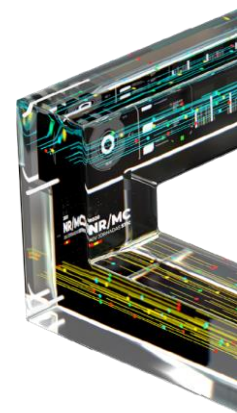


# #XIVJORNADASCCNCERT

**“Por qué exigir cualificaciones del CCN y no análisis de empresas privadas. Caso de uso del producto cualificado de Stormshield”**





***Borja Pérez***

***Stormshield***

***Borja.perez@Stormshield.eu***

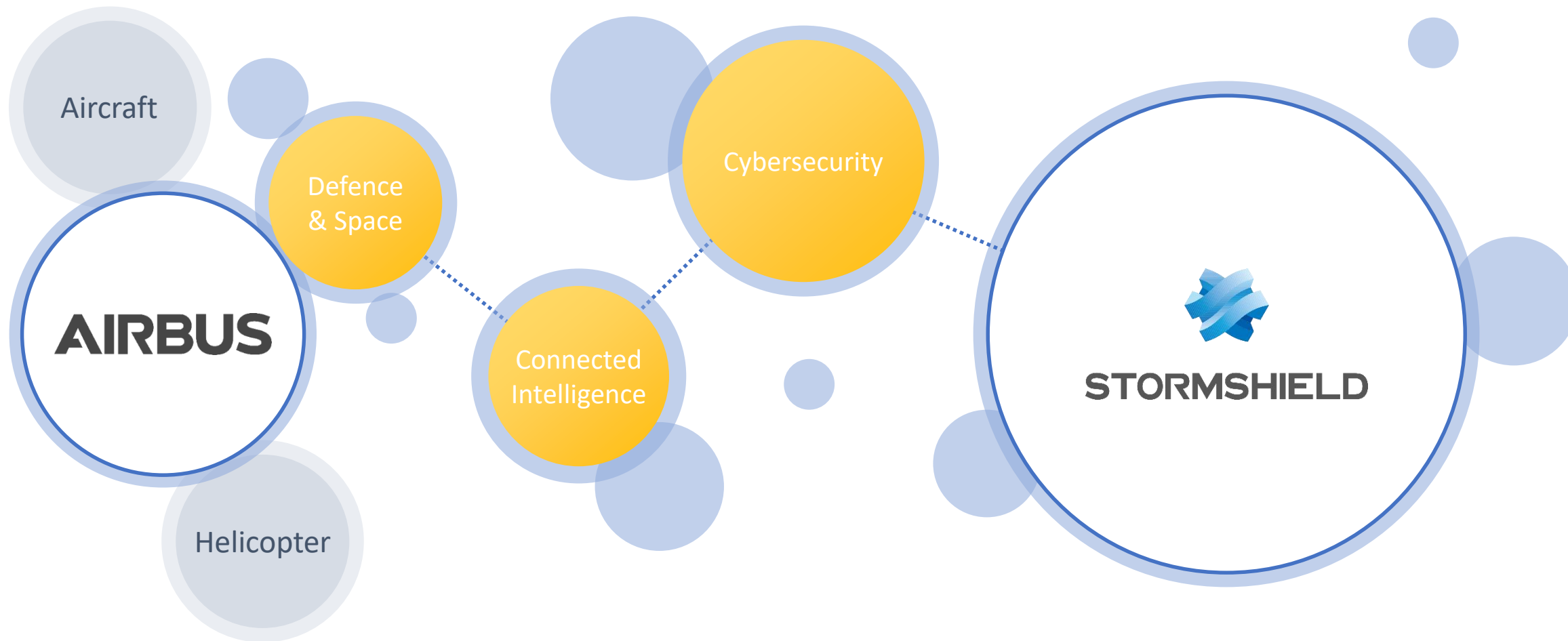
---

# Agenda

- Importancia de organismos de certificación públicos:
  - CCN
  - ENISA
  - Otros (Eu Restricted, OTAN, ANSSI,...)
  - Auditoría del código fuente.
- Qué miden realmente analistas como Gartner.
- Cómo ayuda el CCN a mejorar los productos de seguridad.
- Stormshield: Primer firewall en obtener ambas cualificaciones: Producto cualificado y producto aprobado.
- Entorno IT y OT (también infraestructura crítica).
- Caso práctico de uso: Gestión de vulnerabilidades e IDS/IPS.

