Synoptek

Security Testing and Training

Service Definition

Table of Contents

1 INTRODUCTION

This Service Definition is subject to all terms and conditions of the Service Order to which it was attached. This Service Definition describes and contains additional terms that apply to Synoptek's Security Testing and Training (the "Service").

The service definitions found herein reflect Synoptek's standards at the time the Service Order(s) was issued. Synoptek reserves the right to change any particular standard herein to reflect the current Synoptek best practices or industry standards at its sole discretion with or without notice.

2 SERVICE OFFERING

Synoptek's Security Testing and Training is designed to reduce your exposure and shrink your organization's attack surface. Our Security Testing and Training provides you with a comprehensive approach that integrates baseline testing using mock attacks, engaging interactive web-based training, and continuous assessment through simulated phishing attacks to build a more resilient and secure organization. Our security personnel will continue to advise on ever changing threats and recommended actions.

Synoptek's Security Testing and Training establishes a phish-prone baseline of your employees, delivers an engaging On-Demand training experience with interactivity and provides actionable analysis to help you and your organization improve your resiliency towards social engineering attacks.

Key Features and Benefits:

- User Security Training
- Supports Compliance
- Simulated Phishing Attacks
- Automated Re-Phishing
- Quarterly Tests and Reports
- Quick Deployment
- Random Attack Delivery
- Improved Security Behavior

3 SOLUTION PURPOSE

Your employees are frequently exposed to sophisticated social engineering attacks. Synoptek's Security Testing and Training aims to train your employees and help them keep information security top of mind, strengthening this critical link in your organization's IT Security chain.

4 HOW IT WORKS

Traditional Security Testing and Training programs can prove challenging or ineffective for most organizations. Organizations simply just do not have the resources, time or ability to support to drive a successful campaign that engages and trains the end user. Synoptek's Security Testing and Training takes a completely new approach to user

engagement and training. Synoptek leverages a world-class platform that integrates simulated phishing and on-demand training. Phase one of your campaign begins with a baseline test to collect the phish-prone percentage of your users. In Phase two, your campaign steps users through effective, interactive on-demand browser-based training and USB drive testing is instantiated. Phase three and four of your campaign sees a new wave of simulated phishing attacks to your organization to reinforce your employee's training. The result, is a robust solution that increases your end user's resiliency towards social engineering. Each Phase lasts approximately three months.

5 WHAT'S INCLUDED

Your subscription to Synoptek's Security Testing and Training includes the following:

1. **Baseline Testing.** Using an initial phish campaign, Synoptek will establish a baseline percentage of users who fall victim within your organization.
2. **User Training.** Synoptek will provide On-Demand, interactive, engaging training with common traps, demonstrations and new scenario-based 'Danger Zone' exercises. Training Modules include:
    a. Security Awareness Training
    b. Basic Security Testing and Training Course
    c. Ransomware
    d. Ransomware for Hospitals
    e. Strong Passwords
    f. Handling Sensitive Information Securely
    g. Mobile Device Security
    h. Basics of Credit Card Security
    i. PCI Compliance Simplified
    j. Financial Institution Physical Security
    k. GLBA Compliance Course
3. **Phish Your Users.** Simulated phishing attacks leveraging highly realistic phishing messages, delivered over time, throughout the campaign. Each employee receives a different phishing email at a different time. Some Phishing Email topics include:
    a. **Banking**
    b. **Social Networking**
    c. **IT**
    d. **Government**
    e. **Human Resources**
    f. **Seasonal**
    g. **Current Events**
    h. **Brand Knock-Offs**
    i. **General Phishing for Sensitive Information**
    j. **Many Others!**

4. **Monthly Campaigns, Quarterly Results.** Enterprise-strength reporting, showing stats and graphs for phishing failures, USB failures and training. Users are phished once per month at a minimum; results are aggregated into a quarterly report.
5. **Continuous Improvement.** At a minimum, users will be phished once per month with both training and re-phishing provided to users that fail the initial phish. This monthly phishing and training are intended to keep your employees sharp and up to date with the latest threats.
6. **USB Drive Test.** You will be shipped five (5) USB thumb drives (styles may vary) for the second phase after service is established and annually thereafter at the beginning of each subsequent calendar year. Each of these drives will contain a 'beaconized' Microsoft Office file. Once executed, this file will report a failure and include any available details such as the username and geo-location. You are encouraged to place these drives on-site in high traffic areas.
    a. Test cycles end in Q4 of the given year and renew in Q1 of the following calendar year;
    b. USB Drive test cycles occur once per year;
    c. In the first quarter of each new year, Synoptek will deliver new drives;
    d. In addition to the annual USB drive test – Synoptek will deliver an initial batch of 5 drives at the beginning of service to establish a USB-test-drive baseline;
    e. Reporting is included at the end of each phase

6 SERVICE LIMITATIONS

Synoptek's Security Testing and Training is an excellent addition to an organization's strategy of defense in depth. Synoptek's Security Testing and Training is not a comprehensive solution for preventing all threats, attacks or variations of malware that may be leveraged against your organization. As a result, it should be expected that this service alone cannot guarantee that your end users will be able to detect or prevent *all* threats or other social engineering attacks and is best used in conjunction with other security tools and resources.

Synoptek will, upon campaign refresh (once quarterly), automatically pull down your users from Active Directory and insert their information into the tool in order to capture all of your current users for the new phishing campaign. The seats you are contracted to pay for may increase or decrease, dependent upon the number of users that we pull into the tool through this method.

7 EMAIL WHITELISTING

To properly facilitate Phishing Campaigns and subsequent Training Notifications, a pre-defined group of IP addresses or Domains must be whitelisted. Where Synoptek is responsible for the IT infrastructure of a client's organization, pre-authorization to whitelist this pre-defined group is granted. For infrastructure not under the Synoptek umbrella, Synoptek will coordinate with your team to perform the whitelisting before the campaigns can begin. This ensures that your anti-spam filters do not block the various components of the campaign.

8 Appendix A

Sample Phased Deployment of Synoptek's Security Testing and Training: