CASE STUDY: NETPLUZ

Unlocking MSSP Capabilities with Automated Penetration Testing

Customer

The customer, Netpluz Asia Pte Ltd (Netpluz Asia), is a regional Managed IT and Communications Service Provider serving businesses in the greater Asia Pacific region with reliable and high-performance communication services across data, voice, video, mobility, analytics as well as cybersecurity, to over 2000 customers in the region, with key clients in the Enterprise and Financial Services segment. Their current services infrastructure is deployed both on-premises in a data center, as well as in the cloud, including Windows® based virtual machines, delivering services to customers remotely and through VPN.

Challenge

Netpluz Asia has a robust managed security services portfolio that includes Managed Security Operation Center (SOC), Network/Infrastructure Vulnerability Assessment & Penetration Testing (VAPT), Web Server/Application VAPT, Compromise Assessment, Mobile Application VAPT, API Testing, Wireless VAPT, and Phishing E-mail Simulation among others. To address the current cybersecurity landscape and deliver end-to-end cybersecurity solutions, Netpluz Asia wanted to include Managed Detection and Response (MDR) services as part of their Managed SOC, without the need for incremental resources and security analyst skillsets, which they lacked. Moreover, customers typically subscribed to managed VAPT services twice a year, primarily for health checks on their internal web server and applications and risk assessment on their internal network defenses. Therefore, balancing the return on investment between the cost of integrating and providing an MDR-integrated VAPT tool, versus the frequency of the subscription services, posed another obstacle to the team.

"As an MSSP, we strive to deliver cyber-resilient, end-to-end security solutions and services for our customers. The RidgeBot solution has helped us expand our offerings to deliver automated and integrated VASP services."

Mr. Lau Leng Fong
Chief Executive Officer, Netpluz Asia Pte Ltd

Solution

With Ridge Security's automated pen-testing platform, RidgeBot, Netpluz Asia was able offer additional services to address the needs and challenges of their customers. Specifically, Netpluz Asia was able to offer an end-to-end MDR solution that included exposure detection, as part of their managed VAPT services.

RidgeBot helped integrate Vulnerability Assessment data into their Managed Security Operation Center, delivering automated pen-testing that streamlined operations and reduced the overall cost of an otherwise manual VASP tool.

Benefits

Most customers look for a one-stop shop, with automated pen-testing to increase the accuracy and efficiency of their threat detection and response initiatives. Risk-based vulnerability management, with automated pen-testing, gives clear visibility to customers on the security risks and the security posture of their environment. This gives them the ability to prioritize security investments in high-risk areas to eliminate or minimize the potential of a breach. With RidgeBot integrated into the core SOC services offering, Netpluz Asia was able to deliver an advanced and automated pen-testing tool that includes threat monitoring, detection, and response from a remote SOC, allowing customers to retain their security posture through deep, continuous detection, analysis, and mitigation of active threats.

- Continuous and automated, user-friendly pen-testing tool helps uncover risks and vulnerabilities as the network evolves, including connected devices at the edge and in the cloud.
- Templates and tools help fine-tune and customize tasks so that security-related events are visible to SIEM and SOAR platforms for maximum efficacy and efficiency.
- Complete visibility into the threat landscape, with kill chain for all attacks and detailed reports for compliance requirements.

Request a Demo of RidgeBot

See Ridge Security RidgeBot in action. Learn how RidgeBot can fit into your enterprise providing both Automated Penetration Testing and Adversary Cyber Emulation testing.