IBM Security® QRadar® SOAR and RidgeBot® Integrated Security Protection

Executive Summary

The fast-evolving threat landscape combined with increasing organizational and technological intricacies create an exceedingly complex environment that leaves an organization vulnerable to attack. Automated security tools, such as Ridge Security's RidgeBot® penetration testing and exploitation, continuously probe the resilience of your assets and report on vulnerabilities detected as well as documenting successfully exploited attack vectors. It is imperative to integrate these test-and-exploit results into a SOAR dashboard to provide insightful,actionable, accurate and timely threat intelligence to your SecOps team.

The Challenge

Attack surfaces continue to expand dramatically due to increasing adoption of cloud workloads and data storage, a significant WFA workforce, growing virtualization of the network perimeter, and evermore sophisticated cybercriminals and attack resources. To stay a step 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.

The early decisions you make when responding to a potential security incident often make the difference between containing it or a crisis occurring. Unfortunately, most organizations are still using manual processes or custom code without full security orchestration, automation and response (SOAR) functionality.

IBM Security® QRadar® SOAR lets you get started quicker, improve your SecOps efficiency and ensure your incident response processes are met with an intelligent automation and orchestration solution that timestamps key actions and aides threat investigation and response.

Joint Solution Description

IBM QRadar® SOAR helps you manage costs and time with prebuilt integrations for a broad ecosystem of 300+ connectors, while helping your SecOps team respond more quickly and effectively, cutting response time by up to 85%. It alleviates the burden and delay of manual processes on scarce, highly-trained security staff and security specialists. The incidence and sophistication of attacks and breaches are trending upwards, necessitating machine-assisted tools to arm limited-staff-and-budget SecOps with the automation and orchestration solutions that allow them to effectively defend your company's business. Additionally, IBM QRadar® SOAR solutions help you manage your response to more than 180 international privacy and data breach regulations.

Ridge Security and IBM have partnered to deliver an industry-leading SOAR solution to address these challenges. The integration of RidgeBot® and IBM QRadar® SOAR delivers cost-effective continuous automated penetration testing of your network and assets, automated asset inventory and profiling, automated security validation, and orchestration capabilities.

Solution Components

- **Ridge Security RidgeBot®:** Cost-effective automated test&exploit that provides continuous automated penetration testing and an exploitation software robot that continuously probes and validates your network and assets. The results prioritize exploitable vulnerabilities and provides remedial steps. RidgeBot® also automatically inventories and profiles your assets.

- **IBM QRadar® orchestration:** Helps you speed up incident response (IR) with automation, improves SecOps efficiency, and closes skill gaps. IBM QRadar® SOAR playbooks integrate RidgeBot® tasks and their results.

Solution Benefits

A	RidgeBot® performs continuous, automated penetration testing and exploitation, asset profiling, attack surface identification and vulnerability risk assessment.
B	Enriches IBM QRadar® SOAR's accelerated incident response capabilities with RidgeBot's at-scale security validation, asset profiling, attack surface identification and pen-testing.
C	RidgeBot's automation tests 100x faster than human testers, and instantly replicates to address complex infrastructure. RidgeBot® reports integrate with IBM QRadar® SOAR to enable instant, focused investigation and decision making.
D	IBM QRadar® SOAR orchestration solutions have a low barrier to entry for analysts to build automation, provide automated responses for high-fidelity alerts, quickly identify real incidents, eliminate false positives, and allow all security tools to actively participate in a coordinated streamlined threat intelligence strategy.

