NOTE: TLDR summary toward the bottom.

Thank you for your continued communications on this front and we sincerely apologize for the frustration this has caused. I assure you, from the moment it was escalated, we have had an all-hands-on-deck approach to try and uncover the root-cause of these instances.

The original plan/idea (based on what we saw at the time as the only approach) was to move some districts to a different cluster. Although this was doable - albeit time consuming and extremely delicate - we weren't 100% confident this would have solved the issues Ohio was experiencing. The reason for the uncertainty was based on the simple fact that traffic patterns and spikes typically associated with an 'outage' weren't there, and we wanted to have 100% certainty our next steps would provide you the enjoyable and effortless Securly experience we all want your end-users to have. With that said, our DevOps Team dedicated the majority of their time the past few weeks scrubbing through all traffic patterns and various clusters to determine the underlying source for the disruptions. I will summarize their findings and fixes below.

2 Sections/Explanations:
– The first section of bullet points are dedicated to the weekly outages you were seeing the first part of this year: 2022
– The second section is dedicated to a root cause of less frequent/predictable disruptions you saw in November 2021, January 2022, and the first week of March 2022.

Section 1:

- **Database(s):** DB4 and DB0. When Support gets an IP to register, they are added to both databases. DB4 is a list of all IPs associated with a particular School Domain (aka FID). DB0 are the individual IPs stored in the system with each individual IP having an FID associated with it. All of your IP addresses have been cross-referenced and added to the DB in the event any were missing - but I do not believe there were any missing IP's.
- **TTL (time to live) Root Issue:** We created a setting for IP addresses coming from Securly Home users to expire every week regardless of login attempts. This prevented registering IP's from various locations a student - or parent - may log in from (Starbucks, for example) to become a fixed IP in our database (DB4 and DB0 for future reference). This setting carried over to districts specific to the cluster a lot of your end-users are assigned to.
- **TTL Fix:** Our DevOps/Engineer Team has since updated the TTL to 90 days as opposed to a week. This will essentially allow for a 'forever' status based solely on the fact that it will 'refresh the clock' (so to speak) once a login from *any* user is done from that particular IP address. The only time this would be an issue, or cause disruption, is if there are absolutely zero attempts to log in from an IP address outside of the 90 day window.

- **Action Items moving forward:** The only items needed is to ensure all new IP addresses you gain are communicated to Support, via a support ticket, so we can register them appropriately. Much like we do with Securly Home users, we will still recognize a new IP address, this action item is more-so for additional peace of mind and an added layer of communication.

Section 2:

- We saw intermittent problems primarily related to Google search. We have data from our Site Reliability Engineer (SRE) system that logs problematic scenarios with squid servers. SRE tests each component, every second, on every cluster and reports errors/failures back to us so we can see if the clusters are working as expected. With that said, internally, we were not able to reproduce any disruptions, but we continued to dig and that ultimately led to a couple of changes:
    - We recognized one action-item we could do to help would be to revert any experimental technology (product releases) on the Ohio/US-East2 cluster. This allows additional time to vet recent product releases prior to applying them to your cluster.
    - Based on the correlation of time-stamps from when we started noticing disruptions, we also reverted the Redis Auto Scaling Group (ASG) technology we have been using on the cluster since November. We believe that may have had a bad interaction with some recent releases.

Since those updates/fixes, things are running better than ever in Ohio but we are continuing to investigate reports from our DB and traffic patterns.

TLDR:

- There was a week-long TTL for all IP addresses that would reset and prompt a new login from the end-user. This caused disruptions and it is why you noticed this as a weekly occurrence. The TTL is now permanent and all IP addresses are also permanent so you will not see the disruption occur moving forward.
- We saw a correlation between the time disruptions occurred and the time we placed Redis on our Ohio (US-E2) ASG so we have removed that.

I hope this recap gives you the confidence you need moving forward. We are happy to continue serving your districts in a way geared toward gaining yours - and your district's - trust in the solutions we provide.