OBSERVATORIO
Industría y Tecnología

Ciberseguridad
en entornos OT

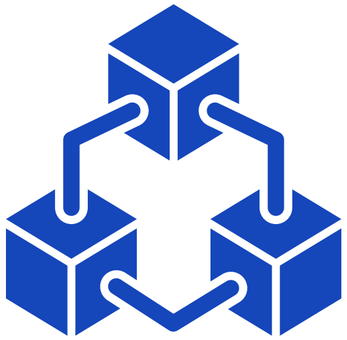
FUJITSU

kynegos

OCTUBRE 2025

¡Bienvenidos
a la sesión de Ciberseguridad OT!

Índice



1. ¿Cuánto sabéis de Ciberseguridad OT?

¿Qué es la Ciberseguridad OT?

Industria 4.0

Hemos pasado de sistemas industriales aislados a entornos totalmente conectados, con un alto grado de automatización, sensorización y control remoto. Hoy, las fábricas son más eficientes, inteligentes y autónomas, pero también más expuestas a nuevas amenazas digitales.

1

¿Cuánto sabéis de Ciberseguridad OT?

Vamos a poner a prueba vuestro conocimiento sobre la protección de entornos OT

¿Puede afectar un ransomware a los Sistemas de Control Industrial?

A. No, es un tipo de malware que solo afecta a equipos corporativos

B. Sí, pero solo a equipos con sistemas Windows Antiguos

C. Sí, porque los Sistemas de Control Industrial pueden contener componentes con los mismos sistemas operativos que los equipos corporativos

D. No, porque los sistemas industriales están aislados del exterior

2

¿Cuánto sabéis de Ciberseguridad OT?

Vamos a poner a prueba vuestro conocimiento sobre la protección de entornos OT

¿Cuántos dispositivos OT conectados se espera que haya en el mundo para 2030?

A. 15 millones

B. 200 millones

C. 1.000 millones

D. Más de 3.000 millones

3

¿Cuánto sabéis de Ciberseguridad OT?

Vamos a poner a prueba vuestro conocimiento sobre la protección de entornos OT

En caso de detectar una infección por ransomware en un equipo...

A. Notifico inmediatamente según los canales internos establecidos

B. Trato de resolverlo pagando el rescate

C. Tiro del cable de red

D. Apago el equipo inmediatamente

4

¿Cuánto sabéis de Ciberseguridad OT?

Vamos a poner a prueba vuestro conocimiento sobre la protección de entornos OT

¿Cuál es el tiempo medio que una empresa industrial tarda en detectar una intrusión en sus sistemas y que realmente comienza a actuar?

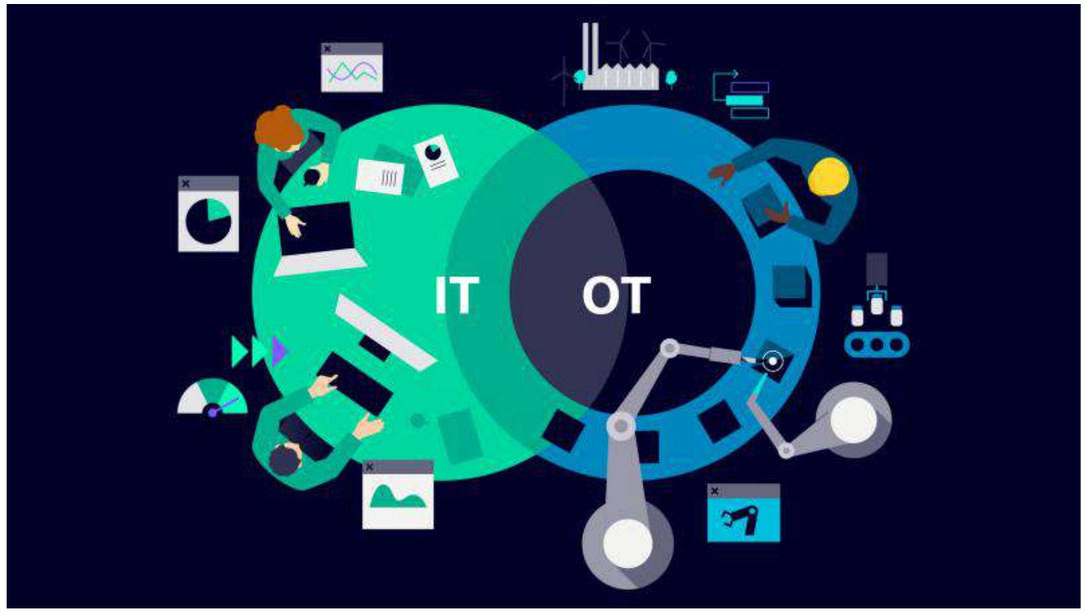
A. 12 horas

B. 5 días

C. 50 días

D. Más de 200 días

¿Qué es la Ciberseguridad OT?



