

Maintenance Notifications

- [06 March, 2024](#)

06 March, 2024

Issue Summary

A network outage occurring on 6MAR2024 impacted front-end access to the Cyber Crucible dashboard and telemetry access via API. This issue has since been resolved as of 7MAR2024.

Root Cause

At 0400 UTC on 6MAR2024, telemetry traffic began escalating to an eventual 1600% of normal agent traffic. Additionally, the network bandwidth between AWS instances began to throttle to limited speeds between the AWS-hosted load balancers, servers, and databases. Across multiple zones, bandwidth constraints were variable and ranged from complete transmission loss (0% of capacity) to 50% of capacity. AWS DNS availability was also compromised. Network traffic inbound to Cyber Crucible was confirmed to be valid agent traffic from existing customers. Bot traffic to load balancers did not increase in volume. The additional bandwidth was not the primary driver for server unavailability, but exacerbated the middleware and database bandwidth issues. The spike in agent traffic during that time has partially subsided. At this time, Cyber Crucible communicates no correlation between published cloud outages on 6MAR2024 to the AWS issues or the spike in traffic.

Impact

Access to the Cyber Crucible dashboard and APIs would have been delayed or unavailable. Telemetry from installed agents was fully preserved, and may have been delayed in submission to the database, but no telemetry was lost. Agent endpoint protections were completely unaffected, functioning as normal, as no analysis or protections rely on network connection to any upstream APIs. At this time all telemetry has “caught up” in the dashboard.

Resolution

Cyber Crucible created multiple servers inside and outside of AWS. Network stability inside of AWS seems to have improved overnight (7MAR2024), with improvements observed as early as 0200 UTC. Cyber Crucible is currently operating at 500% server capacity, calculated based on the peak traffic bandwidth which has subsided. The team has been replacing AWS hosted servers as they lose network connectivity.

To be clear, additional server scaling was not an effective resolution in this matter.

Cyber Crucible has begun to transition from using AWS as a sole cloud hosting provider. Work to support being cloud-platform agnostic has already been in progress for months, with initial plans to move from AWS as a sole provider in Q2 of 2024. End to end testing, including all

necessary double-encryption and x509 authentication schemes for our various servers and services, was completed at the end of February 2024. The network issues that we experienced with AWS have accelerated the move, originally planned for Q2, to begin a month ahead of schedule.