Cisco Secure Endpoint Global Threat Alerts (GTA) - Häufig gestellte Fragen zum Ende des Service

Inhalt

Einleitung

Häufig gestellte Fragen

- Zeitplan für das Ende des Servicezeitraums
- Welche Produkte sind betroffen?
- Durch welche Produkte wird diese Funktion ersetzt?
- Welche Maßnahmen müssen Kunden ergreifen?
- Wird diese Änderung Auswirkungen auf mich haben?
- Welche Auswirkungen hat mein Produkt?
- Welche Auswirkungen hat mein Service derzeit?
- Was muss ich tun, um die Außerbetriebnahme dieser Funktion vorzubereiten?
- Muss ich irgendwelche Maßnahmen ergreifen, nachdem die Funktion außer Betrieb genommen wurde?

Einleitung

Dieses Dokument beantwortet häufig gestellte Fragen zur Einstellung der Funktion "Global Threat Alerts" von Cisco Secure Endpoint.

Ankündigung des Serviceendes

Cisco Secure Endpoint stellt die Funktion Global Threat Analytics (GTA) ein. Ab dem 1. Februar können sich Kunden nicht mehr bei GTA anmelden. Ab dem 31. Juli erhalten die Kunden keine Veranstaltungsdaten mehr, die von der GTA generiert wurden.

Häufig gestellte Fragen

Zeitplan für das Ende des Servicezeitraums

- 6. Februar 2024 - Kunden können sich nicht mehr für GTA-bezogene Funktionen anmelden.
- 31. Juli 2024 - Der GTA Cloud Service hört auf, Daten zu verarbeiten. Das GTA-Backend und das Dashboard werden außer Betrieb genommen. Es werden keine neuen Kundenveranstaltungen generiert.

Welche Produkte sind betroffen?

- Cisco Secure Endpoint AKA AMP für Endgeräte

- Cisco Global Threat Analytics
- Cisco Secure Network Analytics AKA Stealth Watch Enterprise

Durch welche Produkte wird diese Funktion ersetzt?

- XDR stellt die engste Abgleichung in Bezug auf die Funktionalität dar, bietet jedoch keinen 1:1-Ersatz für die von Global Threat Analytics bereitgestellten Funktionen.

Welche Maßnahmen müssen Kunden ergreifen?

- Sichere Endgeräte von Cisco
  - Keine Kundenaktion erforderlich.
  - Details: Ab dem 31. Juli stellt Secure Endpoint keine Warnungen mehr dar, die von der GTA-Funktion generiert wurden.
- Globale Bedrohungsanalysen
  - Keine Kundenaktion erforderlich.
  - Was zu erwarten ist: Ab dem 31. Juli werden die Daten nicht mehr vom GTA-Dienst aufgenommen, die Datenverarbeitung wird gestoppt und es werden keine weiteren Ereignisse generiert. Kunden wird empfohlen, den Versand von Daten an GTA auf ihren unterstützten Appliances zu deaktivieren.

Wird diese Änderung Auswirkungen auf mich haben?

- Wenn Sie Secure Endpoint oder Secure Network Analytics besitzen und die GTA-Funktion aktiviert haben, wirkt sich diese Änderung auf Ihre Produkte aus.

Welche Auswirkungen hat mein Produkt?

- Sichere Endgeräte
  - Secure Endpoint erhält keine Warnungen und Telemetriedaten mehr von Global Threat Analytics. Dadurch werden weniger Konsolenbenachrichtigungen für Netzwerkverkehr mit schädlichen IPs und URLs erstellt.

- Sichere Netzwerkanalysen
  - Das Widget "Globale Bedrohungswarnungen" auf dem SNA Dashboard ist nach Version 7.5.1 nicht mehr verfügbar. Bei früheren Versionen bleibt das GTA-Widget auf dem SNA Dashboard erhalten und kann nicht geladen werden. Kunden von Cisco Secure Network Analytics können ähnliche Ergebnisse wie der GTA-Service erzielen, indem sie die Funktion "Central Analytics" verwenden, die mit der Data Store-Architektur verfügbar ist, und sie in den Talos Threat Intelligence-Feed integrieren. o Weitere Informationen zu den Auswirkungen auf SNA finden Sie in den Häufig gestellten Fragen zu globalen Bedrohungswarnungen (GTA) zum Ende des Service (EOS).

Welche Auswirkungen hat mein Service derzeit?

- Kunden, die die GTA-Funktion nutzen, sind davon erst am 31. Juli 2024 betroffen.

Was muss ich tun, um die Außerbetriebnahme dieser Funktion vorzubereiten?

- Sicheres Endgerät: Es ist keine Kundenaktion erforderlich.
- Sichere Netzwerkanalysen: Es ist kein Eingreifen des Kunden erforderlich.

Muss ich irgendwelche Maßnahmen ergreifen, nachdem die Funktion außer Betrieb genommen wurde?

- Kunden sollten in Betracht ziehen, den Versand von Protokollen von ihren Web Security Appliance (WSA)- oder F5-Proxys an den GTA-Service zu deaktivieren.
- Für SNA:
  - Funktion in der zentralen Verwaltung (SMC) ausschalten
  (Gehen Sie zu Inventar > wählen Sie Ihre SMC > Appliance-Konfiguration > Allgemein > Externe Dienste > deaktivieren Sie die Option "Globale Bedrohungswarnungen aktivieren")
  - Wiederholen Sie den Vorgang mit Ihren Flow Collectors (FCs).
  ODER
  - Upgrade auf Version 7.5.1, wenn verfügbar im Sommer 2024

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.