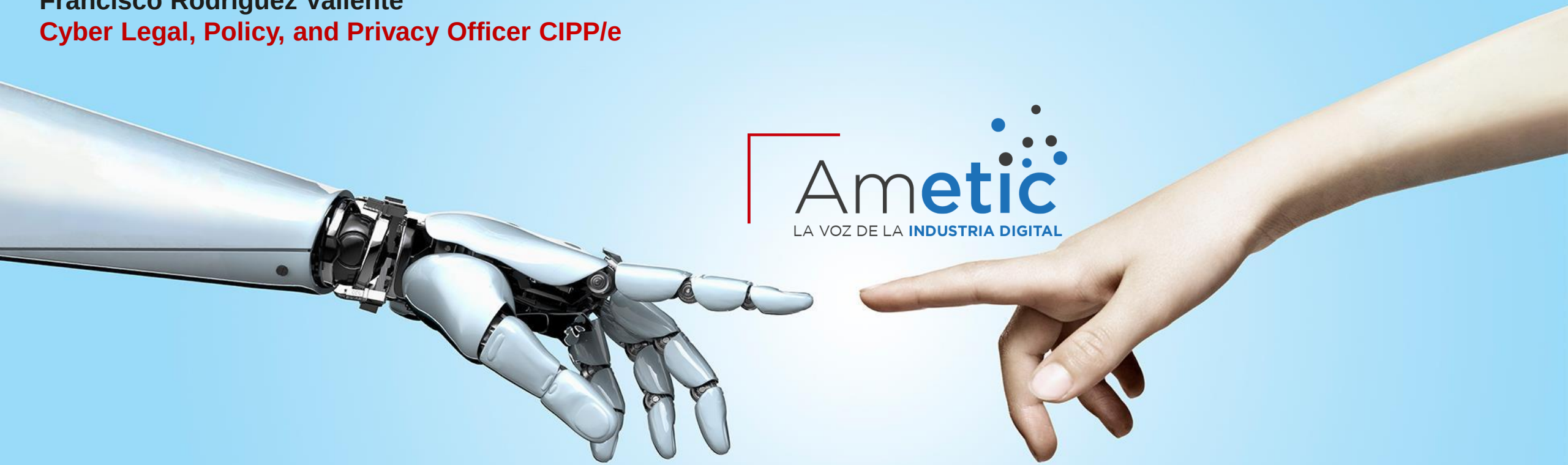
Buenas prácticas de la ciberseguridad Española
Contribución al desarrollo de talento y conocimiento

Francisco Rodríguez Valiente
Cyber Legal, Policy, and Privacy Officer CIPP/e



Ametic
LA VOZ DE LA INDUSTRIA DIGITAL

universidad de león

HUAWEI

Centro de Experiencia en Ciberseguridad de Huawei en la Universidad de León

Ametic
LA VOZ DE LA INDUSTRIA DIGITAL

HUAWEI

MoU with University of León (ULE): increasing Cyber Security awareness and skills development

2023.01 — MOU Kick off ceremony

2023.04-05 — **Professional development:** **5G Security Training with attendees from ULE and other stakeholders**

2023.06 — **Security Operations drill** **5G Cyber Range event :** Spain CS stakeholders participation

2023.10 — **León CSEC opening (CS Experience Center)**

1) **First use case: "Securing 5G Private Networks" methodology: L1 and L2**
2) **Q&A for SME´s Cybersecurity whitepaper presented at ENISE**

2024 — **New workstreams**

universidad de león

Training Agenda: 6 days

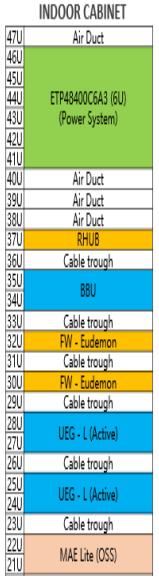
5G Cyber Security Concept and Industry Consensus Overview — 0.5 day
- 5G Cyber Security Development Trend

