Informe de industria destacado de 2021: Manufactura

Con amenazas a los entornos de OT cada vez más sofisticadas y las cadenas de suministro bajo mayor presión, nunca ha sido tan importante un enfoque unificado de la seguridad en los entornos de TI y OT.

Ventajas fundamentales

- ✔ Independiente de protocolos y tecnologías, opera sin puntos de referencia fijos
- ✔ Cobertura unificada de las TI, OT e IoT
- ✔ Detecta nuevas amenazas en tiempo real a medida que surgen
- ✔ Comprende toda la comunicación en un entorno, desde el tráfico regular PLC, a las redes sensoras IIoT distribuidas

2020: Una nueva era de ataques a OT

En junio de 2020, una nueva y sofisticada variedad de ransomware, EKANS, llegó a varias instalaciones de fabricación de Honda en todo el mundo. Causó una interrupción que paralizó las operaciones en numerosos países y provocó una gran pérdida de horas de producción y, por consiguiente, de horas no trabajadas pero remuneradas. A lo que hubo que añadir los costos de poner los sistemas en funcionamiento sin ceder a las demandas de rescate.

Lo diferente de EKANS fue que el ataque se dirigió directamente a las vulnerabilidades de los ICS, en lugar de pasar a través de software de TI sin parches como puerta de enlace. Con la capacidad de atacar 64 mecanismos ICS específicos en su cadena de eliminación, EKANS representa una nueva frontera en el futuro de los ciberataques OT.

Además, en un momento en el que nunca ha habido más presión sobre los fabricantes para satisfacer la demanda global y mantener las cadenas de suministro que conectan el comercio global, es fundamental priorizar la seguridad de la tecnología OT. En la primavera de 2020, muchos fabricantes se encontraron repentinamente cambiando para producir productos que nunca antes habían fabricado, revisando sus líneas de producción e implementando nuevas tecnologías, y muchas de estas transformaciones parecen estar destinadas a permanecer en su lugar a largo plazo.

> "Hace diez años, la ciberseguridad era simplemente un firewall. Hoy en día, con el 5G y el trabajo remoto, las empresas están más en riesgo con las amenazas. Ahí es donde entra en juego Darktrace."
>
> Frédéric Carricaburu, CIO, Saniflo

> "Cyber AI Analyst de Darktrace cambia las reglas del juego, porque lleva a las personas de mirar un monitor a realmente comenzar a trabajar en las artimañas, y reduce el tiempo de calificación"
>
> Laura Tibodeau, CIO, AmSty

Un sistema inmunológico para la industria de manufactura.

El Industrial Immune System de Darktrace aprovecha la tecnología de inteligencia artificial para proteger los entornos ciberfísicos críticos y complejos de cientos de fabricantes en todo el mundo. La tecnología del Darktrace Immune System se escala para cubrir distintas máquinas conectadas, configuraciones y entornos. Mediante el uso de machine learning supervisado y no supervisado, la IA de Darktrace no se limita a ningún formato digital en particular, sino que aprende por sí mismo a velocidad y escala.

Siguiendo el modelo del propio sistema inmunológico del cuerpo humano, el Industrial Immune System de Darktrace aprende cómo operan e interactúan en una vasta infraestructura digital ciberfísica los dispositivos ciberfísicos conectados y la tecnología operativa, así como los usuarios y los sistemas de TI.

La IA de Darktrace desarrolla un "patrón de vida" mientras ingiere información digital "en curso", lo que significa que no requiere capacitación adicional ni conjuntos de datos adicionales. Por lo tanto, Darktrace puede discernir inmediatamente la actividad amenazante donde y cuando sea, desde el piso de la fábrica hasta la bandeja de entrada del correo de un empleado, en tiempo real.

Propiedad intelectual expuesta por malware avanzado: Fabricación médica

En una empresa europea de fabricación de productos médicos, un asistente administrativo recibió un correo electrónico de phishing con respecto a los pagos con una factura adjunta. Creyendo que el archivo adjunto era auténtico, hizo clic en él y, sin saberlo, descargó un malware de acción rápida que había pasado todos los demás controles de seguridad.

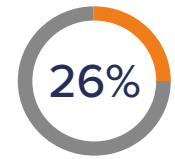
El software malicioso sofisticado estaba dirigido específicamente a la propiedad intelectual de la organización, que incluía fórmulas médicas altamente confidenciales. Si estos activos se vieran comprometidos, la empresa estaría expuesta a un riesgo significativo para su competitividad y reputación.

Una vez que el malware se descargó, el dispositivo rápidamente comenzó a conectarse a un destino externo poco común mientras intentaba moverse lateralmente a otros entornos. En dos segundos, la IA de Darktrace identificó la presencia extranjera emergente.

"El machine learning puede detectar cosas que no podemos predecir ni definir. Es como buscar una aguja en un pajar enorme."

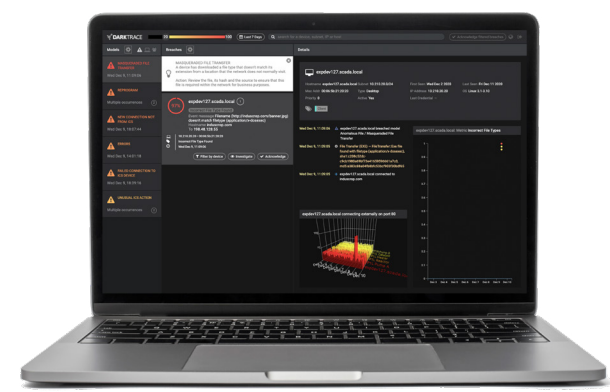
Stuart Berman, Information Security Architect, Steelcase

Medimos la seguridad en la industria manufacturera



de las empresas no tienen una división que supervisa la seguridad en los sistemas de gestión de la fábrica.

Darktrace detectó más de 6.500 instancias sospechosas de protocolo de ICS usadas en miles de entornos de red de IT de sus clientes en el verano de 2020.



El panel de OT Engineer muestra solo las alertas más relevantes desde el punto de vista operativo