Hackeos memorables en IoT.
¿Se podrían haber evitado?

Hola!

Me llamo **Fernando Ramírez**

CEO en **Hispasec**

framirez@hispasec.com @fdrg21

Indice

1.
La empresa

Hispasec, Unaaldia y Koodous

HISPASEC

“

Desde **1999** Hispasec **desarrolla productos y provee servicios** de seguridad informática a empresas de todo el mundo.

Ofreciendo un servicio vanguardista gracias a nuestros **proyectos de I+D**, referentes mundiales, lo que nos convierte en una empresa que, no solo da servicios al cliente final, sino que muchas empresas de seguridad son a la vez clientes nuestros.

UAD

“

En **1998** nació el boletín de noticias unaaldia, desde entonces hasta hoy unaaldia ha enviado **una noticia de seguridad diaria a sus suscriptores.**

- > 50k lectores.
- Más de 7.200 noticias enviadas.
- Suscriptores en todos los países de habla hispana.

“

KOODOUS

Nace en 2015. **Koodous** es un **antivirus colaborativo** gratuito, hecho entre todos.

- Más de 34 millones de aplicaciones.
- > 500 analistas de malware.

“

Reconocimiento internacional

BSIDES LAS VEGAS

black hat®

Servicios VS Producto

Servicios

Antifraude

Auditoría técnica

Formación

Soc

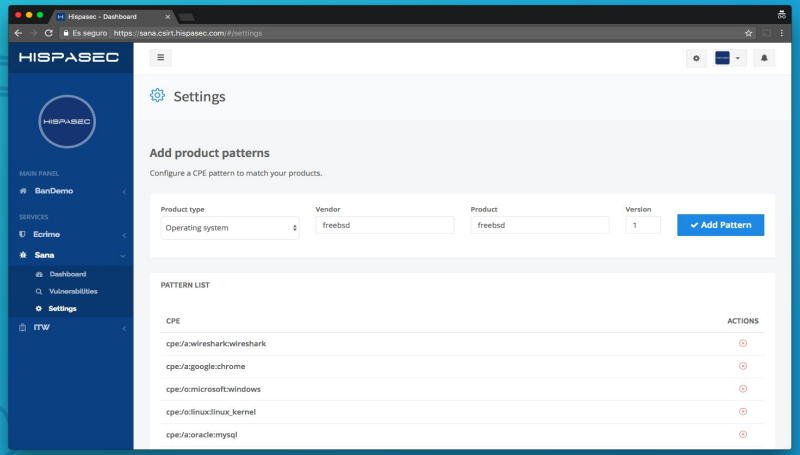
Producto

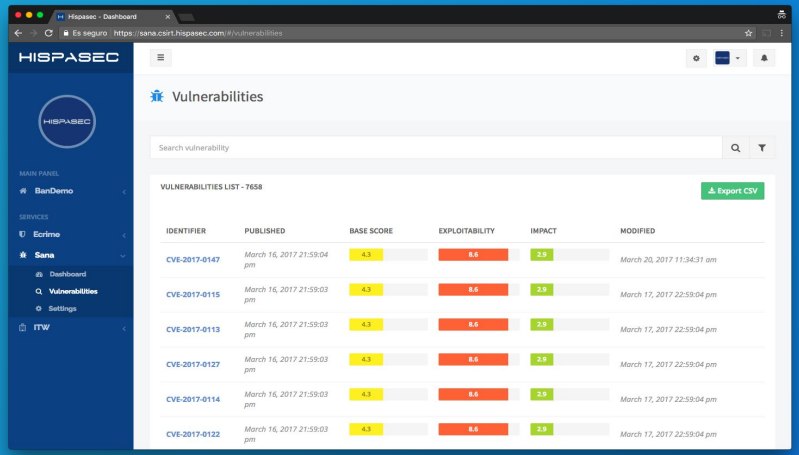
Sana 2001 - ....

