



CYBERGUARD

INTEGRAL · INFORMATION · IMPROVEMENT





CIBERSEGURETAT

una recomanació
del nou reglament



- › ¿Què cal fer si som víctimes d'un robatori d'informació?





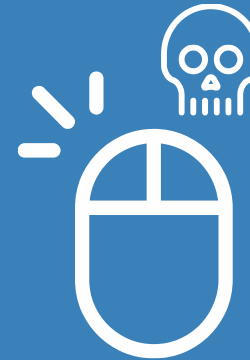
Classificació de vulnerabilitats:



Atacs
d'origen extern



Atacs
d'origen interns



Riscos associats
al mal ús



Hola!

Joel Gámez

Director tècnic de CYBERGUARD

info@cyberguard.es



Escenari actual del món de la ciberdelinqüència





Introducció a l'automatització de processos fets servir pels cibercriminals

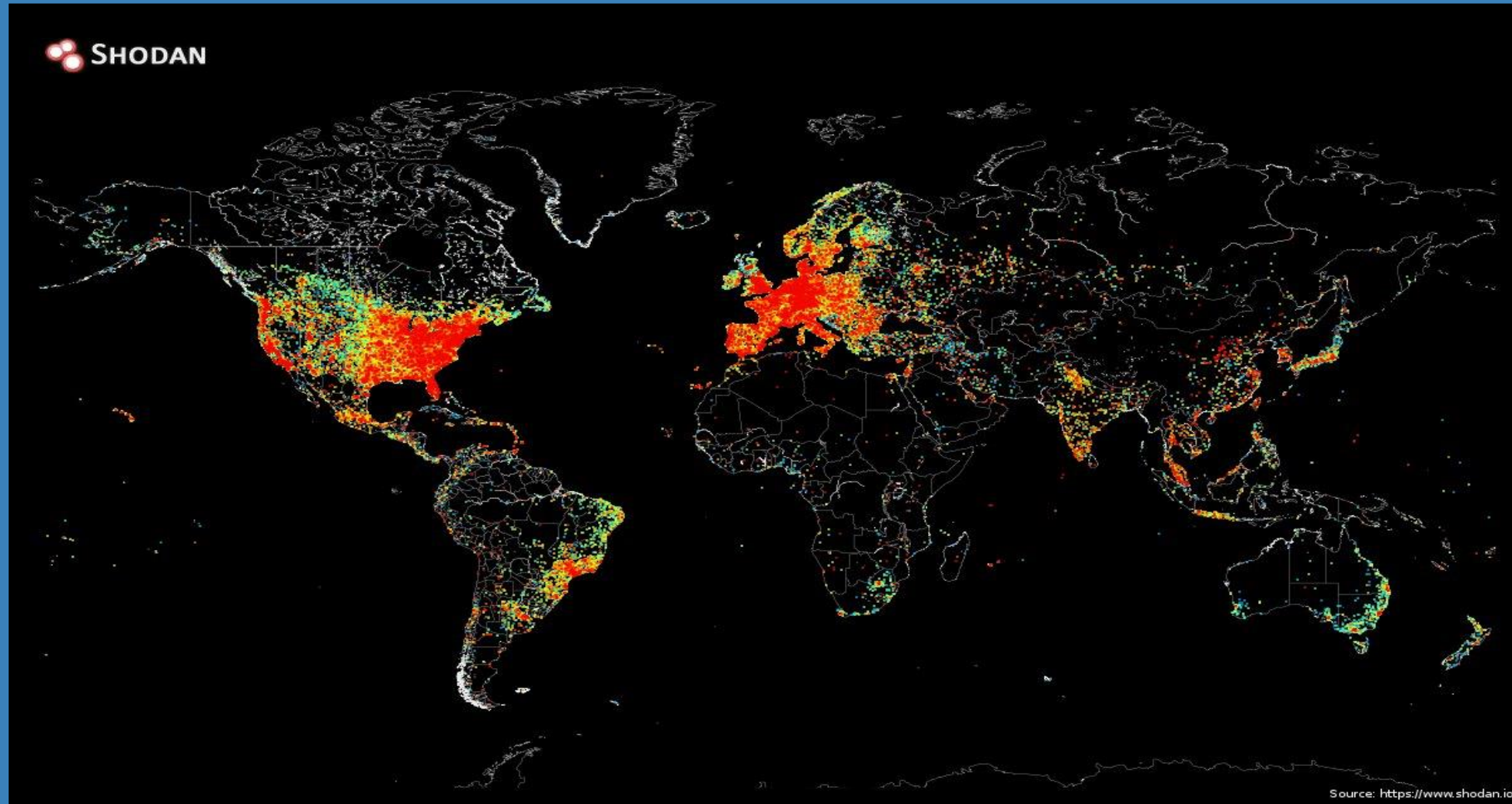
Atacs massius a servidors d'accés públic amb Shodan, Censys o Zoomeye

