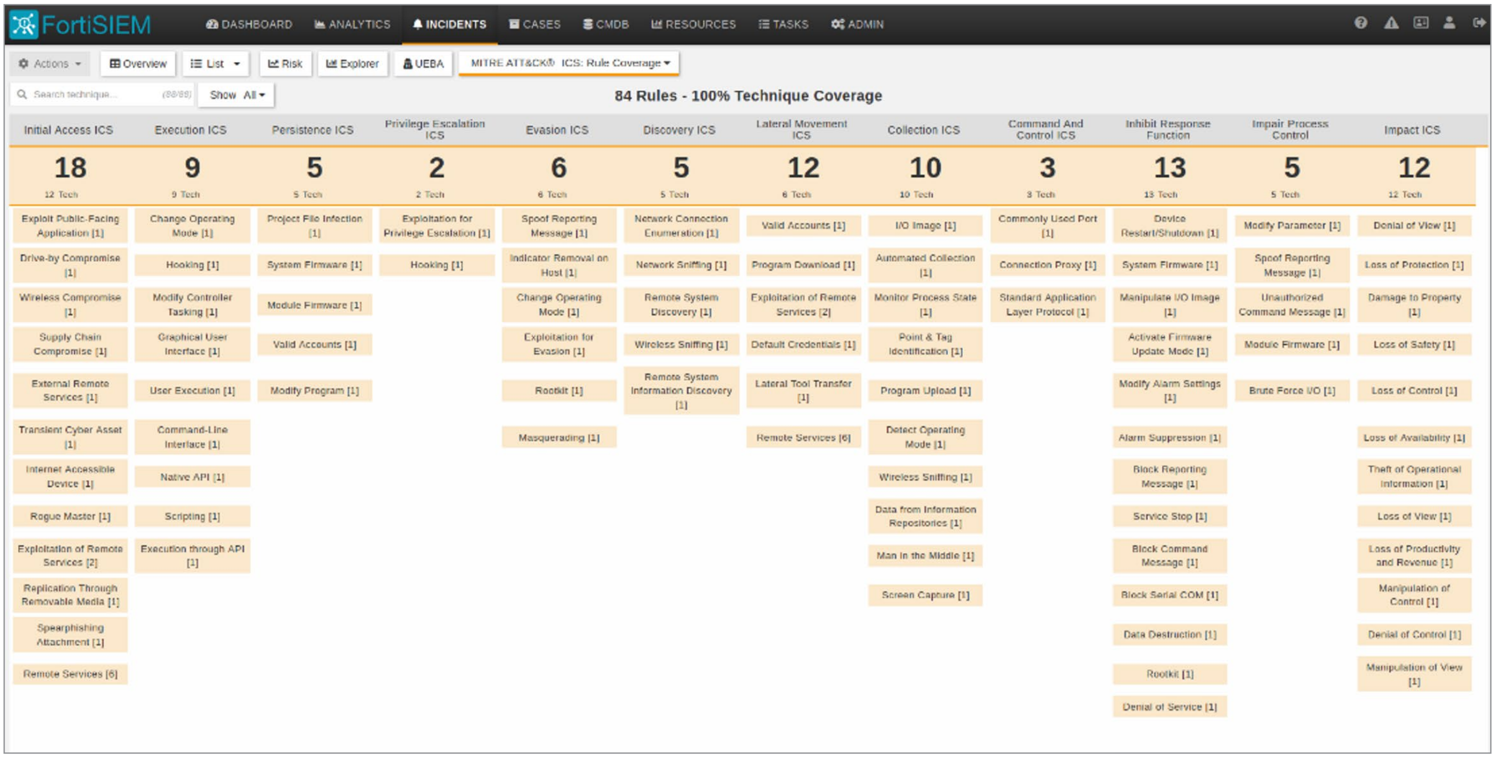
Figure 24. NIS2 Capability: Logging and Monitoring

Logging and Monitoring

Fortinet Security Fabric elements align with preventative security controls within NIS2. They also support data logging of information to help incident responders understand the root cause of a cyber event, which, in turn, translates to improved containment and eradication of the threat, leading to quicker recovery (see Figure 24).

