

An aerial, high-angle view of a dense urban landscape, likely Tokyo, with the Tokyo Skytree visible in the distance. The image is dark and serves as a background for the text.

FORTINET®

Ciberseguridad en ICS y Sistemas SCADA

25-Enero-2017

CiberSeguridad en ICS y Sistemas SCADA

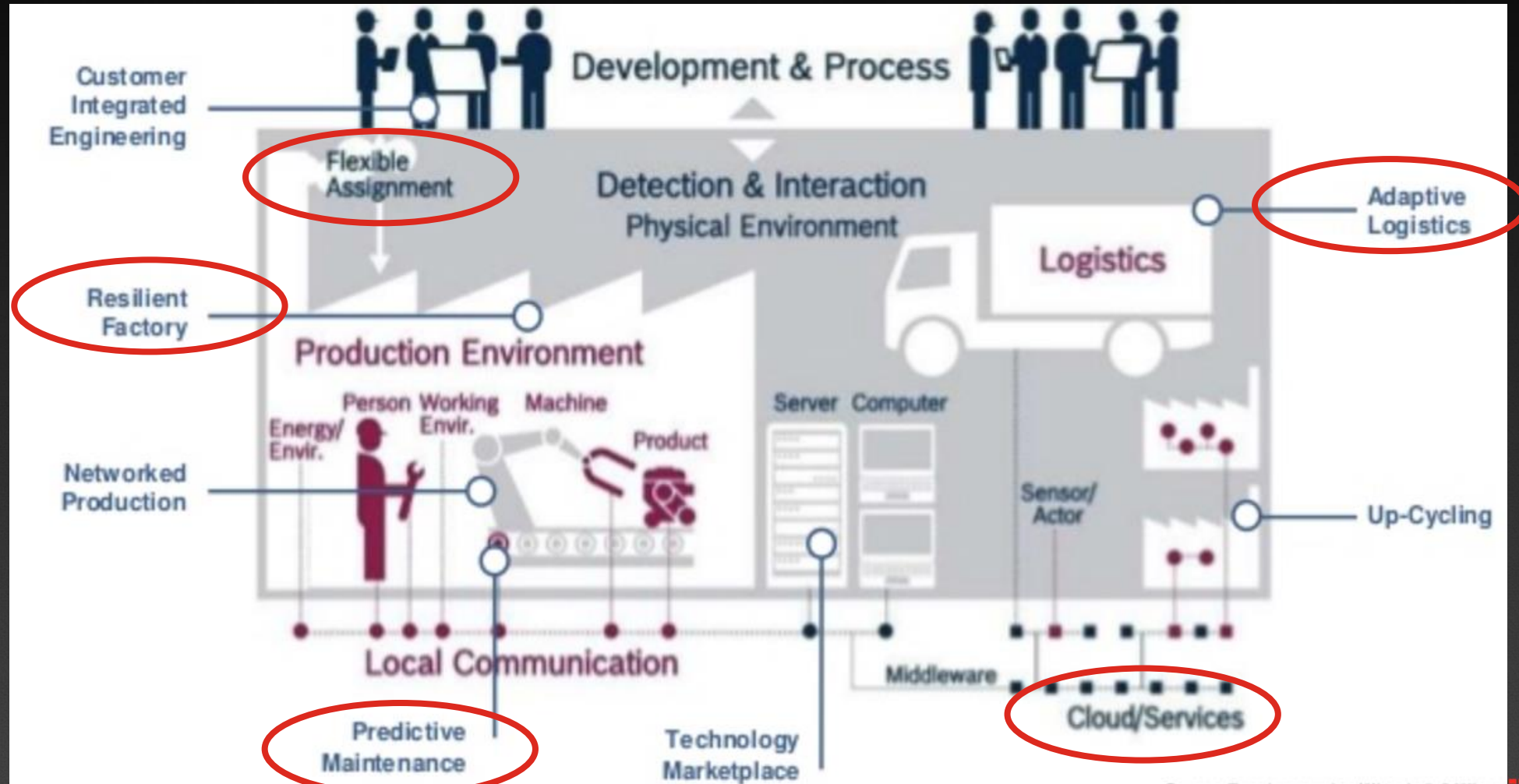
AGENDA

- Introducción: Industria 4.0
- Propuestas en CiberSeguridad: Virtual Patching
- Aproximación V. Patching de Fortinet
- Vídeo Demostración ataque y protección ICS

¿Que es Industria 4.0 o Smart Factory?