Convergencia IT/OT

La frontera entre los sistemas de oficina (IT) y los de planta (OT) se ha desdibujado. Ahora, la producción, la logística y la gestión empresarial están interconectadas.
Esta unión mejora la eficiencia y la visibilidad, pero también abre la puerta a riesgos cruzados

5

¿Cuánto sabéis de Ciberseguridad OT?

Vamos a poner a prueba vuestro conocimiento sobre la protección de entornos OT

¿Qué porcentaje de incidentes de ciberseguridad en entornos industriales en 2024 se debieron a vulnerabilidades en la conexión entre IT y OT?

A. 25%

B. 40%

C. 60%

D. 75%

¿Cuánto sabéis de Ciberseguridad OT?

Vamos a poner a prueba vuestro conocimiento sobre la protección de entornos OT

¿Cuál es uno de los principales retos técnicos reportados para proteger sistemas OT conectados a redes IT?

A. Falta de personal especializado

B. Protocolos incompatibles y obsoletos

C. Coste excesivo de las herramientas de seguridad

D. Lentitud en la actualización de software

7

¿Cuánto sabéis de Ciberseguridad OT?

Vamos a poner a prueba vuestro conocimiento sobre la protección de entornos OT

¿Qué práctica se considera esencial para frenar la propagación de ataques entre IT y OT?

A. Monitorización tradicional

B. Segmentación y microsegmentación avanzada

C. Backup manual

D. Uso de protocolos cifrados

8

¿Cuánto sabéis de Ciberseguridad OT?

Vamos a poner a prueba vuestro conocimiento sobre la protección de entornos OT

¿Cuál es la principal prioridad en entornos OT frente a los entornos IT?

A. Confidentiality

B. Integrity

C. Availability

D. Safety

¿Qué es la Ciberseguridad OT?

Principales retos y riesgos

El creciente grado de interconexión y la convergencia con IT aumentan la exposición de los sistemas de control industriales, generando nuevos riesgos. Esta realidad implica retos tanto tecnológicos como humanos para garantizar la seguridad y continuidad de los entornos industriales.

9

¿Cuánto sabéis de Ciberseguridad OT?

Vamos a poner a prueba vuestro conocimiento sobre la protección de entornos OT

¿Qué incremento de ataques a infraestructuras esenciales se detectó en España durante 2024?

A. 15%

B. 23%

C. 43%

D. 61%

10

¿Cuánto sabéis de Ciberseguridad OT?

Vamos a poner a prueba vuestro conocimiento sobre la protección de entornos OT

¿Qué sector industrial fue el más atacado en 2024?

A. Energía

B. Automoción

C. Manufactura

D. Sanidad

¿Cuánto sabéis de Ciberseguridad OT?

Vamos a poner a prueba vuestro conocimiento sobre la protección de entornos OT

¿Qué normativa europea establece requisitos de seguridad para operadores de infraestructuras críticas y es legalmente vinculante en España?

A. ISO 9001

B. NIS2

C. GDPR

D. IEC 62443

¿Cuánto sabéis de Ciberseguridad OT?

Vamos a poner a prueba vuestro conocimiento sobre la protección de entornos OT

¿Cuál es la medida más efectiva para mitigar riesgos de ciberseguridad en la cadena de suministro OT?

