



# AI Driven Security Operations for NIS2 compliance

Andrei Perețianu

Business Development Manager Security Operations

# Fortinet is one of the largest cybersecurity companies in the world.



*Founded:* **October 2000**

*Founded by:* **Ken Xie and Michael Xie**

*Headquarters:* **Sunnyvale, CA**

*Fortinet IPO (FTNT):* **November 2009**

*Listed in both:* **NASDAQ 100 and S&P 500 Indices**

*Member of:* **2023 Dow Jones Sustainability World and North America Indices**



Global Customer Base

**750K+**

Customers

**>50%**

Global Firewall  
Shipments

2023 Billings

**\$6.4B+**

(as of Dec. 31, 2023)

**~\$2.5B+**

Investment in Innovation  
since 2017, with 91% R&D  
(as of Dec. 31, 2023)

Market Capitalization

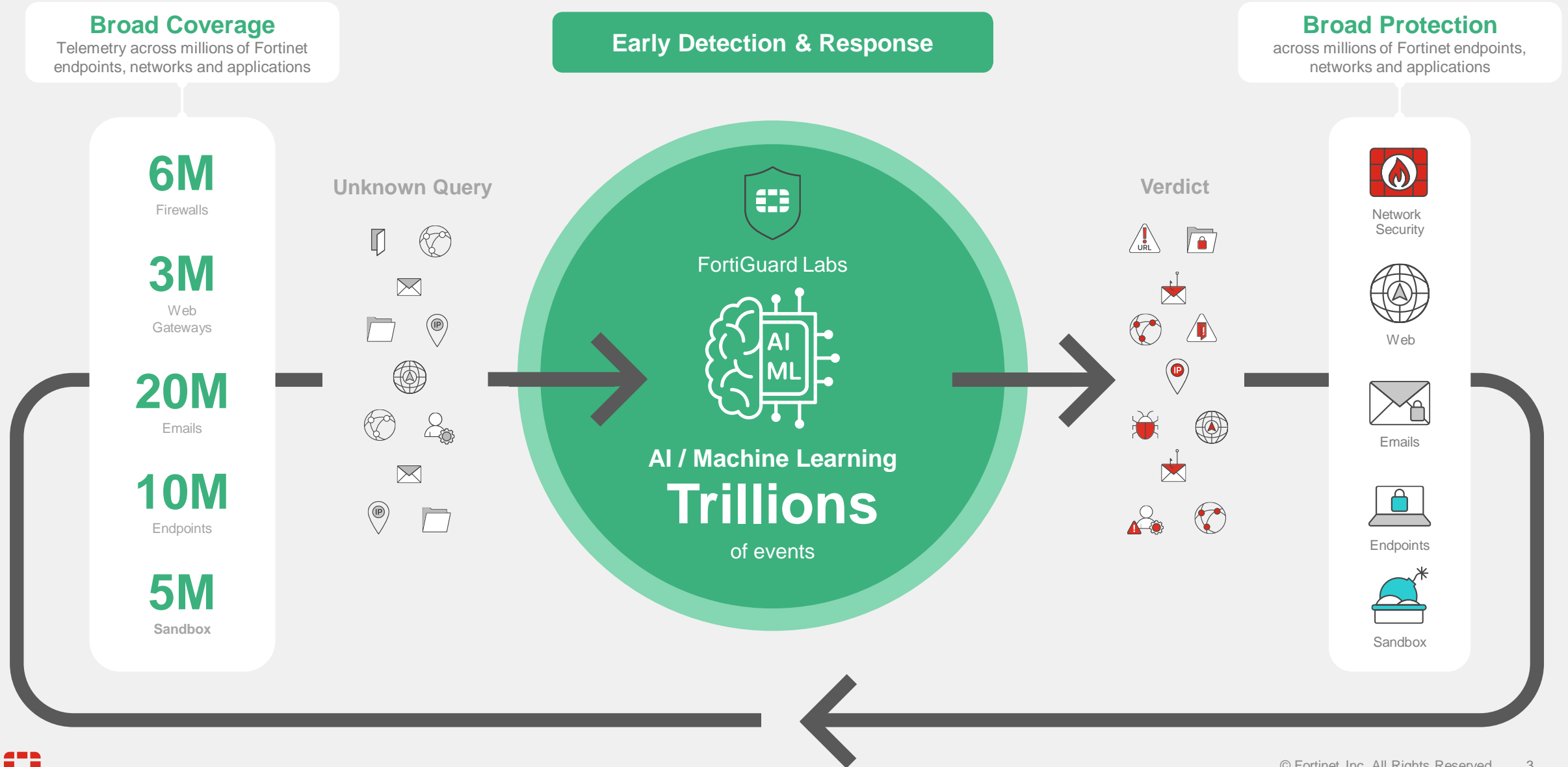
**\$52.1B**

(as of March 31, 2024)

Security Investment  
Grade Rating:

**BBB+ Baa1**

# FortiGuard AI-Powered Security at Breadth and Scale



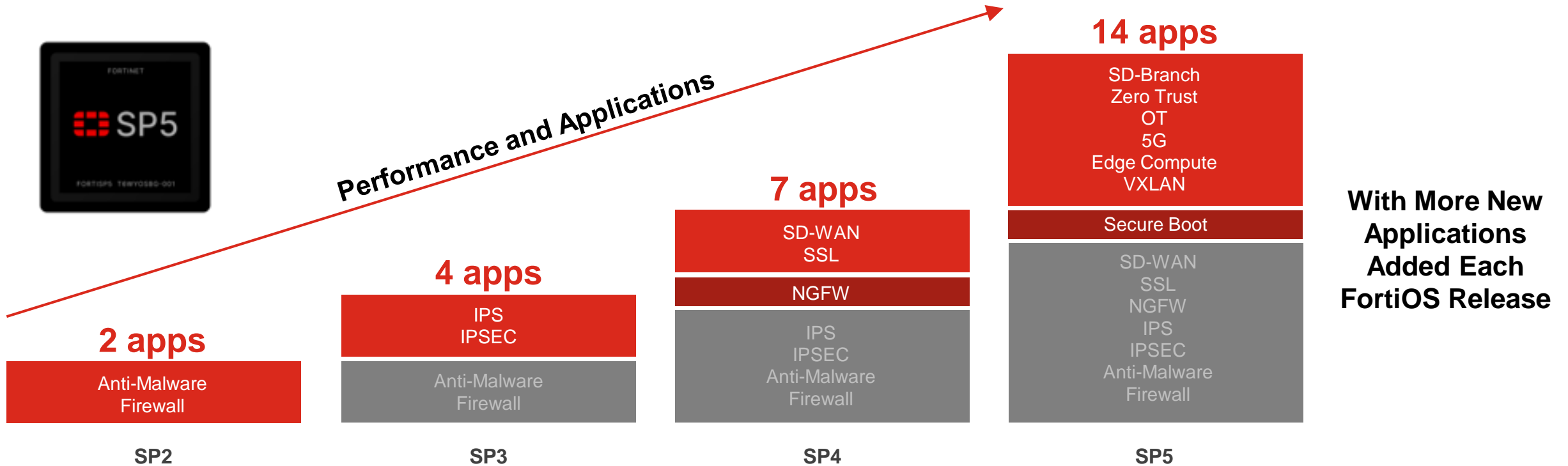
# World's Most Powerful Networking Security Operating System

FortiOS has been developed organically supporting 30+ networking and cybersecurity functions



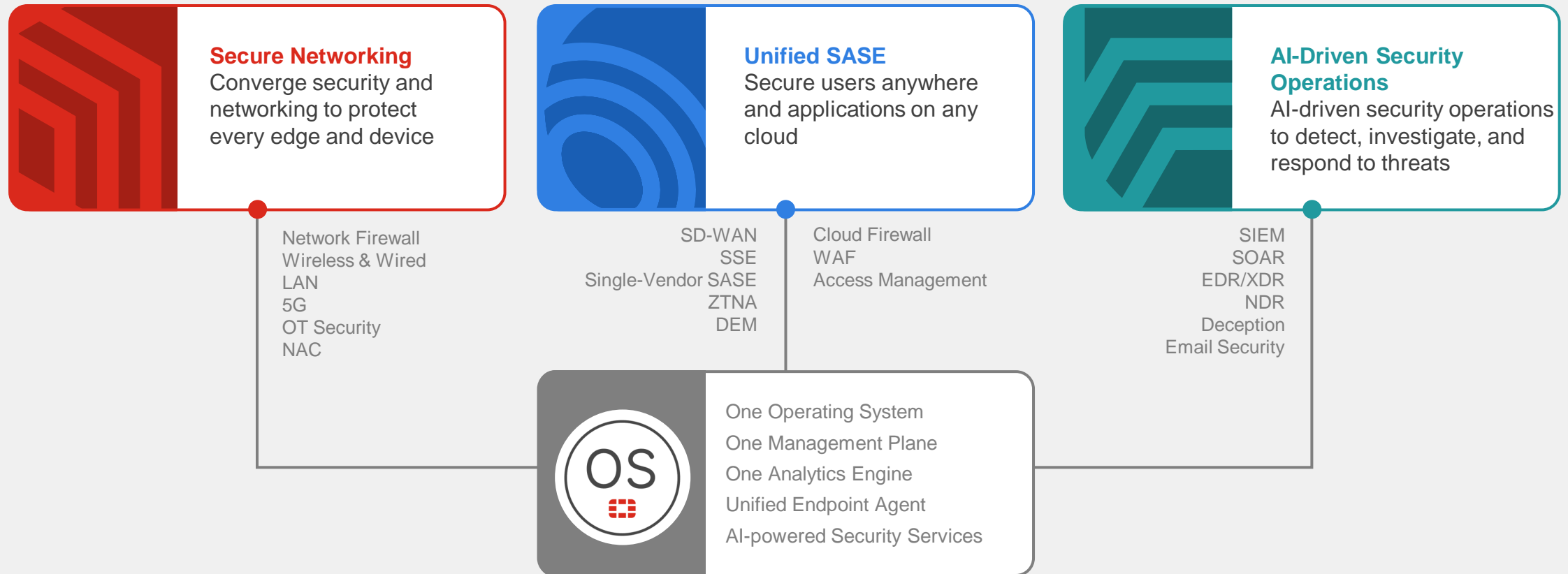
# FortiASIC Accelerates FortiOS Functions

FortiSP5 concurrently supports 2x more applications than the previous generation

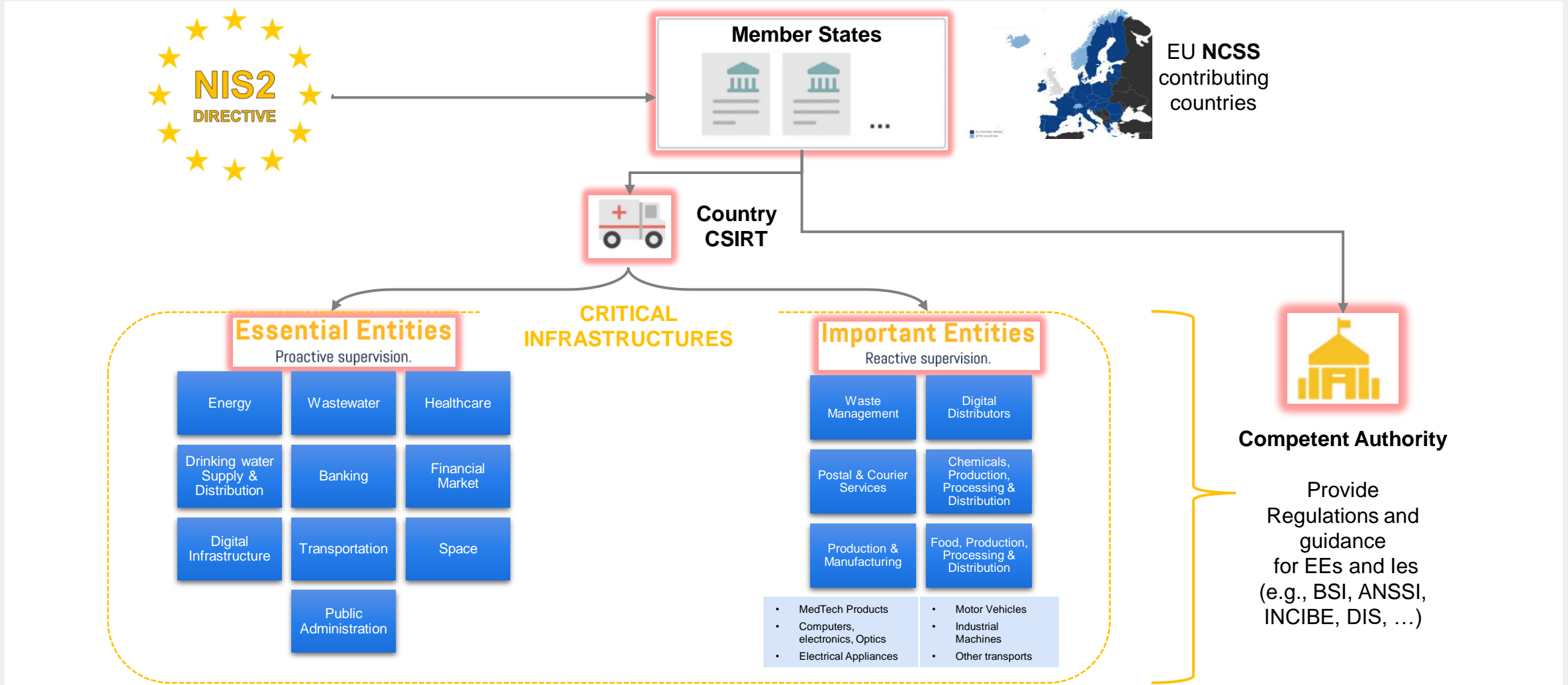


# The Fortinet Security Fabric Platform

The Only Cybersecurity Platform Delivering Unprecedented Integration and Automation



# NIS2 Directive Flow of Stakeholders Responsibilities



Member states are required to transpose NIS2 into national laws by **Oct 17th 2024**

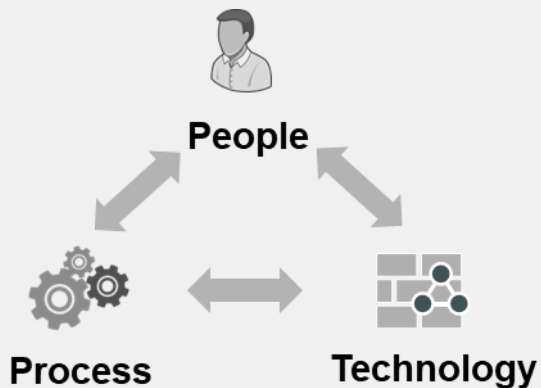


# NIS2 Compliance pillars for EEs & IEs

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



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



Cybersecurity Framework

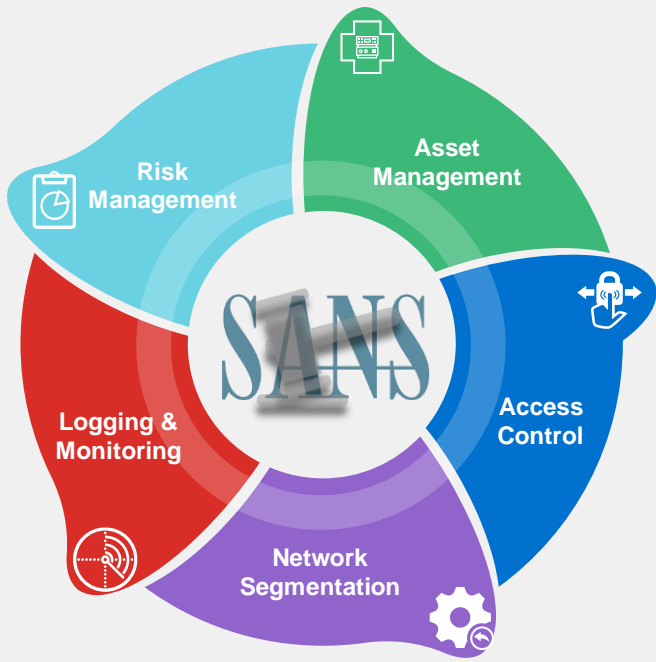


NIST SP 800-82



# A NIS2 Technology Mapping for Compliance

Integrated Security Platform for Automation, Orchestration, and Compliance



## Asset Management



SIEM



NAC



NGFW



API

## Access Control to Networks & Assets



NGFW



NAC



FAC



Client



Tokens

## Segmentation, Protection & Response



NGFW



Switch



WIFI



XDR



Tokens

## Events, Alerts and Incident Detection



SOAR



SIEM



Analyzer



SandBox



Deception

## Risk Management



Manager



SIEM



Analyzer



Single Pane Management



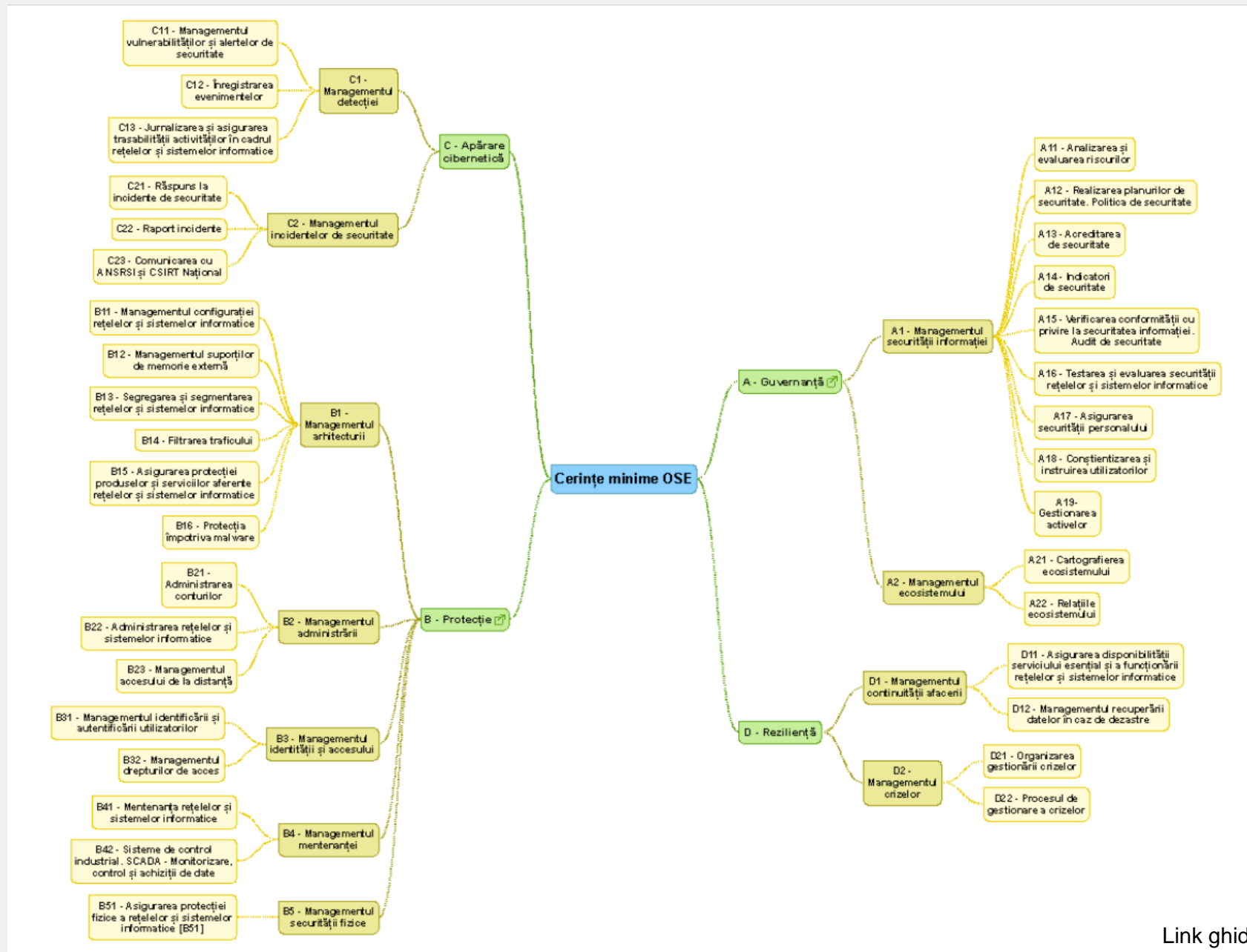
Threat Intelligence



Interoperability



# Cerinte minime OSE – Ghid DNSC

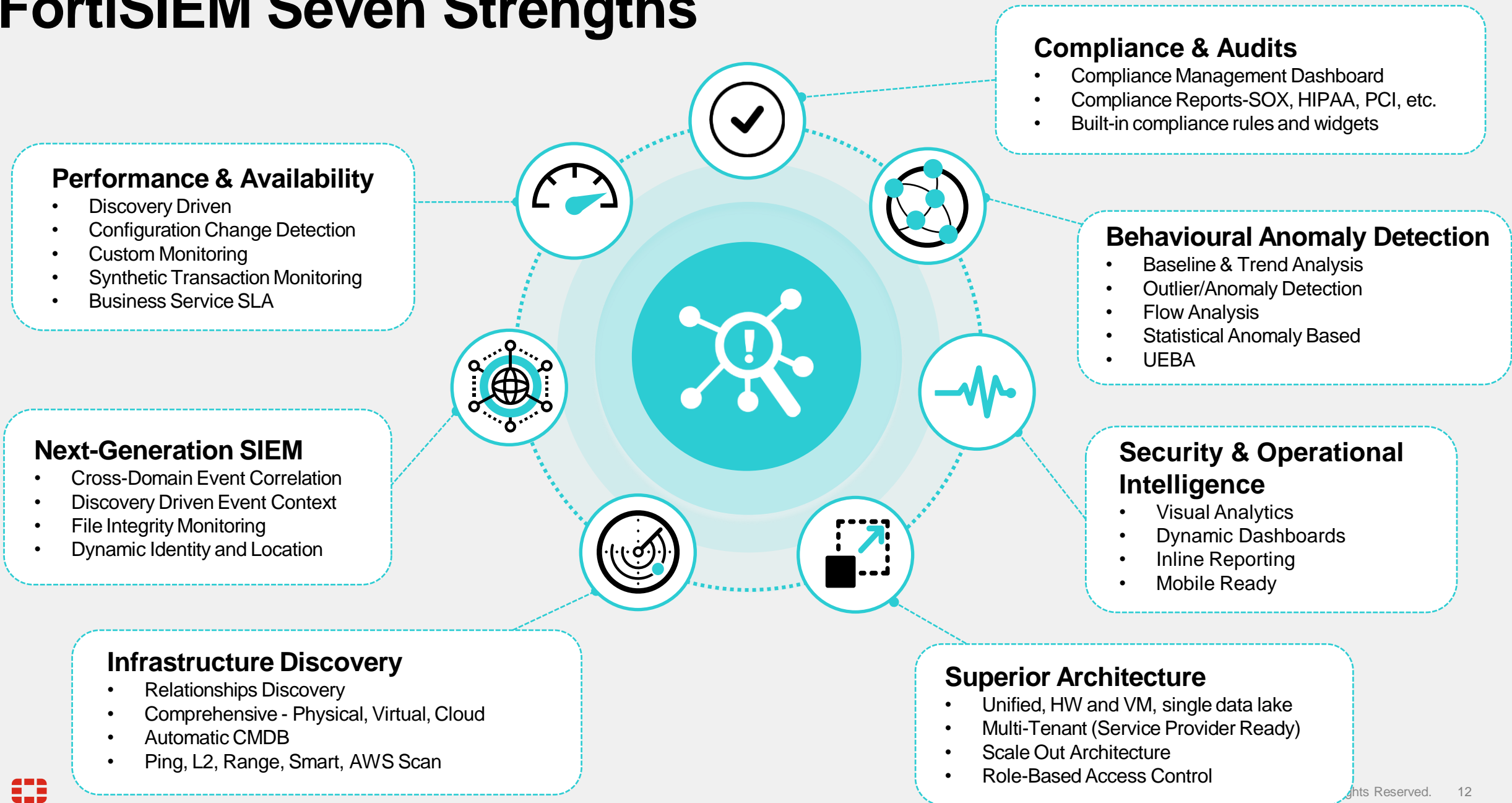


# FortiSIEM mapare cerinte NIS

Domeniu	Sub-domeniu	Masura securitate	Implementare	Solutie Fortinet
A Guvernanta	A1 Managementul securității informației	A13 Acreditarea de securitate	A131 Acreditarea rețelelor și sistemelor informatice	FortiSIEM poate genera rapoarte predefinite de tipul: PCI, COBIT, SOX, ISO, ISO 27001, HIPAA, GLBA, FISMA, NERC, GPG13, SANS Critical Control, NIST800-53, and NIST800-171
		A14 Indicatori de securitate	A141 Indicatori de securitate	FortiSIEM poate furniza indicatori de evaluare a securității
		A19 Gestionarea activelor	A191 Inventarierea și gestionarea activelor	FortiSIEM pentru CMDB inclus FortiRecon pentru scanare vulnerabilitati externe FortiClient pentru vulnerabilitate la nivel de statii de lucru In FortiCare se pot vedea vulnerabilitatile cunoscute pe echipamente Fortinet
	A2 Managementul ecosistemului	A21 Cartografierea ecosistemului	A211 Descrierea ecosistemului	FortiSIEM - CMDB & Business services
		A22 Relațiile Ecosistemului	A221 Stabilirea relațiilor ecosistemului A222 Acorduri la nivel de serviciu	FortiSIEM - CMDB & Business services FortiSIEM - CMDB & Business services
B Protecție	B1 Managementul arhitecturii	B11 Managementul configurației rețelelor și sistemelor informatice	B111 Arhitectura NIS	In FortiSIEM se pot defini Business Service Groups unde se urmaresc serviciile critic si interdependentele intre ele
		B12 Managementul suporturilor de memorie externă	B121 Suporturi de memorie externă	FortiEDR FortiClient FortiEMS Evenimente si alerte pot fi agregate in FortiSIEM
	B2 Managementul administrării	B21 Administrarea conturilor	B211 Conturi de administrare	FortiAuthenticator FortiPAM Poate fi controlat si automatizat cu FortiSIEM si FortiSOAR
		B22 Administrarea rețelelor și sistemelor informatice	B221 Utilizarea sistemelor de administrare	Cerinta este suportata de toate produsele Fortinet Log-urile sunt aduse in FortiSIEM In FortiPAM administrarea parolelor
	B4 Managementul mentenanței	B41 Mentenanța rețelelor și sistemelor informatice	B411 Menținere securitate	FortiSIEM FortiClient FortiEMS FortiSOAR
			B412 Actualizare resurse	FortiSIEM FortiClient FortiSOAR
B42 Sisteme de control industrial. SCADA - Monitorizare, control și achiziții de date	B421 Sisteme de control industriale	FortiGate cu licenta OT FortiNAC FortiSIEM FortiEDR FortiNDR		
C Apararea	C1 Managementul Detecției	C11 Managementul vulnerabilităților și alertelor de securitate	C111 Fluxul alertelor de securitate	FortiEDR FortiNDR FortiSIEM FortiGate
		C12 Înregistrarea evenimentelor	C121 Monitorizare evenimente C122 Sisteme de management	FortiSIEM FortiSIEM
		C13 Jurnalizarea și asigurarea trasabilității activităților în cadrul rețelelor și sistemelor de comunicații	C131 Jurnalizare și trasabilitate	FortiSIEM
	C2 Managementul incidentelor de Securitate	C21 Răspuns la incidente de securitate	C211 Fluxul incidentelor	FortiSIEM FortiSOAR Fortinet Incident Response Services
			C212 Monitorizarea incidentelor	FortiSIEM
			C213 Gestionarea incidentelor	FortiSIEM FortiSOAR
		C22 Raport incidente de securitate	C221 Raportarea incidentelor	FortiSIEM FortiSOAR
C23 Comunicarea cu ANRSI și CSIRT Național	C231 Interconectare națională	FortiSIEM FortiSOAR		



# FortiSIEM Seven Strengths



## Performance & Availability

- Discovery Driven
- Configuration Change Detection
- Custom Monitoring
- Synthetic Transaction Monitoring
- Business Service SLA