¿Es el uso de tecnología más avanzada? NO EXACTAMENTE.

Integración de IT y OT





¿QUÉ ES VIRTUAL PATCHING?

¿Qué es Virtual Patching?

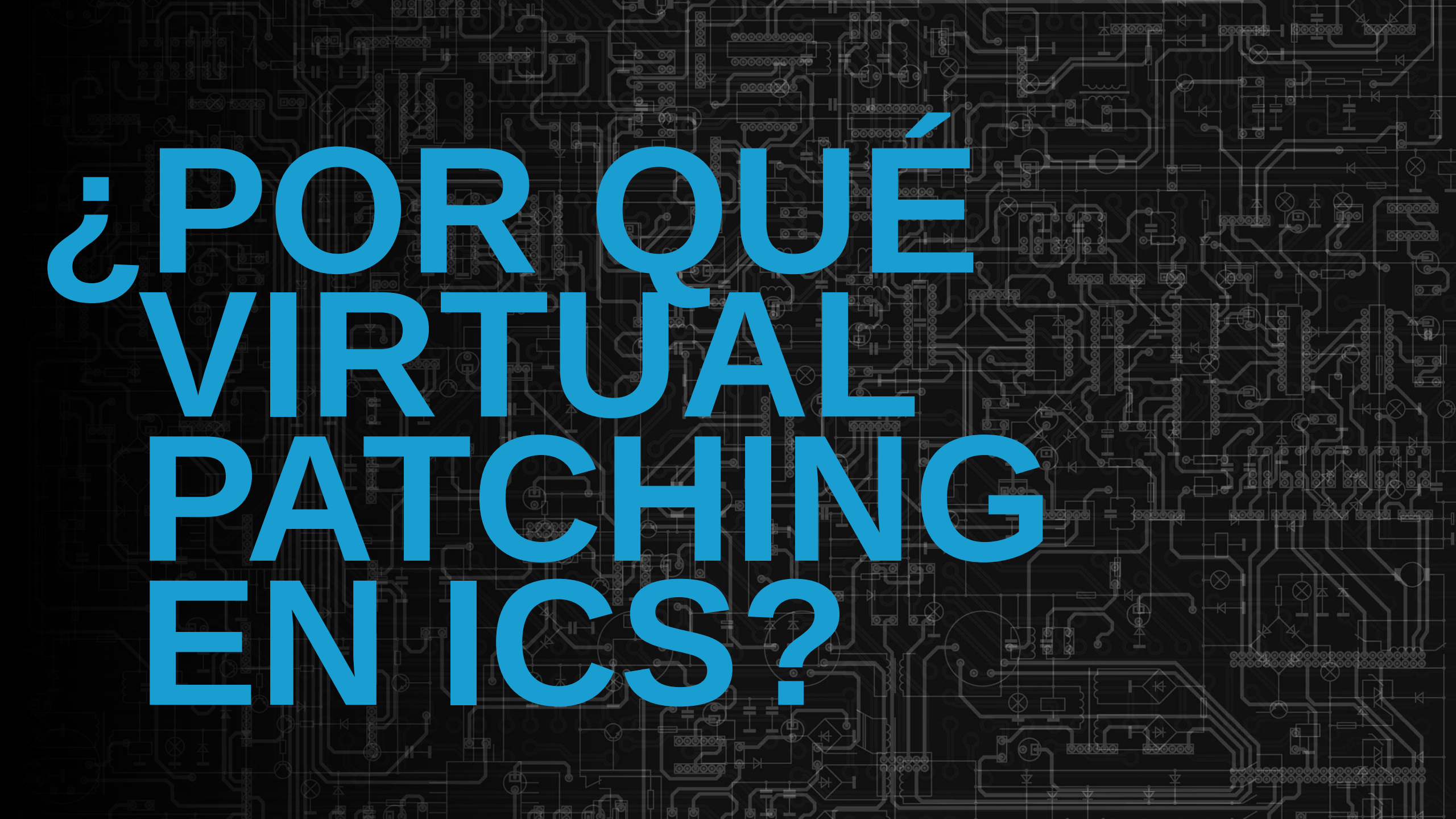


PATCH (según Wikipedia)



- En informática, un parche consta de cambios que se aplican a un programa, para corregir errores, agregarle funcionalidad, actualizarlo, etc.

