

| State of Pentesting 2024



THE STATE
OF PENTESTING
REPORT 2024

Speaker: Caroline Wong, CSO, Cobalt



Caroline Wong is the Chief Strategy Officer at Cobalt. She has 15+ years of cybersecurity leadership, including practitioner, product, and consulting roles.

Caroline authored the popular textbook, *Security Metrics: A Beginner's Guide*. She teaches cybersecurity courses on LinkedIn Learning and hosts the *Humans of InfoSec* podcast.



Agenda

1

AI Security

2

Survey Responses: Security Budgets

3

Key Takeaways & Tips



State of Pentesting Report 2024 Methodology

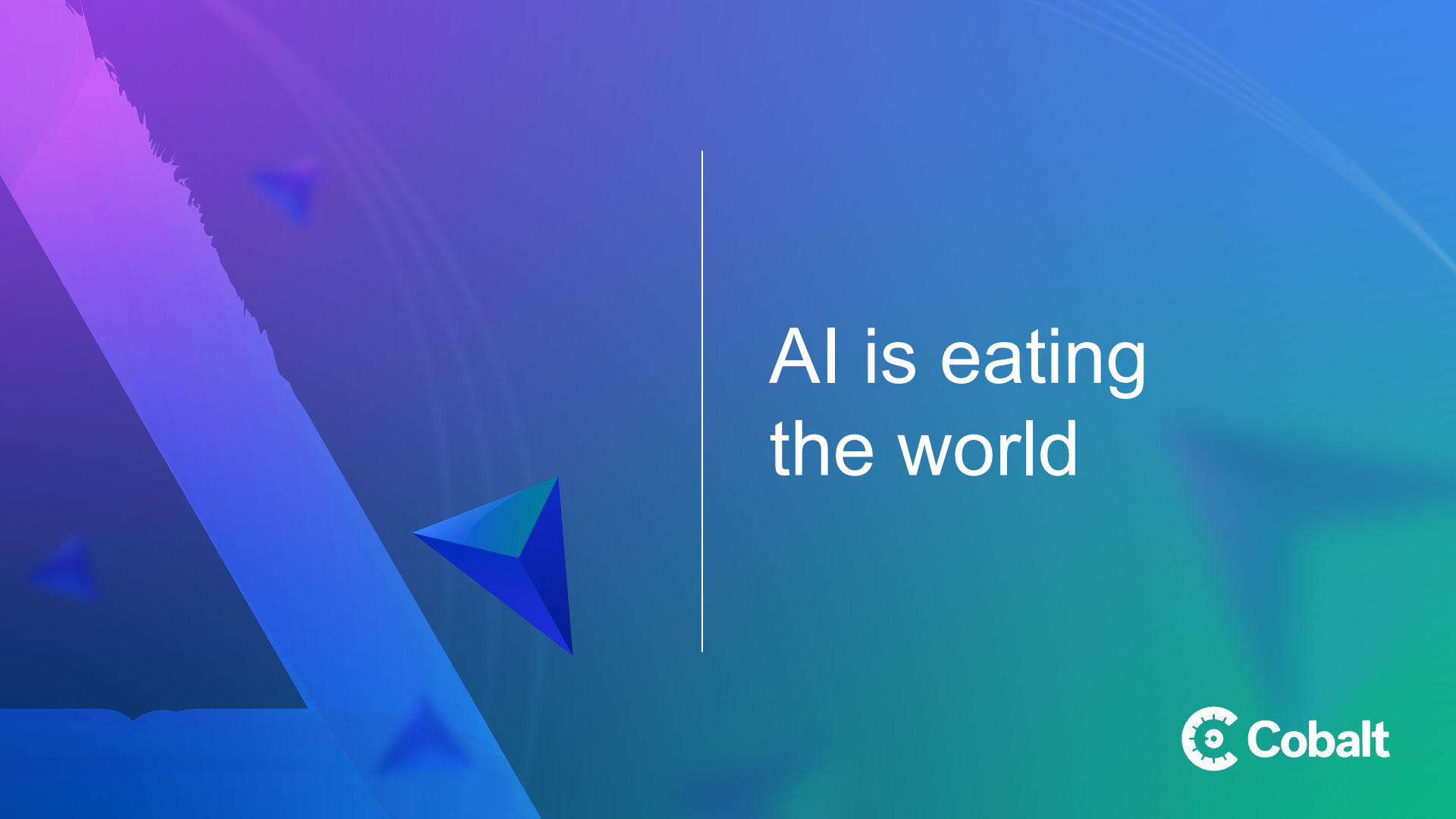
Cobalt's 6th Annual State of Pentesting report includes two types of data sets:

- Anonymized pentest data collected via Cobalt's proprietary Pentest as a Service platform (referred to as "Cobalt's Pentest Data");
- Survey responses on questions related to talent shortages, emerging threats, AI, and pentesting practices (referred to as "Survey Data")

For more details on testing types and survey participation, please see the methodology section of the State of Pentesting Report 2024

Cobalt Pentest data was collected between January 1, 2023, and December 31, 2023. Our Offensive Security testing platform collected data from **4,068 pentests** that covered multiple asset types.

Cobalt distributed an online survey to **904 cybersecurity professionals** in the United States and the United Kingdom.



AI is eating
the world

The Rise of AI: Pace of AI Adoption

First it was software, now its large language models and generative AI. As a result, security teams are scrambling to both use and secure this new technology.

75%

of respondents to our survey say that their team has adopted new AI tools in the past 12 months.

57%

of respondents say the demand for AI has outpaced the security team's ability to keep up and that their team is not well-equipped to properly test the security of AI tools.



The Rise of AI: Better Social Engineering



Your PayPal account has been limited.

Hi Dear Customer,

We just wanted to let you know that a recent **Unauthorized** login was found in your Paypal account **t Which is** blocked successfully.

You can't use your account at the **movement**. Please **Verify And Secure** your account by following link

[Verify Now](#)