Virustotal 2008-2012

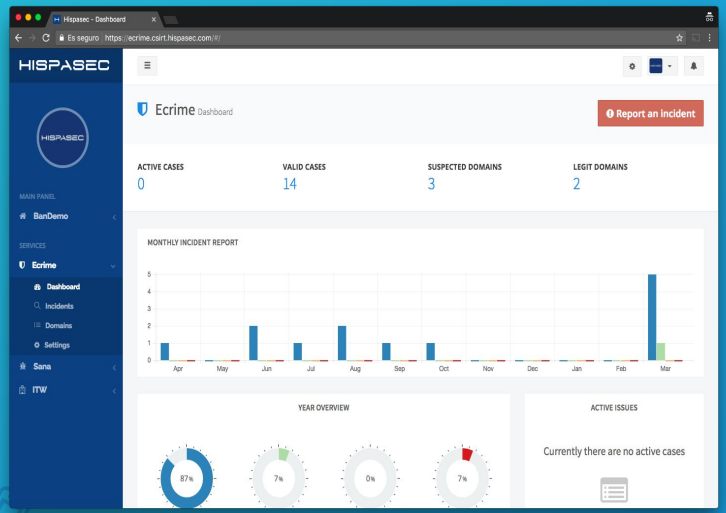
Koodous 2014 - ....

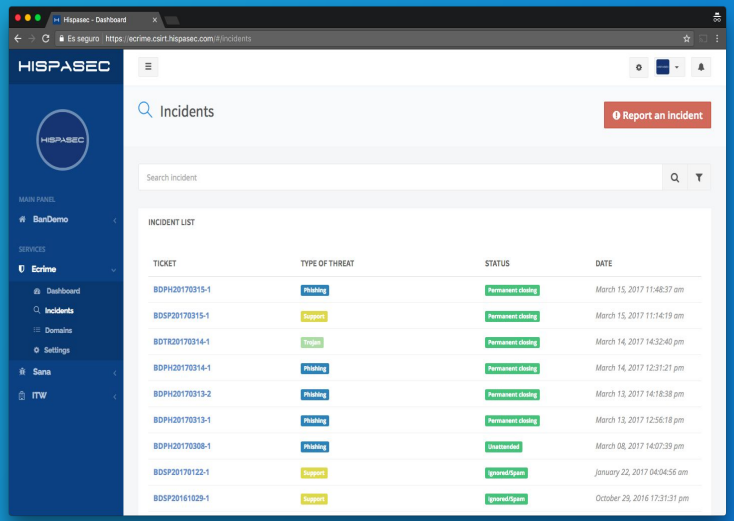
Sana


Hispasec - Dashboard
Es seguro | https://sana.csirt.hispasec.com/#/settings
HISPASEC
MAIN PANEL
BanDemo
SERVICES
Ecrime
Sana
Dashboard
Vulnerabilities
Settings
ITW
Settings
Add product patterns
Configure a CPE pattern to match your products.
Product type
Operating system
Vendor
freebsd
Product
freebsd
Version
1
Add Pattern
PATTERN LIST
CPE
ACTIONS
cpe:/a:wireshark:wireshark
cpe:/a:google:chrome
cpe:/o:microsoft:windows
cpe:/o:linux:linux_kernel
cpe:/a:oracle:mysql


Hispasec - Dashboard
Es seguro | https://sana.csirt.hispasec.com/#/vulnerabilities
HISPASEC
MAIN PANEL
BanDemo
SERVICES
Ecrime
Sana
Dashboard
Vulnerabilities
Settings
ITW
Vulnerabilities
Search vulnerability
VULNERABILITIES LIST - 7658
Export CSV
IDENTIFIER
PUBLISHED
BASE SCORE
EXPLOITABILITY
IMPACT
MODIFIED
CVE-2017-0147
March 16, 2017 21:59:04 pm
4.3
8.6
2.9
March 20, 2017 11:34:31 am
CVE-2017-0115
March 16, 2017 21:59:03 pm
4.3
8.6
2.9
March 17, 2017 22:59:04 pm
CVE-2017-0113
March 16, 2017 21:59:03 pm
4.3
8.6
2.9
March 17, 2017 22:59:04 pm
CVE-2017-0127
March 16, 2017 21:59:03 pm
4.3
8.6
2.9
March 17, 2017 22:59:04 pm
CVE-2017-0114
March 16, 2017 21:59:03 pm
4.3
8.6
2.9
March 17, 2017 22:59:04 pm
CVE-2017-0122
March 16, 2017 21:59:03 pm
4.3
8.6
2.9
March 17, 2017 22:59:04 pm

Antifraude


HISPASEC
Ecrime Dashboard
Report an incident
ACTIVE CASES
0
VALID CASES
14
SUSPECTED DOMAINS
3
LEGIT DOMAINS
2
MONTHLY INCIDENT REPORT
YEAR OVERVIEW
ACTIVE ISSUES
Currently there are no active cases


HISPASEC
Incidents
Report an incident
Search incident
INCIDENT LIST
TICKET
TYPE OF THREAT
STATUS
DATE

Auditoría técnica

Auditoría perimetral
Test de intrusión (Pentest)
Auditoría WiFi
Auditoría de código
Auditoría interna
Auditoría de aplicaciones Web
Auditoría de aplicaciones móviles

20 años en ciberseguridad son muchos

2.
¿Qué es IoT?

