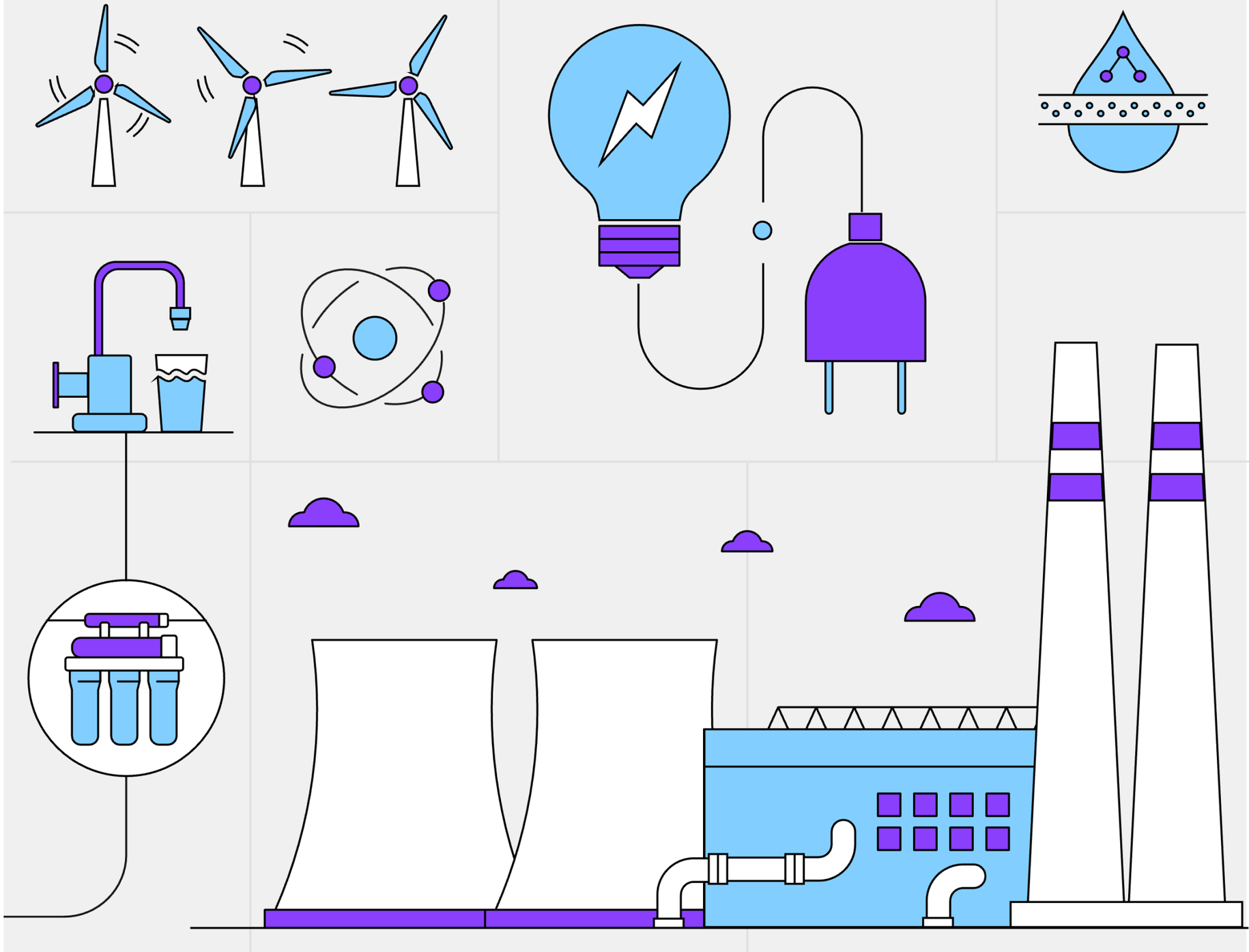
CIRED
HRVATSKI OGRANAK

NIS2 OT imperative of EES security – What is your strategy?

