pellera

Red Team Report

2024 Penetration Testing Findings & 2025 Strategies

Pellera
Red Team Report

2024 Penetration Testing Findings & 2025 Strategies

CONTENTS

Prepared by: Pellera Cybersecurity Practice
pellera.com | 866.910.4425

INTRODUCTION

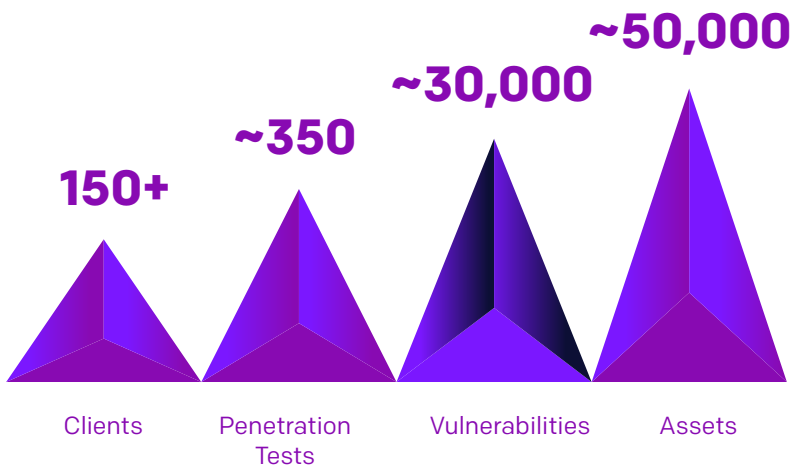
Organizations and their data are constantly at risk, with the continued growth of malicious adversaries and threat actor groups ready to take advantage of any technological or human-related vulnerability to achieve their objectives. The cybersecurity industry continues to grow, with a **projected $212 billion in spending expected in 2025**[1], in an attempt to keep pace with this evolving threat landscape and consistent increase in attack surface.

Companies continue **to struggle with the cybersecurity basics, leading to breaches** with significant costs and consequences. The data shows that over the last several years, similar vulnerabilities and tactics have yielded the most success. Some organizations make iterative or even substantial improvements towards attack surface reduction, adversarial detection capabilities, and overall cybersecurity resiliency. However, they are the exception, as the **majority continue to fall behind in their ability to prevent, detect, and respond** to the ever-increasing quantity of vulnerabilities and attack vectors.

Successful cybersecurity programs implement controls at the people, process, and technology layers. A **comprehensive and strategic approach**, combined with consistent validation of the information security program, is necessary to reduce risk and mitigate threats.

METHODOLOGY

This report is an analysis of the combined penetration testing results of **Pellera's 30+ penetration testers**. A key differentiator for our Penetration Testing practice is our people, all highly certified individuals who continuously review the tools, tactics, and techniques used by real-world malicious actors, so that Pellera can replicate those attack capabilities into our processes. Pellera's Red Team takes a comprehensive hacker mentality to identify our clients' weaknesses before they can be exploited by malicious adversaries.



1. https://www.gartner.com/en/newsroom/press-releases/2024-08-28-gartner-forecasts-global-information-security-spending-to-grow-15-percent-in-2025

EXECUTIVE SUMMARY

Externally and internally, credential abuse is one of the most commonly abused weaknesses that companies currently face. Credential-related weaknesses account for the most common form of initial access, aid in lateral movement, and can frequently be abused to escalate to administrative access across an environment.

Multi-factor authentication (MFA) at the perimeter is not enough. Organizations require better processes and technologies for limiting credential access, automating strong password selection and rotation, and eliminating credential reuse. **Organizations should also consider implementing segmentation and MFA for critical internal systems and services**.

A review of the test cases and exploitable vulnerabilities that the Pellera Red Team most commonly abused illustrates how much organizations continue to struggle to protect credentials.

