Innovarpel 2023

Digitalización y Ciberseguridad
en la Industria del Oil&Gas

Hotel Colón | Quito, Ecuador
21 y 22 de noviembre de 2023

ORGANIZA
arpel ASOCIACIÓN DE EMPRESAS DE PETRÓLEO, GAS Y ENERGÍA RENOVABLE DE AMÉRICA LATINA Y EL CARIBE

REALIZA
SEMINARIUM

Generando la ciber-resiliencia industrial

Julio Cesar Ardita

Consultor experto de ciberseguridad

jardita@cisiar.org

Generando la ciber-resiliencia industrial

Agenda

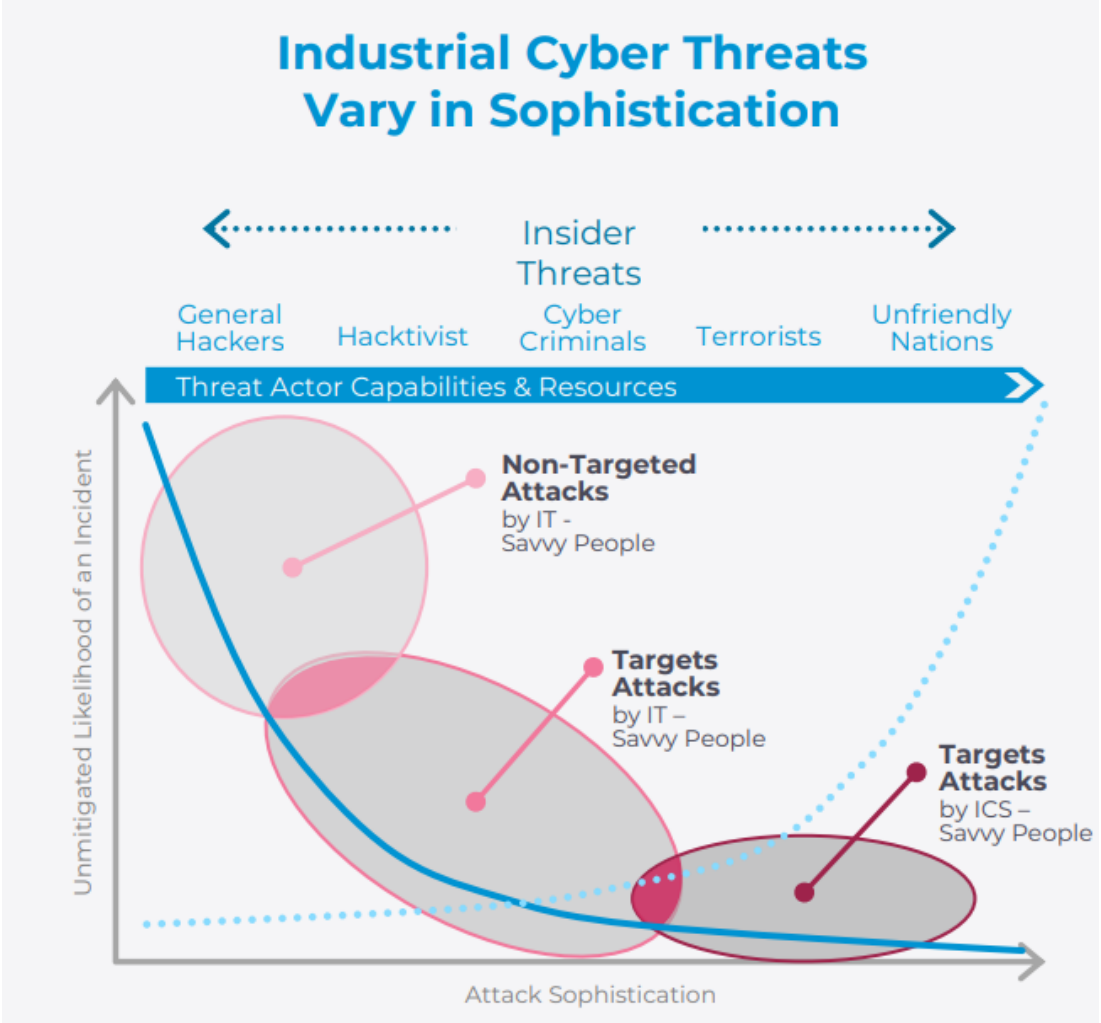
- Ciberincidentes en sistemas industriales
- Gestión de ciberincidentes en el mundo OT
- Ciber-resiliencia a través de procesos, personas y tecnologías

Generando la ciber-resiliencia industrial

Ciberincidentes en sistemas industriales

"Our adversaries in the cyber realm include spies from nation-states who seek our secrets and intellectual property; organized criminals who want to steal our identities and money; terrorists who aspire to attack our power grid, water supply, or other infrastructure; and hacktivist groups who are trying to make a political or social statement."

— Richard A. McFeely, executive assistant director, criminal, cyber, response, and services branch, FBI[7]



Generando la ciber-resiliencia industrial

Ciberincidentes en sistemas industriales

EN EL PASADO

- Impacto en la operación e infraestructura de IT
- Ataques genéricos
- Mecanismos de ataques ruidosos y relativamente fáciles de detectar

ACTUALMENTE

- Foco específico en acceder a los recursos informáticos más críticos (“Crown jewels”)
- Ataques dirigidos a entornos OT
- Se utilizan técnicas silenciosas
- Se busca la “persistencia” sin ser detectado

Generando la ciber-resiliencia industrial

Ciberincidentes en sistemas industriales

Incidentes de seguridad sobre sistemas industriales en Latinoamérica

- Hay más interconexión entre redes industriales y las redes corporativas e internet.

- Actualizaciones de sistemas. Sistemas antiguos legacy que se actualizan a nuevas versiones con nuevas tecnologías embebidas (sistemas abiertos, web, java, etc.).

- Hay baja conciencia de ciberseguridad en los ingenieros locales, los representantes locales y los proveedores internacionales.

- Excusas de ahorro de costos y facilidad de operación por sobre temas de seguridad.

- Desconocimiento de aspectos de seguridad técnicos.

- Apertura de “back-doors” para el acceso administrativo y de proveedores.

