





NIS2 is IT en OT!
NIS2-opvolgwebinars



Praktische afspraken

- Vragen via chat
- Iedereen op mute
- Q&A na de presentatie
- Evaluatie met link naar de slides worden na de webinar doorgestuurd



inetum 
realdolmen
Positive digital flow

FORTINET®

Inetum-Realdolmen

**Advanced
Partner**

📞 Phone: +32 2 801 55 55
🏠 Huizingen, Vlaams Brabant, Belgium
🌐 <http://www.realdolmen.com>

Reseller Business Model(s): Cloud,
Integrator, MSSP

Partner Specialization(s): Operational
Technology, Public Cloud Security, SD-WAN,
Security Operations



NIS2 Compliance for OT Asset Owners

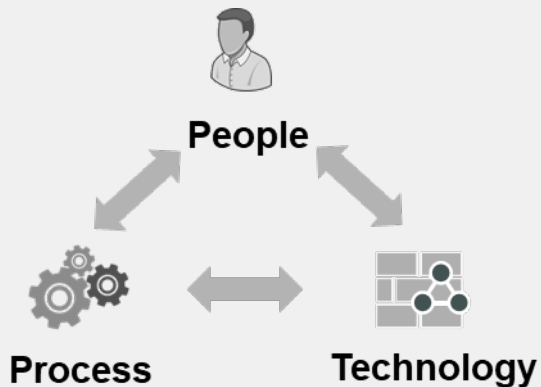


NIS2 Compliance pillars for EEs & IEs

NIS 2
Directive

Cyber Risk
Management
Measures

Cooperation &
Information
Sharing



Cyber Risk Management
Measures

Policies on risk analysis and information system security

Incident handling

Business continuity, Disaster Recovery, and crisis management

Supply chain security

Network Security, Systems Security & Vulnerability Management

Policies & Procedures to assess the effectiveness of risk management measures

The use of cryptography and encryption

Basic cyber hygiene practices and cybersecurity training

Human resources security, access control policies and asset management

Multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems



ISO 27001:2013
Information technology – Security techniques –
Information security management systems –
Requirements



ISA/IEC 62443 Standards Series
Industrial Automation and Control
System Cybersecurity Standards