## Compliance & Audits

- Compliance Management Dashboard
- Compliance Reports-SOX, HIPAA, PCI, etc.
- Built-in compliance rules and widgets

## Behavioural Anomaly Detection

- Baseline & Trend Analysis
- Outlier/Anomaly Detection
- Flow Analysis
- Statistical Anomaly Based
- UEBA

## Next-Generation SIEM

- Cross-Domain Event Correlation
- Discovery Driven Event Context
- File Integrity Monitoring
- Dynamic Identity and Location

## Security & Operational Intelligence

- Visual Analytics
- Dynamic Dashboards
- Inline Reporting
- Mobile Ready

## Infrastructure Discovery

- Relationships Discovery
- Comprehensive - Physical, Virtual, Cloud
- Automatic CMDB
- Ping, L2, Range, Smart, AWS Scan

## Superior Architecture

- Unified, HW and VM, single data lake
- Multi-Tenant (Service Provider Ready)
- Scale Out Architecture
- Role-Based Access Control



# CMDB Overview

The screenshot displays the FortiSIEM CMDB interface. At the top, navigation tabs include DASHBOARD, ANALYTICS, INCIDENTS, CASES, CMDB, RESOURCES, TASKS, and ADMIN. A summary bar shows counts for various device types: Routers (7), Firewalls (11), Windows (10), Unix (3), ESX (0), AWS (0), and Azure (0). The left sidebar lists device categories such as Network Device, Network Segment, and Server. The main area shows a table of devices with columns for Name, IP, Type, Status, Discovered, Method, Agent Policy, Agent Status, Monitor Status, Event Status, AWS Account, and AWS Instance. The 'FortiGate90D' device is highlighted in orange. Below the table, a detailed view for 'FortiGate90D' is shown, including tabs for Summary, Properties, Monitor, Software, Hardware, Configuration, and Relationships. The 'Summary' tab is active, displaying general information, health overview, incidents, and statistics.

Name	IP	Type	Status	Discovered	Method	Agent Policy	Agent Status	Monitor Status	Event Status	AWS Account	AWS Instance
FG240D	192.168.3.1	Fortinet FortiOS	Pending	Sep 10 2019, 02:49:49 PM	SNMP				Normal		
FG240D	10.10.240.1	Fortinet FortiOS	Pending	Sep 10 2019, 02:48:49 PM	SNMP						
FGT90D	10.10.100.1	Fortinet FortiOS	Pending	Aug 22 2019, 10:10:16 PM	LOG						
FGVM04	10.77.1.3	Fortinet FortiOS	Pending	Aug 22 2019, 10:17:48 PM	LOG						
FortiGate50B	172.16.255.82	Fortinet FortiOS	Pending	Sep 10 2019, 02:48:50 PM	SNMP				Normal		
FortiGate90D	10.1.1.1	Fortinet FortiOS	Pending	Sep 10 2019, 02:48:50 PM	SNMP				Critical		
HOST-10	10.10.240.6	Cisco ASA	Pending	Jul 24 2019, 01:14:38 PM	LOG						
PA-500	172.16.1.2	Palo Alto PAN-OS	Pending	Sep 10 2019, 02:48:50 PM	SNMP				Critical		
10-01-10-10-10	172.16.3.10	Juniper SSG ScreenOS	Pending	Jul 24 2019, 01:10:51 PM	LOG				Critical		
SJ-Main	192.168.19.65	Cisco ASA	Pending	Oct 10 2016, 10:30:05 AM	SNMP, PING				Normal		

**Device Summary**

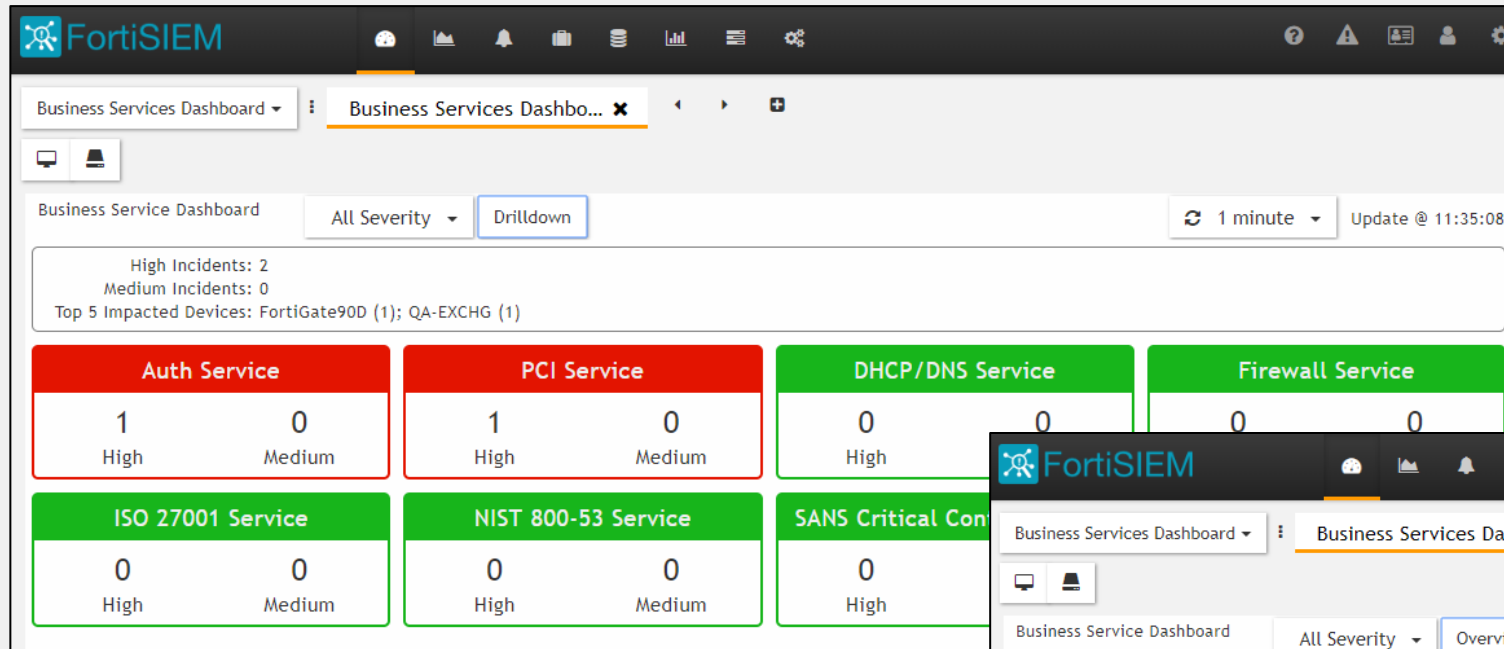
**Auto Asset Discovery & Auto Asset Categorization**

**Configuration Auditing**

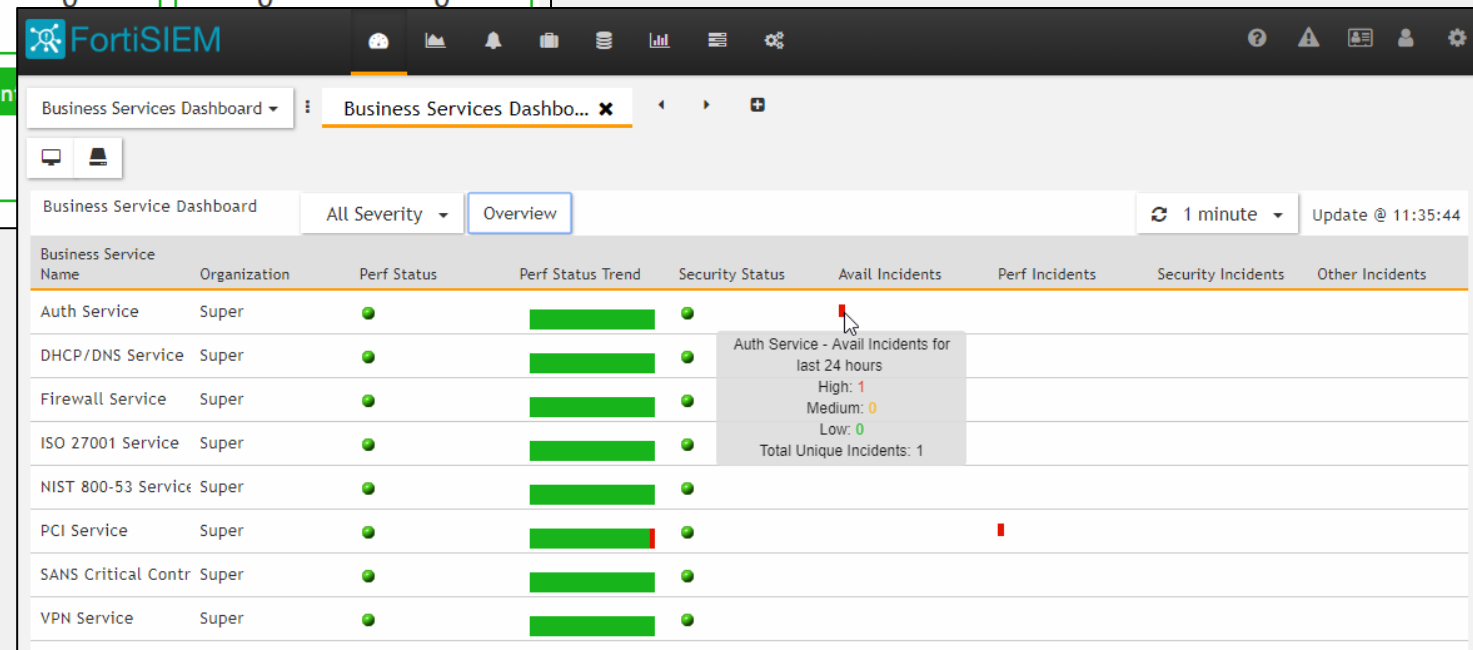
**Device Detail**



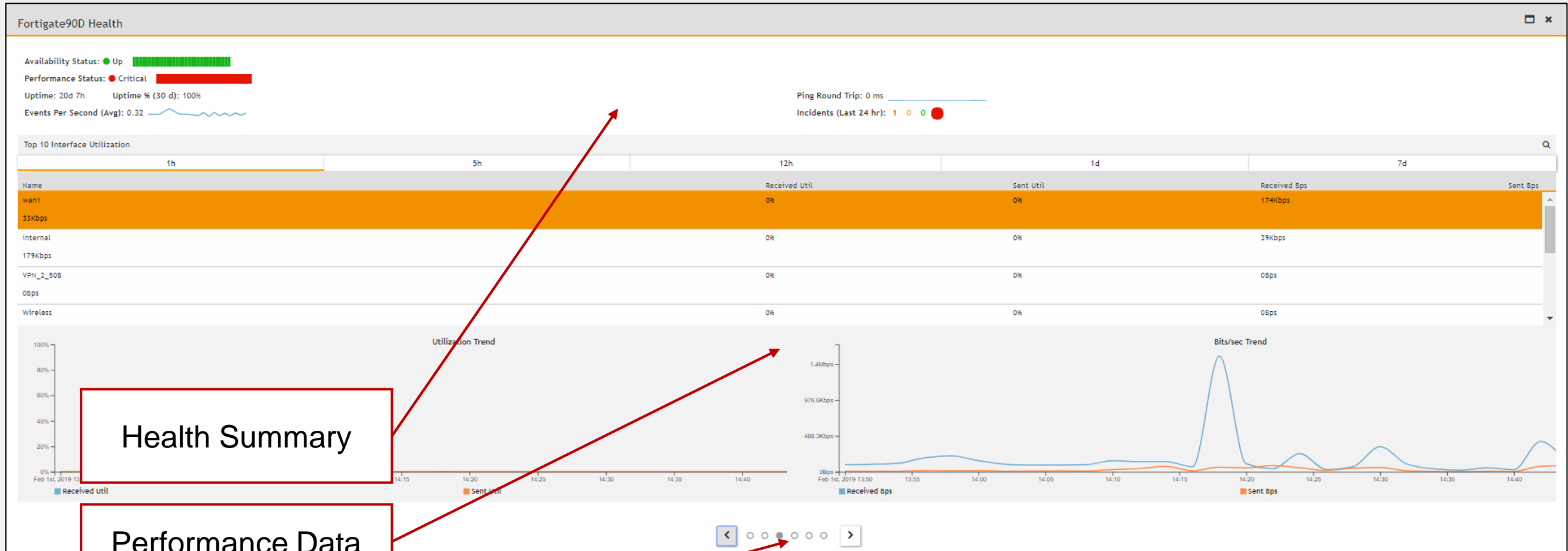
# CMDB Business Services



- Group disparate devices
- Monitor via dedicated dashboards
- Report, alert and monitor critical services



# CMDB Performance and Availability Monitoring



Health Summary

Performance Data

Additional Data



# Fortinet GenAI Advisor

Simplify and automate critical analyst activities that require advanced expertise and valuable time



# GenAI Assistant for FortiSIEM

Interpret logs and incidents, suggest actions, build rich queries and reports using natural language, and more...

The screenshot shows the FortiSIEM dashboard with a list of incidents on the left. The main area displays a chat window for 'Fortinet Advisor' with the following content:

**Action** Dec 06 2023, 09:50:59 PM You

Can you analyze this log and tell me what action should I take? "<86>Dec 6 13:50:12 date=2016-09-13 time=13:55:42 devname=FG240D3913800441 devid=FG240D3913800441 logid=0100032002 type=event subtype=system level=alert vd=root logdesc="Admin login failed" sn=0 user="root" ui=ssh(221.229.172.66) method=ssh srcip=221.229.172.66 dstip=46.4.19.86 action=login status=failed reason="passwd\_invalid" msg="Administrator root login failed from ssh(221.229.172.66) because of invalid password"

**Fortinet Advisor** Dec 06 2023, 09:51:11 PM

Based on the provided log, it appears that there was a failed login attempt with the reason "passwd\_invalid". The user "FSM\_9189044428" tried to log in via SSH from the source IP "221.229.172.66" to the destination IP "FSM\_2030775028".

To address this incident, you should take the following actions:

1. Verify the user's credentials: Check if the password for "FSM\_9189044428" is correct and up to date. If not, update the password and inform the user.
2. Investigate any potential security breaches: Look for any suspicious activity or signs of unauthorized access. Check the system logs for any related events or anomalies.
3. Implement additional security measures: Consider implementing measures like two-factor authentication or IP whitelisting to enhance the security of SSH logins.
4. Communicate with the user: Inform the user about the failed login attempt and advise them to ensure the correct password is used. Additionally, educate them about best practices for secure login procedures.

"incidentRptDevName": "FG240D3913800441",  
"incidentDetail": "",  
"ruleName": "Successful VPN Logon From Outside My Country",  
"incidentId": 1661  
}"

The screenshot shows a chat window for 'Fortinet Advisor' with the following content:

**Action** Dec 06 2023, 06:07:16 PM You

Can you analyze this log and tell me what action should I take? "<86>Dec 6 10:06:33 sp114 systemd: pam\_unix(systemd-user:session): session opened for user root by (uid=0)"

**Fortinet Advisor** Dec 06 2023, 06:07:29 PM

As an Incident and log analysis assistant, I can analyze the log you provided.

The log entry you shared is related to a user session being opened on a system. Here are some key details from the log entry:

- Timestamp: Dec 6, 10:06:33
- Hostname: sp114
- User: root
- Action: session opened for user root
- Performed by: (uid=0)

Based on this information, it appears that a user with the ID root has initiated a session on the system sp114. The session was opened by a process with the user ID (uid) 0, which typically represents the root user or a superuser.

To determine the appropriate action to take, it would depend on the context and any specific concerns or policies you have in place. Here are a few considerations:

1. User Activity: Review the user's activity and determine if it aligns with expected behavior. If the user is authorized to have a session on the system and their actions are within the scope of their role, no immediate action may be required.
2. Privileged User: Since the session was opened by a process with uid=0, it indicates a privileged user initiated the session. It's important to ensure that this privilege is not being misused or compromised. Review the purpose of the session and monitor any subsequent activities by the user.

- Analyze this incident and tell me what action to take
- What blocking activities will help contain this incident?
- Create a report of events per critical incident of the last 30 days
- Get the latest known vulnerabilities in my environment



# FortiSOAR mapare cerinte NIS

Domeniu	Sub-domeniu	Masura securitate	Implementare	Solutie Fortinet
B Protectie	B2 Managementul administrării	B21 Administrarea conturilor	B211 Conturi de administrare	FortiAuthenticator FortiPAM Poate fi controlat si automatizat cu FortiSIEM si FortiSOAR
	B3 Managementul identității și accesului	B31 Managementul identificării și autentificării utilizatorilor	B311 Identificarea utilizatorilor	FortiAuthenticator FortiPAM Procedurile se pot automatiza cu FortiSOAR
	B4 Managementul mentenanței	B41 Mentenanța rețelelor și sistemelor informatice	B411 Menținere securitate	FortiSIEM FortiClient FortiEMS FortiSOAR
			B412 Actualizare resurse	FortiSIEM FortiClient FortiSOAR
C Apararea	C2 Managementul incidentelor de Securitate	C21 Răspuns la incidente de securitate	C211 Fluxul incidentelor	FortiSIEM FortiSOAR Fortinet Incident Response Services
			C213 Gestionarea incidentelor	FortiSIEM FortiSOAR
		C22 Raport incidente de securitate	C221 Raportarea incidentelor	FortiSIEM FortiSOAR
		C23 Comunicarea cu ANRSI și CSIRT Național	C231 Interconectare națională	FortiSIEM FortiSOAR
		C233 Gestionare informații primite de la DNSC	Cerinta procedurala, care ar putea fi automatizata cu FortiSOAR	
D Rezilienta	D2 Managementul crizelor	D22 Procesul de gestionare a crizelor	D221 Gestionarea crizelor cibernetice	Fortinet Incident Response Services - Table Top Excercises FortiSOAR - War Rooms, integrare cu platforme de comunicare (Teams, etc)



# Using SOAR with AI to Speed Automation Processes

Centralize, Standardize, and Automate IT/OT Security Operations

The screenshot shows the FortiSOAR workflow editor. On the left, a 'Set Variable' step is configured with the name 'Setting a New Variable'. The main workspace displays a workflow with several steps: 'Start' (MANUAL), 'Configurations' (SET VARIABLE), 'Start Investigation' (UPDATE RECORD), 'Match Source IP in Intern...' (CYOPS UTILITIES 3.0.5), and 'Is Source IP Internal' (DECISION). A 'Virus Total' step is expanded, showing its 'data' field with sub-fields: 'attributes' (containing 'id', 'links', 'relationships', 'type'), 'message', and 'status'. A search bar at the top of the workspace allows for finding step output, expressions, and blocks.

### Maximize Your ROI with FortiSOAR

Steps	Manual	FortiSOAR
Enrich Artifacts to Identify IOCs	45 to 60 minutes	3 minutes
Perform Triaging on Events from SIEM	20 minutes	1 minute
Submit a Zip to the Detonation Engine	1 hour to 6 hours	1 minute
Isolate Affected Devices	10 minutes	1 minute
Analyze, Create, and Annotate an Incident	60 minutes	5 minutes
Block IOCs on a Firewall (e.g. FortiGate)	45 minutes to 2 hours	2 minutes
Remediation and Incident Response	60 minutes to 6 hours	5 minutes
Prepare and send an Incident Summary Report	2 to 3 hours	2 minutes
<b>TOTAL</b>	<b>4.5 TO 15 hours</b>	<b>20 minutes</b>

Zip → Artifacts  
Detonation Engine → Sandbox  
IOC → Indicators of Compromise

Typical ROI for FortiSOAR is < 6 months



# Asset & Vulnerability Management



NGFW



API



SIEM



NAC



SOAR

- *IT/OT tailored Asset Discovery*



- *Zone/Level Context based on Purdue Model*



- *Integrations with 3<sup>rd</sup> party Vulnerability Management vendors*



- *Vulnerability Management and Orchestration*

Assets

412 Items + Add

ID	Display Name	Hostname	IP Address	MAC Address	Asset Criticality	Location	Asset Risk	Asset Status	Level	Asset Tag	Property Of	Operating System	Asset Registra
899	UPS-APC_North_A_33	HMI-UPS-APC-BAT_33	10.0.1.29	E4-55-E5-55-81-L1	Medium	Transmission-North-Zone-A	Low	Active	Level 2	Substation	Other	05/12/2023...	
901	RTU_East_Q_13	HMI-SSA-13	10.0.0.111	E4-62-E5-DF-51-11	Critical	Transmission-East-Zone-Q	High	Active	Level 2	Substation	Other	05/12/2023...	
912	SCADA_ABB_03	SCADA-03	192.168.0.7	00:01:A0:C1:E0:11	Very Critical	Control Center-SCADA-Room	High	Active	Level 3	Control Center	SCADA ops	UNIX	
915	Firewall_CC_DMZ_3	Firewall_CC_DMZ_3	192.168.54...	00:40:5e:00:53:GC	High	Control_Center_DC_Farm	Minimal	Active	Level 3.5	Control Center	Other		
914	Firewall_104_North_A_2	Firewall_104_North_A_2	192.168.110...	00:40:5e:00:53:FW	High	Transmission_North_Zone_A	Minimal	Active	Level 2.5	Substation	Other		
699	Workstation-33	WORKSTATION-33	10.200.3.23	00:01:A0:C1:E0:11	Low	Control Center-Floor-3	Low	Active	Level 3	Control Center	OS X		
908	Eng-Workstation-Field-201	ENG-WS-FL-201	10.0.0.230	00:01:A0:C1:E0:55	High	Substation Field	Critical	Active	Level 2	Substation	Windows 10		
913	WSUS-CC-01	WSUS-01	192.168.10.3	00:01:A0:C1:E0:11	Low	Control Center DC farm	Minimal	Active	Level 3.5	Control Center	Server 2012		
759	Workstation-18	10.200.3.23	10.200.3.23	00:01:A0:C1:E0:64	Low	17th Floor	Minimal	Active	Level 4	Enterprise-IT	Infra	OS X	
896	Eng-Workstation-CC-64	ENG-WS-64	10.200.3.23	00:01:A0:C1:E0:21	High	Control-Center-Floor-2	Critical	Active	Level 3	Control Center	Windows 10		
911	BMS-01	BMS-01	192.168.4.3	00:01:A0:C1:E0:11	High	Control Center-SCADA-Room	Low	Active	Level 3	Control Center	UNIX		
910	SCADA_ABB_02	SCADA-02	192.168.0.6	00:01:A0:C1:E0:11	Very Critical	Control Center-SCADA-Room	High	Active	Level 3	Control Center	SCADA ops	UNIX	
909	SCADA_ABB_01	SCADA-01	192.168.0.5	00:01:A0:C1:E0:11	Very Critical	Control Center-SCADA-Room	High	Active	Level 3	Control Center	SCADA ops	UNIX	
897	Router_101_GW_North_12	Alcatel_110R_North_33	12.1.1.100	E4-62-E5-DF-51-01	High	Transmission-North-Zone-A	Critical	Active	Level 2.5	Substation	Other	05/12/2023...	
900	Protection_Relay_North_16	PR-SSA-16	10.0.0.200	E4-99-E5-DF-51-6C	Critical	Transmission-North-Zone-A	Medium	Active	Level 1	Substation	Other	05/12/2023...	
907	MailServer - 04	MailServer -04	198.168.21...	00:40:5e:00:53:af	Critical	Control Center DC Farm	High	Active	Level 3.5	Control Center	Server 2012		
905	SCMS_South_D_04	HMI-SSA-04	10.0.0.76	E4-62-E5-DF-51-7C	Critical	Transmission-South-Zone-D	Critical	Active	Level 2	Substation	Windows 7	05/12/2023...	
898	GW_104_South_D_1115	GW_104_SEL_1115	10.0.1.1	E4-62-E5-DF-51-89	High	Transmission-South-Zone-D	Minimal	Active	Level 2	Substation	Windows 7	05/12/2023...	
902	Fault_MGT_North_A_55	HMI-FM-55	10.0.0.1 (1)	E4-62-E5-DF-51-6E	High	Transmission-North-Zone-A	Low	Active	Level 2	Substation	Windows 7	05/12/2023...	
906	Printer_North_A_078	Printer-Substation-HP-078	10.0.0.178	E4-55-E5-DF-51-01	Low	Transmission-North-Zone-A	Low	Active	Level 2	Substation	Other	05/12/2023...	
903	RTU_South_D_68	RTU-SSA-68	10.0.0.155	E4-62-E5-DF-51-11	Critical	Transmission-South-Zone-D	High	Active	Level 2	Substation	Other	05/12/2023...	

Asset Inventory with context

Several Technology ... Product Integration & Process Automation are key



# Incident reporting to CSIRT



FortiSOAR™

Indicators

Malicious Indicators

264 Items - 2 selected

Execute

ID	Reputation	Type	Value	Country	Status	First Seen	TLP
4104	Malicious	URL	http://alle13net2.com:5511		TBD	05/10/2023 04:50 PM	Red
4112	Malicious	Email Address	cto_office@seedsofgrace.co.uk		TBD	05/10/2023 04:50 PM	Amber
4097	Malicious	File	Password_Update_Guide_8402.docx		Excluded	05/04/2023 02:56 PM	Amber
4091	Malicious	File	Password_Update_Guide_7358.docx		Excluded	05/03/2023 11:39 AM	Amber
4092	Malicious	URL	http://41.216.182.160/skid.arm7		TBD	05/03/2023 11:39 AM	Red
4093	Malicious	IP Address	41.216.182.160		TBD	05/03/2023 11:39 AM	Amber
4088	Malicious	IP Address	42.235.67.150		TBD	05/02/2023 06:00 PM	Amber
4082	Malicious	File	Password_Update_Guide_4128.docx		Excluded	05/02/2023 05:40 PM	Amber
4080	Malicious	Email Address	cto_office@prweekus.com		TBD	05/02/2023 05:35 PM	Amber
4065	Malicious	URL	http://103.107.9.37:57575/Mozi.m		TBD	04/28/2023 06:00 PM	Red
4057	Malicious	File	Password_Update_Guide_1304.docx		Excluded	04/28/2023 05:48 PM	Amber
4061	Malicious	Email Address	cto_office@netflix-jp-accounts0-se...		TBD	04/28/2023 05:48 PM	Amber
4058	Malicious	IP Address	117.223.85.3		TBD	04/28/2023 05:48 PM	Amber
4053	Malicious	IP Address	123.8.135.64		TBD	04/28/2023 04:17 PM	Amber
4052	Malicious	URL	http://123.8.135.64:51689/bin.sh		TBD	04/28/2023 04:17 PM	Amber
4045	Malicious	URL	http://27.45.14.49:56622/Mozi.m		TBD	04/28/2023 03:20 PM	Amber
4044	Malicious	IP Address	27.45.14.49		TBD	04/28/2023 03:20 PM	Amber
4038	Malicious	URL	http://104.244.74.252/mpsl		TBD	04/28/2023 03:19 PM	Red
3955	Malicious	File	Password_Update_Guide_8958.docx		Excluded	04/20/2023 12:53 PM	Amber
3963	Malicious	FileHash-MD5	0673d2be8ee345c9919dd710609...		TBD	04/20/2023 01:04 PM	Amber

Playbooks / Collections / 01 - Drafts / Send\_IOC\_to\_CSIRT

Active Send\_IOC\_to\_CSIRT

Description NIS2: Sending IOCs to CSIRT Eucyclone  
Last Modified 05/13/2023 07:40 AM by CS Admin

CSIRT x NIS2 x + Add Tags

Start (MANUAL)

Get Selected IOCs (CREATE RECORD)

Approval from SOC Direct... (APPROVAL)

Send Email (SMTP 2.5.0)

Update War Room (UPDATE RECORD)



# Reporting to Board



**Dashboard** Operational Technology - CIP-005

**EACM Devices**

15 Items + Add

IP Address	MAC Address	Hostname	Category	Class	Vender	Asset Criticality	Asset State	Zone	Tags	Level	ESP Zone	Facility	Modified On
172.10.11.123	12:D5:T0:67:H0:P2	NW05	Server	Software	NetFlow	Super High	Active	Enterprise	EACM	Level 4	PPLTESP	Pleasanton Plant	10/06/2022 0...
172.10.11.123 (1)...	12:D5:T0:67:H0:P2	NW06 (1)	Server	Software	NetFlow	Super High	Active	Enterprise	EACM	Level 5	PPLTESP	Pleasanton Plant	10/06/2022 0...
172.10.11.123 (1)...	12:D5:T0:67:H0:P2	NW08	Server	Software	NetFlow	Super High	Active	Enterprise	EACM	Level 5	CPPEP	Copperfield Po...	10/06/2022 0...
172.104.1.10 (1) ...	0D:1E:64:T8:89:56	Firewall - 01 (1) ...	Firewall	Hardware	Zscaler	High	Active	Enterprise	EACM EAP	Level 5	CPPLTESP	Copperfield Po...	10/07/2022 1...
172.10.11.123 (1)	12:D5:T0:67:H0:P2	NW06	Server	Software	NetFlow	Super High	Active	Enterprise	EACM	Level 5	PPLTESP	Pleasanton Plant	10/06/2022 0...

<< 1 of 3 >> Items Per Page 5

**EAP Asset Found Suspicious**

**Dashboard** Operational Technology - CIP-002

**BCA Asset**

**PCA Asset**

**TCA Asset**

**EAP Asset**

**EACM Asset**

**Unknown Asset**

**Assets by Criticality**

**Assets by CIP Asset Type**

**Assets by Category**

**BCA Asset List**

Asset Name	Zone
cpu - d3	Enterprise
Copperfield Power Plant	Enterprise
cpu - d5 (8)	Enterprise
Pleasanton Plant	Enterprise
cpu - d7 (3)	Enterprise
Copperfield Power Plant	Enterprise
win7	Enterprise
Copperfield Power Plant	Enterprise

**PCA Asset List**

Asset Name	Zone
win7 (1) (2)	Enterprise
Copperfield Power Plant	Enterprise
cpu - d7 (2)	Enterprise
Wheatstone Substation	Enterprise
cpu - d7	Enterprise
Copperfield Power Plant	Enterprise
mcs24 (1) (1) (2)	Call
Copperfield Power Plant	Enterprise

**TCA Asset List**

Asset Name	Zone
Pen Drive - 178 (1)	Enterprise
Pleasanton Plant	Enterprise
Router - d47 (2)	Enterprise
Pleasanton Plant	Enterprise
Pen Drive - 254	Enterprise
Pleasanton Plant	Enterprise
Router - d47 (2) (1)	Enterprise
Pleasanton Plant	Enterprise
Router - d45 (1) (1) (1)	Enterprise
Pleasanton Plant	Enterprise

**EAP Asset List**

Asset Name	Zone
Firewall - 05 (1) (1) (2) (1)	Enterprise
Pleasanton Plant	Enterprise
Firewall - 05 (1) (1) (3)	Enterprise
Copperfield Power Plant	Enterprise
Firewall - 05	Enterprise
Copperfield Power Plant	Enterprise
FortiGate - 53 (1)	Enterprise
Copperfield Power Plant	Enterprise
Sophos - 907 (1) (1)	Enterprise
Copperfield Power Plant	Enterprise



# Crisis Communication



The screenshot displays the FortiSOAR War Room interface for a crisis communication event. The main dashboard includes several key metrics:

- Time Elapsed:** 21h 44m (Since the War Room was setup)
- Assets Impacted:** 1 (0 High)
- Artifacts Analyzed:** 6 (2 Malicious)
- Threat Types:** 1 (Suspicious Email)

The interface also features a summary table for the incident:

Field	Value
Email Sender	cto_office@new-hypesquad-join.com
Origin	External Email
Technique Description	Adversaries may send spearphishing messages with a malicious attachment to elicit sensitive information. Spearphishing for information frequently involves social engineering techniques, such as phishing, to collect information (ex: [Establish Accounts](https://attack.mitre.org/techniques/T1585) or [Credential Harvesting]). All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or organization. Spearphishing attacks often involve a file to the spearphishing email and usually rely upon the recipient populating information.

The interface includes a navigation menu with options like Dashboard, Task Management, Investigate, and Communication. A chat window on the right shows a conversation between FortiSOAR SME and a user, discussing the incident and requesting further investigation.

- Collaboration between OT, IT, Safety, Engineering and Legal teams
- From NIS2 Directive perspective Incident reporting obligations needs to be met in tight deadlines.
- Helps to consolidate all the artifacts and Indicators of compromise
- Easy to track all the vulnerable and compromised assets, helps in faster containment and remediation



# FortiEDR mapare cerinte NIS

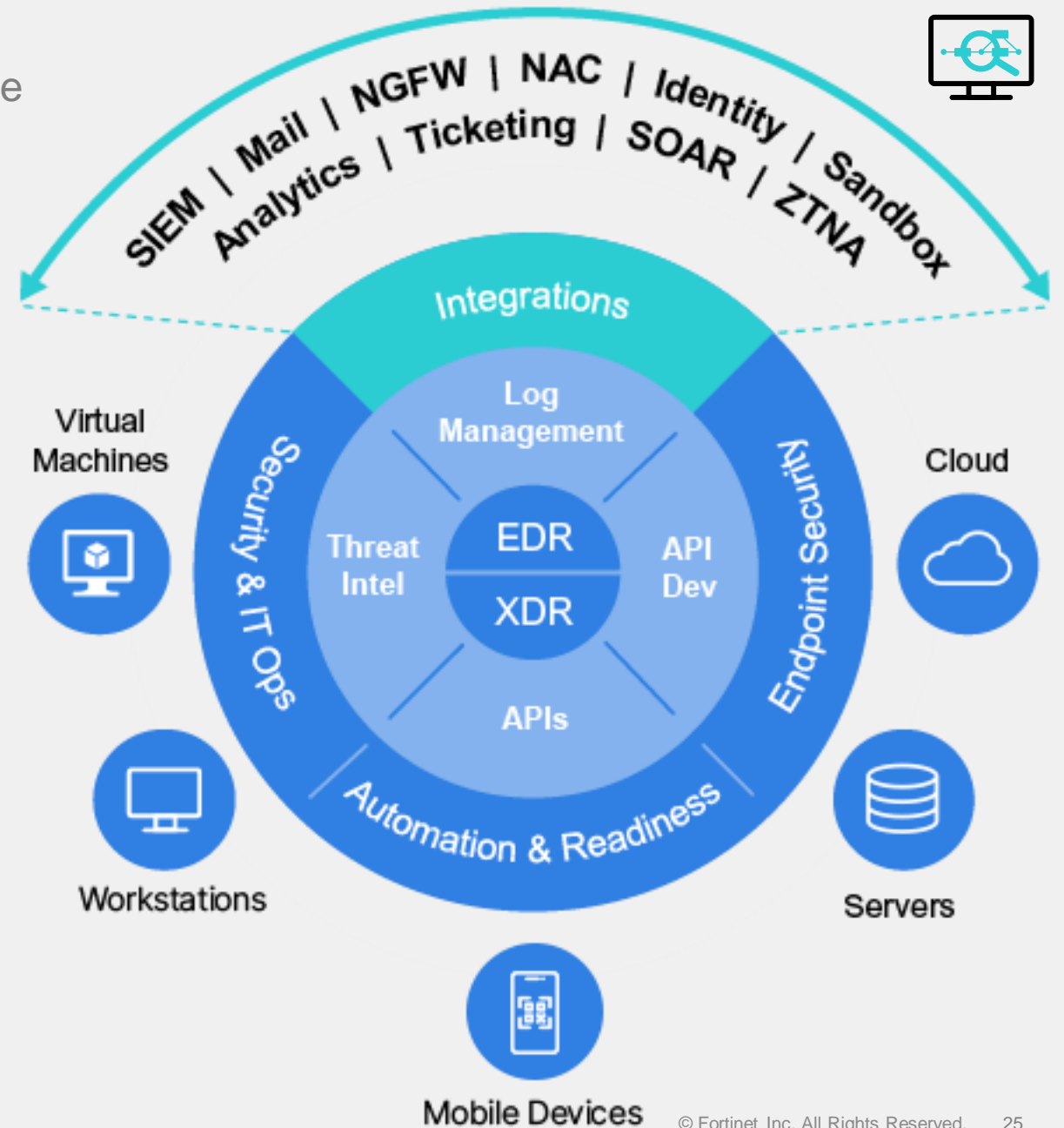
Domeniu	Sub-domeniu	Masura securitate	Implementare	Solutie Fortinet
B Protectie	B1 Managementul arhitecturii	B12 Managementul suportilor de memorie externă	B121 Suportii de memorie externă	FortiEDR FortiClient FortiEMS <b>Evenimente si alerte pot fi agregate in FortiSIEM</b>
		B16 Protecția împotriva malware	B161 Protecție malware	Pe baza de semnaturi: FortiClient FortiEDR FortiMail FortiGate Pentru 0-day: FortiNDR FortiSandbox
	B4 Managementul mentenanței	B42 Sisteme de control industrial. SCADA - Monitorizare, control și achiziții de date	B421 Sisteme de control industriale	FortiGate cu licenta OT FortiNAC FortiSIEM FortiEDR FortiNDR
C Apararea	C1 Managementul Detecției	C11 Managementul vulnerabilităților și alertelor de securitate	C111 Fluxul alertelor de securitate	FortiEDR FortiNDR FortiSIEM FortiGate



# FortiEDR Design Principles

Cloud-Native Endpoint Protection, Detection & Response

- Kernel-based EPP/EDR client
  - Lightweight agent
  - Superior visibility
  - Evasion resistant
- Support for legacy OSes and hybrid environments with feature parity
- Ransomware-proof code tracing
- Multi-Data lake without need of replication with flat licensing
- Fully integrated with rich API base
- Superior automated response options
- Complemented by managed services



# High Marks From 3rd Parties



4.7/5.0

Garner Peer Insights

95%

Customers Recommend Solution

98%

Overall Sub-Technique  
Detection

95%

Analytic Detection  
Rate

Zero

Delayed Detections

75/75

General Attack

25/25

Targeted Attack

100%

Protection Accuracy

Only Outperforming  
Leader



# FortiRecon mapare cerinte NIS

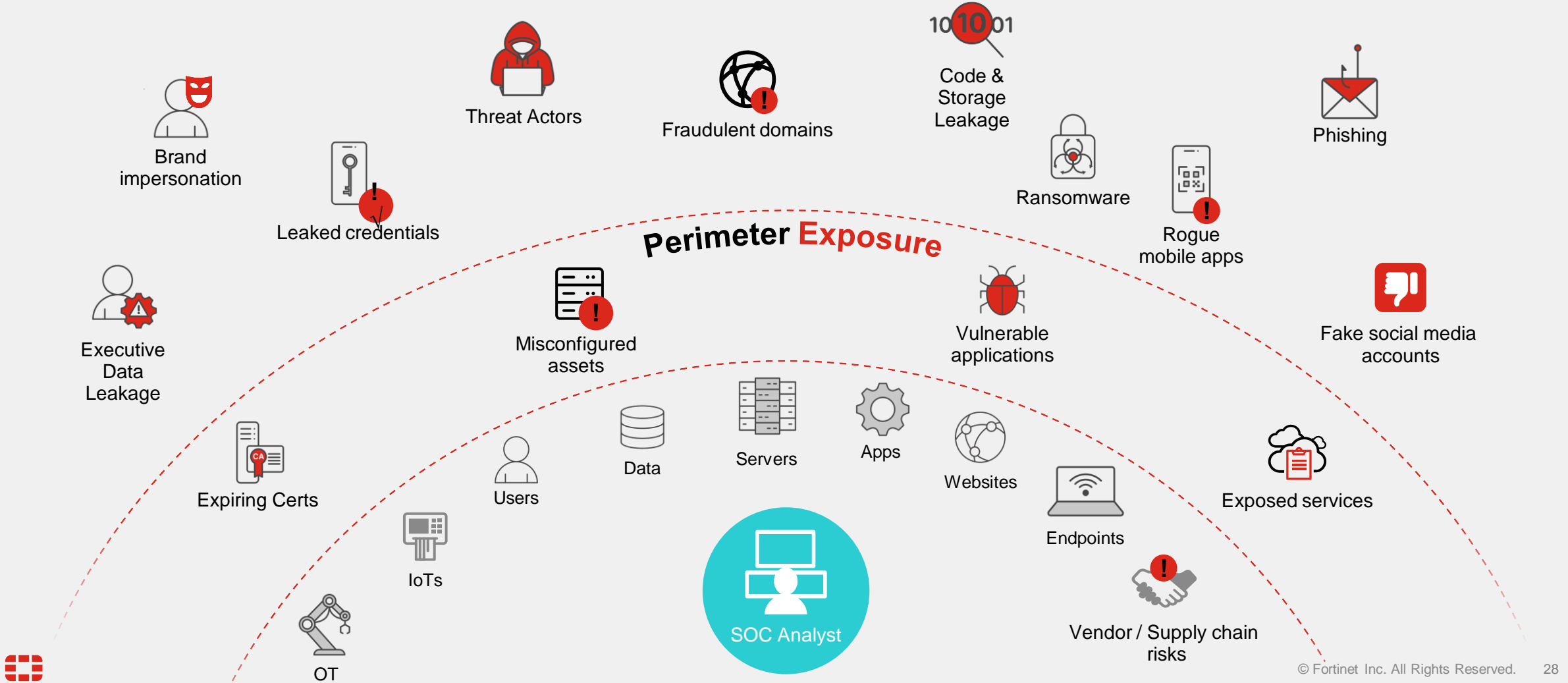
Domeniu	Sub-domeniu	Masura securitate	Implementare	Solutie Fortinet
A Guvernanta	A1 Managementul securității informației	A13 Acreditarea de securitate	A131 Acreditarea rețelelor și sistemelor informatice	FortiSIEM poate genera rapoarte predefinite de tipul: PCI, COBIT, SOX, ISO, ISO 27001, HIPAA, GLBA, FISMA, NERC, GPG13, SANS Critical Control, NIST800-53, and NIST800-171 <b>FortiRecon</b> pentru managementul riscului extern
		A19 Gestionarea activelor	A191 Inventarierea și gestionarea activelor	FortiSIEM pentru CMDB inclus <b>FortiRecon</b> pentru scanare vulnerabilitati externe FortiClient pentru vulnerabilitate la nivel de statii de lucru In FortiCare se pot vedea vulnerabilitatile cunoscute pe echipamente Fortinet
C Apararea	C1 Managementul Detecției	C11 Managementul vulnerabilităților și alertelor de securitate	C112 Evaluarea și monitorizarea vulnerabilităților	Fortinet Vulnerability Assessment - Professional service FortiClient - end point vulnerability <b>FortiRecon</b> - suprafata externa





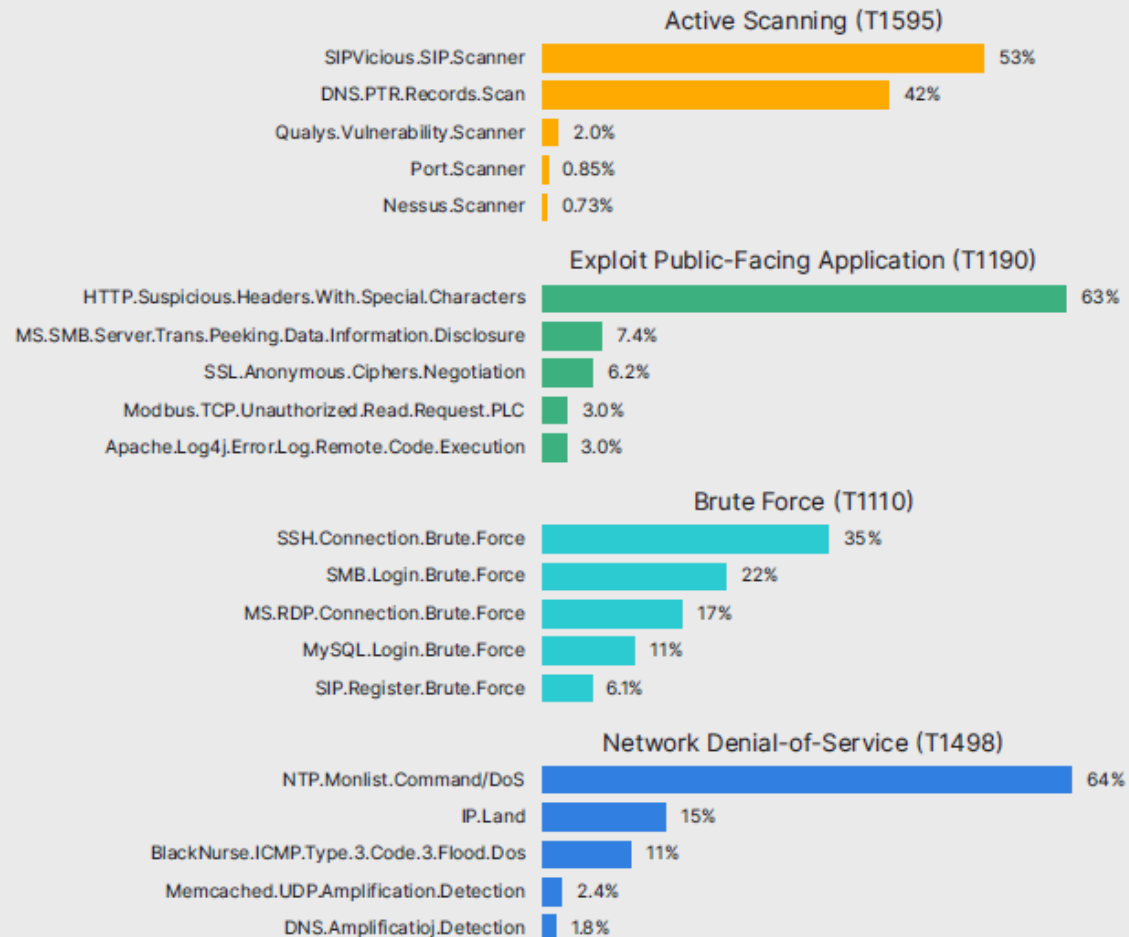
# The Ever-Expanding External Threat Landscape

## External Exposure



# FortiGuard Global Threat Landscape Report

Most prevalent recon and initial access detections associated with MITRE ATT&CK techniques





# FortiRecon - Understanding Your Posture

**Digital Risk Prevention Service**  
Mitigating risks to your external attack surface



## External Attack Surface Management

Monitor and remediate external attack surface



## Brand Protection

Detect Brand Impersonation, web site typo-squatting, rogue applications



## Adversary Centric Intelligence

Curated FortiGuard Threat Intelligence

**External Attack Surface Management**

**Brand Protection**

**Adversary Centric Intelligence**



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 grid of small white dots in the bottom right, and various dark gray geometric shapes (squares and semi-circles) scattered across the background.

**FORTINET**