

# Wie überwache ich den Agent-Status (Agent Health)?

## Offline/Online-Agent-Überwachung

### Seite „Agents“

Auf der Seite „Agents“ wird das Datum und die Uhrzeit der letzten Anmeldung **pro Aktivität** erfasst. Allgemein gesprochen sollte, wenn ein Software-Agent funktioniert und mit dem Internet verbunden ist, jedes Verhalten ein Datum aufweisen, das weniger als ein paar Stunden zurückliegt. Manche Aktivitäten werden durch Vorgänge auf dem Endpunkt ausgelöst, während andere zeitgesteuert erfolgen, jedoch mit einem „Jitter“-Versatz von bis zu 30 Sekunden, damit Kunden keine Spitzen bei der Netzwerkaktivität erleben.

85753879.png?width=680

## Verwaltung der Offline-Benachrichtigungen

Um Benachrichtigungen für Offline-Agenten einzurichten, verwenden Sie die Seite „Security Notifications“.

Diese Benachrichtigungen sind für folgende Situationen vorgesehen:

1. Es liegt ein Netzwerkproblem zwischen einem Agenten und den Cyber Crucible-Servern vor. Dies kann entweder durch eine Firewall (durch einen Hacker verursacht oder durch normale IT-Vorgänge) bedingt sein, oder der Agent läuft, ist jedoch offline. Der Schutz bleibt während Offline-Zeiten bestehen, jedoch erfolgen Sicherheitsteam-Benachrichtigungen erst, wenn der Agent wieder online ist.

2. Es liegt ein Problem mit der Cyber Crucible-Software vor. Dies ist sehr, sehr selten. Bitte [öffnen Sie unverzüglich ein Support-Ticket](#) bei Cyber Crucible, falls dies auftritt.
3. Der Rechner ist ausgeschaltet. Dies ist das häufigste Szenario. Eine Erörterung bewährter Vorgehensweisen folgt als Nächstes.

85688410.png?width=680

## Bewährte Vorgehensweisen für Offline-Benachrichtigungen

Ein wichtiger Aspekt bei Offline-Benachrichtigungen ist, dass ein ausgeschalteter Rechner den Cyber Crucible-Servern als offline erscheint. Arbeitsplatzrechner, die im normalen Geschäftsbetrieb häufig ein- und ausgeschaltet werden, würden während Mittagspausen, Reisen zwischen Standorten oder an Feiertagen Offline-Benachrichtigungen erzeugen.

Bewährte Vorgehensweisen für Gruppen trennen Server bereits von Arbeitsplatzrechnern. Server werden typischerweise am besten mit kürzeren Offline-Benachrichtigungszeiträumen bedient, falls ein Problem auftritt. Auf Arbeitsplatzrechner ausgerichtete Gruppen eignen sich am besten für längere Zeiträume, bevor sie als offline gemeldet werden.

Viele Cyber Crucible-Kunden halten es für am besten, automatisierte Benachrichtigungen nur für Servergruppen zu erstellen und regelmäßig eines der Datumsfelder auf der Seite „Manage Agents“ nach einem Datum zu filtern, beispielsweise „Zeige mir Agenten, deren Feld ‚Machine Data Update‘ in der vergangenen Woche nicht aktualisiert wurde“.

85688417.png?width=453

## Agenten, die nicht vollständig aktualisiert sind

Cyber Crucible-Agenten erfordern einen Neustart, um aktualisiert zu werden. Weiterführende Informationen zu den Aktualisierungsalgorithmen finden Sie [hier](#). Wenn ein Agent meldet, dass ein Neustart zu einer Aktualisierung führen wird, listet die Seite „Agents“ auf, welche Rechner eine Aktualisierung benötigen und bereit sind, beim Neustart zu aktualisieren. Manchmal stapeln Rechner, wenn sie nicht häufig neu gestartet werden (typischerweise Server), mehrere Aktualisierungen, bevor tatsächlich ein Upgrade erfolgt. Ein Beispiel dafür ist im Screenshot zu sehen. Die letzte Neustartzeit ist ebenfalls verfügbar.

Der wöchentliche Cyber Crucible-Führungsbericht weist die Anzahl der Agenten aus, die ein Upgrade benötigen, sowie wie viele davon bereit sind, sofort nach einem Neustart zu aktualisieren. Die zwei häufigsten Gründe, warum ein Rechner eine Aktualisierung benötigt, aber nicht

bereit/vorbereitet ist, sind:

1. Der Rechner war offline, beispielsweise weil ein Mitarbeiter im Urlaub war.
2. Der Rechner hatte einen Hardware- oder größeren Softwareausfall/-austausch, und Cyber Crucible befindet sich tatsächlich nicht mehr auf diesem Rechner.

Abgesehen von diesen beiden Fällen erfolgen Aktualisierungen normalerweise sehr schnell und ohne Beteiligung von Administratoren, außer im Rahmen der üblichen Patch- und Neustartvorgänge.

85688423.png

---

Revision #1

Created 2026-07-24 04:12:22 UTC by Dennis Underwood

Updated 2026-07-24 04:12:22 UTC by Dennis Underwood