



OPTIMIZACIÓN DE LA SEGURIDAD DE OT MEDIANTE LA EVALUACIÓN AUTOMÁTICA DE ATACANTES

Presentación basada en el White Paper:
**What's Your Next Move? Optimizing OT Security Through Automatic Attacker
Evaluation (2019)**

White Papers and Reports



Security Brief: COVID19-Themed Malware and Cyber-Attacks



Conducting IEC-62443 Assessments Using Radiflow Products



Security Brief: Fear of Cyber-Retaliation by Iranian Attack Groups



Security Brief: A 2020 View of Industrial Cyber Security



451 Research Reviews and Approves of Radiflow's OT-MSSP Offering



Radiflow Insights: Attacks on manufacturing: a clear and present danger



¿QUIÉN ES YEHOANATAN KFIR?



Académica

- La Universidad Hebrea de Jerusalén - **Física y Matemáticas** (2002 – 2005).
- Technion-Machon Technologi Le' Israel, **Máster en Administración de Empresas**.
- **Máster Ingeniería Eléctrica**, Tel Aviv University.
- **Doctor of Philosophy – PhD Computer Science**, Bar-Ilan University

¿QUIÉN ES YEHOANATAN KFIR?



Profesional

- **Inteligencia militar israelí (2005 – 2012)**
 - Ingeniero en hardware
 - Desarrollador C ++
 - Responsable de proyectos de I+D+i (Investigación, desarrollo e innovación)
 - Líder del equipo de hardware
 - Gerente Técnico de Producto
- **Vicepresidente de productos, Compañía ciberseguridad (2012 - 2014)**
- **CTO de Radiflow en la actualidad.**

RADIFLOW



CIARA (Cyber Industrial Automated Risk Analysis)

- Radiflow (fundada 2009), formada por:
 - ciber-expertos de unidades militares de élite
 - expertos en automatización de proveedores
 - operadores industriales globales
- Proveedor de soluciones de ciberseguridad para redes de infraestructura crítica.
- Sistemas ICS/SCADA que permite a los usuarios mantener la visibilidad y el control de redes OT.

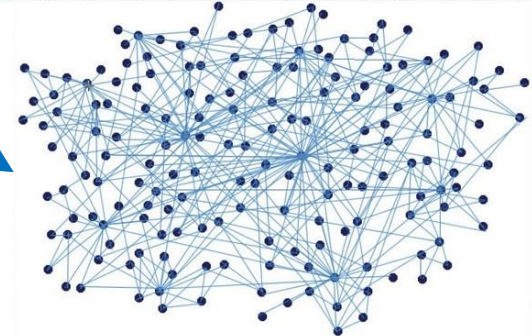
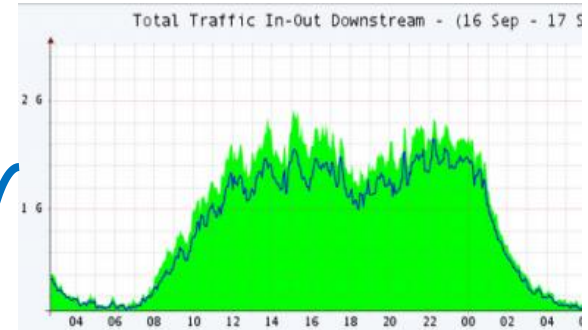
INTRODUCCIÓN

- ICS (sistemas de control industrial) crecen complejidad es necesario automatizar el evaluar su vulnerabilidades.
- Proceso de análisis de vulnerabilidad de una red manualmente, es muy laborioso y propenso a errores.
- Propone un sistema para generar grafos de ataque para sistemas industriales. Basado a monitorización pasiva de redes industriales.



INTRODUCCIÓN

1. **Monitorizar** pasivamente el **tráfico** de la red industrial.
2. **Modelar** la **estrategia de defensa** en función de las prioridades operativas.
3. **Modelar** las **capacidades técnicas** de un **atacante** de redes industriales.
4. **Modelar** la red de comunicación industrial.
5. **Generar** automáticamente el **grafo de ataque** utilizando los parámetros anteriores.



