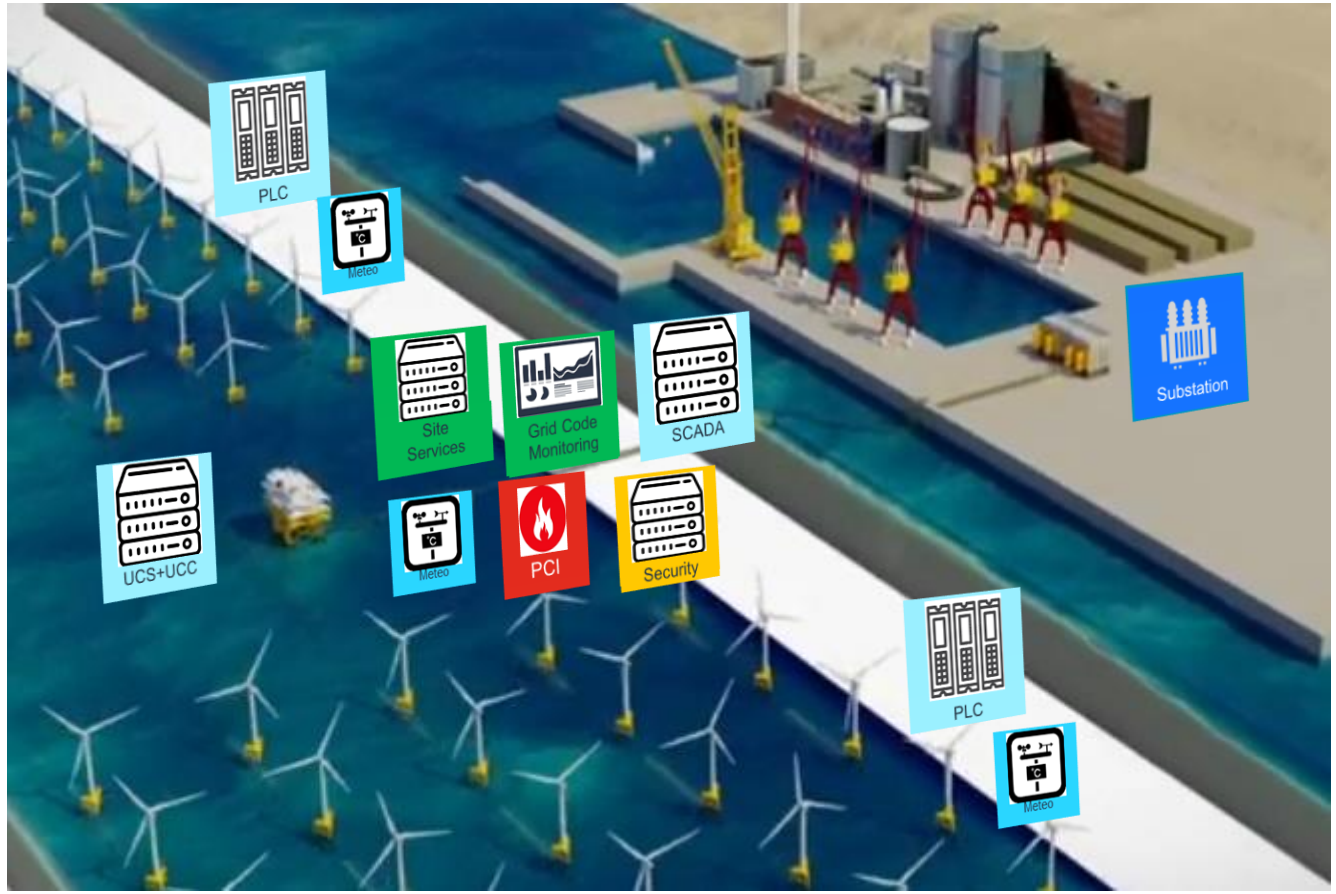
Retos y Soluciones de Ciberseguridad en el Sector Eólico

November 2021

Agustin Valencia Gil-Ortega

Operational Technology IBERIA

Ejemplo – Eólica Marina



Diversidad de Fabricantes

Dificultades Múltiples

Construcción, PeM, O&M

Operación remota

Sensórica y Datos!

Puntos de fallo intermedios

Conexiones Fabricantes

Escritorios remotos, gestión de accesos!

Retos

Organización

- Coordinación para O&M y ante amenazas?
- Preparación para responder a Incidentes?

IT-OT-Suministradores

Disponibilidad y Seguridad

- Obsolescencia? Diversidad de Fabricantes?
- Ransomware?

Digitalización

- Control de las arquitecturas y las Comunicaciones añadidas?
- Control de la sensórica añadida? Conexión a la Nube?

Proveedores (3rd Party)

- Cuántos Usuarios acceden a la infraestructura? A cualquier activo?
- Tenemos trazabilidad de los cambios?

Ransomware en OT!

X10 en 1 año!

Energy & Utilities en el top!

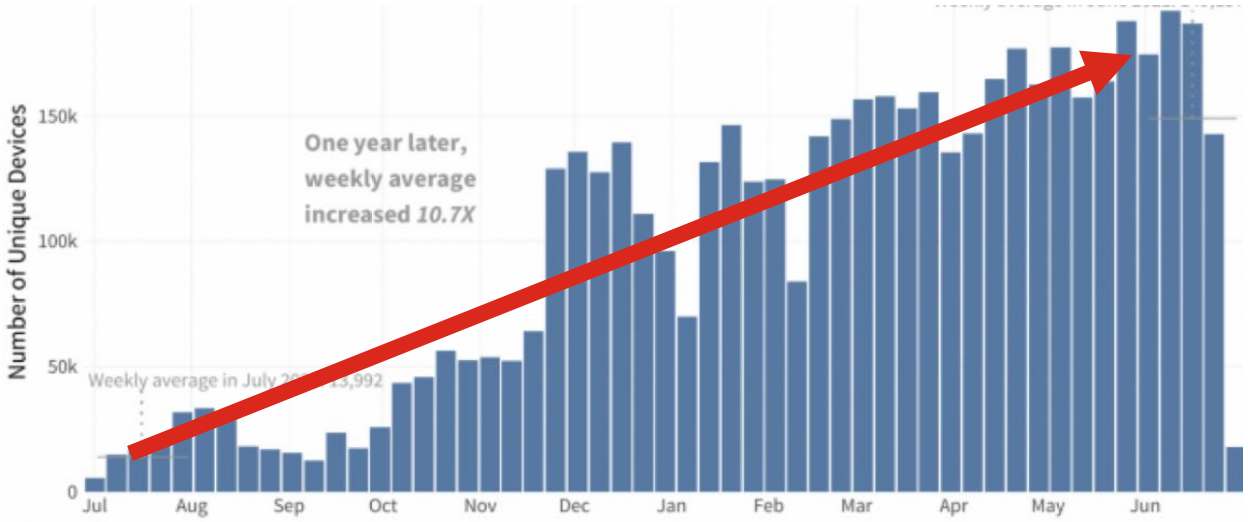


Figure 9: Growth in ransomware detections over last 12 months (Jul '20 - Jun '21).