Atacs dirigits o focalitzats (SpearPhising)

Infraestructures de Ransomware



Atacs massius a servidors d'accés públic





Atacs massius a servidors d'accés públic

The screenshot displays the Shodan website interface. At the top, there is a navigation bar with the Shodan logo, a search input field, and links for 'Explore', 'Developer Pricing', 'Enterprise Access', 'Contact Us', 'New to Shodan?', and 'Login or Register'. Below the navigation bar is a large 'Explore' section with the subtitle 'Discover the Internet using search queries shared by other users.' The main content area is divided into three columns: 'Featured Categories', 'Top Voted', and 'Recently Shared'. The 'Featured Categories' column lists 'Industrial Control Systems', 'Databases', and 'Video Games'. The 'Top Voted' column shows search results for 'Webcam' (9,843 votes), 'Cams' (3,867 votes), and 'Netcam' (2,171 votes). The 'Recently Shared' column shows results for 'Smart Ethernet Remote I/O' (1 share), 'LG Network Storage Devices' (2 shares), and 'default+password' (3 shares).

SHODAN [Search Bar] [Explore] [Developer Pricing] [Enterprise Access] [Contact Us] [New to Shodan?] [Login or Register]

Explore

Discover the Internet using search queries shared by other users.

Featured Categories

- Industrial Control Systems
- Databases
- Video Games

Top Voted

- 9,843** **Webcam**
best ip cam search I have found yet.
[webcam] [surveillance] [cams] 2010-03-15
- 3,867** **Cams**
admin admin
[cam] [webcam] 2012-02-06
- 2,171** **Netcam**
Netcam
[netcam] 2012-01-13
- 1,460**

Recently Shared

- 1** **Smart Ethernet Remote I/O**
ioLogik E2210
[scada] 2018-04-19
- 2** **LG Network Storage Devices**
<https://thehackernews.com/2018/04/hacking-nas-d...>
[lg] [nas] 2018-04-18
- 3** **default+password**
2018-04-18
- 1**



Atacs massius a servidors d'accés públic

```
baal@baal-Aspire-5733Z: ~/bin/python/autosplit
File Edit View Search Terminal Help

--+ Graffiti the world with exploits +--
--+                                     +--
--+      AS                             +--
--+      AutoSploit                     +--
--+      NullArray/Eku                  +--
--+      v(2.0)                         +--

[+] welcome to autosplit, give us a little bit while we configure
[+] checking for services
[-] no arguments have been parsed, defaulting to terminal session. press 99 to quit and help to get help
[+] checking if there are multiple exploit files
[+] attempting to load API keys
[+] Shodan API token loaded from /home/baal/bin/python/autosplit/etc/tokens/shodan.key
[+] Censys API token loaded from /home/baal/bin/python/autosplit/etc/tokens/censys.key
1. Usage And Legal
2. Gather Hosts
3. Custom Hosts
4. Add Single Host
5. View Gathered Hosts
6. Exploit Gathered Hosts
99. Quit

root@autosplit# 2
-----
[?] enter your search query: iis
[?] enter your proxy (blank for none):
[?] do you want to use a (p)ersonal user agent, a (r)andom one, or (d)efault: r
[i] setting HTTP User-Agent to: 'Opera/9.23 (Mac OS X; fr)'
[+] please choose an API to gather from (choosing two or more separate by comma IE; 1,2)
1. Shodan
2. Zoomeye
3. Censys

root@autosplit# 1
searching Shodan with given query 'iis'...
```

