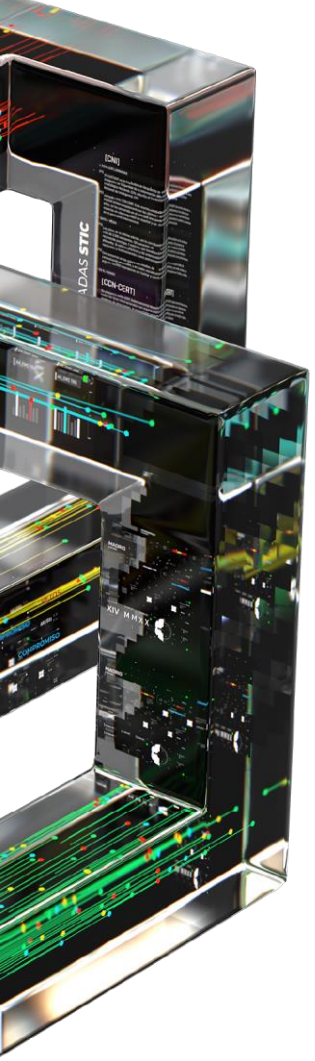
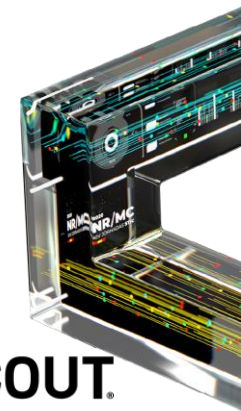


#XIVJORNADASCCNCERT

“PROTECCIÓN, ANÁLISIS Y CUMPLIMIENTO DE LOS ACTIVOS DE REDES INDUSTRIALES BASADO EN ESTADO DE COMPORTAMIENTO DE LA RED”



cn-cert
centro criptológico nacional

FORESCOUT



Miguel Ángel Rodríguez Fernández

FORESCOUT TECHNOLOGIES

miguel.fernandez@forescout.com

UNIR Universidad Internacional de La Rioja
Master of Engineering - MEng, INDUSTRY 4.0
2020 – 2022

Universidad Pontificia Comillas
Bachelor of Science (BS), Computer Science
1990 – 1995

CWNP
CWNA (wifi administrator)

Cisco Networking Academy
CCDP

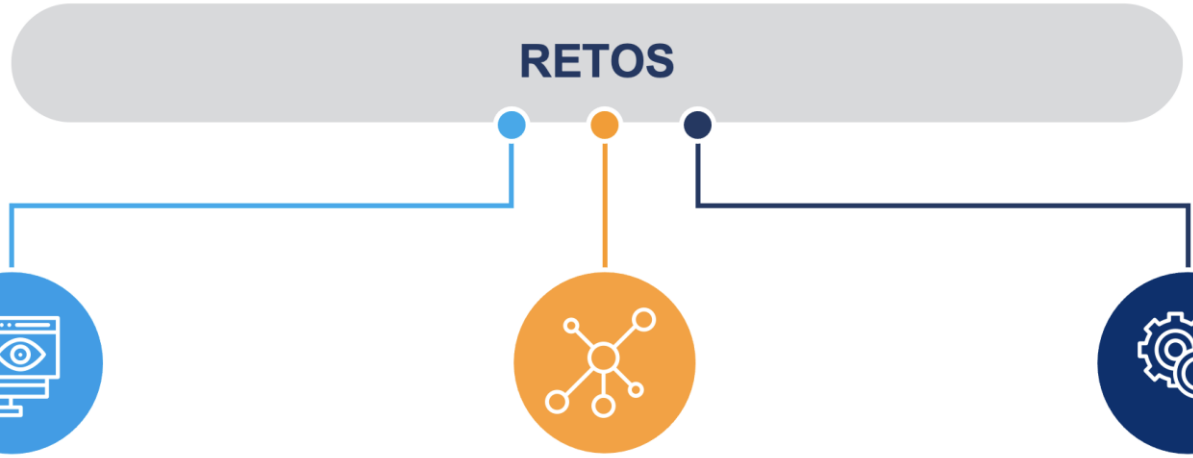
Cisco Networking Academy
CCNP ROUTING

ESCUELAS PIAS
Bachillerato

JUNIPER NETWORKS
JNCIS Security

Juniper networks
JNCIS Routing switching

Retos de Ciberseguridad y otros en el mundo Industrial.