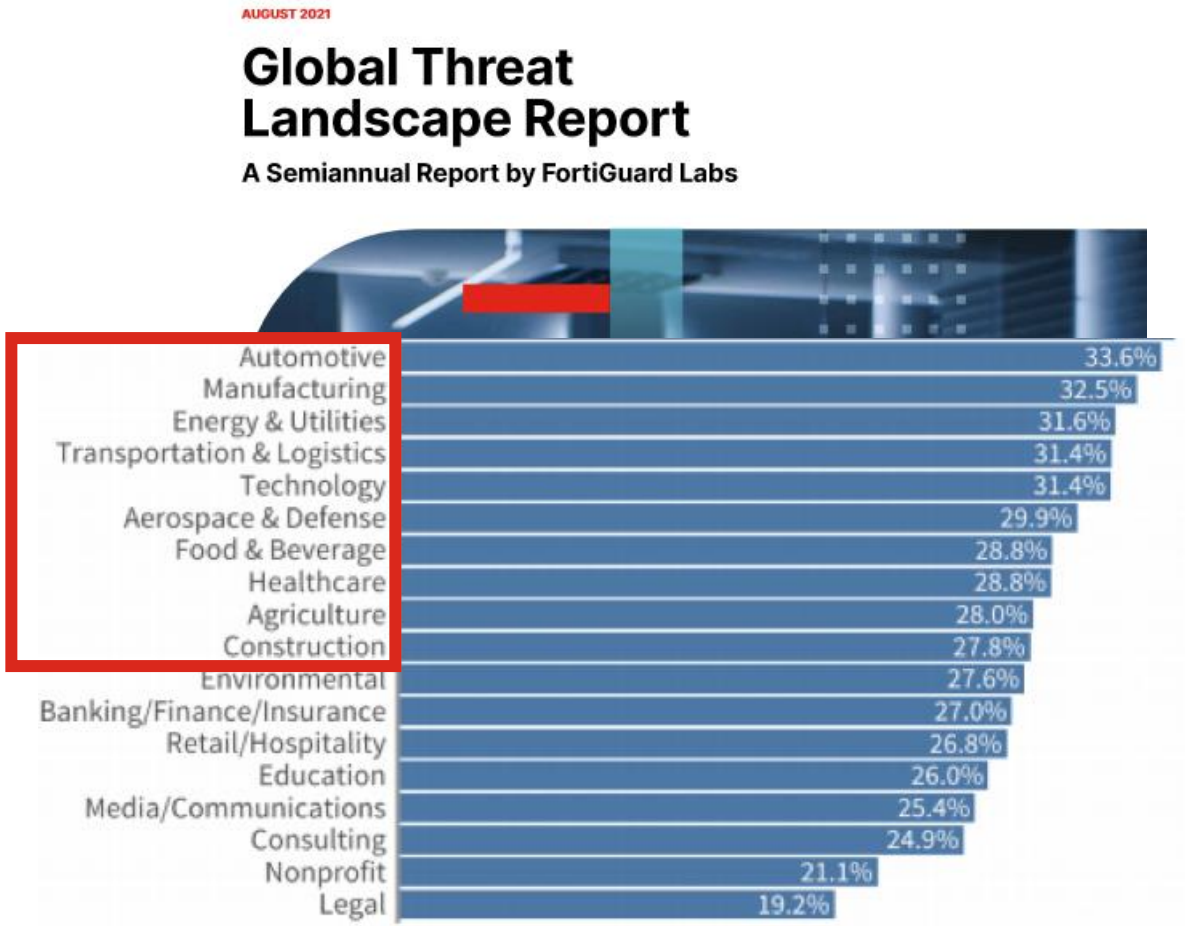
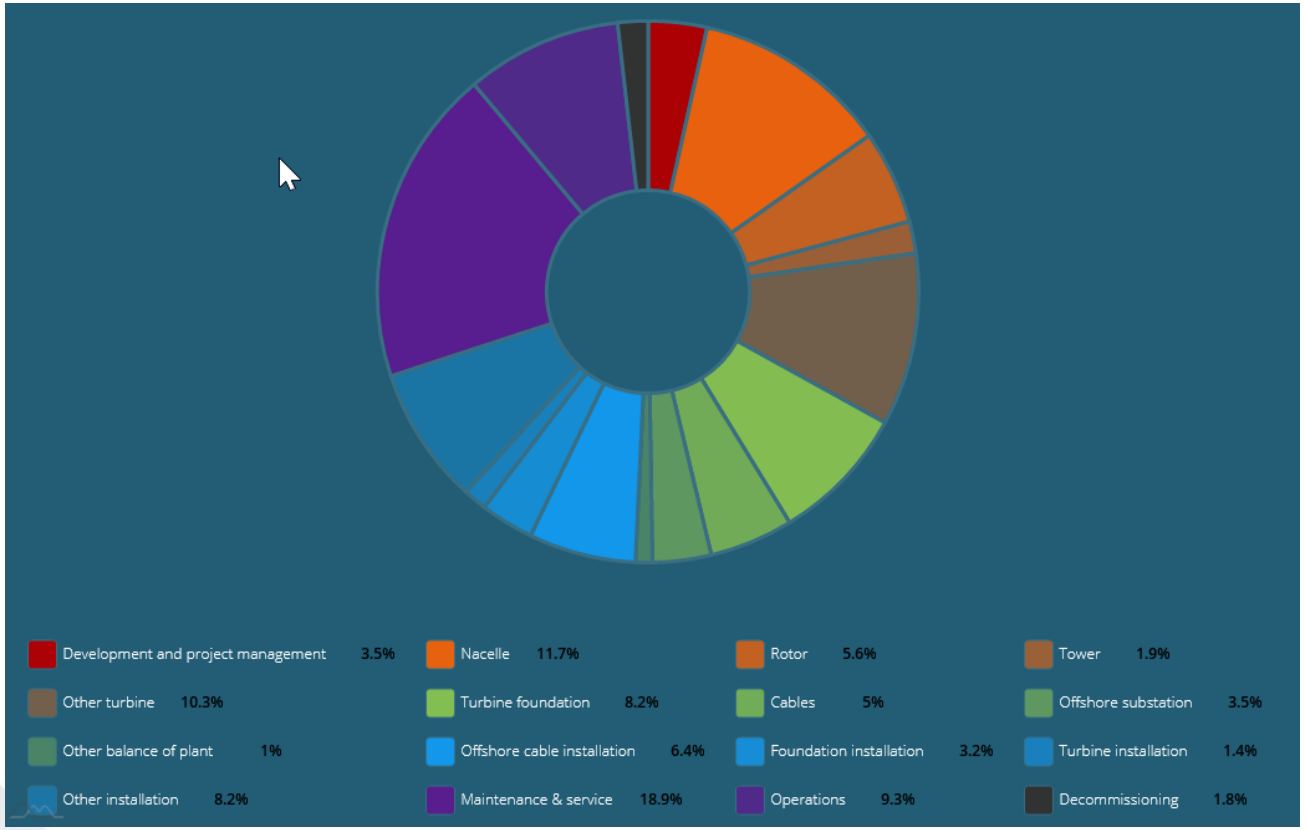


Figure 10: Prevalence of ransomware detections across sectors in 1H 2021.