# Stormshield

*Grupo Airbus*



# Soluciones de seguridad certificadas y cualificadas



UE & OTAN Restreint

---



Common Criteria

---



VISA ANSSI (QS) / FR

---



CCN Aprobado / ES

---

Centro Criptológico Nacional  
National Cryptology Centre

Participación en el trabajo de **ENISA** (European Union Agency for Cybersecurity)  
para el future modelo de certificación

# ¿Qué se pide en los concursos públicos?

## Subtítulo

La solución propuesta deberá posicionarse en el cuadrante superior derecho del “Gartner Magic Quadrant for Enterprise Network Firewalls” durante los 3 años anteriores a la publicación del expediente, (2017, 2016 y 2015), estimándose que es una referencia suficientemente reconocida en el mercado respecto de las soluciones de cortafuegos para redes empresariales y de la madurez de la solución.

8. Por motivos de solvencia técnica se requiere que los equipos ofertados correspondan a un fabricante listado como Líder en el último cuadrante de Gartner Network Firewall que esté publicado en la fecha de comienzo de admisión de ofertas.

### 4.1.- Reconocimientos de terceros

- a) Los equipos objeto de este proyecto ha de ser conforme con lo dispuesto en el Esquema Nacional de Seguridad y deben estar incluidos en la guía CCN-STIC 105 Catálogo de Productos e Seguridad de las Tecnologías de la Información y la Comunicación (CPSTIC) como Productos Cualificados, donde se incluyen aquellos que cumplen los requisitos de seguridad exigidos para el manejo de información sensible en el ENS, en cualquiera de sus categorías (Alta, Media y Básica).
- b) Solución ubicada como líder en el último Cuadrante mágico Endpoint Protection de Gartner.
- c) Solución ubicada como líder en el último cuadrante mágico UTM de Gartner.
- d) La solución de protección de Endpoint deberá aparecer además como líder en el último cuadrante de Forrester.

Els fabricants dels equips tallafocs ofertats hauran d'estar en l'apartat “Leaders” de l'últim quadrant màgic de Gartner de tallafocs del 2019.

---

# ¿Qué mide realmente Gartner?

<https://www.brightworkresearch.com/best-understand-gartners-magic-quadrant/>

- El cuadrante no es una recomendación. Mejor leer el análisis que quedarse en la foto general.
- Gartner habla con directivos de nivel C. No con implementadores de las soluciones.
- No analiza ni prueba productos.
- Parte de la información sobre productos viene de encuestas a clientes y partners de los fabricantes. Propuestos por los fabricantes.
- Información más útil para inversores que para compradores de tecnología.
- Calsificación no basada en producto:
  - 6 de los 15 criterios utilizados tienen algo que ver con el producto (40%).
  - Sólo 2 de los 15 (13%), directamente con producto.
- Beneficia a empresas grandes y de EEUU.

# ¿Qué mide realmente Gartner? Ejemplo

<https://www.brightworkresearch.com/best-understand-gartners-magic-quadrant/>

| Sample Gartner Magic Quadrant Ranking |                         | Small Vendor A | Large Vendor B |
|---------------------------------------|-------------------------|----------------|----------------|
| Completeness of Vision Criteria       | Criteria Category       | Score (1 - 10) | Score (1 - 10) |
| Market Understanding                  | *Product                | 10             | 5              |
| Marketing Strategy                    | Marketing               | 3              | 8              |
| Sales Strategy                        | Sales                   | 4              | 10             |
| Offering (Product) Strategy           | *Product                | 10             | 2              |
| Business Model                        | Finance                 | 5              | 9              |
| Vertical/Industry Strategy            | Industry Specialization | 6              | 8              |
| Innovation                            | Application             | 10             | 2              |
| Geographic Strategy                   | Scale                   | 3              | 10             |
| <i>Total</i>                          |                         | <i>51</i>      | <i>54</i>      |

