Ridge Security RidgeBot® And Microsoft Sentinel Integrated Cloud-native SIEM Solution

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 SIEM or 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 ever-more 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.

Microsoft Sentinel modernizes your security operations center (SecOps) and lets you uncover sophisticated threats and respond decisively with intelligent, comprehensive security information and an event management (SIEM) solution for proactive threat detection, investigation, and response.

Joint Solution Description

Microsoft Sentinel SIEM helps you manage security threats and posture with a broad ecosystem of data connectors that allow your SecOps team to respond more quickly and effectively at significantly lower costs. Microsoft Sentinel allows you to:

1 Eliminate security infrastructure setup and maintenance

2 Elastically scale to meet cloud-level security needs

3 Collect data at cloud scale

4 Detect previously uncovered threats

5 Investigate threats with AI and hunt down suspicious activities

6 Rapidly respond to incidents with built-in orchestration and automation

Ridge Security and Microsoft Sentinel have partnered to deliver an industry-leading SIEM and SOAR solution to address these challenges. The integration of Ridge Security RidgeBot® and Microsoft Sentinel SIEM delivers cost-effective continuous automated penetration testing of your network and assets, automated asset inventory and profiling, automated security validation, and risk-based vulnerability management using intelligent robots. RidgeBot® results are integrated into Microsoft Sentinel SIEM's management 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.

Microsoft Sentinel

Orchestration helps you speed up incident response (IR) with automation, improves SecOps efficiency, and provides a comprehensive, validated view of network vulnerabilities and risks. Microsoft Sentinel integrates RidgeBot® tasks, their results and log files detailing prioritized vulnerabilities and risks.

Solution Benefits

A RidgeBot® performs continuous, automated penetration testing and exploitation, asset profiling, attack surface identification and vulnerability risk assessment.

B RidgeBot® enriches Microsoft Sentinel's cloud-scale incident response capabilities with RidgeBot's elastic 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® logs and reports integrate with Microsoft Sentinel SIEM to enable instant, proactive threat detection, focused investigation and response decision making.

D Microsoft Sentinel orchestration eliminates security infrastructure setup and maintenance by leveraging RidgeBot’s automated inventory and asset profiling.

E Microsoft Sentinel provides behavior analytics drawn from RidgeBot® task results, allowing SecOps to stay ahead of evolving threats.

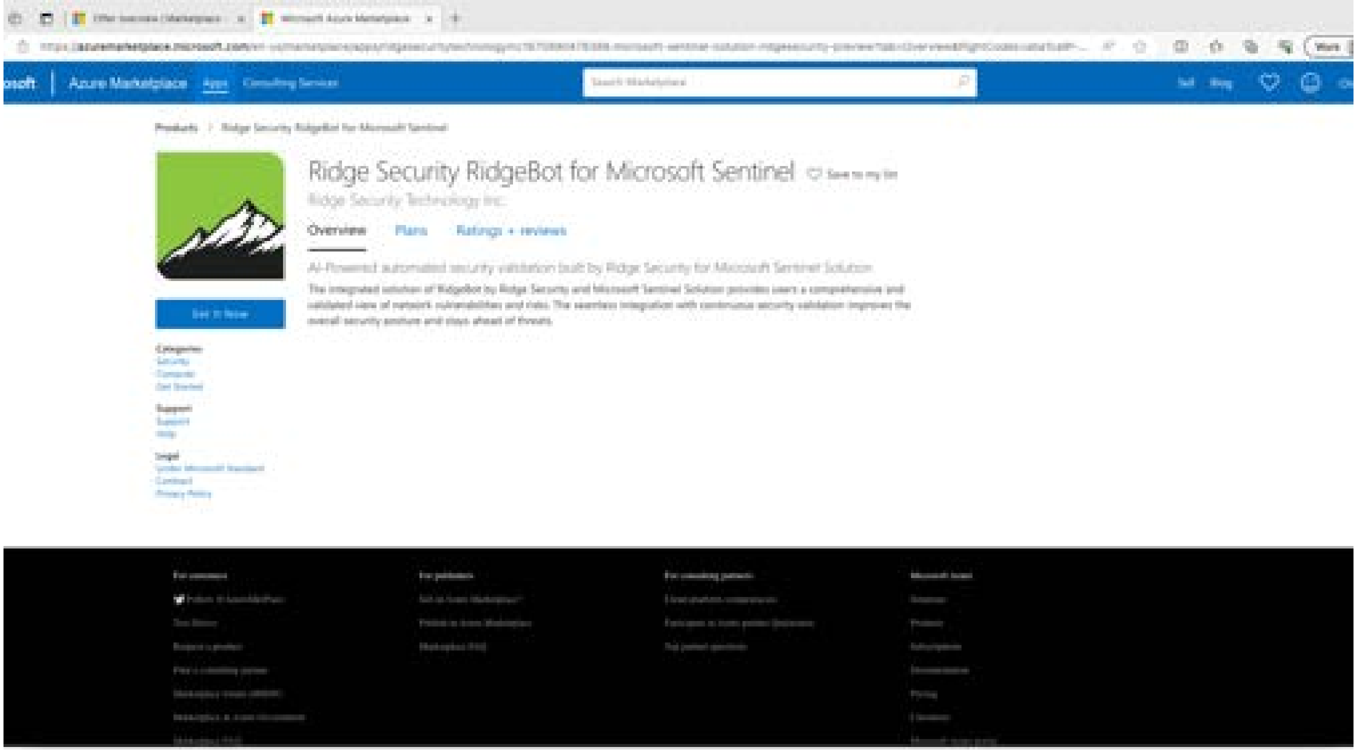
F Microsoft Sentinel with RidgeBot® quickly identifies real incidents, eliminate false positives, and allow all security tools to actively participate in a coordinated streamlined threat intelligence strategy.