One gray area within OT/ICS environments involves endpoint detection and response (EDR) capabilities. Unlike implementation of EDR on traditional IT networks, such implementation on control system assets can have unintended operational risks. False positives within EDRs that are set to prevention mode may disable or delete legitimate programs required during safety or reliability events. FortiEDR takes this into consideration by allowing a detection-only mode that can flag specific issues but will not proactively shut down a service that is running on the asset. With adequate testing in OT/ICS environments, this can provide better data for post-event analysis and forensics.

EDR, however, can provide only partial visibility into a potential incident. It is critical for industrial organizations to gain as much visibility across their OT environments as possible to drive quicker and more complete incident response capabilities. Centralizing logs for trends, analysis, and reporting provides additional benefits to build a single-pane-of-glass approach to reviewing incident data. Utilizing the Fortinet Security Fabric, operators and incident responders can link access logs, device information, and network traffic to provide a complete picture during post-incident forensics. FortiSIEM, the hub for this information, can provide insights based on this information, as seen in Figure 25 on the next page. This will be an invaluable set of data for the mandatory NIS2 reporting requirements.

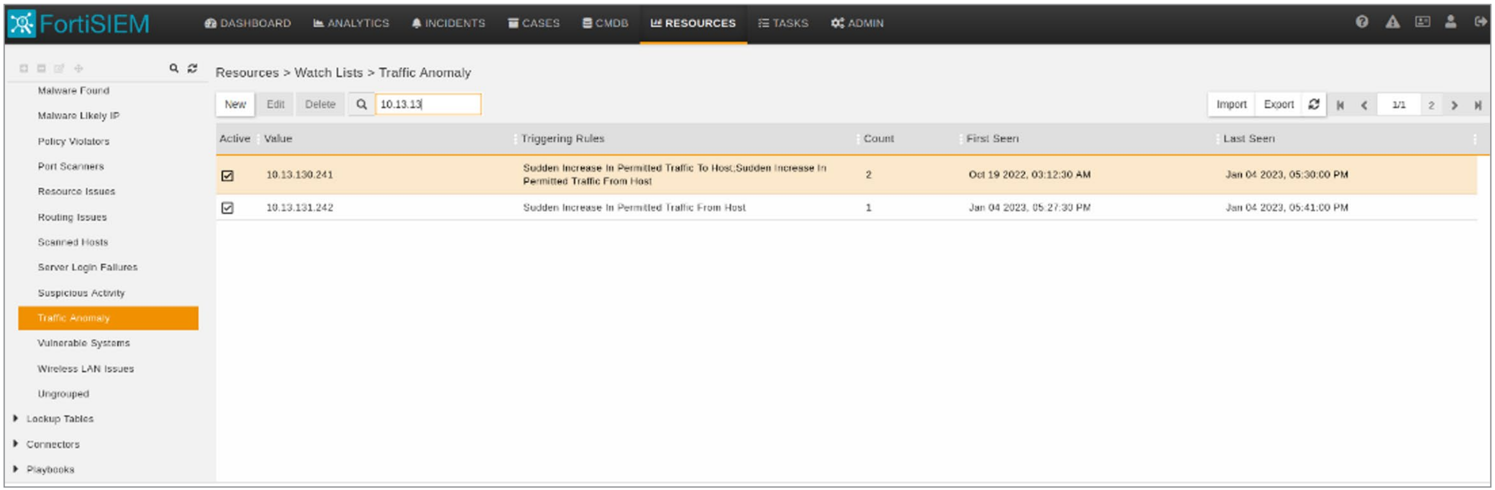


84 Rules - 100% Technique Coverage

Initial Access ICS	Execution ICS	Persistence ICS	Privilege Escalation ICS	Evasion ICS	Discovery ICS	Lateral Movement ICS	Collection ICS	Command And Control ICS	Inhibit Response Function	Impair Process Control	Impact ICS
18	9	5	2	6	5	12	10	3	13	5	12
12 Tech	9 Tech	5 Tech	2 Tech	6 Tech	5 Tech	6 Tech	10 Tech	3 Tech	13 Tech	5 Tech	12 Tech
Exploit Public-Facing Application [1]	Change Operating Mode [1]	Project File Infection [1]	Exploitation for Privilege Escalation [1]	Spoof Reporting Message [1]	Network Connection Enumeration [1]	Valid Accounts [1]	I/O Image [1]	Commonly Used Port [1]	Device Restart/Shutdown [1]	Modify Parameter [1]	Denial of View [1]
Drive-by Compromise [1]	Hooking [1]	System Firmware [1]	Hooking [1]	Indicator Removal on Host [1]	Network Sniffing [1]	Program Download [1]	Automated Collection [1]	Connection Proxy [1]	System Firmware [1]	Spoof Reporting Message [1]	Loss of Protection [1]
Wireless Compromise [1]	Modify Controller Tasking [1]	Module Firmware [1]		Change Operating Mode [1]	Remote System Discovery [1]	Exploitation of Remote Services [2]	Monitor Process State [1]	Standard Application Layer Protocol [1]	Manipulate I/O Image [1]	Unauthorized Command Message [1]	Damage to Property [1]