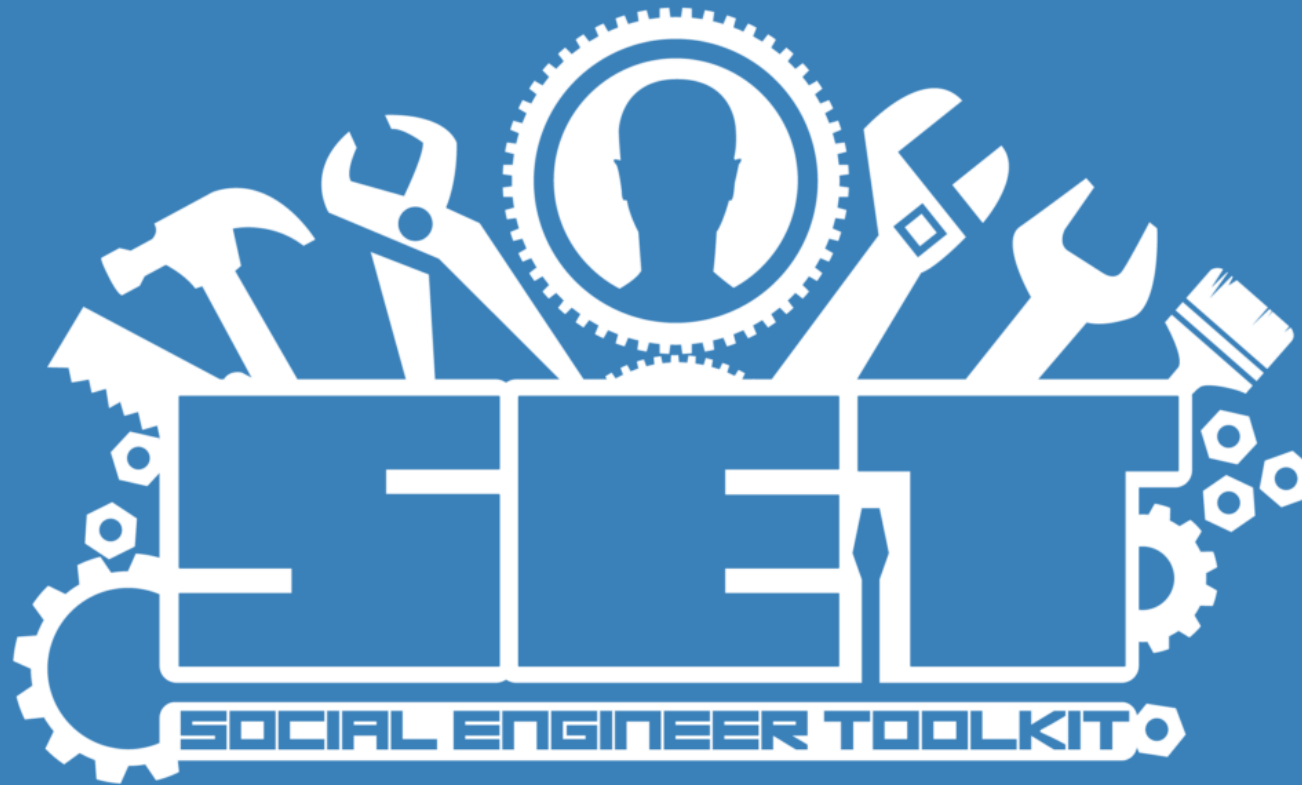


Atacs dirigits o focalitzats (SpearPishing)





Atacs dirigits o focalitzats (SpearPishing)





Atacs dirigits o focalitzats (SpearPhishing)

```
[---] The Social-Engineer Toolkit (SET) [---]
[---] Created by: David Kennedy (ReL1K) [---]
[---] Version: 7.0.3 [---]
[---] Codename: 'RemembRance' [---]
[---] Follow us on Twitter: @TrustedSec [---]
[---] Follow me on Twitter: @HackingDave [---]
[---] Homepage: https://www.trustedsec.com [---]
```

Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

Join us on irc.freenode.net in channel #setoolkit

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: <https://www.trustedsec.com>

Select from the menu:

- 1) Social-Engineering Attacks
- 2) Fast-Track Penetration Testing
- 3) Third Party Modules
- 4) Update the Social-Engineer Toolkit
- 5) Update SET configuration
- 6) Help, Credits, and About

99) Exit the Social-Engineer Toolkit

set> █

alien linux



Infrastructures de Ransomware





Infraestructuras de Ransomware

WannaCry

WannaCry, también conocido como **WanaCrypt0r 2.0**,¹ es un *programa dañino* de tipo *ransomware*.