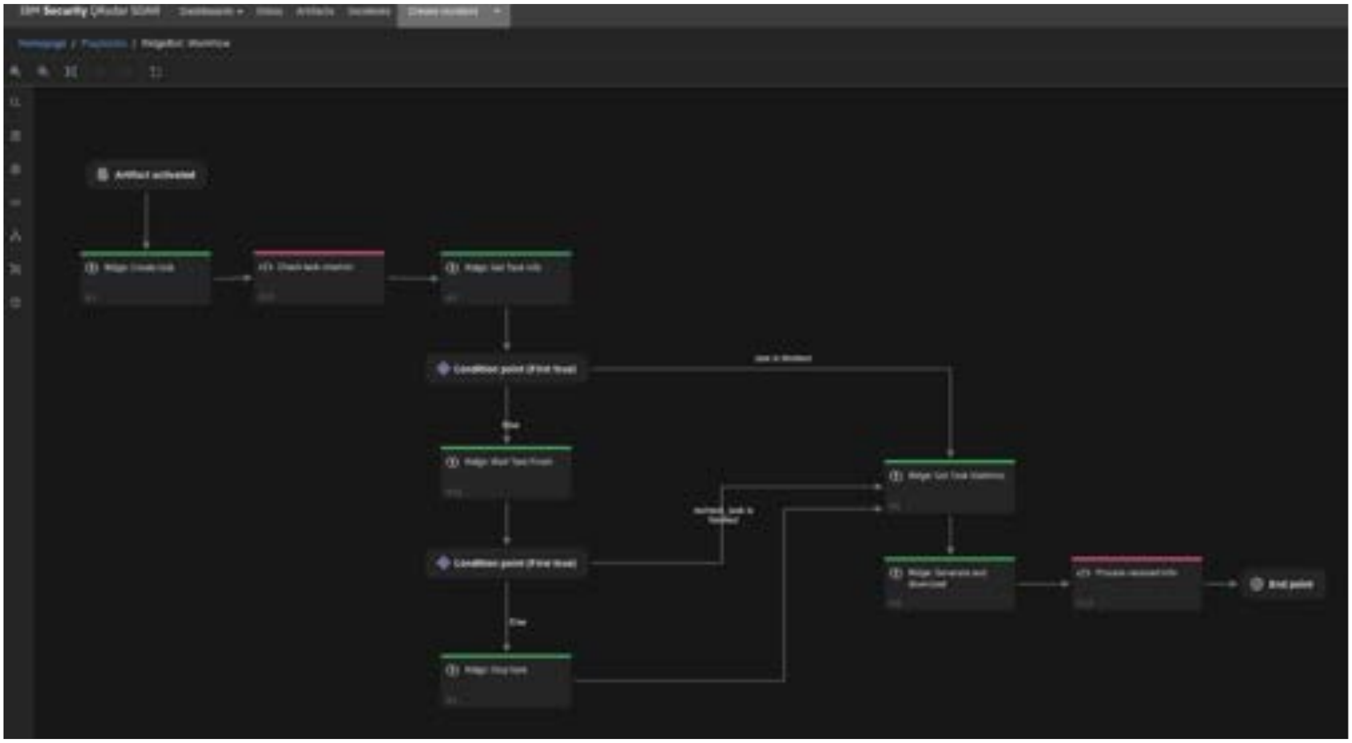
Joint Solution Integration

The Ridge Security RidgeBot® connector facilitates automated interactions—such as creating and executing penetration testing tasks —between a Ridge Security RidgeBot® server and IBM QRadar® SOAR playbooks.

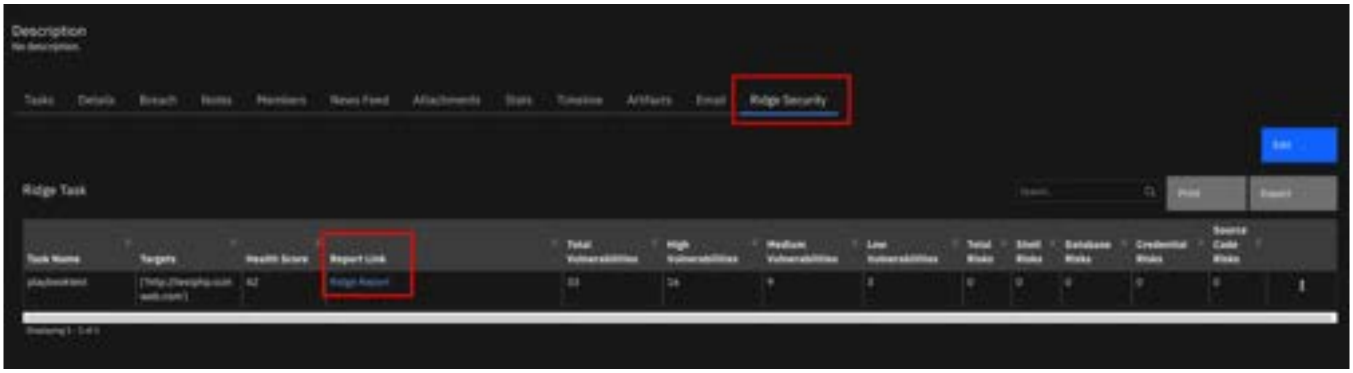
The RidgeBot® Connector (v4.2.3 or later) provides six automated operations that can be included in IBM QRadar® SOAR playbooks as of release V48.0. These operations allow QRadar® SOAR to create and execute RidgeBot® tasks. IBM QRadar® SOAR integrations are part of an open integration framework supported by IBM and other leading security companies.

Create task	Creates a default intranet or web penetration RidgeBot® testing task.
Generate and download	Generates and downloads a RidgeBot® test report from a completed RidgeBot® task.
Get Task Statistics	Retrieves statistics of an existing RidgeBot® task, including fields such as the number of assets found and the number of vulnerabilities found per risk category.
Get Task Info	Generates and downloads a RidgeBot® test report from a completed RidgeBot® task.
Stop Task	Stops a running or unfinished RidgeBot® task by specifying the Task ID.
Wait Task Finish	Checks RidgeBot® task status and waits until the task is complete.

A workflow to execute a RidgeBot® task is configured by defining an IBM QRadar® SOAR playbook. You create an QRadar® SOAR incident and then create a RidgeBot task in the incident's workflow, as shown below. The workflow waits until the RidgeBot® task is completed, then retrieves the task statistics and generates and downloads the RidgeBot® report resulting from the task's execution.



The RidgeBot® report can be accessed by navigating to the IBM QRadar® SOAR task display. Click on the Ridge Security tab and then on the Report Link in the page, as shown below.



Ridge Task

Task Name	Targets	Health Score	Report Link	Total Vulnerabilities	High Vulnerabilities	Medium Vulnerabilities	Low Vulnerabilities	Total Risks	Shell Risks	Database Risks	Credential Risks	Source Code Risks
playbooktest	['http://testphp.vulnweb.com']	62	Ridge Report	33	16	9	8	0	0	0	0	0

Displaying 1 - 1 of 1

Watch this video to see how the configuration is done.

About Ridge Security RidgeBot®

Ridge Security enables enterprise and web application teams, ISVs, governments, education, DevOps, SecOps and anyone else responsible for ensuring software security, to affordably 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.

Ridge Security Technology Inc.
www.ridgesecurity.ai