Costes vs Riesgos

Cybersecurity Costs for an Offshore Windfarm? <0,1%

https://guidetoanoffshorewindfarm.com/wind-farm-costs

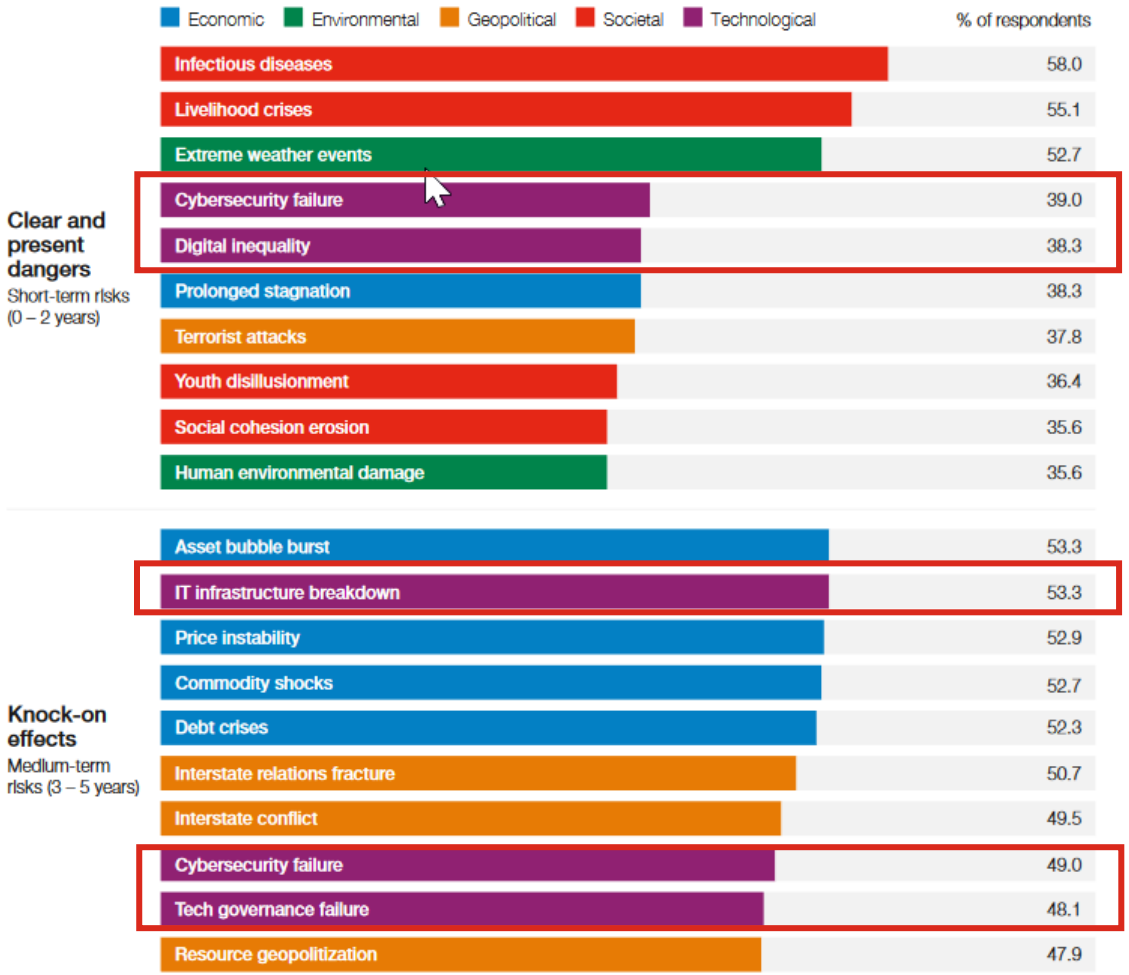


Cybersecurity Risks?

The Global Risks Report 2021

Global Risks Horizon

When do respondents forecast risks will become a critical threat to the world?



Resiliencia – Arquitecturas Seguras

Tolerante a fallos únicos

Alta Disponibilidad

Organizaciones Implicadas

Segmentación

Microsegmentación

Convergencia Comunicaciones

Visión completa Ciberseguridad

Criterios de Redundancia

Procesos/Activos Críticos
Comunicaciones

Criterios de O&M

Mínima Exposición
Acceso Remoto Seguro
Actualizaciones

Criterios de Pérdida máxima

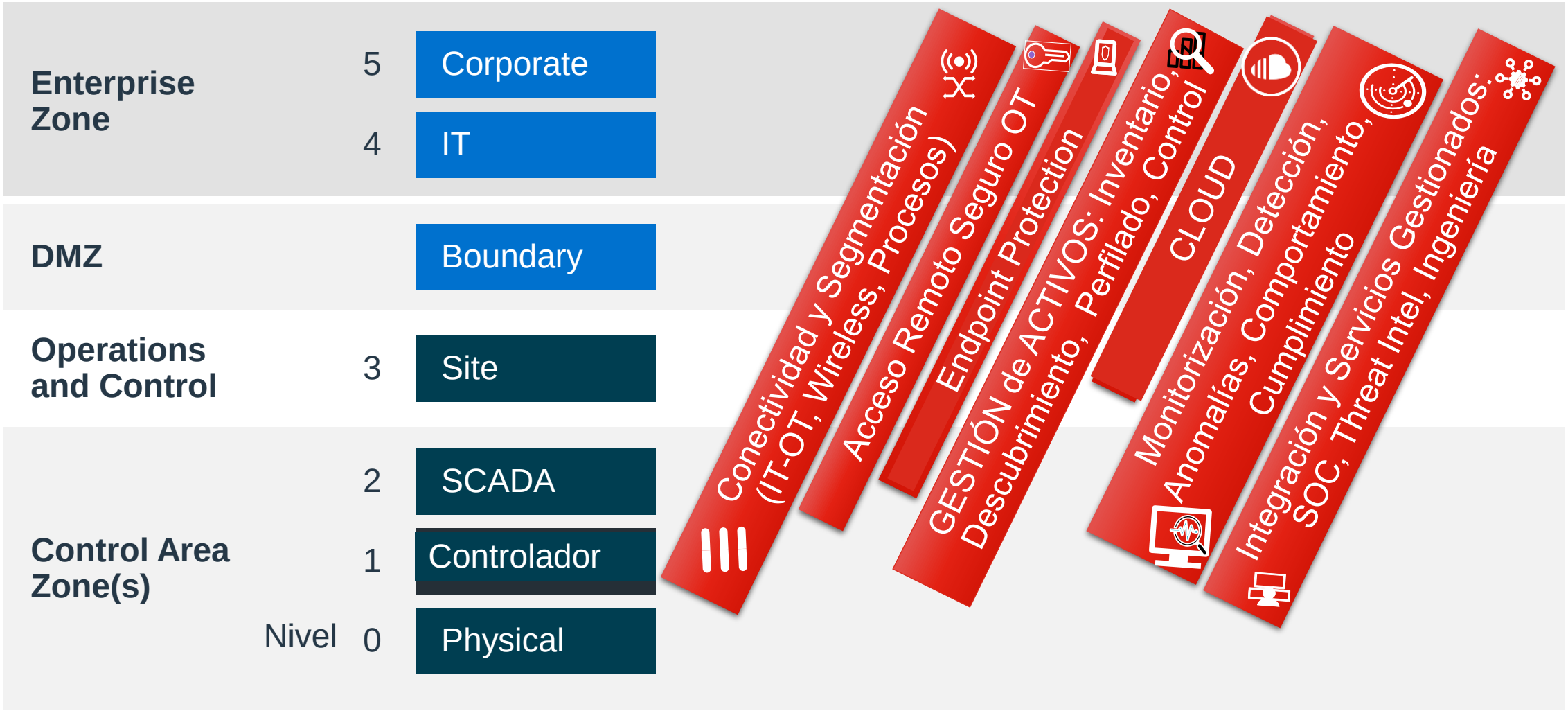
Turbinas/Ramales
Compromiso equipos vulnerables
Dispersión de Malware

Zero Trust!

