How Globe Telecom Secures its Expanding Portfolio with Automated Security Validation

Highlight Achievements

- An internal SecOps team is able to test across Globe Telecom's many portfolio companies without the need for additional headcount
- Improved cyber readiness against ransomware variants with on-demand testing
- Achieved cost savings by consolidating automated pentesting and security validation into one solution

Background Information

Globe Telecom, Inc. is the leading telecommunications provider in the Philippines. The company operates one of the nation's largest wireless networks for voice and data, and maintains one of the most extensive broadband and fiber infrastructures in the region, serving millions of consumers and enterprises. In addition to the company's main telecommunications operations, Globe Telecom maintains numerous subsidiaries, each contributing to the group's complex digital infrastructure.

Globe Telecom's internal SOC is responsible for assessing and ensuring a strong security posture both within the parent organization as well as across the organization's subsidiaries. The Globe Telecom SOC is responsible for a wide variety of security functions, and is composed of specialized teams dedicated to Vulnerability Management, Threat Response, SOC Automation and Development, and internal red-teaming.

The Challenge: Struggling to test an extensive IT ecosystem of subsidiaries

As Globe Telecom's portfolio grew, the scope of work scaled significantly from supporting an IT ecosystem of a few subsidiaries to over a dozen. Although Globe Telecom maintains a robust internal SOC, the team recognized the limits of consistently increasing headcount to meet growing demands.

The Globe Telecom SOC had several solutions in place, already utilizing separate security tools for automated pentesting and vulnerability assessment. However, both presented operational limitations for their larger mission to secure both headquarters and the subsidiaries. The agent-based validation solution was limited to headquarter's assets where agents were deployed, and their automated pentesting solution had a locked IP range. While this ensured quality testing for Globe Telecom, it presented problems for testing across their expanded network.

Additionally, there were concerns of becoming collateral damage in the rise of ransomware campaigns amid the COVID-19 pandemic and the surge in Ransomware-as-a-Service (RaaS) amid worldwide geo-conflicts. This created an urgent need for a solution capable of validating organizational defenses against specific ransomware strains.

The Need: Robust Security Capabilities, Coupled with Platform Flexibility

Globe Telecom was searching for a comprehensive security validation and pentesting solution to augment the capabilities of their in-house red team. Specifically, the team needed a solution capable of proactively testing against specific ransomware variants, such as Conti, to validate that their perimeter security (EDR) configurations could effectively detect and prevent the threat. Additionally, the SOC team required a solution that provided the operational flexibility necessary to seamlessly test across their dynamic ecosystem of subsidiaries.

The Solution: Streamlined Operations Supported by Agentless and Flexible Automated Security Validation Platform

Operational Flexibility

Globe Telecom leverages Pentera's agentless, flexible platform to overcome operational challenges, allowing its internal red team to conduct unrestricted testing across all environments. With Pentera's adaptable IP configuration, IP range is no longer a limitation and the Globes Telecom SOC can effortlessly extend security validation across its constantly evolving network of portfolio companies. This has equipped their SOC with the agility and comprehensive scope necessary to strengthen their security posture.

Red Team Scalability

Globe Telecom utilizes Pentera as a central tool to extend the capabilities of its internal red team across its network of subsidiary companies. Garrett Silao, VP of Globe Telecom's Security Operations Center, emphasized that:

> **Pentera streamlines and accelerates our testing process by eliminating the need for manual attack simulation and simplifying the setup of custom attack paths. Its attack engine enhances our red team capabilities, allowing us to test a broader range of TTPs and vulnerabilities efficiently. Beyond its operational benefits, Pentera also serves as a valuable educational resource, helping my team develop deeper penetration testing and red team expertise.**

Increased Frequency of Testing

Globe Telecom was operating a fairly common compliance-based testing schedule, however realizing the extended gaps between assessments they wanted to upgrade their proactive testing practices.

> **We had the usual annual pentest for regulatory purposes, but we recognized the limitations of a one-time annual test while changes happen in the IT infrastructure throughout the year. If you pentest only one month out of the year, you still have 11 months of changes that haven't been accounted for.**

With Pentera, Globe Telecom's SOC is running a monthly automated pentest within their headquarters while simultaneously increasing the cadence of scheduled routine tests across the extended network.

Peace of Mind Against Ransomware

To address the rising threat of ransomware, Globe Telecom utilizes Pentera's RansomwareReady™ module to proactively test its defenses against specific, high-risk ransomware strains. This capability allows the SOC to evaluate the effectiveness of their perimeter defenses, particularly their EDR, to detect and respond to such attacks. This proactive approach ensures that Globe Telecom is not only prepared to defend against known ransomware variants, but also has the flexibility to quickly adjust its strategies as new threats emerge.

We were running a best of breed strategy with our security, but best of breed becomes expensive in the long run. Eventually you end up with 30 solutions with overlapping capabilities. If you can find one solution that can do multiple functions well without introducing risk, consolidating becomes the right choice.

Garrett Silao
VP, Security Operations Center

Results: Improved Security Posture Coupled with Operational and Economic Efficiency

With Pentera, the Globe Telecom SOC team overcame the operational constraints of their previous solutions and seamlessly extended security testing across the parent corporation and its wider network. The SOC now benefits from increased testing frequency and a streamlined testing and validation process that provides better visibility into exploitable security gaps across subsidiaries. The SOC is confident in their ability to mitigate potential ransomware risks with minimal disruption to business operations. This enhanced efficiency has established a proactive defense against ransomware threats and strengthened their security posture. Pentera's advanced testing and validation capabilities also enabled the SOC to optimize their security stack, reducing costs by eliminating redundant tools and lowering licensing fees associated with multiple platforms.

.

About Pentera

Pentera is the category leader for Automated Security Validation™, allowing any organization to test all cybersecurity layers, over all the attack surfaces, unfolding true, current security exposures at any moment, at any scale. Thousands of security professionals and service providers around the world use Pentera to guide remediation and close security gaps before they are exploited.