VIRTUAL PATCHING

The background of the image is a dark gray, almost black, surface covered with a complex, light gray circuit board pattern. This pattern consists of numerous interconnected lines, loops, and small geometric shapes representing electronic components like resistors, capacitors, and integrated circuits. The overall effect is a dense, technical, and futuristic aesthetic.

**¿POR QUÉ
VIRTUAL
PATCHING
EN ICS?**

¿Por qué Virtual Patching en ICS?

- **Sistema Operativo más utilizado en ICS: Windows XP (SP3)**
 - » Sin soporte del fabricante
 - » Muy pocos Antivirus disponibles
 - » Muchas vulnerabilidades publicadas (conocidas)
- **Fabricantes de ICS en ocasiones no soportan cambiar, actualizar o parchear el Sistema Operativo**
- **Fabricantes de ICS en ocasiones no soportan instalación de software antivirus en el DCS**

¿Por qué Virtual Patching en ICS?

- **Redes OT unidas a redes IT**
- **Costes de parcheo por parte del fabricante ICS muy elevados**
 - » Con coste recurrente anual
- **El parcheo del fabricante no contiene protección AntiMalware**
- **Parcheando, no se pueden crear areas de seguridad**

¿Por qué Virtual Patching en ICS?

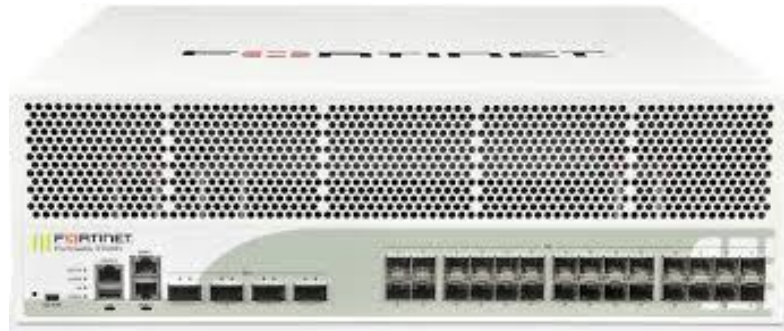
- El parcheo de fabricante solo se aplica a PCs industriales, no a otro tipo de sistemas (PLC, Robots, etc.)
- Existen ICS conectados directamente a internet
- Passwords “empotradas” en el código de algunos ICS (Backdoors)

The background is a dark, textured image of a computer screen. It shows a file download progress bar with the text 'Loading File:' and 'From: Internet to My Computer'. There is an hourglass icon indicating time. A keyboard is visible at the bottom right, with a 'Cancel' button highlighted.