Seguridad embedida en comunicaciones

Estándares de Referencia ➔ IEC 62443 3-2 *//* NIST 800-82

Visión Completa de la Seguridad

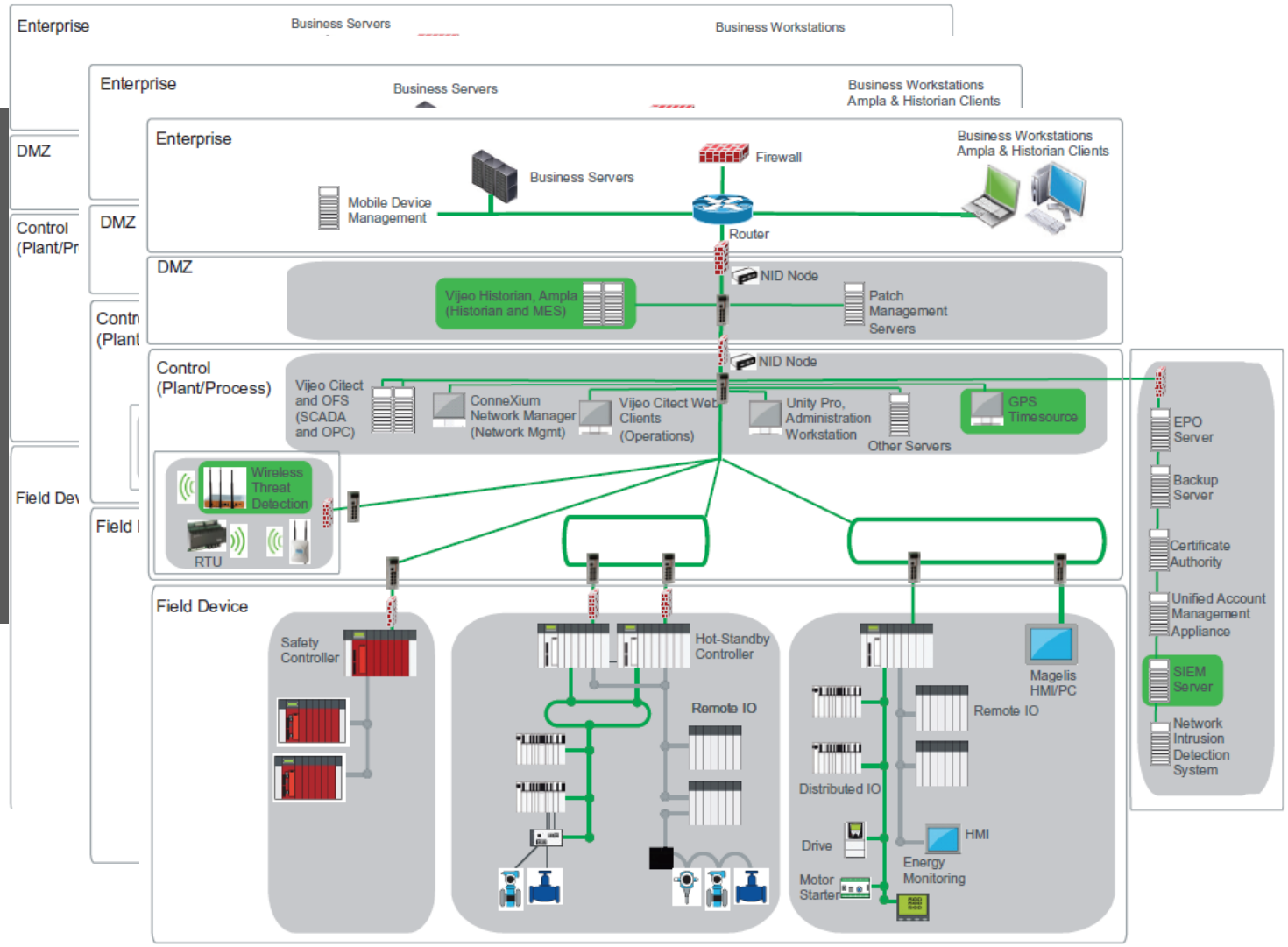


Para referencia

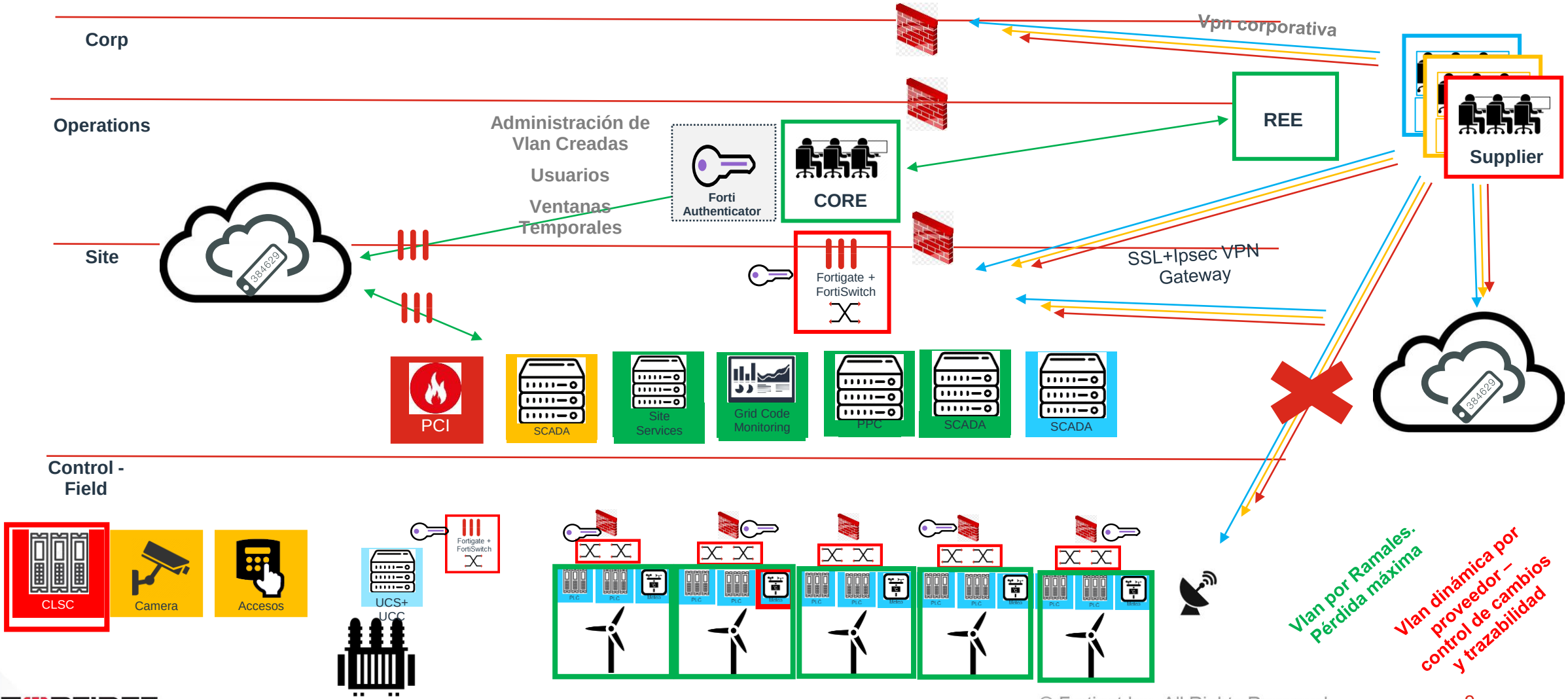
Controles Técnicos Según Niveles de Seguridad