Generando la ciber-resiliencia industrial

Ciberincidentes en sistemas industriales

Diferencias entre un ataque a una red industrial y a una red corporativa

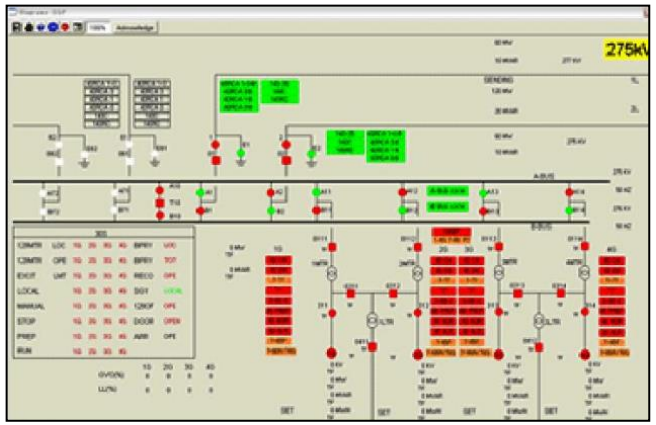
En un ataque a una red industrial:

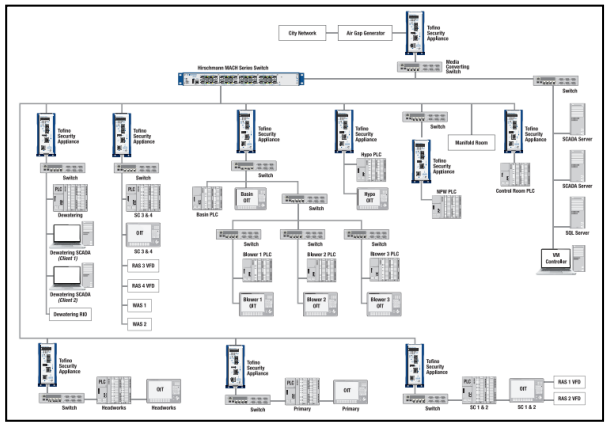
- Se debe conocer otras tecnologías y protocolos distintos con sus propios sistemas, aplicaciones y configuraciones.

- Se deben pasar medidas de seguridad más sólidas (doble factor de autenticación, IDS, IPS, firewalls internos, equipos pivot, etc).

- Se debe tener conocimiento y saber cómo operar un ICS (hay miles de sistemas HMI y configuraciones customizadas).

- **Se necesita mucho más tiempo**.





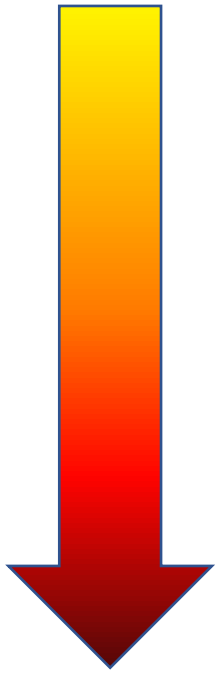
Generando la ciber-resiliencia industrial

Ciberincidentes en sistemas industriales

Diferencias entre un ataque a una red industrial y a una red corporativa

Nivel de dificultad en un ataque a un ICS (*):

+ Fácil



+ Difícil

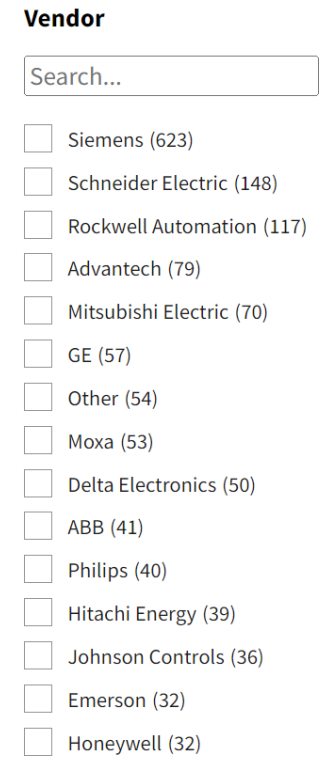
Comprometer la seguridad de un ICS

Extraer información

Hacer una parada del ICS

Dañar (romper) el ICS

Daño al equipamiento (sensores)



https://www.cisa.gov/news-events/cybersecurity-advisories

(*) The Industrial Control System Cyber Kill Chain - SANS

Generando la ciber-resiliencia industrial

Ciberincidentes en sistemas industriales

SOCIEDAD

Toyota detiene la producción en todo Japón, tras un ataque de ransomware

Toyota se ha visto obligado a detener la producción en todas sus plantas en Japón tras un ataque de ransomware a un proveedor clave, según los informes.

El mayor fabricante de automóviles del mundo, afirmó que suspendería 28 líneas de producción en 14 fábricas, el martes, con una reanudación prevista para el miércoles, según Nikkei.

El ciberataque afectó al proveedor de piezas de plástico Kojima Industries y amenazó con extenderse a los sistemas informáticos de Toyota a través de su sistema de control de la producción justo a tiempo "Kanban", según el informe. Se dice que los expertos en cibernética de Toyota se encuentran en Kojima para determinar el impacto y el origen del ataque.

EMPRESAS DE ENERGÍA AFECTADAS POR ATAQUES DE RANSOMWARE

Posted on Febrero 18, 2021 by Security Summit

Recientemente se ha informado que Centrais Eletricas Brasileiras (Eletrobras) y Companhia Paranaense de Energia (Copel), dos importantes empresas de servicios eléctricos de Brasil han anunciado que han sufrido ataques de ransomware. Ambos ataques de ransomware interrumpieron las operaciones y obligaron a las empresas a suspender algunos de sus sistemas.

IMAGE: VALERIIA NEGANOV VIA UNSPLASH

Alexander Martin

June 15th, 2023

News Cybercrime

Oil and gas giant Shell confirms it was impacted by Clop ransomware attacks

Shell confirmed on Thursday it had been impacted by the Clop ransomware gang's breach of the MOVEit file transfer tool after the group listed the British oil and gas multinational on its extortion site.

It is the second time that Shell — which employs more than 80,000 people globally and reported revenues in excess of $381 billion last year — has been hit by the Clop gang targeting a file transfer service.

A spokesperson for Shell told Recorded Future News: "We are aware of a cyber security incident that has impacted a third-party tool from Progress called MOVEit Transfer, which is used by a small number of Shell employees and customers."

SABOTAJE INFORMÁTICO

TGS logra controlar un ciberataque contra el sistema de gestión virtual de su red de gasoductos

Por Redaccion EconoJournal

Dom 3 abril 2022

TGS, una de las dos transportistas de gas del país, sufrió un ciberataque contra su sistema SPAC, la plataforma de procesamiento de solicitudes, asignación y programación de los volúmenes de gas se cargan en la red de gasoductos. Desde la empresa afirmaron que la operación del sistema de transporte no estuvo en riesgo en ningún momento.