MODELADO DE LA ESTRATEGIA DE DEFENSA

- **Objetivo:** mantener el proceso físico en las condiciones deseadas (seguridad y la fiabilidad).
- **Mantener los dispositivos que controlan el proceso físico** (garantizar la continuidad del proceso físico).
- Definir **cómo** un **atacante** puede **dañar** este dispositivos.
- **Métrica** para determinar el **impacto** en los dispositivos de red: **CVSS v3** (en función C.I.D.).



MODELADO DE LA ESTRATEGIA DE DEFENSA

- Dispositivos y zonas de la red industrial pueden tener diferentes estrategias de defensa.

| | Confidentiality | Integrity | Availability |
|---------------------------------------|-----------------|-----------|--------------|
| PLC | High | High | Low |
| HMI | High | Medium | Medium |
| Engineering Station | Low | Low | High |
| Other -Server, Router, OPC, Historian | Medium | Medium | Low |

MODELADO DEL ATACANTE

- Éxito de un atacante depende experiencia en:
 - Explotación de protocolos
 - Explotación de vulnerabilidades de los dispositivos
- Distinguimos 3 niveles de capacidades:
 - **Bajo:** capaces de explotar sólo los protocolos de TI.
 - **Medio:** capaces de explotar protocolos de TI y OT (abierto sólo).
 - **Alto:** capaces de explotar protocolos de TI y OT(inclusive propietarios).

MODELADO DEL ATACANTE

- Mucho tiempo se creyó que los **sistemas SCADA** eran **seguros** porque **utilizaban protocolos propietarios**.
- Distinguimos entre 3 niveles de experiencia capaces de explotar las vulnerabilidades de los dispositivos:
 - **Bajo:** capaz de explotar sólo las **vulnerabilidades conocidas** públicamente con *exploits* públicos.
 - **Medio:** el atacante es capaz de **desarrollar sus propios *exploits*** para las vulnerabilidades conocidas.
 - **Alto:** el atacante es capaz de realizar una investigación para encontrar **nuevas vulnerabilidades** y es capaz de explotarlas.



MODELADO DEL ATACANTE

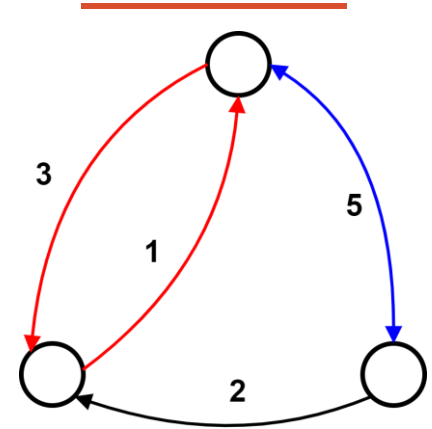
| Notation | Property Description | Values |
|-----------------------|---|--|
| A_{protocol} | El nivel de experiencia en la explotación de protocolos de red legítimos. | <ul style="list-style-type: none"> • Low –Exploiting IT protocols • Medium – Exploiting IT and OT Data-plane protocols • High – Exploiting IT, OT Data-plane and OT Control-plane protocols |
| A_{vuln} | El nivel de experiencia en la explotación de vulnerabilidades de dispositivos. | <ul style="list-style-type: none"> • Low—using only public exploits • Medium – able to develop exploits for known vulnerabilities • High – able to research and exploit zero-days |

| | | Abusing protocols | | |
|-------------------------------|--------|-------------------|--------|------|
| | | Low | Medium | High |
| Abusing device vulnerabilites | Low | | | |
| | Medium | | | |
| | High | | | |

