CASE STUDY

T-Systems Partners with Ridge Security to Enhance Its Managed Offensive Security Services

Ridge Security Technology Inc. www.ridgesecurity.ai

The Customer

With locations in 26 countries and over 26,000 employees (December 31, 2024), as well as annual revenues of over EUR 4.0 billion (2024), T-Systems is one of the leading providers of digital services in Europe. The Deutsche Telekom subsidiary is headquartered in Germany and has a presence in Europe as well as in selected core markets and strategic production locations. T-Systems offers end-to-end IT solutions, driving the digital transformation of companies in all industries and institutions worldwide.

T-Systems is one of the most successful providers of security solutions and services for companies and public administrations. Customers benefit from the high level of protection with which Deutsche Telekom secures its own infrastructure. T-Systems operates its own interconnected Security Operations Centers (SOC) around the globe. With the help of AI, around 2,500 security experts analyze up to 2.5 billion security-relevant events from around 3,300 global data sources every day.

The Challenges

Today's organizations face growing risks and can no longer afford a passive approach to security. Offensive cybersecurity has become a business imperative, demanding both technical adaptation and cultural transformation within organizations. Relying solely on reactive security measures leaves businesses vulnerable to undetected, high-risk threats, posing significant jeopardy to operations.

Manual security testing poses additional challenges due to its "run-and-done" nature, which prioritizes the rapid identification of vulnerabilities over in-depth analysis and remediation planning. Critical gaps often remain, exposing organizations to persistent and evolving threats that demand more robust and proactive solutions.

The Solution

RidgeBot's automated penetration testing, combined with T-System's cyber threat intelligence capabilities, significantly reduces potential attack vectors and exploitable vulnerabilities. Through Ridge Security's solutions, T-Systems delivers continuous scanning, validation, and monitoring to uncover weaknesses such as outdated software, misconfigurations, poor authentication practices, and insufficient access controls. This forms the basis of a comprehensive offensive security service tailored to the specific needs of each client.

The process begins with a planning phase that defines the scope of engagement, followed by execution led by T-Systems Offensive Security Team. The team is composed of professionals holding offensive security certifications that are widely recognized in the industry, ensuring adherence to best practices and regulatory standards.

A multinational client has leveraged RidgeBot® to automate penetration testing across up to 300 IP addresses. The greatest value, however, came from executing emulation exercises using ACE to test their detection and response mechanisms. These simulations revealed critical areas for improvement that would typically remain hidden without an exploitable external vulnerability, emulating what could happen if an attacker had already gained a foothold within internal systems.

"Proactively discovering exposures, validating findings, and mitigating risks swiftly, this is the essence of preemptive cybersecurity," said Edgar Flores, Offensive Security Manager at T-Systems.

Transitioning from manual penetration testing to automated testing with RidgeBot® was seamless, thanks to T-Systems extensive expertise developed through years of conducting manual assessments. The result: faster, more accurate, and more resilient service delivery. While the T-Systems offensive SOC team simulates real-world attacks with RidgeBot®, the defense team simultaneously monitors and flags any activity that may represent high-risk threats, offering clients a complete view of their exposure and readiness.

The initial phases of the penetration testing process—such as reconnaissance and enumeration—can be efficiently handled by the RidgeBot® solution. This automation allows for faster execution across a larger volume of IP addresses, enabling T-Systems' offensive security team to focus on delivering high-value insights through in-depth analysis and expert validation of the findings.

Flores emphasized, "Successful operations demand the best security technologies, skilled personnel, and refined processes. This is the value T-Systems delivers with Ridge Security as a trusted partner."

The Benefits

RidgeBot's automated penetration testing enhances T-Systems' security operations by overcoming the limitations of manual testing. With RidgeBot®, penetration testing becomes cost-effective, continuous, and rigorous, requiring less time and effort. Once RidgeBot® is installed and communication with target systems validated, testing schedules ensure ongoing penetration testing and vulnerability management, strengthening clients' security postures. RidgeBot® also facilitates efficient coverage of both internal and external networks. According to Flores, "Automated penetration testing with RidgeBot® has used 30% of the time to get the job done compared to manual testing—ultimately lowering costs for our customers."

RidgeBot's pre-built use cases further simplify security defense processes,

"Automated penetration testing with RidgeBot® has used 30% of the time to get the job done compared to manual testing—ultimately lowering costs for our customers."

Edgar Flores, Offensive Security Manager at T-Systems

while ACE enables T-Systems to emulate advanced threats effectively. For example, ACE tests PowerShell executions, detecting files with specific hash signatures integrated into the operating system. These capabilities enable T-Systems to safeguard clients by conducting thorough evaluations across multiple technology layers, ensuring early detection and minimizing attack surfaces.

Ridge Security's automated pentesting, vulnerability validation, and lateral movement simulation all efficiently roll into CTEM. They are covering all the different aspects needed for continuous threat exposure management to reduce surface attacks, providing metrics, findings, and data around our client's current states of exposure. This capability is drastically needed today; it is leading the way for the future.

About Ridge Security Technology Inc.

Ridge Security is a leader in adversarial exposure validation and is dedicated to developing innovative cybersecurity solutions designed to protect organizations from advanced cyber threats. Ridge Security's products incorporate advanced artificial intelligence to deliver comprehensive security validation. With a focus on automation, intelligence, and actionable insights, Ridge Security enables security teams to proactively defend against and respond to evolving cyber challenges.