EBOOK

Regulating Utilities:

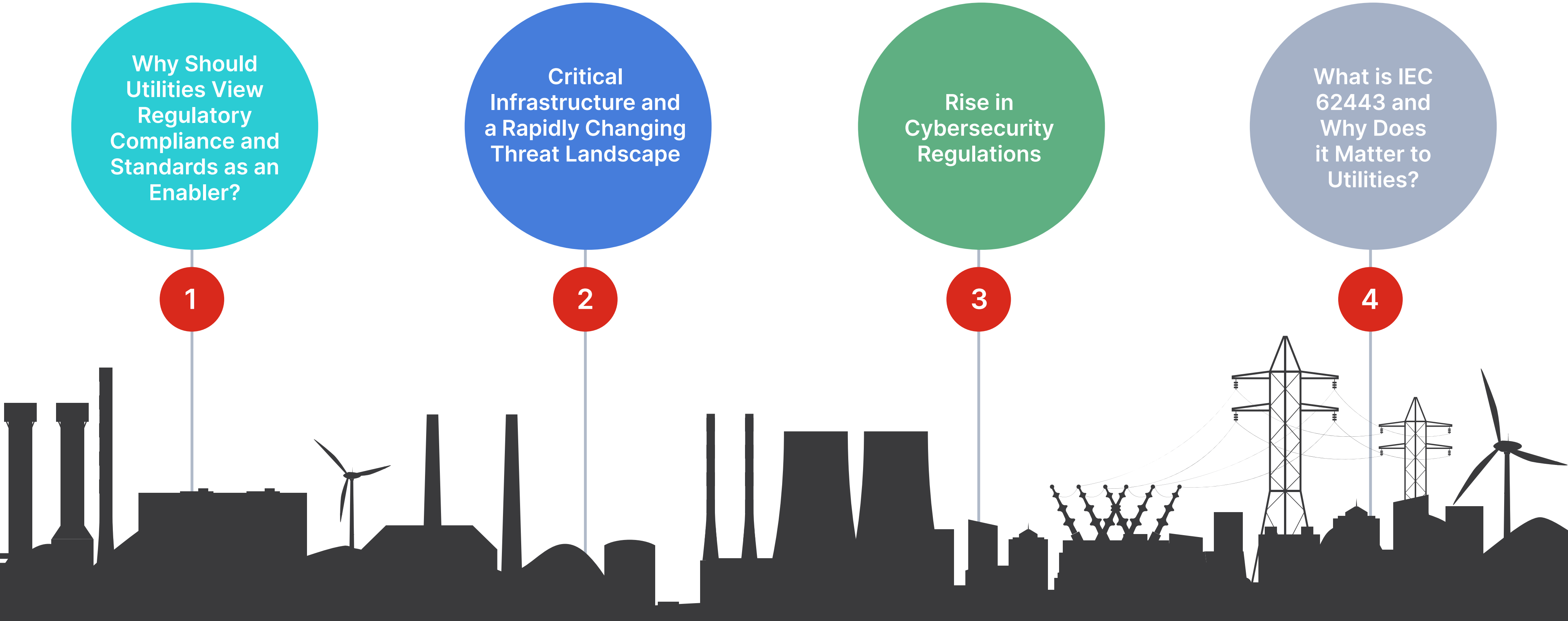
How-to guide for staying compliant

Introduction

The Network and Information Security 2 (NIS2) directive was approved by the European Union (EU) Council in Nov 2022. The directive gives EU member states until October 2024 to transpose NIS2 into national law to ensur its critical infrastructure sector's compliance. However, reaching cybersecurity compliance for utilities warrant a long cybersecurity program that will require an early start.

Alongside NIS2, utilities can also use the IEC 62443 and ISO 27001 standards that are focused on operational technology (OT) and information technology (IT) cybersecurity. It will be an opportunity for utilities—such as power, water, and gas distribution—to get ahead of the NIS2 directive, which imposes stricter risk management, incident response, and incident reporting obligations on operators of essential services than its predecessor, the NIS.

The directive encourages a proactive response to a dynamic threat environment and considers the increased need for threat information sharing.