A. Establecer acuerdos de seguridad y requisitos contractuales con proveedores

B. Auditorías y evaluaciones de seguridad a terceros

C. Implantar soluciones de monitorización de la red de proveedores

D. Capacitación periódica del personal de proveedores en ciberseguridad

2. Anatomía de un ataque OT

Anatomía de un ataque OT

Cómo atacar entornos industriales

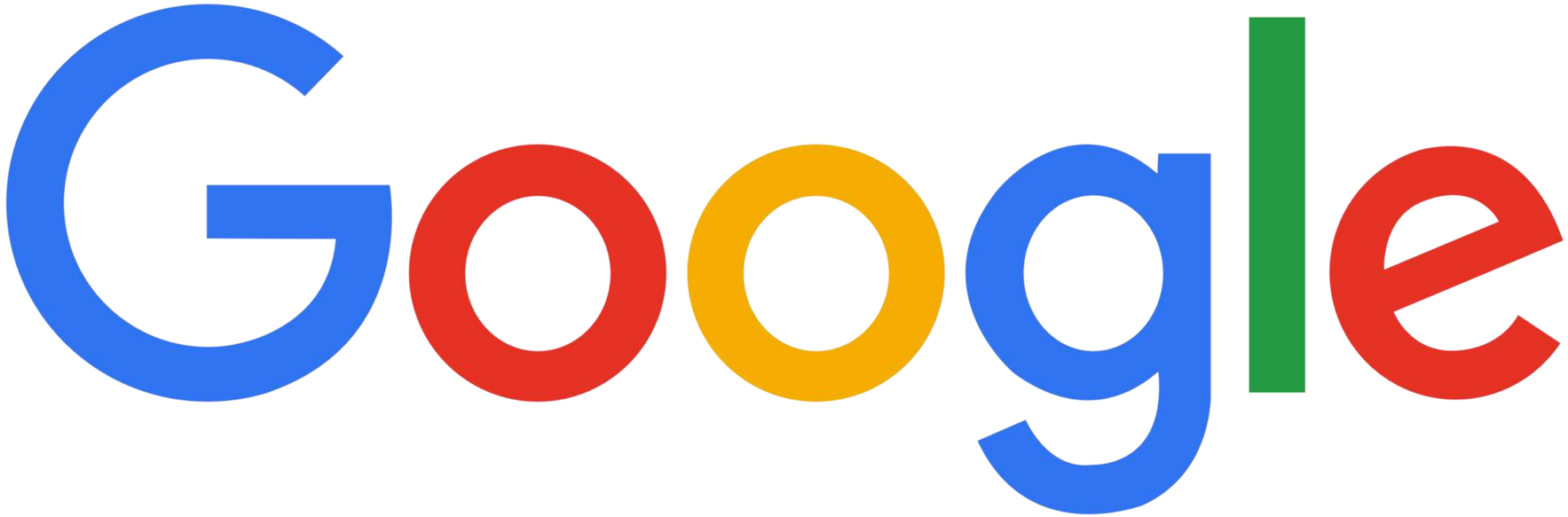
El número de ataques a infraestructuras industriales sigue aumentando, pero no necesariamente son más complejos. Muchas instalaciones presentan un nivel de madurez de ciberseguridad limitado, lo que permite que ataques relativamente sencillos puedan materializarse con éxito.

Primeros pasos de un ataque OT

¿Por dónde empiezan los atacantes?

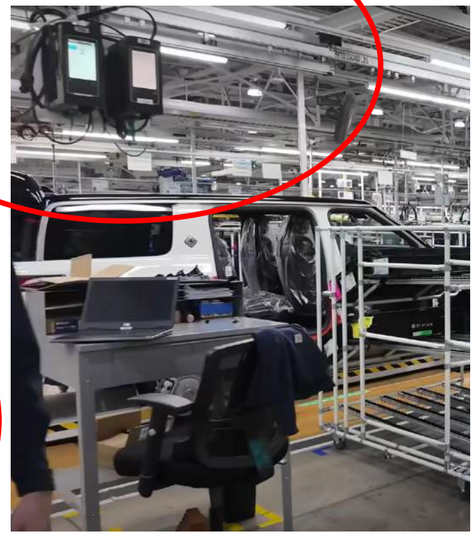
Pista: La dark web no suele ser el primer paso...

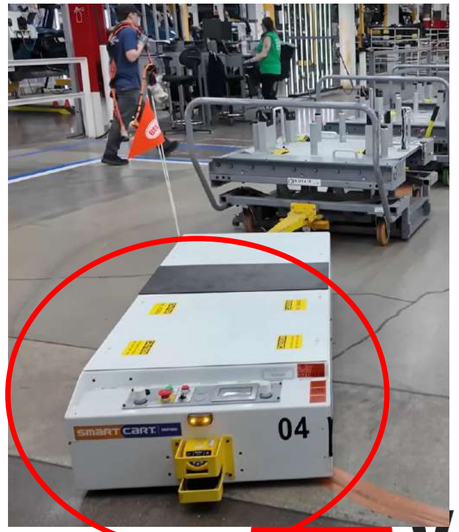
Primeros pasos de un ataque OT



Primeros pasos de un ataque OT

Primeros pasos de un ataque OT





YouTube

Primeros pasos de un ataque OT

Primeros pasos de un ataque OT

[redacted]