Pilares IEC-62443

- 1. Identification and authentication control (IAC)
- 2. Use control (UC)
- 3. System integrity (SI)
- 4. Data confidentiality (DC)
- 5. Restricted data flow (RDF)
- 6. Timely response to events (TRE)
- 7. Resource Availability (RA)



Arquitectura Planta Eólica



Vulnerabilidades y Obsolescencia

IPS
Virtual Patching

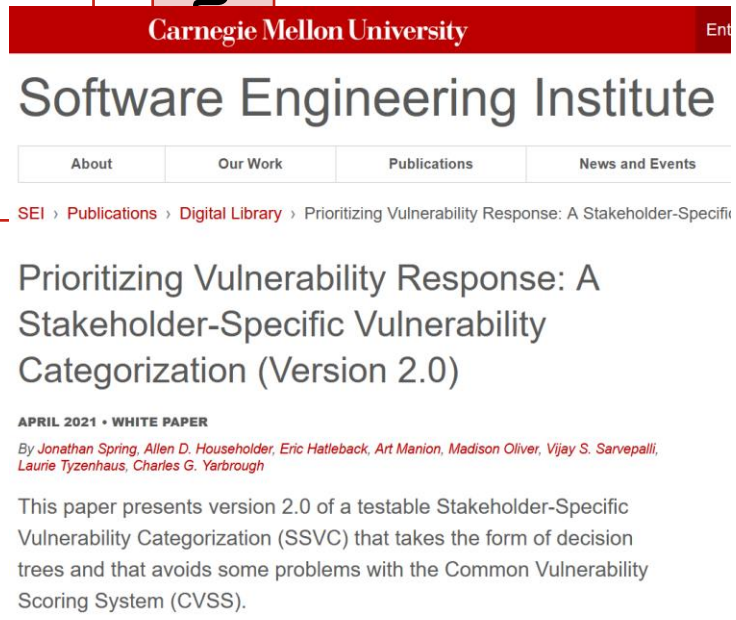
EDR

Ámbitos

- Sistema Operativo
- Aplicaciones
- Hardware
- Comunicaciones
- Arquitecturas

Controles y Mitiga

- Visibilidad
- Monitorización
- Parcheo Virtual
- Inteligencia de Amenazas


Carnegie Mellon University

Software Engineering Institute

About | Our Work | Publications | News and Events

SEI › Publications › Digital Library › Prioritizing Vulnerability Response: A Stakeholder-Specific

Prioritizing Vulnerability Response: A Stakeholder-Specific Vulnerability Categorization (Version 2.0)

APRIL 2021 • WHITE PAPER

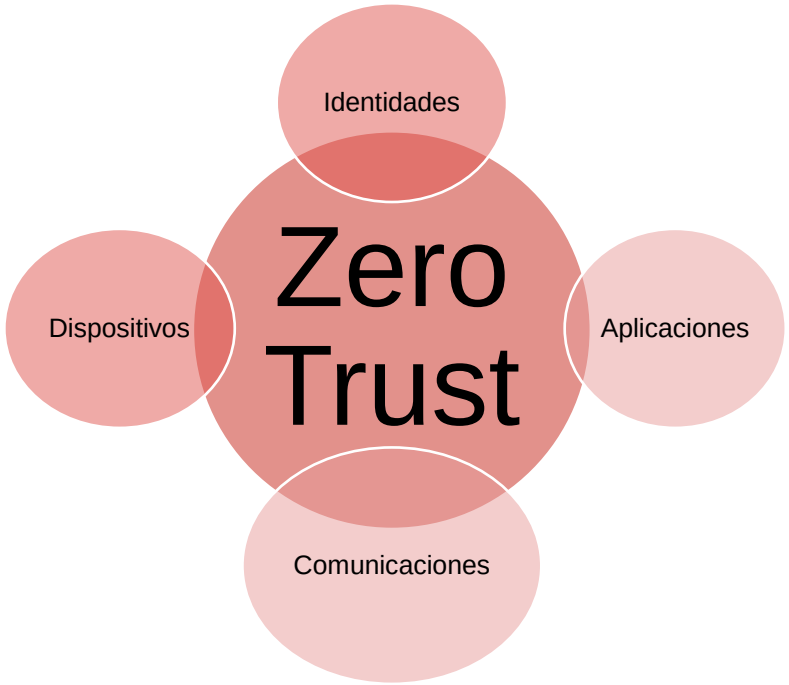
By Jonathan Spring, Allen D. Householder, Eric Hatleback, Art Manion, Madison Oliver, Vijay S. Sarvepalli, Laurie Tyzenhaus, Charles G. Yarbrough

This paper presents version 2.0 of a testable Stakeholder-Specific Vulnerability Categorization (SSVC) that takes the form of decision trees and that avoids some problems with the Common Vulnerability Scoring System (CVSS).

¿Publicación de Vulnerabilidades vs Capacidad de Parcheo?