Supply Chain Compromise [1]	Graphical User Interface [1]	Valid Accounts [1]		Exploitation for Evasion [1]	Wireless Sniffing [1]	Default Credentials [1]	Point & Tag Identification [1]		Activate Firmware Update Mode [1]	Module Firmware [1]	Loss of Safety [1]
External Remote Services [1]	User Execution [1]	Modify Program [1]		Rootkit [1]	Remote System Information Discovery [1]	Lateral Tool Transfer [1]	Program Upload [1]		Modify Alarm Settings [1]	Brute Force I/O [1]	Loss of Control [1]
Transient Cyber Asset [1]	Command-Line Interface [1]			Masquerading [1]		Remote Services [6]	Detect Operating Mode [1]		Alarm Suppression [1]		Loss of Availability [1]
Internet Accessible Device [1]	Native API [1]						Wireless Sniffing [1]		Block Reporting Message [1]		Theft of Operational Information [1]
Rogue Master [1]	Scripting [1]						Data from Information Repositories [1]		Service Stop [1]		Loss of View [1]
Exploitation of Remote Services [2]	Execution through API [1]						Man in the Middle [1]		Block Command Message [1]		Loss of Productivity and Revenue [1]
Replication Through Removable Media [1]							Screen Capture [1]		Block Serial COM [1]		Manipulation of Control [1]
Spearphishing Attachment [1]									Data Destruction [1]		Denial of Control [1]
Remote Services [6]									Rootkit [1]		Manipulation of View [1]
									Denial of Service [1]		

Figure 25. FortiSIEM MITRE ATT&CK for ICS View

Because FortiSIEM has access to additional elements of the Fortinet Security Fabric, other capabilities can provide insight into access control and device data. For example, the CMDB application can tailor watch lists for certain event types, which may have specific risks associated with Level 2 and Level 3 devices within the ICS network (as seen in Figure 26) and even inherit discovered assets by third-party tools. Customizing alerts, watch lists, and analytics to the specific entity environment can further aid incident response teams monitoring ICS networks.



Resources > Watch Lists > Traffic Anomaly

10.13.13

Active	Value	Triggering Rules	Count	First Seen	Last Seen
☑	10.13.130.241	Sudden Increase In Permitted Traffic To Host,Sudden Increase In Permitted Traffic From Host	2	Oct 19 2022, 03:12:30 AM	Jan 04 2023, 05:30:00 PM
☑	10.13.131.242	Sudden Increase In Permitted Traffic From Host	1	Jan 04 2023, 05:27:30 PM	Jan 04 2023, 05:41:00 PM

Figure 26. Example FortiSIEM Watch List Showing Traffic Anomaly

NIS2 provides specific guidance on incident response and working with member-state CSIRTs. When coordinating with CSIRTs for reporting purposes, it will be beneficial to leverage centralized data repositories for ICS networks where possible. To do this, entities must be clear about their technology options for ingesting logs (syslog, Windows WMI, or various locally installed agents). While the FortiSIEM instance that we tested had capabilities for both Linux variants and Windows, individual usage requirements for individual control systems should also be tested, especially if an agent is required for resource-constrained devices.