| Ability to Execute                     | Criteria Category                                     | Score (1 - 10) | Score (1 - 10) |
|----------------------------------------|-------------------------------------------------------|----------------|----------------|
| Product/Service                        | *Product                                              | 10             | 2              |
| Overall Viability                      | Finance                                               | 4              | 10             |
| Sales Execution/Pricing                | Sales                                                 | 2              | 9              |
| Market Responsiveness and Track Record | Strategy                                              | 3              | 10             |
| Marketing Execution                    | Marketing                                             | 3              | 9              |
| Customer Experience                    | *Product                                              | 10             | 2              |
| Operations                             | *Multifaceted (But should be counted for the product) | 6              | 7              |
| <i>Total</i>                           |                                                       | <i>38</i>      | <i>49</i>      |

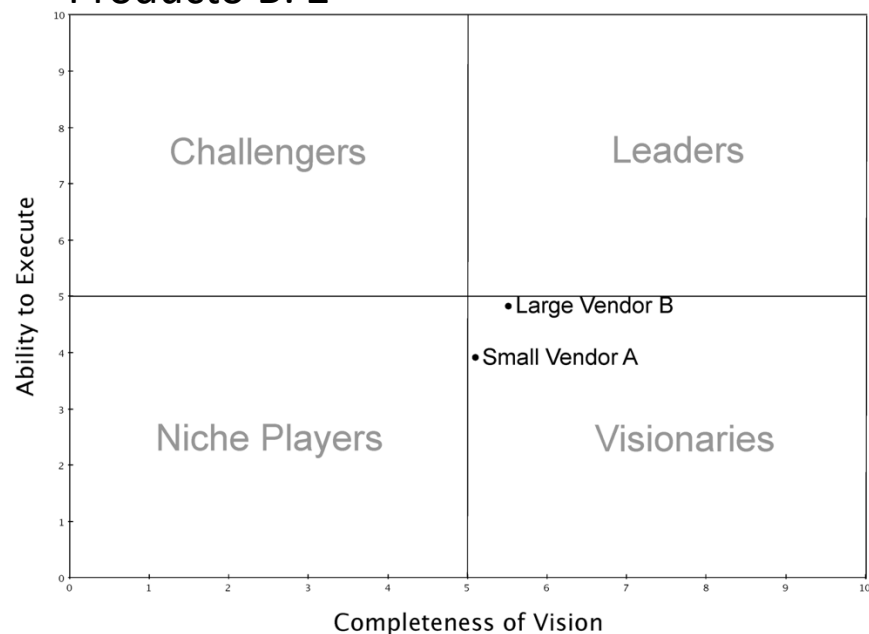
# ¿Qué mide realmente Gartner? Ejemplo

<https://www.brightworkresearch.com/best-understand-gartners-magic-quadrant/>

Con los valores de la tabla anterior.

Producto A: 10

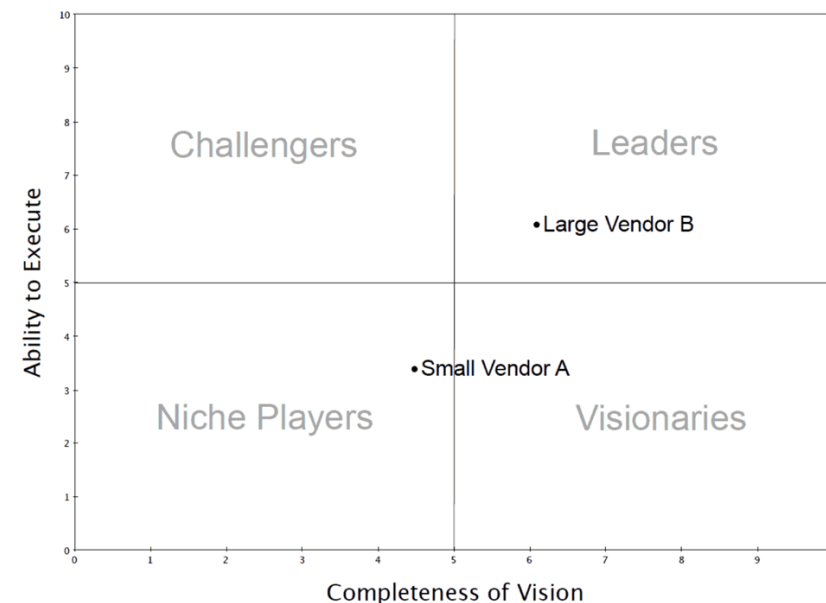
Producto B: 2



Modificando los valores.

