GALACTIC ADVISORS

CREATED FOR
Anderson Training Test

DATE
11/18/2025

Vulnerability Detection and Analysis Report

REPORT CONTENTS

EXECUTIVE SUMMARY

With cyber threats evolving at an alarming rate, organizations face increasing risks of data breaches and financial losses. Recent studies reveal that 75% of organizations have experienced a cybersecurity incident in the past year, highlighting the urgency for robust security measures. In today's digital landscape, vulnerabilities within network infrastructure and devices present significant risks to organizations' operations and reputation.

Galactic's Vulnerability Report provides a comprehensive assessment of an organization's susceptibility to cyber attacks by analyzing more than 10 devices within the environment. Our report aims to uncover weaknesses in network infrastructure, applications, and systems that could be exploited by cybercriminals.

By identifying vulnerabilities such as outdated software, misconfigurations, and weak passwords, your organization can take proactive measures to mitigate potential risks and enhance overall security posture.

Together we can build a future where cybersecurity is not only a necessity but a standard practice.

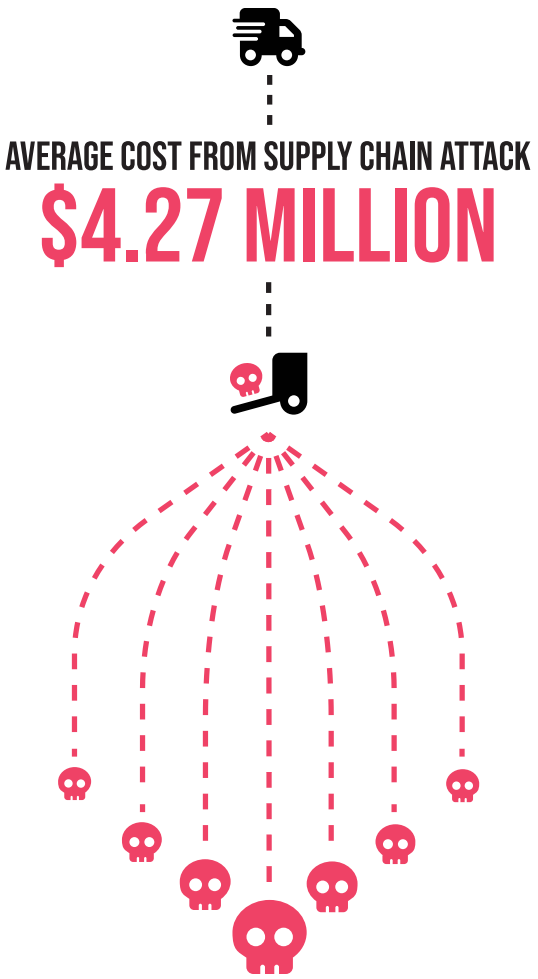
ANALYSIS SCORECARD

238
VULNERABILITIES FOUND

0	High Risk Items
1	Moderate Risk Items
237	Low Risk Items

METHODS

Galactic employs advanced tools and methodologies for conducting vulnerability scans, meticulously analyzing network infrastructure and devices. Our team simulates real-world attack scenarios to uncover vulnerabilities such as outdated software, misconfigurations, and weak passwords. By emulating the tactics of malicious actors, we provide organizations with invaluable insights into their security posture, enabling them to enhance their defenses effectively.



During the scan, we examined various aspects of your network infrastructure, including routers, switches, servers, endpoints, and applications. We look for common vulnerabilities such as outdated software versions, missing security patches, default configurations, and weak passwords. Additionally, we assess the network's perimeter defenses, including firewalls, intrusion detection systems, and access control mechanisms, to identify any gaps or misconfigurations that could be exploited by attackers.

Our goal is to provide organizations with a detailed overview of their current security posture and highlight areas of improvement. By simulating real-world attack scenarios and identifying vulnerabilities before they are exploited by malicious actors, Galactic helps organizations strengthen their defenses and mitigate the risk of cyber attacks.

Let's dive in.

Data leaks, sabotage, or falling victim to phishing attacks, leading to financial losses, reputational damage, and regulatory penalties. Galactic replicates these attack methods and produces findings based on what a hacker would see were these attacks to take place in your organization. By doing so, your organization can continue to bolster its defenses and decrease the likelihood of such an event.

As our Cyber Risk Progress Report reveals, understanding and addressing these risks are essential for safeguarding your organization's data, finances, and reputation. Let's delve into the findings of our security assessment and take proactive steps to mitigate these threats effectively.

YOUR MOST VULNERABLE AREAS

The external attack surface of your organization is composed of IP addresses. Think of them as the phone numbers that someone could call to get into your network. Below we have listed the 10 most vulnerable IP addresses on your network, indicating risk level. We have also listed vulnerabilities that are new to your network, as well as those which have been removed from your network, and those which remain. For a complete listing of IP addresses scanned, refer to the detail report.

RISK LEVEL	ITEM	VULNERABILITIES FOUND
Medium	General Surveillance Warning	1

VULNERABILITIES

General Surveillance Warning Medium

See antivirus and firewall section - it does not appear that alerting is properly configured to detect an advanced persistent threat in the environment.

Recommendation: See antivirus and firewall section to address issues.

Description: See antivirus and firewall section - it does not appear that alerting is properly configured to detect an advanced persist ent threat in the environment.
Isselectone: 1
Recommendation: See antivirus and firewall section to address issues.

WHY ANALYZE YOUR VULNERABILITIES?

Vulnerabilities provide the perfect entry point for attackers—that's what makes this assessment crucial. It helps you stay on top of your networks security and ensure you're well-equipped to defend against emerging threats.

Cybersecurity vulnerability statistics to know:

- Over 40,000 vulnerabilities were reported in 2024, marking a 38% increase from 2023.
- 70% of breaches involved known vulnerabilities that were left unpatched.
- 57% of organizations experienced a data breach caused by a vulnerability in the last year.
- Vulnerability exploitation accounts for 21% of confirmed breaches.

But it's not just about the numbers; it's about **taking action**. By conducting regular vulnerability assessments, you can identify weaknesses in your network infrastructure, applications, and systems. This allows you to patch vulnerabilities promptly and implement security measures to protect your data and assets.

Remember, cybersecurity is a journey, not a destination. Stay proactive and continue to address these vulnerabilities head-on.