Costo: $$$	Impacto: MEDIO	Complejidad: ALTO

3.A: ¿Mantiene el WWS una lista de las amenazas y tácticas, técnicas y procedimientos (TTP) de los atacantes para realizar ataques informáticos relevantes para el WWS?

Recomendación: Reciba alertas de la CISA, priorice la lista de vulnerabilidades conocidas aprovechadas (KEV) y mantenga documentación sobre los TTP relevantes para el WWS.

¿Por qué es importante este control?

Los atacantes suelen emplear pasos o métodos comunes durante un ataque informático, conocidos como TTP. Si un WWS es consciente de los TTP comunes, puede monitorearlos en la red del WWS y detectar un ataque antes de que interrumpa o dañe las operaciones.

Este control es importante porque ayuda a un WWS a estar al tanto y detectar amenazas a sus redes de TO y TI.

Consejos de implementación

El WWS debe monitorear los componentes internos y externos como parte de su programa de ciberseguridad de TO y TI. El monitoreo externo observa los eventos en el límite de la red, y el monitoreo interno captura los eventos dentro de los sistemas del WWS.

Adopte las medidas y mitigaciones recomendadas en las alertas de la CISA, como alertas de tráfico de red sospechoso o sistemas comerciales de prevención y detección para detectar amenazas clave cuando sea factible. Incluir el catálogo de vulnerabilidades conocidas aprovechadas (KEV) de la CISA en sus alertas de vulnerabilidad ayuda a las organizaciones a priorizar y abordar las vulnerabilidades que están siendo aprovechadas activamente por delincuentes. Estas alertas proporcionan información crítica sobre las estrategias de mitigación y son esenciales para priorizar los esfuerzos de seguridad para cerrar rápidamente las brechas más peligrosas en las defensas informáticas.

ORIENTACIÓN ADICIONAL

- Las alertas y los avisos proporcionan información oportuna sobre problemas actuales de ciberseguridad y TTP, vulnerabilidades y exploits. Regístrese para recibir alertas y avisos por correo electrónico por parte de la CISA del DHS. Otras fuentes útiles para comprender los TTP y las acciones que puede realizar un atacante para moverse a través de una red de TO o TI son los marcos de MITRE ATT&CK y de MITRE ATT&CK para ICS, respectivamente.
- Hay muchas herramientas disponibles comercialmente que un WWS puede usar para monitorear ciertos tipos de ataques o intrusiones informáticos en la red del WWS. Estas herramientas incluyen sistemas de detección de intrusiones/sistemas de prevención de intrusiones (IDS/IPS), reglas de cortafuegos que filtran y alertan sobre cierto tráfico y herramientas de monitoreo de la red del ICS.
- Estas herramientas pueden enviar alertas a un sistema de monitoreo central, a menudo llamado herramienta de monitoreo de información y eventos del sistema (SIEM). Una herramienta SIEM extrae datos de muchas fuentes (p. ej., IDS/IPS, cortafuegos, herramientas de monitoreo de red, eventos de Windows) en un panel y puede alertar al WWS sobre actividad de red inusual o maliciosa.

Siga su plan de respuesta a incidentes (consulte la hoja informativa 2.S) para la contención, eliminación y recuperación de cualquier amenaza identificada.

Recursos

Estándar 800-82 (revisión 3) del NIST, Guía para la seguridad de la tecnología operacional (TO): Consulte el Apéndice F.7.18 (página 291) para obtener más información sobre la integridad del sistema y de la información (sección "System and Information Integrity"). *https://csrc.nist.gov/pubs/sp/800/82/r3/final*

Estándar 800-53 (revisión 5) del NIST, Controles de seguridad y privacidad para sistemas de información y organizaciones: Consulte el control SI-4 (página 336) para obtener más información sobre el monitoreo del sistema (sección "System Monitoring"). *https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final*

Alertas de la CISA del DHS: Consulte este recurso para registrarse para recibir alertas por correo electrónico del Sistema Nacional de Concientización Informática de la CISA del DHS sobre nuevas vulnerabilidades.
https://www.cisa.gov/uscert/ncas/alerts

MITRE ATT&CK y MITRE ATT&CK para ICS: Consulte estos recursos para obtener más información sobre los TTP comunes en los sistemas de TO y TI, respectivamente.
https://attack.mitre.org/matrices/ics/;
https://attack.mitre.org/matrices/enterprise/