INTRODUCCIÓN - IMAGINA ESTO

Su próspera fábrica/empresa es un árbol frutal bien cuidado y productivo.

A veces tus ramas y frutos se ven afectados por plagas externas y puedes monitorearlas y eliminarlas, y estás acostumbrado.

Pero, ¿qué pasa si un gusano penetra en el núcleo de su árbol? Llamémoslo un pequeño y peligroso gusano TO.

¿Cómo lo encontrarás?

¿Cómo bloqueará su devastadora adquisición?

¿Cómo evitarás el daño?

¿Cómo vas a luchar contra él antes de que sea demasiado tarde?

¿Cómo te asegurarás de que tu árbol siga dando frutos?

Y AHORA UN POCO DE REALIDAD

En los últimos años ha habido una creciente concienciación, tanto entre los fabricantes de equipos y terminales Scada, como entre los operadores de infraestructuras críticas, de la sensibilidad de estos sistemas frente a ciberataques y fallos inusuales del sistema en la operativa. área de red (OT) de los sistemas de control.

Al mismo tiempo, la implementación de una protección real para las capas inferiores de la red operativa es muy problemática debido a la antigüedad de los sistemas, el equipo final y la complejidad del proceso. En la práctica, puede encontrar una protección significativa y efectiva para las capas superiores: la red de control de TI (¿recuerda las plagas de madera externas, las que practica y prepara para su detección y eliminación?), Pero las capas inferiores a menudo están menos protegidas.

los sistemas de control Scada todavía tienen una capacidad bastante limitada para monitorear con precisión el rendimiento de los dispositivos finales críticos, que es donde surge la necesidad real de una protección más sólida.

EJEMPLOS DE DEVASTADORES ATAQUES TO EN LOS ÚLTIMOS AÑOS >>>>>>

Stuxnet - Junio de 2010:

Ataque al programa nuclear iraní dañando los sistemas de control industrial tipo Scada fabricados por la empresa "Siemens", que controla las centrífugas en la planta de enriquecimiento de Natanz.

Aramco - Agosto 2012:

Ataque a instalaciones petroleras en Arabia Saudita. El ex jefe de la NSA, el general Keith Alexander, afirmó que los ataques maliciosos contra la empresa energética de Medio Oriente, Saudi Aramco, en 2012 fueron un "despertar" para todos que podría tener graves consecuencias para la seguridad de las redes de infraestructura crítica.

Colonial Pipeline - Maio 2021:

Corte de energía a la costa este de los EE. UU.
El ataque se llevó a cabo mediante un "ransomware" que deshabilitó el equipo informático que gestiona el oleoducto central de la empresa.
puede tener graves consecuencias para la seguridad de las redes de infraestructura crítica.

SAMSecOT

OT Cyber Consulting

QUIENES SOMOS Y QUE OFRECEMOS

SAMSecOT trabaja en consultoría de ciberseguridad para sistemas operativos, el responsable de nuestro equipo profesional trae consigo una vasta experiencia de cerca de 20 años en el área de ciber OT, entre estos, 13 fueron en puestos gerenciales en NISA para ciberseguridad y regulación en una amplia gama de organizaciones, empresas de TI y entidades gubernamentales.
Se desempeña en el área de seguridad de la información, cuenta con amplia experiencia en la implementación de soluciones tecnológicas para proteger el ciberespacio en infraestructura nacional y fabricantes internacionales.
Tiene experiencia en monitoreo tecnológico profesional de cuerpos en la industria de petróleo y gas.

Basados en la vasta experiencia y conocimiento que hemos adquirido, hemos desarrollado el método del **Ciclo de Ciberseguridad**, el cual está compuesto por cinco productos que brindan una visión amplia, actualizada, detallada y objetiva de la situación a través de pruebas de campo, pruebas y evaluaciones de riesgos. La imagen que se obtendrá a través de ellos, permite un ajuste óptimo de soluciones de seguridad OT precisas y adaptadas a su empresa u organización.

Más sobre nuestros productos y más preguntas y dudas: estaremos encantados de atenderle
+55(11)913152442 I amitai@samsecot.com