SOLUTION BRIEF

Fortinet and Ridge Security Integrated Solution

World-Class SOAR Capabilities Integrate Automated Penetration, Exploitation, and Attack Vector Results

Executive Summary

The fast-evolving threat landscape and increasing organizational and technological intricacies create an exceedingly complex environment that leaves an organizations vulnerable to attack. Automated security tools continuously probe your assets' resilience, report on vulnerabilities detected, and document successfully exploited attack vectors. Integrating these test-and-exploit results into a SOAR dashboard is imperative to provide insightful, actionable, accurate, and timely threat intelligence to your SecOps team.

The Challenge

Attack surfaces continue to expand dramatically due to the increasing adoption of cloud workloads and data storage, a growing work-from-anywhere (WFA) workforce, virtualization of the network perimeter, and evermore sophisticated cybercriminals and attack resources. To stay ahead of the bad actors, you require an adaptive, automated ecosystem of specialized security tools integrated into an exemplary operational interface for immediate situational awareness to drive rapid SecOps response and action.

Joint Solution Description

Fortinet and Ridge Security are committed to delivering cutting-edge security solutions that empower SecOps teams to increase productivity and speed of response to threats. This integration provides cost-effective continuous automated penetration testing of a network, asset inventory and profiling, security validation, and risk-based vulnerability management using intelligence robots.

Fortinet's FortiSOAR unburdens SecOps teams overloaded with too many tools, alerts, and manual processes by centralizing, standardizing, and automating SecOps workflows. Ridge Security's RidgeBot automates the continuous probing and exploitation of a network and its assets, distilling results into clear priorities and curating a remedial path. Together, the joint solution alleviates the burden on scarce, highly trained security staff and specialists by empowering teams with an automation and orchestration solution to effectively defend your company's business.

Solution Components

FortiSOAR is a holistic security orchestration, automation, and response workbench designed for SOC teams to efficiently respond to the ever-increasing influx of alerts, manage repetitive manual processes, and bolster the shortage of resources. With broad integrations, rich use-case functions, hundreds of prebuilt workflows, and simple playbook creation, this patented and customizable security operations platform provides automated playbooks and incident triaging, and real-time remediation for enterprises to identify, defend, and counter attacks. FortiSOAR is the security operations hub that connects to everything and automates anything, helping protect your organization from attack.