NIST
Cybersecurity Framework



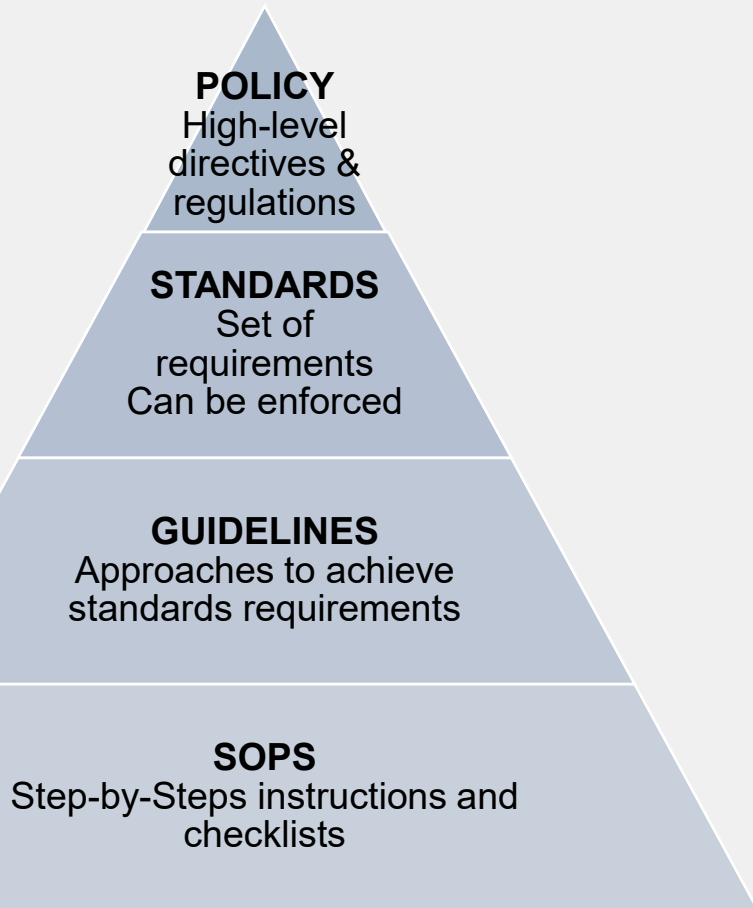
NIST
SP 800-82










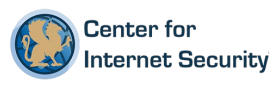
Cybersecurity Capability
Maturity Model



Main OT Security Frameworks



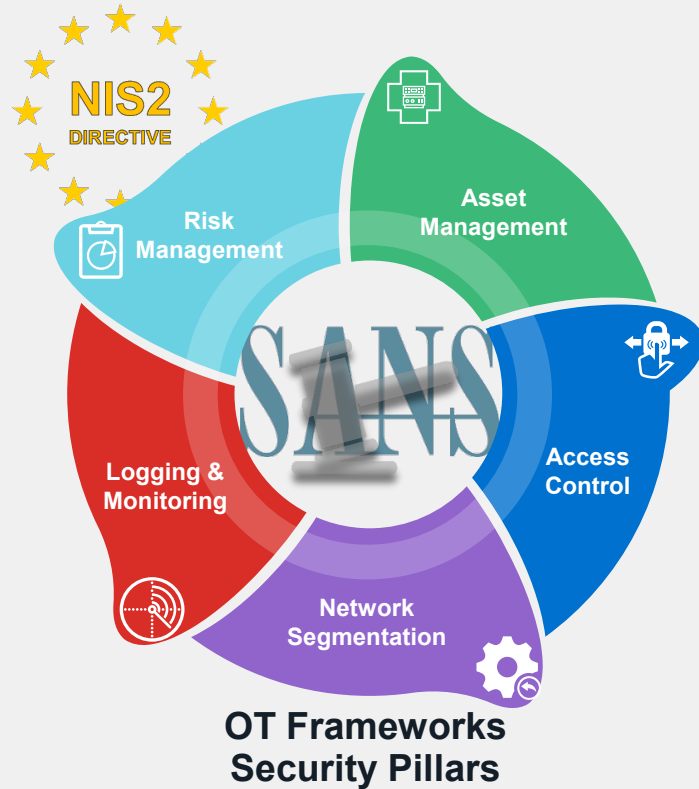
Key Frameworks	Type	Body	Origin	Scope	GEO
NIS Directives	Policies	ENISA	EU (+ UKI)	OES & DSP (*) IT/OT	EU
ISA/IEC 62443 (formerly ISA-99)	Standards	ISA,IEC, ANSI	International	Multi-Industry OT	Multi
IEC/ISO 27000s	Standards	ISO, IEC	International	Multi-Industry IT/OT	Multi
NERC-CIP	Standards	NERC	US	Electricity IT/OT	NAM
NIST CSF	Guidelines (Framework)	NIST	US	Multi-Industry IT/OT	Multi
NIST SP 800-82	Guidelines	NIST	US	Multi-Industry OT	Multi
NIST SP 800-53	Guidelines	NIST	US	Multi-Industry IT/OT	Multi
Critical Security Controls (CIS Top 18)	Guidelines	CIS	US	Multi-Industry OT	Multi

Which OT Security Framework is important for you?



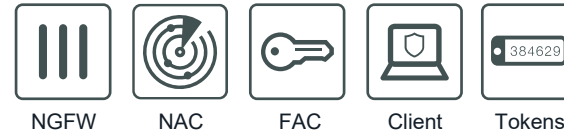
A NIS2 Technology Mapping for Compliance



Asset Management



Access Control to Networks & Assets



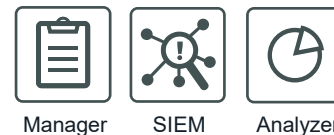
Segmentation, Protection & Response



Events, Alerts and Incident Detection



Risk Management



Single Pane Management



Threat Intelligence



Interoperability



NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

Center for
Internet Security

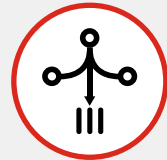


Fortinet Solution Offering for ICS/OT

FortiGate and FortiSwitch Rugged with FortiAP Outdoor



Ruggedized Design
Fan-less and use of robust components ensure reliable operation in harsh industrial environments.



Consolidated Security Architecture
FortiGate running FortiOS consolidated security offers better protection and lower cost of ownership than multiple point products.