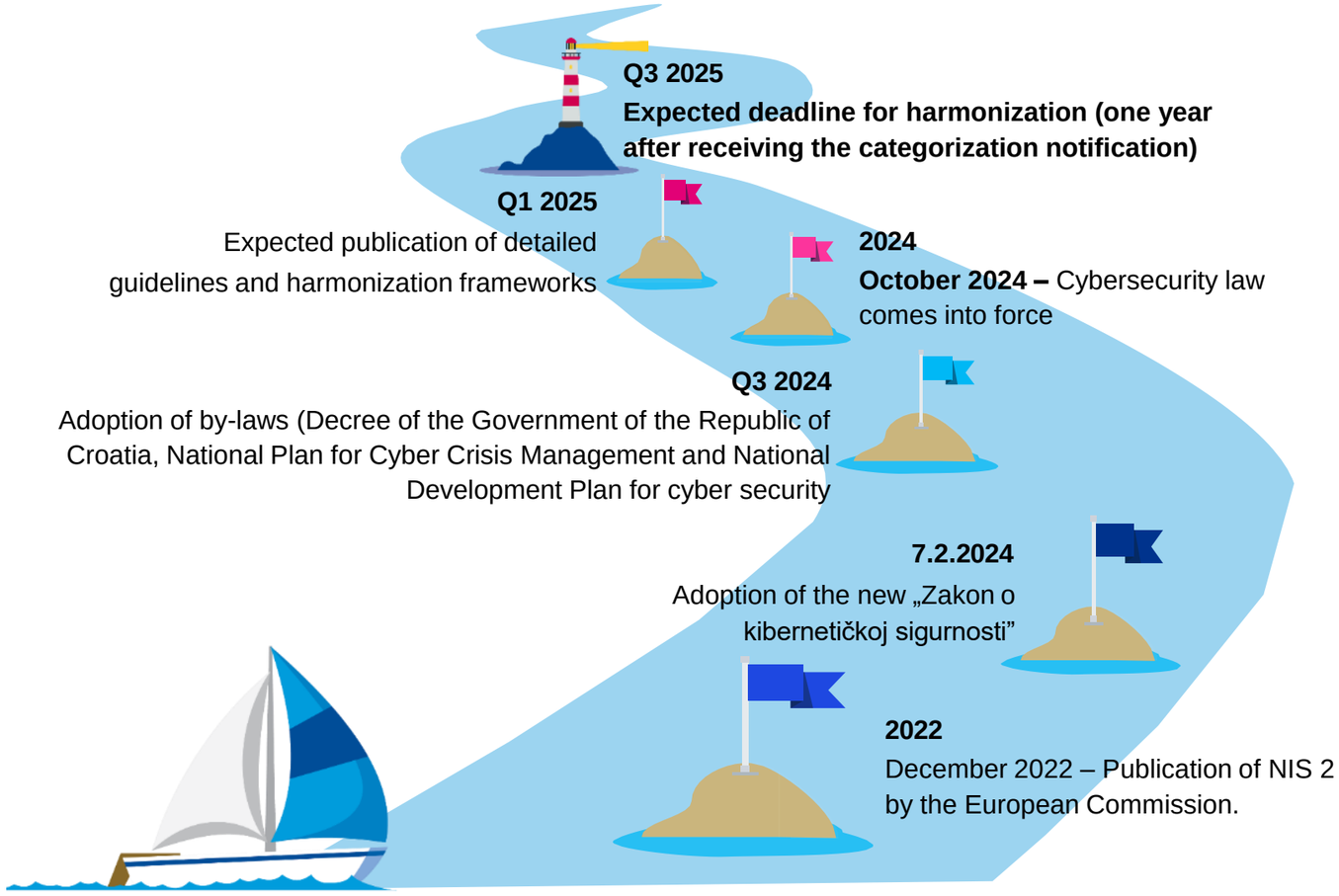


March 2024

Ivan Turčin, dipl ing. el.

IBM

DIRECTIVE (EU) 2022/2555 on measures for a high common level of cybersecurity throughout the EU (NIS 2)



Key areas that impact you

Senior Management and Executive oversight and accountability

Management bodies to approve cybersecurity risk measures taken, supervise implementation, follow specific training and be accountable for non-compliance.

- Adopt (Information and Communication technology) ICT governance and control frameworks.
- Assess the effectiveness of the risk management measures that have been undertaken.

- Requirements around disaster recovery, communications and crisis management.
- Learn and evolve both from external events as well as the entity's own ICT incidents.

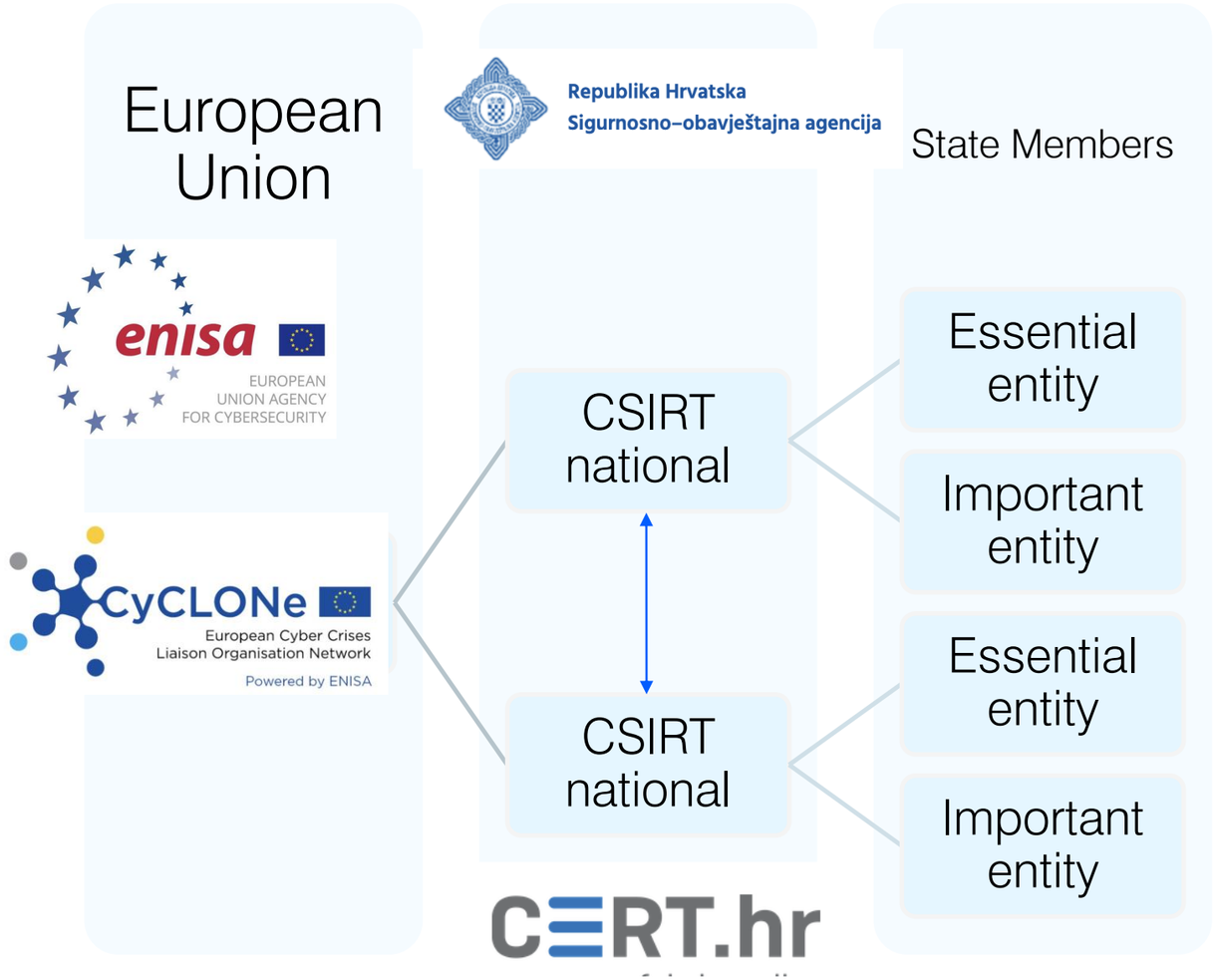
- Streamline ICT incident reporting through the logging and classification of ICT incidents.
- Multitude of reporting requirements imposed on an entity.