Estrategias de Priorización? ➔ Inventario y Criticidad

3rd Party Threats – Control de Accesos



Control de Accesos

Authentication

Control Identidades

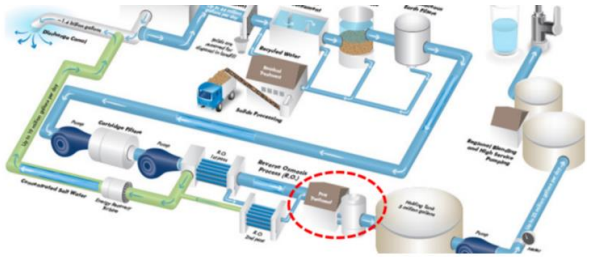
AD

Azure AD

Cert Authority

Control de Dispositivos

NAC



Oldsmar, water treatment and why cybersecurity is so important

Control de Comunicaciones
Control de Aplicaciones

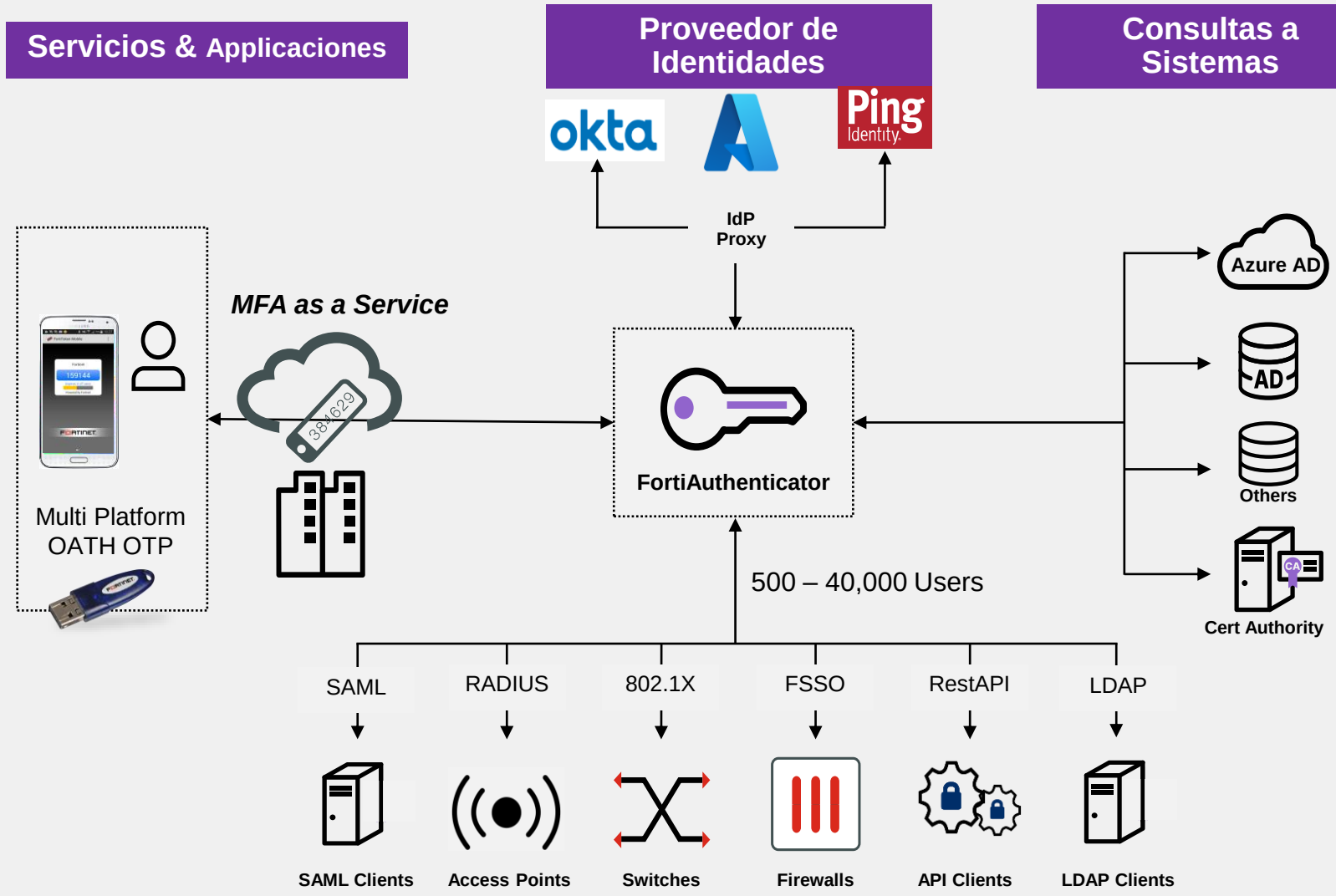
NGFW

EDR

WiFI AP

Switch

Acceso Remoto Seguro



Zero Trust Access

- **Gestión Centralizada**
- Interfaz fácil de usar y portal de autoservicio
- **Identidades, Accesos, Multiplataforma**
- **Control Basado en Roles –RBAC- (Employee, Guest, Partners, etc.) y Acceso Remoto**
- **MFA multiplataforma,** Adaptable y “As-a-Service”
- Single-Sign-On, Fortinet SSO and Web SSO
- **Acceso Temporizado**
- Gestión de Ciclo de Vida de Certificados

