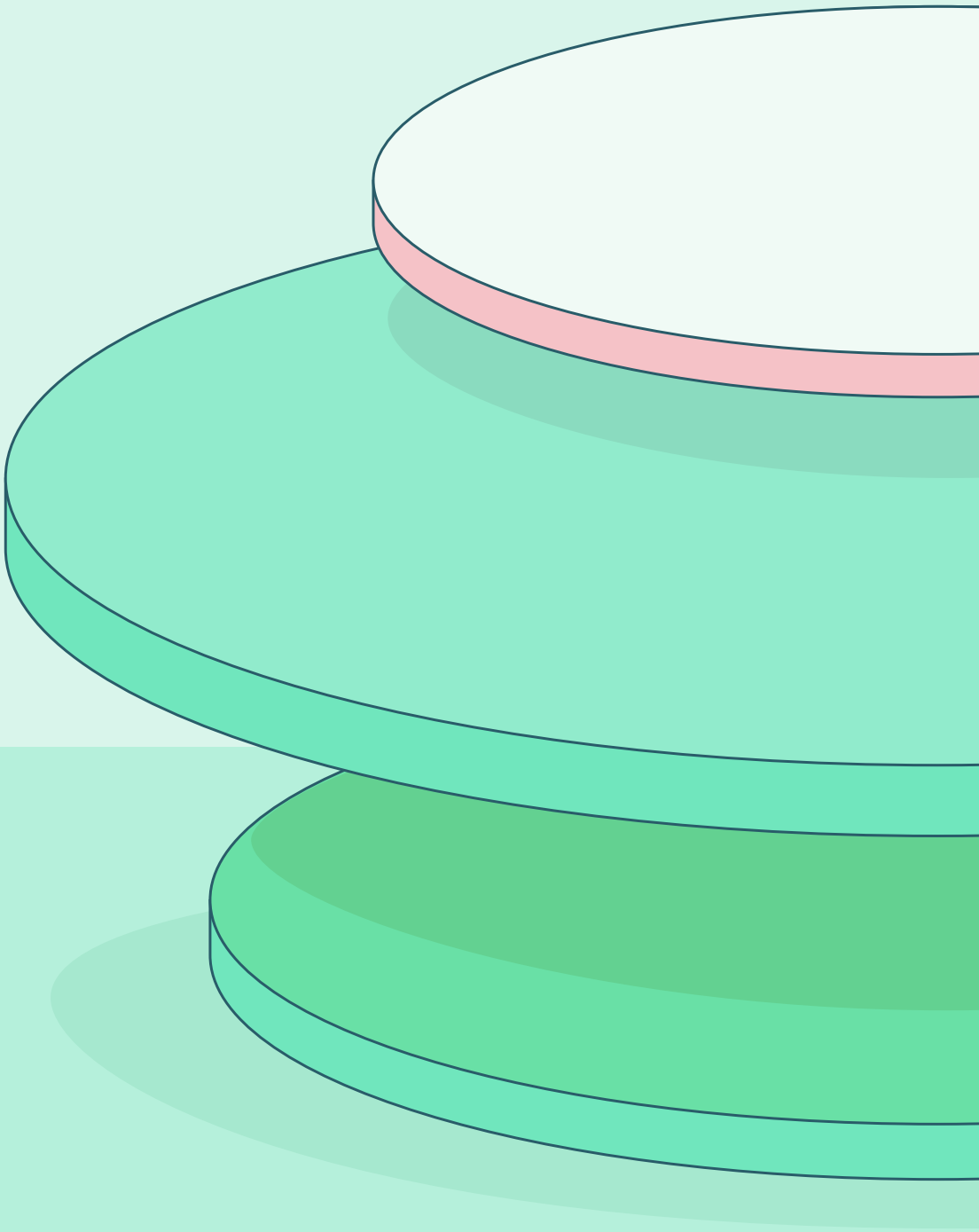
VULCAN.