While SIEMs are foundational for aggregating data, NIS2's focus on incident response may lead industrial organizations to explore security orchestration, automation, and response (SOAR) technology for their ICS networks. Tying FortiSIEM to FortiSOAR for OT can offer some additional capabilities for incident response teams, including coordinating across multiple technologies and datasets of OT-specific information, automating various detection workflows, and aiding in establishing playbooks for response and recovery.

Risk Analysis

Risk assessments (see Figure 27) need to include consideration of how ICSes can be manipulated and what the physical, environmental, and financial impacts will be. That information can lead to better determination of critical assets and systems as well as prioritization of security controls to mitigate potential risks or known vulnerabilities.

Robust risk management requires addressing the effectiveness of technical controls. FortiAnalyzer and FortiManager help to overcome the traditional checklist approach by providing visibility into all devices and connections, monitoring rules management, and detecting where rules have not been properly added or updated according to policies. (Virtual patching for industrial networks might gain importance as disclosed vulnerabilities grow and patching capabilities remain low.) Another example is to detect VPNs connected to third parties that are no longer working with the organization.

Asset Management
Risk Assessment
Capabilities Within the NIS Directive

Figure 27. NIS2 Capability: Risk Assessment

Risk analysis should consider all the information pulled from the Fortinet Security Fabric, including asset inventories, communication paths, and network segmentation. However, external data can also be invaluable for evaluating risks to OT. For example, an entity could use FortiRecon to examine which OT assets, if any, are exposed to the internet directly. This exposure would be a misconfiguration and should be a violation of any NIS2 security measure. By utilizing FortiRecon as a sanity check against erroneously connected devices, an entity could proactively decrease its overall cyber risk by disconnecting the asset or providing a dedicated remote access solution aligned with its level of risk.

Bringing It All Together: FortiManager

At the center of all this information, FortiManager (seen in Figure 28) provides a single-pane-of-glass dashboard for accessing data across NIS2 considerations outlined in this paper.

By leveraging Fortinet across multiple sites (including corporate networks) and using information-gathering tools in a properly architected ICS DMZ, entities can pull insights from multiple facilities. These insights could not only be helpful during incident response, but also highlight trends across assets, users, and networks. FortiManager also supports a closed network deployment option to help with publishing critical updates to Fortinet devices in an isolated industrial network without internet connectivity.