Resiliencia – Integración en el Ciclo de Vida

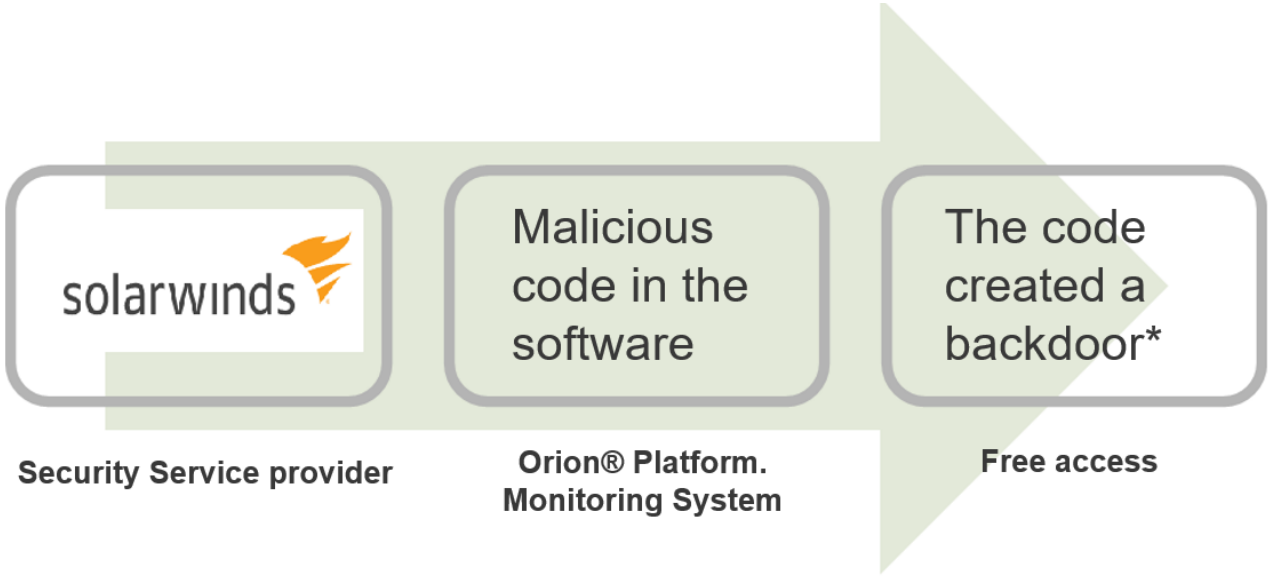
White Papers

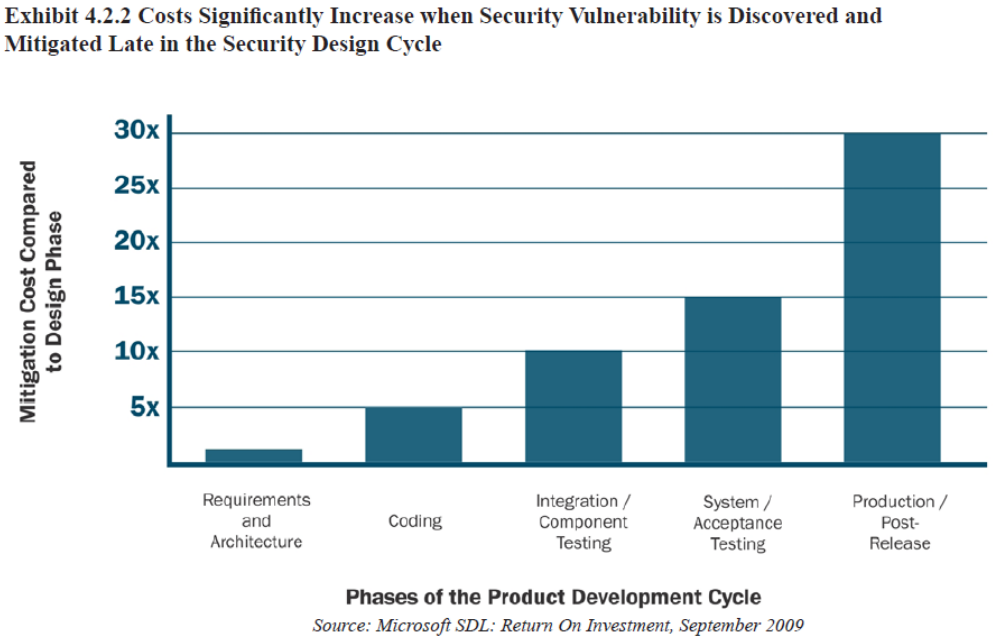
Published: 30 November 2020

Cyber Resilience in the Electricity Ecosystem: Securing the Value Chain

Value Chain	Product	Operations		
	PRODUCT SUPPLY	SOLUTION DESIGN	COMMISSIONING	OPERATIONS
ROLES[1]				
ASSET OWNER	*Opportunity to enhance the security of the overall process through dialogues with relevant stakeholders.*	2 Ensure security in environment & design	2 Ensure secure roll-out	3 Ensures security whether using internal or external resources to operate
SYSTEM INTEGRATOR		2 Ensure security in environment & design	2 Ensure secure roll-out	3 Ensure security as per contractual agreements
ASSET (LESS) OPERATOR				3 Ensure security as per contractual agreements
PRODUCT SUPPLIER	1 Product Design; 1 Development; 1 Manufacturing	OT support (including FAT); Ensure security in environment & design; Ensure secure roll-out; Primary Technology support (e.g. transformer)		4 OT support; Extended OT support; OT security contracts; Primary Technology support