- Monitor third-party contractual arrangements at all stages.
- Have a strategy on ICT Third Party risk.

- Provides a list of security measures that shall be implemented.
- Regulations encourage collaboration among trusted communities of entities.

NIS2: CEOs or legal representatives can be suspended.

Organisational Structure



Power Generation Ecosystem

Brute Force Password

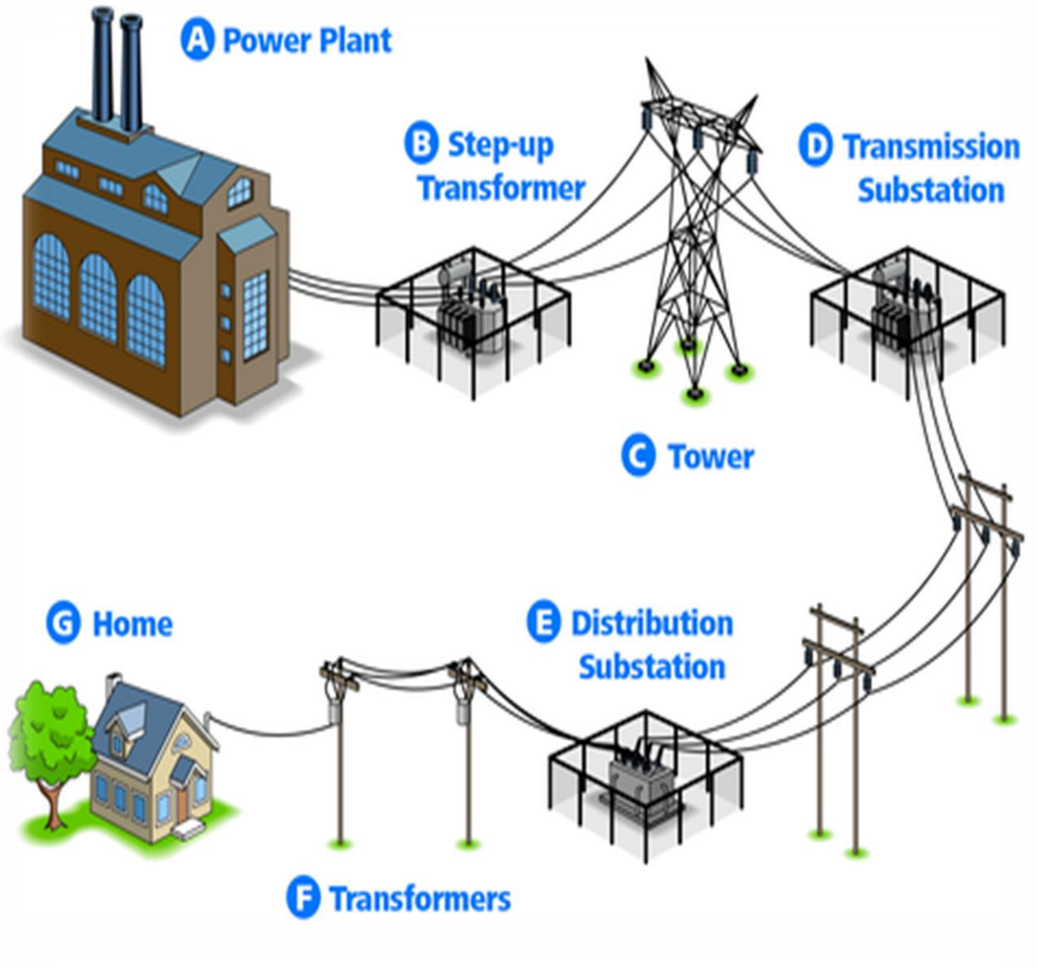
Insider

Ransomeware

Man in the Middle

DDOS

Nation Central Control



Phishing

Account take over

Malware Bomb

- Maintenance Systems
- Scheduling Systems
- Billing
- Physical Security System
- Load Balancing & Models
- Safety Systems

