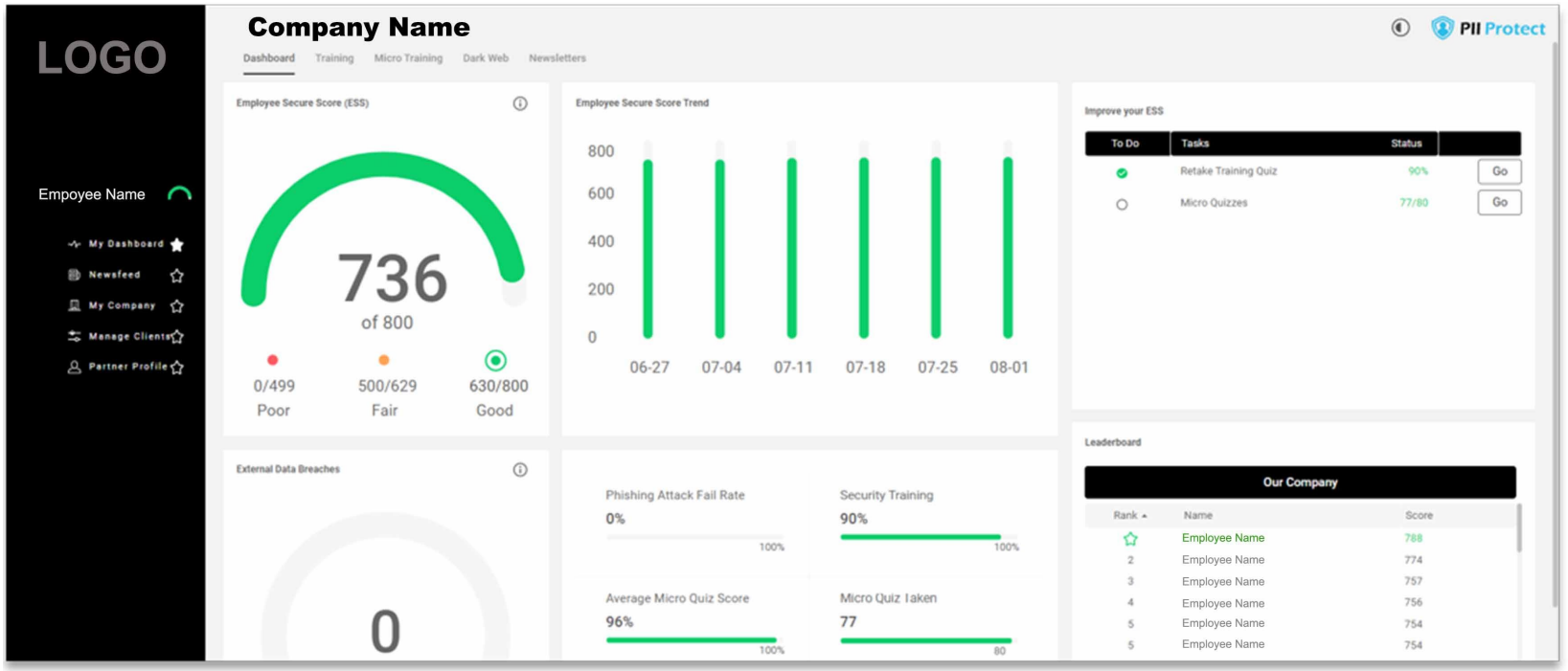
Numata Cyber 365

The Numata Cyber 356 offering is layered with many features and benefits, aiming to **equip** and **empower** your employees and holistically strengthen the cybersecurity posture within your organisation. We pride ourselves on our relentless drive to continuously improve our offering on a regular basis to ensure we deliver tangible value to our clients.