1. Why Should Utilities View Regulatory Compliance and Standards as an Enabler?
2. Critical Infrastructure and a Rapidly Changing Threat Landscape
3. Rise in Cybersecurity Regulations
4. What is IEC 62443 and Why Does it Matter to Utilities?

"The average cost of a **ransomware attack in 2022 was $4.54 million,** according to an IBM study."

1

Why Should Utilities View Regulatory Compliance and Standards as an Enabler?

Utilities are an attractive target for state-sponsored threat actors and ransomware gangs for two reasons. First, attacks on utilities affect a lot of households and businesses; and second, disrupting operations carries the additional threat of causing physical harm to people and the environment.

The energy sector faces additional cyber risks due to highly interconnected energy grids and gas pipelines across Europe, difficulties implementing real-time cybersecurity capabilities, and the co-existence of decades-old OT with cutting-edge technology, such as Internet of Things (IoT) devices. The European Commission in 2019 recommended the sector use the latest industry standards to address real-time requirements, cascading effects, and legacy and state-of-the-art technology.[1]

Cybersecurity can be viewed as a cost of doing business, but having a strong security posture improves resilience, agility, and responsiveness to a rapidly changing threat landscape. For utilities, it enables a swifter incident response and streamlined reporting under NIS2. But it also requires a holistic approach to cybersecurity spanning IT and OT environments.

The estimated cost of responding to ransomware attacks is trending upwards and includes lost income due to business disruption, legal fees, incident response, monitoring, malware discovery and removal, data restoration, hiring external security experts, and more. The double-extortion phenomenon, where attackers may leak stolen data, creates additional risks to reputation.

The average cost of a ransomware attack in 2022 was $4.54 million, according to an IBM study, which found it took victims an average of 277 days to identify and contain all breach types, giving attackers months to enumerate a network's critical systems, exfiltrate sensitive data, and lay the foundations for a higher impact attack.[2]

The results of ENISA's 2022 NIS Investments survey support the notion that cybersecurity is an enabler.

The European cybersecurity agency ENISA found in its NIS Investments 2022 report that ransomware was more costly than any other type of cybersecurity incident in 2021 and was also the most common attack, with 32% of organizations covered by NIS reporting at least one ransomware incident in the year. The two largest costs resulting from ransomware attacks were incident response at 33% of total direct costs, followed by disaster recovery and business continuity expenses at 22%. Other significant direct costs were loss of revenue (9%), legal costs from fees, fines and lawsuits (7%), loss of property (6%), and crisis management (4%).

While the pace of cyberattacks is unlikely to slow in the future, the results of ENISA's survey suggest that investing in cybersecurity does improve responsiveness and reporting capabilities.[3] Over a fifth of respondents (21%) reported that implementing NIS programs helped in the recovery from cybersecurity incidents, while 62% said it helped detect cybersecurity incidents. A further 11% found support from the national cyber security incident response team (CSIRT) helpful when faced with an incident.

But many of Europe's critical infrastructure operators are only at the beginning of the journey to implement robust cybersecurity defenses and threat intelligence.

The security operations center (SOC) is the heart of an organization's threat intelligence, incident response, threat hunting, and data forensic capabilities. However, ENISA found that over a third (37%) of operators of essential services (OESs) and digital service providers (DSPs) did not operate a SOC in 2021.

Despite the importance of an SOC to cybersecurity capabilities, ENISA found that many organizations in water (59%), energy (28%), and transport (28%) lacked any form of SOC, be it in-house or operated by a third-party. In addition, 32% of energy operators did not monitor a single OT process through a SOC.

Despite a strong relationship between vulnerabilities and data compromises, patching remains slow in many sectors. Most OESs and DSPs (69%) reported that the majority of their cybersecurity incidents were caused by attackers exploiting unpatched vulnerabilities. Yet, ENISA found that 53% of organizations had a "rigid patching policy" that only covered 20% of their assets, while 13.5% had no visibility over the patching of 40% or more of their information assets.