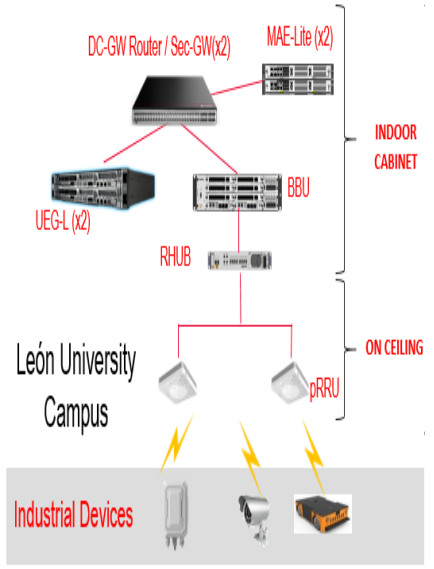
5G Cyber Security Standards and Certifications Interpretation — 1 day
- 3GPP 5G Security Standards
- NESAS&SCAS Security Certification Standards

5G Cyber Security Threat Analysis and Countermeasures Introduction — 1.5 days
- Overview of Network Security Threat Analysis Methods
- App and Service Security Threat Analysis and Countermeasures
- 5G Mobile Terminal Security Threat Analysis and Countermeasures
- 5G Wireless Access Network Security Threat Analysis and Countermeasures
- 5G Core Network Security Threat Analysis and Countermeasures
- 5G Cloud Infrastructure Security Threat Analysis and Countermeasures
- 5G Network Operation and Management Security Threat Analysis and Countermeasures

5G Cyber Security Solution Design — 3 days
- 5G RAN Security Solution
- 5G Core Security Solution
- 5G Cloud Infrastructure Security Solution
- 5G Network Slicing Security
- 5G MEC Security Solution
- 5G Communication Capability Exposure Security