Features and Benefits

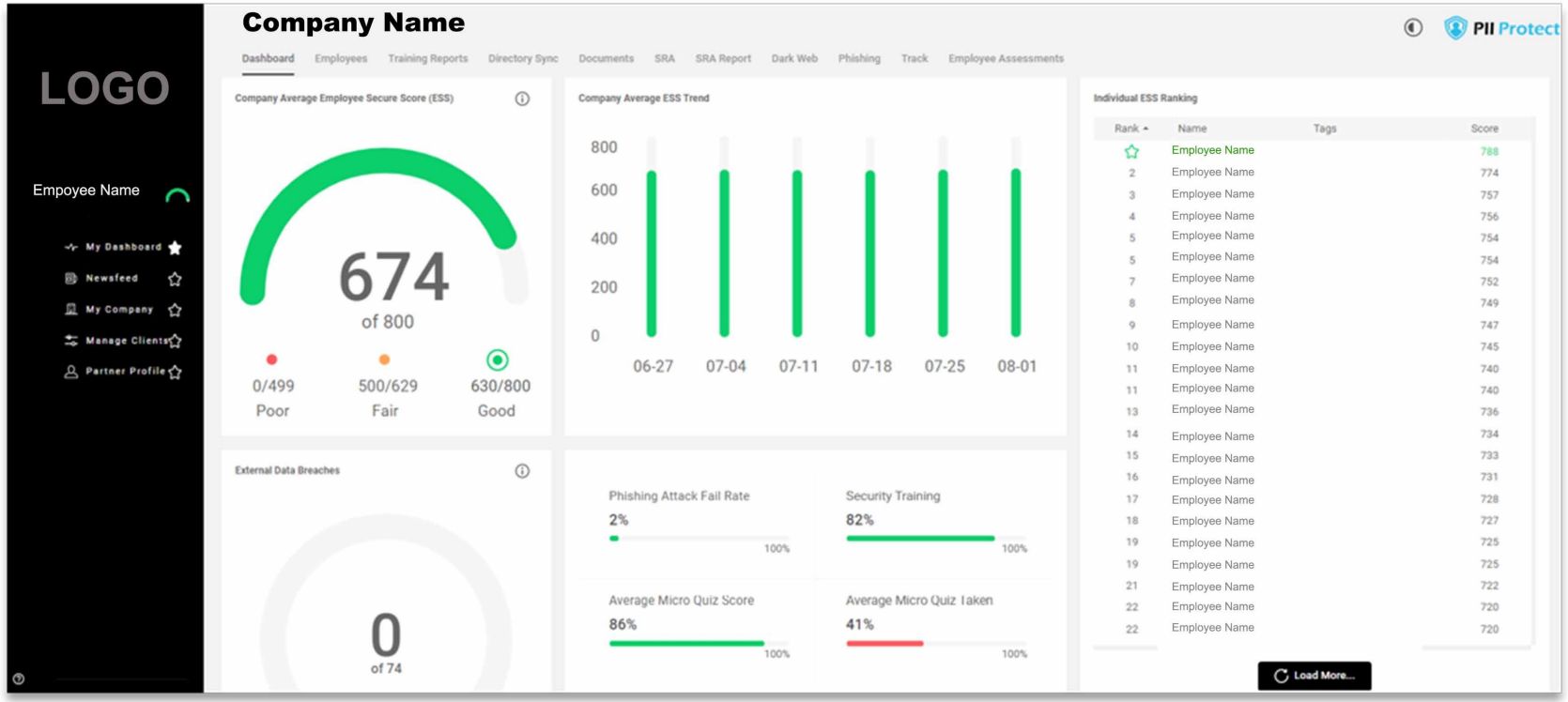
Personal Dashboard

Each employee will receive their own personal dashboard, giving them a virtual perspective of their cybersecurity posture. On this dashboard they have visibility into the organization's cybersecurity leader board, their personal micro training courses, their score for the annual training and their phishing fail rate percentage. Included on this dashboard is access to annual training, micro training, policies (including policy acknowledgement), and the Dark Web scan.