Producto A: 7

Producto B: 7



---

# ¿Qué es necesario para entrar en el CPSTIC?

- La adquisición de un producto de seguridad TIC que va a manejar información nacional clasificada o información sensible debe estar precedida de un **proceso de comprobación** de que los mecanismos de seguridad implementados en el producto son adecuados para proteger dicha información.
- Para la inclusión de un producto en el catálogo, el CCN tendrá en cuenta una serie de criterios, como, la clasificación de la información que puede manejar (Difusión Limitada, Confidencial, Reservado, Secreto), las características de seguridad del producto, la categoría del sistema de información en el que puede emplearse (alta, media, básica1), las certificaciones aportadas, el entorno donde se vaya a emplear, etc. En función de esta información, se determinarán las **pruebas o evaluaciones** que deberá superar el producto de seguridad TIC correspondiente.

# Catálogo de Productos STIC (CPSTIC)



## Listado de productos **cualificados**



Son productos que tienen certificadas sus funcionalidades de seguridad y **aptos para ser utilizados en sistemas afectados por el ENS**, en cualquiera de sus categorías (Alta, Media y Básica). El campo “Clasificación” que aparece en la ficha de cada producto indica hasta que categoría (Alta o Media) del sistema afectado por el ENS es apto el producto correspondiente. Los **productos con clasificación “ALTA”** podrán emplearse en sistemas clasificados como ENS categoría ALTA, MEDIA o BÁSICA y los productos con clasificación “MEDIA” podrán emplearse en sistemas clasificados como ENS categoría MEDIA o BÁSICA.



## Listado de productos **aprobados**

Son productos cuyo uso está aprobado en **sistemas que manejen información clasificada**.

# Catálogo de Productos STIC (CPSTIC)

Stormshield figura en ambos listados: **cualificados y aprobados**

<https://oc.ccn.cni.es/index.php/en/cis-product-catalogue/list-of-qualified-products/558-stormshield-network-security-utm-ng-firewall-appliances-desde-sn200-a-sn6100-en-4-compilaciones-distintas-s-m-l-y-xl-3-10-1>

<https://oc.ccn.cni.es/index.php/en/cis-product-catalogue/list-of-approved-products/572-stormshield-network-security-utm-ng-firewall-appliances-desde-sn200-a-sn6100-en-4-compilaciones-distintas-s-m-l-y-xl-version-3-10-1>

## Stormshield Network Security UTM/NG-Firewall (Appliances desde SN200 a SN6100 en 4 compilaciones distintas: S, M, L y XL) Versión 3.10.1

Category: **Protection of Communications**

Manufacturer: - **Stormshield SAS**

Family: **Firewall**

Classification: **Todos los niveles**

Inclusion Date: **2020-06-01**

Date Review Validity: **2021-01-07**

Firewalls de nueva generación de capa 7, IPS y concentrador de túneles VPN. Con capacidades de bloqueo de amenazas avanzadas, ataques de día cero, filtrado de navegación web o gestión de vulnerabilidades.

El mismo equipamiento realiza inspección profunda de protocolos OT, además de IT.

Procedimiento de empleo seguro pendiente de publicación.



