HERRAMIENTAS DE PROTECCIÓN DE UN ENTORNO OT

Las siguientes características propias de los entornos industriales aumentan las vulnerabilidades y riesgos a los que son susceptibles estos dispositivos:

- Obsolescencia de los sistemas y gran dificultad para actualizarlos.
- Falta de visibilidad de los dispositivos o activos que están conectados en la Red.
- Falta de seguridad de las arquitecturas de Red.
- Variedad y diversidad de equipamiento.
- Falta de una correcta y adecuada gestión de la configuración de los dispositivos, o las vulnerabilidades de los equipos, ya que no están preparados para los riesgos de hoy en día.
- Incremento de la conectividad de cada vez más dispositivos industriales a la Red, lo que ha hecho aumentar las amenazas y vulnerabilidades para estos sistemas.

Adquirir y hacer uso de herramientas especializadas en la protección de estos entornos resulta esencial para obtener un grado adecuado de seguridad.

La empresa de ciberseguridad industrial, Claroty, realizó un informe de «Riesgos y Vulnerabilidades ICS» con datos e información de las vulnerabilidades que encontraron en la primera mitad del año 2021. En los seis meses del periodo de duración del informe, habían descubierto más de 600 vulnerabilidades.

HERRAMIENTAS O TÉCNICAS QUE SE DEBEN IMPLEMENTAR EN CUALQUIER ENTORNO INDUSTRIAL

Inventario de activos

SIEM

IDS e IPS

Firewall

SOC y NOC

Antivirus

***Honeypot* industrial**

Sistemas EDR

Sistemas XDR