5G MPN Laboratory for University of León

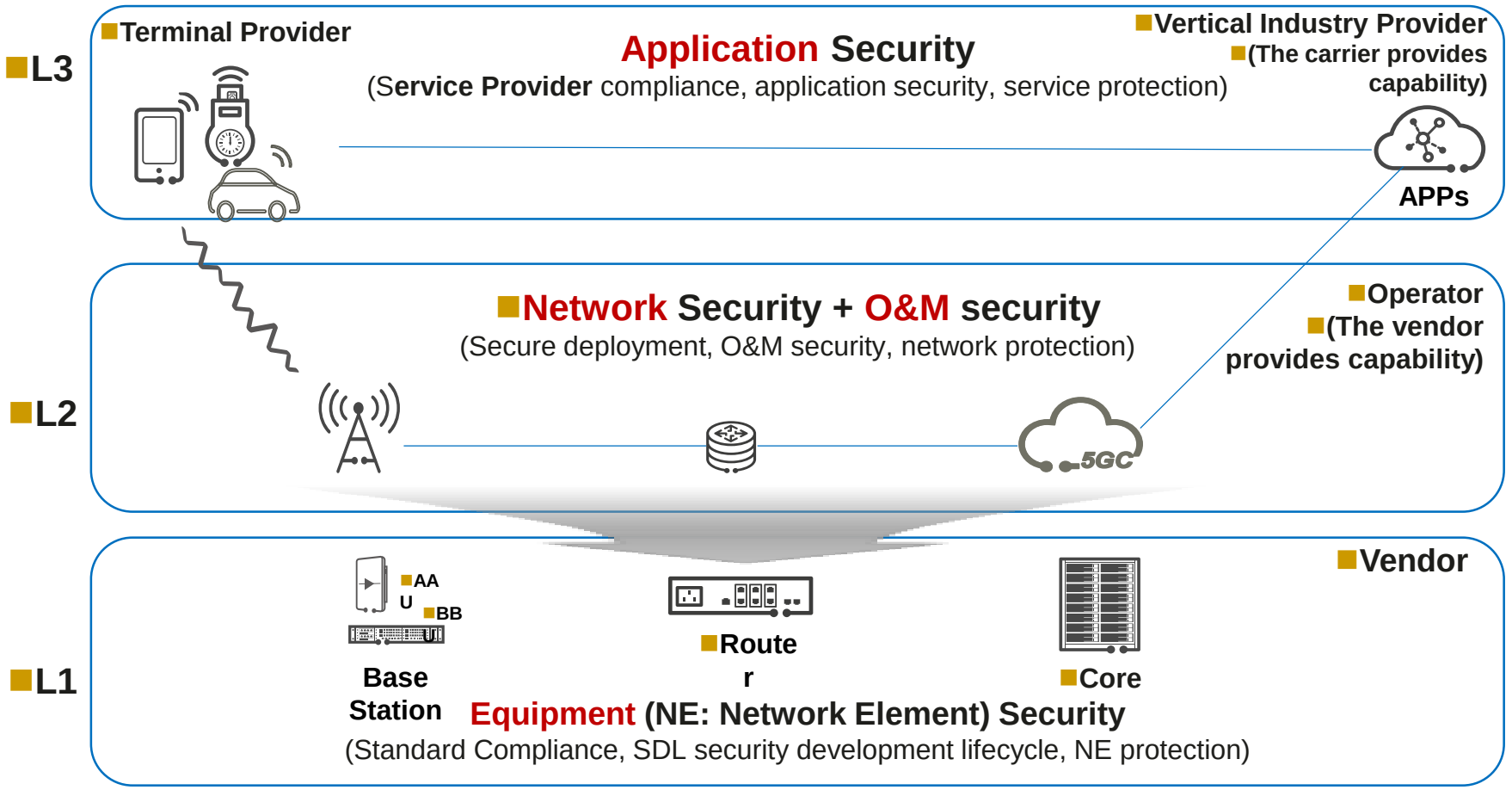




Ametic
LA VOZ DE LA INDUSTRIA DIGITAL

HUAWEI

Ciberseguridad E2E en 5G: modelo por capas aceptado por la industria



Estándares y metodologías en la industria

ISO/IEC 62443 IACS,
ISO/IEC 27034

NIST CSF,
NCSC CAF, 3GPP,
GSMA 5G CKB
(5G Cybersecurity Knowledge Base)

ISO19600, NIST SSDF,
NIST SP800-160, 3GPP,
GSMA NESAS / 3GPP SCAS
(Network Equipment Security Assurance Scheme /
SeCurity Assurance Specification

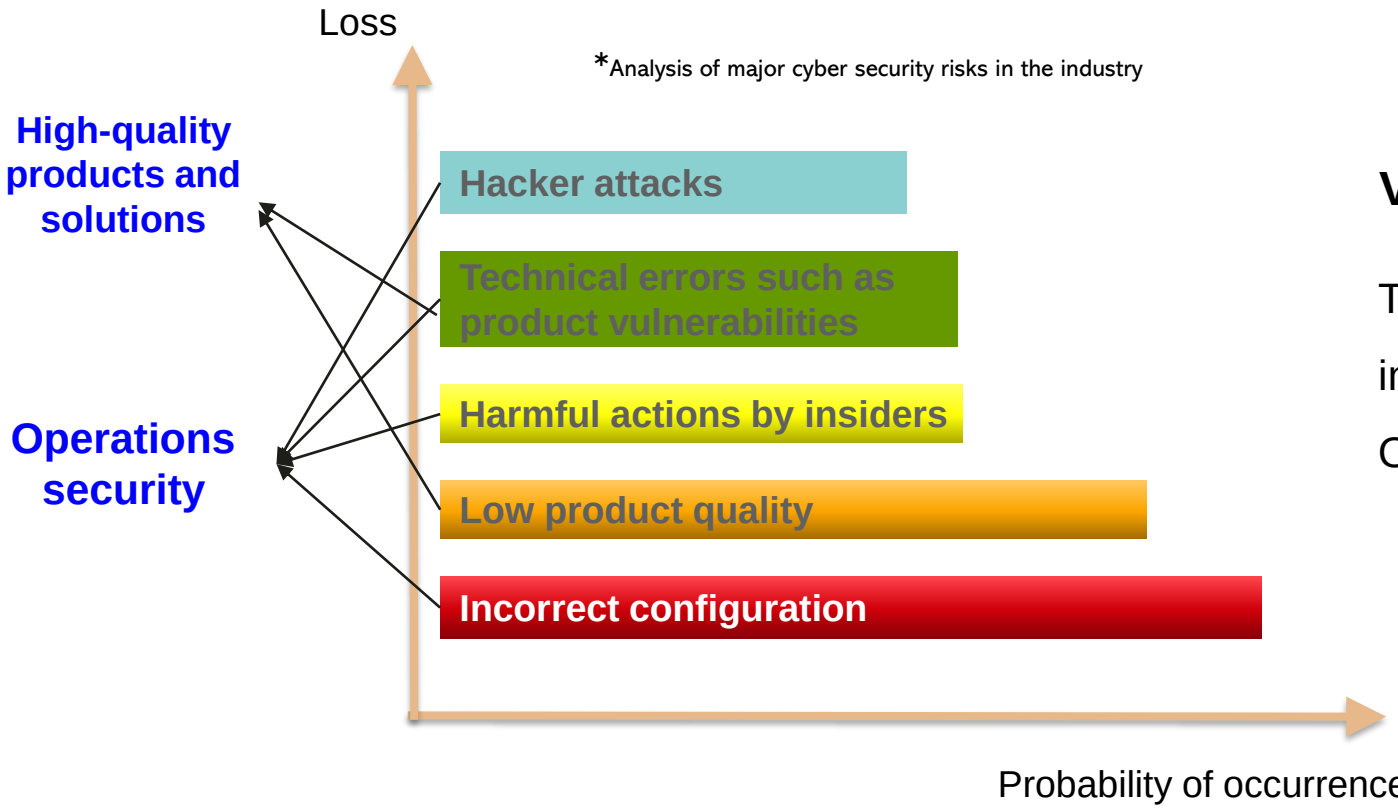
El modelo de seguridad por capas es ampliamente aceptado en la industria de las telecomunicaciones.

La seguridad en redes 5G se sustenta en la "responsabilidad compartida" entre los diferentes actores.

Ametic
LA VOZ DE LA INDUSTRIA DIGITAL

HUAWEI

¿Qué hace a una red insegura?



Viewpoints of the security industry:

To ensure cyber security across the industry, it is necessary to focus on both O&M security and product security.

Network operators shall first consider purchasing **high-quality and secure products** and then pay attention to the **secure operations of equipment**, including correct security configuration and prompt vulnerability remediation.

Ametic
LA VOZ DE LA INDUSTRIA DIGITAL

HUAWEI

Security Configuration Check Tool (5G RAN Base Station):

Helps Customers Implement Baseline Management More Conveniently and Intelligently

GSMA

Cyber Security Knowledge base

Flexible and customizable Baseline management

Manually configured based on network requirements

Auto Fast Identify risks.

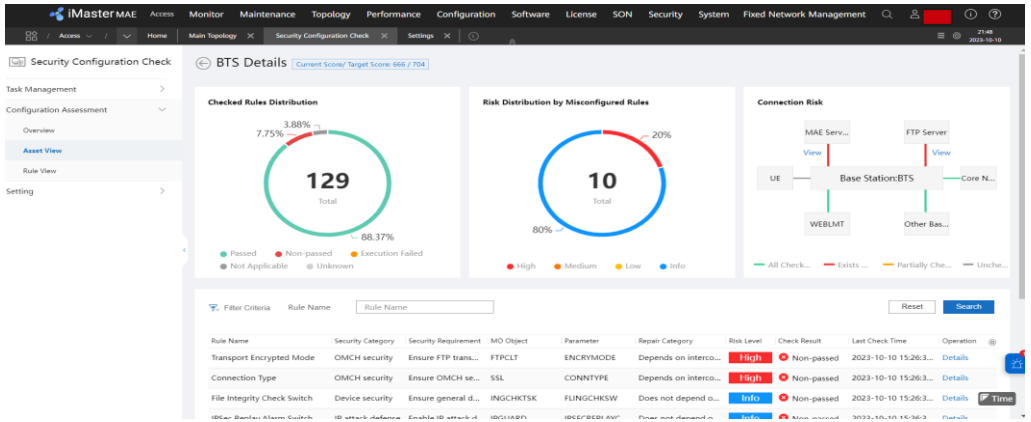
Automatic check, minute-level/10,000 base stations