APROXIMACIÓN V. PATCHING DE FORTINET

Aproximación V. Patching de Fortinet

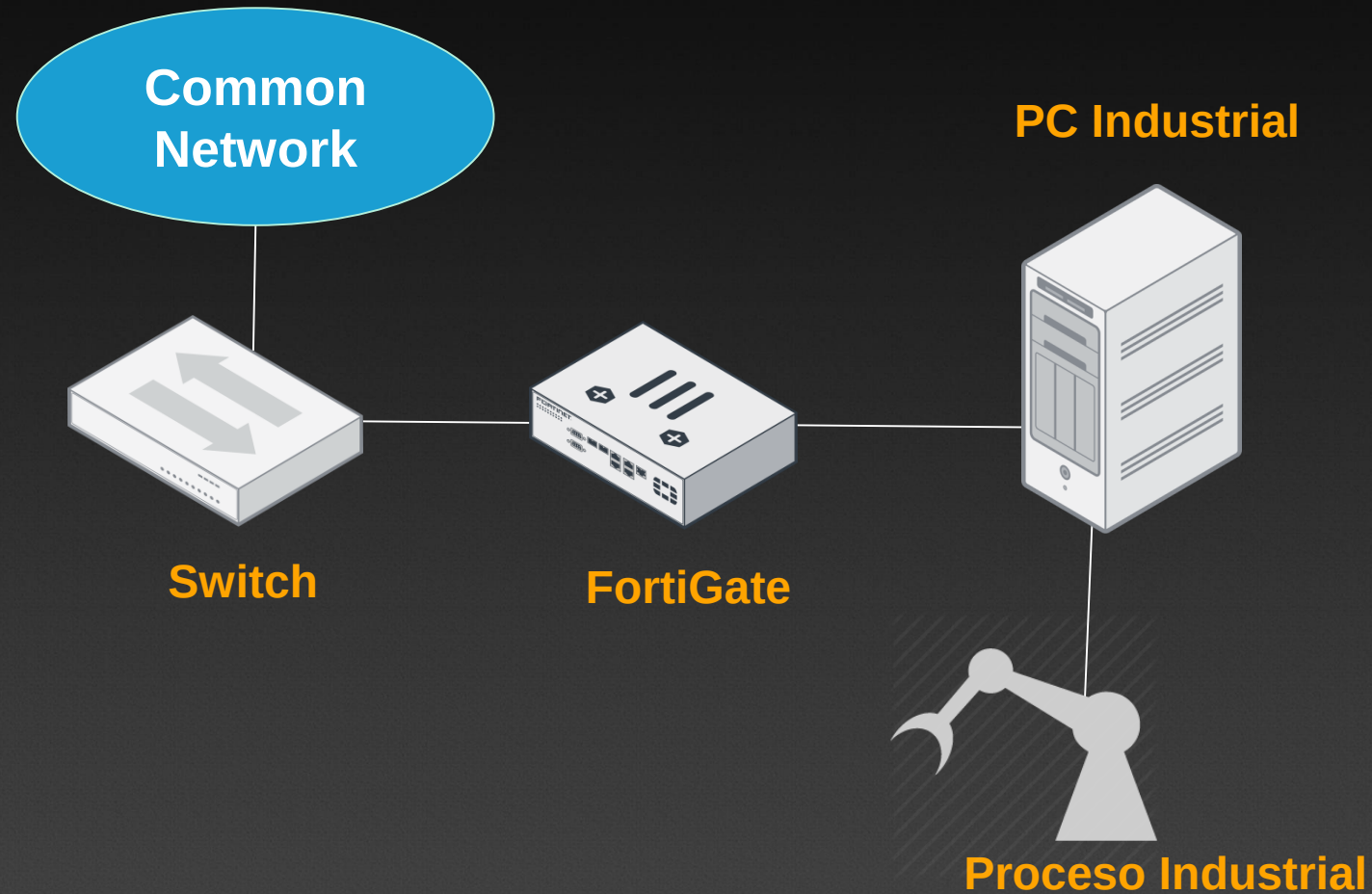
Solución para ICS: Firewalls Ruggerizados específicos para entornos industriales.



Dispositivos Ruggerizados

FortiGate

- Implementación en modo Bridge (transparente)
 - » Soporte de VLAN



FortiGate

- Protección IPS/IDS
 - » Posibilidad de creación de firmas manuales

The image displays the FortiGate IPS/IDS configuration interface. On the left, a list of signatures is shown, including 'pass', 'SSH.EVITAR.FLOOD', '2BGal.Disp_album.SQL.Injection', '2Wire.Wireless.Router.XSRF.Password.Reset', '3Com.3CDaemon.FTP.Server.Buffer.Overflow', '3Com.3CDaemon.FTP.Server.Information.Disclosure', '3Com.Intelligent.Management.Center.Information.D', '3Com.OfficeConnect.ADSL.Wireless.Firewall.Router', '3COM.OfficeConnect.DoS', '3D.Life.Player.WebPlayer.ActiveX.Control.Buffer.Ove', '3ivx.MPEG4.File.Processing.Buffer.Overflow', '3S.CODESYS.Gateway.Server.Heap.Buffer.Overflow', '3S.Pocknet.VMS.ActiveX.Control.Buffer.Overflow', and '4D.WebStar.FTP.Command.Buffer.Overflow'. The 'Severity' column shows 'High' for the first few signatures. The 'Target' column shows 'Server' and 'Windows'. The 'OS' column shows 'cOS Solaris BSD', 'aris, MacOS', and 'Windows'. The 'Action' column shows 'Block' and 'Pass'.

In the center, a network diagram illustrates the setup. A blue oval labeled 'Common Network' is connected to a 'Switch' (represented by a switch icon). The 'Switch' is connected to a 'FortiGate' (represented by a FortiGate icon with a shield). The 'FortiGate' is connected to a 'PC Industrial' (represented by a server icon) and a 'Brazo Robótico' (represented by a robotic arm icon).