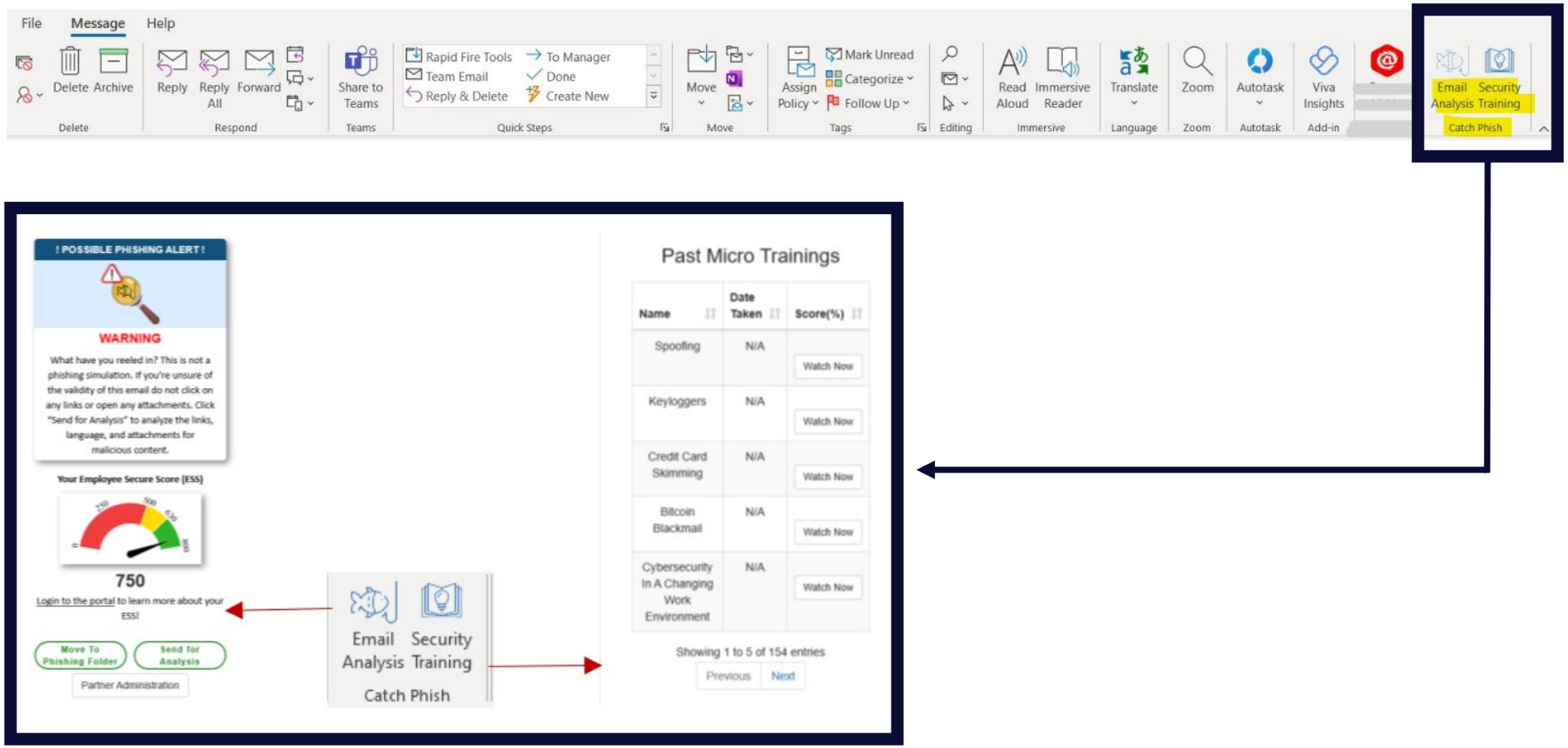
Company Dashboard

Your Cybersecurity Managers will have easy access to reports that give visibility into each employee's cyber posture through the company dashboard. This dashboard allows for identifying employee security risks at a glace or at a deeper level e.g. employees ESS, last logins, data breaches, policy acknowledgement, phishing fail rates.



On-Demand Email Educational tool

Our catch phish email educational tool gives you around-the-clock access to catch phishing or spam emails right inside your Outlook email application. This educational tool will assist employees in assessing the danger of the sender, links, attachments, and message of an email. In addition to educating users, the tool also rewards your employees when they do reel in one of our phishing tests, adding bonus points to their overall risk profile.



Annual Security Awareness training

We have a comprehensive online annual cybersecurity training course, that is updated each year, which consists of global cybersecurity best practices when it comes to protecting your organisation. The training is divided into 5 crucial cybersecurity topics, followed by a 20-question quiz. This annual training will take employees approximately 35min to complete, whereafter, on successful completion, the employee will receive a digital certificate.

Continuous Micro Cybersecurity Awareness Training

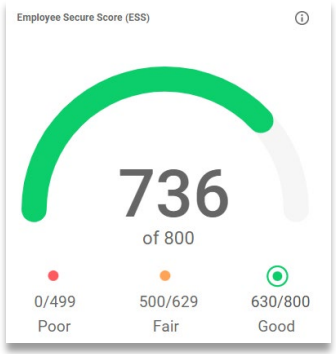
We believe that continuous, bite-sized, colorful training on cybersecurity positively impacts the awareness within the organisation. That is why we have micro training course that get sent out on a weekly basis. These 2-minute-long videos, followed by a 4-question quiz, are not only brimming with best practices within an organisation, but with helpful tips for your personal life too.