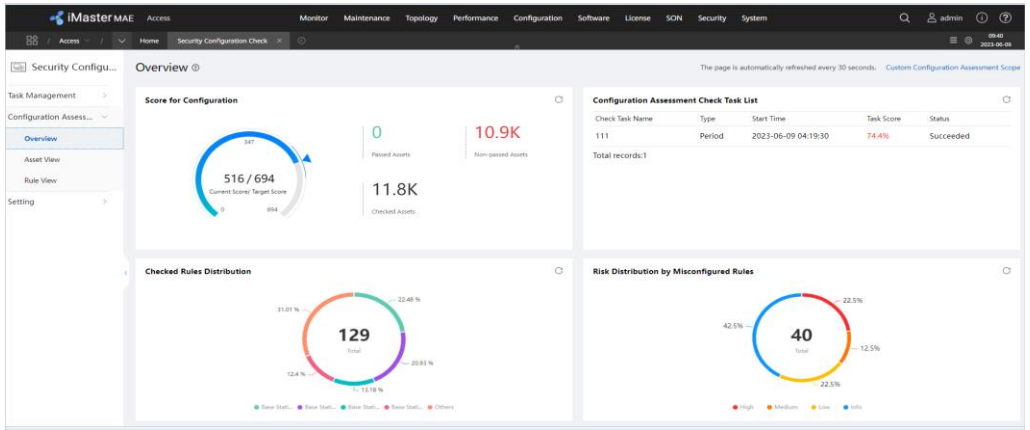
multi-dimensional Risk Quantification

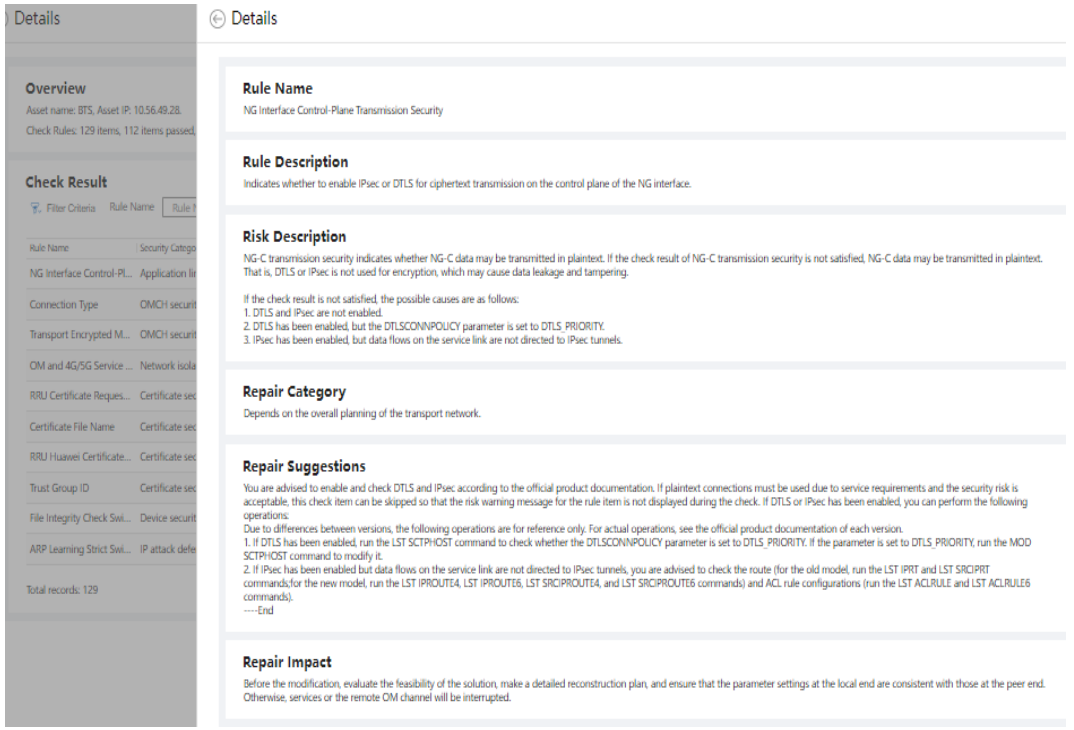
Automatically displaying check results

Precise risk Closed-loop guidance

Manually fix the problem according to the customer's process.