While 63% of banking entities patched systems within a month, only 23% of drinking water entities patched systems this quickly. In energy, financial market infrastructure, healthcare, and transport, no more than 42% of systems were patched within a month, with the majority in each sector taking one to six months to resolve.

These figures illustrate why investing in cybersecurity is a cost but also an enabler, helping organizations achieve compliance, while improving responsiveness to an ever-changing threat landscape.

2

Critical Infrastructure and a Rapidly Changing Threat Landscape

While threat actors’ tactics don’t change much over time, the threat landscape does. An attack on utilities can start with a spearphishing email that compromises credentials for the corporate virtual private network (VPN), email server, or other business system. Attackers often then move laterally within an IT network and may, in the case of utilities, cross the IT-OT boundary to compromise or disable Control Systems.

Accelerating digital transformation among Europe’s leading utilities has also created a greater need for a strong cybersecurity posture as more enterprises deploy IoT technology to monitor, and sometimes remotely control, industrial systems.

In March 2023, ENISA forecast that within a decade IoT will permeate “large parts of transport, power and water grids, and industrial infrastructure to increase efficiency and improve intelligent decision-making”. It predicts the ongoing skill shortage will “lead to a lack of knowledge, training, and understanding of the cyber-physical ecosystem by 2030, leading to IT and OT security maintenance issues arising from the misconfiguration, delayed maintenance, and inadequate end-of-life support of discontinued IoT software.”[4]

In March 2023, ENISA forecast that within a decade **IoT will permeate “large parts of transport, power and water grids, and industrial infrastructure to increase efficiency and improve intelligent decision-making”.**

Critical Infrastructure and a Rapidly Changing Threat Landscape

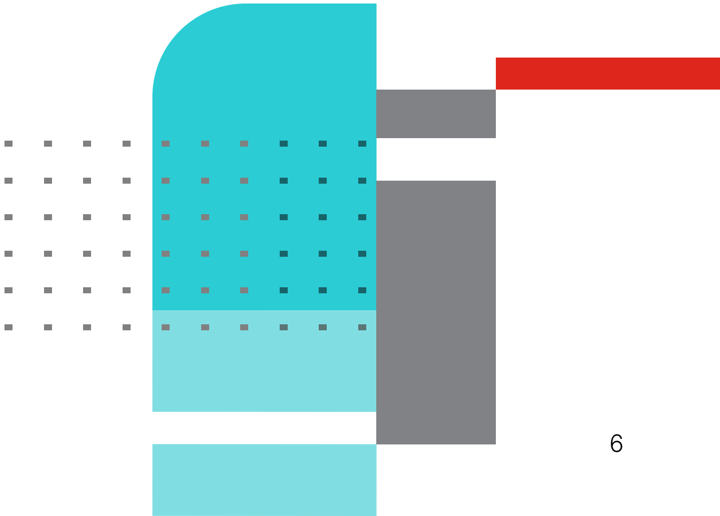
While NIS2 and international cybersecurity frameworks do support the need for utilities to secure their IT/OT environments, they have developed alongside an increasing awareness that cyberattacks on critical infrastructure are not the stuff of fiction, but a real threat to replace with critical infrastructure globally:

- A cyberattack on German wind farm operator Deutsche Windtechnik in April 2022 disabled remote data monitoring connections to its wind turbines for days.[5]
- In February 2022, the day Russia invaded Ukraine, US satellite communications provider Viasat's KA-SAT modems were hit by modem-wiping malware that caused widespread internet connectivity issues for residents and businesses in Central and Eastern Europe.[6]
- The Viasat disruption disabled 5,800 wind turbines in Central Europe after knocking out remote monitoring and control capabilities.[7]
- Large German municipal energy provider Enercity suffered a cyberattack on its IT systems in October 2022 but reassured customers its OT systems were not affected.[8]
- Italian oil and gas services firm Saipem was infected in December 2018 by a variant of the destructive Shamoon malware, disabling hundreds of computers in its Middle East, India, and UK locations.[9]
- Physical attacks on network cables are growing concern. In October 2022, German rail operator Deutsche Bahn suffered a three-hour disruption after saboteurs cut fibre optic cables that disabled its digital train radio communications system.[10]
- In the same month, attackers cut a major telecommunications cable in south of France disrupting connectivity to Asia, Europe, and the US.[11] This followed an act of sabotage on backbone network cables in Paris that disrupted fixed line and mobile internet connectivity to several other regions of France.[12]
- In August 2022, UK water supply operator South Staffordshire PLC confirmed that ransomware attackers had stolen customer data from its IT systems.[13]

Cyberattacks pose a unique challenge for entities managing integrated IT and OT environments. The W&WW sector in the EU and US share characteristics that make them more susceptible to cyberattacks.