Cybersecurity

Hackers Breached Colonial Pipeline Using Compromised Password

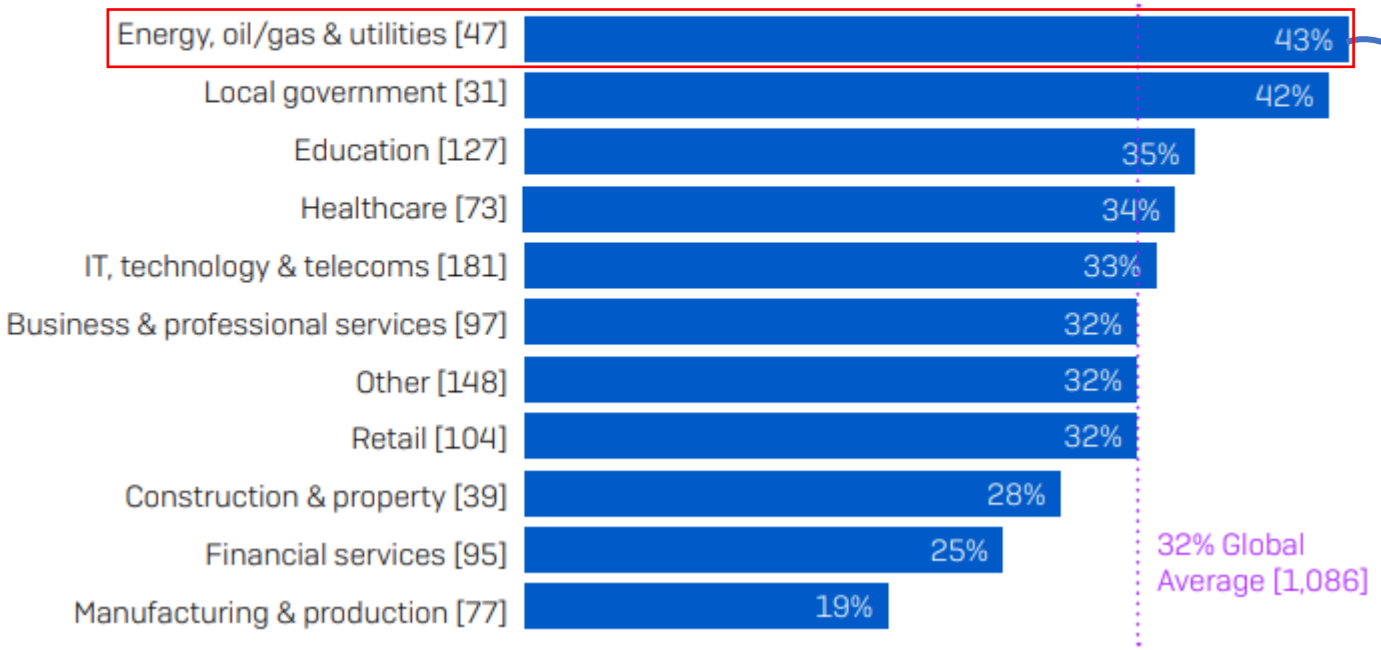
By William Turton and Kartikay Mehrotra
4 de junio de 2021 16:58 GMT-3

