Purple Team Assessment

The Purple Team Assessment Overview

Skyhawk Security AI-based Autonomous Purple Team

Continuous Proactive Protection continuously analyzes customer cloud infrastructure, proactively runs attack simulation against it and uses the results to expose the attack surface, validated automated response and remediation recommendations to ensure the cloud has the most up to date security defenses in place. This continuous protection process includes learning and automated adaptation of threat detection methods. This enables security teams to take a proactive and adaptive approach to their security strategy for the very first time.

Why do we call this the Purple Team?

Skyhawk Security's Continuous Proactive Protection has several capabilities, and the key capabilities are centered around the AI-based Red Team and AI-based Blue Team. Leveraging a AI-based Simulation Twin, Skyhawk can identify where there are gaps in your cloud security and then prioritize those based on the business value of the asset behind the vulnerability. This approach, termed "Exposure Hunting," replaces traditional threat hunting by identifying exposures before they evolve into threats or incidents, thereby preventing cloud breaches.

What is the assessment?

Skyhawk Security will evaluate how vulnerable your most precious data assets, or crown jewels, are. It will leverage all the log files and telemetry data that you provide to it and analyze that information. It will map out the paths to your most precious data assets, the crown jewels, and then show the least resistant path(s) to those assets.

How can can I get started?

In just one hour the environment is onboarded and then it is confirmed the platform is receiving the appropriate data for analysis. Beyond the initial onboarding, no further settings or configurations are needed, making it a zero-touch process.

What will you get?

A comprehensive report is produced detailing your risk and exposure to your crown jewels, including weaponized exposures, critical and prioritized vulnerabilities, and attack vector permutations to your business critical crown jewels. These verified security issues will be prioritized by the business value of the asset behind it as well as by remediation's prevention effectiveness, namely the impact of how many attack vectors will be addressed by each remediation step. For example, fixing one security issue will eliminate dozens of different vectors to access your precious business data. The report also provides evidence of security posture, which is incredibly valuable when preparing for SOC 2 audits and communicating risk to stakeholders.

Finally, the report will include an executive summary and what steps should be taken to improve the security of your cloud. It will point to the technical details that were used to form these conclusions and recommendations.

About Skyhawk Security

Skyhawk Security is the leader in Purple Team-Powered CDR, leveraging a multi-layer AI-based approach to identify and stop cloud threats before they become breaches. Skyhawk revolutionizes CDR with its Continuous Proactive Protection, an AI-powered Autonomous Purple Team, enabling security teams to take a proactive approach to cloud security for the very first time. Led by a team of cyber security and cloud professionals who built the original CSPM category, Skyhawk's platform evolves cloud security posture management far beyond scanning and static configuration analysis, continuously adapting and improving threat detection so that it is always aligned with cloud architecture. Skyhawk Security is a spin-off of Radware® (NASDAQ:RDWR).

Skyhawk Purple Team Assessment
Workflow and Technical Requirements

1. Schedule 1 hour assessment onboarding meeting with Skyhawk

Meeting Agenda

a. Review (short demo refresh) Skyhawk Purple Team

b. Provide access to Skyhawk Portal for cloud account onboarding for the assessment

   1. Skyhawk engineer to gather the following information prior to the initial 1 hour meeting:

      i. Customer name

      ii. Customer Lead email address

c. Customer verifies login to portal

d. Customer walk-thru to onboard cloud account with Skyhawk Engineer (technical requirements detail in the following section). If a vulnerability scanner is in use, we will onboard it for vulnerabilities to be included in the assessment.

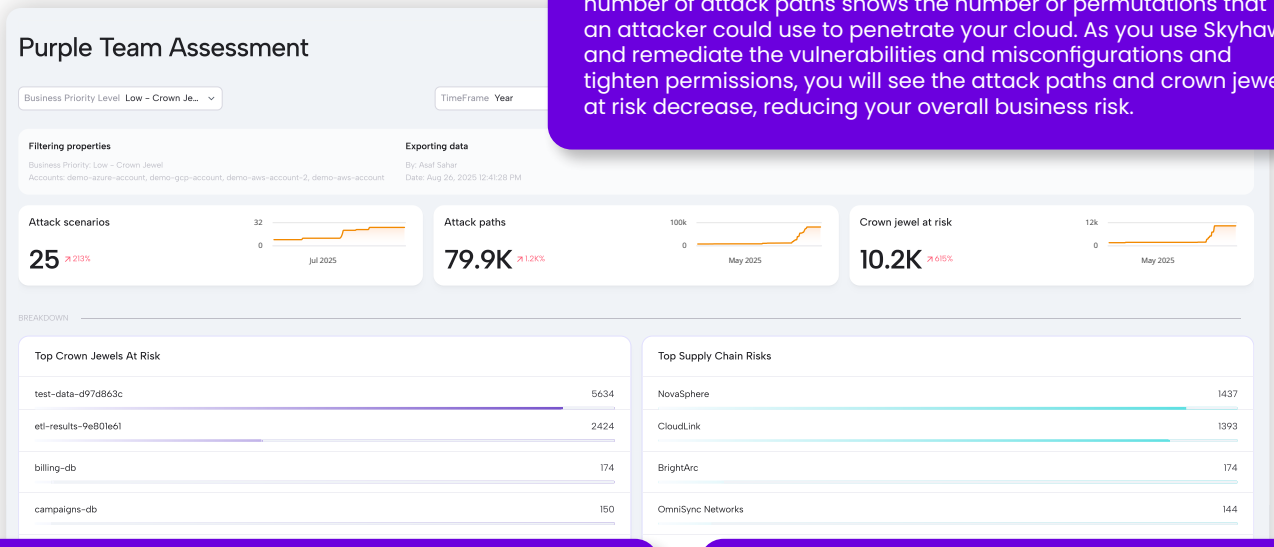
e. Skyhawk engineer verifies successful onboarding and schedules follow up meeting to review Purple Team Assessment Results

Technical onboarding requirements and steps:

The Technical requirements for onboarding are minimal. Read only access to your cloud accounts is needed to onboard and ensure the platform is recieving the appropriate data for analysis. Beyond the intial onboarding, no further settings or confiurations are needed, making it a zero-touch process. This allows your team to continue with regular activities without significant interruption.

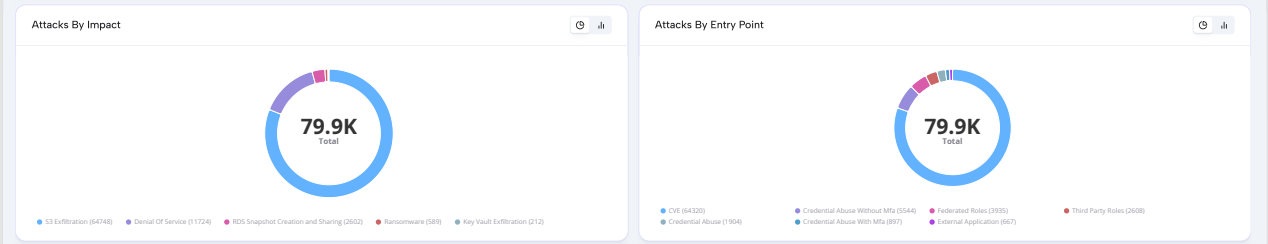
Purple Team Assessment Report

These are the top metrics in the report and give you an overview of your current cloud security. The trends in this report show an increase in attack scenarios and crown jewels at risk, which is not good and indicated by the red increases noted in each box. The number of attack paths shows the number or permutations that an attacker could use to penetrate your cloud. As you use Skyhawk and remediate the vulnerabilities and misconfigurations and tighten permissions, you will see the attack paths and crown jewels at risk decrease, reducing your overall business risk.

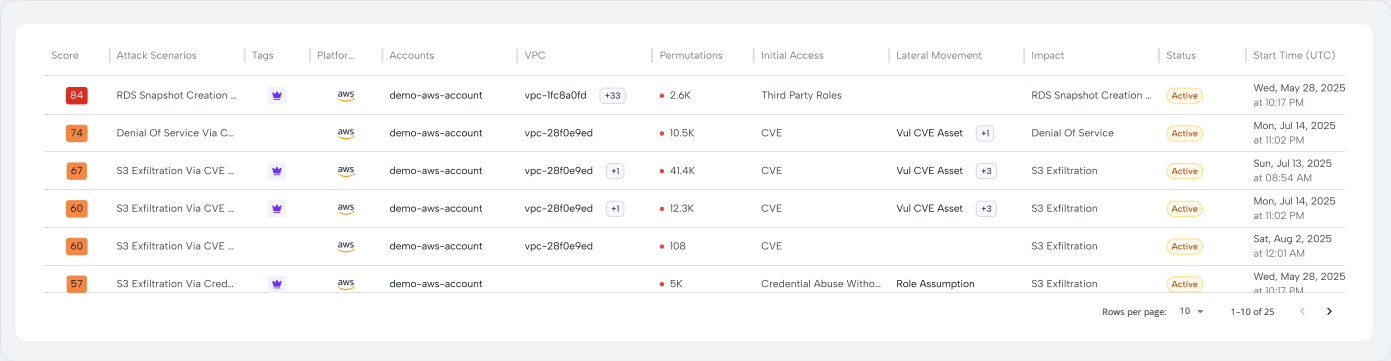


Here you can see the different analysis that is performed by the report. The top crown jewels at risk, you can understand the assets that could impose the most damage. At the top supply chain, you can see which of your 3rd parties are exposing you to risk. The impact type, you can see what type of asset would be affected and attacks by entry point shows you here you have a lot of CVEs, you can see the common entry point to the environment.

These are a list of attack scenarios and you can see which ones the score takes into account all the risk attributes of the scenario. The highest risk issues should be resolved first. It takes into account permutations, assets at risk, potential damage and the likelihood that the damage would occur. Type of asset, how complex it is to do the initial access. CVE – much higher likelihood to happen.



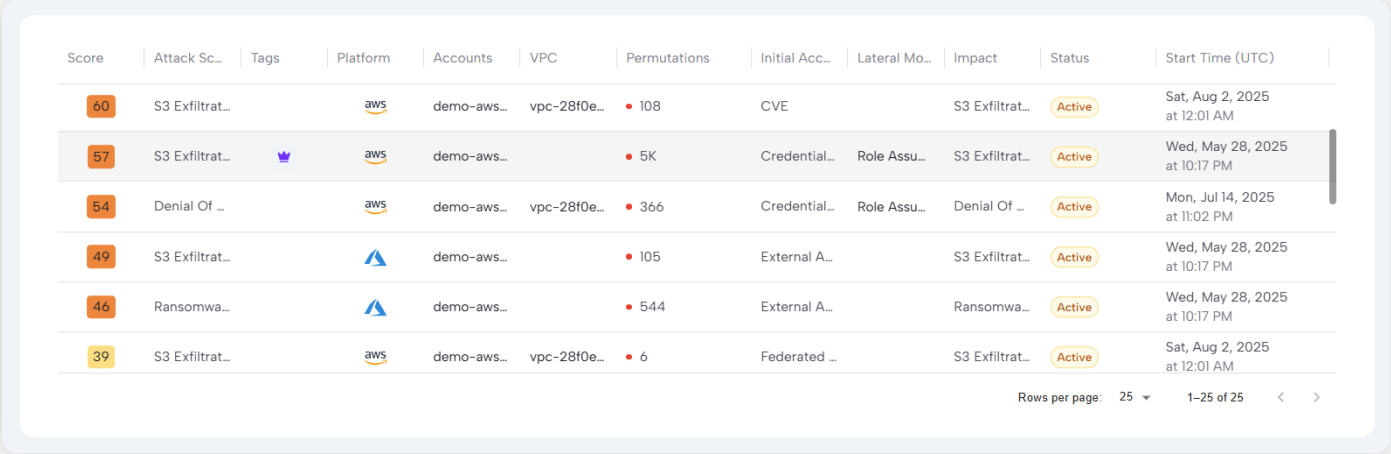
These charts show the entry points which are responsible for the most attacks and the distribution of impacts, data exfiltration, ransomare, and others. This demonstrates to security teams what is the most likely attack they will see in their cloud.



Score	Attack Scenarios	Tags	Platfor...	Accounts	VPC	Permutations	Initial Access	Lateral Movement	Impact	Status	Start Time (UTC)
84	RDS Snapshot Creation ...		aws	demo-aws-account	vpc-1fc8a0fd +33	2.6K	Third Party Roles		RDS Snapshot Creation ...	Active	Wed, May 28, 2025 at 10:17 PM
74	Denial Of Service Via C...		aws	demo-aws-account	vpc-28f0e9ed	10.5K	CVE	Vul CVE Asset +1	Denial Of Service	Active	Mon, Jul 14, 2025 at 11:02 PM
67	S3 Exfiltration Via CVE ...		aws	demo-aws-account	vpc-28f0e9ed +1	41.4K	CVE	Vul CVE Asset +3	S3 Exfiltration	Active	Sun, Jul 13, 2025 at 08:54 AM
60	S3 Exfiltration Via CVE ...		aws	demo-aws-account	vpc-28f0e9ed +1	12.3K	CVE	Vul CVE Asset +3	S3 Exfiltration	Active	Mon, Jul 14, 2025 at 11:02 PM
60	S3 Exfiltration Via CVE ...		aws	demo-aws-account	vpc-28f0e9ed	108	CVE		S3 Exfiltration	Active	Sat, Aug 2, 2025 at 12:01 AM
57	S3 Exfiltration Via Cred...		aws	demo-aws-account		5K	Credential Abuse Witho...	Role Assumption	S3 Exfiltration	Active	Wed, May 28, 2025 at 10:17 PM

Rows per page: 10 1–10 of 25

Here we can see the prioritization of risk by the risk score, a higher number is a higher risk. This sample listing of each scenario shows what assets will be impacted and which weakness in the attack surface exposes the asset. Each of these represent a simulated attack and what would happen, the data that was compromised and the entry point that was manipulated. Please note: The Status Column shows how many paths there are to this asset. Most here have 30, which means there are 30 variations in the attack path for the threat actor to leverage to gain access to the asset. These scenarios will be updated daily to reflect changes in your cloud account and cloud security. As the attack surface exposure is reduced, you will see the number in the "Status" column decrease, indicating there are fewer attack paths for the threat actor to leverage to compromise this asset.

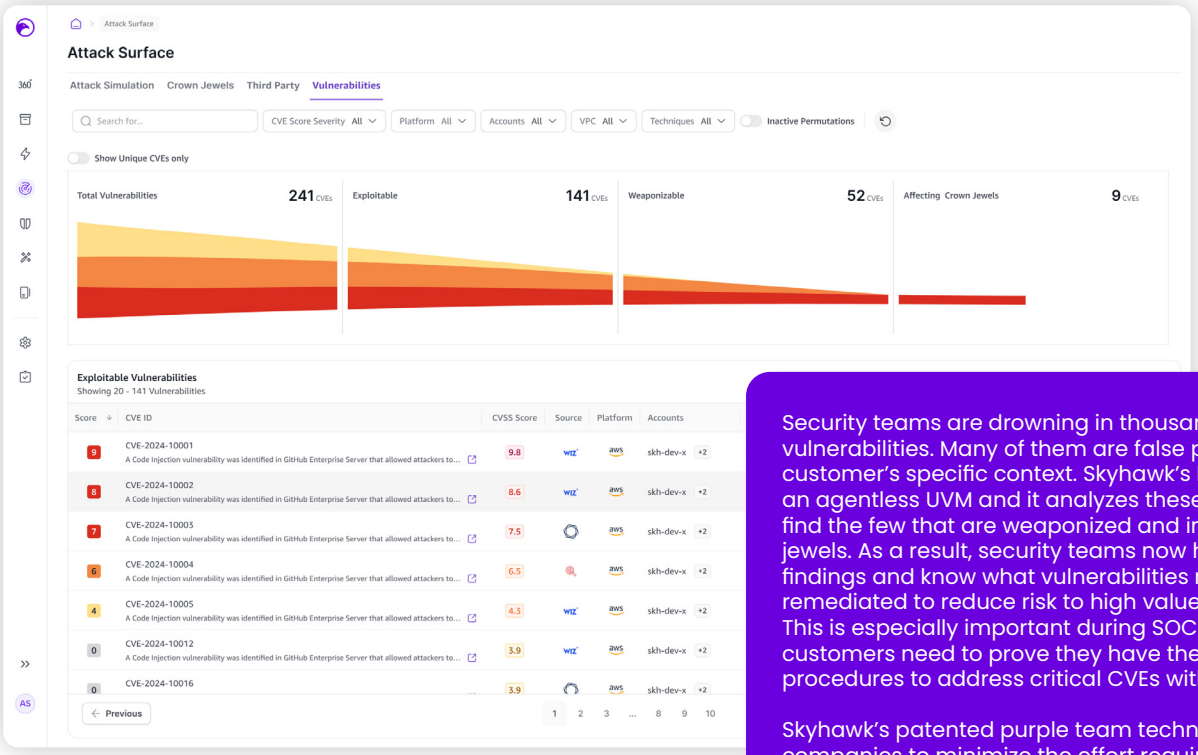


Score	Attack Sc...	Tags	Platform	Accounts	VPC	Permutations	Initial Acc...	Lateral Mo...	Impact	Status	Start Time (UTC)
60	S3 Exfiltrat...		aws	demo-aws...	vpc-28f0e...	108	CVE		S3 Exfiltrat...	Active	Sat, Aug 2, 2025 at 12:01 AM
57	S3 Exfiltrat...		aws	demo-aws...		5K	Credential...	Role Assu...	S3 Exfiltrat...	Active	Wed, May 28, 2025 at 10:17 PM
54	Denial Of ...		aws	demo-aws...	vpc-28f0e...	366	Credential...	Role Assu...	Denial Of ...	Active	Mon, Jul 14, 2025 at 11:02 PM
49	S3 Exfiltrat...		azure	demo-aws...		105	External A...		S3 Exfiltrat...	Active	Wed, May 28, 2025 at 10:17 PM
46	Ransomwa...		azure	demo-aws...		544	External A...		Ransomwa...	Active	Wed, May 28, 2025 at 10:17 PM
39	S3 Exfiltrat...		aws	demo-aws...	vpc-28f0e...	6	Federated ...		S3 Exfiltrat...	Active	Sat, Aug 2, 2025 at 12:01 AM

Rows per page: 25 1–25 of 25

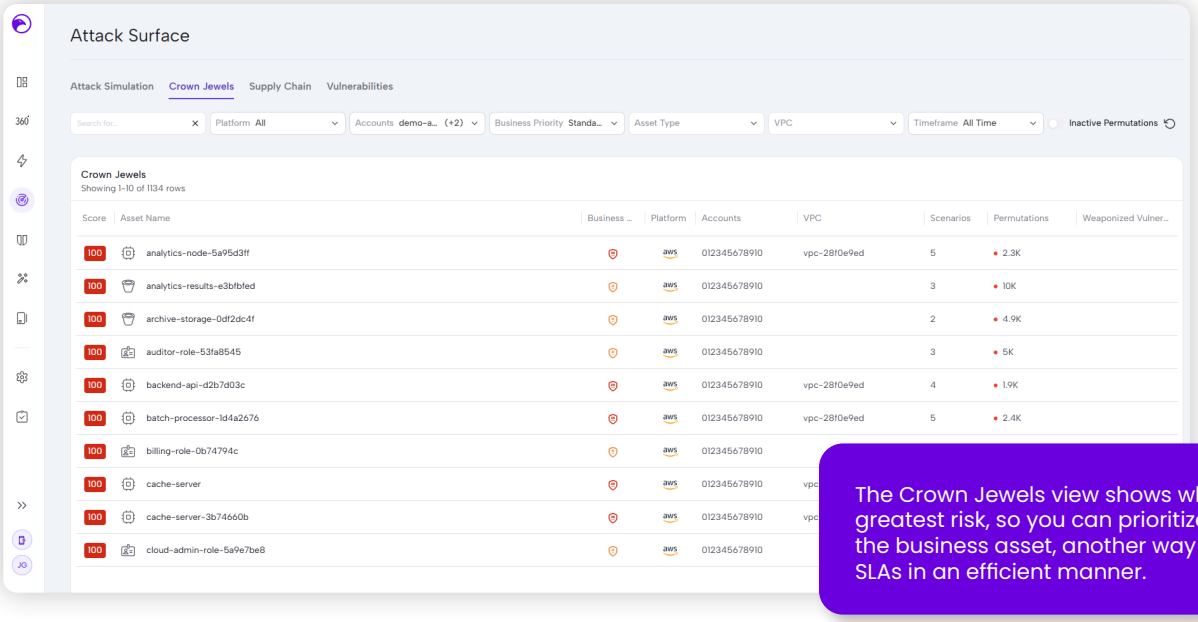
New Attack Surface and Vulnerability (UVM) Reporting

In addition to the Purple Team Assessment reports, the platform also covers vulnerabilities prioritization as well as an analysis of top crown jewels that are at risk. This information helps demonstrate to auditors that the correct cloud vulnerabilities are addressed within the company's SLA.



Security teams are drowning in thousands of vulnerabilities. Many of them are false positives in the customer's specific context. Skyhawk's Purple Team is an agentless UVM and it analyzes these vulnerabilities to find the few that are weaponized and impacting crown jewels. As a result, security teams now have actionable findings and know what vulnerabilities need to be remediated to reduce risk to high value business assets. This is especially important during SOC 2 audits, where customers need to prove they have the processes and procedures to address critical CVEs within defined SLAs.

Skyhawk's patented purple team technology allows companies to minimize the effort required to adhere to the SOC 2 SLA, with proven evidence for auditors.



The Crown Jewels view shows which are at the greatest risk, so you can prioritize remediations by the business asset, another way to adhere SOC2 SLAs in an efficient manner.

Contact us today to learn more at skyhawk.security

SKYHAWK SECURITY