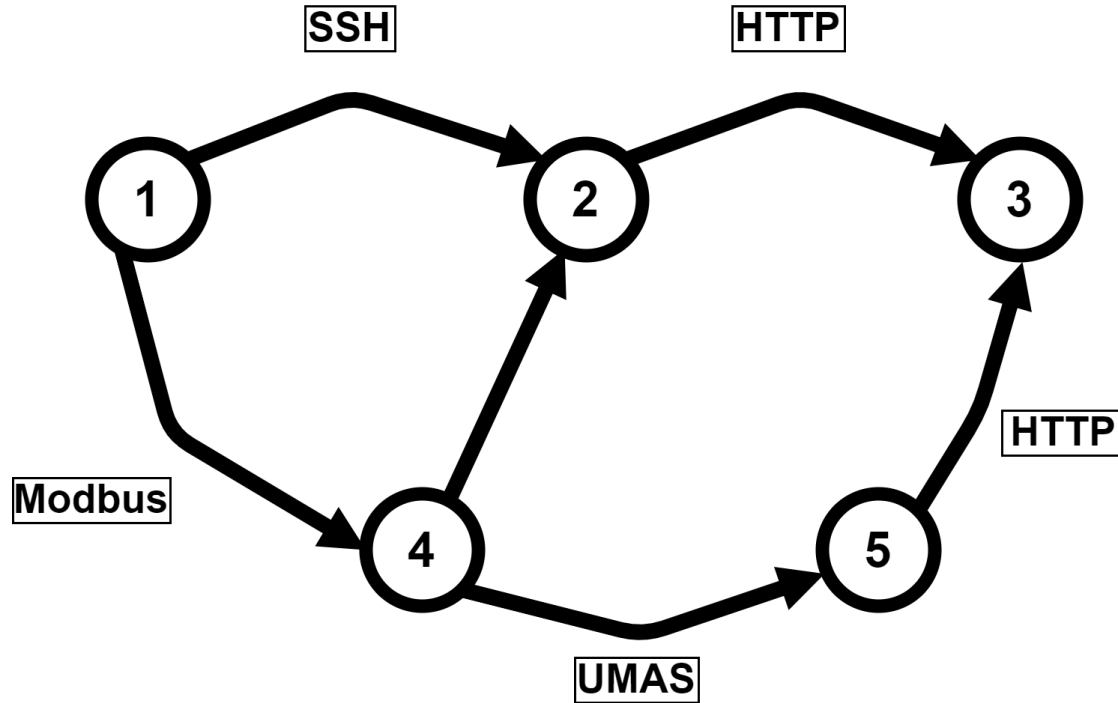
$$\text{attackerlevel} = A_{\text{protocol}} * A_{\text{vuln}}$$