The US W&WW sector consists of over 153,000 public drinking water systems and over 16,000 wastewater treatment systems, many of which are small with limited resources. The sector is known to allocate more resources to protecting physical infrastructure over IT and OT infrastructure, and to use outdated control system devices and firmware, according to CISA.

Following the attack on South Staffordshire PLC, an ENISA official said it deals with "thousands" of W&WW operators in the EU and that small operators often have no cybersecurity experts on staff.[14] Speedy patching is hampered by staff needing to physically install updates on OT devices in the field. The EU-wide drought has also constrained the W&WW sector's redundancy options because they lack fall-back options in the event of a cyberattack impacting OT.



Cyberattacks, in particular distributed denial of service (DDoS) attacks, against EU in critical infrastructure sectors have risen sharply since **February 2022**.

Impacts include:

- Inability of W&WW facility personnel to access SCADA system controls at any time
- Access of SCADA systems by unauthorized individuals or groups

Mitigations include:

- Require multi-factor authentication (MFA)
- Use blocklisting and allowlisting and audit these logs to identify instances of unauthorized access
- Use manual start and stop features
- Audit networks for systems using remote access services
- Introduce segmentation between IT and OT
- Implement demilitarized zones (DMZs), firewalls, jump servers, and one-way communication diodes to prevent unregulated communication between the IT and OT networks
- Use network maps
- Remove unnecessary equipment from network.

The war in Ukraine illustrates how rapidly the threat landscape can change. At the outset, CISA warned organizations to be prepared for destructive malware.[15]

Cyberattacks, in particular distributed denial of service (DDoS) attacks, against EU in critical infrastructure sectors have risen sharply since February 2022, from 45.9 attacks per month in the first half of 2022 to 117 per month in Q1 2023, according to Thales.[16]

CISA also warned on the anniversary of Russia's invasion of "disruptive and defacement attacks" on the websites of US and EU organizations aimed at sowing "chaos and social discord". DDoS attacks on European targets were dominated by pro-Russian hacktivist groups like KillNet that targeted organizations in Poland, Baltic nations, and the Nordics.

Espionage campaigns from Russian threat actors loomed large too. According to Microsoft, in the year to February 2023, the non-Ukraine sectors most targeted by Russian threat actors were government, IT/communications, think tanks and NGOs, energy, education, transportation, professional services and nuclear. Excluding Ukraine, the most targeted nations were the US, Poland, UK, Lithuania, Latvia, Norway, Romania, Denmark, France, Sweden, and Finland.

Microsoft noted that supply chain attacks abusing trusted IT sector customer relationships have affected entities in multiple critical infrastructure sectors.[17]

3

Rise in Cybersecurity Regulations

The original 2016 NIS directive established a **high common level of cybersecurity** for critical infrastructure for all Member States.

The original 2016 NIS directive established a high common level of cybersecurity for critical infrastructure for all Member States by introducing risk management and reporting obligations for OESs and digital service providers (DSPs).

Its successor, NIS2, and the EU Cybersecurity Act certification framework, have matured cybersecurity regulations befitting today's threat landscape.[18] NIS2 introduces tighter supervisory measures, stricter enforcement requirements, and harmonized sanctions across the EU with the aim of improving cyber risk management and incident response.

NIS2 also strengthens the role of the ENISA cybersecurity agency, bolsters cross-border cooperation via the Computer Security Incidents Response Teams (CSIRTs) Network, and establishes administrative fines up to €10 million or 2% of the entities' total turnover worldwide, whichever is higher.[19]

NIS2 broadens the definition of OESs by including "essential entities" (EEs) and "important entities" (IEs). Medium- and large-sized entities are subject to NIS2, which sets out "minimum rules" for sectors and their obligations.

