Phishing Awareness Assessment

Solution Brief

Challenges

The ever-present phishing threat continues to be a major breach entry point, even with significant investments in email security. Employees are the first line of defense against such attacks, making it crucial to regularly test their alertness and awareness of emerging phishing techniques through efficient pre-emptive measures.

However, running phishing awareness campaigns is resource intensive, requiring creating production-safe inactive payloads to gauge the potential reach of successfully luring an employee, tracking phishing email success rates and attribution, and crafting a variety of high-quality, well-designed phishing emails and, when necessary, fake landing pages.

Due to limited resources, many organizations opt to rely on annual phishing awareness training instead of addressing these challenges head-on.

Overview

Cymulate's Phishing Awareness campaigns evaluate employees' security awareness levels by simulating phishing attacks and identifying potential target opportunities.

Creating a customized assessment with the phishing simulation module user-friendly drag-and-drop menu is quick and easy. Options include the selection of email text, attachments with production-safe payloads, fake landing pages, and more.

Employees' interactions with the mock phishing emails are automatically recorded, logging hazardous behaviors such as clicking links or entering credentials. This identifies employees in need of additional phishing awareness training.

Benefits

- Customization wizard
- Scalable
- Repeatable
- Schedulable
- Automated report generation

Phishing Awareness with Cymulate

Main Features

Drag-and-Drop phishing element repository
With customizable hundreds email templates, landing pages, and office templates to create attack phishing awareness campaigns.

Automated phishing campaign simulations
With real production-safe payload, links to fake malicious websites identify employees who need additional phishing awareness training.

Automatically generated reports
Including every action taken by employees interacting with the campaign email phish.

Case Studies and Customer Success Stories

Persistent Systems

A digital engineering and enterprise modernization partner, with over 22,000 employees located across 18 countries.

Use Case- Red team automation and customization

Persistent red team uses Advanced Scenarios to automate their assessments, as well as scale their adversarial activities with pro-active threat hunting and health checks. Most recently, the team used this module to test a golden ticket attack. Any gaps that are found during these assessments are automatically documented in a mitigation report so they can be remediated immediately, before an attacker can exploit them.

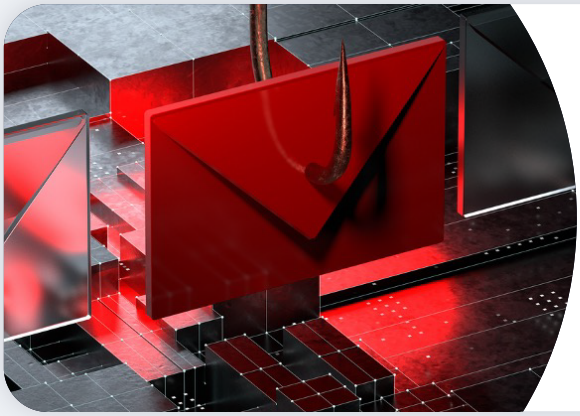
Read more

“Working with Cymulate is like having a complete red team on board — without the added expense.”

Mor Asher, Infosec Manager, Telit (Global leader in Internet of Things)

Read more

Additional Resources



Cymulate

Blog Post -The GoDaddy Phishing Awareness Test

Read more

Backed by the Industry

Awards and Accolades

About Cymulate

Cymulate provides organizations with comprehensive security control validation and in-depth insights into breach feasibility. This modular solution addresses a wide variety of business and technical use cases and scales from out-of-the-box simulations to full customization for advanced attack simulations. With Cymulate, companies assess, optimize, rationalize, and prove their security program with minimal resource investment. Security professionals and business stakeholders leverage these insights to reduce cyber risk, justify investments, provide proof of security resilience to executive leadership, and gain evidence for compliance and regulatory purposes.

Contact us for a live demo, or get started with a free trial

Start Your Free Trial

info@cymulate.com | www.cymulate.com