GRAFO DE ATAQUE

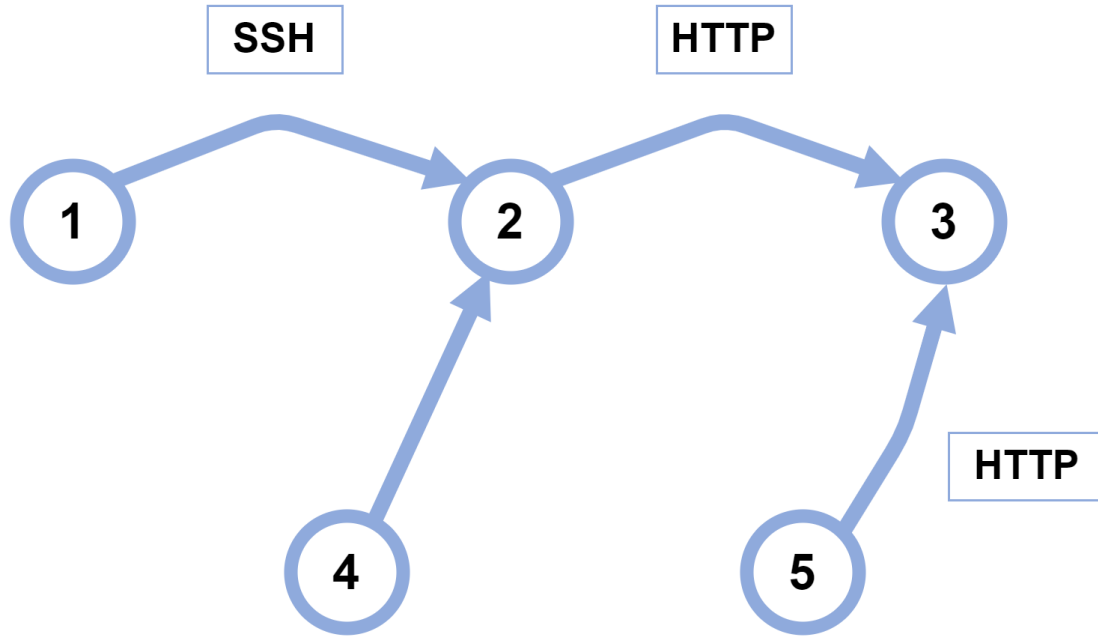
- Modelamos la **red de comunicación como un grafo direccional** $G=(V,E)$, donde:
 - **V**: los nodos representan todos los dispositivos de la red.
 - **E**: las aristas (x, y) de nodos en V , que representan un enlace de comunicación de x a y .
- **Grafo de Ataque**: multigrafo dirigido y ponderado.
- Los **pesos** representan **lo fácil** que es para un atacante **utilizar esa arista** para pasar del dispositivo x al dispositivo y .
- Distinguimos entre las **aristas** creadas a partir de la **explotación de protocolos** y las creadas a partir de la **explotación de vulnerabilidades**. Las aristas basadas en la explotación de vulnerabilidades se puntual mediante CVSS v3.



Network Graph, G

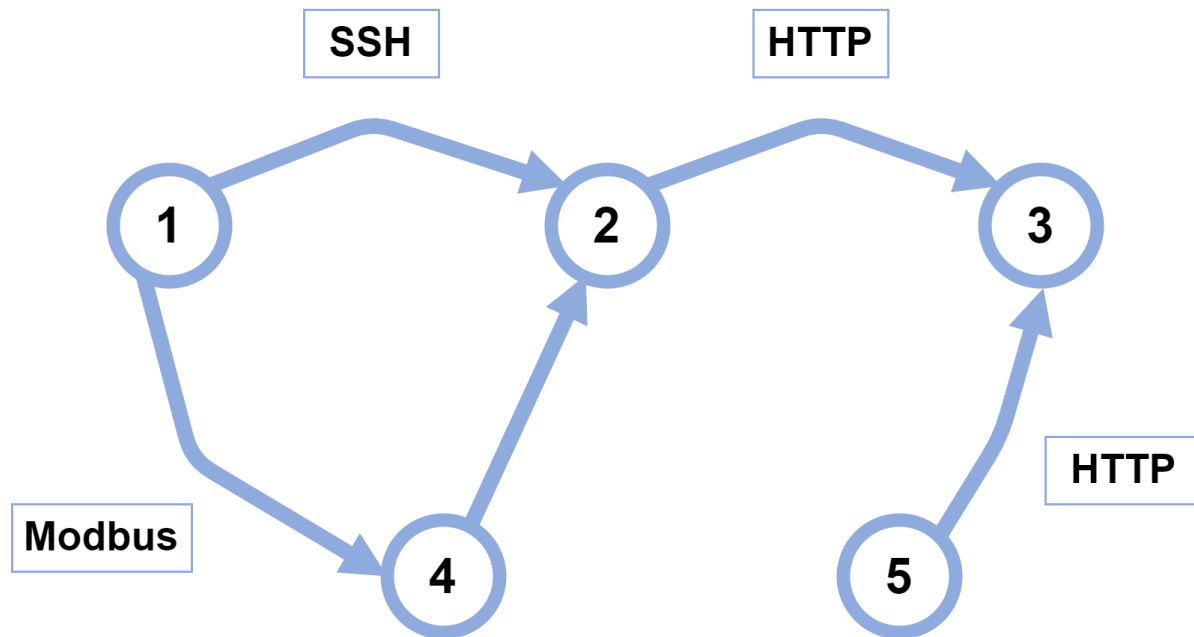


Network Graph, G_A : Protocols



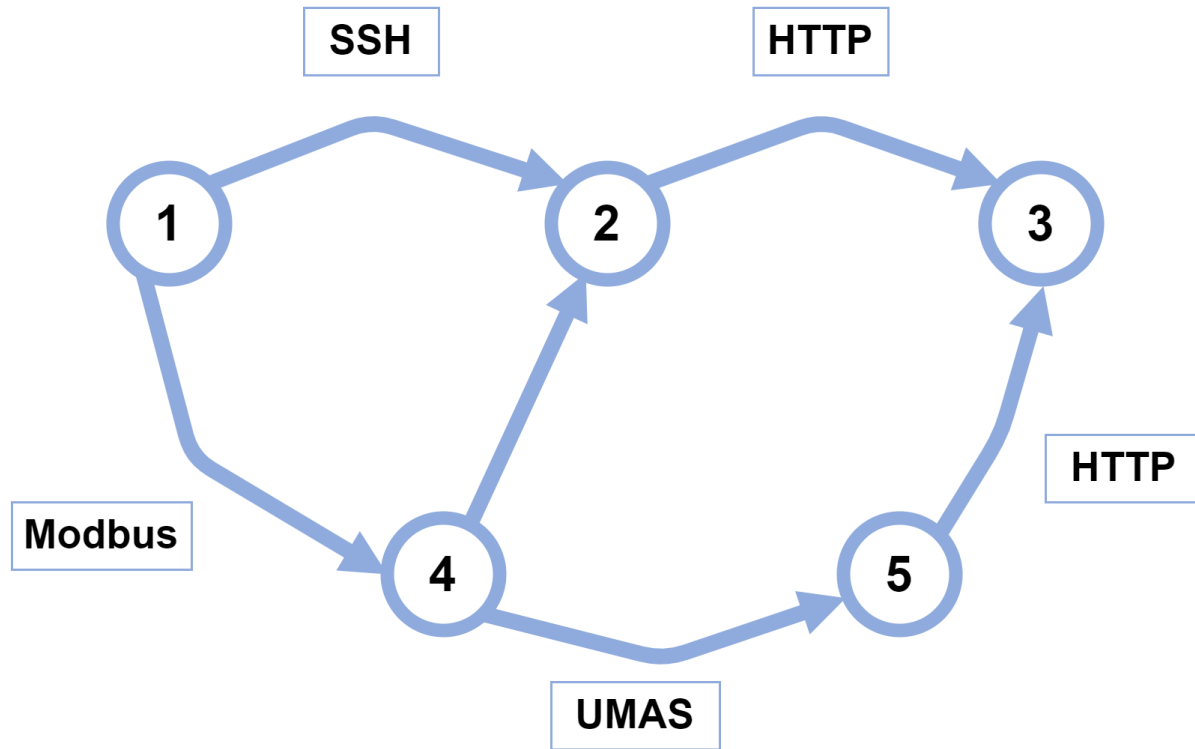
0 - Exploiting IT protocols

Network Graph, G_A : Protocols



1 - Exploiting IT and OT Data-plane protocols


Network Graph, G_A : Protocols



2 - Exploiting IT, OT Data-plane and OT control-plane protocols

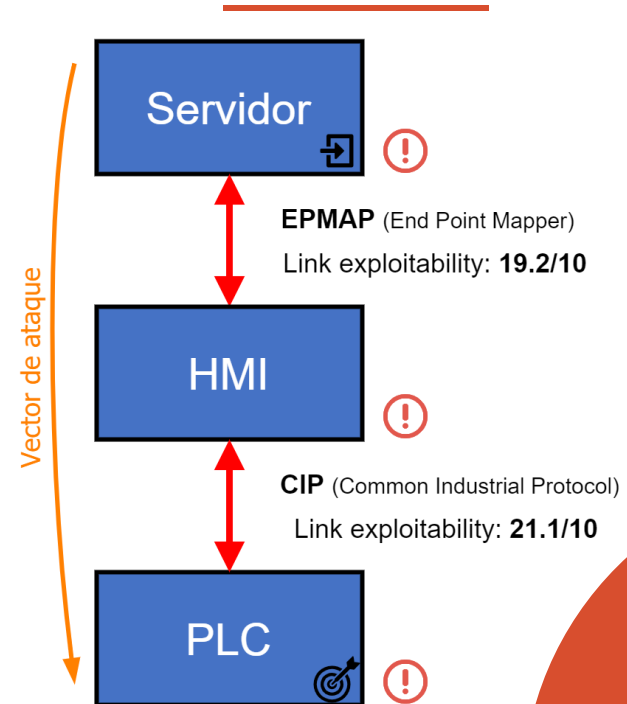
RUTAS Y PRIORIZACIÓN DE LOS PARCHES

La propagación del atacante en la red se realiza por pasos:

- El atacante obtiene el control de un dispositivo aleatorio.