Ciberseguridad

- Poca Visibilidad en Redes OT
- Incapacidad de. Discriminar si los Sistemas son Vulnerables.
- Demasiados Logs y Alarmas para correlacionar.
- Complejidad de Integración con otras Herramientas de Gestión (SIEM).
- Diferentes herramientas y personal poco experto
- Soluciones de seguridad IT y con estrategias de integración de adquisiciones.

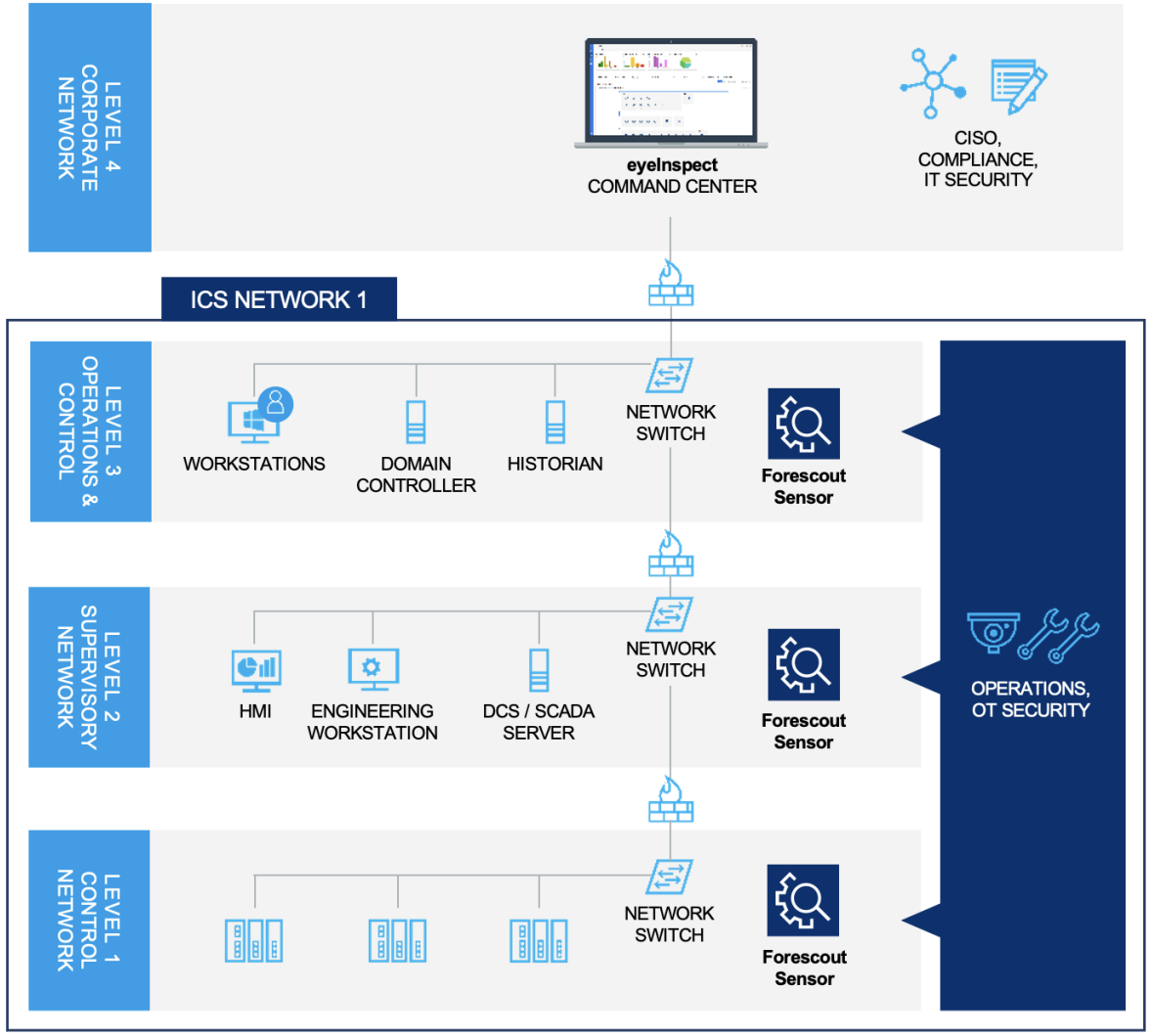
Infraestructura

- No hay claro conocimiento de los dispositivos OT en la red ni redes de mapas lógicos.
- Estrategia de Segmentación limitada.
- Incapacidad de comprender los paquetes/flujos de tráfico.
- Cumplimiento del dispositivo.
- FW/Switch cumplen la norma ??

Operaciones

- Capacidad de monitorización y Cumplimiento escaso.
- Inventariado de red no en tiempo real.
- Seguimiento de firmware y CVE de fabricante del dispositivo.
- OPEX elevado por visitas en tiempo real a las plantas.
- No se controla el acceso de la red.

Resolución de los Retos de Ciberseguridad.



