Telos Ghost for Penetration Testing

Telos Ghost: The Perfect Cover for More Realistic Threat Testing.

Telos Ghost masks the presence of pen testers and network resources and misattributes the team's digital identities for a more realistic testing scenario.

Today's organizations are operating in an environment where security breaches have become the norm. The new realities of cyberattacks dictate that penetration testing is a must for most organizations and in some industries penetration-testing is required by law in order to meet security and compliance regulations.

The Challenge: Evolving Techniques of Cybercriminals.

According to recent statistics, 98% of all cyber-attacks rely on social engineering to manipulate users or employees into making security mistakes and divulge sensitive or confidential information. Many of the social engineering campaigns deployed by cybercriminals use techniques like IP obfuscation and misattribution to disguise their presence on a network and mask their true intentions as they transverse the organization's internal network, exfiltrating or encrypting data for ransom demands or other nefarious purposes. With cyberattacks becoming more common and bad actors utilizing more sophisticated techniques to accomplish their mission, penetration testing needs to evolve to include the technologies used by hackers in order to provide more realistic threat scenarios.

The Solution: More Realistic Threat Testing with Telos Ghost

Telos Ghost is a cloud-based obfuscation and non-attribution network that masks penetration testers' identities, misattributes their location, and hide their presence on network resources. With Telos Ghost, pen-testers have in their toolkit many of the same technologies deployed by hackers to infiltrate an organization's network and avoid detection. Telos Ghost's unique attributes can enhance penetration testing and elevate it to the next level to provide a more realistic recreation of actual attack scenarios thus enabling them to more accurately assess the organization's ability to defend against malicious threats.

Challenge

- 98% of cyberattacks rely on social engineering.
- Increasingly sophisticated attack tactics utilized by hackers.
- Creating testing scenarios representative of real-life attacks.

Solution

- Utilize the same technologies as hackers to generate as close to real-life scenarios as possible.
- Managed attribution to create convincing online persona to match the fraud scheme.
- Ability to hide critical resources from internet or potential hackers during pen-testing simulation.

Benefits

- Convincing phishing scenario for victims and creating scenarios as close to real-life as possible.
- Protection of critical servers and applications during testing.
- Accurate assessment of security team capabilities to defend against cyberattacks.

Telos Ghost provides the following features to help elevate penetration-testing to the next level:

Managed attribution. Enable pen-testers to shape personas to match the fraud scheme. Technical attribution lets you specify your location, swap end-point IP addresses, and change your point of presence on demand. Personal attribution establishes a convincing online persona and ensures all of your activities are consistent, making it more convincing for the victim and more difficult for the organization to detect. By recreating a scenario as close to real-life as possible, the response of the organization's security team is as close to a real security incident as possible.

Hide penetration testers to create a realistic attack scenario. If the penetration testers are simulating an attack on critical resources and need to hide their activities from the public internet, Telos Ghost makes the penetration team and their devices invisible to the security personnel of the targeted organization. Pen testers can work without fear of discovery.

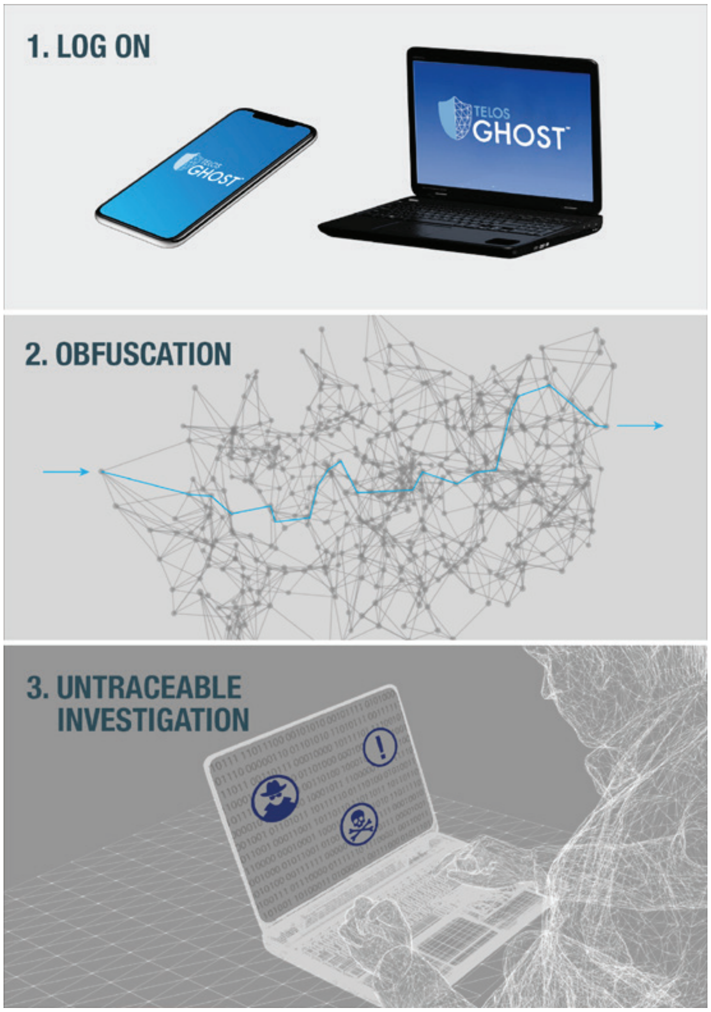
Virtual network. Spin up a pre-configured environment for testing purposes. Penetration testing may be performed in a production system or one which is set aside for testing. Using the Telos Ghost network, pen testers can spin up a virtual network with predefined configurations for simulated attacks.

As a software-defined network, Telos Ghost consists of virtual resources designed to work together, hosted in and dispersed across a variety of highly secure cloud regions. Telos Ghost supports the tools and techniques you use for accomplishing your cyber testing requirements.

Contact Telos for More Information

If you would like further information or a demonstration of the capabilities of Telos Ghost, please contact Telos Sales: 1-800-70-TELOS or sales@telos.com. We look forward to learning more about your requirements for anonymous networking and sharing how Telos Ghost can help protect your people and information

Learn more at www.telos.com/telos-ghost


1. LOG ON
TELOS GHOST
2. OBFUSCATION
3. UNTRACEABLE INVESTIGATION