12 de julio de 2013 ·

a punto de ir ya para casa a dormir, despues de pasar la guardia de noche. ahora fin de semana libre. — en Ge[redacted]

facebook

Primeros pasos de un ataque OT

Experiencia

Open to new challenges
Look at · Jornada completa
ene. 2021 - actualidad · 1 año 6 meses
Europe

Ford Motor Company
Jornada completa · 12 años 3 meses

23MY S650 Mustang and Troller Programs - Advanced Engineering - Product Development Engineer
ago. 2020 - ene. 2021 · 6 meses
Brazil - USA

• Mustang 2.3L I4 and 5.0L V8 engines low and high-pressure ducts package analysis plus pre-design
• Troller Engine change from X.XL TD to X.XL TD powertrain package analysis

S550 Mustang Program - PTI Leader and Product Development Engineer (Powertrain)
ago. 2010 - ago. 2020 · 10 años 1 mes
Brazil - USA

• As PTI leader supported FSA teams (Exhaust, Mounts, Fuel, Cooling) in the United States market due to meetings, analytical staff, bench test, evaluating test results, vehicle build sign off, launch, supplier … ver más

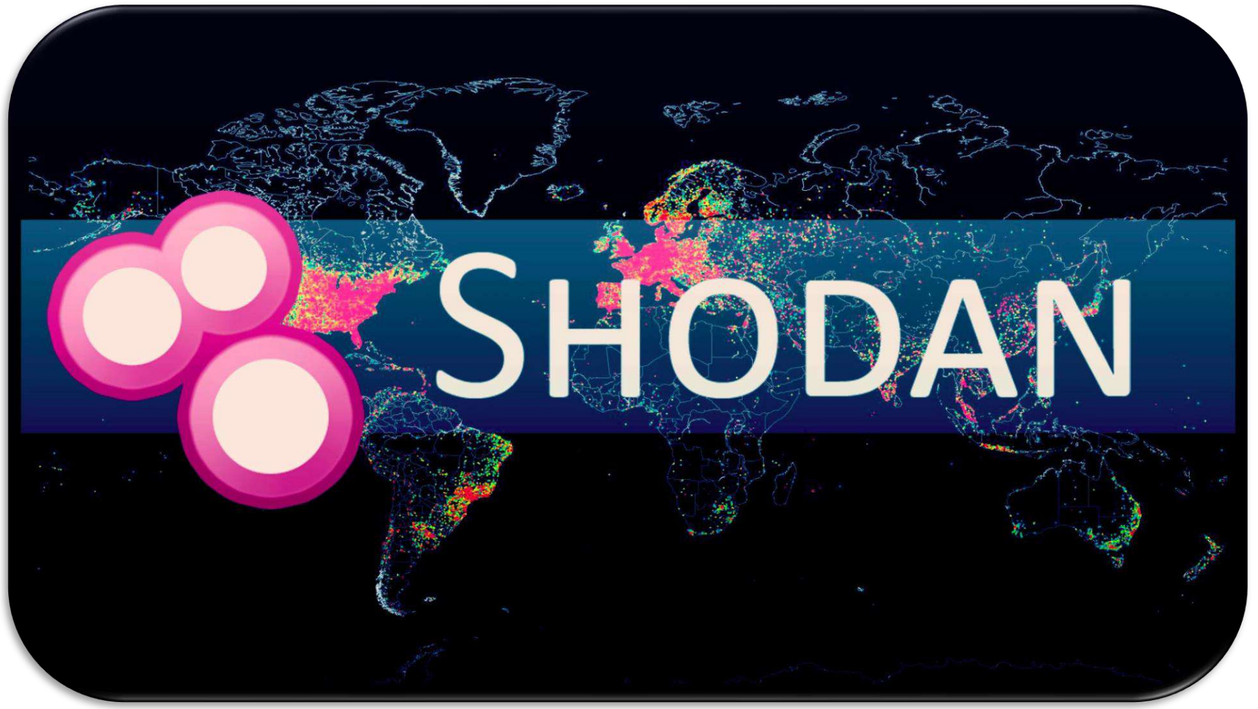
B515 Program Management Engineer (Powertrain)
nov. 2008 - ago. 2010 · 1 año 10 meses
Brazil

• As leader worked daily with multiples regions of the Globo as China, India, Thailand, Australia, UK, Germany, and the US, sharing experiences, motivating, driving and delivering inputs as well as requesting out … ver más