Top Test Cases

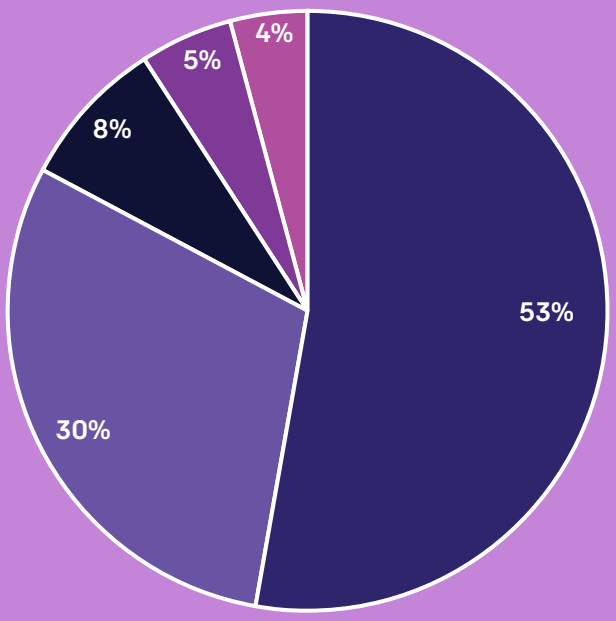
Pellera penetration testers found the most success in abusing these test cases to further their objectives.

1. Use of default credentials
2. Credential relay attacks
3. Abuse of default Windows legacy network protocols that enable poisoning and credential theft
4. Missing patches
5. Access and authorization bypass issues in applications
6. Insecure or incorrect implementation of IPv6 traffic routing that enables poisoning and credential theft
7. Use of weak and predictable passwords
8. Kerberoasting
9. Injection attacks in applications
10. Abuse of Active Directory Certificate Services misconfigurations

Key Vulnerability Statistics

Top 10 Exploitable Vulnerabilities

1. SMB signing not required
2. IPMI v2.0 password hash disclosure
3. Local administrator credential reuse
4. LDAP signing & channel binding not required
5. Default credentials
6. Multicast name resolution poisoning
7. Kerberoasting
8. Service account credentials stored in plaintext
9. Password reuse
10. MS17-010 EternalBlue



Frequency of Vulnerability Classes

- Misconfiguration
- Patching
- Credential Abuse
- Unsupported Software
- Insecure Code

NOTABLE TRENDS

The most notable trend over the last year was not in the vulnerabilities or test cases, but in the way Pellera's clients leverage our penetration testing services. Pellera's Penetration Testing as a Service (PTaaS) model saw **tremendous 95% growth in 2024**.

Point-in-time annual assessments no longer cut it for organizations that want to keep pace with a continuously changing threat landscape. More and more clients are performing regular testing throughout the year and follow-up testing as significant changes are made to applications and networks. This testing is further being supplemented with targeted testing, including ransomware readiness assessments, cloud security assessments, and purple teaming engagements. This is the perfect fit for the PTaaS model, where our clients can leverage one contract to support regular testing throughout the year.

Another trend was the use of PTaaS by clients with many current acquisitions or plans to perform numerous acquisitions over the course of a year. Penetration tests are being conducted against these subsidiaries as they are onboarded and prior to being integrated with the client's networks and systems to determine potential risk.

These additional trends also stand out and are likely to continue to grow:

Social engineering via phone: Requests for vishing- and smishing-based social engineering campaigns increased, similarly to what Pellera observed in 2023. These forms of social engineering were overlooked in the past, but our clients are increasingly requesting them as real-world threat actors have pivoted more to these techniques. Additionally, many clients requested some form of artificial intelligence (AI) be used in social engineering engagements, with the most common scenario being some form of audio trained on publicly accessible voice data of key executives within their organizations.

Application security and AI: Organizations continue to increase the frequency of testing for their applications, often integrating the Pellera application penetration testing team into their software lifecycle development processes, performing targeted penetration tests against code that had undergone significant changes.

Unsurprisingly, there was a **growing interest in testing new AI features of applications** in 2024. More and more clients are integrating AI into their applications and requesting Pellera perform comprehensive testing that includes AI attack cases against that functionality prior to production release. Critical and high-risk findings were frequently identified in these AI applications by Pellera and remediated by our clients, reducing the risk of data theft, exposure, or other significant incidents.

OWASP Top 10 Correlation

		2024	2023
A1	Broken Access Control	18%	14%
A2	Cryptographic Failures	1%	1%
A3	Injection	52%	48%
A4	Insecure Design	<1%	<1%
A5	Security Misconfiguration	<1%	2%
A6	Vulnerable and Outdated Components	19%	23%
A7	Identification and Authentication Failures	1%	1%
A8	Software and Data Integrity Failures	<1%	<1%
A9	Security Logging and Monitoring Failures	<1%	<1%
A10	Server-Side Request Forgery	9%	<1%
	Vulnerabilities Outside of Clear Alignment With OWASP Classifications	12%	12%

KEY TAKEAWAYS

Organizations are becoming more proactive in their testing approaches in an attempt to stay ahead of the curve with respect to the introduction of new risks. Networks, applications, and environments are constantly changing, and with change comes the potential to introduce new risks and vulnerabilities. Frequent testing reduces the risk that a change will result in a vulnerability or risk going unnoticed for a prolonged period.