3rd Party Threats – Control de Cambios



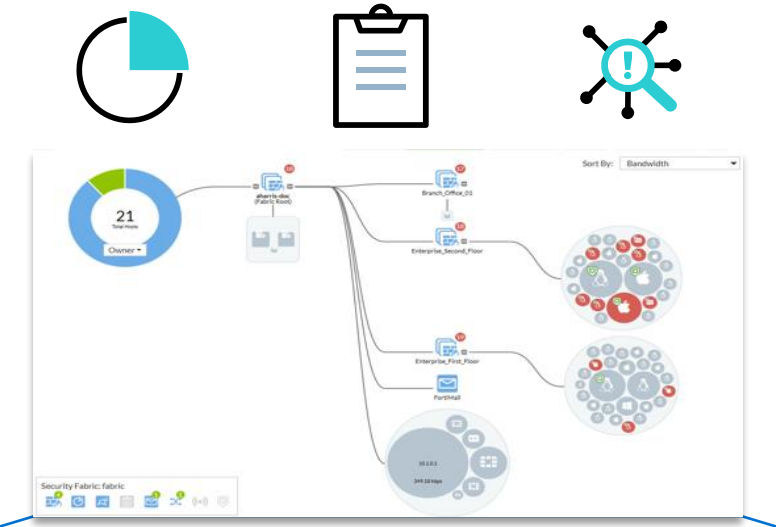


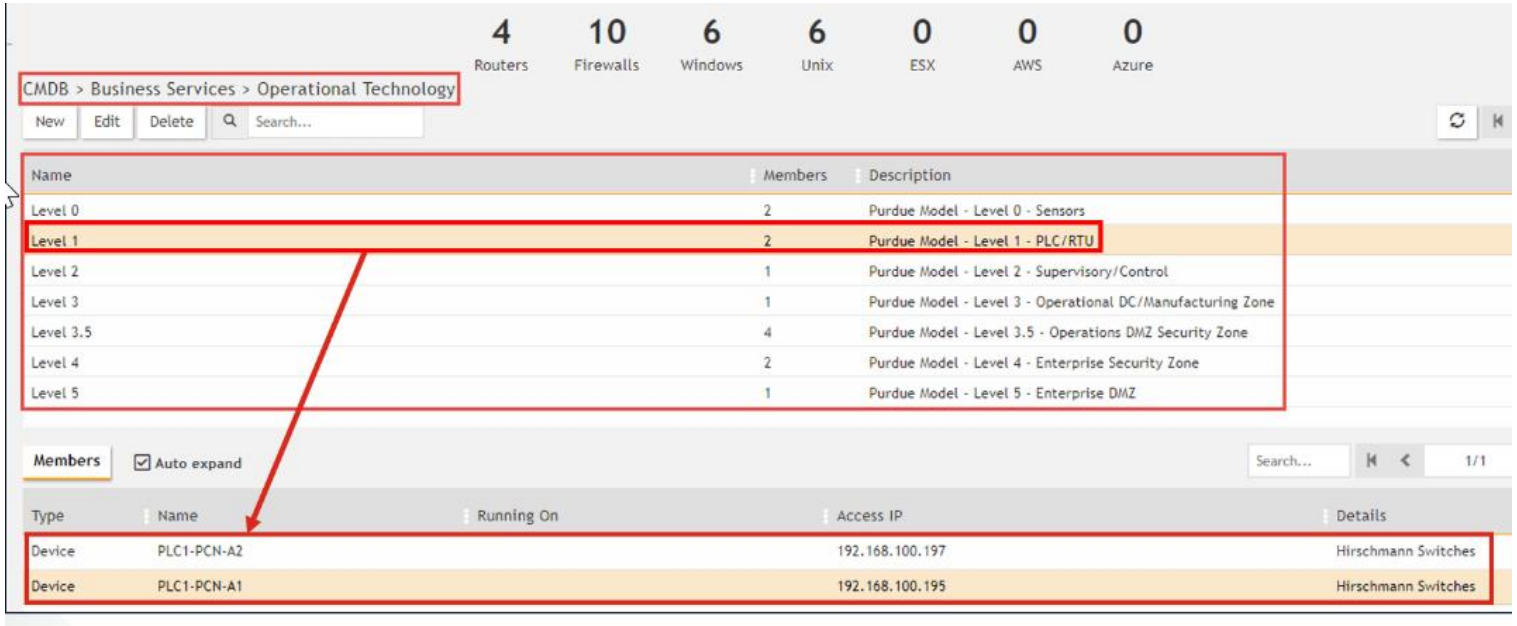
Proyecto	Commissioning	O&M

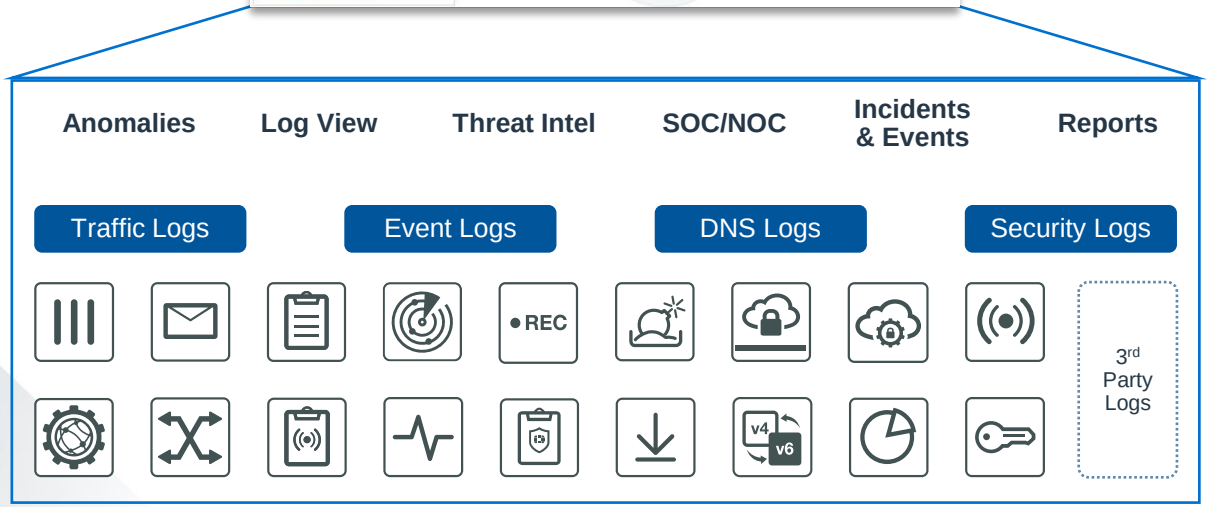
• Inventarios
  • Usuarios
  • Aplicaciones
  • Comunicaciones
• Herramientas Seguridad
	• Verificación
	• Revocación credenciales
	• Documentación “As-Left”
		• Mecanismos de Control de Acceso
		• Descubrimiento de Activos
		• Monitorización y Detección
		• Auditorías

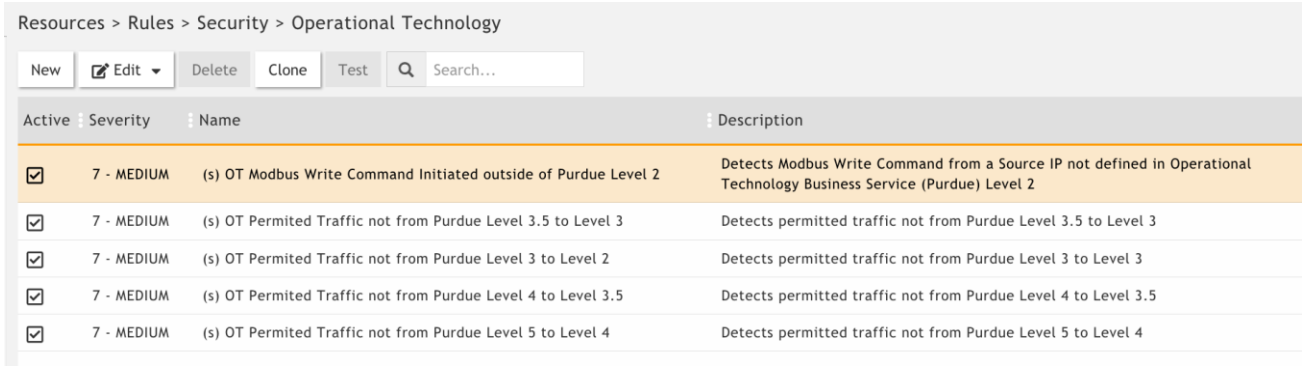
Centralización de Inventario, Logs y Monitorización OT

Para referencia



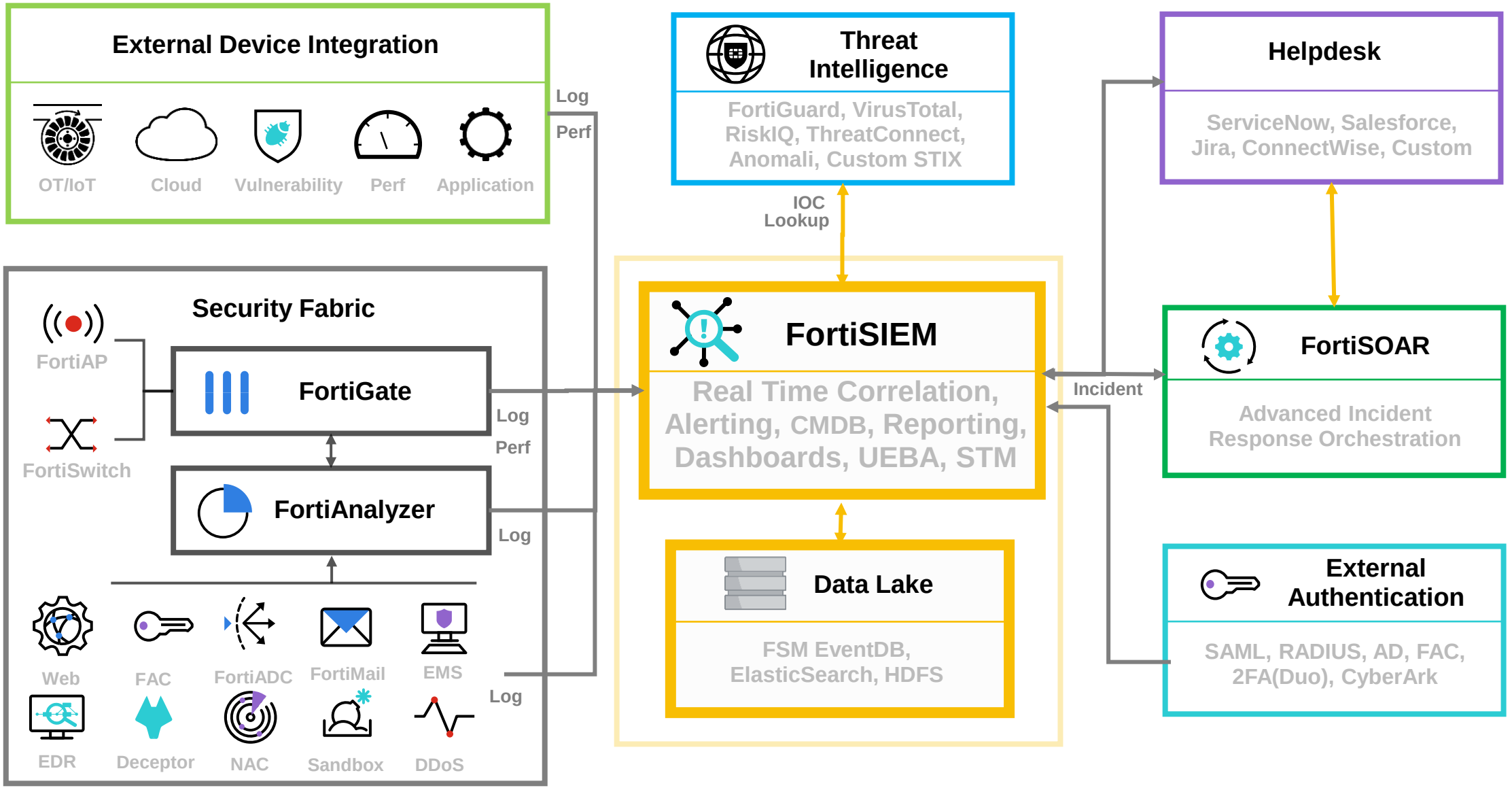






Detección e Inteligencia de Amenazas

Para referencia



Agustín Valencia Gil-Ortega
Business Development Manager
Operational Technology IBERIA
valenciaa@fortinet.com
https://ready.fortinet.com/ot
https://apps.kaonadn.net/516958160368435 2/index.html