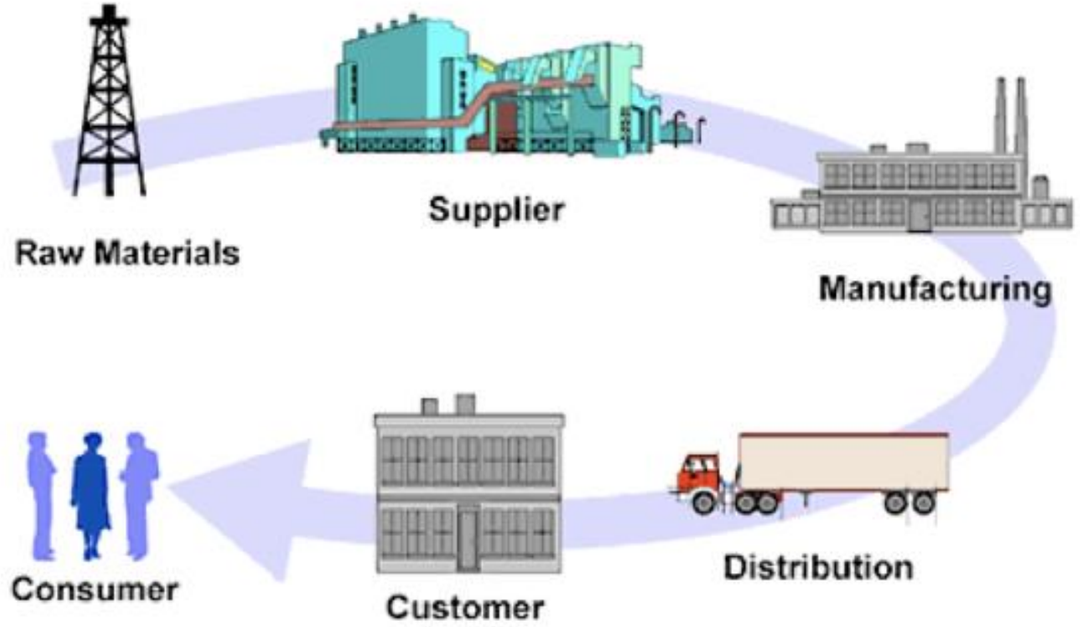
Manufacturing and Supply Chain

Brute Force Password Insider

Ransomeware

Man in the Middle

DDOS



- MES (Mauf. Execution systems)
- Quality Systems
- Supply Chain Management
- Back dock / WIP Control
- Track and Trace
- Safety Systems