At the bottom, a pagination bar shows '1 / 198' and '[Total: 9856]'. A red arrow points to the '[Total: 9856]' text.

FortiGate

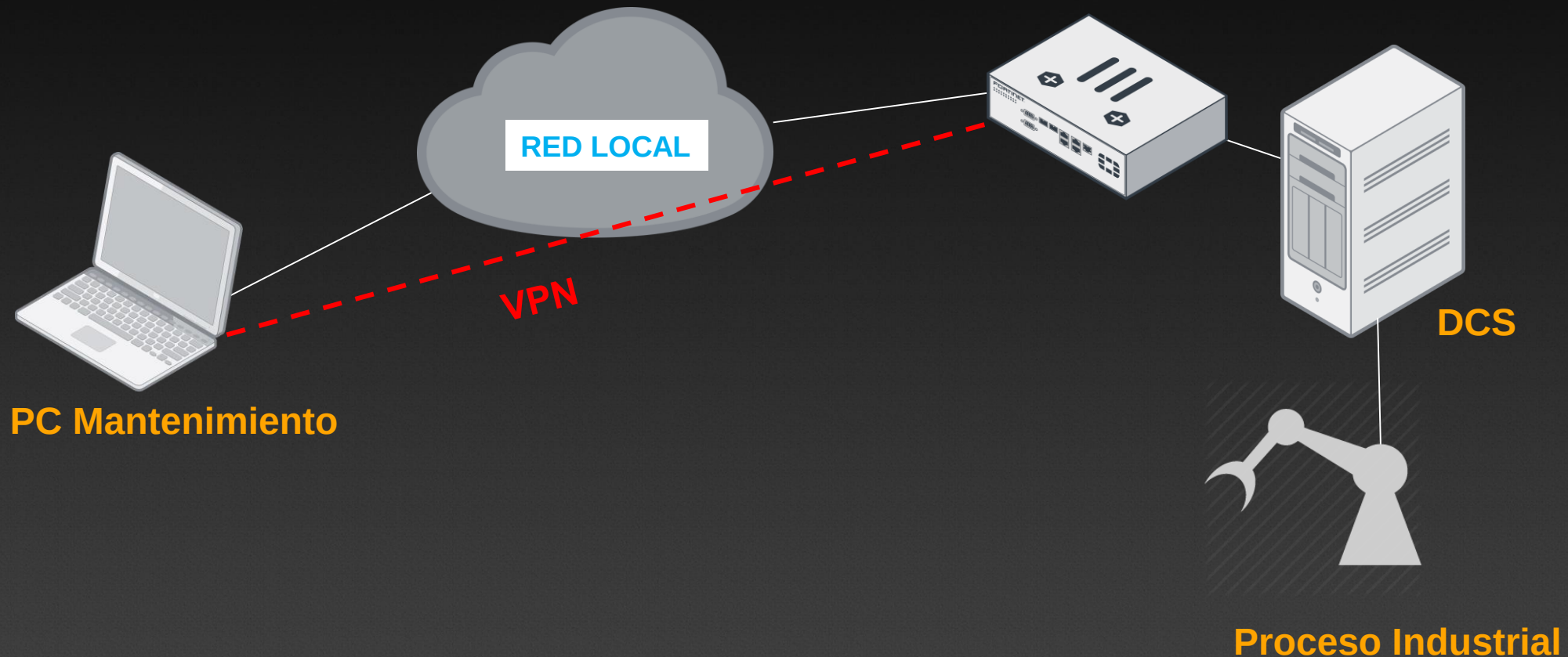
- Control de Aplicaciones Industriales
 - » Posibilidad de creación de firmas manuales

The screenshot displays the FortiGate web interface. On the left, a sidebar lists various applications and services, including 'FAZ-ftnt.es-lab.fortinet.com', 'Monitor.HTTP.GET', 'my_app', 'TESTUOC', 'twitterappsearch', '1kxun', '1und1.Mail', '2ch', '2ch_Post', '2shared_File.Download', '2shared_File.Upload', '3PC', '4shared', '4shared_File.Download', '4shared_File.Upload', '4Sync', '4Sync_File.Upload', and '8tracks'. The main area features a network diagram with a 'Common Network' (blue oval) connected to a 'Switch' (white box), which is connected to a 'FortiGate' (white box with a shield icon). The 'FortiGate' is connected to a 'PC Industrial' (white box) and a 'Brazo Robótico' (robot arm icon). Below the diagram, a table lists applications with columns for 'Name', 'Popularity', and 'Risk'. The table includes entries for 'Storage.Backup', 'Browser-Based, Client-Server', and 'Video/Audio'. A red arrow points to the bottom right of the interface, indicating the total number of applications: '[Total: 2891]'.

Name	Popularity	Risk
Storage.Backup	★★★★★	★★★★★
Browser-Based, Client-Server	★★★★★	★★★★★
Storage.Backup	★★★★★	★★★★★
Browser-Based, Client-Server	★★★★★	★★★★★
Storage.Backup	★★★★★	★★★★★
Browser-Based, Client-Server	★★★★★	★★★★★
Video/Audio	★★★★★	★★★★★

1 / 58 [Total: 2891]

- Acceso para mantenimientos remotos mediante VPN



FortiGate

- Autenticación fuerte (usuario + password + OTP)

Conectando a la VPN Fortinet-Francia

**VPN Authentication**
Fortinet-Francia

Nombre de Usuario

Password

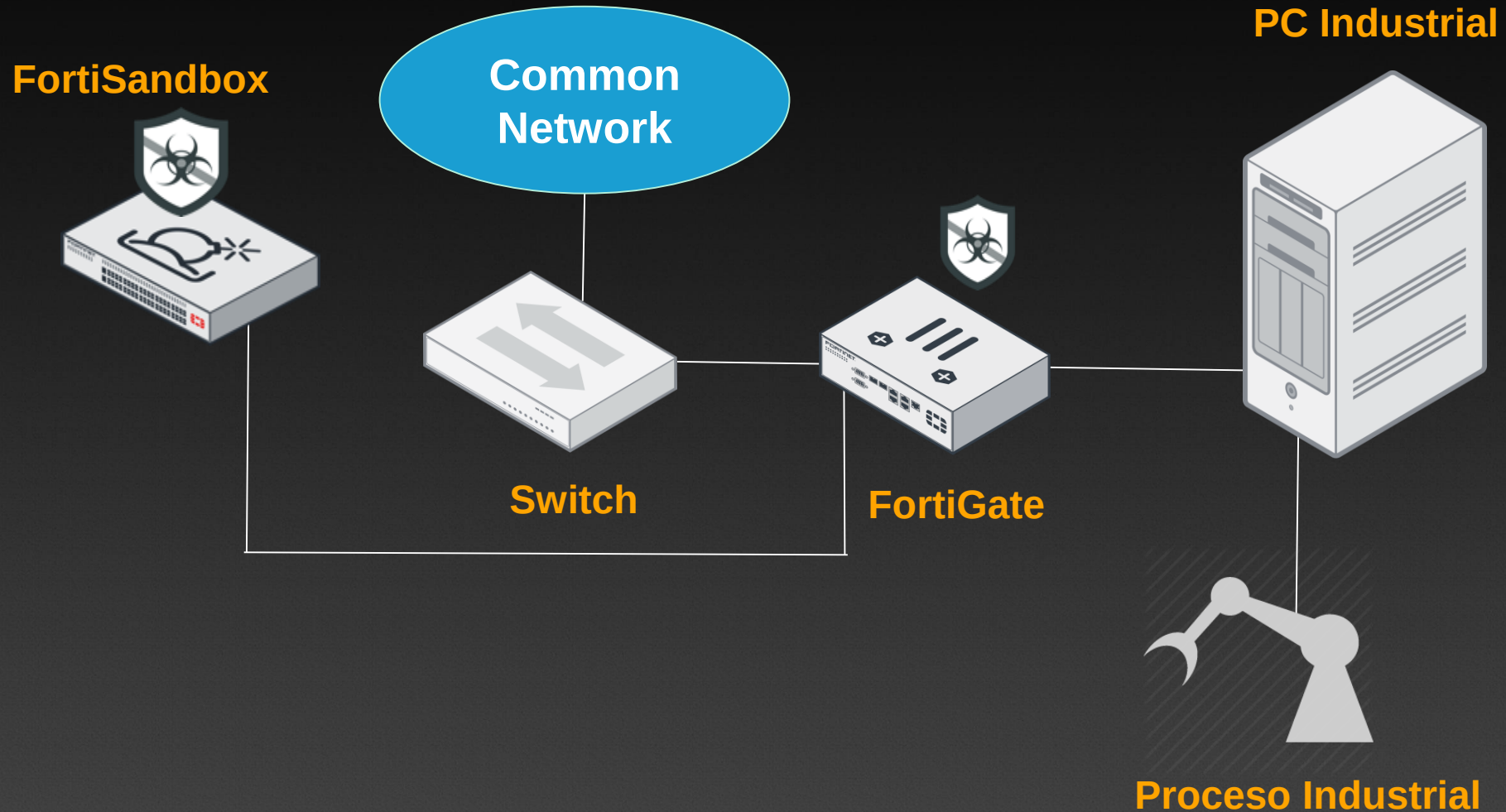
Respuesta

A FortiToken code is required for SSL-VPN login authentication.



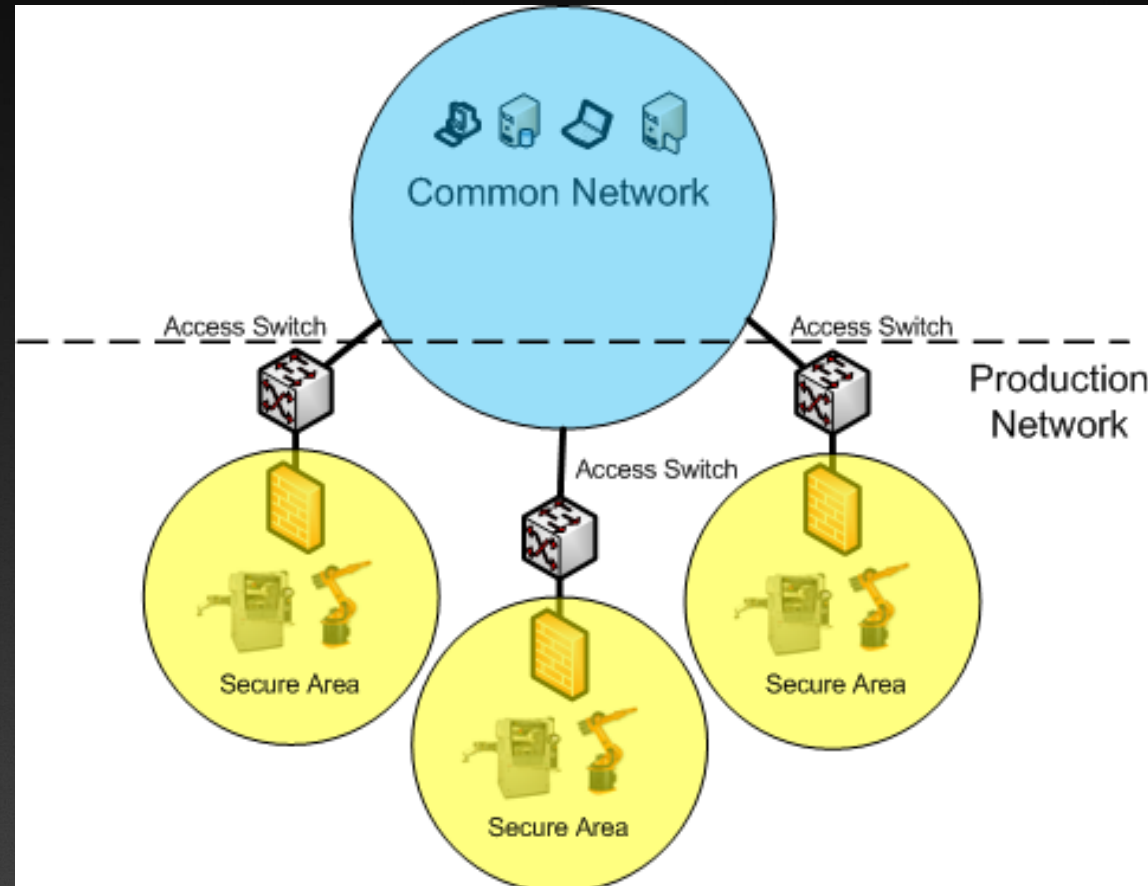
FortiGate + FortiSandbox

■ Protección Antimalware en la red



FortiGate

- Firewall para segmentación de áreas de seguridad



VIDEO-DEMO ATAQUE Y PROTECCIÓN ICS

¡ Gracias !

FORTINET®