Q2 2024

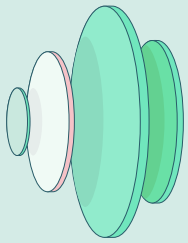
Vulnerability Watch

Quarterly trends, themes and insights from the world of cyber security vulnerabilities

VOYAGER18

Table of contents

Introduction



This report highlights significant vulnerabilities identified in the second quarter of 2024. Updated through July 1st, it describes the possible repercussions of these vulnerabilities and provides suggestions for organizations to bolster their vulnerability risk management practices. As with previous iterations, while the report offers detailed technical information on CVEs, it also delves deeper than just the Common Vulnerability Scoring System (CVSS) severity rating by incorporating data about their Exploitability Score (EPSS) and their listing in the Cybersecurity and Infrastructure Security Agency (CISA) catalog, along with other pertinent information.

The story of Q2 2024

Q2 2024 has been turbulent. With critical data issues (as we'll see below) and an overall increase in vulnerabilities, organizations are left with major questions about how they are managing their exposure risk. As compliance standards grow tighter and threat actors grow bolder, security teams are facing some of their biggest challenges yet.

Here are just some of the trends that defined the past quarter in the world of cyber security:

NVD confusion

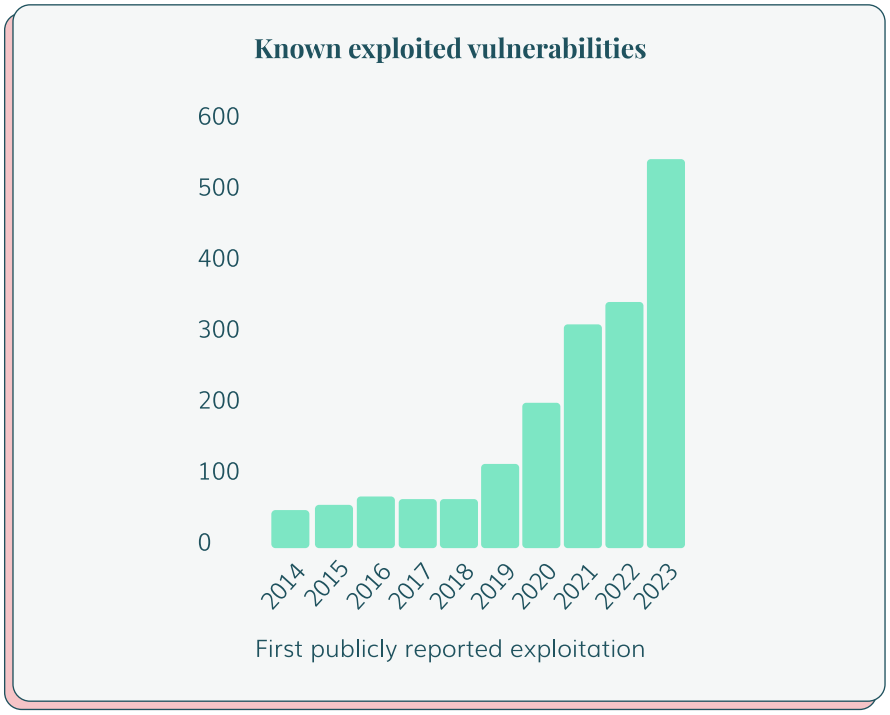
For several months, the cyber security community has grappled with significant disruptions in the National Vulnerability Database (NVD). The problems began in February when the NVD ceased enriching CVEs with essential metadata, impeding effective vulnerability tracking and response. A flawed system upgrade in May compounded these issues, causing delays in vulnerability assessments and increasing the risk of exploitation.

The resultant confusion and operational inefficiencies led to the formation of a new consortium aimed at stabilizing the NVD. This initiative underscores the critical importance of reliable, timely vulnerability data for maintaining robust exposure risk defenses. The cyber security sector now faces an urgent need to restore trust and functionality in the NVD to support global security efforts.

Given the ongoing issues with NVD data, this quarter's report contains severity scores based on CVSS v3 and third-party estimates where necessary.

Mounting data concerns

Over 10,000 CVEs were discovered in Q2 2024[1], an increase of more than 3,000 from the previous quarter. In addition, the general increase in known exploited vulnerabilities[2] over the past decade provides ominous context for exposure risk management professionals:



Considering also the relentless adoption of AI, cloud infrastructures, and other emerging technologies, the message becomes clear: The data is compounding and the attack surface widening. Meanwhile, implementing an increasingly large stack of security tools and scanners means that security teams are facing environments that are fast growing out of their control.