COMPLETA VISBILIDAD DE LOS DISPOSITIVOS

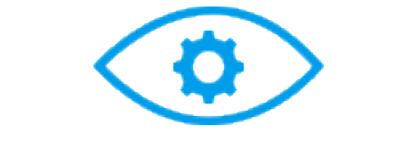
- ✓ Visualización de los dispositivos y flujos de Comunicación.
- ✓ Recogida de la información complete de los dispositivos.
- ✓ Monitorización y Gestión del Inventario.

GESTION Y CONFIGURACION DEL INVENTARIO

- ✓ Agrupación de Dispositivos y clasificación base.
- ✓ Análisis de impacto de Alertas a los dispositivos.
- ✓ Automatización de Tareas de Cumplimineto.

INTEGRACIÓN ATRAVES DE LA. ORGANIZACIÓN.

- ✓ SEGMENTACION BASADA A NIVEL DE POLITICAS
- ✓ INTEGRACIÓN DE ANÁLISIS DE FLUJOS DE TRÁFICO (NetFlow, SPAN, etc.)
- ✓ INTEGRACIÓN Y CONTROL DE POLÍTICAS DE PROTECCIÓN.



ICS/OT DETECCIÓN DE AMENAZAS

EL INVENTARIADO DE DISPOSITIVOS Ofrece miles de indicadores cómo queries de amenzasa dentro de su ICS/OT.



OPTIMIZACIÓON Y ANÁLISIS DE RIESGO DE ACTIVOS OT.

SE AGREGAN MILES DE ALERTAS DE FORMA AUTOMATÍCA.



LANZAMINETO DE PRUEBA SOBRE GRUPOS DE DISPOSITIVOS

MEJORAS DE DETECCIÓN TIOS DE ACTIVOS ANALIZANDO SU HUELLA.



