Fehlerbehebung für Active Directory-Benutzer, die im Bericht zur Aktivitätssuche in Umbrella fehlen

Inhalt

Einleitung

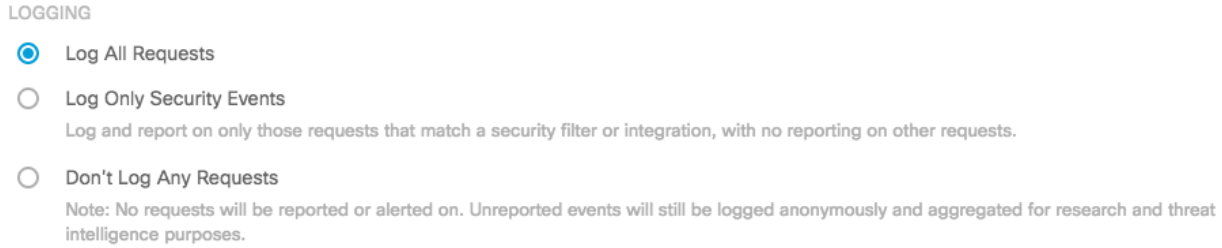
Dieses Dokument beschreibt den Bericht zur Aktivitätssuche in Cisco Umbrella. Der Aktivitätssuchbericht ist ein nahezu vollständiger Bericht aller DNS-Abfragen, die Ihre Benutzer durchführen. Wenn Sie die Cisco Umbrella Active Directory (AD)-Integration eingerichtet haben, können Sie erwarten, dass Ihre AD-Benutzer die Spalte "Identität" in Ihrer Aktivitätssuche ausfüllen. Es gibt jedoch Situationen, in denen die Benutzer in der Spalte "Identität" fehlen.

Auflösung

Wenn Sie der Meinung sind, dass Sie AD-Benutzer direkt in der Spalte Identität in der Aktivitätssuche sehen sollten, diese jedoch nicht sehen, oder wenn Sie einige, jedoch nicht so viele sehen, wie Sie erwartet haben, sollten Sie einige Punkte überprüfen:

1. Standorte und Active Directory
    - Überprüfen Sie alle AD-Komponenten, um sicherzustellen, dass keine Fehler oder Probleme gemeldet werden. Wenn auf einer der Komponenten graue, orangefarbene oder rote Statusanzeigen angezeigt werden, erhalten Sie diese Informationen, und öffnen Sie ein Support-Ticket (umbrella-support@cisco.com).
        - Diagnosetest eines betroffenen Benutzers (ein Benutzer, der nicht in der Aktivitätssuche angezeigt wird)
        - Screenshot der Konsole der virtuellen Appliance (VA) mit erweiterten Fehlermeldungen
        - AD Connector - Audit-Protokolle
2. Protokolleinstellungen
    - In den erweiterten Einstellungen jeder Richtlinie gibt es unten einen Abschnitt, der sich mit dem Umfang der Protokollierung befasst. Sie können diese Einstellung wie folgt festlegen:
        - Alle Anforderungen protokollieren
        - Nur Sicherheitsereignisse protokollieren

    - Keine Anforderungen protokollieren
- Wenn Ihre Richtlinie derzeit auf "Nur Sicherheitsereignisse protokollieren" festgelegt ist, kann dies erklären, warum Sie nicht so viele Abfragen sehen, wie Sie erwarten, oder überhaupt keine Ergebnisse von einigen Benutzern.



3. Korrekte Richtlinienpriorität
    - Wenn eine Richtlinie auf eine Netzwerkidentität angewendet wird, die in der Liste der Richtlinien höher ist als die AD-Benutzerrichtlinie, wird die Netzwerkidentitätsrichtlinie wahrscheinlich angewendet. Dies wiederum bedeutet, dass Sie auf der Aktivitätssuche das Netzwerk als die gemeldete Identität sehen. Lesen Sie auch die Cisco Umbrella-Dokumentation zu Best Practices und der Richtlinienpriorität.

Ursache

Woher erhält die Aktivitätssuche die "Identität"?

Wenn eine DNS-Abfrage in Umbrella eingeht und die AD-Integration wie erwartet funktioniert, werden diese Informationen in der Abfrage weitergegeben:

- Interne IP-Adresse
- AD-Identitäts-Hash (Benutzer, Host oder beide)
- Ausgangs-IP
- Domäne, die abgefragt wird

Der AD-Identitäts-Hash wird der Abfrage von der virtuellen Appliance hinzugefügt, an die diese Informationen übergeben werden, sowie der entsprechenden internen IP-Adresse für das Anmeldeereignis vom AD Connector.

Cisco Umbrella verwendet diese Informationen, um das Unternehmen zu finden und zu bestimmen, welche Richtlinie angewendet werden soll. Wenn Sie keine Richtlinien speziell auf Ihre AD-Benutzer angewendet haben, aber über eine Richtlinie für Ihre Netzwerke oder Standorte verfügen, wendet Cisco Umbrella die Richtlinie unter Verwendung dieser Identität an. Dies bedeutet, dass, wenn die Abfrage, die Identität und die Antwort in der Aktivitätssuche gemeldet werden, die Identität, die die gemeldete Richtlinie ausgelöst hat. Die anderen Informationen werden in der Anforderung weiterhin gekennzeichnet, sodass Sie weiterhin nach einem AD-Benutzer suchen und die Aktivität abrufen können, die ein Netzwerk als Identität meldet. Wenn Sie die Daten der Aktivitätssuche in eine CSV-Datei exportieren, werden zudem alle Identitätsinformationen angezeigt, die mit der Abfrage verknüpft sind.

Zusätzliche Informationen

Wenn Sie immer noch keine AD-Benutzer sehen, wenden Sie sich an den Support (umbrella-support@cisco.com) mit einem Diagnosetestergebnis und allen relevanten AD Connector Audit Logs.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.