Primeros pasos de un ataque OT

Primeros pasos de un ataque OT

Primeros pasos de un ataque OT



Primeros pasos de un ataque OT

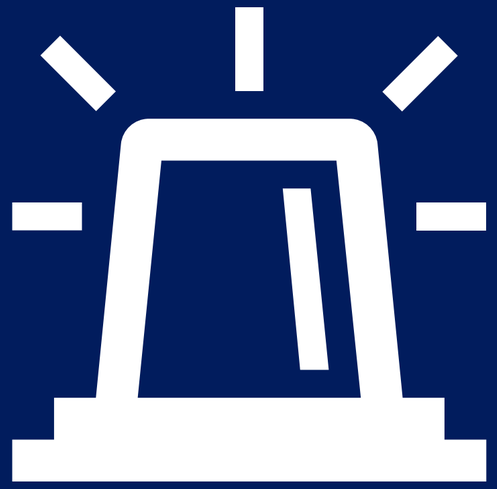
Primeros pasos de un ataque OT

FaceCheck.ID

Have I Been Pwned

Primeros pasos de un ataque OT

¿Qué encontrarían de vosotros?



YA HAN COMPROMETIDO NUESTRA ORGANIZACIÓN

AHORA ES EL MOMENTO DE TOMAR DECISIONES

3. Estrategia y toma de decisiones en un incidente

Actividad

Supervivencia a un Ciberataque en Infraestructura Crítica

Son las 10:00 de la mañana en la central industrial de InfraTech. De repente, las pantallas de control muestran comportamientos anómalos: **un atacante ha penetrado la red corporativa y amenaza con deshabilitar sistemas críticos de la planta**.

Vuestro equipo de ciberseguridad, liderado por el CISO, se encuentra en la sala de crisis. La infraestructura está sufriendo un ataque coordinado que podría escalar en cualquier momento, afectando la producción e incluso la seguridad física.

Contáis con una serie de herramientas de seguridad implementadas en la empresa y posibles acciones de respuesta. Sin embargo, **el tiempo es limitado: estimáis que solo tenéis 5 horas** de margen efectivo para actuar antes de que el ataque cause daños irreparables.
Debéis **decidir qué acciones emprender y qué herramientas utilizar para resistir el máximo tiempo posible y neutralizar la amenaza** hasta que lleguen refuerzos especializados. Cada opción disponible conlleva cierto tiempo de ejecución (horas) que consume parte de esas 5 horas totales.

Actividad

Supervivencia a un Ciberataque en Infraestructura Crítica

Instrucciones:

Primero, cada miembro del equipo decidirá individualmente qué haría: qué medidas tomaría y en qué orden de prioridad, sin exceder las horas disponibles.

Después, nos agruparemos para negociar una decisión consensuada sobre qué acciones llevar a cabo, eligiendo un representante para explicar el plan final.

Límite de tiempo total (10 min):

5 horas (300 minutos) de acciones a repartir. Ningún plan debe exceder este límite de “horas” disponibles, representando la capacidad limitada de reacción ante el avance del ataque.