Generando la ciber-resiliencia industrial

Ciberincidentes en sistemas industriales

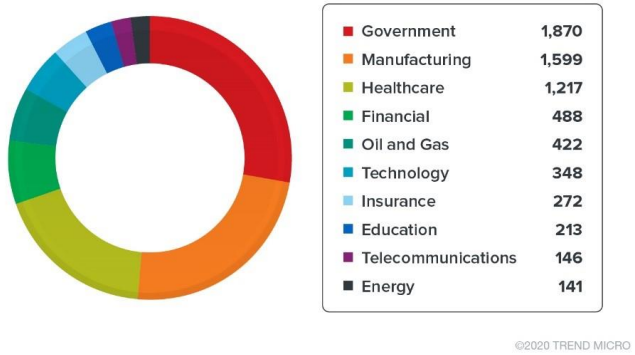
Ransomware

Porcentaje de rescates pagados según industria



Ref.: https://secure2.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf

Industrias afectadas por Ransomware en 2020



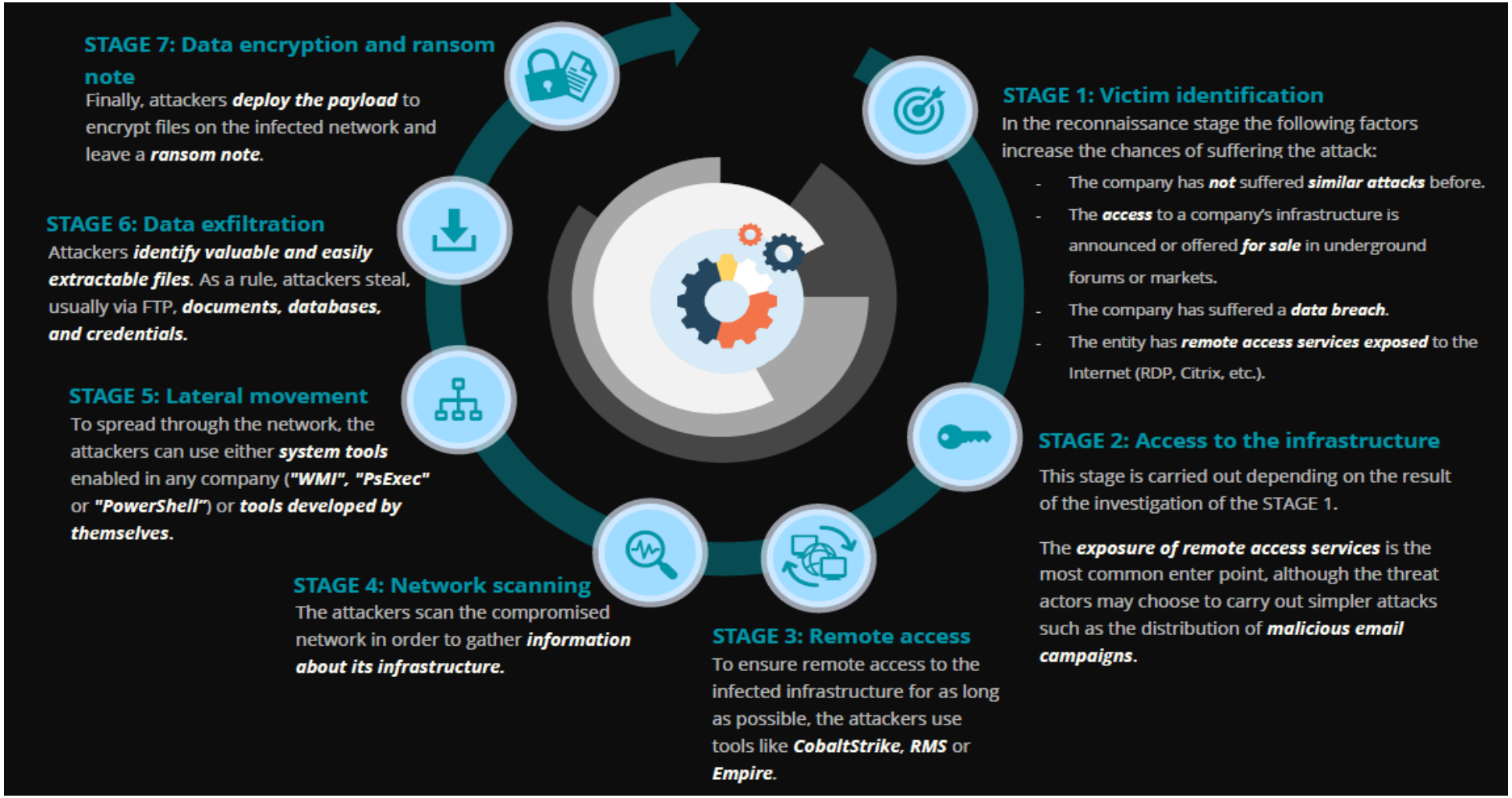
Fuente: www.trendmicro.com

Debido a que las empresas pertenecientes a los rubros de **Oil&Gas** poseen en su mayoría infraestructura *legacy*, se dificulta la tarea de actualizar y restaurar los sistemas comprometidos, provocando que se considere el pago del rescate como la solución más rápida para volver a operar.

Generando la ciber-resiliencia industrial

Ciberincidentes en sistemas industriales

Taxonomía de un ataque de ransomware

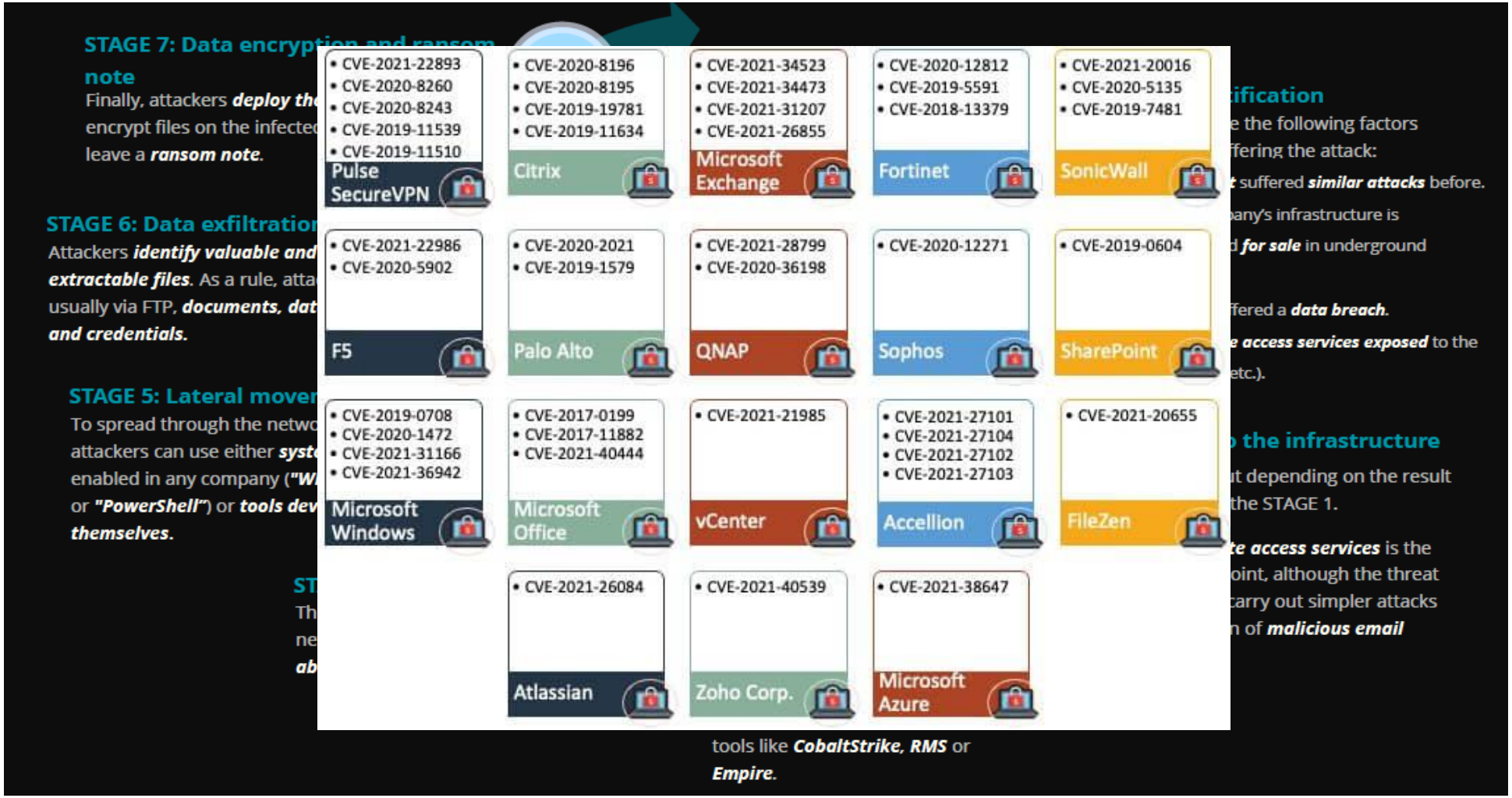


Innovarpel 2023

Generando la ciber-resiliencia industrial

Ciberincidentes en sistemas industriales

Taxonomía de un ataque de ransomware



Generando la ciber-resiliencia industrial

Gestión de ciberincidentes en el mundo OT

La **ciber-resiliencia** es una cualidad inherente a un organismo, entidad, empresa o estado que le permite hacer frente a una crisis de ciberseguridad sin que su actividad se vea afectada.

Es la administración de las amenazas tecnológicas de modo tal que sea posible gestionar de manera efectiva los ataques cibernéticos utilizando metodologías de prevención y gestión de incidentes de ciberseguridad

Generando la ciber-resiliencia industrial

Gestión de ciberincidentes en el mundo OT

¿Estamos preparados para responder a un incidente de seguridad?

Hay poca relación entre los ingenieros que administran los sistemas industriales y las áreas de IT y Seguridad de la Información en las Organizaciones.

Hay pocos registros (logs) con información y casi siempre están implementados por defecto. Tener logs y monitoreo de alertas y eventos es crucial para poder detectar, frenar un ataque a tiempo y/o poder investigar que sucedió.

Hay desconocimiento técnico de ciberseguridad entre los ingenieros. Cosas que técnicamente se pueden y no se pueden hacer. Por ejemplo: rootkits, explotación de vulnerabilidades, by-pass de medidas de protección, etc.

Generando la ciber-resiliencia industrial

Gestión de ciberincidentes en el mundo OT

Metodología para la gestión de ciber-incidentes

El ciclo de vida de respuesta a ciber-incidentes **comienza antes** de que ocurra un incidente. Se requiere un conjunto de capacidades ***proactivas*** y ***reactivas*** para que las operaciones de una organización se adapten y respondan rápidamente a los incidentes cibernéticos y continúen con un impacto limitado en el negocio.