Joint Solution Integration

The Ridge Security RidgeBot® and Microsoft Sentinel integrated solution provides users with a comprehensive, validated and always up-to-date view of network vulnerabilities and risks. The seamless integration of continuous security validation improves your overall security posture and lets you stay ahead of established and emerging threats.

After onboarding Microsoft Sentinel into your workspace, using the various data connectors allows you to start ingesting all your security data into Microsoft Sentinel for a comprehensive view of vulnerabilities and risks. Microsoft Sentinel provides numerous out-of-the-box connectors which integrate in real time. The Ridge Security RidgeBot® data connector facilitates automated interactions—such as creating and executing penetration testing tasks, and digesting the resulting logs—between a Ridge Security RidgeBot® server and Microsoft Sentinel SIEM.

Access the RidgeBot® data connector for Microsoft Sentinel as shown below.

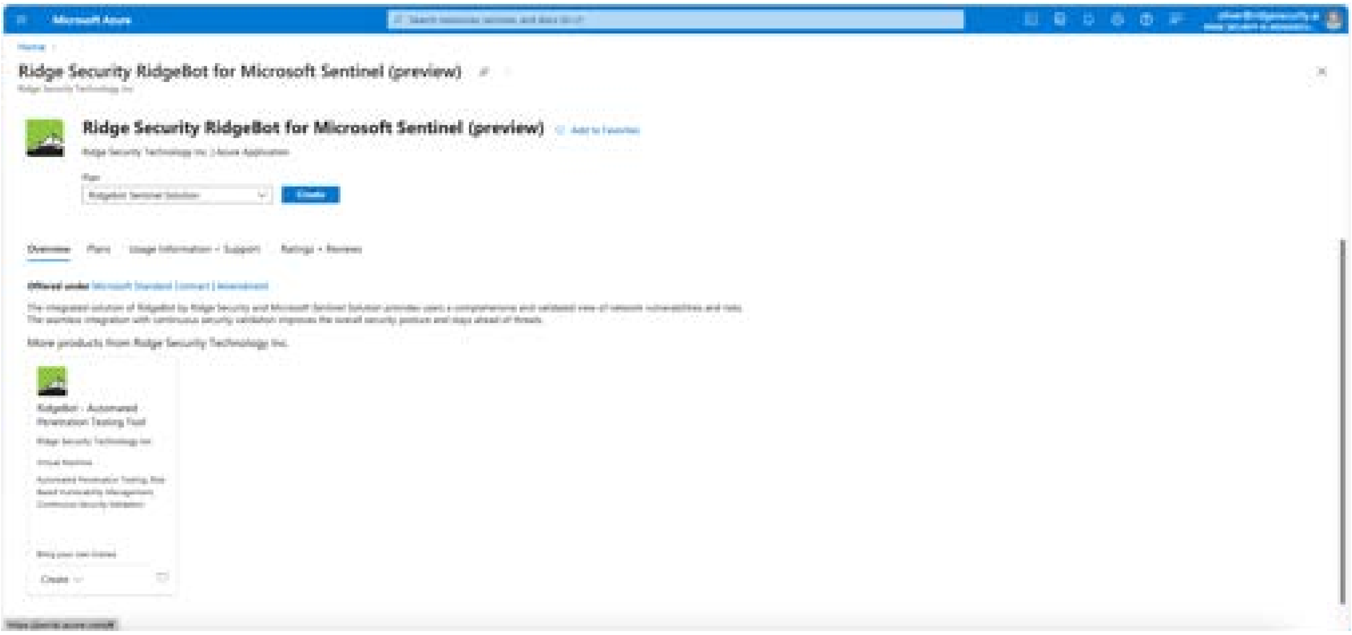


Ridge Security RidgeBot for Microsoft Sentinel

Ridge Security Technology Inc.

AI-Powered automated security validation built by Ridge Security for Microsoft Sentinel Solution