Índice [ocultar]

- 1 Ciberataque global
 - 1.1 Origen
- 2 Véase también
- 3 Referencias

Ciberataque global [editar]

El 12 de mayo de 2017 entre las 8 y las 17:08 horas UTC² se registró un **ataque a escala mundial** que afectó a las empresas **Telefónica**, **Iberdrola** y **Gas Natural**, entre otras compañías en **España**,³ así como al **servicio de salud británico**, como confirmó el **Centro Nacional de Inteligencia**.^{4 5 6 7 8} La prensa digital informaba aquel día que al menos 141 000 computadores habían sido atacados en todo el mundo.^{9 10 11}

Los expertos sostienen que WannaCry usó la vulnerabilidad **EternalBlue**, desarrollada por la **Agencia de Seguridad Nacional** estadounidense y filtrada por el grupo **The Shadow Brokers**, que permite atacar computadores con el sistema operativo **Microsoft Windows**¹ no actualizados debidamente. La compañía **Microsoft** había comenzado a distribuir actualizaciones de seguridad al día siguiente de conocerse esta vulnerabilidad, el 10 de marzo de 2017,¹² a través de **Windows Update**, pero sólomente para las versiones de Windows posteriores a **Windows Vista**. El 13 de mayo de 2017, ante la supuesta gravedad del ataque, publicó un parche separado para Windows 8, Server 2003 y XP.¹³ Muchos computadores que no tenían aplicadas las actualizaciones de seguridad MS17-010 de marzo de 2017 quedaron gravemente afectados,¹⁰ con sus archivos cifrados y mostrando un mensaje en pantalla que exigía un rescate de 300 dólares en **bitcoins** a cambio de descifrar los archivos.

En realidad, un experto de Reino Unido evitó en gran medida la expansión del ciberataque global. El autor del blog **MalwareTech** estaba estudiando el programa dañino cuando se dio cuenta de que el mismo intentaba conectarse a un dominio no registrado: si no lo lograba, cifraba el equipo; si lo lograba, se detenía.² Una vez que este experto en seguridad registró el dominio, a las 17:08 UTC del 12 de mayo, cesó el ataque. Todas las medidas urgentes que se tomaron a partir de esa hora fueron prácticamente innecesarias.

Un análisis del *malware* ha sido publicado por **Microsoft**.¹⁴

WannaCry



■ Países afectados por el ciberataque.

Información	
Nombre técnico	WanaCrypt0r 2.0
Alias	Wannadecryptor
Clasificación	Gusano informático
Tipo	ransomware
Sistema operativo	Windows XP, Windows 7, Windows 8.1, Windows 10 y Windows Server 2008 ✎

[editar datos en Wikidata]



Atacs, infeccions i vulnerabilitats més comunes

Atacs externs per força bruta i malware

Atacs interns a través de xarxes sense fils,
backdoors i eines de hacking

Exfiltració i mala praxis d'us de les dades



Atacs externs per força bruta, malware i vulnerabilitats web





Atacs externs per força bruta, malware i vulnerabilitats web

```
Parrot Terminal
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
[user@parrot]~$ medusa -d
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

Available modules in ".":

Available modules in "/usr/lib/medusa/modules":
+ cvs.mod : Brute force module for CVS sessions : version 2.0
+ ftp.mod : Brute force module for FTP/FTPS sessions : version 2.1
+ http.mod : Brute force module for HTTP : version 2.1
+ imap.mod : Brute force module for IMAP sessions : version 2.0
+ mssql.mod : Brute force module for MS-SQL sessions : version 2.0
+ mysql.mod : Brute force module for MySQL sessions : version 2.0
+ nntp.mod : Brute force module for NNTP sessions : version 2.0
+ pcan anywhere.mod : Brute force module for Pcan anywhere sessions : version 2.0
+ pop3.mod : Brute force module for POP3 sessions : version 2.0
+ postgres.mod : Brute force module for PostgreSQL sessions : version 2.0
+ rdp.mod : Brute force module for RDP (Microsoft Terminal Server) sessions : version 0.1
+ rexec.mod : Brute force module for REXEC sessions : version 2.0
+ rlogin.mod : Brute force module for RLOGIN sessions : version 2.0
+ rsh.mod : Brute force module for RSH sessions : version 2.0
+ smbnt.mod : Brute force module for SMB (LM/NTLM/LMv2/NTLMv2) sessions : version 2.1
+ smtp-vrfy.mod : Brute force module for verifying SMTP accounts (VRFY/EXPN/RCPT TO) : version 2.1
+ smtp.mod : Brute force module for SMTP Authentication with TLS : version 2.0
+ snmp.mod : Brute force module for SNMP Community Strings : version 2.1
+ ssh.mod : Brute force module for SSH v2 sessions : version 2.1
+ svn.mod : Brute force module for Subversion sessions : version 2.1
+ telnet.mod : Brute force module for telnet sessions : version 2.0
+ vmauthd.mod : Brute force module for the VMware Authentication Daemon : version 2.0
+ vnc.mod : Brute force module for VNC sessions : version 2.1
+ web-form.mod : Brute force module for web forms : version 2.1
+ wrapper.mod : Generic Wrapper Module : version 2.0

[user@parrot]~$
```



Atacs externs per força bruta, malware i vulnerabilitats web





Atacs externs per força bruta i malware

ENDESA

NO HAGAS CLICK

RESUMEN DE LA FACTURA

Fecha factura: 30 de mayo de 2016

Periodo de facturación: del 28/04/2016 al 29/05/2016

Factura nº: PD3485XX794885

Ref.Factura: 72970720 6332 44476

Total Factura: 577,43 €

Datos del Cliente

código personal: 14697298

Actividad económica (CNAE): 3782

CUPS: ES28278466QEFP

Potencia contratada: 26,3, 26,3 Y 26,3 kW

Tarifa de acceso: 3.0A

Contrato de acceso: 4738264336

Número de Contador: 61123677

[CONSULTA TU FACTURA Y CONSUMO](#)



Atacs interns a través de xarxes sense fils, backdoors i eines de hacking





Atacs interns a través de xarxes sense fils, backdoors i eines de hacking





Atacs interns a través de xarxes sense fils, backdoors i eines de hacking





Atacs interns a través de xarxes sense fils, backdoors i eines de hacking





Atacs interns a través de xarxes sense fils, backdoors i eines de hacking

```
ee\ _
< 0
J . . . . .
| | . . . . .
L | | . . . . .
J | | . . . . .
| | . . . . .
) ^ ^ (
( . / \ . )

[1] CREATE BACKDOOR WITH MSFVENOM
[2] CREATE FUD 100% BACKDOOR ( SLOW BUT POWERFULL )
[3] CREATE A LISTENERS
[4] JUMP TO MSFCONSOLE
[5] SEARCHSPLOIT
[6] HELP
[7] CREDITS

Screetsec@Fatrat: █
```