Newsfeed

The newsfeed is a resource center built directly into the portal that will serve as a communication tool to post additional training content like infographics, important scam alerts, announcements and more.

Employee Secure Score

Employee Secure Score (ESS) factors in the employee's annual training score, participation in micro trainings, simulated phishing fail rate, and external data breaches linked to their email address. The ESS metric is designed to determine cybersecurity risks on an individual level to quickly identify threats and track program improvement at a glance.



Monthly Security Newsletters

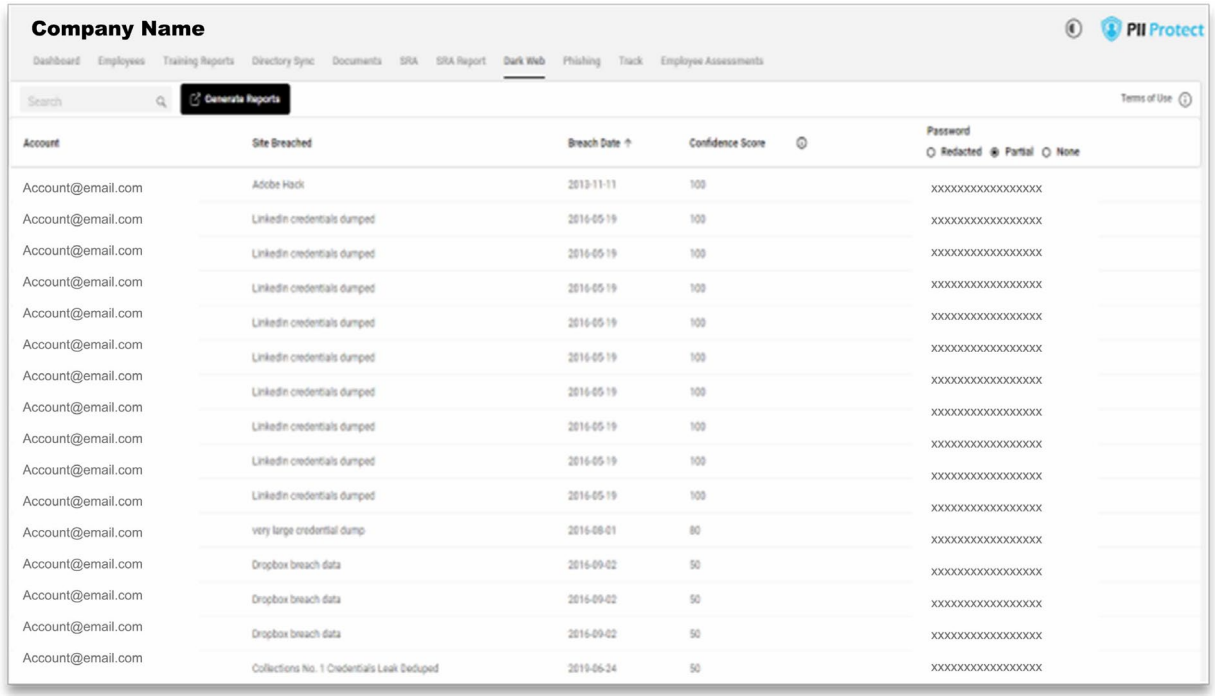
In the last week of every month, all your employees will be sent a personalised email with an update on their ESS, a closer look at their cybersecurity posture and a security newsletter.

Customer Success Coordinator

Your Cybersecurity Managers will have a dedicated Customer Success Coordinator (CSC) that will assist with the program rollout. The CSC will provide support to ensure a successful program throughout the organisation. Once you are live on the portal, your CSC will set up a x1 managers dashboard walkthrough meeting and x2 health check-in meetings 4-6 weeks apart.