Ease of Management
Allows rapid provision and deployment, monitoring of device and threat status while providing actionable reports.

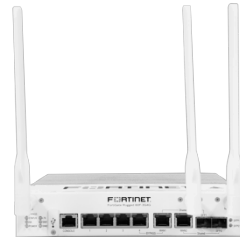
FortiGate Rugged Series



FGR-70F 3G/4G
SoC4-powered, security and VPN gateway with compact, fanless design and embedded 3G/4G/LTE



FGR-70F
SoC4-powered, security and VPN gateway with compact, fanless design



FGR-60F 3G/4G
SoC-4-powered, security and VPN gateway with embedded 3G/4G/LTE



FGR-60F
SoC4-powered, security and VPN gateway

FortiDeceptor Rugged



- **FORTIDECEPTOR RUGGED 100G**
- A Non-Intrusive, Agentless Deception Solution to Detect and Stop Active In-Network Attacks

FortiSwitch Rugged, FortiAP Outdoor Series



FSR-112D-POE and FSR-424F
Fan-less passive cooling with DIN-rail or wall-mountable. Power over Ethernet capable including PoE+. Redundant power input terminals. Mean time between failure greater than 25 years.



FortiExtender Vehicle
4G Dual SIM, GPS
Wifi + Bluetooth
Semi-Ruggedized
Use Cases:
Ambulances, truck tracking



FortiAP Rugged 432FR
External Antennas
IP67, Indoor/Outdoor Use
PoE Powered
Wall- and pole-mountable
Wi-Fi Alliance Certified
Class I Division 2 Hazardous Locations



FortiGuard OT Security Service

Operational Technology Security Service

The FortiGuard Operational Technology (OT) Security Service for FortiGate combines IPS and Application Control signatures tailored to OT environments, enabling asset owners and operators to detect and protect against network-level threats while gaining extensive visibility into OT applications and protocols.

Search



ID Lookup Encyclopedia

3,781

Number of OT Threat rules

664

Number of OT Virtual Patch rules

777

Number of OT Detection rules

Version Updates

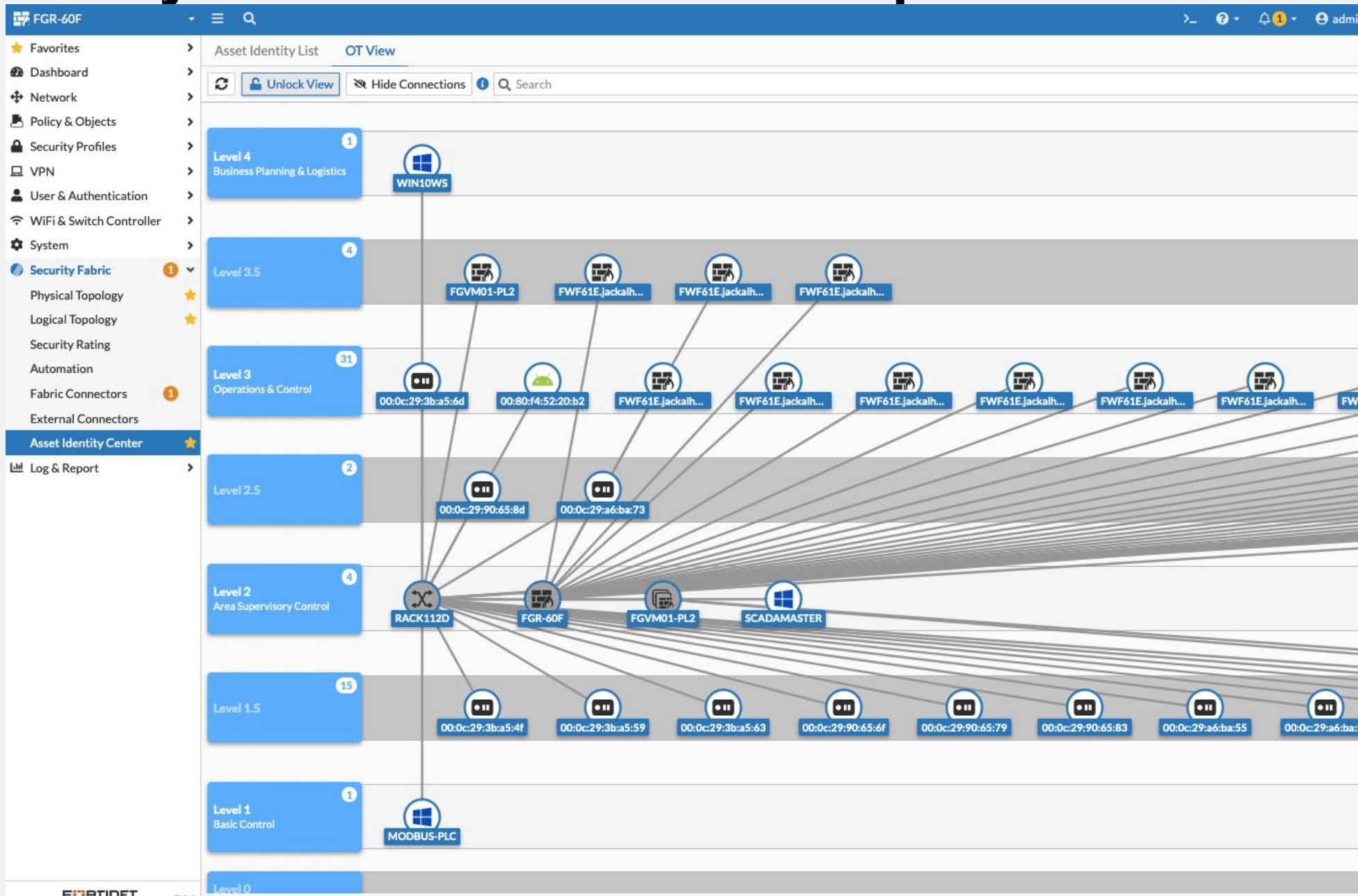
OT Threat	27.749	7 hours ago	Added (34)	Modified (4)
OT Virtual Patch	27.748	1 day ago	Added (10)	
OT Detection	27.748	1 day ago	Added (10)	