This was a narrative driven home time and again during May's RSA conference, where we heard from multiple partners and attendees that data overload had become one of the critical concerns of 2024.

[1] https://www.cvedetails.com/browse-by-date.php

[2] Patrick Garrity, the CyberRisk Summit, June 2024

In focus: Breaches of Q2 2024

Over the past three months, several organizations experienced significant breaches of their data. Below, we explore two of the most significant:

CDK cyber attack

In June 2024, CDK Global, a major SaaS provider for automotive dealerships, suffered two severe cyber attacks. These attacks forced the company to shut down its systems, impacting thousands of dealerships across North America. The breaches involved phishing, lateral movement, privilege escalation, and ransomware deployment.

The attacks highlight the need for robust cyber security measures, including regular system updates, employee training, advanced threat detection, and secure backups. The incidents underscore the vulnerabilities in interconnected digital infrastructures and the importance of proactive security strategies.

Snowflake breach

In June 2024[3], Snowflake experienced a significant data breach. The breach, attributed to compromised user credentials rather than inherent vulnerabilities in Snowflake's systems, affected high-profile clients like Santander Bank and Ticketmaster, compromising millions of customer records. The attack involved malware and was linked to the threat actor "Whitewarlock". Snowflake has been actively investigating and communicating with affected customers, emphasizing the importance of securing credentials and monitoring for suspicious activity.

Other trends to keep an eye on

Q2 has also featured a number of challenges that have affected the cyber security community more generally:

AI and machine learning in cyber security

The unprecedented advancement of AI over the past two years has continued to confound IT security teams responsible for mitigating the risks of an uncharted new technology.

Indeed, with the widespread use of AI, the risk of sensitive data leakage increases significantly. According to The State of AI and Security Survey Report[4], over 95% of respondents believe that dynamic content created by Large Language Models (LLMs) complicates the detection of phishing attempts.

[3] Overview of the Snowflake Breach: Threat Actor Offers Data of Cloud Company's Customers

[4] Patrick Garrity, the CyberRisk Summit, June 2024

Threat actors are now utilizing LLMs like ChatGPT to generate highly targeted phishing attacks that can evade traditional email security filters, spread advanced malware, and manipulate AI chatbots into revealing sensitive information.

Supply chain threats

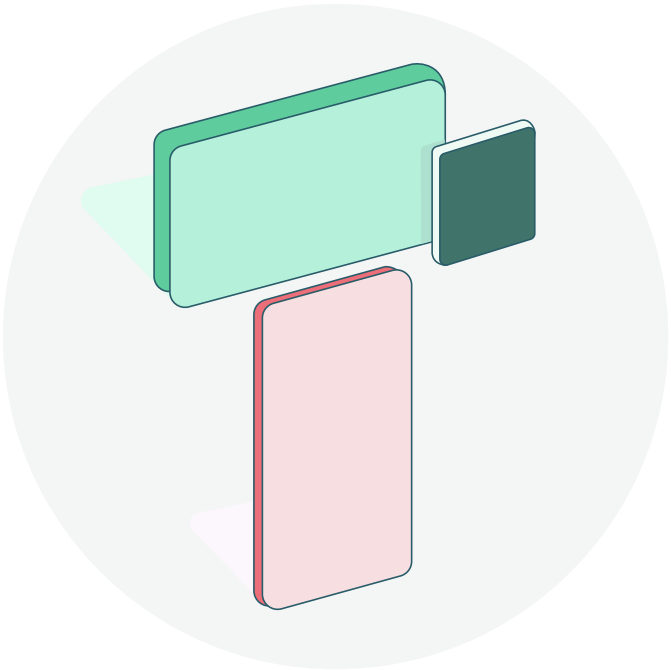
The interconnected systems of today present new vulnerabilities, with hackers focusing on weaker links in supply chains, often targeting smaller vendors with less robust security. Once they breach these entry points, they can infiltrate the primary organization and its partners, leading to widespread disruption and data breaches.

IoT challenges

The Internet of Things (IoT) connects a wide range of devices, from smart home gadgets to industrial systems. While convenient, it creates a large, often insecure attack surface.

A recent survey[5] revealed that 22% of organizations experienced a significant or business-disrupting IoT security incident in the past year.

Hackers can exploit these devices to access networks, launch denial-of-service attacks, or disrupt critical infrastructure.



[5] Survey on 2024 IoT Security Crisis

Notable vulnerabilites of Q2 2024

CVE-2024-29990

Affected products:	Azure Kubernetes Service Confidential Containers
Product category:	Cloud security
Severity:	CVSS (v3): 9.0 | EPSS: 0.091%
Type:	Elevation of privilege
Impact:	Confidentiality (H), Integrity (H), Availability (H)
PoC:	Yes
Exploit in the wild:	No
CISA catalog:	No
Remediation action:	Read more
MITRE advisory:	Read more

CVE-2024-29990 is a critical vulnerability in Microsoft Azure Kubernetes Service Confidential Containers that allows an unauthenticated attacker to gain elevated privileges and access sensitive resources beyond the intended security boundaries. It enables credential theft and control over confidential guest accounts and containers. Microsoft has released a security update to address this vulnerability, and patching is the recommended mitigation.

CVE-2024-3400

Affected products:	Palo Alto Networks GlobalProtect
Product category:	Firewall management software
Severity:	CVSS (v3): 10.0 | EPSS: 95.703%
Type:	Command injection
Impact:	Confidentiality (H), Integrity (H), Availability (H)
PoC:	Yes
Exploit in the wild:	Yes
CISA catalog:	Yes
Remediation action:	Read more
MITRE advisory:	Read more

CVE-2024-3400 is a command injection vulnerability in the GlobalProtect feature of Palo Alto Networks PAN-OS software. It allows attackers to inject malicious commands through user input, potentially leading to system exploitation or data manipulation. Applying vendor-provided security updates is recommended to mitigate this vulnerability.

CVE-2024-4040

Affected products:	CrushFTP server versions below 10.7.1 and 11.1.0
Product category:	File transfer server
Severity:	CVSS (v3): 10.0 | EPSS: 96.607%
Type:	Template injection, remote code execution (RCE)
Impact:	Confidentiality (H), Integrity (H), Availability (H)
PoC:	Yes
Exploit in the wild:	Yes
CISA catalog:	Yes
Remediation action:	Read more
MITRE advisory:	Read more

CVE-2024-4040 is a critical server-side template injection vulnerability in CrushFTP file transfer server versions before 10.7.1 and 11.1.0. It allows unauthenticated remote attackers to read files outside the sandbox, bypass authentication, gain administrative access, and achieve remote code execution. CrushFTP has released patched versions 10.7.1 and 11.1.0 to mitigate this actively exploited vulnerability. Immediate patching is strongly recommended.

CVE-2024-30051

Affected products:	Windows DWM Core Library
Product category:	Operating system
Severity:	CVSS (v3): 7.8 | EPSS: 0.048%
Type:	Out-of-bounds write
Impact:	Confidentiality (H), Integrity (H), Availability (H)
PoC:	Yes
Exploit in the wild:	Yes
CISA catalog:	Yes
Remediation action:	Read more
MITRE advisory:	Read more

CVE-2024-30051 is a critical out-of-bounds write vulnerability in the Desktop Window Manager of Microsoft Windows. It allows attackers to execute arbitrary code with SYSTEM privileges by sending a crafted message to dwm.exe. The vulnerability exists due to improper input validation. Microsoft has released security updates to address CVE-2024-30051, which affects Windows 10, 11, and the server. Applying these patches is crucial to mitigate the risk of exploitation, as proof-of-concept exploits have been demonstrated.

CVE-2024-4323

Affected products:	Fluent Bit versions 2.0.7 through 3.0.3
Product category:	IT Management
Severity:	CVSS (Tenable): 9.8 | EPSS: 0.043%
Type:	Memory corruption
Impact:	Confidentiality (H), Integrity (H), Availability (H)
PoC:	Yes
Exploit in the wild:	No
CISA catalog:	No
Remediation action:	Read more
MITRE advisory:	Read more

CVE-2024-4323 is a critical vulnerability in Fluent Bit versions 2.0.7 through 3.0.3, with a severity score of 9.8/10. It allows memory corruption due to improper validation of input names in the HTTP server's traces API endpoint. Exploitation can lead to denial of service, information disclosure, or remote code execution. Proof-of-concept exploits have been published. Fluent Bit 3.0.4 addresses the issue. Users should update immediately and restrict access to the vulnerable HTTP endpoint as an additional precaution.

CVE-2024-34359

Affected products:	Llama-cpp-Python package in Hugging Face
Product category:	Integrated AI
Severity:	CVSS (GitHub): 9.6 | EPSS: 0.043%
Type:	Remote code execution (RCE)
Impact:	Confidentiality (H), Integrity (H), Availability (H)
PoC:	Yes
Exploit in the wild:	No
CISA catalog:	No
Remediation action:	Read more
MITRE advisory:	Read more

CVE-2024-34359, dubbed "Llama Drama", is a critical vulnerability in the llama-cpp-Python package that allows remote code execution via server-side template injection. It exists in the Llama class used for loading machine learning models, enabling attackers to execute arbitrary code by controlling the chat template parsed using an unsandboxed Jinja2 environment. Over 6,000 AI models on Hugging Face are potentially vulnerable. The issue has been patched in version 0.2.72. Updating is crucial, and restricting network access to vulnerable systems is recommended until patched.

CVE-2024-4985

Affected products:	GitHub Enterprise Server (GHES)
Product category:	Open-source software
Severity:	CVSS (GitHub): 10.0 | EPSS: 0.045%
Type:	Authentication bypass
Impact:	Confidentiality (H), Integrity (H), Availability (H)
PoC:	Yes
Exploit in the wild:	No
CISA catalog:	No
Remediation action:	Read more
MITRE advisory:	Read more

CVE-2024-4985 is a critical authentication bypass vulnerability that affects GitHub Enterprise Server (GHES) versions prior to 3.13.0 when using SAML single sign-on with encrypted assertions. It allows an attacker to forge a SAML response to gain unauthorized site administrator access without prior authentication. The issue was fixed in versions 3.9.15, 3.10.12, 3.11.10, and 3.12.4. Users should update to a patched version immediately and restrict access to GHES instances until updated to mitigate the risk.

CVE-2024-5274

Affected products:	Google Chrome V8 engine
Product category:	Browser
Severity:	CVSS (v3): 8.8 | EPSS: 0.299%
Type:	Out-of-bounds memory access
Impact:	Confidentiality (H), Integrity (H), Availability (H)
PoC:	Yes
Exploit in the wild:	Yes
CISA catalog:	Yes
Remediation action:	Read more
MITRE advisory:	Read more

CVE-2024-5274 is a critical zero-day vulnerability in Google Chrome's V8 engine that allows attackers to perform out-of-bounds memory access, crashes, and potential code execution. It is being actively exploited in the wild and is the eighth Chrome zero-day fixed in 2024. CISA has added it to the Known Exploited Vulnerabilities Catalog, having urged patching by June 18. Users should update to Chrome 125.0.6422.112/.113 for Windows/macOS or 125.0.6422.112 for Linux to mitigate this actively exploited vulnerability.

CVE-2024-4358

Affected products:	Progress Telerik Report Server
Product category:	Report manager
Severity:	CVSS (v3): 9.8 | EPSS: 93.837%
Type:	Authentication bypass
Impact:	Confidentiality (H), Integrity (H), Availability (H)
PoC:	Yes
Exploit in the wild:	Yes
CISA catalog:	No
Remediation action:	Read more
MITRE advisory:	Read more

CVE-2024-4358 is a critical authentication bypass vulnerability in Progress Telerik Report Server that allows an attacker to create a user with system administrator privileges. When chained with CVE-2024-1800, an insecure deserialization vulnerability, it can lead to remote code execution. Exploit code is available, and immediate patching to the latest version is recommended to mitigate the risk.

CVE-2024-1800

Affected products:	Progress Telerik Report Server
Product category:	Report manager
Severity:	CVSS (RedHat): 8.1 | EPSS: 0.046%
Type:	Insecure deserialization
Impact:	Confidentiality (H), Integrity (H), Availability (H)
PoC:	Yes
Exploit in the wild:	Yes
CISA catalog:	No
Remediation action:	Read more
MITRE advisory:	Read more

CVE-2024-1800 is an insecure deserialization vulnerability in Progress Telerik Report Server that allows an attacker to execute code as SYSTEM. Together with CVE-2024-4358, it enables the creation of a malicious report for remote code execution. Immediate patching to the latest version is recommended to mitigate this critical vulnerability.

CVE-2024-6387

Affected products:	OpenSSH: • Versions before 4.4p1 • Versions 8.5p1 to 9.8p1
Product category:	Server & network
Severity:	CVSS N/A | EPSS: N/A
Type:	Remote code execution
Impact:	Confidentiality (H), Integrity (H), Availability (H)
PoC:	Yes
Exploit in the wild:	No
CISA catalog:	No
Remediation action:	Read more
MITRE advisory:	Read more

CVE-2024-6387, termed regreSSHion, is a critical vulnerability in OpenSSH, permitting remote, unauthenticated attackers to execute arbitrary code on affected servers. It affects versions before 4.4p1 and between 8.5p1 to 9.8p1 of OpenSSH. The flaw arises from a buffer overflow during the SSH handshake due to improper input validation. Currently, there are no reports of it being exploited in the wild. Mitigation includes updating to OpenSSH version 9.8 or later, restricting access to trusted networks, using key-based authentication, and regular monitoring and auditing.

GitHub comment malware

Affected products:	GitHub & Counterfeit Microsoft Repositories
Product category:	Open-source
Severity:	N/A
Type:	Malware
Impact:	N/A
PoC:	Yes
Exploit in the wild:	Yes
CISA catalog:	No
Remediation action:	Read more
MITRE advisory:	N/A

GitHub comment malware is a technique used by attackers to distribute malware by uploading malicious files as part of a GitHub comment. This gives the malware a URL that appears to be associated with a legitimate repository, making it seem more trustworthy to potential victims who may be more likely to click on the link. Once clicked, the malware is downloaded and executed on the victim's system.

Researchers have found thousands of malicious GitHub comments containing links to various types of malware, including remote access tools (RATs), information stealers, and cryptocurrency miners. While GitHub has taken steps to detect and remove these comments, the problem persists, and users should be cautious when clicking links in GitHub comments, even if they appear to be from legitimate repositories.

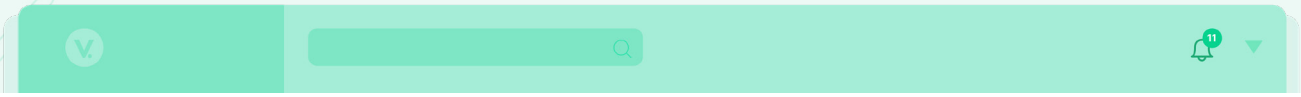
Summary

Q2 has seen a continuation of themes we documented in the first quarter of 2024. AI remains a threat, compliance standards are going nowhere, and vulnerability data continues to compound. Security teams are well aware of these challenges, and those taking a more holistic view will reap the rewards in the future. Exposure management - the broader category encompassing the many approaches needed to mitigate vulnerability risk in 2024 and beyond - will play an enormous role as organizations search for more effective ways to manage their threat landscape.

About Vulcan Cyber

The Vulcan Cyber ExposureOS is the one platform for managing exposure risk across IT and cloud-native surfaces. At its core, the platform aggregates and correlates security findings from your infrastructure, code, application, and cloud environments into the exposure data lake. The platfrom then provides asset risk context, recommendations for the best fixes, and automated remediation workflows to streamline tedious mitigation tasks. Our commitment to innovation has earned recognition as a 2023 Forrester Wave Leader and Omdia RBVM leader. Prominent security teams, such as those at Anaplan and Deloitte, trust Vulcan Cyber to help them own their risk.

Start owning your risk. Try Vulcan Free >>



About Voyager18

The Vulcan Cyber research team, also known as Voyager18, is a team of cyber experts working to leverage machine learning and cyber research to ensure Vulcan Cyber remains a cyber security leader. The team's main objective is to research the latest cyber risk trends, including new attack types and remediations. Most prominently, they discovered AI package hallucination in OpenAI's ChatGPT. Voyager18 is also responsible for bringing innovation to the Vulcan Cyber platform so that our customers get improved and customized cyber risk management capabilities. Alongside regular improvements and alerts, the team's work on mapping the MITRE ATT&CK framework to relevant CVEs provides granular interest into the most critical vulnerabilities.

Stay up to date with the latest research here >>