Dark Web

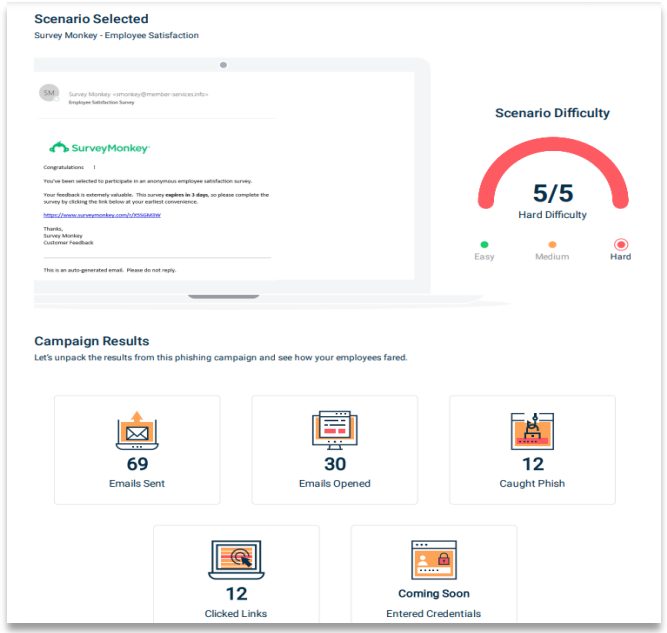
Numata performs 24/7 dark web monitoring for up to 3 email domains. All data, new and old, found on the Dark Web can be used maliciously by cybercriminals. Exposed passwords can provide keys to various sites and services if still in use. Email addresses found can be used for direct phishing campaigns and personal data can be used to build advanced social engineering attacks. In addition to the ongoing monitoring, Numata offers a monthly report that provides an overview of global data breaches for the month and insight into breaches connected to your email domains.



Bi-Monthly Phishing Simulations

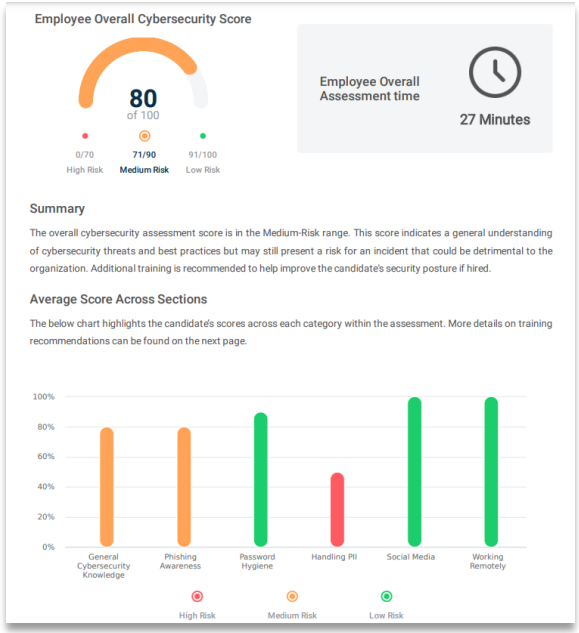
All employees will receive bi-monthly phishing simulations. Sending employees fake phishing emails, known as phishing simulations, is a great way to test their ability in identifying potentially malicious messages on an ongoing basis.

Cybercriminals are continuously improving their phishing techniques, making it difficult for technical safeguards like spam filters to identify them and keep them out of your employees' inboxes. That means employees are on the front lines to protect your network and should be trained on how to identify a phishing email – what better way than a "safe" attack to keep employees alert!



Employee Assessments

You will have access to employee assessments that can be used to help you identify security gaps in your human layer of defence, through a quick questionnaire. We have a *baseline employee cybersecurity assessment* and a *pre-employment cybersecurity assessment* to assist in identifying potential risk during the recruitment process.



Reports
Tagged internal cybersecurity managers will have access to various reports. These reports are great for evaluation metrics during quarterly reviews. You can download annual training reports, micro training reports, an ESS report, a dark web scan, a phishing simulation report and employee assessment reports.

Written Security Policies and Policy Acknowledgement Feature
We have a variety of security policy templates that are available for you to mould according to your business environment. Your cybersecurity awareness training portal has a convenient location for you to upload all of your policies.

Security Incident Tracking and Logging feature
You will also have a convenient location to log and keep track of all security incidents. This includes a date of the incident, description, number of records, source, cause, assets involved, systems involved, impact level and resolution details. Security incidents can range from a laptop being stolen, to a company data breach through a phishing email.

Monthly Executive Report
At the beginning of each month, your CSC will send your tagged managers the “Company ESS Report”. This report will highlight your high-risk employees at a glance. Your CSC will also give any feedback and updates with regards to the cybersecurity posture of our organisation within this reporting.