The integrated solution of RidgeBot by Ridge Security and Microsoft Sentinel Solution provides users a comprehensive and validated view of network vulnerabilities and risks. The seamless integration with continuous security validation improves the overall security posture and stays ahead of threats.



Microsoft Azure

Home >

Ridge Security RidgeBot for Microsoft Sentinel (preview)

Ridge Security Technology Inc

Ridge Security RidgeBot for Microsoft Sentinel (preview)

Ridge Security Technology Inc. | Azure Application

Plan

RidgeBot Sentinel Solution

Offered under Microsoft Standard Contract | Amendment

The integrated solution of RidgeBot by Ridge Security and Microsoft Sentinel Solution provides users a comprehensive and validated view of network vulnerabilities and risks. The seamless integration with continuous security validation improves the overall security posture and stays ahead of threats.

More products from Ridge Security Technology Inc.

RidgeBot - Automated Penetration Testing Tool

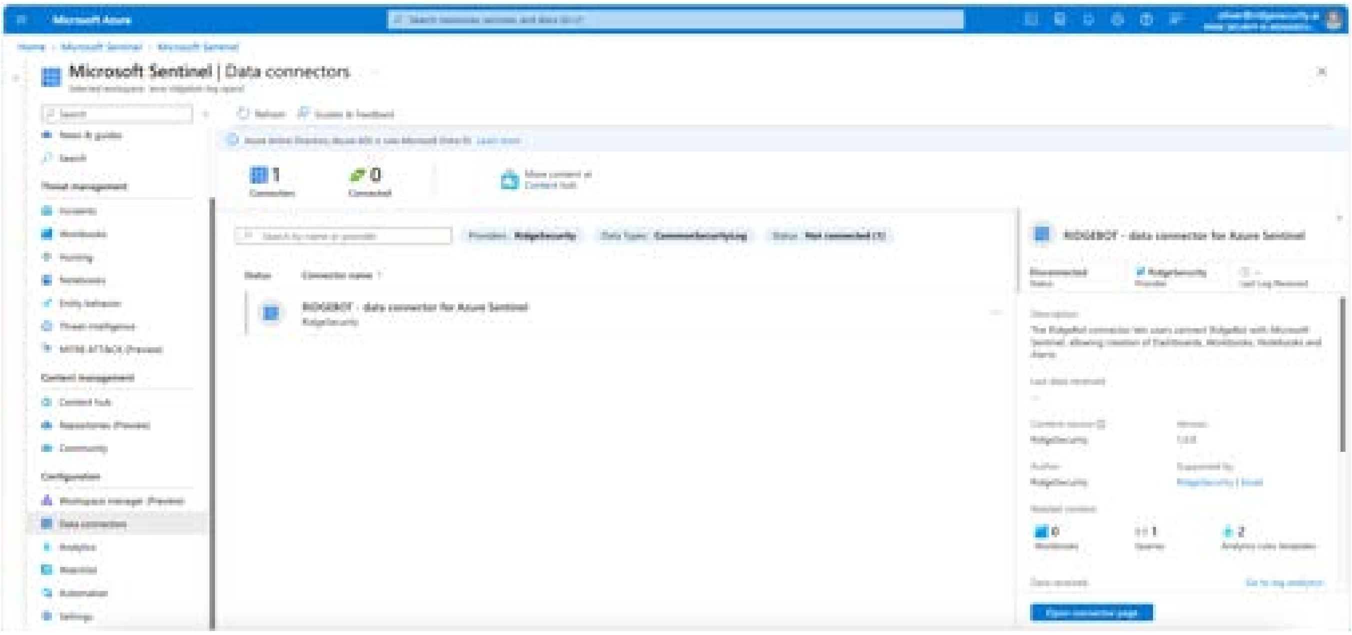
Ridge Security Technology Inc

Virtual Machine

Automated Penetration Testing, Risk Based Vulnerability Management, Continuous Security Validation

Bring your own license

The RidgeBot® data connector now shows up in your Microsoft Sentinel interface by navigating to “Data connectors” on the left-hand panel, as shown below.



Microsoft Azure

Home > Microsoft Sentinel > Microsoft Sentinel

Microsoft Sentinel | Data connectors

1 Connectors

0 Connected

More content at Content hub

Providers : RidgeSecurity

Data Types : CommonSecurityLog

Status : Not connected (1)

Status	Connector name ↑
	RIDGEBOT - data connector for Azure Sentinel RidgeSecurity

RIDGEBOT - data connector for Azure Sentinel

Disconnected
Status

RidgeSecurity
Provider

--
Last Log Received

Description

The RidgeBot connector lets users connect RidgeBot with Microsoft Sentinel, allowing creation of Dashboards, Workbooks, Notebooks and Alerts.

Last data received

--

Content source: RidgeSecurity

Version: 1.0.0

Author: RidgeSecurity

Supported by: RidgeSecurity | Email

Related content

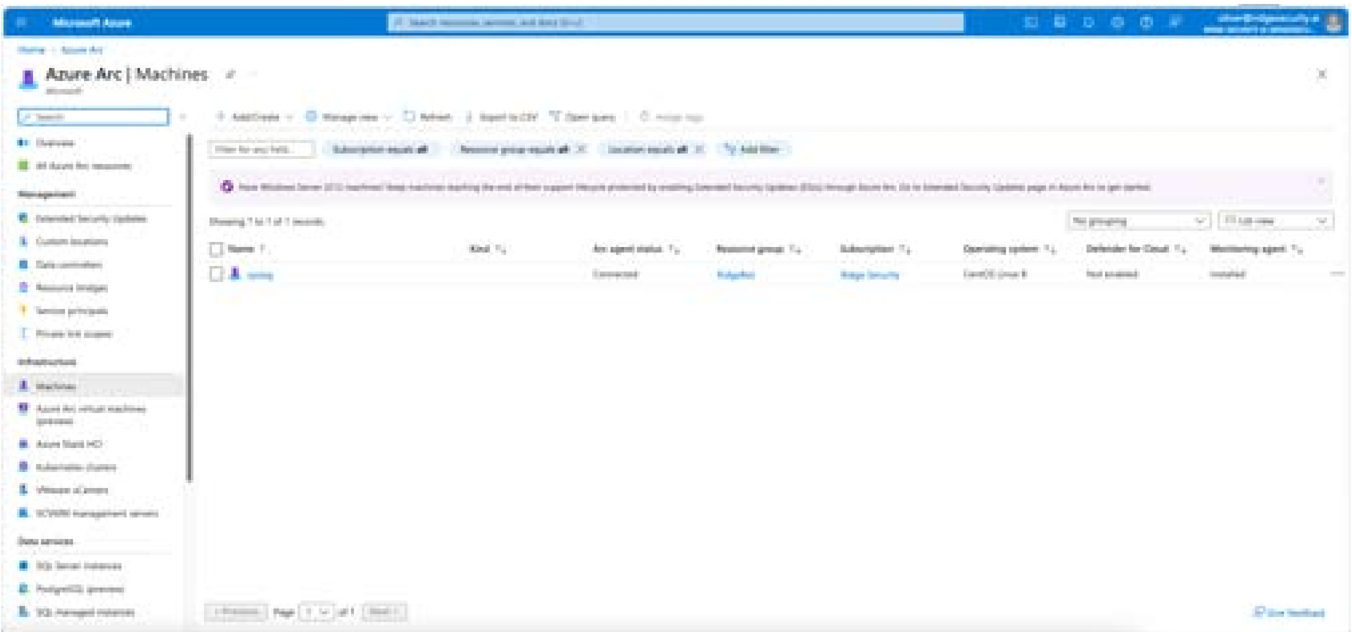
0 Workbooks

1 Queries

2 Analytics rules templates

Data received

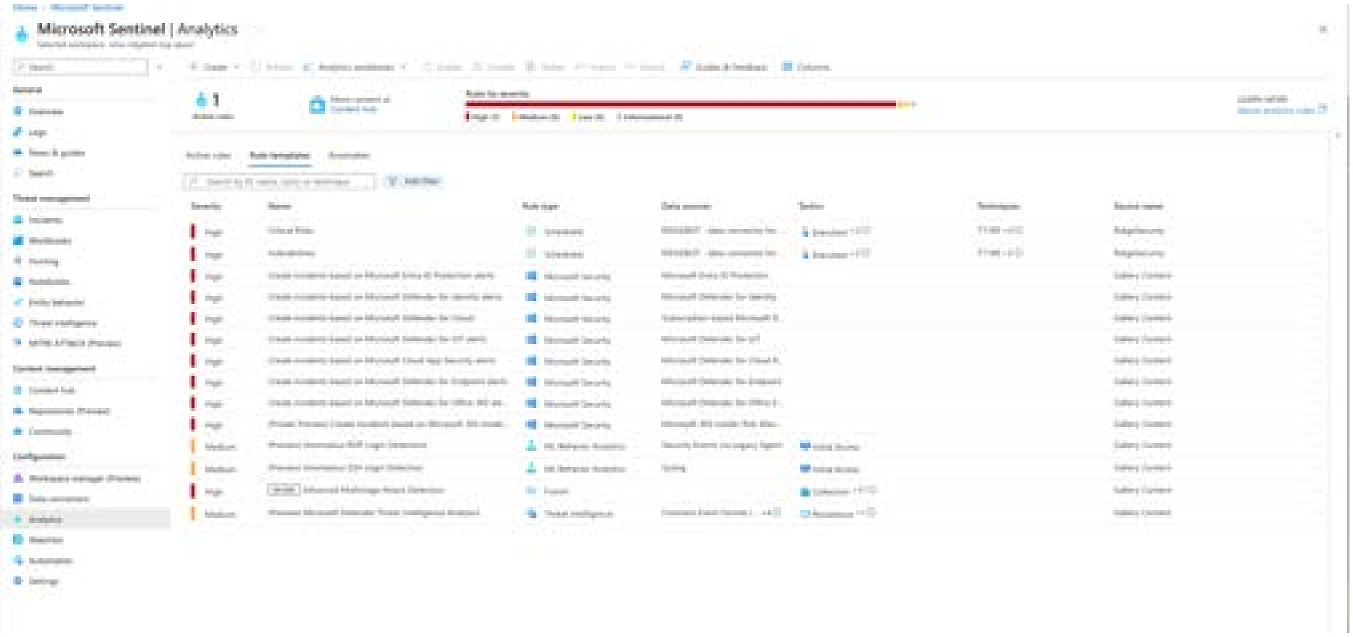
The RidgeBot® syslog server shows up in your Microsoft Sentinel interface by navigating to “Machines” on the left-hand panel, as shown below.



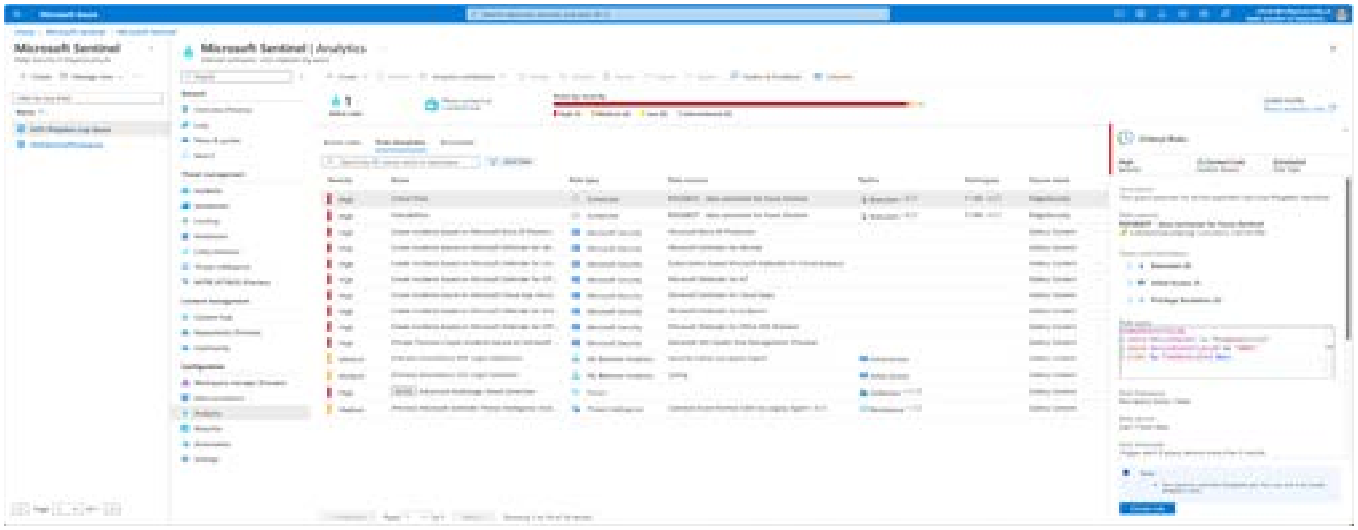
Showing 1 to 1 of 1 records.

Name	Kind	Arc agent status	Resource group	Subscription	Operating system	Defender for Cloud	Monitoring agent
syslog		Connected	RidgeBot	Ridge Security	CentOS Linux 8	Not enabled	Installed

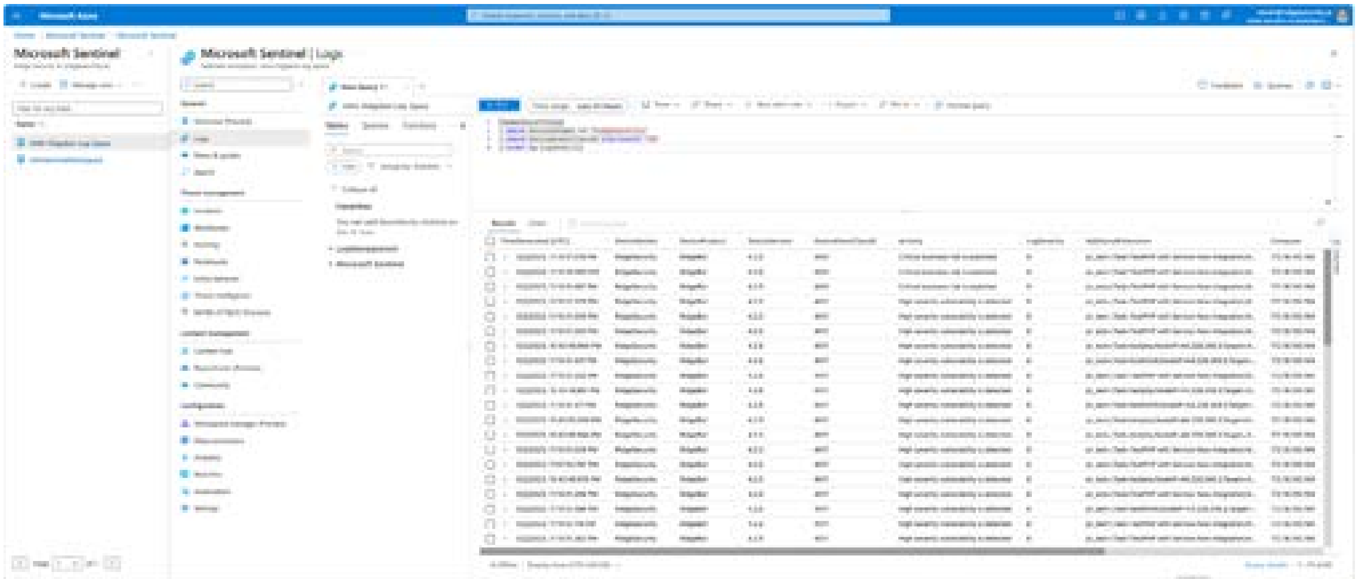
Schedule and view RidgeBot® penetration tasks from the Microsoft Sentinel interface by navigating to “Analytics” on the left-hand panel, as shown below.



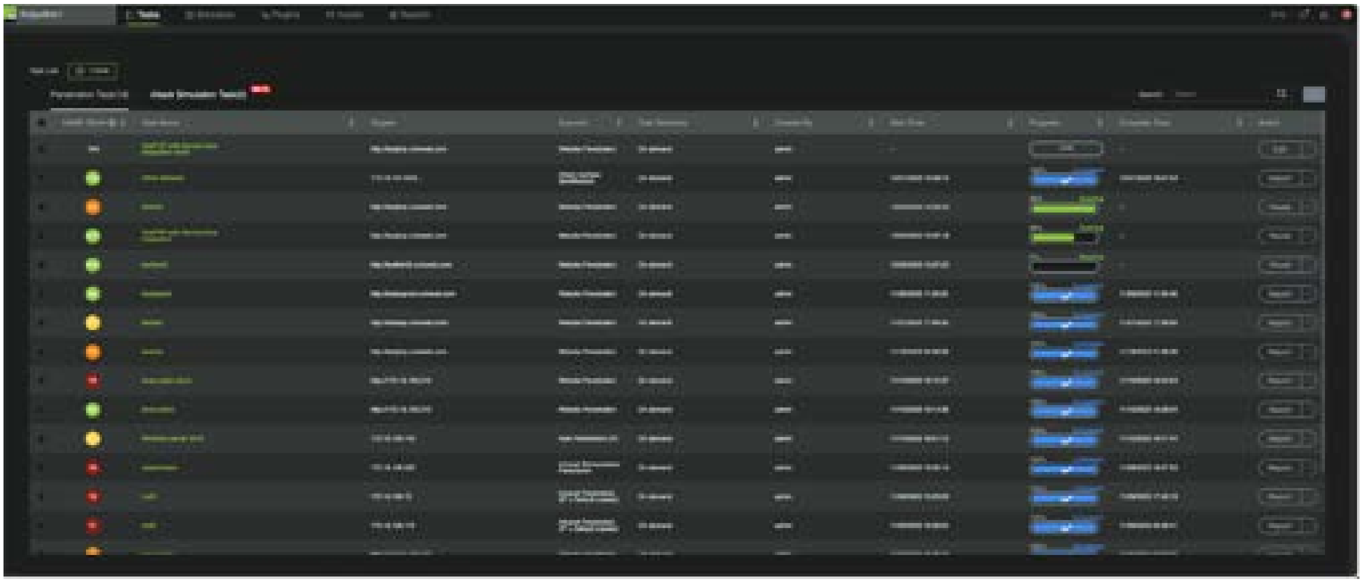
Severity	Name	Rule type	Data sources	Tactics	Techniques	Source name
High	Critical Risks	Scheduled	RIDGEBOT - data connector for ...	Execution +2	T1190 +2	RidgeSecurity
High	Vulnerabilities	Scheduled	RIDGEBOT - data connector for ...	Execution +2	T1190 +2	RidgeSecurity
High	Create incidents based on Microsoft Entra ID Protection alerts	Microsoft Security	Microsoft Entra ID Protection			Gallery Content
High	Create incidents based on Microsoft Defender for Identity alerts	Microsoft Security	Microsoft Defender for Identity			Gallery Content
High	Create incidents based on Microsoft Defender for Cloud	Microsoft Security	Subscription-based Microsoft D...			Gallery Content
High	Create incidents based on Microsoft Defender for IoT alerts	Microsoft Security	Microsoft Defender for IoT			Gallery Content
High	Create incidents based on Microsoft Cloud App Security alerts	Microsoft Security	Microsoft Defender for Cloud A...			Gallery Content
High	Create incidents based on Microsoft Defender for Endpoint alerts	Microsoft Security	Microsoft Defender for Endpoint			Gallery Content
High	Create incidents based on Microsoft Defender for Office 365 al...	Microsoft Security	Microsoft Defender for Office 3...			Gallery Content
High	(Preview) Create incidents based on Microsoft 365 Insider...	Microsoft Security	Microsoft 365 Insider Risk Man...			Gallery Content
Medium	(Preview) Anomalous RDP Login Detections	ML Behavior Analytics	Security Events via Legacy Agent	Initial Access		Gallery Content
Medium	(Preview) Anomalous SSH Login Detection	ML Behavior Analytics	Syslog	Initial Access		Gallery Content
High	IN USE Advanced Multistage Attack Detection	Fusion		Collection +11		Gallery Content
Medium	(Preview) Microsoft Defender Threat Intelligence Analytics	Threat Intelligence	Common Event Format (... +4	Reconnaissance +11		Gallery Content



View RidgeBot® task results from the Microsoft Sentinel interface by navigating to “Logs” on the left-hand panel, as shown below.



Penetration task status can also be viewed from the RidgeBot® interface as shown below.



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.