

¿Cómo monitoreo el estado (Health) del Agente?

Monitoreo de Agentes Offline/Online

Página de Agentes

En la página de Agentes, se registra la fecha y hora del último check-in **por actividad**. En términos generales, si un agente de software está funcionando y conectado a Internet, cada comportamiento debería tener una fecha de menos de un par de horas. Algunas actividades son activadas por eventos en el endpoint, mientras que otras se establecen mediante temporizadores, pero con un desfase de "jitter" de hasta 30 segundos, para que los clientes no experimenten picos en la actividad de red.

85753879.png?width=680

Gestión de Notificaciones Offline

Para configurar la notificación de agentes offline, utilice la página de Notificaciones de Seguridad.

Estas notificaciones están pensadas para las siguientes situaciones:

1. Existe un problema de red entre un agente y los servidores de Cyber Crucible. Esto puede deberse a un firewall (provocado por un atacante, o simplemente por operaciones de TI), o a que el agente está en ejecución pero desconectado. La protección se mantiene durante los períodos sin conexión, pero las notificaciones al equipo de seguridad no ocurrirán hasta que el agente vuelva a estar en línea.
2. Existe un problema con el software de Cyber Crucible. Esto es muy, muy poco frecuente. Por favor, [abra un ticket de soporte](#) con Cyber Crucible de inmediato si esto ocurre.

3. La máquina está apagada. Este es el escenario más común. A continuación se analizan las mejores prácticas.

85688410.png?width=680

Mejores prácticas para la notificación offline

Una consideración importante para la notificación offline es que una máquina que ha sido apagada aparecerá como offline ante los servidores de Cyber Crucible. Las estaciones de trabajo, propensas a encenderse y apagarse durante las operaciones normales del negocio, generarían notificaciones offline durante los almuerzos, viajes entre ubicaciones o días festivos.

Las mejores prácticas para los grupos ya dividen los servidores de las estaciones de trabajo. Los servidores normalmente se benefician mejor de períodos de notificación offline más cortos, en caso de que exista un problema. Los grupos enfocados en estaciones de trabajo son más adecuados para períodos más largos de aparición offline.

Muchos clientes de Cyber Crucible consideran mejor crear notificaciones automatizadas solo para los grupos de servidores, y filtrar periódicamente uno de los campos de fecha en la página de Administrar Agentes por una fecha, como "Mostrar los agentes cuyo campo de Actualización de Datos de la Máquina no se haya actualizado en la última semana".

85688417.png?width=453

Agentes Que No Están Completamente Actualizados

Los agentes de Cyber Crucible requieren un reinicio para actualizarse. Puede encontrar una mayor comprensión de los algoritmos de actualización [aquí](#). Cuando un agente reporta que un reinicio dará como resultado una actualización, la página de Agentes indica qué máquinas requieren una actualización y están listas para actualizarse al reiniciar. A veces, las máquinas que no se reinician con frecuencia (normalmente servidores) acumularán varias actualizaciones en espera antes de actualizarse realmente. Vemos un ejemplo de esto en la captura de pantalla. La hora del último reinicio también está disponible.

El informe ejecutivo semanal de Cyber Crucible identifica ese número de agentes que requieren una actualización, y cuántos de ellos están listos para actualizarse tan pronto como se reinicien. Las dos razones más comunes por las que una máquina requiere una actualización, pero no está lista/en espera, son:

1. La máquina ha estado desconectada, como en el caso de un empleado de vacaciones.

2. La máquina tuvo un fallo de hardware o software mayor/renovación, y Cyber Crucible en realidad ya no está en esa máquina.

Aparte de esos dos casos, las actualizaciones normalmente ocurren muy rápidamente, y sin la intervención del administrador más allá de las actividades normales de parcheo y reinicio.

85688423.png

Revision #1

Created 2026-07-24 01:29:29 UTC by Dennis Underwood

Updated 2026-07-24 01:29:29 UTC by Dennis Underwood