

Como monitorar a Integridade do Agente?

Monitoramento de Agente Offline/Online

Página de Agentes

Na página de Agentes, a data e hora do último check-in **por atividade** é registrada. De modo geral, se um agente de software estiver funcionando e conectado à Internet, cada comportamento deverá ter uma data de menos de algumas horas. Algumas atividades são acionadas por atividades no endpoint, enquanto outras são definidas por temporizadores, mas com um deslocamento de “jitter” de até 30 segundos, para que os clientes não tenham picos na atividade de rede.

85753879.png?width=680

Gerenciamento de Notificações Offline

Para configurar a notificação de agentes offline, use a página de Notificações de Segurança.

Essas notificações destinam-se às seguintes situações:

1. Há um problema de rede entre um agente e os servidores da Cyber Crucible. Isso pode ser devido a um firewall (motivado por um hacker, ou apenas por operações de TI), ou o agente está em execução, mas offline. A proteção é mantida durante os períodos offline, mas as notificações à equipe de segurança não ocorrerão até que o agente volte a ficar online.
2. Há um problema com o software da Cyber Crucible. Isso é muito, muito raro. Por favor, [abra um chamado de suporte](#) com a Cyber Crucible imediatamente, caso isso ocorra.
3. A máquina está desligada. Este é o cenário mais comum. A seguir, discutiremos as melhores práticas.

Melhores práticas para Notificação Offline

Uma consideração importante sobre a notificação offline é que uma máquina que foi desligada aparecerá como offline para os servidores da Cyber Crucible. Estações de trabalho, propensas a serem ligadas e desligadas durante as operações normais de negócios, produziriam notificações offline durante pausas para almoço, deslocamentos entre locais ou durante feriados.

As melhores práticas para grupos já separam servidores de estações de trabalho. Servidores geralmente são melhor atendidos com períodos de notificação offline mais curtos, caso haja algum problema. Grupos focados em estações de trabalho são melhores para períodos mais longos de aparência offline.

Muitos clientes da Cyber Crucible consideram melhor criar notificações automatizadas apenas para grupos de servidores, e filtrar periodicamente um dos campos de data na página Gerenciar Agentes por uma data, como “Mostrar-me agentes cujo campo de Atualização de Dados da Máquina não foi atualizado na última semana”.

Agentes Que Não Estão Totalmente Atualizados

Os agentes da Cyber Crucible exigem uma reinicialização para atualizar. Um entendimento mais aprofundado dos algoritmos de atualização pode ser encontrado [aqui](#). Quando um agente informa que uma reinicialização resultará em uma atualização, a página de Agentes lista quais máquinas requerem uma atualização e estão prontas para atualizar após a reinicialização. Às vezes, máquinas que não são reinicializadas com frequência (normalmente servidores) acumulam várias atualizações antes de realmente atualizar. Vemos um exemplo disso na captura de tela. O horário da última reinicialização também está disponível.

O relatório executivo semanal da Cyber Crucible identifica o número de agentes que requerem uma atualização, e quantos deles estão prontos para atualizar assim que forem reinicializados. Os dois motivos mais comuns pelos quais uma máquina requer uma atualização, mas não está pronta/preparada, são:

1. A máquina esteve offline, como um funcionário de férias.
2. A máquina teve uma falha/renovação de hardware ou de software importante, e a Cyber Crucible, na verdade, não está mais nessa máquina.

Fora esses dois casos, as atualizações normalmente ocorrem muito rapidamente, e sem envolvimento do administrador, além das atividades normais de aplicação de patches e reinicialização.

85688423.png

Revision #1

Created 2026-07-24 05:27:38 UTC by Dennis Underwood

Updated 2026-07-24 05:27:38 UTC by Dennis Underwood