Nation Central Control

Phishing

Account take over

Malware Bomb

Europe

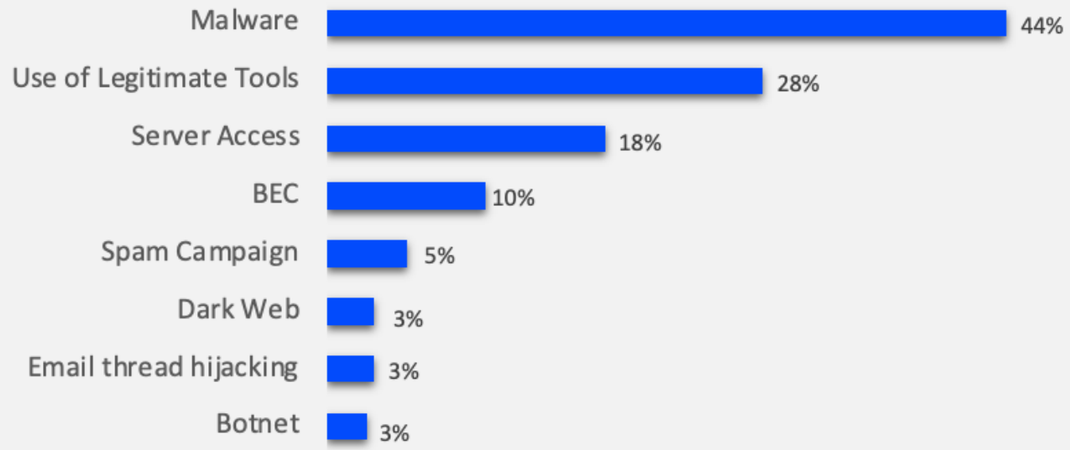
#1

Europe was the first-most attacked geography worldwide in 2023

32%

of attacks in 2023 occurred in the European region, up from 28% in 2022

Top actions on objectives in Europe
Source: IBM X-Force



Energy

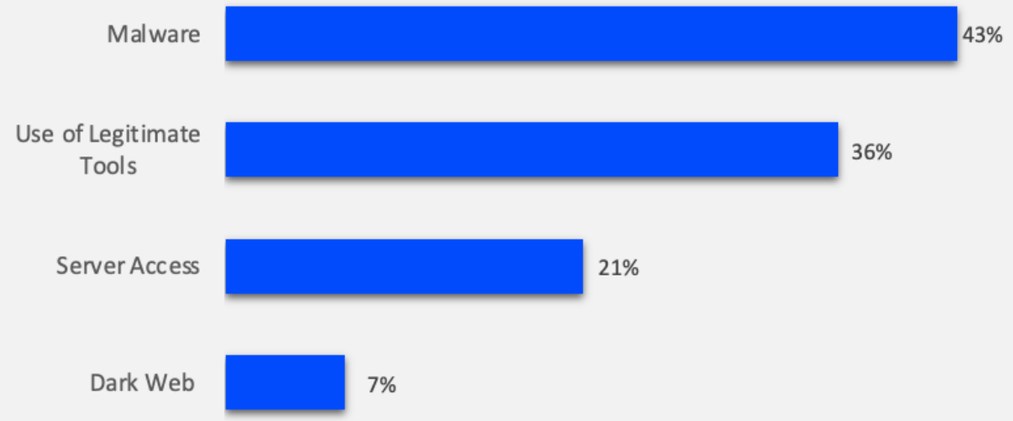
#4

Energy was the fourth-most attacked industry in 2023

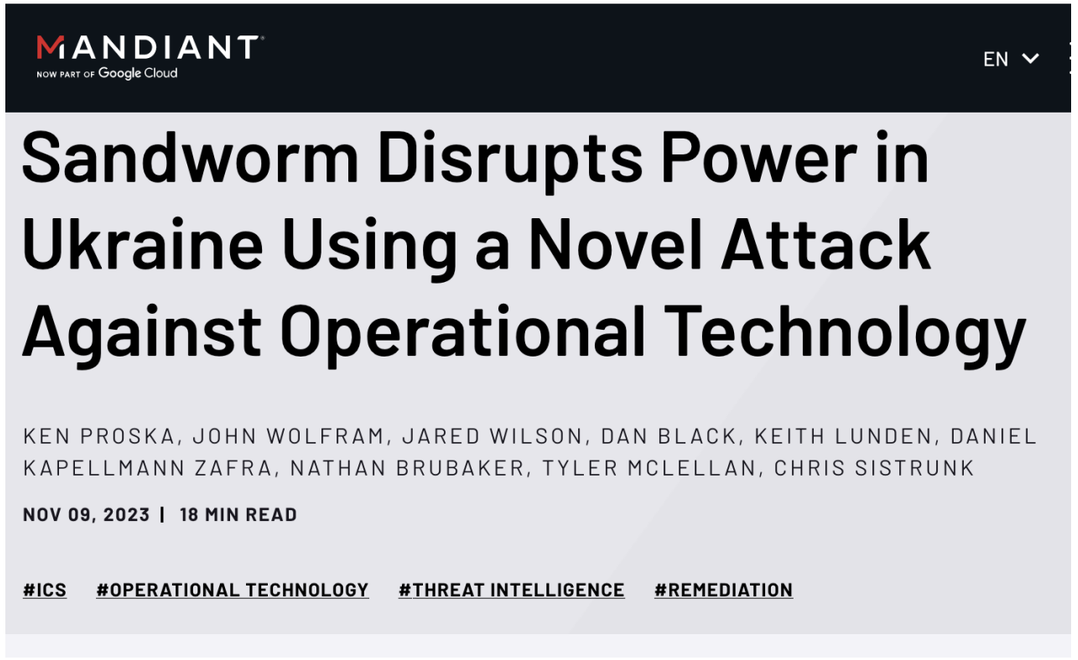
11.1%

of all attacks among the top 10 industries, up from 10.7 in 2022

Top actions on objectives in energy
Source: IBM X-Force



Recent cybersecurity incidents on E&U companies in Europe



Recent cybersecurity incidents on E&U companies

- In August 2023, the Australian utility company Energy One Limited fell victim to a cyberattack that could have had international implications, as the firm's corporate systems in the UK were also affected.[1]
- Mandiant, a part of Google, states that Russian cyber spies were behind a hack that disrupted part of Ukraine's power grid in late 2022, marking a rare and advanced form of cyber warfare.[2,3,4]

Impact of cyber-attacks on E&U companies

- Exposure of sensitive data including billing and revenue information (from smart grid and smart metering systems), control systems information, and employee and customer data.
- Production disruptions or shutdowns resulting in reputational damage.
- Penalties due to violation of regulatory requirements.