Internet of things

HISPASEC

“

El **internet de las cosas** es un concepto que se refiere a una **interconexión digital** de objetos cotidianos con internet.

También, se suele conocer como internet de todas las cosas o internet en las cosas.

Estimación de dispositivos conectados según Gartner & IDC

Año 2016:
6'4 billion dispositivos conectados

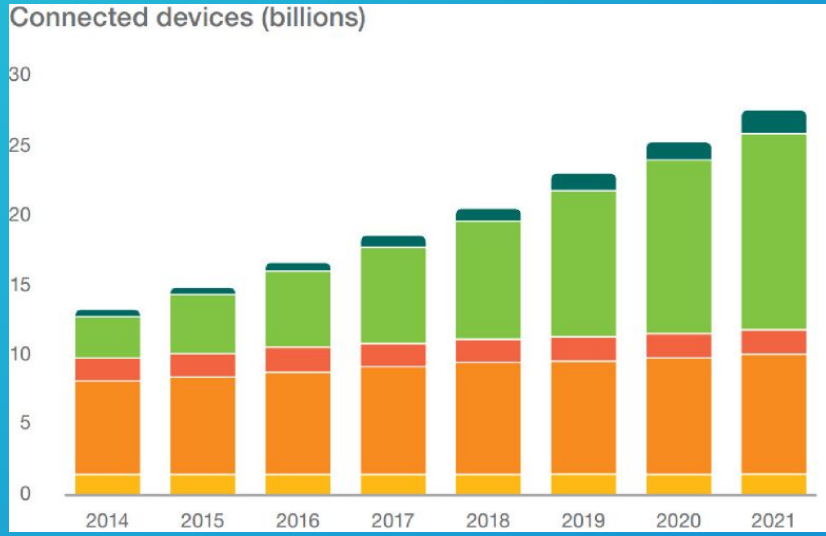
$235 billion

Año 2020:
20 billion dispositivos conectados

$1700 billion

Fuente: Gartner & IDC

Distribución de dispositivos conectados a Internet



	15 billion	28 billion	CAGR 2015–2021
Cellular IoT	0.4	1.5	27%
Non-cellular IoT	4.2	14.2	22%
PC/laptop/tablet	1.7	1.8	1%
Mobile phones	7.1	8.6	3%
Fixed phones	1.3	1.4	0%
	2015	2021	

Fuente: Ericsson mobile report 2016

Previsión mundial de gasto en seguridad en IoT

En los últimos cinco años el gasto se incrementará un 100%

2014	2015	2016	2017	2018
231,86 $	281,54 $	348,32 S	433,95 $	547,20 $

Fuente: IoT Security, Worldwide, Gartner, April 2016

Una nueva ventana llamada IoT

3.
Casos de uso de la seguridad IoT

Ejemplos de hackeos en los dos últimos años.

Vulnerabilidad - Pecera en casino - 2018

Acceden a la base de datos de un casino a través del **termómetro de la pecera del mismo**.

Solución

Correcto inventariado

En muchos casos no somos conscientes de la cantidad de dispositivos que tenemos conectados a nuestra red.

Actualizaciones de seguridad

La dificultad de actualizar estos dispositivos los hace especialmente vulnerables.

Plan de auditoría técnica

Un correcto plan de auditoría sobre nuestra red es básico para cualquier empresa que quiera salvaguardar la seguridad de sus sistemas.

Blue Team - Soc

Un equipo de defensa que esté constantemente revisando la información que circula por nuestra red y aplicando mecanismos de defensa.

Segmentación de red

Una correcta segmentación permite asumir riesgos y segmentar trabajos de auditoría, priorizando y dedicando más recursos a las partes más delicadas.

Plan de seguridad de la información

El conjunto de políticas de administración de la información dentro de una compañía. Suele ir asociado a un SGSI. La norma ISO que lo avala es la 27001

Solución

Correcto inventariado

En muchos casos no somos conscientes de la cantidad de dispositivos que tenemos conectados a nuestra red.

Actualizaciones de seguridad

La dificultad de actualizar estos dispositivos los hace especialmente vulnerables.

Plan de auditoría técnica

Un correcto plan de auditoría sobre nuestra red es básico para cualquier empresa que quiera salvaguardar la seguridad de sus sistemas.

Blue Team - Soc

Un equipo de defensa que esté constantemente revisando la información que circula por nuestra red y aplicando mecanismos de defensa.

Segmentación de red

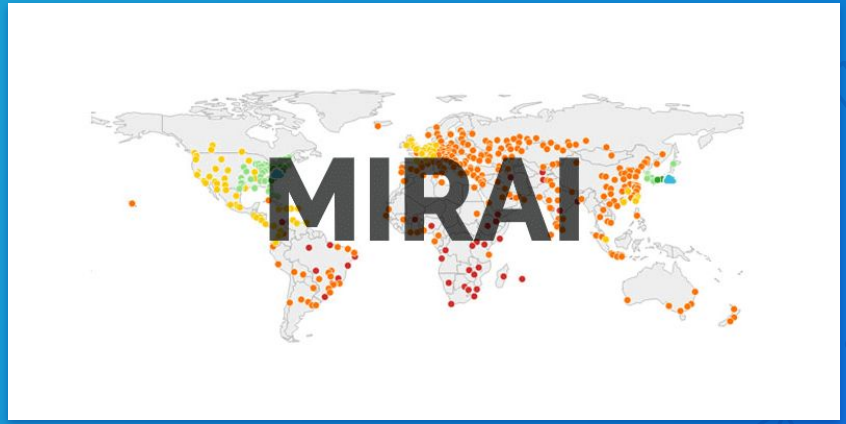
Una correcta segmentación permite asumir riesgos y segmentar trabajos de auditoría, priorizando y dedicando más recursos a las partes más delicadas.

Plan de seguridad de la información

El conjunto de políticas de administración de la información dentro de una compañía. Suele ir asociado a un SGSI. La norma ISO que lo avala es la 27001

Malware - Mirai y Torii

Malware específico para IoT, se aprovecha de la **escasa securización** de estos dispositivos.



Solución

Correcto inventariado

En muchos casos no somos conscientes de la cantidad de dispositivos que tenemos conectados a nuestra red.

Actualizaciones de seguridad

La dificultad de actualizar estos dispositivos los hace especialmente vulnerables.

Plan de auditoría técnica

Un correcto plan de auditoría sobre nuestra red es básico para cualquier empresa que quiera salvaguardar la seguridad de sus sistemas.

Blue Team - Soc

Un equipo de defensa que esté constantemente revisando la información que circula por nuestra red y aplicando mecanismos de defensa.

Segmentación de red

Una correcta segmentación permite asumir riesgos y segmentar trabajos de auditoría, priorizando y dedicando más recursos a las partes más delicadas.

Plan de seguridad de la información

El conjunto de políticas de administración de la información dentro de una compañía. Suele ir asociado a un SGSI. La norma ISO que lo avala es la 27001

Solución

Correcto inventariado

En muchos casos no somos conscientes de la cantidad de dispositivos que tenemos conectados a nuestra red.

Actualizaciones de seguridad

La dificultad de actualizar estos dispositivos los hace especialmente vulnerables.

Plan de auditoría técnica

Un correcto plan de auditoría sobre nuestra red es básico para cualquier empresa que quiera salvaguardar la seguridad de sus sistemas.

Blue Team - Soc

Un equipo de defensa que esté constantemente revisando la información que circula por nuestra red y aplicando mecanismos de defensa.

Segmentación de red

Una correcta segmentación permite asumir riesgos y segmentar trabajos de auditoría, priorizando y dedicando más recursos a las partes más delicadas.

Plan de seguridad de la información

El conjunto de políticas de administración de la información dentro de una compañía. Suele ir asociado a un SGSI. La norma ISO que lo avala es la 27001

Vulnerabilidad - Baby Cam Hackeadas - 2017 en adelante

Son varias las aplicaciones de control de webcam para bebés que han sido **vulneradas**.

Solución

Correcto inventariado

En muchos casos no somos conscientes de la cantidad de dispositivos que tenemos conectados a nuestra red.

