Como impulsar la resiliencia y recuperación en sistemas operativos de tecnología críticos

La tecnología operativa (OT) es el pilar que sustenta procesos claves en industrias críticas, pero que debido a su confiabilidad es comúnmente ignorada desde una perspectiva de seguridad. Existe un supuesto de que, si un sistema ha trabajado bien durante años, seguirá haciéndolo. La realidad es que la convergencia entre OT e IT expone estos sistemas a ataques. La convergencia se encarga de que sistemas OT previamente aislados sean conectados a sistemas IT, lo que significa que ya no son independientes.

Estos activos OT son comúnmente sistemas antiguos que pueden resultar difíciles de actualizar y aplicar parches sin causar tiempos muertos, en el mejor de los casos estos parches se aplican de forma esporádica. Estas vulnerabilidades se acumulan con el tiempo y están listas para explotar cuando la tecnología operativa es conectada a los sistemas de IT. Como resultado 51% de los líderes de IT y encargados de las barreras de seguridad creen que sus sistemas de OT serán víctimas de ataque en los próximos años, de acuerdo con investigación independiente realizada en enero 2026.

La convergencia entre IT/OT ha facilitado el IoT (Internet of Things) Industrial y la transferencia de datos en tiempo real, generando ganancias reales en forma de operaciones más inteligentes y eficientes, pero creando a la vez una superficie para ataques. De manera consecuente, las industrias críticas ahora buscan poner protecciones en sitio e impulsar la resiliencia, así, en caso de un ataque, la organización pueda seguir funcionando sin que se detengan las operaciones de manera masiva.

La inactividad como brecha para los atacantes

Los proveedores en industrias críticas de riesgo tienen un objetivo en sus espaldas, ya que los atacantes saben que los tiempos de inactividad pueden ser altamente disruptivos y costosos, poniendo en jaque la viabilidad del negocio. Si pueden generar tiempo inactivo pueden ejercer más presiones sobre los negocios para exigir un rescate o lograr su objetivo de afectar la economía. Por esta razón Jonathan Ellison, director de National Resilience en NCSC, urge a los proveedores de CINI prepararse para ataques cibernéticos en febrero, estas amenazas deben ser “monitoreadas por los operadores para permitirles tomar pasos informados y bien estructurados para proteger su infraestructura”.

El monitoreo de ambientes OT puede ayudar a detectar actividad anómala que podría ser indicio de un ataque, pero que no es un ejercicio directo debido a las limitaciones prácticas asociadas con estos sitios. Muchos cuentan con ambientes de espacio limitado que impiden la posibilidad de un monitoreo físico, mientras que otros en sitios con bandas bajas o remotas tendrán problemas con la transferencia de

datos y no podrán entregar información en tiempo real. Estas limitaciones hacen que el monitoreo de seguridad tradicional sea poco adecuado.

Para superar estos problemas, las organizaciones críticas deben poder utilizar sensores diseñados específicamente para ambientes industriales que tengan impactos mínimos sobre las operaciones. Estos sensores pasivamente monitorean el tráfico y comportamiento del sistema, recogiendo telemetría que puede ser traducida y enviada a equipos de OT e IT para obtener información valiosa.

Los sensores deben alimentar el SOC

Si la metadata adquirida por estos sensores es dirigida mediante el Centro de Seguridad de Operaciones (SOC), puede ser utilizada para mirar indicadores de compromiso, como intentos de acceso no autorizados, cambios de comando o movimientos laterales. La detección de amenazas y respuestas ven la data correlacionada con inteligencia global para verificar la alerta en minutos, de esta manera el equipo de seguridad puede tomar pasos para mitigar el ataque, evitando que escale. Detectar estos ataques en etapas tempranas minimiza el impacto y reduce la probabilidad que tener que desconectar todos los sistemas.

Si la metadata de un sensor OT es continuamente evaluada de esta manera, puede generar medios proactivos de defensa para impulsar la resiliencia. Esto debido a que conducir el monitoreo y la respuesta simultáneamente entre los sistemas OT e IT puede prevenir que los ataques afecten ambos ambientes. Ningún evento singular puede tumbar el sistema completo, y existe una redundancia significativa para que el sistema pueda seguir operando en caso de una apertura.

La configuración de los sensores OT monitoreados vía SOC pueden ser obtenidos internamente por medio del equipo de seguridad operativa o por un contratista que ofrezca la gestión de detección y respuesta (MRD). Solo añadirá verdadero valor si la alerta que entra tiene un buen contexto. Cada evento capturado debe ser combinado con inteligencia para crear un caso al que se pueda responder. Es un proceso que luego permite una recuperación más rápida si otro evento similar ocurriese en el futuro, permitiendo a la organización de manera efectiva mejorar y fortalecer las deficiencias en el tiempo.

Porque no se recomienda un monitoreo improvisado o ad-hoc

El problema de hoy es que algunas organizaciones críticas están buscando otros medios de monitoreo. La misma investigación citada encontró que el 28% de organizaciones tiene una coordinación manual o ad-hoc para su visibilidad y monitoreo de OT/IT. Quienes responden también reportaron una falta de consistencia cuando viene al monitoreo de ambientes OT, con el 32% utilizando plataformas de detección construidas originalmente para IT, 29% utilizando herramientas activas de visibilidad, y 28% con lógica de detección desarrollada específicamente para la tarea. Estos hallazgos resaltan una necesidad para una mejor integración y monitoreo especializado.

En vez de adaptarse o crear soluciones desde cero, el monitoreo específico de OT debe adecuarse al ambiente al que sirve. Esto es debido a que, mientras ambos ambientes necesitan ser monitoreados, ambos tienen tolerancias muy distintas. IT es mucho mas ruidoso y normalmente generará mayores volúmenes de alerta mientras que en eventos de OT es probable que sean menos frecuentes pero que presentan un riesgo más grande debido a que estos sistemas necesitan mantenerse operativos. Adaptar la seguridad IT para desempeñar la seguridad OT no es necesariamente productivo.

Sin embargo, combinar el monitoreo a través de los dos estados tiene sentido. Si la inteligencia es utilizada, la respuesta puede ser coordinada, lo que resulta en una toma de decisiones mas rápida en el SOC. Además, al utilizar ejercicios de prueba y validación basados en MITRE ATT&CK para la estructura ICS, es posible evaluar como los ataques pueden desarrollarse y probar rápidamente que tan rápido reaccionan los equipos. Ensayar estos escenarios ayuda a mitigar el riesgo de paradas preventivas que pueden llegar a ser tan disruptivas como el mismo ataque. Adicionalmente crear sets de datos con respecto al monitoreo IT/OT puede ayudar con las obligaciones de cumplimiento, como los requerimientos de evaluación de riesgo encapsulados en NIS2.

Los sensores OT pueden suministrar a la industria crítica con la habilidad para mejorar la visibilidad de los activos, detección de amenazas y respuestas. Haciendo esto no solo proporcionan protección, sino control y estabilidad necesaria para impulsar la resiliencia, ayudando a estas organizaciones a prepararse en caso de ataques cibernéticos sobre los que ha advertido NCSC.

Puede leer la noticia original haciendo click aquí.