

# 2024 TAKE COMMAND SUMMIT BY NUMBERS

Over 2,000 security professionals came together at Rapid7's Take Command 2024 Cybersecurity Summit, a day-long virtual event held in partnership with AWS, focused on key issues in cybersecurity. We conducted 10 expert-led sessions and surveyed the attendees along the way. Here's what we learned about new attack intelligence, AI disruption, transparent MDR partnerships, and more.

## KNOW YOUR ADVERSARY

The 2024 Attack Intelligence Report (AIR) is a 14-month analysis of vulnerability and attacker behavior, drawing from Rapid7's research, detection & response, and threat intelligence teams. Key findings include:

For the past three years, **60+% OF VULNERABILITIES** Rapid7 analyzed in network and security appliances were exploited as zero-days.



**75% OF THE CVEs** Rapid7 has analyzed since 2020 have arisen from improper access control and injection.




The 2024 Attack Intelligence Report offers more insights like these, including 1,500 curated vulnerability and exploit data points, over 180 advanced threat campaigns, ransomware incidents, extortion communications, dark web posts, and trillions of security events [here](#).

Ransomware payments were said to have topped **\$1 BILLION IN 2023**.

## OUR WORLD IS CHANGING

The security landscape is more challenging than ever, with emerging threats, evolving regulations, and resource constraints impacting organizations and SOC teams worldwide.

Attacks in 2025 are predicted to cost **10.5 TRILLION**.



To navigate these dynamic forces, security teams must adopt proactive strategies to address risk and drive efficiency.


68% Organizations suffered cyber attack within last 12 months.



**PROFESSIONAL PARANOIA IS SOMETHING THAT I THINK WE SHOULD HOLD DEAR TO US.**

Jaya Bayloo, Chief Security Officer, Rapid7

The average cost of a data breach in 2023 is **4.45 MILLION**.



## AI: FRIEND OR FOE?

AI plays a dual role in helping to combat threats and enabling the creation of convincing phishing emails and scripts.




**8 TIMES OUT OF 10, I'M USING AI TOOLS DURING MY ATTACKS...** I'm looking for targets who have a lot of information on social media.

Rachel Tobac, Friendly Hacker and CEO of SocialProof Security

**YOU CAN'T ACHIEVE EFFICIENCY WITHOUT AUTOMATION....** be it project, be it tooling, be it reports... you have to think that way.

Gaël Frouin, Director IT Security, AAA Northeast

**9%** of Take Command attendees do not intend to implement generative AI into security operations.



**OVER 1/3** plan to use it for detecting advanced threats faster and with more precision.



## COLLABORATION + COMMUNICATION = SUCCESS

AI plays a dual role in helping to combat threats and enabling the creation of convincing phishing emails and scripts.

**70+% OF TAKE COMMAND ATTENDEES AGREE** that the security community has prioritized **technical skills** and **certifications** over soft skills when initiating new security projects.



**GIVING IMPACTED TEAMS A VOICE EARLY ON, AND GETTING THEM INVOLVED, AND GIVING THEM A SENSE OF OWNERSHIP, REALLY HELPED WITH THE SUCCESS OF THE PROJECTS.**

Byron Anderson, Principal InfoSec Engineer, KinderCare Learning Companies

WATCH THE FULL SERIES OF PANEL DISCUSSIONS

[Watch here](#)

Sources

- <sup>1</sup> The Record
- <sup>2</sup> Cybercrime Magazine
- <sup>3</sup> Netwrix Annual Security
- <sup>4</sup> Splunk
- <sup>5-6,7</sup> Rapid7 Post event survey 2024