 - El atacante continúa extendiéndose por la red, dispositivo a dispositivo, elige la forma más fácil de moverse por la red.
 - El atacante elige la arista con la mayor puntuación explotable está conectada a los dispositivos bajo su control.
- 

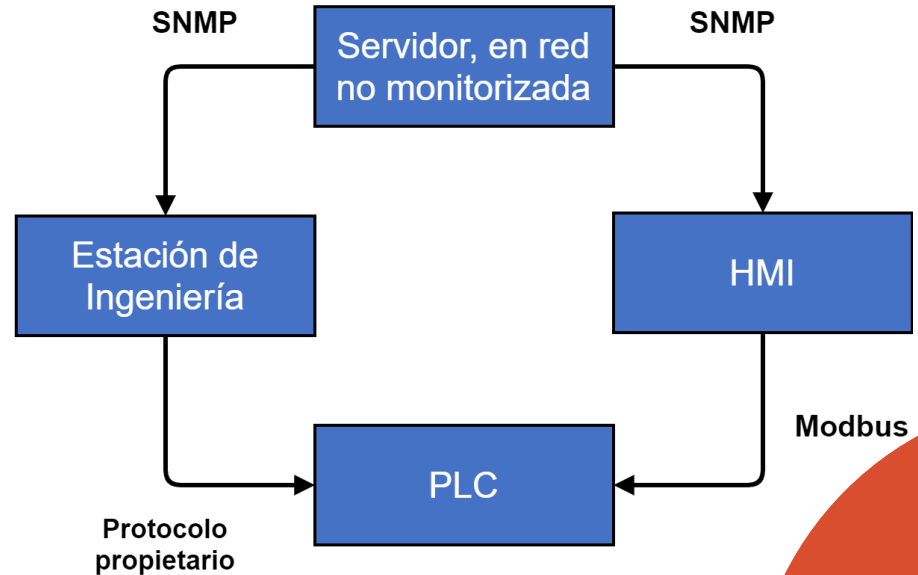
RUTAS Y PRIORIZACIÓN DE LOS PARCHES

- Construimos gráficos de ataque para todas las opciones de ataque posibles en cada gráfico, **podemos calcular la ruta más explotable** entre los dos dispositivos.
- Los **dispositivos** que se encuentran en la mayoría de las rutas, y que son **explotables** por los atacantes de menor nivel, **deben ser parcheados primero**.




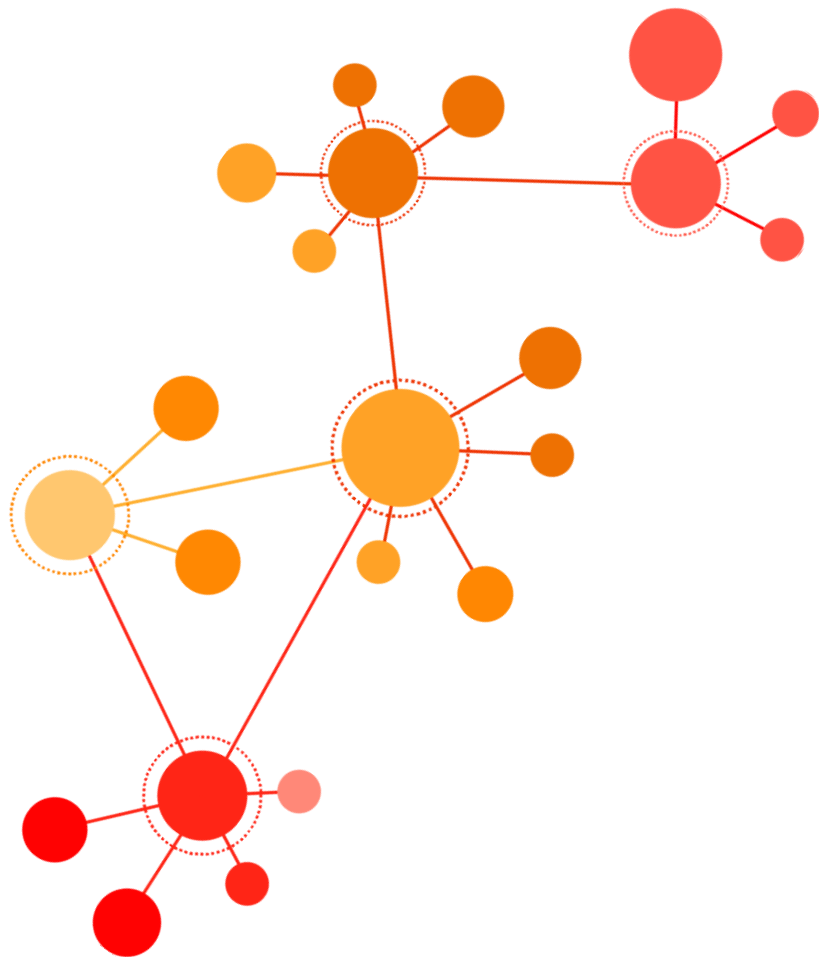
EJEMPLO DE CASO DE USO

- El firmware del PLC tiene una alta puntuación de vulnerabilidad y un alto impacto en la disponibilidad.
- Tanto la estación de ingeniería como la HMI utilizan Windows sin parches.
- Actualizar el PLC es más complicado que parchear la estación de ingeniería o la HMI.



EJEMPLO DE CASO DE USO

1. Un **atacante de bajo nivel** que sólo utiliza **protocolos abiertos**, se debe parchear la HMI.
 2. Un **atacante de nivel medio** con experiencia en **protocolos propietarios** también tendrá la capacidad de **utilizar la estación de ingeniería** para cambiar la lógica del PLC. Se debe **arreglar tanto la HMI como la estación de ingeniería**.
 3. Un **atacante de muy alto nivel** capaz de atacar con un **zero-day**, las dos acciones anteriores serían inútiles. La única medida práctica que podría tomar es instalar un firewall entre el PLC y la red.
- 



CONCLUSIONES

1. Los **grafos de ataque** son un **método esencial** para predecir qué rutas seguirá un atacante en la red.
2. El modelo propuesto tiene **en cuenta** las **características industriales** a la hora de clasificar los vectores de ataque.
3. Esta metodología puede resolver dos grandes retos: **encontrar la ruta más probable del atacante** y **priorizar los parches en redes grandes**.

FIN

Presentación basada en: What's Your Next Move? Optimizing OT Security Through Automatic Attacker Evaluation (2019)



CREDITS: This presentation template was created by **Slidesgo**, including icons by **Flaticon**, and infographics & images by **Freepik**