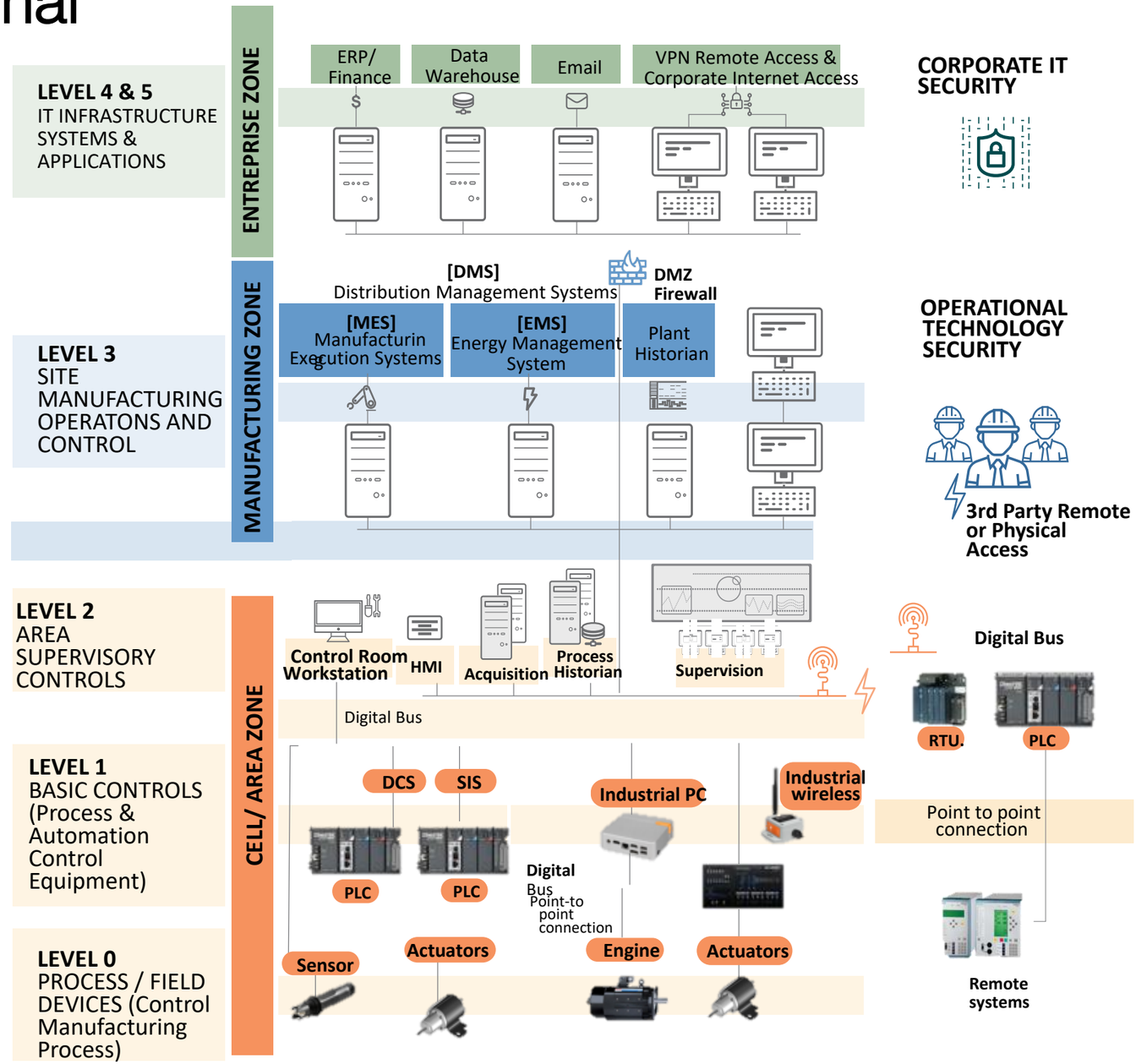
The Topology of Operational Technology

LEVEL 3 - 1 **CHALLENGES**

- Legacy communications networks interfaces
- Unmanaged Ethernet switches/ lack of available ports
- Latency introduction due to SPAN
- Legacy unsupported OS
- ICS/OT system vendor certification requirements for changes
- Attacks from IT into OT
- 3rd Party Access to OT
- Limited asset Information accuracy

LEVEL 0 -1 CHALLENGES

- Legacy systems using proprietary log messages and event triggers
- Hard wired interfaces for signaling
- Serial messaging / signal-based OT protocols



Purdue Framework

The reasons to defend against Cyber Crime….. How did this happen ?

Hack attack causes 'massive damage' at steel works

Click on to see the video

The reasons to defend against Cyber Crime….. How did this happen ?

