STELLAR CYBER®

Unlock a New Capability for MSSPs

Together we provide a high-fidelity Open XDR security environment with automated penetration testing and exploitation to accelerate threat hunting, prevention, detection, remediation and response across your entire IT infrastructure.

Better Together

The incidence and sophistication of attacks and breaches are trending upwards, necessitating machine-assisted tools to arm limited-staff-and-budget SecOps teams with the automation, analytics and orchestration solutions that allow them to effectively defend your company's business.

The Stellar Cyber Open XDR platform integrates all your specialized security tools—with their combined results—and then augments these with next-generation security information and event management (SIEM), orchestration and threat intelligence capabilities. Ridge Security RidgeBot®'s automated and continuous penetration testing and uniquely designed exploitation capabilities integrates with the Stellar Cyber Open XDR platform to enhance visibility, accelerate prevention, detection and response, and strengthen SecOps staff efficiency, effectiveness and productivity. The joint Stellar Cyber and Ridge Security solution helps you:

- **Reduce enterprise risk** by the early and precise identification and remediation of all attack activities while slashing costs, retaining investments in existing tools and accelerating analyst productivity.
- **Integrate the security results** of RidgeBot®'s continuous automated penetration testing, exploitation, attack surface identification and asset risk assessment with Stellar Cyber's AI-powered detection and automatic response technology.
- Combining RidgeBot®'s penetration testing and exploitation capabilities with Stellar Cyber's Open XDR 360-degree network visibility and analytics provides your SecOps team with **streamlined information for instant remedial and response action**.

Business Challenges

Enterprise attack surfaces continue to expand dramatically as a result of increasing adoption of cloud-native applications and data storage, a growing work-from-anywhere workforce, a plethora of fast-changing corporate and personal devices used by today's workers, and evermore sophisticated cybercriminals and attack paths. To stay a step ahead of the bad actors requires an automated, adaptive suite of specialized security tools. When this wealth of tools operates independently, it creates complex management challenges and coverage gaps that result in protracted investigation of time-sensitive information, and place a heavy manual burden on SecOps staff, all of which raises costs and prolongs remedial and response time.

Building 360-degree visibility across the network, endpoints, users, applications, and cloud means pulling together all the available tools and the potentially large volume of data generated by each individual tool. This can be an extremely tedious manual task and is time-intensive for analysts. Automated, AI-assisted vulnerability detection, penetration testing, results integration and analysis promise to improve the ability to piece together complex attacks, reduce alert fatigue, reduce demands on SecOps staff, and speed up response and remediation time.

Benefits

Sophisticated cyber response depends on having always-fresh and relevant information at the fingertips of the SecOps team. Automated security tools such as Ridge Security's RidgeBot® performs continuous penetration testing and exploitation to probe the resilience of your assets and report on vulnerabilities detected and successfully exploited attack vectors. It is imperative to have the penetration test, exploitation and risk results integrated into a single-pane-of-glass dashboard—together with data and events from other tools to provide insightful, actionable, accurate and timely SecOps threat intelligence.

The joint Stellar Cyber and Ridge Security solution provides many benefits:

- automated continuous security validation, penetration testing and vulnerability exploitation
- accelerated threat and risk detection, along with faster formulation of remedial action plans
- integrated management reporting with RidgeBot®'s prioritized risk assessments
- unified analytics, event correlation and alert management
- consolidated incident response leveraging RidgeBot®'s investigative and forensics information
- always-fresh, accurate and contextually relevant SecOps information
- 360-degree visibility and threat protection across networks, endpoints, users, applications and cloud(s)
- enables analysts to quickly respond to high-fidelity detections across the entire kill chain improving both MTTD and MTTR
- radically improves security analysts' productivity and efficiency with dramatically reduced cost

Automated, ethical, robotic, risk-based vulnerability management is the future of penetration testing!

Hackers are already using robots to attack your enterprise, and you can only possibly compete with an army of new SecOps staff. Even minor changes to your enterprise network can create new untapped or newly introduced vulnerabilities. RidgeBot® is the only fully automated penetration test robot that ethically hacks your systems to find, expose and verify vulnerabilities. RidgeBots® act like human attackers, relentlessly locating exploits, then documenting their findings. But unlike humans, RidgeBots® are armed with dynamic attack strategies to try before moving on to the next target, making penetration testing affordable, highly effective and able to run at enterprise scale.

How it Works

RidgeBot®'s penetration test and exploitation logs and test results are integrated into Stellar Cyber's open XDR platform which performs data integration, analytics and correlation of the information received from RidgeBot® and other specialized security tools.
Stellar Cyber offers a highly efficient, integrated XDR approach to improving your cyberattack management and security posture, with tools and technology that work together intelligently to provide simplified yet comprehensive attack surface and security posture management.
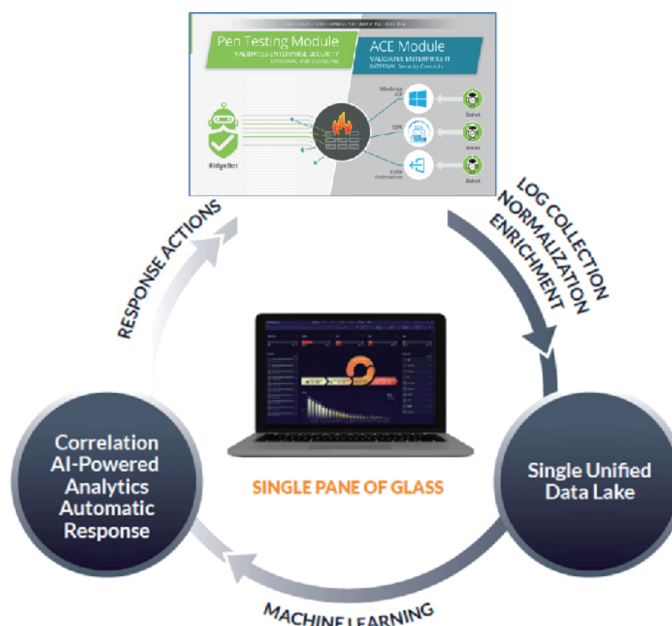
Figure 1: Integration of RidgeBot's Attack Logs into Stellar Cyber XDR Platform

The Stellar Cyber Open XDR platform delivers comprehensive, unified security without complexity, empowering lean security teams of any skill to successfully secure their environments. With Stellar Cyber, organizations reduce risk with early and precise identification and remediation of threats while slashing costs, retaining investments in existing tools, and improving analyst productivity, delivering a 20X improvement in MTTD and an 8X improvement in MTTR. The company is based in Silicon Valley. For more information, contact https://stellarcyber.ai.

Ridge Security's RidgeBot® provides more than just standard penetration testing. It is fully automated and runs on a configured schedule to implement a living and learning security environment that continuously and iteratively assesses your assets for risks. Critically, Ridge-Bot® also attempts to exploit the vulnerabilities detected, with the unique benefit that not only are the vulnerabilities found, but they are prioritized by criticality of the risk they pose. RidgeBot® exploitation results render invaluable recommendations of exactly what fixes must be made—including step-by-step remedial instructions—in your environment to protect against bad actors exploiting the vulnerabilities. For more information: ridgesecurity.ai.