- OT Application Control
- OT Virtual Patching
- OT Device Detection

<https://www.fortiguards.com/services/ots>

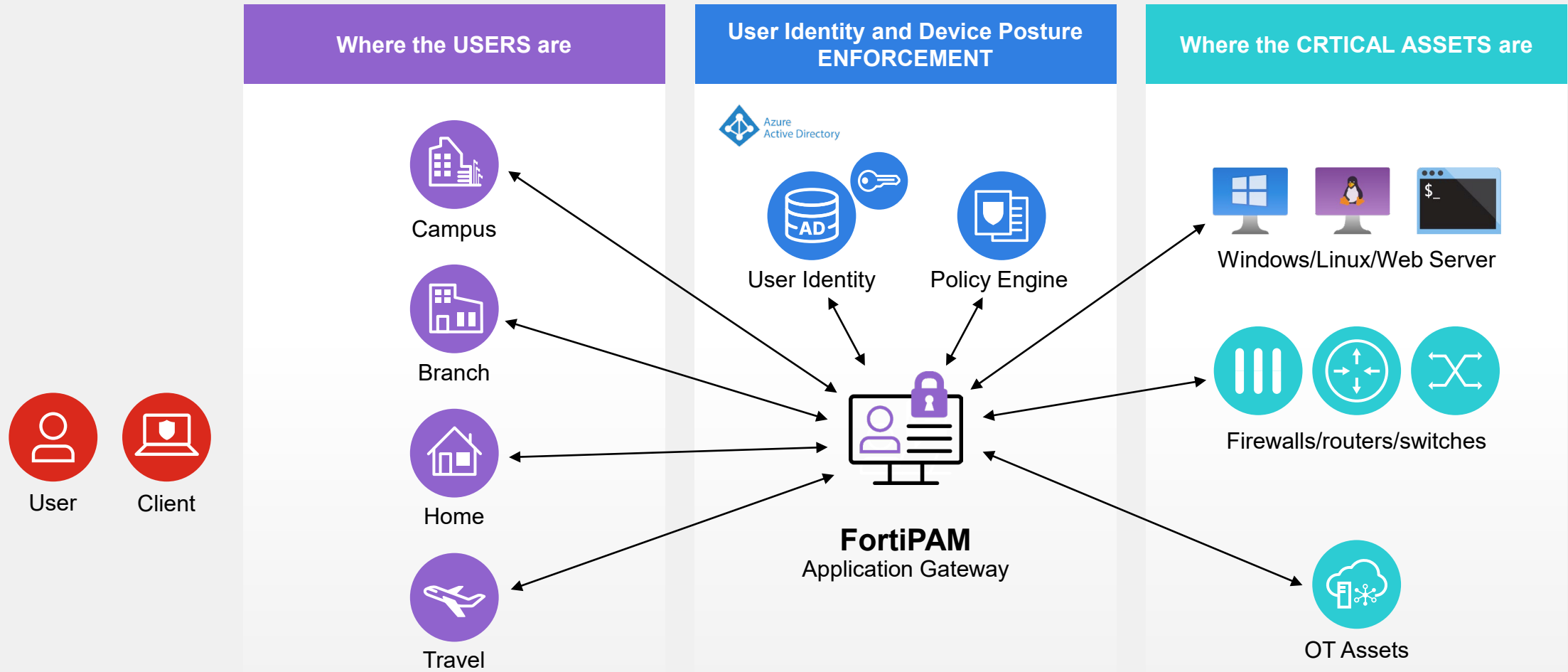


Visibility: Purdue Model Asset Map



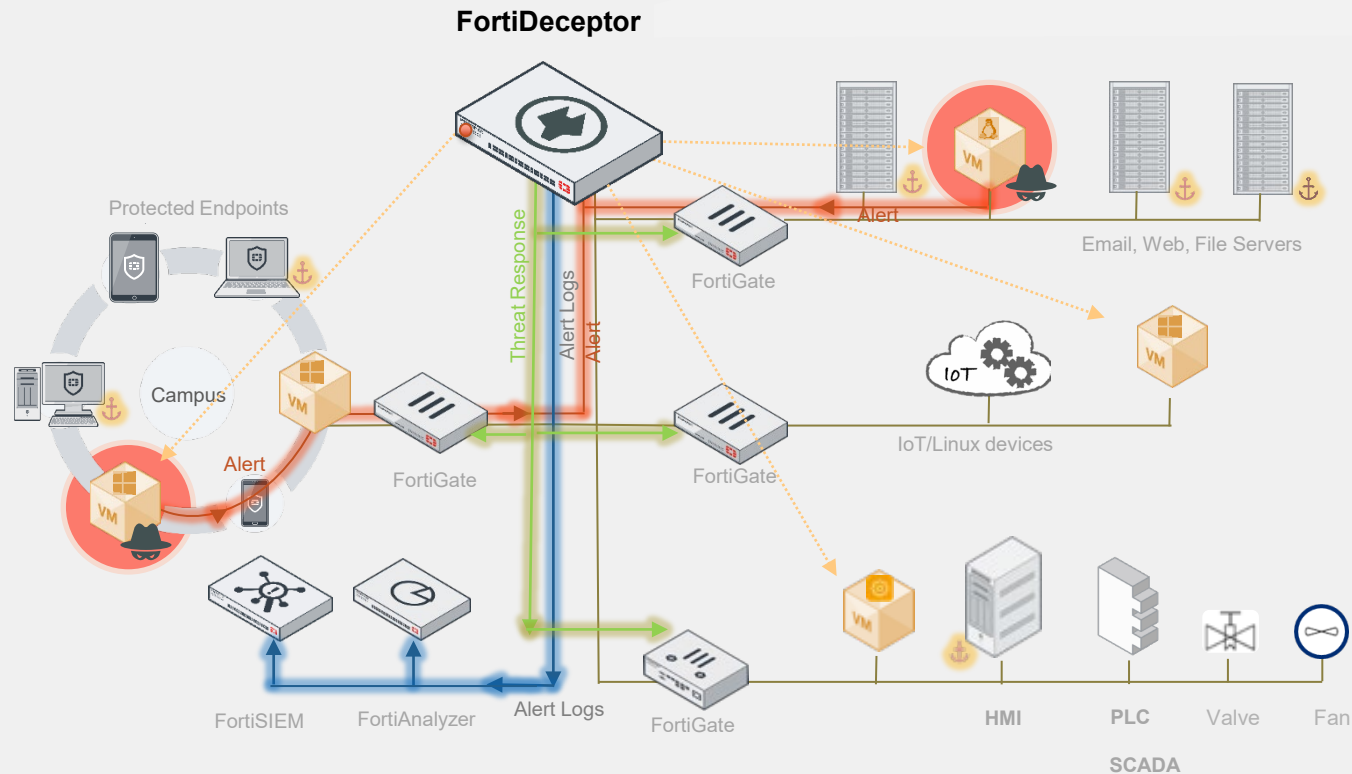
