

06 mars 2024

Résumé de l'incident

Une panne réseau survenue le 06/03/2024 a affecté l'accès à l'interface (front-end) du tableau de bord Cyber Crucible ainsi que l'accès à la télémétrie via API. Ce problème a depuis été résolu au 07/03/2024.

Cause première

À 04h00 UTC le 06/03/2024, le trafic de télémétrie a commencé à augmenter progressivement pour atteindre finalement 1600 % du trafic agent normal. De plus, la bande passante réseau entre les instances AWS a commencé à être limitée à des débits réduits entre les équilibrateurs de charge, serveurs et bases de données hébergés sur AWS. Sur plusieurs zones, les contraintes de bande passante étaient variables et allaient d'une perte totale de transmission (0 % de la capacité) à 50 % de la capacité. La disponibilité du DNS AWS a également été compromise. Le trafic réseau entrant vers Cyber Crucible a été confirmé comme étant du trafic agent valide provenant de clients existants. Le trafic de bots vers les équilibrateurs de charge n'a pas augmenté en volume. La bande passante supplémentaire n'était pas le principal facteur d'indisponibilité des serveurs, mais a aggravé les problèmes de bande passante liés au middleware et aux bases de données. Le pic de trafic agent observé durant cette période s'est partiellement résorbé. À ce stade, Cyber Crucible ne communique sur aucune corrélation entre les pannes cloud publiées le 06/03/2024 et les problèmes AWS ou le pic de trafic.

Impact

L'accès au tableau de bord et aux API de Cyber Crucible aurait pu être retardé ou indisponible. La télémétrie provenant des agents installés a été entièrement préservée et sa transmission à la base de données a pu être retardée, mais aucune télémétrie n'a été perdue. Les protections des agents sur les postes n'ont été absolument pas affectées, fonctionnant normalement, car aucune analyse ni protection ne dépend d'une connexion réseau vers une quelconque API en amont. À ce stade, l'ensemble de la télémétrie a « rattrapé son retard » dans le tableau de bord.

Résolution

Cyber Crucible a créé plusieurs serveurs à l'intérieur et à l'extérieur d'AWS. La stabilité du réseau au sein d'AWS semble s'être améliorée durant la nuit (07/03/2024), avec des améliorations observées dès 02h00 UTC. Cyber Crucible fonctionne actuellement à 500 % de la capacité serveur, calculée sur la base de la bande passante de trafic de pointe qui s'est depuis résorbée. L'équipe a remplacé les serveurs hébergés sur AWS à mesure qu'ils perdaient leur connectivité réseau.

Pour être clair, l'ajout de capacité serveur supplémentaire n'a pas constitué une résolution efficace dans ce cas.

Cyber Crucible a entamé une transition visant à ne plus utiliser AWS comme unique fournisseur d'hébergement cloud.

Les travaux visant à assurer une indépendance vis-à-vis des plateformes cloud étaient déjà en cours depuis plusieurs mois, avec des plans initiaux de transition depuis AWS comme fournisseur unique prévus pour le T2 2024. Les tests de bout en bout, y compris tous les

schémas de double chiffrement et d'authentification x509 nécessaires pour nos différents serveurs et

services, ont été achevés fin février 2024. Les problèmes réseau que nous avons rencontrés avec AWS ont accéléré cette transition, initialement prévue pour le T2, en la faisant débiter un mois avant la date prévue.

Revision #1

Created 2026-07-24 06:46:26 UTC by Dennis Underwood

Updated 2026-07-24 06:46:26 UTC by Dennis Underwood