Type:



---

# Ventajas del CPSTIC

## *Para las AAPP*

- Garantía de que las soluciones son adecuadas para cumplimiento del ENS.
- Procedimientos de empleo seguros disponibles:
  - En la web del CCN  : <https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/1000-procedimientos-de-empleo-seguro/5108-ccn-stic-1415-procedimiento-de-empleo-seguro-utm-ng-firewall-de-stormshield/file.html>
  - En la wiki de la comunidad de ProtAPP  : [https://wikirot.protaapp.com/04\\_tecnologias/#cortafuegos-firewall](https://wikirot.protaapp.com/04_tecnologias/#cortafuegos-firewall)

## *Para los fabricantes*

- Posibilidad de vender a AAPP
- Mejora del producto

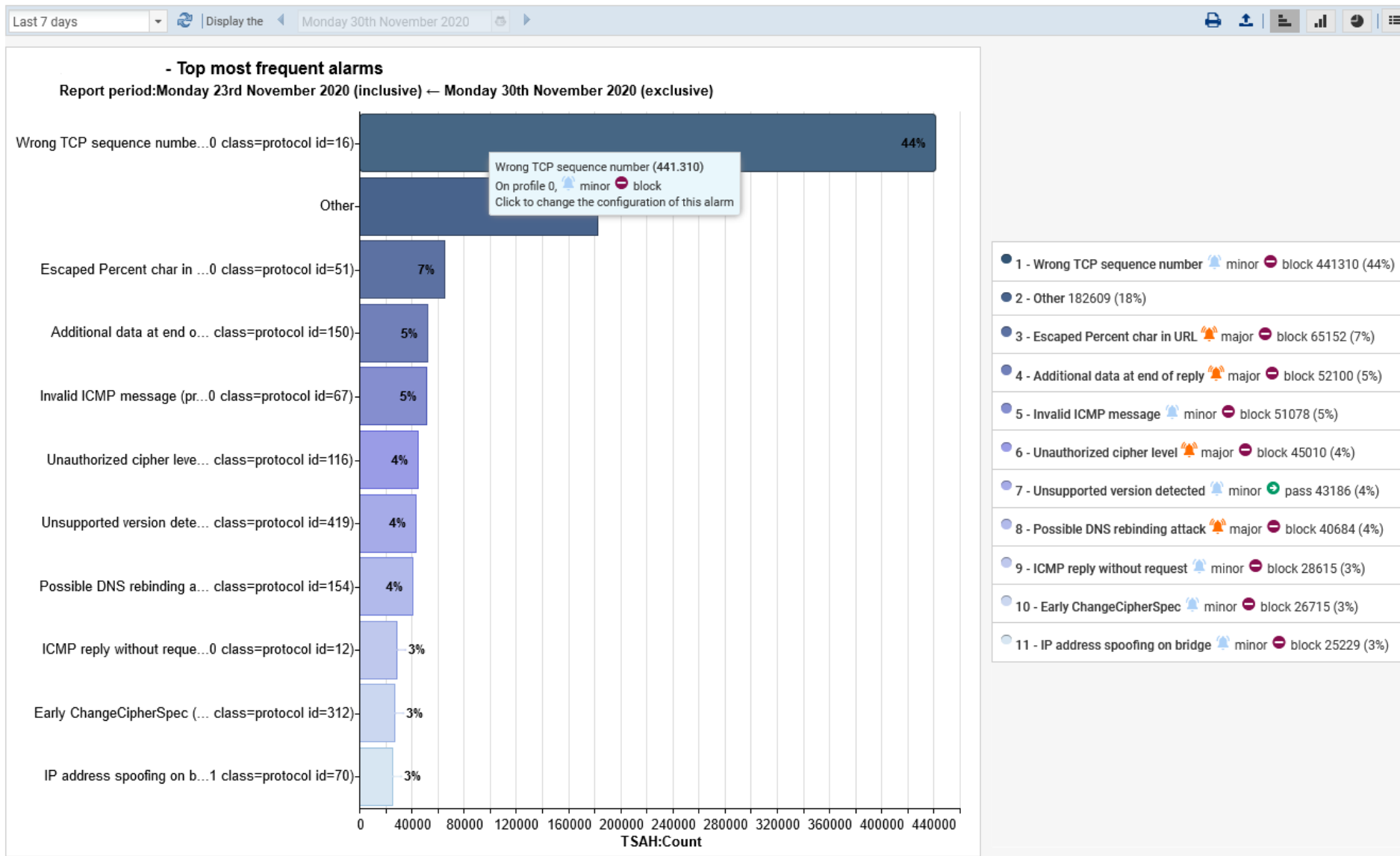
# Caso Práctico de Uso de Producto Cualificado Stormshield Network Security en CPD de CCAA