Proactivo

- **Preparación del Incidente:** Diseño y Desarrollo de un programa de respuesta a incidentes, como estrategia, organización, procesos y procedimientos, como así también Cyber Wargaming
- **Detección del Incidente:** Ayuda a desarrollar el programa de monitoreo cibernético y asistencia con el monitoreo y detección continuo, que pueden integrarse con nuestros Servicios de monitoreo de Servicios de amenazas administrados (MTS)

Ciclo de Vida de un ciberincidente

Reactivo

- **Respuesta:** información y determinación de las prioridades del incidente. Medidas para la mitigación de riesgos tomadas para evitar un mayor impacto en la organización
- **Recuperación:** de incidente en corto plazo, estrategias de remediación y desarrollo de roadmap, retorno, en la medida de lo posible, de las operaciones comerciales y proporcionar mitigación de riesgos a largo plazo. Medidas correctivas a largo plazo. Documentación de lecciones aprendidas.

Generando la ciber-resiliencia industrial

Gestión de ciberincidentes en el mundo OT

Preparación / Detección

- **Prepararse para poder responder ante un Ciber-incidente IT/OT:**
  - **Desarrollando Procedimientos – Normas – DBN (incluso llegando a formar un CSIRT interno)**
  - **Capacitando al equipo de trabajo en herramientas y metodologías de CIR**
  - **Concientizar al equipo de Gestión de Crisis**
  - **Implementar herramientas EDR**
  - **Generando visibilidad (configurando Logs)**
  - **Utilizar un SIEM y tenerlo bien "tuneado" en IT/OT**
  - **Realizar ciber-simulaciones técnicas y ejecutivas**
- **Realizar un monitoreo 7x24**
- **Implementar un servicio de CTI para recibir *feeds* sobre IoC e implementar los mismos**
- **El CISO debe participar de foros oficiales y no oficiales con sus colegas**
- **Obtener un ciberseguro**

Generando la ciber-resiliencia industrial

Gestión de ciberincidentes en el mundo OT

Respuesta – Contención – Recuperación

- **Cuando sucede un ciberincidente crítico, se debe:**
  - **Armar un equipo interdisciplinario liderado por el CISO.**
  - **Dividir las etapas y equipos de trabajo:**
    - **Respuesta y contención**
    - **Remediación y vuelva a la operación**
  - **Doble-validar la evidencia y conclusiones preliminares**
  - **Implementar las medidas de contención lo más pronto posible.**
  - **Liderar el War Room para las actividades de remediación (OT, IT, Proveedores, entre otros)**
  - **Gestionar la cibercrisis (comunicaciones internas, externas, legales, auditoría, comité ejecutivo, entes reguladores, entre otros)**

Generando la ciber-resiliencia industrial

Gestión de ciberincidentes en el mundo OT

Cyber Incident Response

- Análisis y procesamiento de logs de distintas fuentes.
- Correlación de información basado en fechas y horas, direccionamiento IP y usuarios.
- Determinación de la existencia de potencial explotación de vulnerabilidades.

Cyber Threat Intel

- Perfilamiento de direcciones IP maliciosas.
- Investigación de sitios web y direcciones IP sospechosas.
- Análisis de binarios / HASH / Grupos

Análisis Forense

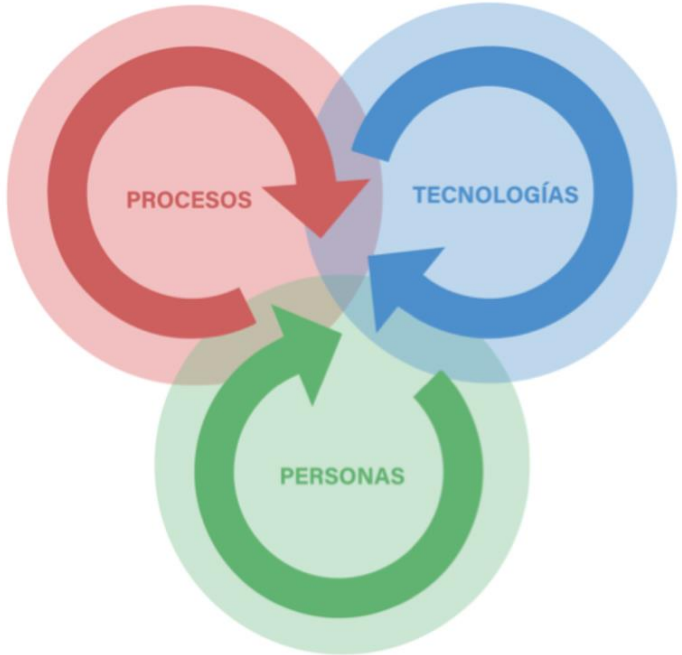
- Análisis forense sobre dispositivos.
- Evaluación de indicadores de compromiso a bajo nivel.
- Reversing de malware.

Generando la ciber-resiliencia industrial

Ciber-resiliencia a través de procesos, personas y tecnologías

Procesos:

- Inventario
- Identificación de CJ (Crown Jewels)
- Estandares ciberseguridad / Compliance
- Procedimientos de CIR
- Playbooks de escenarios
- Simulaciones de ciber-incidentes



Personas:

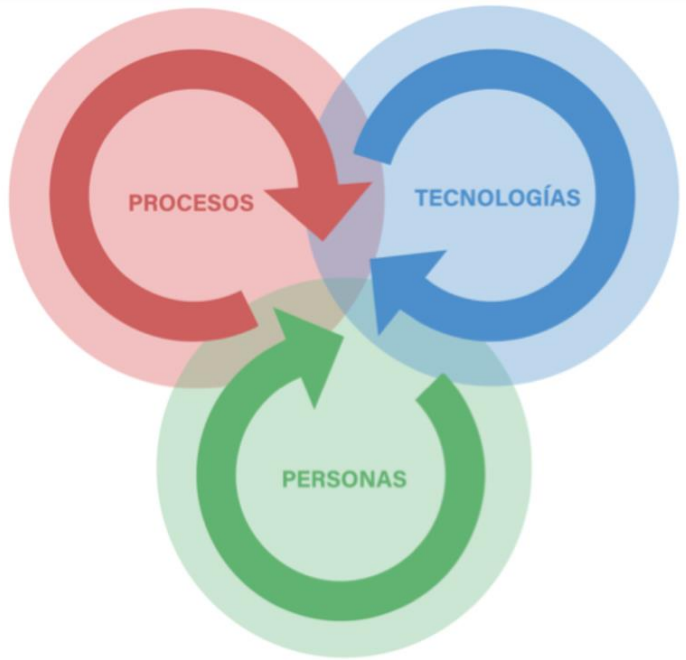
- Gobierno Cyber OT
- Cultura C-Level.
- Concientización personal clave
- Concientización general de empleados
- Concientización general de terceras partes