Actualizaciones de seguridad

La dificultad de actualizar estos dispositivos los hace especialmente vulnerables.

Plan de auditoría técnica

Un correcto plan de auditoría sobre nuestra red es básico para cualquier empresa que quiera salvaguardar la seguridad de sus sistemas.

Blue Team - Soc

Un equipo de defensa que esté constantemente revisando la información que circula por nuestra red y aplicando mecanismos de defensa.

Segmentación de red

Una correcta segmentación permite asumir riesgos y segmentar trabajos de auditoría, priorizando y dedicando más recursos a las partes más delicadas.

Plan de seguridad de la información

El conjunto de políticas de administración de la información dentro de una compañía. Suele ir asociado a un SGSI. La norma ISO que lo avala es la 27001

Solución - punto de vista del fabricante

Correcto inventariado

En muchos casos no somos conscientes de la cantidad de dispositivos que tenemos conectados a nuestra red.

Actualizaciones de seguridad

La dificultad de actualizar estos dispositivos los hace especialmente vulnerables.

Plan de auditoría técnica

Un correcto plan de auditoría sobre nuestra red es básico para cualquier empresa que quiera salvaguardar la seguridad de sus sistemas.

Blue Team - Soc

Un equipo de defensa que esté constantemente revisando la información que circula por nuestra red y aplicando mecanismos de defensa.

Segmentación de red

Una correcta segmentación permite asumir riesgos y segmentar trabajos de auditoría, priorizando y dedicando más recursos a las partes más delicadas.

Plan de seguridad de la información

El conjunto de políticas de administración de la información dentro de una compañía. Suele ir asociado a un SGSI. La norma ISO que lo avala es la 27001

Vulnerabilidad para IoT - Owlet WiFi Heart Monitor

Debilidad en el **tráfico** en red **local** entre el dispositivo y el móvil.

Solución

Correcto inventariado

En muchos casos no somos conscientes de la cantidad de dispositivos que tenemos conectados a nuestra red.

Actualizaciones de seguridad

La dificultad de actualizar estos dispositivos los hace especialmente vulnerables.

Plan de auditoría técnica

Un correcto plan de auditoría sobre nuestra red es básico para cualquier empresa que quiera salvaguardar la seguridad de sus sistemas.

Blue Team - Soc

Un equipo de defensa que esté constantemente revisando la información que circula por nuestra red y aplicando mecanismos de defensa.

Segmentación de red

Una correcta segmentación permite asumir riesgos y segmentar trabajos de auditoría, priorizando y dedicando más recursos a las partes más delicadas.

Plan de seguridad de la información

El conjunto de políticas de administración de la información dentro de una compañía. Suele ir asociado a un SGSI. La norma ISO que lo avala es la 27001

Solución - punto de vista del fabricante

Correcto inventariado

En muchos casos no somos conscientes de la cantidad de dispositivos que tenemos conectados a nuestra red.

Actualizaciones de seguridad

La dificultad de actualizar estos dispositivos los hace especialmente vulnerables.

Plan de auditoría técnica

Un correcto plan de auditoría sobre nuestra red es básico para cualquier empresa que quiera salvaguardar la seguridad de sus sistemas.

Blue Team - Soc

Un equipo de defensa que esté constantemente revisando la información que circula por nuestra red y aplicando mecanismos de defensa.

Segmentación de red

Una correcta segmentación permite asumir riesgos y segmentar trabajos de auditoría, priorizando y dedicando más recursos a las partes más delicadas.

Plan de seguridad de la información

El conjunto de políticas de administración de la información dentro de una compañía. Suele ir asociado a un SGSI. La norma ISO que lo avala es la 27001

Vulnerabilidad - Cerraduras Bluetooth

Envío en **texto plano** de la **contraseña** vía **Bluetooth**.

Solución

Correcto inventariado

En muchos casos no somos conscientes de la cantidad de dispositivos que tenemos conectados a nuestra red.

Actualizaciones de seguridad

La dificultad de actualizar estos dispositivos los hace especialmente vulnerables.

Plan de auditoría técnica

Un correcto plan de auditoría sobre nuestra red es básico para cualquier empresa que quiera salvaguardar la seguridad de sus sistemas.

Blue Team - Soc

Un equipo de defensa que esté constantemente revisando la información que circula por nuestra red y aplicando mecanismos de defensa.