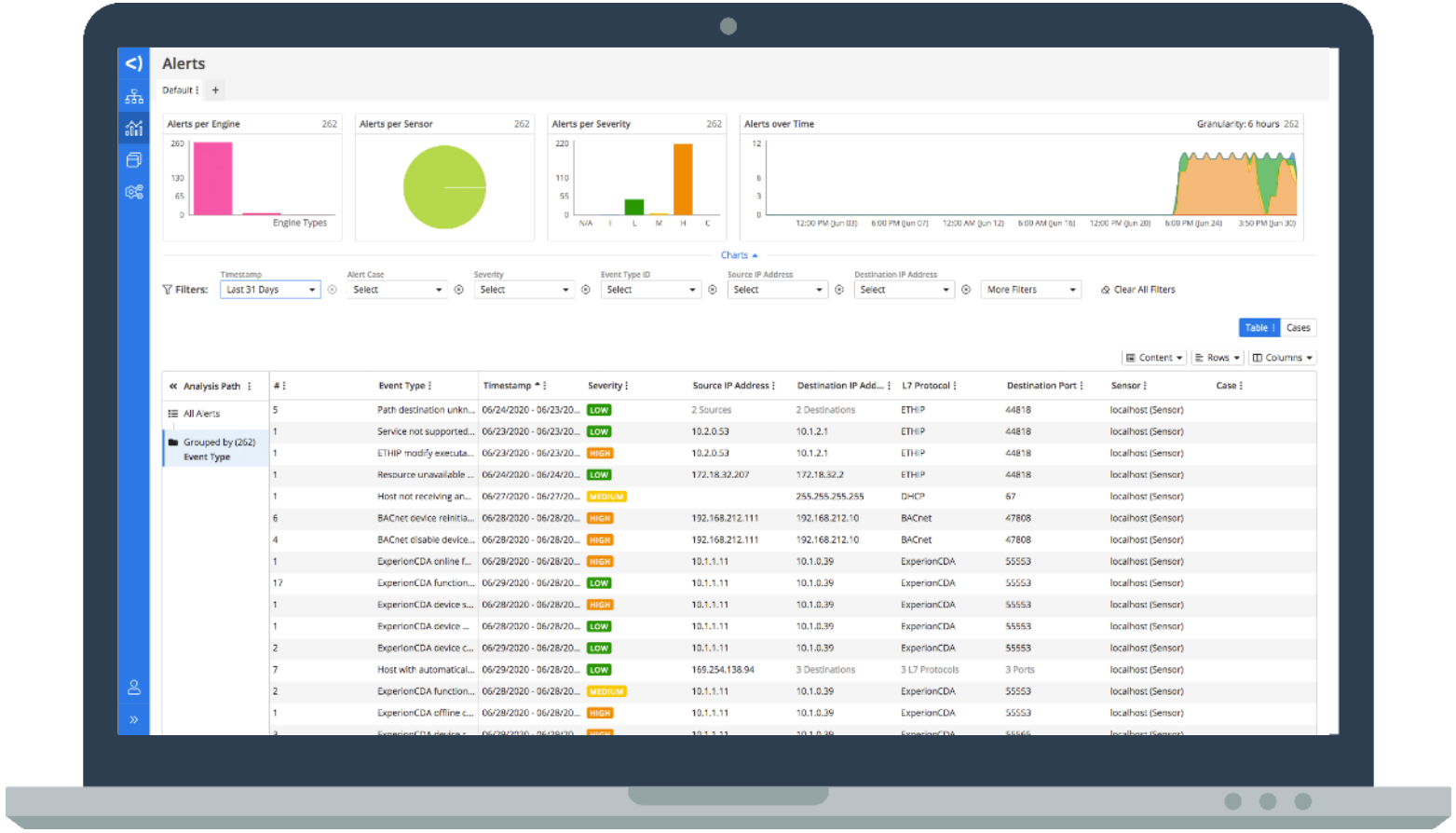
SOLUCION ESCALABLE CON ENTERPRISE COMMAND CENTER

DISTRIBUCCIÓN GEOGRÁFICA BASADO EN SU ARQUITECTURA.

Gestión Inteligente de Activos y Cumplimiento

1. **Necesidad de**: Distinguir dispositivos en cumplimiento y conocidos de los desconocidos y potencialmente peligrosos – Reducir intervenciones manuales relacionados con acceso a la red, remediación de dispositivos y cumplimiento regulatorio.
2. **Visibilidad de Dispositivos e Inteligencia de Activos:** Preocupados por que los dispositivos críticos fueran incorrectamente clasificados y bloqueado su acceso a la red.
3. **Gestión de activos:** Utilizar una clasificación inteligente para que automáticamente identificar, clasificar y categorizar dispositivos OT,IIoT,IoTM.
4. **Segmentación de red:** Colocaron los dispositivos médicos, estaciones de trabajo de enfermería y sistemas de control ambiental en sus propios segmentos de la red (VLAN) restringiendo el acceso a los mismos desde donde era necesario.
5. **Cumplimiento Automatizado:** Informes automatizados y seguridad de puertos para mantener y demostrar cumplimiento con regulación HIPAA. Orquestación de datos de cumplimiento con Firewalls de Nueva Generación NGFW para el refuerzo de políticas.