Generando la ciber-resiliencia industrial

Ciber-resiliencia a través de procesos, personas y tecnologías

Tecnología:

- Gestión de inventario
- AV / EDR para sistemas industriales
- Firewalls industriales
- PIVOT Servers
- Monitoreo local (sondas)
- Monitoreo centralizado de eventos de ciberseguridad
- SOC OT

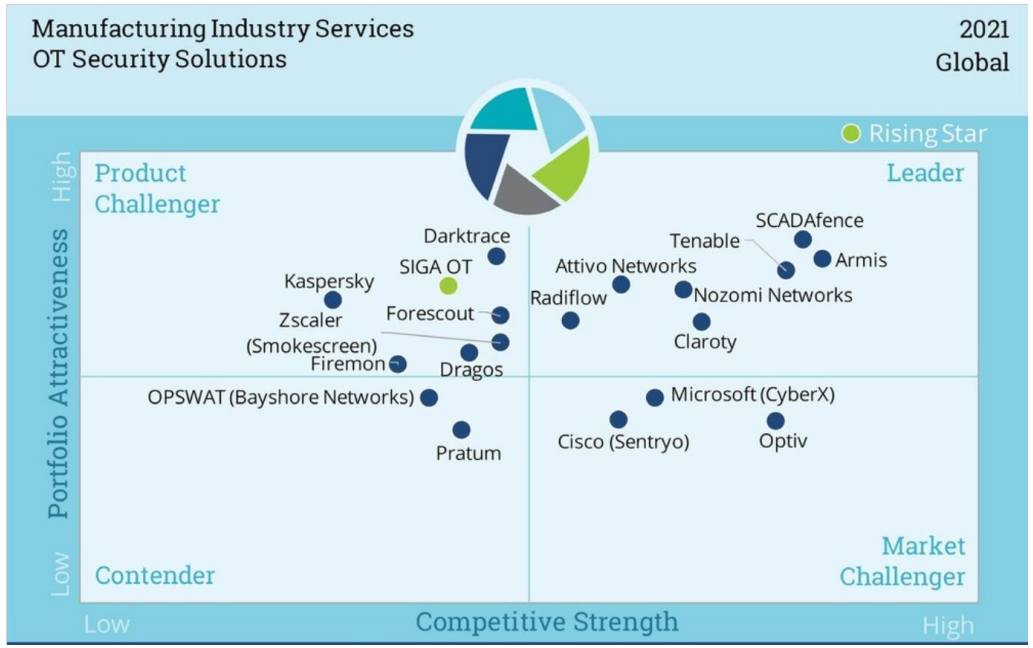


Generando la ciber-resiliencia industrial

Ciber-resiliencia a través de procesos, personas y tecnologías

Herramientas Cyber OT

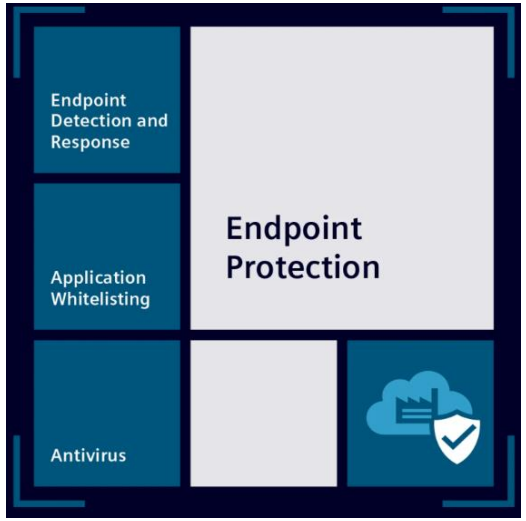
- Inventario
- Scanning de vulnerabilidades
- Análisis de tráfico de red



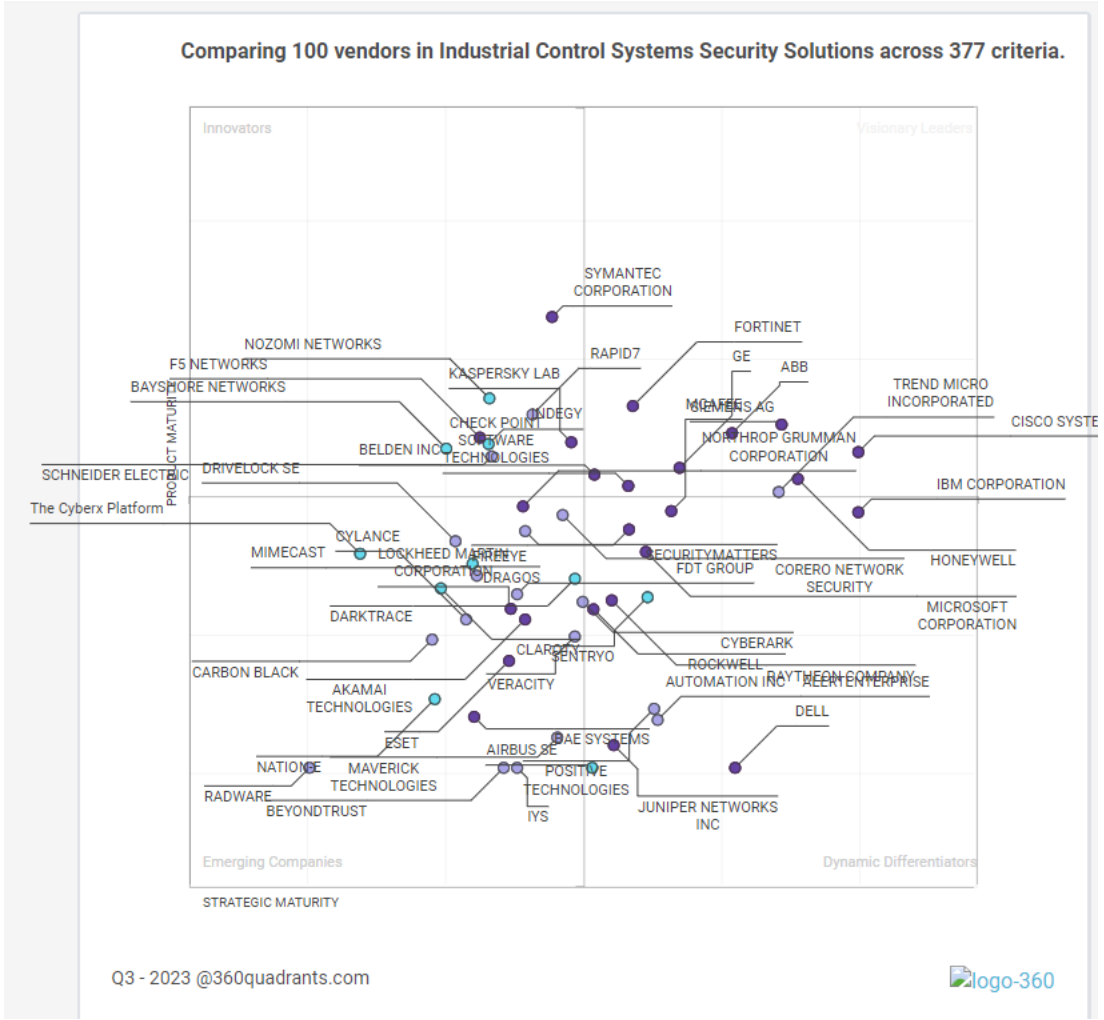
Generando la ciber-resiliencia industrial