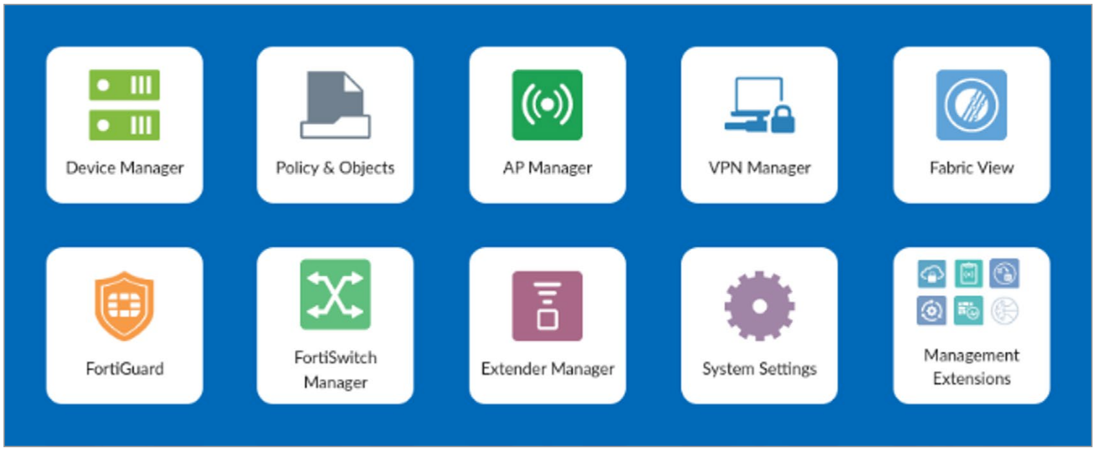
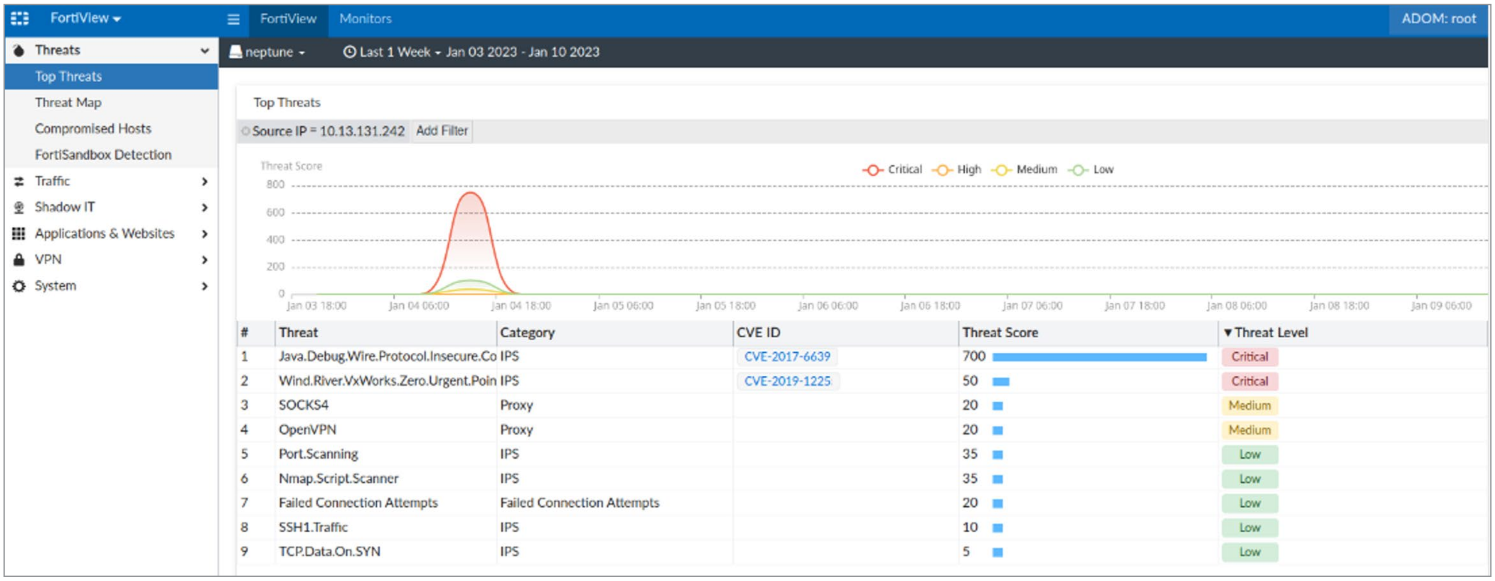


Figure 28. FortiManager main screen highlights aspects of the Fortinet Security Fabric.

When analyzing which aspects of the Fortinet Security Fabric would be helpful for a specific entity environment, operators should consider what information will be useful for reliable operations (similar to the dashboards provided in FortiView in Figure 29).



