

06 de março de 2024

Resumo do Problema

Uma interrupção de rede ocorrida em 06/03/2024 afetou o acesso front-end ao painel do Cyber Crucible e o acesso à telemetria via API. Este problema foi resolvido em 07/03/2024.

Causa Raiz

Às 04h00 UTC de 06/03/2024, o tráfego de telemetria começou a aumentar até atingir eventualmente 1600% do tráfego normal de agentes. Além disso, a largura de banda da rede entre as instâncias da AWS começou a ser limitada a velocidades reduzidas entre os balanceadores de carga, servidores e bancos de dados hospedados na AWS. Em múltiplas zonas, as restrições de largura de banda foram variáveis e variaram de perda total de transmissão (0% da capacidade) a 50% da capacidade. A disponibilidade do DNS da AWS também foi comprometida. Confirmou-se que o tráfego de rede recebido pelo Cyber Crucible era tráfego válido de agentes de clientes existentes. O tráfego de bots para os balanceadores de carga não aumentou em volume. A largura de banda adicional não foi o principal fator para a indisponibilidade dos servidores, mas agravou os problemas de largura de banda do middleware e do banco de dados. O pico no tráfego de agentes durante esse período diminuiu parcialmente. Neste momento, o Cyber Crucible não observa nenhuma correlação entre as interrupções de nuvem divulgadas em 06/03/2024 e os problemas da AWS ou o pico de tráfego.

Impacto

O acesso ao painel e às APIs do Cyber Crucible pode ter sido atrasado ou indisponível. A telemetria dos agentes instalados foi totalmente preservada, podendo ter havido atraso no envio ao banco de dados, mas nenhuma telemetria foi perdida. As proteções dos endpoints dos agentes permaneceram completamente inalteradas, funcionando normalmente, pois nenhuma análise ou proteção depende de conexão de rede com quaisquer APIs upstream. Neste momento, toda a telemetria já foi atualizada no painel.

Resolução

O Cyber Crucible criou múltiplos servidores dentro e fora da AWS. A estabilidade da rede dentro da AWS parece ter melhorado durante a noite (07/03/2024), com melhorias observadas já a partir das 02h00 UTC. O Cyber Crucible está atualmente operando a 500% da capacidade dos servidores, calculada com base na largura de banda de tráfego de pico, que já diminuiu. A equipe tem substituído os servidores hospedados na AWS à medida que perdem a conectividade de rede.

Para deixar claro, o aumento adicional de escala dos servidores não foi uma resolução eficaz nesta questão.

O Cyber Crucible começou a transição do uso da AWS como único provedor de hospedagem em nuvem. O trabalho para viabilizar a agnosticismo em relação à plataforma de nuvem já vinha sendo desenvolvido há meses, com planos iniciais de deixar de usar a AWS como único provedor no segundo trimestre de 2024. Os testes de ponta a ponta, incluindo todos os

esquemas necessários de dupla criptografia e autenticação x509 para nossos diversos servidores e serviços, foram concluídos no final de fevereiro de 2024. Os problemas de rede que enfrentamos com a AWS aceleraram a transição, originalmente planejada para o segundo trimestre, fazendo-a começar um mês antes do previsto.

Revision #1

Created 2026-07-24 05:36:39 UTC by Dennis Underwood

Updated 2026-07-24 05:36:39 UTC by Dennis Underwood