Atacs interns a través de xarxes sense fils, backdoors i eines de hacking



ADD TO CART

HAK5 ESSENTIALS FIELD KIT

\$219.99



ADD TO CART

HAK5 ELITE FIELD KIT

\$599.99



Exfiltració i mala praxis d'us de les dades

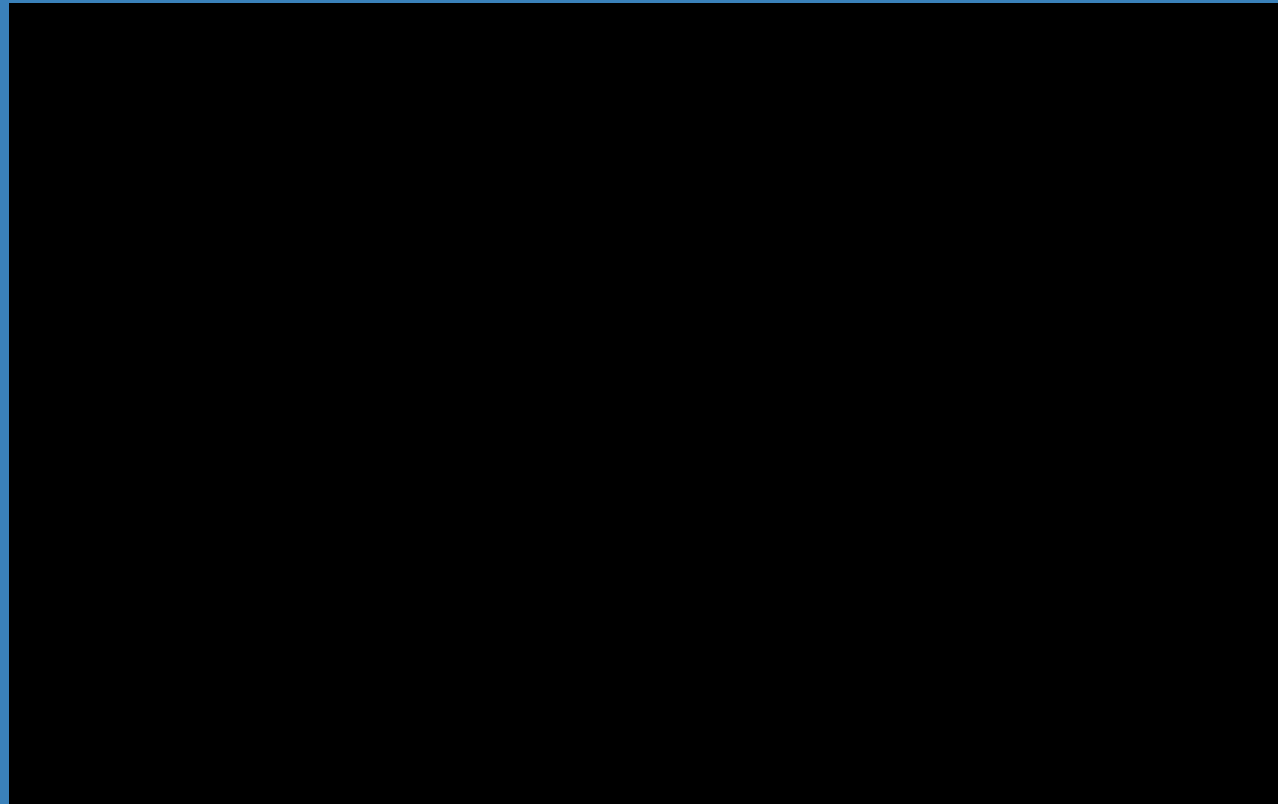
Copia de dades en dispositius externs

Enviament d'informació per correu electrònic

Enviament informació per altres medis
(WeTransfer, Dropbox o Google Drive)



Dramatització i recreació de les tècniques aquí descrites





Primera passa...



AUDITAR



Segona passa...
ACTUAR



Tercera passa...
MANTENIR/ACTUALITZAR



Firewall





Atacs d'origen extern



IPS
Intercept X
XG Firewall

Aturi les amenaces a la porta

- ✓ Aturi el malware i el ransomware.
- ✓ Aturi els atacs de robatori de dades al perímetre de la xarxa.



Atacs d'origen interns



Secure WiFi
User & APP Control

Aconsegueixi connexions Wifi segures

- ✓ Wireless gestionat per dispositiu.
- ✓ Polítiques de seguretat sobre els dispositius d'enmagatzement extern.



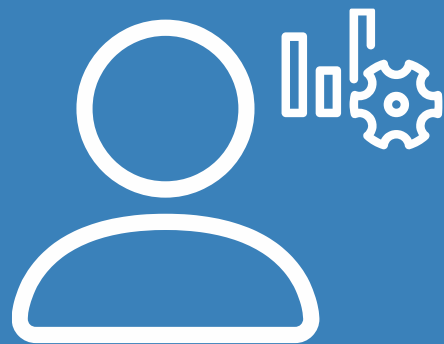
Riscos associats al mal ús



DLP
Email Appliance
Central Device Encryption

Aturi els errors humans

- ✓ Bloquegi i xifri les dades confidencials als correus.
- ✓ Asseguris de que només les persones autoritzades puguin accedir als arxius confidencials.
- ✓ Mantingui les seves dades protegides si perd els seus dispositius o els hi roben.



Manteniment proactiu i periòdic

- ✓ Actualització dels sistemes de seguretat.
- ✓ Manteniment proactiu dels sistemes.



La nostra oferta de seguretat informàtica per empreses

SOL·LUCIÓ INTEGRAL DE SEGURETAT INFORMÀTICA

1- AUDITORIA INFORMÀTICA BÀSICA DE SEGURETAT

- Per detectar les principals debilitats i amenaces.

inclòs en el preu*

* Possibilitat de realitzar auditories més profundes i personalitzades.
Demana'ns més informació.

2- IMPLANTACIÓ FIREWALL I SOLUCIONS DE SEGURETAT

- IPS: Sistema de prevenció d'intrusions.
- Protecció contra amenaces avançades.
- DLP: Protecció contra la filtració de dades.
- Xifrat SPX: Enviament segur de correu electrònic.

desde 1.495 €

3- MANTENIMENT PROACTIU I PERIÒDIC

- Actualització dels sistemes de seguretat.
- Manteniment proactiu dels sistemes.

desde 49 € / mes



CYBERGUARD

INTEGRAL · INFORMATION · IMPROVEMENT

Gràcies!



+34 93 159 59 05

info@cyberguard.es

www.cyberguard.es