More frequent testing combined with targeted high value specialized testing such as purple teaming and ransomware readiness assessments increases an organization's ability to detect and respond to common attack vectors and enhance organizational resiliency to advanced attacks.

Purple teaming enhances detection and response capabilities

As companies continue to mature, adding a purple teaming component to regular penetration tests provides better value. This testing approach highlights gaps in visibility to common tools, tactics, and techniques employed by malicious threat actors. Based on the MITRE ATT&CK framework, regular purple teaming engagements enable organizations to more quickly identify as companies continue to mature, adding a purple teaming component to regular penetration tests provides better value. This testing approach highlights gaps in visibility to common tools, tactics, and techniques employed by malicious threat actors. Based on the MITRE ATT&CK framework, regular purple teaming engagements enable organizations to more quickly identify and respond to a real incident, reducing the impact and cost of a breach.

Ransomware is here to stay

Ransomware is too profitable to go away any time soon. Pellera's Ransomware Readiness Assessments take a comprehensive look at our clients' ability to detect, respond to, and recover from a potential ransomware incident. Our clients are finding great value in these assessments as they provide a scorecard highlighting areas needing the most improvement and include recommendations that provide the most risk reduction for the least cost and effort.

AI is on everyone's minds

From testing the AI functionality being added to existing applications to leveraging AI in attack techniques, the rewards and risks of using AI is top of mind. Organizations that don't prioritize assessing themselves for AI-related vulnerabilities are playing with fire. To safely use AI and be protected from its potential for malicious use, controls must be implemented for people, processes, policies, technologies, and at the code level.

Top Five Things to Do Now

1. **Incorporate** more frequent testing into the information security program. One year is too long of a timeframe in the fast-paced world of cybersecurity, the threat landscape changes quickly, and frequent testing reduces the risk of vulnerabilities and other issues being introduced over the course of a year.

2. **Perform** AI-specific penetration testing against any applications incorporating AI into their functionality prior to production release.

3. **Update** security policies and processes to better provide awareness for phone-based (vishing and smishing) attacks and the use of sophisticated techniques such as AI.

4. **Supplement** penetration tests with purple team engagements and ransomware assessments to improve visibility to the tools, tactics, and techniques used by real threat actor groups.

5. **Combine** privileged access management (PAM) solutions with phishing-resistant MFA solutions such as WebAuthn, FIDO2, and passkeys to better protect credentials from compromise and malicious use.

20%-30%
Savings Over Single Tests

86 NPS
Client Satisfaction Score

100%
Human Tested & Validated

100%
US-Based Testers Employed by Pellera

Know Sooner & Act Faster With Pellera PTaaS

Our PTaaS solution delivers the flexibility and pricing advantages you need to stay on top of emerging vulnerabilities in dynamic environments. We connect the essential elements of comprehensive, effective penetration testing with budget advantages to arm you with information that protects your organization in its current state.

- Certified, creative testers with an adversarial mindset
- Near-real-time progress tracking and reporting
- Advanced security tools
- Layered threat intelligence
- Custom dashboards
- Direct access to testers and project management
- Risk-ranked vulnerabilities
- Detailed and prioritized remediation steps

Penetration Testing Services

Supercharge the exposure and exploitation of weaknesses in your environment. Our penetration testing is people-powered and technology-driven for creative exploitation as advanced as real-world adversaries. Delivered as single engagements or regular assessments under PTaaS.

Application	Red & Purple Teaming
Cloud	Social Engineering
Network	Ransomware Readiness

Top-Level Certifications

Pellera Advanced Testing
By the Numbers

20+ Years of Experience

250+ Penetration Tests Each Year

150+ Unique Clients Served Each Year

30+ Staff Resources

15 Top-Secret Clearance

AUTHOR

Josh Berry

Director of Advanced Testing & Governance, Risk & Compliance

josh.berry@pellera.com