FortiPAM as (Remote) Access Gateway

The components of a ZTNA PAM solution



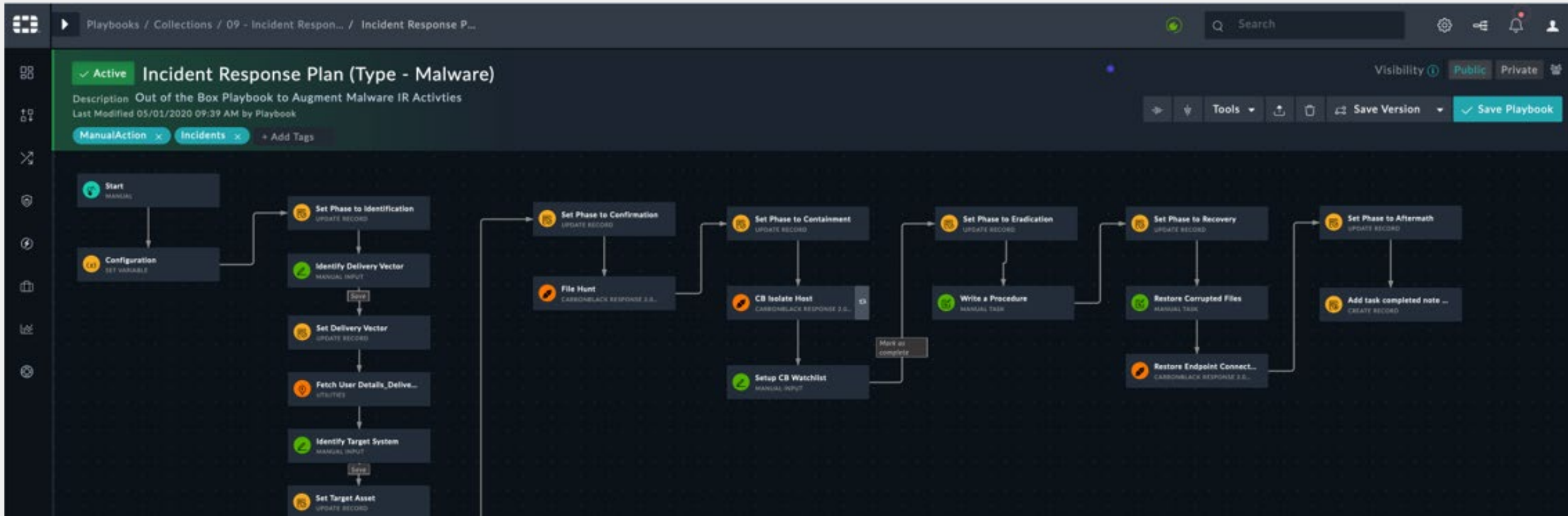
FortiDeceptor: Attack LifeCycle

Deceive > Expose > Eliminate



- Non-intrusive deployment
- High Value
- Early Warning
- Manual/Automatic blocking

FortiSOAR :Security Platform Integration Playbooks



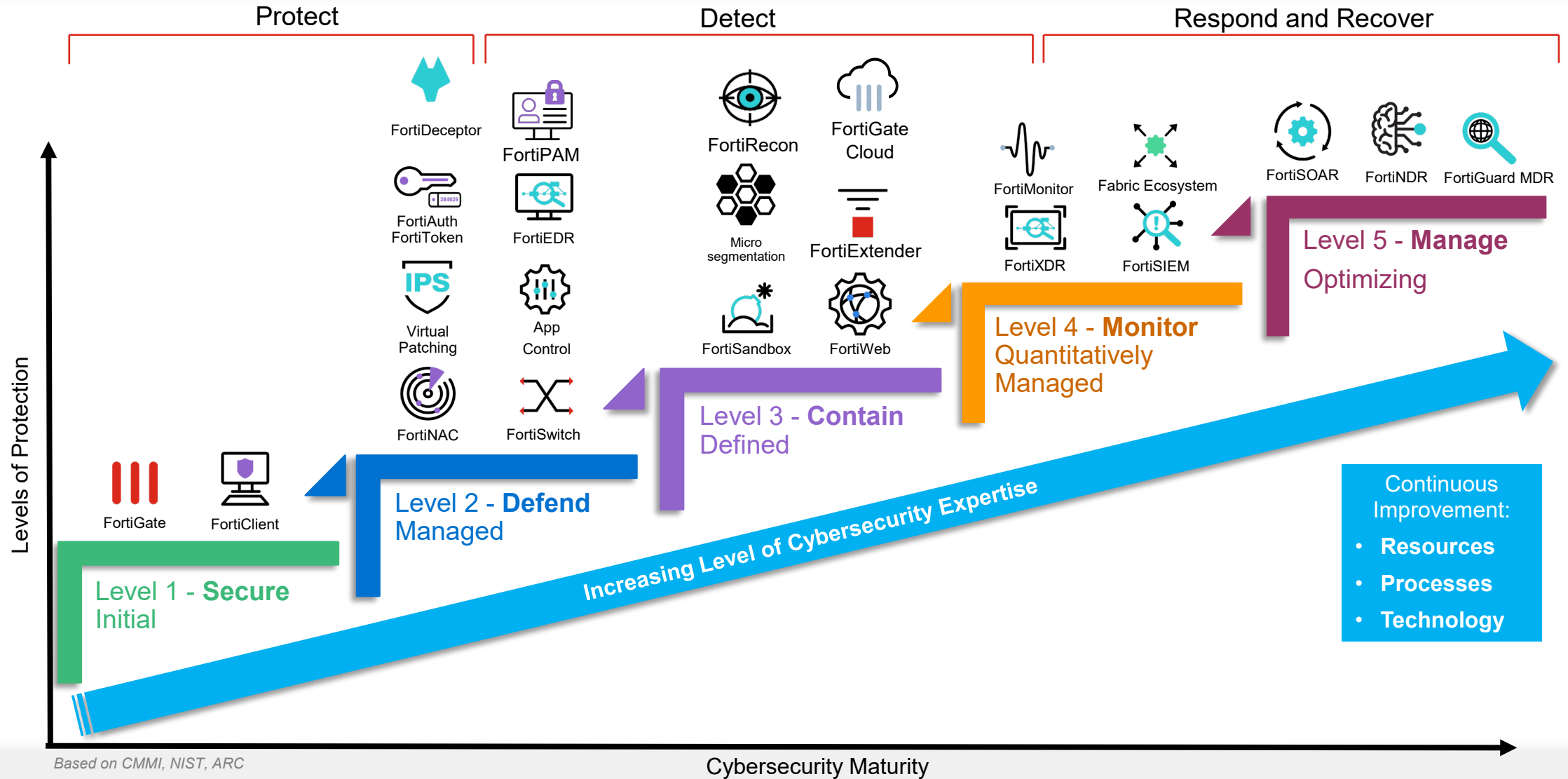
Structure and Automate

- Incident Response Plan
- Reporting to authorities
- Risk Scoring
- IT & OT collaboration



Cyber Security Maturity Scale

Applied to Fortinet's Portfolio



How Inetum-Realdolmen can help

At Inetum-Realdolmen, we understand the importance of cybersecurity and the need to comply with regulatory frameworks such as NIS2

We provide tools and guidance to help you meet the minimum measures required by NIS2, such as risk assessments, security procedures, and incident response plans

Our team of cybersecurity experts can work with you to assess your current security posture and develop a customized security plan that meets your specific needs

You can have peace of mind knowing that your systems and data are protected by industry-leading security solutions.

CYBERSECURITY ACCELERATOR PROGRAM



Identify & Inspire

Audit & Assessment
Ethical hacking
Roadmap
Proof of Concept

Protect & Integrate

Zero Trust implementation

- Identities
- Devices
- Data
- Applications
- Networks & Infrastructure

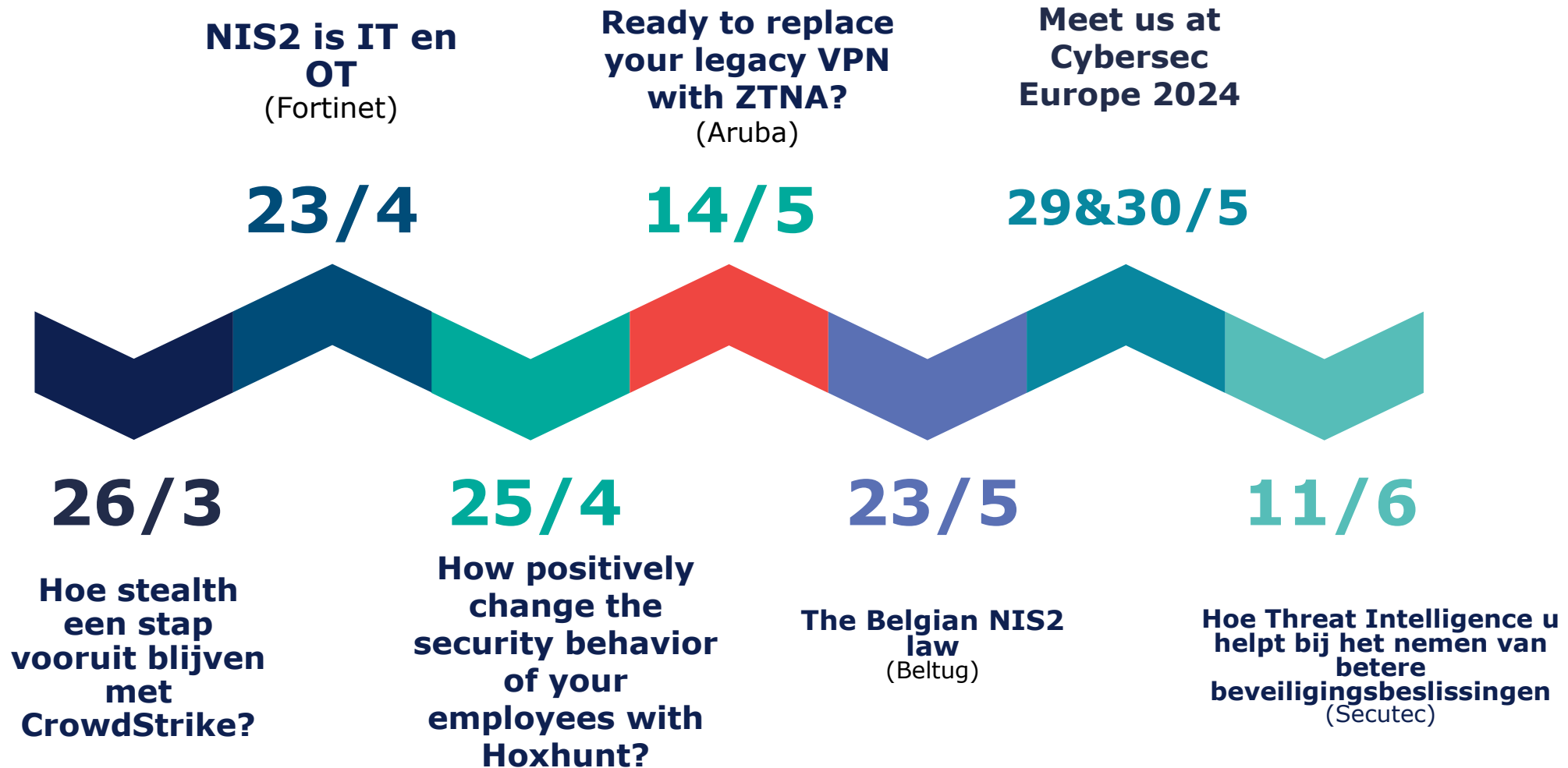
Detect & Operate

Managed Security Services
Vulnerability Management
MDR Services

Respond & Optimize

Incident Response
Governance
CISO as a Service
User Awareness

Opvolgevents NIS2



The image features the Fortinet logo centered on a black background. The logo consists of the word "FORTINET" in a bold, white, sans-serif font. The letter "O" is stylized with a red and white grid pattern. Surrounding the logo are several decorative elements: a red horizontal bar in the top left, a red horizontal bar in the top right, a red horizontal bar in the bottom left, a red horizontal bar in the middle right, a grey grid of dots in the bottom right, and various grey geometric shapes (squares and semi-circles) scattered across the background.

FORTINET