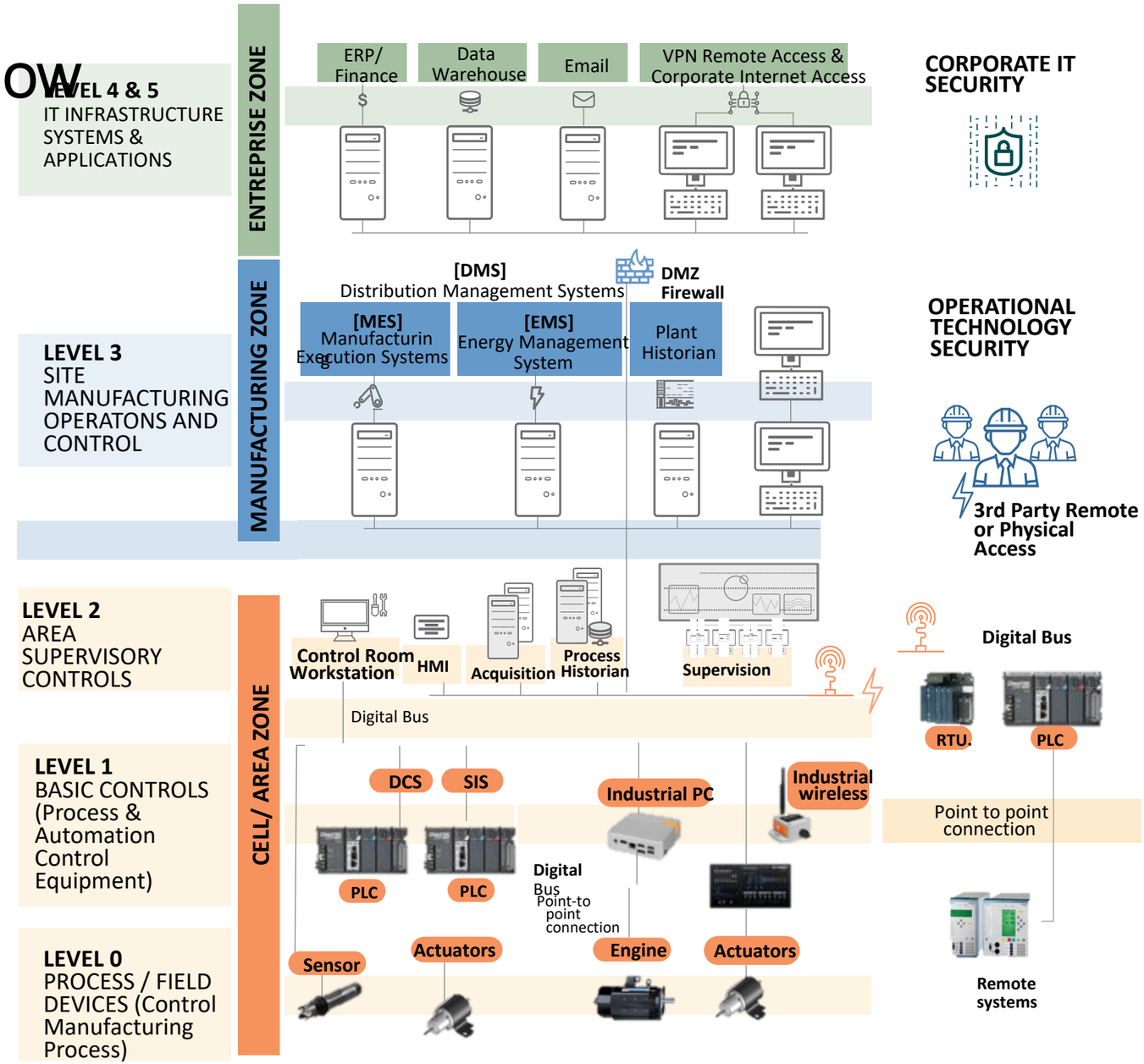
Firewall Penetration

Lateral Movement in the IT owned by OT N/W

Gained Access to the SCADA or Master Program

Found the correct settings and fail safe

Updated the PLC



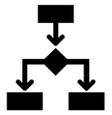
Purdue Framework

OT Transformation Journeys – 4 Key Questions

How do you ensure workers & 3rd parties are securely accessing operational environments remotely?

Implement secure remote access solutions (VPNs, 2FA, RBAC) to restrict access to authorized personnel only.

Protect operational environments from unauthorized access and security threats, especially with remote work and third-party vendors.



How do you manage IT threats today, and do you integrate insights from your operational environments?

Implement a threat management program that includes threat intelligence, vulnerability management, and incident response.

Threat management helps protect operational environments from cyber attacks, sensitive data, and downtime.

How do you comply with applicable legal and regulatory requirements such as NIS2?

Implement a governance program for compliance, conduct regular risk assessments and security audits.

Compliance is required to avoid fines and reputational damage, NIS2 requires appropriate security measures.

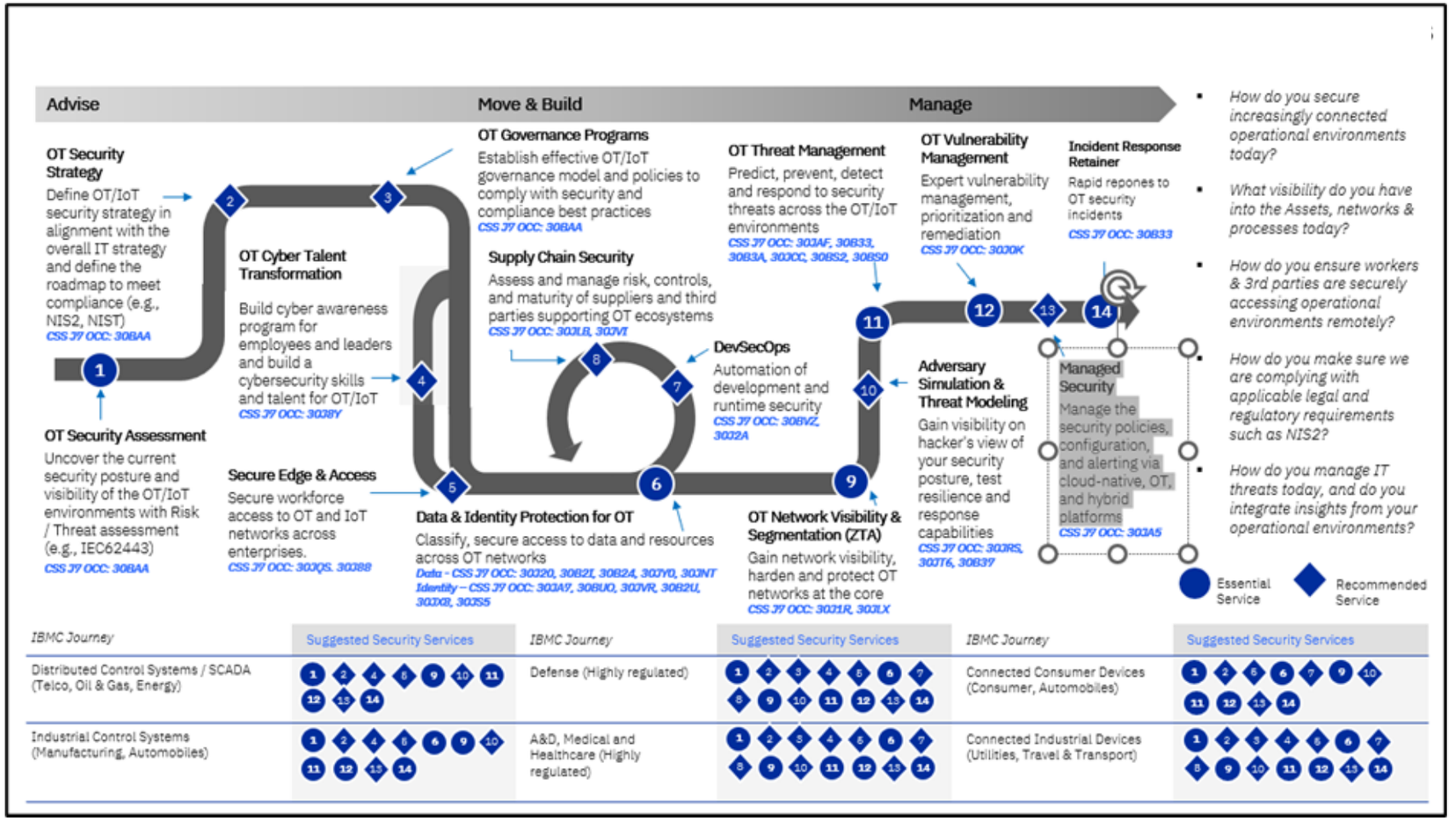
How do you secure edge and access to OT and IoT networks across enterprises?