Optimización y Análisis de Riesgos en las Redes OT.



Detecta las amenazas y Reduce de forma Proactiva el MTTR de la Red.

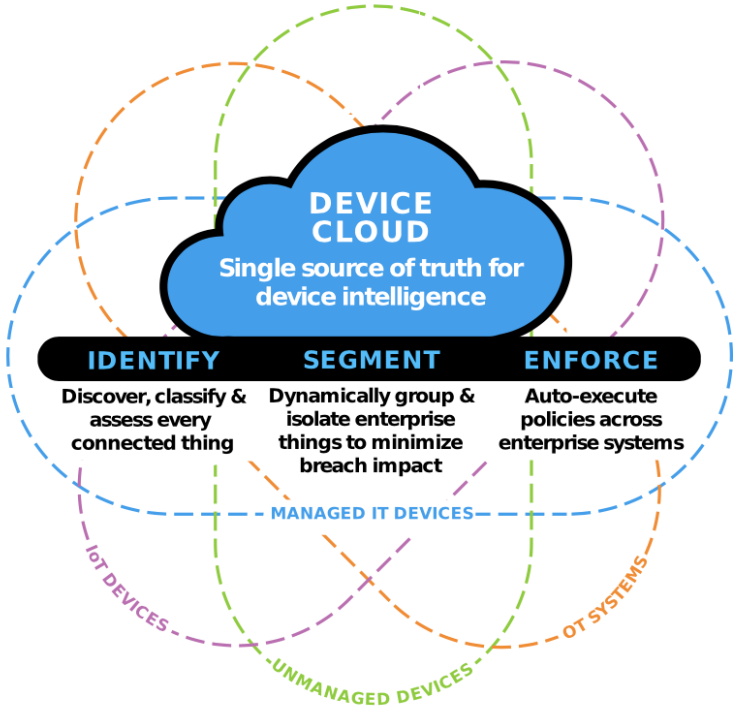
Riesgos en los Activos Con la inteligencia programada basados en los valores de Operaciones y de CiberSeguridad.

Comprender el impacto de Negocio.Vlaorando los indicadores de compromise y vulnerabilidades

Organización de Alertas con agragaciones de las mismas de forma ordenada.

Priorizar Eventos de alto Riesgo .

Nuestra Misión: Defensa activa para la Enterprise of Things

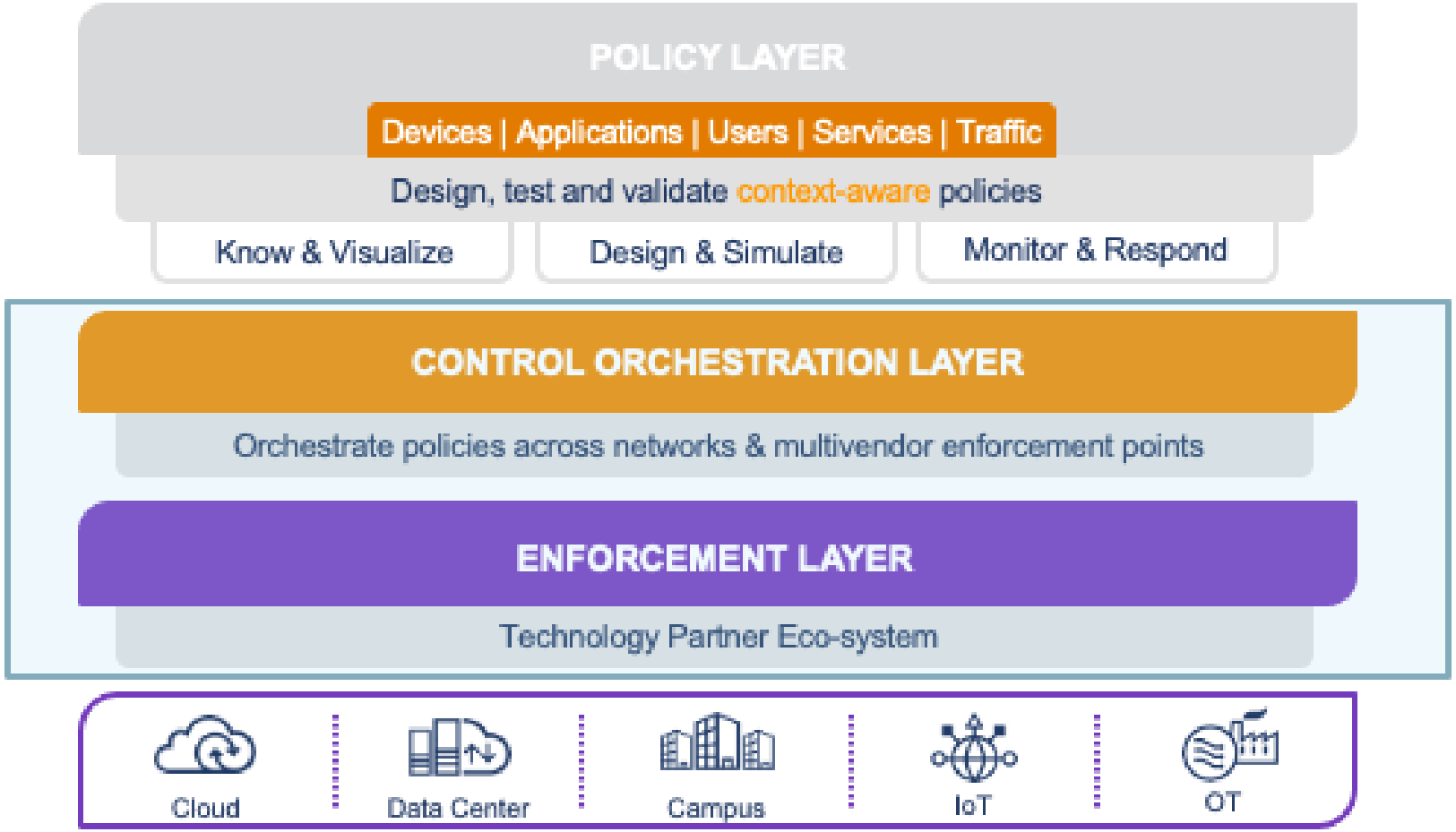


A Zero Trust Platform for

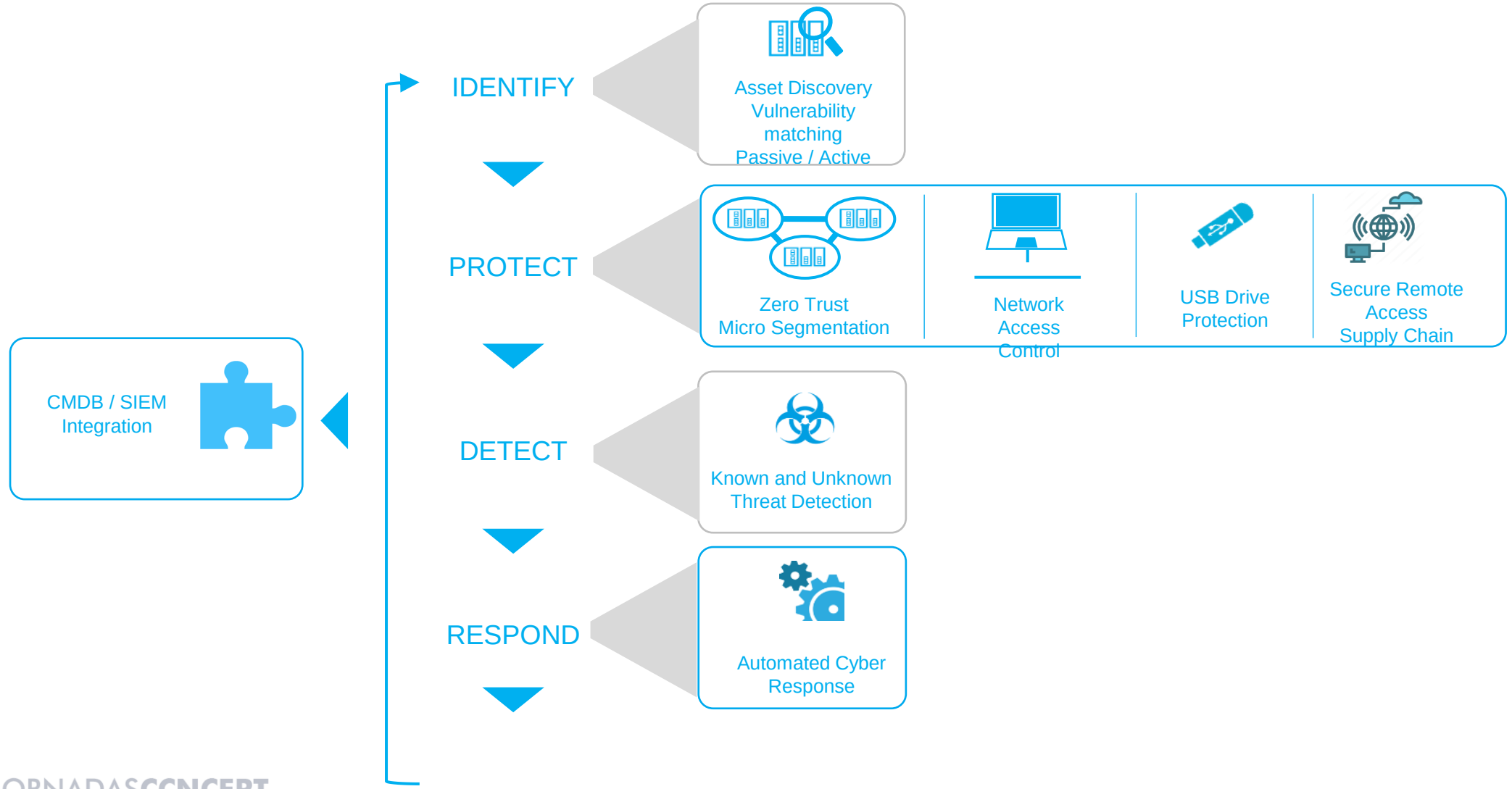
Network Access Control · IoT Security · Network Segmentation · OT Security

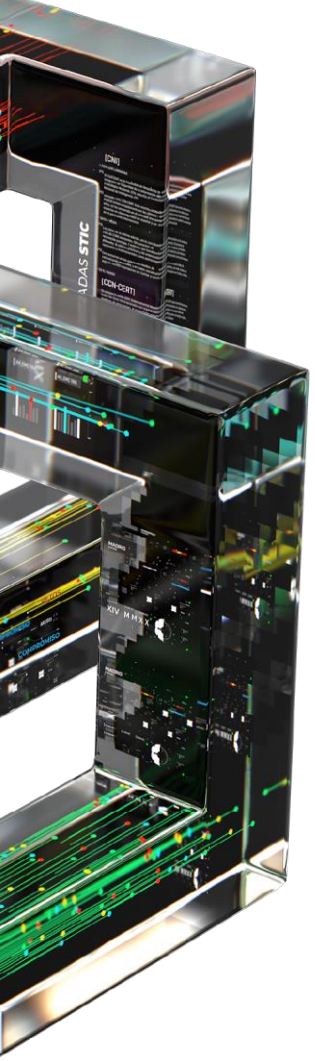
Asset Inventory · Device Compliance · Security Orchestration

La Misión: Orquestación y Control de la Ciberseguridad en la Red OT.

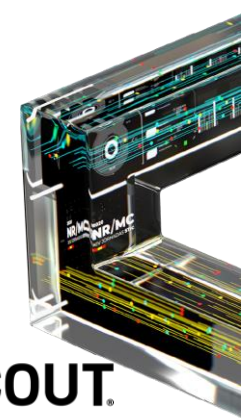


Cumplimiento dentro del Framework de Ciberseguridad





#XIVJORNADASCCNCERT



cn-cert
centro criptológico nacional

FORESCOUT