Technical Testing – Managed Phishing and Security Awareness Training (Co-Managed)

Monthly phishing campaigns are run for Client based on Clients defined workflow, throughout the annual term. Security awareness training is provided prior to the phishing campaigns and supplemental training is provided to users who fail phishing campaign simulations. As well, Client will have co-managed access to perform ad-hoc phishing campaigns and administer ad-hoc security awareness training to their users

Support

- eSentire will provide onboarding, user level, administer level guides supporting the Clients usage of the SaaS platform. Support is available during normal business hours (EST).

Reporting/Dashboards:

- Awareness and Education
- Exposures
- Course Completion Summaries
- NIST CSF Alignment
- Onboarding Summary
- Phishclick Analysis
- Phishforward Report
- Phishforward Summary
- Outdated Browser Summary
- Security Dissonance Summary
- Survey Results Summary
- Technology Summary
- Top Division Risk Summary
- Top User Risk Summary
- Security News Bulletin
- Phishing simulation Report
- Data Captured Phish Report

Responsibilities

- eSentire will provide 12 phishing campaigns per year (one campaign per month):
  - Each phishing campaign will be selected from the phishing campaign templates library
  - Each phishing campaign will be sent out every 30 days from the initial campaign or on custom workflow agreed upon by Client and the MRS team.
- eSentire will also provide general security awareness training through the online Learning Management System (LMS).

- eSentire's online Learning Management System (LMS) will provide targeted security training for users who fail phishing campaigns
- Client may request on a quarterly basis, a one hour review of the findings of the campaigns with an eSentire Information Security Consultant
- Client must use Two-Factor Authentication (2FA)

Exclusions

- Client may not adjust frequency of delivery
- eSentire reserves the right to limit support effort as required