SKYHAWK
SECURITY

Purple Team Assessment 2024

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.

What is the impact to your team?

The impact on your team is minimal. We require just one hour to on-board and ensure we are receiving the appropriate data for analysis. Beyond the initial onboarding, no further settings or configurations are needed, making it a zero-touch process. This allows your team to continue their regular activities without significant interruption.

What will you get?

We will create a comprehensive report, 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 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 originator of Cloud Threat Detection and Response (CDR) and Cloud Native Autonomous Purple Team, 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 the 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 AWS 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 verify login to portal

d. Customer walk-thru to onboard AWS account with Skyhawk Engineer (technical requirements detail in the following section). If AWS Inspector 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

AWS account onboarding requirements and steps:

a. To provide a Skyhawk Purple Team assessment (attack surface exposures) on a AWS account by the Skyhawk service:

   1. In the Skyhawk Onboarding wizard for AWS, we will complete the setup as follows:

      i. Create a cross-account role in your AWS account to allow access from Skyhawk's AWS account (Skyhawk account information provided in the onboarding wizard).

      ii. Attach the required Identity and Access Management (IAM) permission policies to the role.

   2. The following permission policies are required for Skyhawk to collect configuration metadata:

      i. SecurityAudit policy—An AWS-managed policy provided out-of-the-box. This policy grants access to read security configuration metadata, such as information about the configuration of users, servers, databases, and more. For details, see AWS security configuration policy definition.

      ii. AWSWAFReadOnlyAccess policy—An AWS-managed policy provided out-of-the-box. This policy provides read-only access to AWS WAF configuration metadata. For more information, see AWS read-only access policy definition

   3. Connect your account to the Skyhawk service.

   4. If AWS Inspector is being used, we will utilize the built-in integration wizard after the AWS account is onboarded.

   5. Notes: Skyhawk cannot make changes directly to your AWS account. You do not need to install agents or deploy any additional software to your cloud for Skyhawk Purple Team to assess your account.

2. Schedule 1 hour assessment results review meeting with Skyhawk

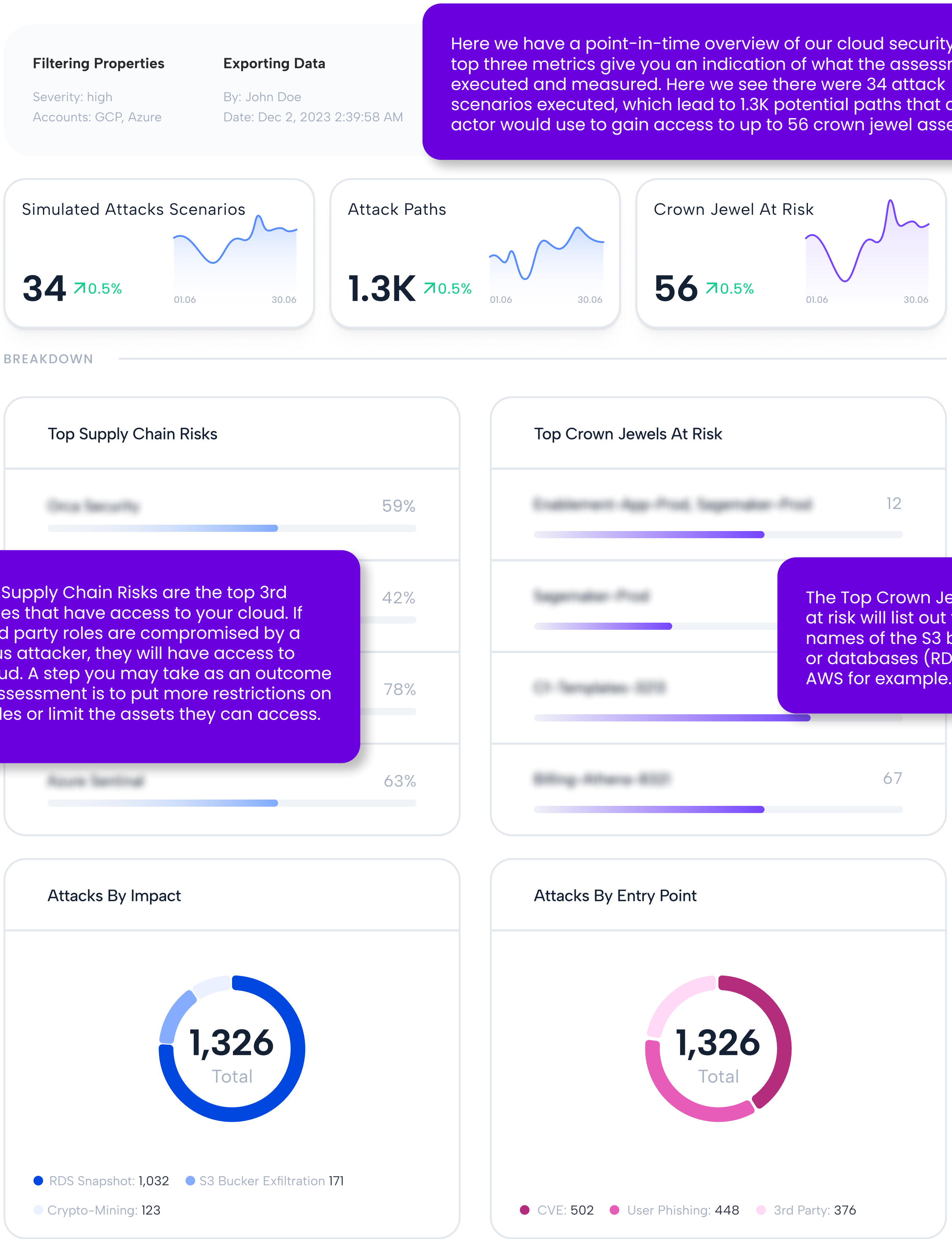
a. Skyhawk will walk-thru and review in detail the Purple Team results with the Customer Team

b. Skyhawk will review the Purple Team Assessment report with the customer team

c. Note: The results review meeting may require 2 meetings depending on the number of results to review along with fully addressing all questions raised.

3. Skyhawk will provide the Purple Team Assessment final report which we will create, the report details 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.

Purple Team Assessment Report



Filtering Properties

Severity: high
Accounts: GCP, Azure

Exporting Data

By: John Doe
Date: Dec 2, 2023 2:39:58 AM

Here we have a point-in-time overview of our cloud security. These top three metrics give you an indication of what the assessment executed and measured. Here we see there were 34 attack scenarios executed, which lead to 1.3K potential paths that a threat actor would use to gain access to up to 56 crown jewel assets.

Simulated Attacks Scenarios

34 ↗0.5%

Attack Paths

1.3K ↗0.5%

Crown Jewel At Risk

56 ↗0.5%

BREAKDOWN

Top Supply Chain Risks

[redacted]	59%
	42%
	78%
[redacted]	63%

The Top Supply Chain Risks are the top 3rd party roles that have access to your cloud. If these 3rd party roles are compromised by a malicious attacker, they will have access to your cloud. A step you may take as an outcome of this assessment is to put more restrictions on these roles or limit the assets they can access.

Top Crown Jewels At Risk

[redacted]	12
[redacted]	
[redacted]	
[redacted]	67

The Top Crown Jewels at risk will list out the names of the S3 buckets or databases (RDS) in AWS for example.

Attacks By Impact

1,326
Total

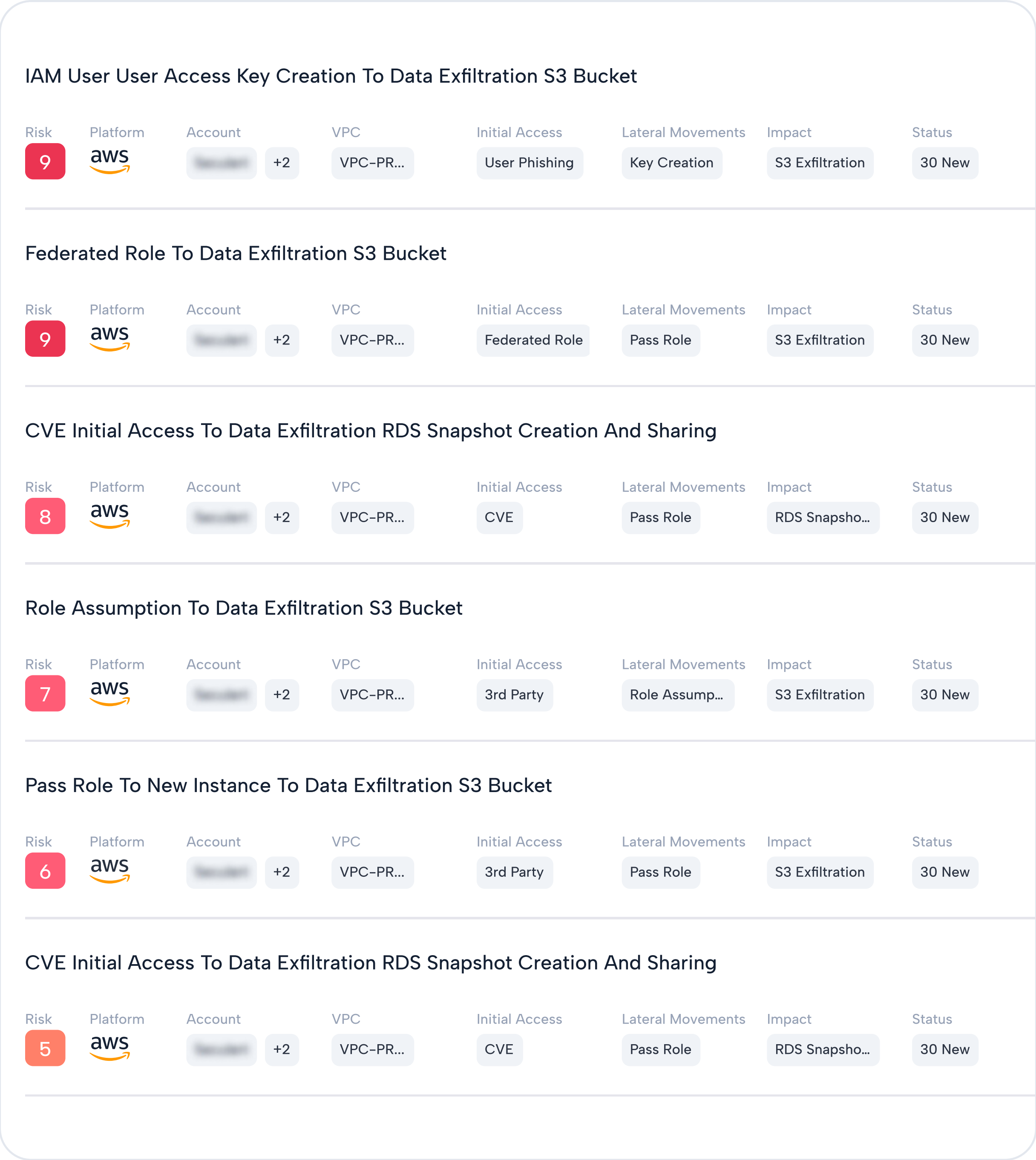
● RDS Snapshot: 1,032 ● S3 Bucker Exfiltration 171
● Crypto-Mining: 123

Attacks By Entry Point

1,326
Total

● CVE: 502 ● User Phishing: 448 ● 3rd Party: 376

These charts show the low-hanging fruit for the team to fix. For example, there are over 500 CVEs that need to be addresses as soon as possible to reduce the attack surface. Additionally, there are over 1,000 RDS Snapshots, which is almost 80% of the impacts, where most organizations store their most valuable data - and we can see they are exposed.



IAM User User Access Key Creation To Data Exfiltration S3 Bucket

Risk	Platform	Account		VPC	Initial Access	Lateral Movements	Impact	Status
9	aws	[redacted]	+2	VPC-PR...	User Phishing	Key Creation	S3 Exfiltration	30 New

Federated Role To Data Exfiltration S3 Bucket

Risk	Platform	Account		VPC	Initial Access	Lateral Movements	Impact	Status
9	aws	[redacted]	+2	VPC-PR...	Federated Role	Pass Role	S3 Exfiltration	30 New

CVE Initial Access To Data Exfiltration RDS Snapshot Creation And Sharing

Risk	Platform	Account		VPC	Initial Access	Lateral Movements	Impact	Status
8	aws	[redacted]	+2	VPC-PR...	CVE	Pass Role	RDS Snapsho...	30 New

Role Assumption To Data Exfiltration S3 Bucket

Risk	Platform	Account		VPC	Initial Access	Lateral Movements	Impact	Status
7	aws	[redacted]	+2	VPC-PR...	3rd Party	Role Assump...	S3 Exfiltration	30 New

Pass Role To New Instance To Data Exfiltration S3 Bucket

Risk	Platform	Account		VPC	Initial Access	Lateral Movements	Impact	Status
6	aws	[redacted]	+2	VPC-PR...	3rd Party	Pass Role	S3 Exfiltration	30 New

CVE Initial Access To Data Exfiltration RDS Snapshot Creation And Sharing

Risk	Platform	Account		VPC	Initial Access	Lateral Movements	Impact	Status
5	aws	[redacted]	+2	VPC-PR...	CVE	Pass Role	RDS Snapsho...	30 New

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.

Contact us today to learn more at skyhawk.security

Skyhawk 2024 © All rights reserved.