While not prescriptive, NIS2 stipulates 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 to deliver services. Industrial control systems (ICS) and OT environments are in scope as the production centers of critical infrastructure.

The requirement to implement cybersecurity measures to a level "appropriate to the risk presented" implies that operators understand the impacts of a cyber event to finances, safety, business continuity, reputation, and the national and environmental context it operates within.

Utilities should assess the severity of impacts to each facet of the operation, which will assist with NIS2's 24-hour window for reporting a significant incident to a national CSIRT followed by an initial impact assessment within 72 hours. Entities are to submit a final report within one month of the incident.

To address NIS2 business continuity obligations, utilities should include data backups for industrial equipment, including logic for controllers, data for HMIs, and engineering workstations. EEs and IEs can address supply chain risks by vetting contracts and assurances offered by suppliers, including original equipment manufacturers (OEMs), and OT vendors and integrators.

“Member States should, where useful, **encourage the use of European and international standards and technical specifications** relevant to the security and resilience measures applicable to critical entities.”

Ideally, operators should link each supplier with risk scenarios and methodically evaluate suppliers’ end-of-life and end-of-support timelines; safeguards against counterfeit products; and supply chain assurances. Operators should also formalize vulnerability notifications and incident-related service level agreement requirements.

Other considerations for OT/ICS equipment include the testing and auditing of security measurements; identifying where to appropriately implement encryption and cryptography for ICS equipment; and establishing an industrial cyber risk management program with adequate oversight and accountability measures.

Utilities will likely be expected to address security measures beyond NIS2 by implementing frameworks like ISA/IEC 62443, the international standard for ICS.

“Member States should, where useful, encourage the use of European and international standards and technical specifications relevant to the security and resilience measures applicable to critical entities.”

Organizations can use **IEC 62443** to strengthen their protection of ICS by using it as a framework to assess and mitigate ICS security vulnerabilities.

4

What is IEC 62443 and Why Does it Matter to Utilities?

The International Electrotechnical Commission (IEC) IEC 62443 set of standards outlines requirements and processes for implementing and maintaining electronically secure industrial automation and control systems (IACS).[20]

The standard's roots trace back to the International Society of Automation (ISA)'s ISA99 standards committee, which was established in 2002 and foresaw the impact of cybersecurity threats to US critical infrastructure.

Organizations can use IEC 62443 to strengthen their protection of ICS by using it as a framework to assess and mitigate ICS security vulnerabilities.[21] A useful concept in IEC 62443 are the "security Zones" and "conduits", which allows an organization to break down monolithic ICS cybersecurity risks into more manageable components that can be measured and categorized based on individual business risk.

This makes it easier to assess the gaps between existing security controls and the standard's definition of the assigned security level, which ranges from 1 to 4. Within this framework, certain controls—like multi-factor authentication for untrusted networks or device identification and authentication—are required to meet each level.

Other standards, frameworks, and best practices include:

- NISTIR 7628
- NIST SP 800-82
- NERC CIP
- IEC 62351
- API 1164
- ISO 27019
- Network Code on Cybersecurity[22]

How Fortinet Can Help

The NIS2 directive is built around five pillars:

- Asset management
- Access control to networks and assets
- Network segmentation, protection, and response
- Events, alerts, incident detection, and reporting to the European cyber crisis liaison organization network (EU-CyCLONe)[23]
- Risk management and risk assurance: risk posture definition, risk mitigation highlights, continuous risk and brand monitoring

NIS2 provides requirements to create a cybersecurity program based on strengthening cyber risk management and cyber incident response. These define an organization's capabilities to measure its cybersecurity posture and recover from an incident by operators understanding their industrial environment, protecting their critical assets, and monitoring IT/OT networks for malicious communications.

Fortinet maintains a comprehensive portfolio of cybersecurity solutions to help customers to address all five pillars, supported by a dedicated team of Fortinet cybersecurity experts with in-depth industry expertise to guide customers through the configuration of cybersecurity solutions for IT and OT environments.