Segmentación de red

Una correcta segmentación permite asumir riesgos y segmentar trabajos de auditoría, priorizando y dedicando más recursos a las partes más delicadas.

Plan de seguridad de la información

El conjunto de políticas de administración de la información dentro de una compañía. Suele ir asociado a un SGSI. La norma ISO que lo avala es la 27001

Solución Vecino

Correcto inventariado

En muchos casos no somos conscientes de la cantidad de dispositivos que tenemos conectados a nuestra red.

Actualizaciones de seguridad

La dificultad de actualizar estos dispositivos los hace especialmente vulnerables.

Plan de auditoría técnica

Un correcto plan de auditoría sobre nuestra red es básico para cualquier empresa que quiera salvaguardar la seguridad de sus sistemas.

Blue Team - Soc

Un equipo de defensa que esté constantemente revisando la información que circula por nuestra red y aplicando mecanismos de defensa.

Segmentación de red

Una correcta segmentación permite asumir riesgos y segmentar trabajos de auditoría, priorizando y dedicando más recursos a las partes más delicadas.

Plan de seguridad de la información

El conjunto de políticas de administración de la información dentro de una compañía. Suele ir asociado a un SGSI. La norma ISO que lo avala es la 27001

Vulnerabilidad - Bomba de insulina

Usada **mundialmente**, en **2015** se reportan 8 vulnerabilidades, en **2018** se espera una versión que corrija los fallos de su predecesor.

Solución

Correcto inventariado

En muchos casos no somos conscientes de la cantidad de dispositivos que tenemos conectados a nuestra red.

Actualizaciones de seguridad

La dificultad de actualizar estos dispositivos los hace especialmente vulnerables.

Plan de auditoría técnica

Un correcto plan de auditoría sobre nuestra red es básico para cualquier empresa que quiera salvaguardar la seguridad de sus sistemas.

Blue Team - Soc

Un equipo de defensa que esté constantemente revisando la información que circula por nuestra red y aplicando mecanismos de defensa.

Segmentación de red

Una correcta segmentación permite asumir riesgos y segmentar trabajos de auditoría, priorizando y dedicando más recursos a las partes más delicadas.

Plan de seguridad de la información

El conjunto de políticas de administración de la información dentro de una compañía. Suele ir asociado a un SGSI. La norma ISO que lo avala es la 27001

Solución

Correcto inventariado

En muchos casos no somos conscientes de la cantidad de dispositivos que tenemos conectados a nuestra red.

Actualizaciones de seguridad

La dificultad de actualizar estos dispositivos los hace especialmente vulnerables.

Plan de auditoría técnica

Un correcto plan de auditoría sobre nuestra red es básico para cualquier empresa que quiera salvaguardar la seguridad de sus sistemas.

Blue Team - Soc

Un equipo de defensa que esté constantemente revisando la información que circula por nuestra red y aplicando mecanismos de defensa.

Segmentación de red

Una correcta segmentación permite asumir riesgos y segmentar trabajos de auditoría, priorizando y dedicando más recursos a las partes más delicadas.

Plan de seguridad de la información

El conjunto de políticas de administración de la información dentro de una compañía. Suele ir asociado a un SGSI. La norma ISO que lo avala es la 27001

Vulnerabilidad - Marcapasos Hackeado 'St Jude Medical'

La vulnerabilidad obliga a **medio millón de personas** a cambiar el dispositivo instalado. La explotación de la **vulnerabilidad** podría causarles la **muerte**.

Solución

Correcto inventariado

En muchos casos no somos conscientes de la cantidad de dispositivos que tenemos conectados a nuestra red.

Actualizaciones de seguridad

La dificultad de actualizar estos dispositivos los hace especialmente vulnerables.

Plan de auditoría técnica

Un correcto plan de auditoría sobre nuestra red es básico para cualquier empresa que quiera salvaguardar la seguridad de sus sistemas.

Blue Team - Soc

Un equipo de defensa que esté constantemente revisando la información que circula por nuestra red y aplicando mecanismos de defensa.

Segmentación de red

Una correcta segmentación permite asumir riesgos y segmentar trabajos de auditoría, priorizando y dedicando más recursos a las partes más delicadas.

Plan de seguridad de la información

El conjunto de políticas de administración de la información dentro de una compañía. Suele ir asociado a un SGSI. La norma ISO que lo avala es la 27001

Solución - Punto de vista del fabricante

Correcto inventariado

En muchos casos no somos conscientes de la cantidad de dispositivos que tenemos conectados a nuestra red.