#	Threat	Category	CVE ID	Threat Score	▾Threat Level
1	Java.Debug.Wire.Protocol.Insecure.Co	IPS	CVE-2017-6639	700	Critical
2	Wind.River.VxWorks.Zero.Urgent.Poin	IPS	CVE-2019-1225	50	Critical
3	SOCKS4	Proxy		20	Medium
4	OpenVPN	Proxy		20	Medium
5	Port.Scanning	IPS		35	Low
6	Nmap.Script.Scanner	IPS		35	Low
7	Failed Connection Attempts	Failed Connection Attempts		20	Low
8	SSH1.Traffic	IPS		10	Low
9	TCP.Data.On.SYN	IPS		5	Low

Figure 29. Example FortiSIEM Watch List Showing Traffic Anomaly

New technology often requires additional training and resources, and it can easily overwhelm security analysts. Moreover, some views and insights will be considered valuable for some subject-matter experts but may not be used by others. Flexibility is important when determining technology requirements across industrial security programs, including the NIS2 Directive.

Summary: Using Compliance to Improve OT Security

NIS2 represents improvement from the original NIS Directive, in terms of both scope and organizational impact. By focusing on specific sectors as well as medium and large entities, NIS2 shifts the discussion toward organizations that have substantial societal impact if they are unavailable or compromised due to a cyberattack. These organizations rely on ICS and OT environments, making the focus of operations, physics, and engineering critical to securing those networks.

With mandatory penalties and required governance for essential and important entities, NIS2 will undoubtedly result in some growing pains for organizations that have not traditionally invested in OT security. "The SANS State of ICS/OT Cybersecurity in 2022 and Beyond" survey identified an increase in ICS/OT budgets across industries[12] and the EU's Impact Analysis for NIS2 estimates continued growth in cybersecurity investment at a rate of 22% or more.[13]

NIS2 contains programmatic elements that will improve security for many essential and important entities. Throughout this paper, we have explored an approach to design (utilizing the ICS410 Reference Architecture) and to operating the security infrastructure (by examining several products in the Fortinet Security Fabric) for ICS/OT to address NIS2.

By linking distinct capabilities to risk management and incident response, operators that embrace NIS2 will find themselves with a more resilient and more secure critical infrastructure. The security elements can, and should, be implemented as an ingrained element of operations.

These security capabilities, as outlined within NIS2, will leverage technologies such as the Fortinet Security Fabric, but they must also be complemented by a knowledgeable workforce and maintain repeatable processes to ensure compliance. Any process for cybersecurity within OT should include, at a minimum, testing for the specific ICS in question, which can be linked to FAT and SAT phases of the process's life cycle. Because OT devices are deterministic in nature, entities must understand the capabilities of any technology deployed in production. They must also offer training for operators to ensure effectiveness.

Some organizations will also find that integrating IT and OT security teams is easier when technologies align across the organization. This can help provide better visibility and potentially cross-training for security teams to understand OT security. By integrating common tools where possible, skills can be easily transferred across different environments and security management can be simplified, providing a greater operational benefit to the organization.

[12] Read more about the 2022 survey here: www.sans.org/white-papers/state-ics-ot-cybersecurity-2022-beyond

[13] The European Commission's "Impact assessment Proposal for directive on measures for high common level of cybersecurity across the Union" https://digital-strategy.ec.europa.eu/en/library/impact-assessment-proposal-directive-measures-high-common-level-cybersecurity-across-union

The Fortinet technologies tested in this implementation guide show how capabilities can be provided to improve both security and compliance with NIS2. Compliance with any standard should be a repeatable "sanity check" for a security program. NIS2 is no different.

Compliance requires more than technology. An NIS2-based program requires an adequate budget, trained personnel, and sustainable processes. The right technology, however, should enable robust compliance management. FortiManager, as an example, provides a link between the multiple capabilities required within a security program and can help operators across complex facilities and environments—regardless of the OES industry. By using additional features of the Fortinet Security Fabric, supported by knowledgeable teams of industrial defenders, operators should be able to improve both cyber-risk management and incident response capabilities.

Sponsor

SANS would like to thank this paper's sponsor:

FORTINET®