Evaluation of Simulated Phishing Platform for Oscorp

Executive Summary

Human behavior remains one of the most significant risk factors in an organization's security posture. While technical controls continue to improve, attackers consistently exploit human trust, curiosity, and lack of awareness. Simulated phishing campaigns can be an effective tool to address this risk, but they should be part of a broader, continuous security awareness strategy rather than a standalone solution.

Current State at Oscorp

Oscorp currently relies on a single, static security training module that employees complete upon onboarding. This module was introduced in 2013 and focuses on general security tips. While foundational training is valuable, a one-time module is no longer sufficient to address today's evolving threat landscape, particularly as phishing techniques have become more sophisticated and targeted.

Assessment of Simulated Phishing

Simulated phishing campaigns are an effective method for reinforcing employee awareness by providing real-world, hands-on learning experiences. These simulations help employees recognize how easily phishing attempts can bypass technical defenses and exploit human judgment.

Running simulated phishing exercises on a recurring basis (every 6–12 months) can:

- Reinforce recognition of phishing tactics
- Normalize reporting suspicious emails
- Provide measurable data on employee risk and improvement over time

However, simulated phishing alone does not fully address human risk and should be supplemented with additional engagement strategies.

Additional Recommended Security Awareness Measures

To maximize the return on investment and strengthen Oscorp's overall security posture, simulated phishing should be combined with complementary initiatives, such as:

- **Physical social engineering simulations** (e.g., leaving USB devices in common areas to assess employee behavior and reinforce device security awareness)
- **Visual reminders** around the workplace, including posters highlighting strong password practices and examples of phishing emails
- **In-person security awareness sessions**, such as informal lunch-and-learn discussions, to encourage open dialogue about security best practices, reporting procedures, and real-world examples

These approaches help reinforce security concepts through multiple learning methods, increasing retention and behavioral change.

Recommendation

Given Oscorp's current excess budget and the outdated nature of its existing security training, investing in a simulated phishing platform is recommended as part of a broader security awareness modernization effort. When combined with recurring training, visual reminders, and interactive engagement, simulated phishing can significantly reduce human-related security risk and improve Oscorp's overall security maturity.