Ciber-resiliencia a través de procesos, personas y tecnologías

AV / EDR



Industrial Firewall



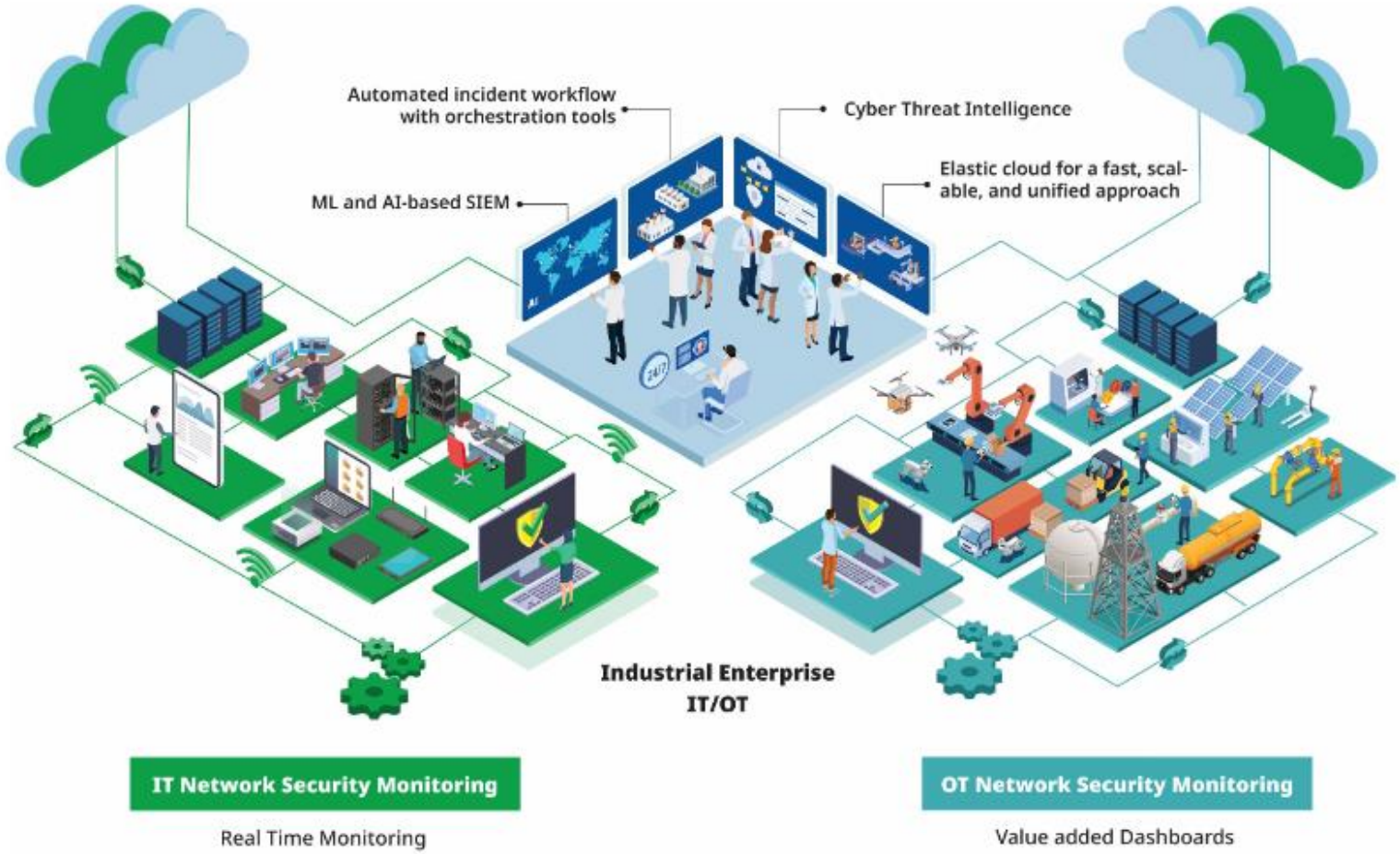
Generando la ciber-resiliencia industrial

Ciber-resiliencia a través de procesos, personas y tecnologías

Industrial Cyber SOC

- SOC IT
- SOC OT
- SOC integrado

- SOC local
- SOC híbrido
- SOCaaS



Generando la ciber-resiliencia industrial

Ciber-resiliencia a través de procesos, personas y tecnologías

Simulaciones de ciberincidentes

Tres preguntas que nos acercan a las simulaciones

Necesitamos crecer en ciber y entender la mejor manera de administrar los riesgos.
¿Cómo hacemos esto?

Somos buenos para manejar incidentes comunes ... *¡¿Pero estamos realmente preparados para una crisis cibernética ?!*

Queremos probar nuestra respuesta de arriba a abajo en un entorno altamente realista.
... ¿Cómo hacemos esto?

Niveles de Mando

Equipo(s) estratégicos de Crisis

- Miembros de la Junta Ejecutiva y no Ejecutiva
- Lideres de Negocios C-suite/Senior

Equipo(s) táctico de incidentes

- Equipo de gestión de incidencias empresariales
- Equipo de gestión de TI (Hasta CISO / CIO)

Personal Operativo

- Equipo de Cyber Incident Response
- Personal técnico de TI (Gerentes, Analistas, etc.)