Implement secure edge solutions and access controls.

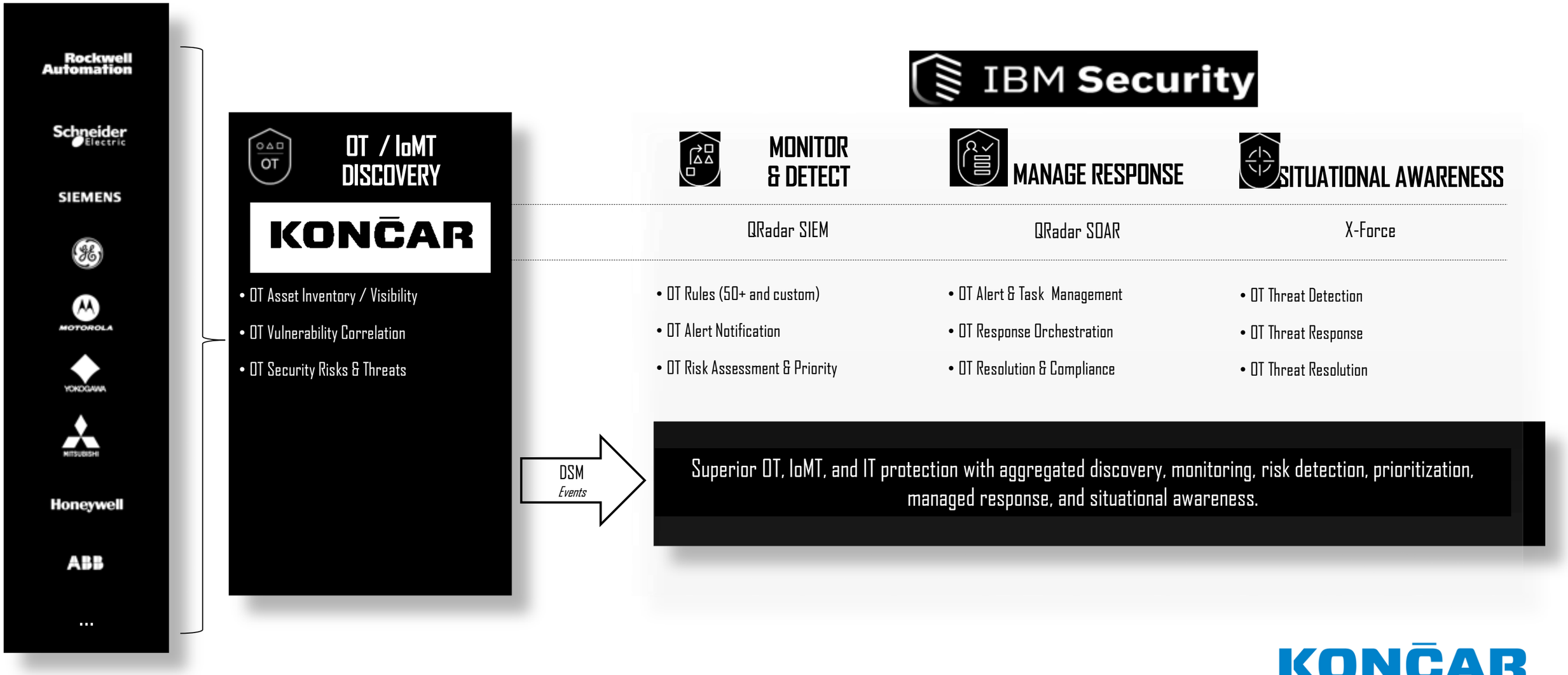
Unauthorized access to OT and IoT networks can pose a significant threat to the safety and security of industrial operations.

OT Transformation

""Implementing cybersecurity measures in a client's OT transformation journey can protect critical infrastructure, prevent financial losses, ensure compliance with regulations, safeguard customer data, ensure business continuity, protect intellectual property, and improve system performance, ultimately leading to a successful and secure digital transformation."



OT Security Solution



KONČAR DIGITAL

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
February 2024

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

Statement of Good Security Practices: No IT system or product should be considered completely secure, and no single product, service or security measure can be completely effective in preventing improper use or access. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation. Statements regarding IBM’s future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.