Kind regards,
PayPal Service

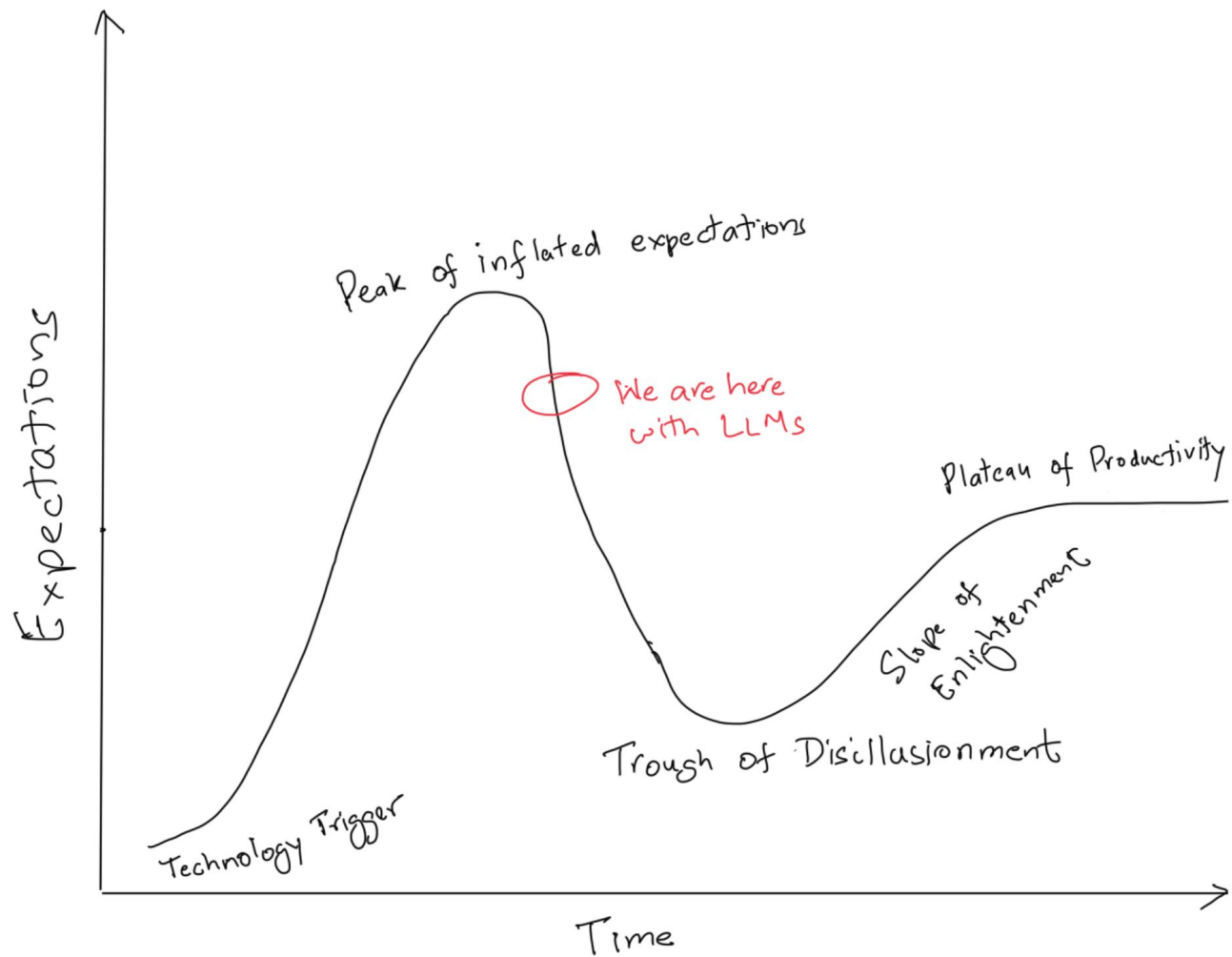
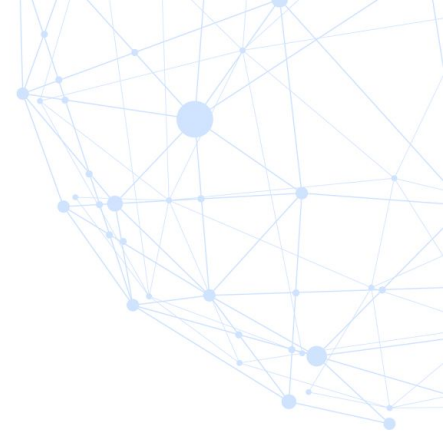
What are we seeing as we test LLM/AI Apps?

The overwhelming majority (>90%) of our engagements in 2023 for AI testing are to assess vulnerabilities in chatbots or copilots that are embedded in a software product.

