PENTERA | CASE STUDY

hibank
A MEMBER OF BNI GROUP

Hibank Strengthens Cyber Resilience with Continuous Security Validation

Highlight Achievements

- Pinpoints vulnerabilities across the full attack surface and prioritizes them by their business risk profile
- Timely vulnerability detection and remediation without disrupting production systems
- Provides detailed attack path visualizations to facilitate clear communication, accelerating mitigation efforts

Background Information

Hibank is a digital-first financial institution in Indonesia. The bank's business model centers on providing seamless, technology-driven banking services to ensure the best customer experience alongside operational efficiency.

Hibank operates in a hybrid IT environment, with many of its applications still on-prem. The bank focuses on migrating manual processes to digital platforms, including mobile and internet banking, as well as back-office applications. Committed to robust cybersecurity, hibank implements advanced measures to protect its extensive digital footprint.

The Challenge: Turning an inefficient and costly manual pentesting into a seamless, cost-effective process

Before deploying Pentera, hibank relied on expensive third-party consultants, who would only conduct periodic assessments based on regulatory demands and ad-hoc tests for critical applications. This approach wasn't scalable and left much of the bank's attack surface untested for long periods of time.

There were numerous challenges the team at hibank had to overcome so they could pentest more frequently. To begin with, there was a major concern that the manual pentesters could cause performance issues and downtime of critical applications during working hours. Not able to tolerate the risk to business continuity, the bank's security team was forced to run tests outside of normal business hours. However, this frequently became a scheduling headache with the pentesters who didn't have much flexibility after working hours. Adding to their concern was their lack of control over the skill level of the individual pentesters brought in to test their environment.

The Need: Automated security validation that wouldn't pose any risk to business operations

With its business model geared to support digital transformation of its banking services, hibank's digital footprint was forever expanding, and so was its attack surface. The Cyber Security team quickly realized they needed a scalable, efficient, and cost-effective solution that would provide continuous security validation, but without affecting business operations.

The CISO was also looking for a solution that would improve the communication between the cybersecurity and IT admin teams; looking for a tool that would help build consensus on which vulnerabilities were proven to be exploitable and should be prioritized first.

The Solution: Pentesting across the environment without any disruption

Product Evaluation Process

Hibank's security team kicked off their evaluation of Pentera with a 1-day POV. It was important to determine that the Pentera Platform wouldn't have any impact on the performance of their banking application. They were pleased to discover that Pentera was able to cover a larger scope of their IT network without a whiff of disruption. For Lim Siaw Liang, the CISO at hibank, this was a game changer.

Lim Siaw Liang and his team continued to scan and pentest across all applications in production, including core banking applications. As an agentless solution, the Pentera runs didn't affect the stable throughput of their banking applications. Hibank's team was extremely pleased to see that with Pentera they could test all their security controls during business hours without it causing any discernible impact.

Easy Deployment

Once Pentera was fully implemented on the hibank network, the security team found it easy to operate, whether that be to define and schedule tests, add new users, or understand the analysis provided. Lim Siaw Liang and his team particularly like the visibility Pentera provides into the attack path, showing a 'spider web' of the most vulnerable assets that an attacker could get access to and compromise. This feature greatly improves communication across the IT team by clearly defining the most vulnerable assets. Having this mapped out makes it easier to explain to developers and system administrators where attackers could breach their system's backend, helping them to prioritize remediation efforts.

Support Red Teaming

Since deploying Pentera Core, Lim Siaw Liang and his team can determine how effective their implemented tools are at assessing and detecting emulated attacks by Pentera. Paying attention to the coverage of their defense layers and the time duration to detection, they vary the testing conditions from noisier attacks to more quiet, stealthier conditions. In this process, the team discovered that Pentera could bypass one of their antivirus solutions, alerting them to the possibility that if Pentera can, attackers could too.

SOC Team Optimization

Hibank's IT team is also using Pentera to conduct ad-hoc audits of their outsourced SOC team. These tests are conducted in silent mode to assess the effectiveness of their SOC's responsiveness and protection capabilities. Using a 24/7 SOC, Lim Siaw Liang wants confirmation they're responding to all incidents, particularly those in the middle of the night.

> **Raising the bar of KPIs addressing vulnerability mitigation time, the new standard of expected performance is to mitigate all critical and high vulnerabilities within one week.**

Lim Siaw Liang
Chief of Cyber Security Officer,
hibank

Results: Systematic reduction of cyber exposures across networks

Using Pentera, Lim Siaw Liang has a lot more confidence in the security posture of his IT environment now compared to what he did before. Raising the bar of KPIs addressing vulnerability mitigation time, his new standard of expected performance is to mitigate all critical and high vulnerabilities within one week. He is confident that his team can systematically mitigate critical exposures and vulnerabilities, with clear directions of where they pose the most threat at their root cause.

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.