# Caso Práctico de Uso de Producto Cualificado



- SNS en CPD aporta las siguientes medidas adicionales a los firewalls existentes (dos fabricantes distintos)
  - IDS de todo el tráfico (DMZ y LAN) a través de un port span.
  - Segunda capa de Sandboxing.
  - Gestión de vulnerabilidades en tiempo real sin lanzar escaneos que introducen retardos.

## SECURITY / TOP MOST FREQUENT ALARMS



## LOG / VULNERABILITIES

Customized time range
Refresh
Search...
Advanced search
Actions

SEARCH FROM - 10/21/2020 04:45:00 PM - TO - 10/21/2020 05:45:59 PM

| Saved at               | Severity | Message                                                                           | Source Name |
|------------------------|----------|-----------------------------------------------------------------------------------|-------------|
| 10/21/2020 05:41:57 PM | High     | Oracle Java SE January 2017 Critical Patch Multiple Vulnerabilities               | Anonymized  |
| 10/21/2020 05:41:57 PM | High     | Oracle Java April 2016 Critical Patch Multiple Vulnerabilities                    | Anonymized  |
| 10/21/2020 05:41:57 PM | High     | Oracle Java July 2017 Critical Patch Multiple Vulnerabilities                     | Anonymized  |
| 10/21/2020 05:41:57 PM | High     | Oracle Java SE Hotspot Remote Code Execution Vulnerability Fixed by 8u77 and 7u99 | Anonymized  |
| 10/21/2020 05:41:57 PM | High     | Oracle Java SE October 2016 Critical Patch Multiple Vulnerabilities               | Anonymized  |
| 10/21/2020 05:41:57 PM | High     | Oracle Java July 2016 Critical Patch Multiple Vulnerabilities                     | Anonymized  |
| 10/21/2020 05:41:48 PM | Low      | OpenSSH Untrusted Cookie Creation Handling Security Bypass Weakness               | Anonymized  |
| 10/21/2020 05:41:48 PM | Low      | OpenSSH Cipher-Block Chaining Mode Plaintext Recovery Vulnerability               | Anonymized  |
| 10/21/2020 05:41:48 PM | Low      | OpenSSH 'ForceCommand' Directive Security Bypass Weakness                         | Anonymized  |
| 10/21/2020 05:41:48 PM | Low      | OpenSSH 'X11UseLocalhost' X11 Forwarding Session Hijacking Issue                  | Anonymized  |
| 10/21/2020 05:41:48 PM | Low      | OpenSSH Forwarded X Connection Information Disclosure Vulnerability               | Anonymized  |
| 10/21/2020 05:41:48 PM | Moderate | OpenSSH SSHD Information Exposure Via Timing Discrepancy Vulnerability            | Anonymized  |
| 10/21/2020 05:41:48 PM | Low      | OpenSSH Privilege Separation Monitor Key Signature Authentication Bypass          | Anonymized  |
| 10/21/2020 05:41:48 PM | Moderate | OpenSSH PAM Privilege Escalation Vulnerability                                    | Anonymized  |
| 10/21/2020 05:41:48 PM | Low      | OpenSSH World-Writable TTYs Vulnerability Fixed by 7.0                            | Anonymized  |
| 10/21/2020 05:41:48 PM | High     | OpenSSH PermitRootLogin Bypass Vulnerability Fixed by 7.1                         | Anonymized  |
| 10/21/2020 05:41:48 PM | Moderate | OpenSSH Portable Version Multiple Vulnerabilities Fixed by 7.0p1                  | Anonymized  |
| 10/21/2020 05:41:48 PM | Moderate | OpenSSH Multiple Security Bypass Vulnerabilities Fixed by 6.9                     | Anonymized  |
| 10/21/2020 05:41:48 PM | Low      | OpenSSH Certificate Validation Security Bypass Vulnerability                      | Anonymized  |
| 10/21/2020 05:41:48 PM | Moderate | OpenSSH AcceptEnv Wildcard Security Bypass Vulnerability Fixed by 6.6             | Anonymized  |
| 10/21/2020 05:41:48 PM | Low      | Portable OpenSSH 'ssh-keysign' Utility Host Keys Unauthorized Access              | Anonymized  |
| 10/21/2020 05:41:48 PM | Moderate | OpenSSH MaxAuthTries Security Bypass Vulnerability                                | Anonymized  |
| 10/21/2020 05:41:09 PM | High     | Google Chrome OS Unspecified Vulnerabilities Fixed by 60.0.3112.112               | Anonymized  |
| 10/21/2020 05:41:09 PM | High     | Google Chrome OS Unspecified Vulnerabilities Fixed by 60.0.3112.101               | Anonymized  |
| 10/21/2020 05:41:09 PM | High     | Google Chrome Multiple Vulnerabilities Fixed by 59.0.3071.86                      | Anonymized  |
| 10/21/2020 05:41:09 PM | High     | Google Chrome Multiple Vulnerabilities Fixed by 60.0.3112.78                      | Anonymized  |
| 10/21/2020 05:41:09 PM | High     | Google Chrome Multiple Vulnerabilities Fixed by 59.0.3071.104                     | Anonymized  |
| 10/21/2020 05:41:09 PM | High     | Google Chrome OS Unspecified Vulnerabilities Fixed by 58.0.3029.140               | Anonymized  |

