Education Sector Case Study

Solving the Password Problem in Education

Credential attacks continue to impact the education sector. As a result of the growing threat, one of the world's leading private research universities based in California turned to Enzoic to shore up its defenses and eliminate the use of compromised credentials. It found that our modern, easy-to-use solution kept exposed passwords out and seamlessly integrated with its authentication systems.

EDUCATION SECTOR

The education sector is a prime target for credential attacks due to password reuse. So, we sat down with one of our California-based higher education customers to discuss how Enzoic has helped mitigate the risks from exposed passwords.

TELL US MORE ABOUT YOUR SITUATION?

Higher education is similar to a decentralized company with many different populations and diverse needs. Our community spans students straight from high school to alumni that graduated decades ago spread across the globe. As a result, passwords remain an effective and affordable authentication solution. However, to keep our systems secure we determined we needed a way to prevent the use of compromised credentials.

Our in-house Cyber Threat Intelligence (CTI) team helped validate the magnitude of the password problem by showing the tactics, techniques, and procedures bad actors were actually using to target the university every day. Insights from the team highlighted that compromised credentials were a consistent vector hackers were exploiting and previously exposed passwords from major breaches were active in our environment.

CAN YOU TELL US MORE ABOUT THE EVALUATION PROCESS AND WHY YOU CHOSE ENZOIC?

We wanted a very secure and easy to use solution to detect when university passwords were exposed. We did a thorough examination of Enzoic’s data and found they had more recent credentials from data breaches than others.

Another critical requirement was keeping third parties involved with the solution at arm's length due to the risk of supply chain attacks, as the SolarWinds attack highlighted! Our evaluation involved a review of the Enzoic's SDK code we’d be using. We were pleased that it was open source. We also liked their password hash comparison method. Unlike others, theirs used a single-blind approach. All of these factors made Enzoic the perfect choice.

CAN YOU DESCRIBE SOME OF THE WAYS THE SOLUTION IS BEING USED?

We recently introduced a single sign-on (SSO) system with ForgeRock.Given our CTI team's findings around credential attacks, it was vital that we add password screening.

We also integrated Enzoic with our emergency shutdown process called the Big Red Button. The intelligence from Enzoic notifies us if a password is compromised. This allows us to immediately shut down the account, scramble the password and disconnect all active sessions. It was a game-changer for our cyber teams to have that feature available.

HOW MUCH TRAINING WAS REQUIRED TO GET YOUR TEAMS UP TO SPEED?

The solution is easy for everyone involved and minimal time was required to train our helpdesk teams. From a technical perspective, the APIs are straightforward and, coupled with the excellent documentation, it was a pain free process.

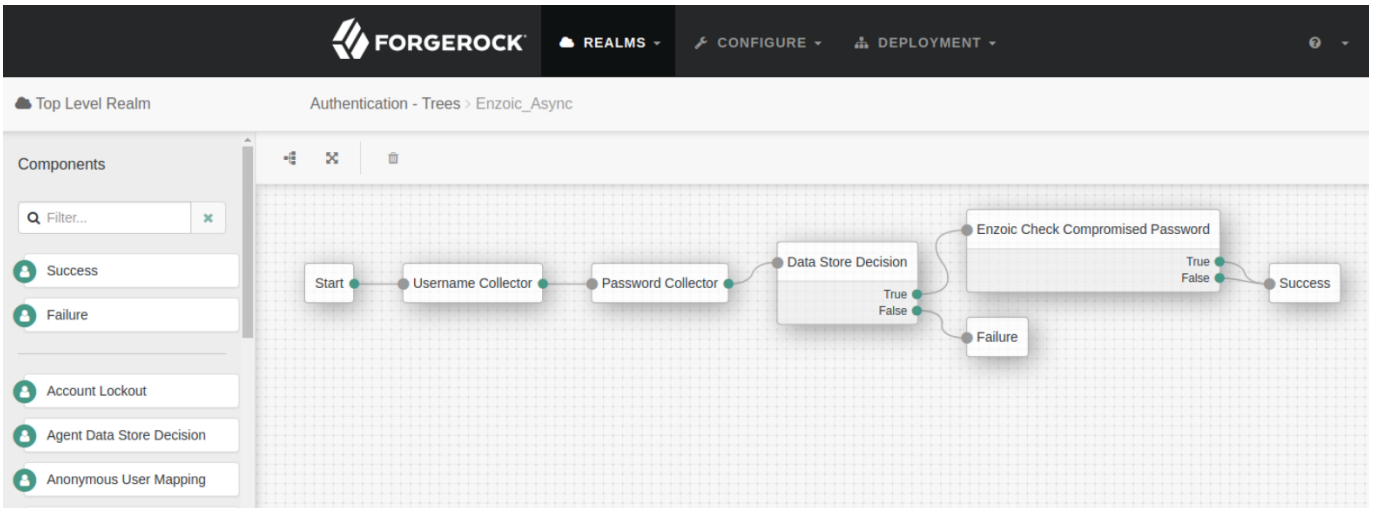
WHAT ARE YOUR FUTURE PLANS?

We want to focus our limited cybersecurity resources in the right places. We know that's on people and behaviors - and that means passwords. Our plan is to roll out the SSO solution from ForgeRock across the entire university ecosystem. This will allow us to get Enzoic's password screening to the largest number of departments with the least friction.

HOW WOULD YOU SUMMARIZE THE ENZOIC SOLUTION IN UNDER 30 SECONDS?

Protecting against password attacks is essential to the safety of our university. Enzoic makes that simple. It's an excellent service that's saved our butts quite a bit!

Configuration of Enzoic-Sync Auth Tree depicted below:



The Enzoic Sync Auth Tree will check if the password is compromised using the Enzoic API. This tree then waits for a response from Enzoic before proceeding. If the password is compromised, the user will not able to login.