Most Common Vulnerabilities

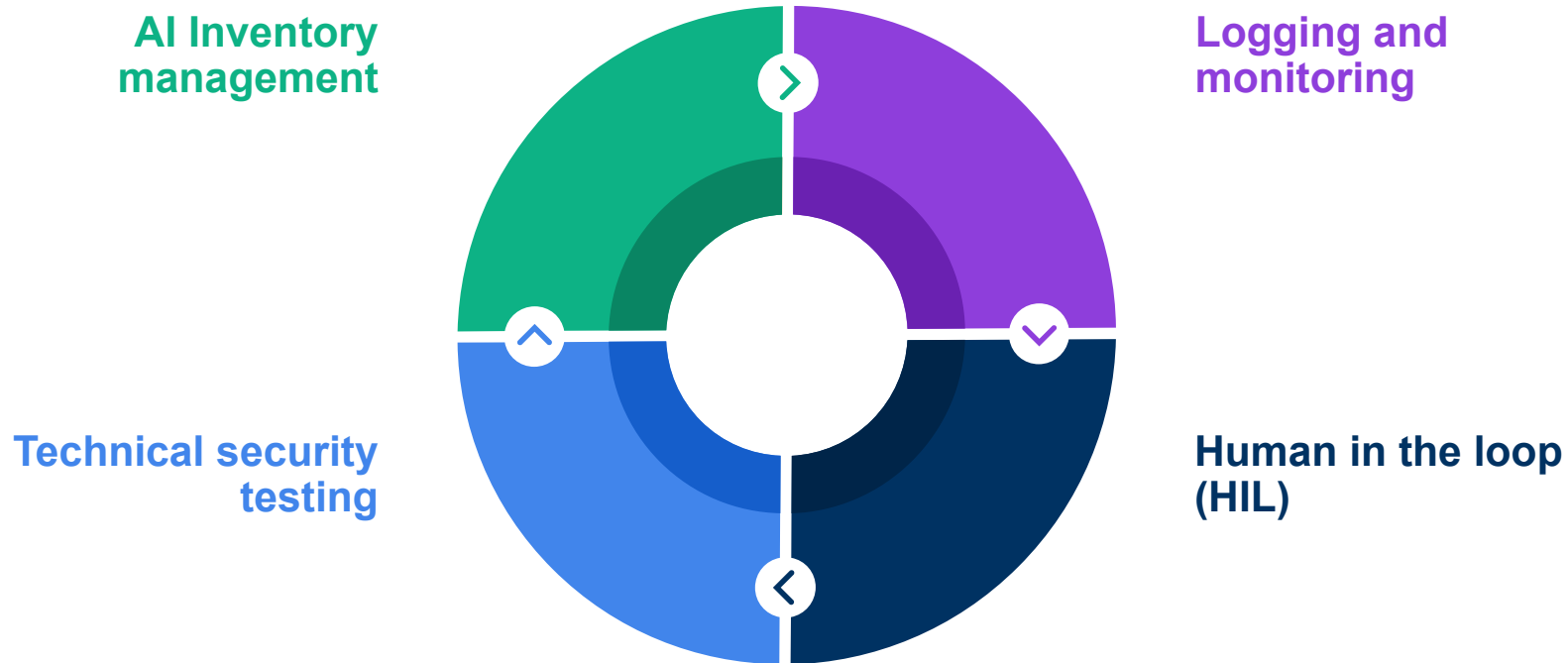
1. **Prompt injection (including jailbreak):** This manipulates the LLM through inputs, causing unintended actions. Direct prompt injections overwrite system prompts that can potentially lead to unauthorized actions being performed such as “forget all previous instructions”, while indirect ones manipulate inputs from external sources by embedding a prompt injection and performing common web attacks such as SQLi and command injection.
2. **Model denial of service:** Attackers cause resource-heavy operations on LLMs, leading to service degradation or high costs. The vulnerability is magnified due to the resource-intensive nature of LLMs and unpredictability of user inputs.
3. **Prompt leaking (sensitive information disclosure):** LLMs may inadvertently reveal confidential data in their responses, leading to unauthorized data access, privacy violations, and security breaches.

Some engagements have our testers focus only on Prompt Injection.



<https://healthcareconsumer.ai/the-upcoming-disillusionment-with-llms/>

AI Security Controls





Budgets & Security
Teams are decreasing,

Findings are
increasing.

The digital attack surface is increasing, but security is getting worse.

As companies adopt new technologies to get to market faster, the breadth of what security teams need to protect is increasing. This is especially true of software:

1. **Shift to Cloud & DevSecops:** Increased adoption of cloud and agile/devops practices results in both greater exposure of assets and an increased rate of change to those assets. This means vulnerabilities can be patched faster but tracking and managing those findings becomes a larger organizational burden.
2. **Open Source code:** software is now assembled with glue-code holding together third-party libraries and packages.
3. **AI-generated code:** According to GitHub, staggering 92% of US-based developers are integrating AI tools into their workflows. This increases the speed of delivering new features and functions and further increases the rate of change to software.