Ametic
LA VOZ DE LA INDUSTRIA DIGITAL

HUAWEI

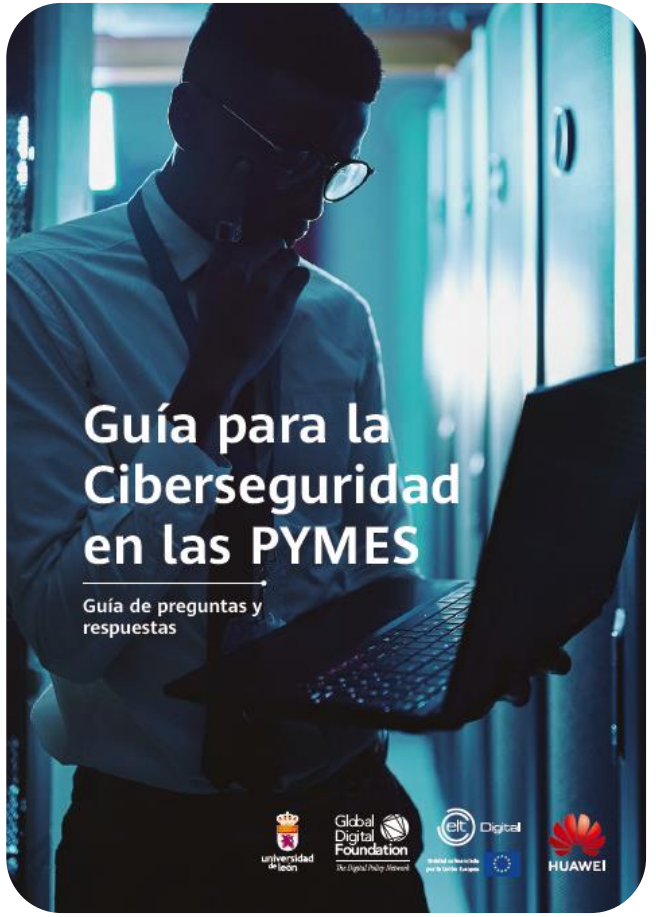
Guía para la Ciberseguridad en las PYMES (SME)

Ametic
LA VOZ DE LA INDUSTRIA DIGITAL

HUAWEI

¿Por qué las PYMES (SME) son tan importantes?

■ **Ciberseguridad de la cadena de suministro:** **Resistencia de cada empresa, producto o servicio que interviene en la entrega de un producto o solución al usuario final.**



https://www.huawei.com/-/media/corporate/local-site/es/pdf/guia-de-ciberseguridad-para-pymes-huawei.pdf?la=es

Guía para la Ciberseguridad en las PYMES: Debilidades de las PYMES

Desafíos

Inversión

Falta de cualificación y competencia

El factor humano

La importancia de la formación se debe a que el 82% de las brechas ocurren como resultado de un error humano.

82%
Consecuencia de errores humanos

Ciber-resiliencia en la UE

2021

1,0%

Los ataques a la cadena de suministro representan solo el 1% de todos los ciberataques.

2022

17,0%

Los ataques a la cadena de suministro representan el 17% de todos los ciberataques.

[1] https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes
[2] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

01
Cifrado, robo o modificación de la información, por ejemplo, para pedir un rescate o revender los datos.

02
Supervisión de los flujos de datos, por ejemplo, en beneficio del atacante.

03
Tomar el control de un dispositivo, por ejemplo, para provocar un incidente.

Guía para la Ciberseguridad en las PYMES: ¿Qué se puede hacer?

Identificar procesos y recursos críticos de la empresa (Riesgos)

Implantar medidas de seguridad

- Control de acceso estricto, gestión segura de contraseñas
- Gestión vulnerabilidades
- Copia de seguridad de los datos
- Instalación y mantenimiento de cortafuegos
- Acceso Wifi protegido
- Redes privadas (VPN)

Herramientas y dispositivos

Planes de recuperación y de comunicación

Dirección

Reconocer

Amenazas

- DDOS
- Malware
- Phishing
- Ransomware

Qué hacer

¿Cuál es la política de la UE y España en materia de apoyo a las PYMES desde el punto de vista de la ciberseguridad?

Regulación

- Cyber Security Act
- Directiva NIS2
- Cyber Resilience Act

Inversión Europa y España

INVEST EU

HORIZONTE EUROPA

€10 bil

La UE ha asignado 10.000 millones de euros para acciones de colaboración en materia de ciberseguridad dentro del programa de investigación, innovación y ciencia Horizonte Europa 2021-2027.

España | digital 2026

Activa Ciberseguridad

https://www.industriaconectada40.gob.es/programas-apoyo/Paginas/ACTIVA-Ciberseguridad.aspx

KIT DIGITAL

https://www.red.es/es/iniciativas/proyectos/kit-digital

Organismos de Referencia

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD