The Integrated Solution Guide of Trellix Helix and Ridge Security RidgeBot

An adaptable and composable security environment depends on having real-time and relevant information at the fingertips of your SecOps team. Automated security validation tools such as Ridge Security's RidgeBot penetration testing and exploitation continuously probe the resilience of your assets and report on vulnerabilities detected and successfully exploited attack vectors. It is imperative to have these penetration test and exploit results integrated into a single-pane-of-glass dashboard to provide insightful, actionable, accurate and timely threat intelligence to your SecOps team.

The Business Problem

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, you require an adaptive, living ecosystem of specialized security tools integrated into an exemplary operational interface for immediate situational awareness to drive rapid SecOps response and action.

Trellix Helix and Ridge Security Joint Solution

The sophistication of attacks and breaches are trending upwards, necessitating machine-assisted tools to arm limited-staff-and-budget SecOps teams with the automation and orchestration solutions that allow them to effectively defend your company's business.
Trellix Helix provides operations to work in a proactive approach against advanced and sophisticated threats. Through a cloud- based SaaS platform, Trellix Helix integrates your security tools, providing a much deeper holistic view of an organization's security posture. Trellix Helix security operations platforms, enables organizations to take control of any incident from detection to response. In addition, through integrating security tools with next generation security information and event management (SIEM) orchestration and threat intelligence leverages organizations to utilize untapped potential security investments.
Integrating Ridge Security with Trellix Helix is a win- win situation for our mutual customers. In an effective and efficient manner, organizations can drive faster detection and response times by integrating Ridge Security's RidgeBot. Ridge Security's RidgeBot automated and continuous penetration testing and specialized exploitation capabilities integrated with the Trellix Helix platform's streamlined orchestration strengthen SecOps staff efficiency, effectiveness and productivity by continuously providing clear and a holistic risk visibility of the IT environment.

The joint solution provides many benefits:

- automated continuous security validation, penetration testing and vulnerability exploitation enabling quicker response times to meet compliance standards
- Prioritize and accelerate remediation response times based on threats and risk detection,
- Gain a comprehensive view and management reporting with RidgeBot's prioritized risk assessments
- Enrich analytics, event correlation and alert management by including RidgeBot's vulnerability feeds
- Improve incident response leveraging RidgeBot's investigative and forensics information
- Access real- time and , accurate and contextually relevant information

RidgeBot's penetration test and exploitation results are exported in syslog format to Trellix Helix. Trellix Helix performs data integration, analytics and correlation of the information received from RidgeBot and specialized security tools by other vendors.
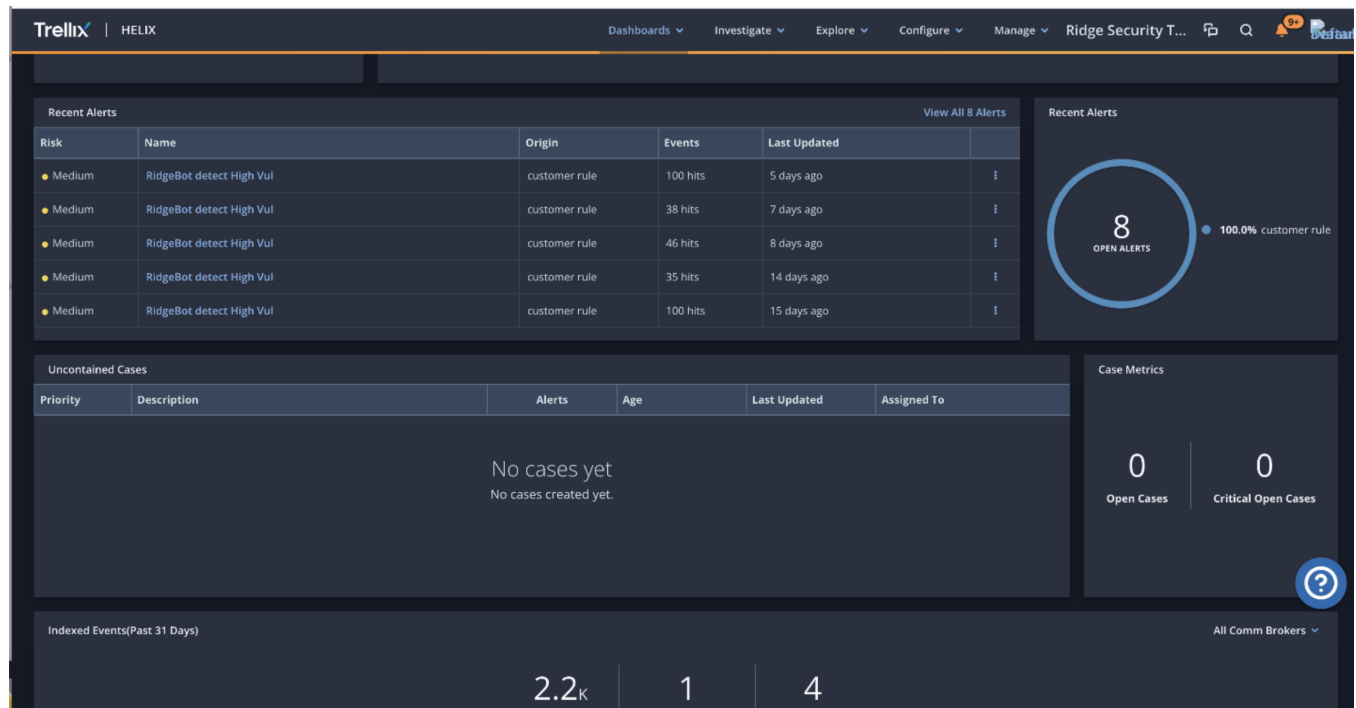
Benefits of Using RidgeBot