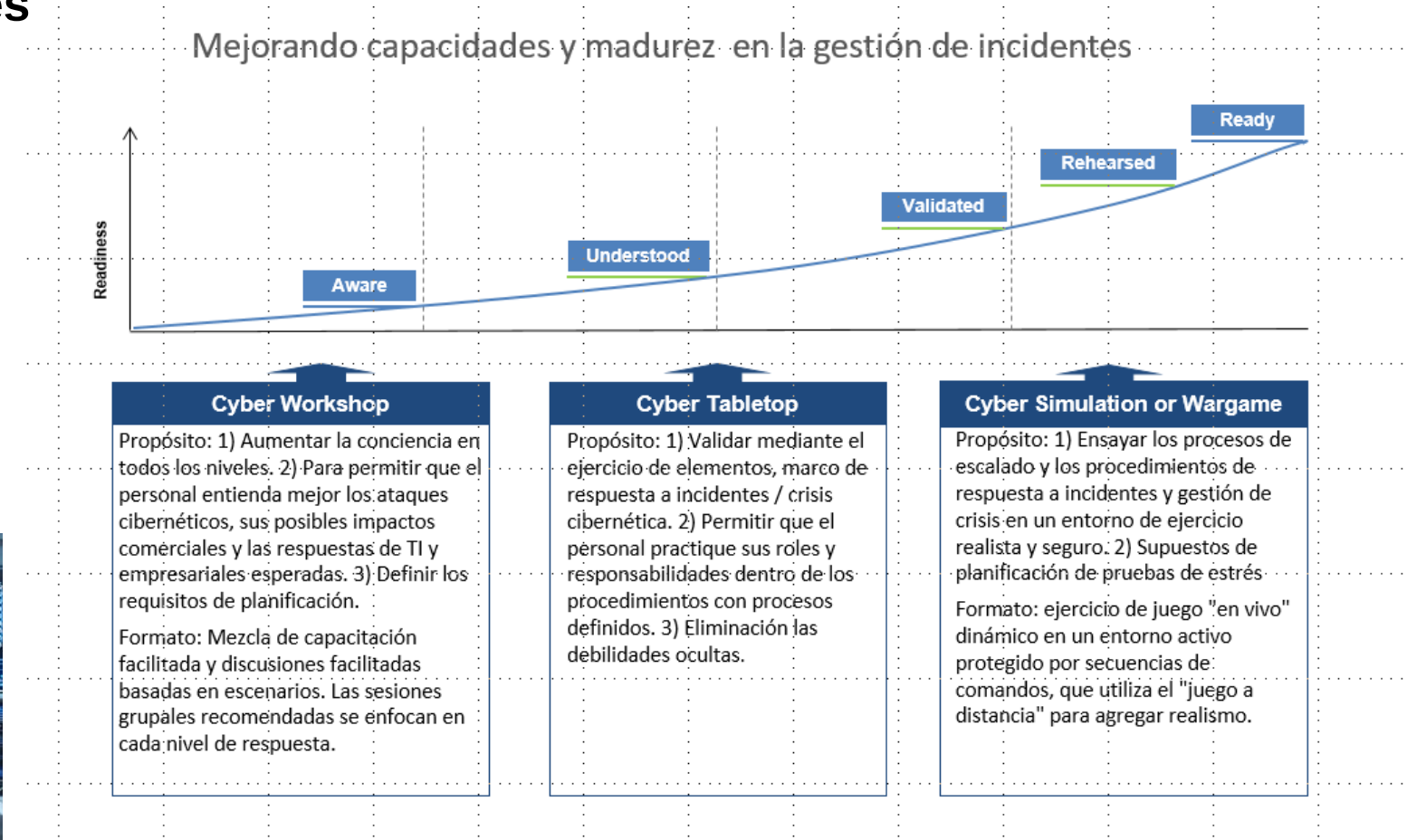
Generando la ciber-resiliencia industrial

Ciber-resiliencia a través de procesos, personas y tecnologías

Simulaciones de ciberincidentes

Nivel del ejercicio:

- Ejecutivo
- Técnico



Generando la ciber-resiliencia industrial

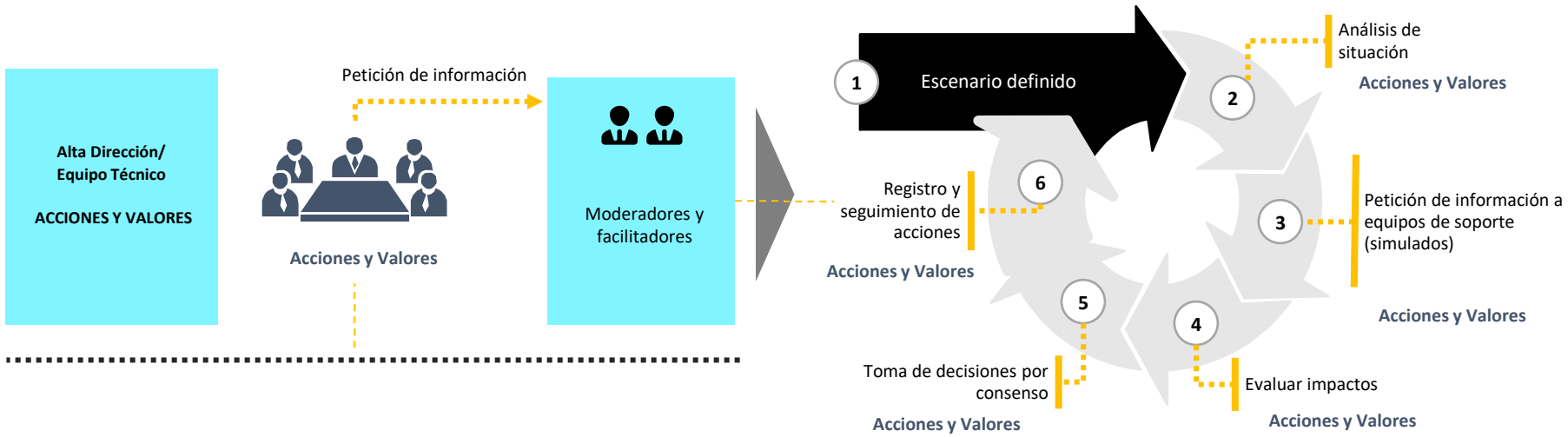
Ciber-resiliencia a través de procesos, personas y tecnologías

Simulaciones de ciberincidentes

Dinámica de la sesión

La Alta Dirección / Equipo Técnico, asistido por un equipo experto, se enfrentará a una crisis...

… que evolucionará en todas sus fases dependiendo de las acciones y decisiones tomadas en tiempo real.



Conclusiones

Los sistemas de control industrial están siendo cada vez más atacados por los intrusos, ya que entienden el impacto causado en la operación.

Es necesario desarrollar las capacidades de ciber resiliencia en los entornos OT para estar preparado de la mejor manera ante un potencial ciber-ataque incluyendo procesos, tecnología y personas.

El monitoreo preventivo (SOC) es clave para poder detectar y prevenir los ciber-ataques a tiempo y las simulaciones de las taxonomías de los ciber-ataques son esenciales para poder proteger la organización.

Julio Cesar Ardita

jardita@cisiar.org

Innovarpel 2023

Digitalización y Ciberseguridad
en la Industria del Oil&Gas

Hotel Colón | Quito, Ecuador

21 y 22 de noviembre de 2023

ORGANIZA

arpel
ASOCIACIÓN DE EMPRESAS DE PETRÓLEO, GAS Y ENERGÍA RENOVABLE DE AMÉRICA LATINA Y EL CARIBE

REALIZA

SEMINARIUM