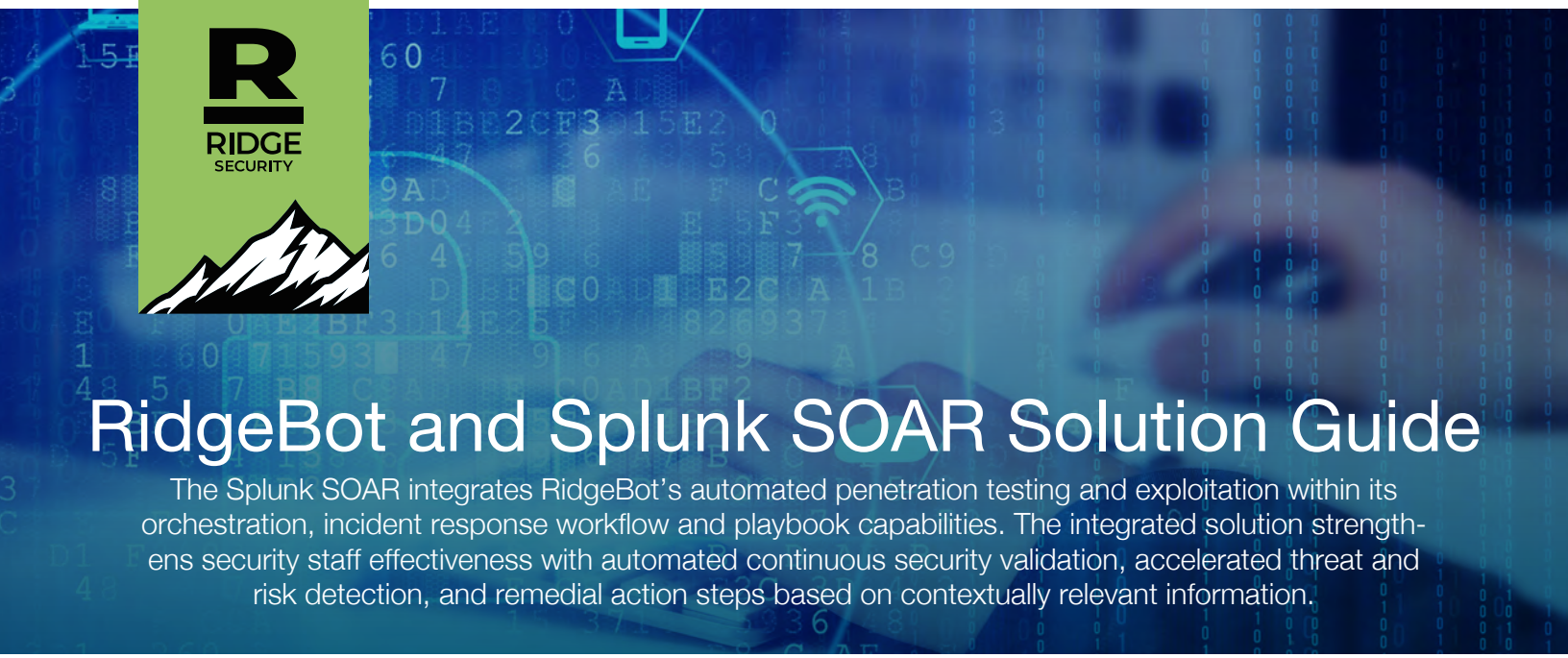


RidgeBot and Splunk SOAR Solution Guide

The Splunk SOAR integrates RidgeBot's automated penetration testing and exploitation within its orchestration, incident response workflow and playbook capabilities. The integrated solution strengthens security staff effectiveness with automated continuous security validation, accelerated threat and risk detection, and remedial action steps based on contextually relevant information.

RidgeBot

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 operation with Splunk SOAR incident response workflows automate Red-Blue team operation, and unifies security infrastructure orchestration. Splunk SOAR integrates RidgeBot pentesting into your SIEM solution playbook, generating an automatic notification when RidgeBot detects a risk on a target

Splunk SOAR

Splunk SOAR provides security orchestration, automation and response capabilities that allow security analysts to work smarter by automating repetitive tasks; respond to security incidents faster with automated alert triage, investigation, and response; increase productivity, efficiency and accuracy; and strengthen defenses by connecting and coordinating complex workflows across their team and tools. Splunk SOAR also supports a broad range of security operations center (SOC) functions including event and case management, integrated threat intelligence, collaboration tools and reporting.

Solution Diagram

RidgeBot capabilities are accessed by creating tasks in the Splunk SOAR. Statistics and reports generated by the RidgeBot tasks are uploaded to the Splunk Vault for easy integration into Splunk SOAR Reporting and Metrics.

Automated

Allows Splunk SOAR to create RidgeBot tasks to integrate automated, continuous pentesting into incident management, workflows and playbooks.

At Scale

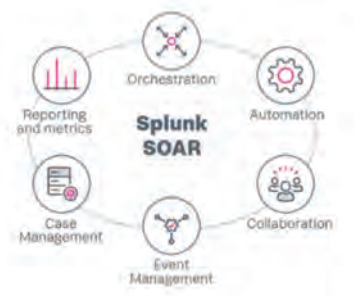
Enriches Splunk SOAR's event management capabilities with RidgeBot's at-scale security validation, asset profiling, attack surface identification and pentesting.

Faster

RidgeBot's automation tests 100x faster than human testers, and instantly replicates to address complex infrastructure. RidgeBot reports uploaded to Splunk SOAR enables instant, high-fidelity decision making.

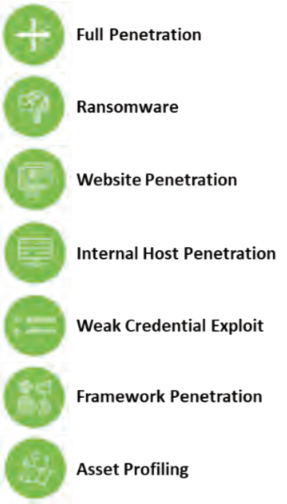
Stronger Defenses

Integrates existing security infrastructure so that all tools actively participate in a coordinated defense strategy. Consolidated threat intelligence streamlines your SOC team, processes and strategy.



- 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



RidgeBot Actions supported by the Splunk SOAR

RidgeBot provides seven actions that allow Splunk SOAR to create and execute RidgeBot tasks. Upon task completion, Splunk SOAR uploads the statistics or report, for example the number of attack surfaces, vulnerabilities and risks identified.

test connectivity	Validates asset configuration connectivity
create task	Creates a RidgeBot asset task
stop task	Stops a RidgeBot asset task
get task info	Gets Ridgebot asset task status and information, with task id
get task info list	Gets status and information of all Ridgebot asset tasks
get task statistics	Gets RidgeBot asset task statistics, with task id
generate and download report	Generate a task report formatted as PDF or CSV format, and download it to the Splunk Vault.