Supervivencia a un Ciberataque en Infraestructura Crítica

1
Aislar la red o los sistemas comprometidos (cortafuegos FortiGate / NAC)
1,0h

8
Notificar a la alta dirección y equipo de comunicaciones (PR interno)
0,5h

15
Implementar segmentación adicional en red OT con FortiGate ISFW
2,0h

19
Preparación de simulacro de notificación a autoridades (ejercicio de crisis)
1,5h

4
Monitorizar registros de actividad de red (*FortiSIEM / FortiAnalyzer*)
1.0h

7
Respaldar datos críticos (realizar copia de seguridad offline)
2,0h

17
Revisión de políticas de backup y restauración
1,0h

9
Contactar equipo externo de respuesta (FortiGuard IR / autoridades)
0,5h

12
Revisión completa de logs históricos en FortiAnalyzer para detectar persistencia
1,5h

16
Simulación de ataque similar para validar mejoras (Red Team interno)
3,0h

13
Revisión de configuración de FortiGate para endurecer reglas internas
1,0h

10
Activar el plan formal de respuesta a incidentes (movilizar al equipo)
0,5h

20
Formación interna sobre el incidente y medidas preventivas
2,0h

14
Auditoría de cuentas privilegiadas en FortiAuthenticator
1,5h

11
Activar FortiDeceptor para desplegar honeypots y obtener inteligencia del atacante
2,0h

2
Analizar el malware en entorno seguro (FortiSandbox)
1,0h

3
Escanear endpoints y detener malware (FortiEDR)
1,0h

5
Cambiar contraseñas de cuentas críticas (credenciales comprometidas)
1,0h

6
Aplicar un parche de seguridad crítico (cerrar la brecha explotada)
2,0h

18
Actualización de manuales de respuesta y playbooks
1,0h

SOLUCIÓN

Supervivencia a un Ciberataque en Infraestructura Crítica

1
Aislar la red o los sistemas comprometidos (cortafuegos FortiGate / NAC)
1,0h

8
Notificar a la alta dirección y equipo de comunicaciones (PR interno)
0,5h

15
Implementar segmentación adicional en red OT con FortiGate ISFW
2,0h

19
Preparación de simulacro de notificación a autoridades (ejercicio de crisis)
1,5h

4
Monitorizar registros de actividad de red (*FortiSIEM / FortiAnalyzer*)
1.0h

7
Respaldar datos críticos (realizar copia de seguridad offline)
2,0h

17
Revisión de políticas de backup y restauración
1,0h

9
Contactar equipo externo de respuesta (FortiGuard IR / autoridades)
0,5h

12
Revisión completa de logs históricos en FortiAnalyzer para detectar persistencia
1,5h

16
Simulación de ataque similar para validar mejoras (Red Team interno)
3,0h

13
Revisión de configuración de FortiGate para endurecer reglas internas
1,0h

10
Activar el plan formal de respuesta a incidentes (movilizar al equipo)
0,5h

20
Formación interna sobre el incidente y medidas preventivas
2,0h

14
Auditoría de cuentas privilegiadas en FortiAuthenticator
1,5h

11
Activar FortiDeceptor para desplegar honeypots y obtener inteligencia del atacante
2,0h

2
Analizar el malware en entorno seguro (FortiSandbox)
1,0h

3
Escanear endpoints y detener malware (FortiEDR)
1,0h

5
Cambiar contraseñas de cuentas críticas (credenciales comprometidas)
1,0h

6
Aplicar un parche de seguridad crítico (cerrar la brecha explotada)
2,0h

18
Actualización de manuales de respuesta y playbooks
1,0h

Supervivencia a un Ciberataque en Infraestructura Crítica

SOLUCIÓN

Si trabajamos con equipos independientes y sin límite de tiempo

1. Contención de la Amenaza

2. Eliminar el vector de ataque – cerrando brecha

3. Comunicación y coordinación estratégica

Supervivencia a un Ciberataque en Infraestructura Crítica

1
Aislar la red o los sistemas comprometidos (cortafuegos FortiGate / NAC)
1,0h

8
Notificar a la alta dirección y equipo de comunicaciones (PR interno)
0,5h

15
Implementar segmentación adicional en red OT con FortiGate ISFW
2,0h

19
Preparación de simulacro de notificación a autoridades (ejercicio de crisis)
1,5h

4
Monitorizar registros de actividad de red (*FortiSIEM / FortiAnalyzer*)
1.0h

7
Respaldar datos críticos (realizar copia de seguridad offline)
2,0h

17
Revisión de políticas de backup y restauración
1,0h

9
Contactar equipo externo de respuesta (FortiGuard IR / autoridades)
0,5h

12
Revisión completa de logs históricos en FortiAnalyzer para detectar persistencia
1,5h

16
Simulación de ataque similar para validar mejoras (Red Team interno)
3,0h

13
Revisión de configuración de FortiGate para endurecer reglas internas
1,0h

10
Activar el plan formal de respuesta a incidentes (movilizar al equipo)
0,5h

20
Formación interna sobre el incidente y medidas preventivas
2,0h

14
Auditoría de cuentas privilegiadas en FortiAuthenticator
1,5h

11
Activar FortiDeceptor para desplegar honeypots y obtener inteligencia del atacante
2,0h

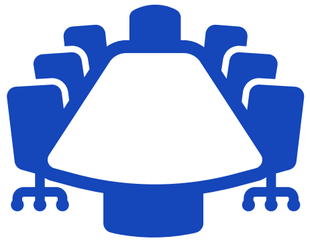
2
Analizar el malware en entorno seguro (FortiSandbox)
1,0h

3
Escanear endpoints y detener malware (FortiEDR)
1,0h

5
Cambiar contraseñas de cuentas críticas (credenciales comprometidas)
1,0h

6
Aplicar un parche de seguridad crítico (cerrar la brecha explotada)
2,0h

18
Actualización de manuales de respuesta y playbooks
1,0h



4. Conclusiones y recomendaciones


PREPARACIÓN


COOPERACIÓN


VIGILANCIA


RESILIENCIA