Solution Components

- Fortinet FortiSOAR
- Ridge Security RidgeBot

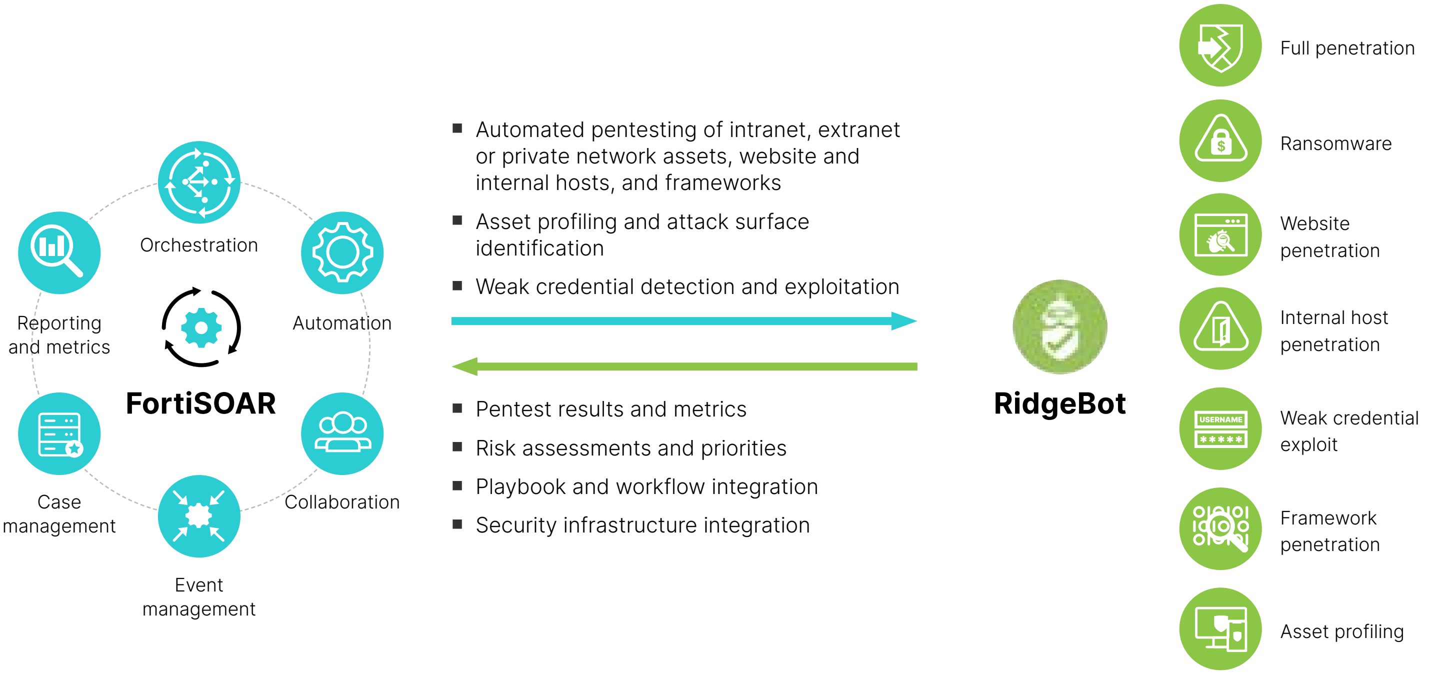
Solution Benefits

- Cost-effective **continuous automated penetration testing**, asset profiling, attack surface identification, and vulnerability risk assessment
- Enables **instant, high-fidelity decision-making** to address complex infrastructure
- Enriches FortiSOAR management capabilities with RidgeBot **at-scale** security validation, asset profiling, attack surface identification, and pen-testing
- Integrates existing security infrastructure for a **coordinated defense strategy**
- Consolidates threat intelligence to streamline SecOps, processes, and strategy

Ridge Security RidgeBot is a cost-effective continuous automated penetration testing and exploitation software robot that continuously probes and validates your network and assets. Its results prioritize exploitable vulnerabilities and provide remedial steps. RidgeBot also automatically inventories and profiles your assets.

Joint Solution Integration

Facilitating automated interactions between a Ridge Security RidgeBot server and FortiSOAR playbooks is as simple as adding the RidgeBot Connector as a step in a FortiSOAR playbook.



- Automated pentesting of intranet, extranet or private network assets, website and internal hosts, and frameworks
- Asset profiling and attack surface identification
- Weak credential detection and exploitation

- Pentest results and metrics
- Risk assessments and priorities
- Playbook and workflow integration
- Security infrastructure integration

Figure 1: Integrating RidgeBot penetration tasks and results into FortiSOAR

The RidgeBot Connector provides five automated operations that can be included in FortiSOAR playbooks from FortiSOAR release 5.0.0 and later. These operations allow FortiSOAR to create and execute RidgeBot tasks. The following bundled playbooks are shown after importing the connector:

Create Task	Creates a default intranet or web penetration RidgeBot testing task.
Get Task Info	Retrieves information about an existing RidgeBot task, including attributes such as start time, end time, and status.
Get Task Statistics	Retrieves statistics from an existing RidgeBot task, including such fields as the number of assets found and the number of vulnerabilities found per risk category.
Generate and Download	Generates and downloads a penetration testing report from a completed RidgeBot task by specifying the Task ID.
Stop Task	Stops a running or unfinished RidgeBot task by specifying the Task ID.

Figure 2: RidgeBot Connector automated operations in FortiSOAR Playbook

Joint Use Case

Automating Penetration and Exploitation Tasks

With the RidgeBot Connector installed, you can manage (create and execute) and automate RidgeBot penetration and exploitation tasks by including them in FortiSOAR playbooks. The results of these tests are then uploaded to FortiSOAR for planning and action by the SecOps team.

About Ridge Security RidgeBot

Ridge Security enables enterprise and web application teams, ISVs, governments, education, DevOps, SecOps, and anyone responsible for ensuring software security to quickly and efficiently test their systems before and after deployment. Ridge Security improves the efficiency of your SecOps team by providing risk-based vulnerability management through continuous automated testing, exploitation, prioritization, and remedial guidance.

www.fortinet.com

August 4, 2023 11:28 AM

2281500-0-0-EN