06 de marzo de 2024

Resumen del problema

Una interrupción de red ocurrida el 6MAR2024 afectó el acceso frontal al panel de control de Cyber Crucible
y el acceso a la telemetría a través de la API. Este problema se ha resuelto desde el 7MAR2024.

Causa raíz

A las 0400 UTC del 6MAR2024, el tráfico de telemetría comenzó a aumentar hasta alcanzar eventualmente el 1600% del tráfico
normal de agentes. Además, el ancho de banda de red entre las instancias de AWS comenzó a limitarse a
velocidades reducidas entre los balanceadores de carga, servidores y bases de datos alojados en AWS. En
múltiples zonas, las restricciones de ancho de banda fueron variables y oscilaron entre una pérdida total de transmisión (0% de capacidad) hasta el 50% de la capacidad. La disponibilidad del DNS de AWS también se vio comprometida.
Se confirmó que el tráfico de red entrante hacia Cyber Crucible era tráfico válido de agentes de clientes
existentes. El tráfico de bots hacia los balanceadores de carga no aumentó en volumen.
El ancho de banda adicional no fue el factor principal de la indisponibilidad de los servidores, pero exacerbó
los problemas de ancho de banda del middleware y la base de datos.
El aumento en el tráfico de agentes durante ese período ha disminuido parcialmente.
En este momento, Cyber Crucible comunica que no existe correlación entre las interrupciones de nube publicadas el
6MAR2024 y los problemas de AWS o el aumento del tráfico.

Impacto

El acceso al panel de control y a las API de Cyber Crucible se habría visto retrasado o no disponible. La telemetría de los agentes instalados se preservó por completo, y pudo haber sufrido retrasos en su envío
a la base de datos, pero no se perdió ninguna telemetría. Las protecciones de los agentes en los endpoints no se vieron
afectadas en absoluto, funcionando con normalidad, ya que ningún análisis o protección depende de la conexión de red con
ninguna API externa. En este momento, toda la telemetría se ha “puesto al día” en el panel de control.

Resolución

Cyber Crucible creó múltiples servidores dentro y fuera de AWS. La estabilidad de la red dentro de AWS parece haber mejorado durante la noche (7MAR2024), observándose mejoras ya desde las 0200 UTC. Cyber Crucible está operando actualmente al 500% de la capacidad de los servidores, calculado en función del
ancho de banda de tráfico máximo, el cual ha disminuido. El equipo ha estado reemplazando los servidores alojados en AWS a medida que estos pierden conectividad de red.

Para ser claros, el escalado adicional de servidores no fue una solución eficaz en este caso. Cyber Crucible ha comenzado la transición para dejar de utilizar AWS como único proveedor de alojamiento en la nube.
El trabajo para lograr independencia de plataforma en la nube ya llevaba meses en curso, con planes iniciales
de dejar de depender exclusivamente de AWS en el segundo trimestre de 2024. Las pruebas de extremo a extremo, incluidos todos los

esquemas necesarios de doble cifrado y autenticación x509 para nuestros diversos servidores y servicios, se completaron a finales de febrero de 2024. Los problemas de red que experimentamos con AWS han acelerado la transición, originalmente planificada para el segundo trimestre, adelantándola un mes
respecto al cronograma.

Revision #1
Created 2026-07-24 01:38:35 UTC by Dennis Underwood
Updated 2026-07-24 01:38:35 UTC by Dennis Underwood