LOG LINE DETAILS

Dates

Saved at

10/21/2020 05:41:57 PM

Date and time

10/21/2020 05:41:58 PM

Time difference between local time ...

+0200

Source

Source Name

Anonymized

Source

Anonymized

group:Misc

Logs

pvm

Severity

High

Message

Oracle Java SE January 2017 Critical Patch Multiple Vulnerabilities

Product

JRE\_1.8.0\_73

Vuln ID

150406

Argument

JRE\_1.8.0\_73

Category

Misc

Exploit

Remote

Solution

Solution

Target client

Client

Target server

Server

Discovered on

2017-01-17

Priority

Major

Page 1

775 logs

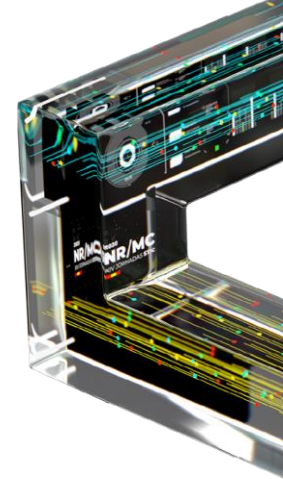
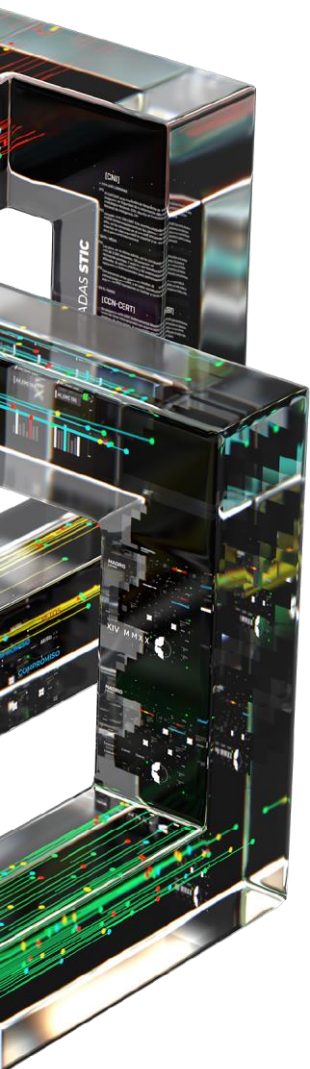
Period displayed: 53m 53s

Previous

Next

Copy

#XIVJORNADASCNCERT



# MUCHAS GRACIAS

## #XIVJORNADASCCNCERT