More software does not result in more security

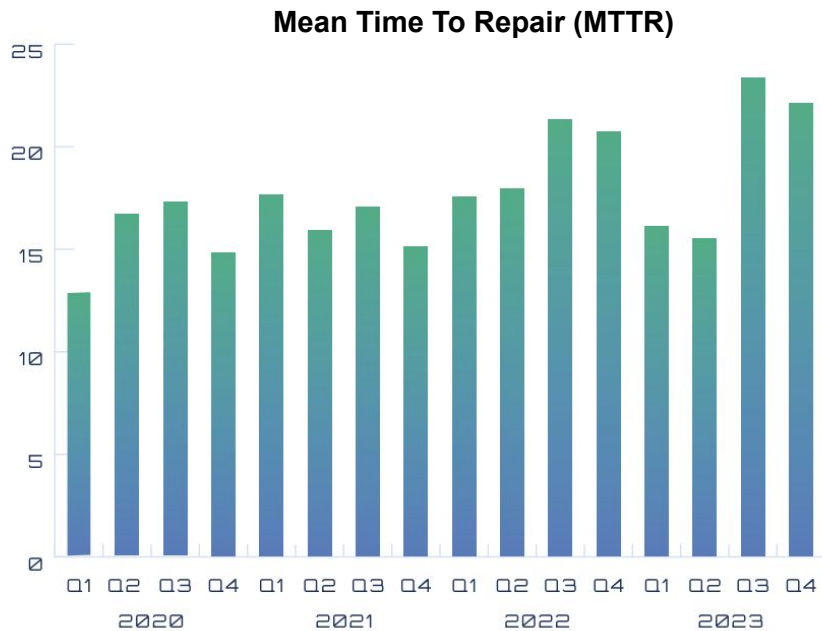
This year's data shows a

21% increase

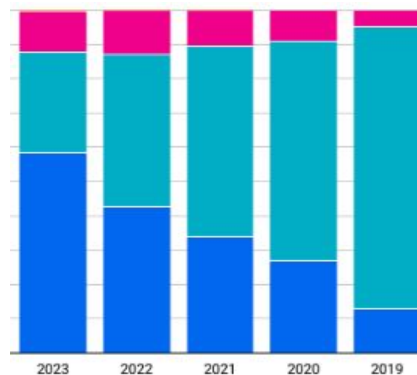
in the number of findings per engagement YoY



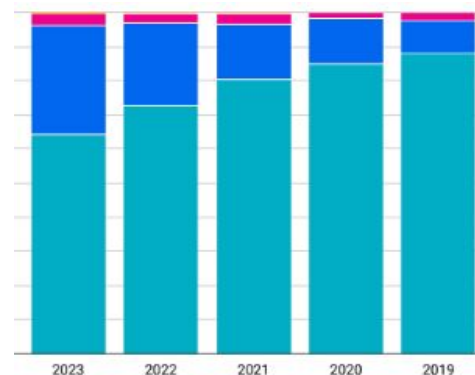
There are more findings, and they are both taking longer to fix or not getting fixed at all



Remediation status across all severities



Remediation for high and critical findings



need_fix valid_fix wont_fix

Organizational Dynamics: Security teams face reduced budgets, resources, and headcount

31% of respondents have faced layoffs in the past six months, and 29% expect to face layoffs this year.

This matches studies elsewhere and exacerbates the already existing talent gap found on most security teams - as seen in reports such as the ISC2 Cybersecurity Workforce Study.

As a result of belt-tightening, security teams are:

- Deprioritizing new technologies (40%)
- Deprioritizing hiring (43%)
- Outsourcing more work (54%)

Security teams are coping by focusing budget on basics of security programs

31% increase in the pentest engagements year-over-year

Key Tips and Take-Aways from Cobalt's State of Pentesting Report 2024

Your Call to Action:

1. Your company needs to have a stance and a policy regarding the use of artificial intelligence
2. Sensitive information going into public LLMs is not good.
3. If you're using AI, it is a target for attacks and must be protected appropriately. *Just like you secure the applications you produce via your "normal" SDLC, you need secure your use of AI.*



The State of Pentesting Report 2024 is here!



Discover market leading insight through analysis
of over 4,000 pentests and more than 900
responses in our annual cybersecurity survey

DOWNLOAD LINK IN CHAT