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, RidgeBot 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 instructions—in your environment to protect against bad actors exploiting the vulnerabilities.

About RidgeBot

Ridge Security RidgeBot's enterprise-class penetration testing achieves automated security validation and risk-based vulnerability management using intelligent robots. It delivers a range of capabilities including automated asset profiling, attack surface identification, iterative and continuous security validation, automated and on-demand penetration testing, vulnerability exploitation and remediation, risk assessment and prioritization, and automated reports and metrics.

RidgeBot-reported exposures and exploits can be remedied immediately based on risk-prioritized actions. Automated tests can run continuously at the scale of your network, providing rapid high-fidelity intelligence on your security posture. The shift from manual-based, labor-intensive testing to machine-assisted automation alleviates the severe shortage of security professionals; it allows human security experts to automate repetitive daily tasks and instead devote their time to threat defense strategy and technology.

Blending RidgeBot's results, risk assessments and remedial recommendations into the Trellix Helix platform unifies security infrastructure into highly efficient SecOps orchestration and operation.

About Trellix Helix

With increasingly sophisticated cyberthreats exposing vulnerabilities, cybersecurity has never been as challenging. Instead of a reactive attitude with standalone products, which compounds complexity, your business can instead take a comprehensive, proactive approach. With the Trellix Helix SaaS security operations platform, you can build a holistic foundation that empowers your SecOps team to take control of any incident, from detection to response.

Trellix Helix offers a highly efficient, integrated 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. Trellix Helix unifies visibility and gives control to enterprises by collecting, correlating, and analyzing critical data for meaning threat awareness. Organizations can accelerate their response times through improving SOC functionality such as alert management, search analysis and automating their response with pre-build and customizable playbooks.

Learn More

For more information, contact your Trellix representative or channel partner, or visit www.trellix.com.

Trellix Compatible Solution

RidgeBot version V4.0.0
Trellix Helix version 2022.6.0-9

Challenges

The results of all your specialized security tools—such as RidgeBot's automated penetration testing and exploitation—must be visible in an integrated, actionable SecOps dashboard.

Trellix Helix Solution

A flexible SecOps platform integrating and augmenting existing tools with nextgen SIEM, orchestration, and threat intelligence. A dashboard with integrated visibility into all your security tools.

Results

he security protection and peace of mind awarded by RidgeBot's automated penetration testing, vulnerability detection, successful threat exploitations and remedial recommendations.

The power of the Trellix Helix platform to support a resilient, efficient and confident SecOps team with accurate, actionable information for immediate situational awareness and a coordinated defense strategy.

Ridge Security Technology Inc.
www.ridgesecurity.ai