Actualizaciones de seguridad

La dificultad de actualizar estos dispositivos los hace especialmente vulnerables.

Plan de auditoría técnica

Un correcto plan de auditoría sobre nuestra red es básico para cualquier empresa que quiera salvaguardar la seguridad de sus sistemas.

Blue Team - Soc

Un equipo de defensa que esté constantemente revisando la información que circula por nuestra red y aplicando mecanismos de defensa.

Segmentación de red

Una correcta segmentación permite asumir riesgos y segmentar trabajos de auditoría, priorizando y dedicando más recursos a las partes más delicadas.

Plan de seguridad de la información

El conjunto de políticas de administración de la información dentro de una compañía. Suele ir asociado a un SGSI. La norma ISO que lo avala es la 27001

Vulnerabilidad - Jeep SUV

Vulnerabilidad obliga a retirar 1,4 millones de vehículos en circulación.

Solución

Correcto inventariado

En muchos casos no somos conscientes de la cantidad de dispositivos que tenemos conectados a nuestra red.

Actualizaciones de seguridad

La dificultad de actualizar estos dispositivos los hace especialmente vulnerables.

Plan de auditoría técnica

Un correcto plan de auditoría sobre nuestra red es básico para cualquier empresa que quiera salvaguardar la seguridad de sus sistemas.

Blue Team - Soc

Un equipo de defensa que esté constantemente revisando la información que circula por nuestra red y aplicando mecanismos de defensa.

Segmentación de red

Una correcta segmentación permite asumir riesgos y segmentar trabajos de auditoría, priorizando y dedicando más recursos a las partes más delicadas.

Plan de seguridad de la información

El conjunto de políticas de administración de la información dentro de una compañía. Suele ir asociado a un SGSI. La norma ISO que lo avala es la 27001

Solución

Correcto inventariado

En muchos casos no somos conscientes de la cantidad de dispositivos que tenemos conectados a nuestra red.

Actualizaciones de seguridad

La dificultad de actualizar estos dispositivos los hace especialmente vulnerables.

Plan de auditoría técnica

Un correcto plan de auditoría sobre nuestra red es básico para cualquier empresa que quiera salvaguardar la seguridad de sus sistemas.

Blue Team - Soc

Un equipo de defensa que esté constantemente revisando la información que circula por nuestra red y aplicando mecanismos de defensa.

Segmentación de red

Una correcta segmentación permite asumir riesgos y segmentar trabajos de auditoría, priorizando y dedicando más recursos a las partes más delicadas.

Plan de seguridad de la información

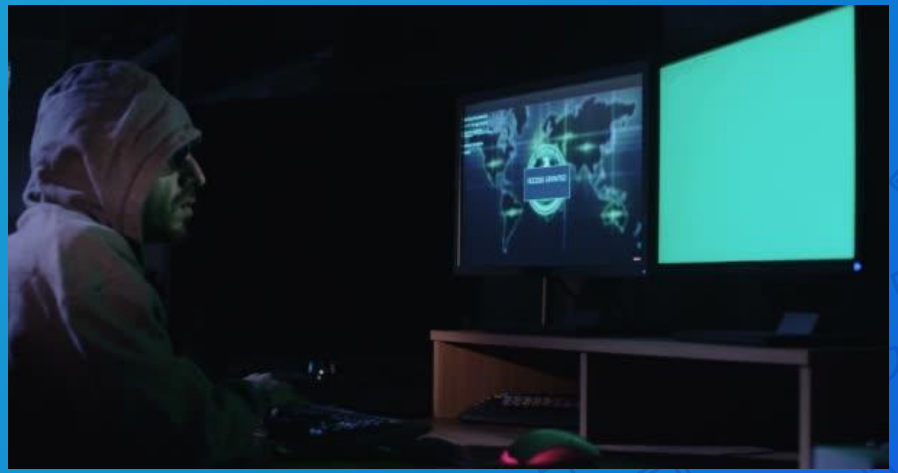
El conjunto de políticas de administración de la información dentro de una compañía. Suele ir asociado a un SGSI. La norma ISO que lo avala es la 27001

La seguridad es un proceso

4.
En la piel del atacante

Demo Time.

En la piel del atacante



5.
Conclusiones

Gracias!

preguntas?