PhishRod
Fortify First Line of Defence

Case Study

Enhancing Cybersecurity Resilience

with Automated Defense Against Phishing

Problem Statement

For an organization that is one of the largest oil & gas giants of Texas, a market leader, and employs 70,000+ employees, it became increasingly difficult to protect their workforce from rising cyberattacks. Phishing attempts and other cyberattacks started disrupting their operations, so a need for an efficient and swift phishing defense mechanism arose.

Solution

To facilitate the organization in thwarting incoming phishing attacks, PhishRod deployed an automated phishing defense mechanism to highlight, quarantine, and delete suspicious emails.

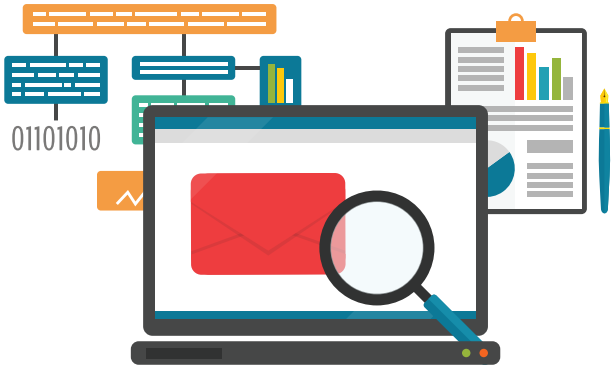
Reporter Plug-In

PhishRod's reporter plug-in was installed throughout the organization, which allowed to automatically scan emails and send them to the quarantine folder if they appeared suspicious. This facilitated the identification of phishing emails before any malicious links were clicked.

However, users could also report any other email that could not automatically be quarantined. The entire concept is based on how end-users can be empowered to understand and detect phishing emails and report them before it's too late.

info@phishrod.co

How PhishScout Works



Once an email is reported, it goes through rigorous investigative steps to determine if it is legitimate or malicious. For PhishScout, verifying the suspiciousness of an email is a two-step process. First, the primary analyst determines whether the email is an actual phishing attempt or a false alarm. If the email does not clear the criteria, it is then forwarded to the secondary analysts who further analyze different dimensions of a suspicious email such as IP Reputation, Domain Reputation, URL Analysis, Payload Analysis, Site Verification, & Email Verification. Once the analyst has enough evidence, the email is either marked safe or deleted from all mailboxes, protecting the organization from any impending harm.

Result

The solution by PhishRod is a combination of human and machine intelligence that collectively thwarts phishing attacks. With the help of automatic detection, investigation, and remediation as required, the automated phishing response mechanism enabled the oil giant to report 1400 emails over a 6-month span, from which 60% were declared as suspicious and timely deleted.