Fortinet's approach recognizes that cybersecurity is a collective effort that depends on raising the capabilities of all players. Partnering with Fortinet ultimately positions utilities to support better information sharing between national authorities and European critical infrastructure operators.

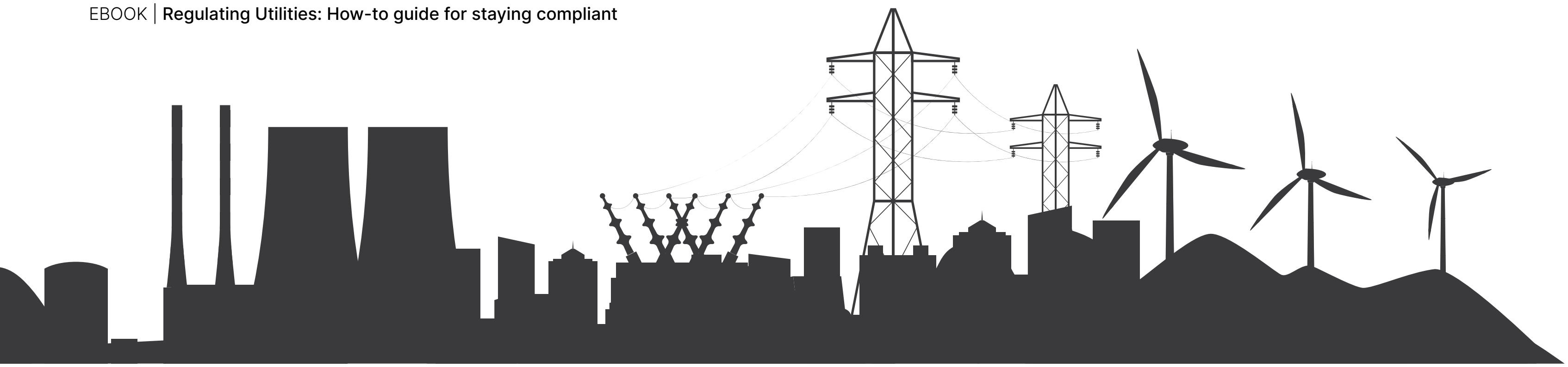
Member state CSIRTs will also collaborate with EU-CyCLONe, which is tasked with EU-wide information sharing and situational awareness in the event an attack targets multiple regions and sectors simultaneously.

Fortinet recommends that EEs and IEs focus on the following actions to support incident handling and reporting:

- Ensure technologies address all aspects of the IEC 62443 standard and provide visibility across the IT and OT networks
- 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 needing them during an incident

Contact Fortinet today to discover how we can help.

utilities@fortinet.com



REFERENCES

1. Commission Recommendation of 3.4.2019 on Cybersecurity in the Energy Sector
2. Cost of a data breach 2022: A million-dollar race to detect and respond
3. NIS Investments 2022
4. ENISA Foresight Cybersecurity Threats for 2030
5. Cyber attack on Deutsche Windtechnik
6. Viasat shares details on KA-SAT satellite service cyberattack
7. Satellite outage knocks out thousands of Enercon's wind turbines
8. Major German energy supplier hit by cyberattack
9. Saipem says Shamoon variant crippled hundreds of computers
10. Deutsche Bahn says sabotage behind massive train disruption
11. European cable cut may impact transoceanic routes
12. The Unsolved Mystery Attack on Internet Cables in Paris
13. South Staffs Water reveals data hack
14. Cyberattack Raises Pressure on European Water Providers During Drought
15. CISA Update: Destructive Malware Targeting Organizations in Ukraine
16. From Ukraine to the Whole of Europe: Cyber Conflict Reaches a Turning Point
17. A year of Russian hybrid warfare in Ukraine
18. The EU Cybersecurity Act
19. CSIRTs Network
20. ISA/IEC 62443 Series of Standards
21. Managing ICS Security with IEC 62443
22. Network Code on Cybersecurity
23. EU CyCLONe

www.fortinet.com

May 17, 2023 03:10 PM

2130261-0-0-EN