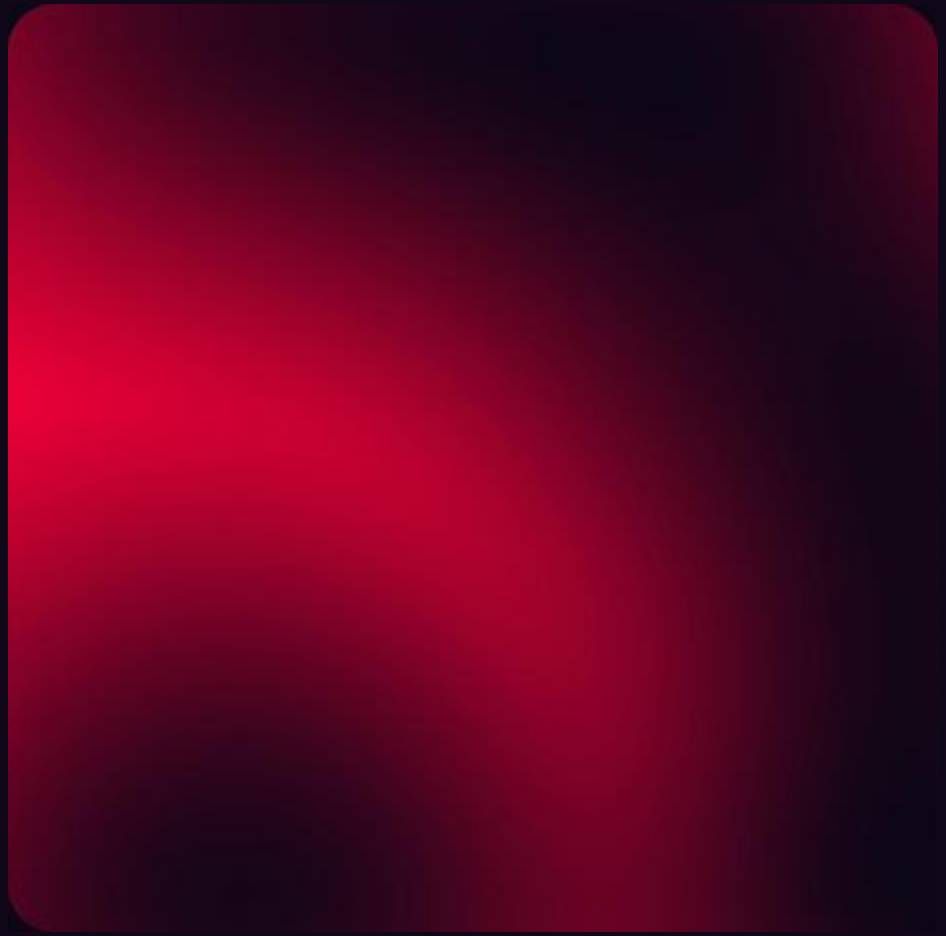
HADRIAN

# AI in Offensive Security

Simulate attackers.
Stop them before they strike.



PRESENTED BY GIL FROMOVITCH

IT-SECURITY MATTERS 2025

# Exploitation outpaces remediation

**+275%**
growth of attacks involving the exploitation of vulnerabilities as the critical path to initiate a breach since 2023 (Source: Verizon)

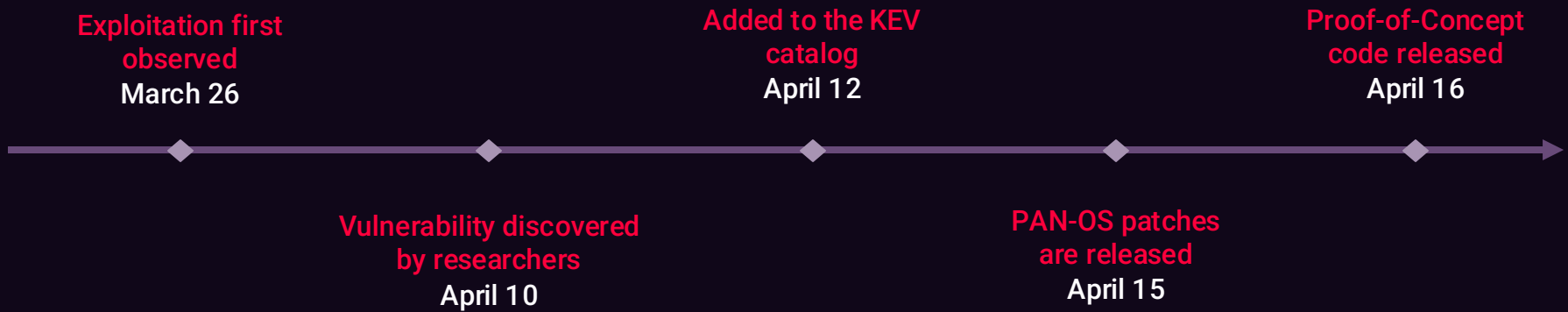
**48 MINUTES**
the average time it took an adversary to move laterally across a network in 2024 with the fastest observed at just 51 seconds (Source: Verizon)

**32 DAYS**
the median time organizations took to patch edge device vulnerabilities in 2024 (Source: Verizon)


MEAN TIME TO EXPLOITATION (Source: Google)

# The need for speed

CVE-2024-3400 - GlobalProtect Command Injection Vulnerability




| Severity | Exploitability | Impact system |
| --- | --- | --- |
| CVSS-B: 10.0 | EPSS: 0.9432 | PAN-OS |

# The need for speed

CVE-2024-3400 - GlobalProtect Command Injection Vulnerability


| Severity | Exploitability | Impact system |
| --- | --- | --- |
| CVSS-B: 10.0 | EPSS: 0.9432 | PAN-OS |

# AI & vibe hacking

Science/Tech

## Detection expert says hackers likely used AI to penetrate airport system

WGCU | By Undetectable.ai/Special to WGCU
Published September 23, 2025 at 9:23 AM EDT

Print

Announcements

## Detecting and countering misuse of AI: August 2025

27 Aug 2025 • 5 min read

Threat Intelligence Report: August 2025


## AI-Powered Villager Pen Testing Tool Hits 11,000 PyPI Downloads Amid Abuse Concerns

Sep 15, 2025 Ravie Lakshmanan


A new artificial intelligenc
attracted nearly 11,000 d
that it could be repurpose


AI | Cyber Security | Cyber Security News 2 min. Read

## Threat Actors Exploit AI to Scale Attacks and Target Autonomous Agents

*Frequent and consistent offensive testing is essential, but it is complex to orchestrate and requires specific skill sets. Technologies are necessary to reduce the level of skill and complexity required to orchestrate offensive testing.*

Gartner

# Building an autonomous attacker

- # Fine-tuned LLMs with 100k+ hacking challenges
- # Train agents to use tools

2X performance on internal benchmarks

# Hadrian’s agentic hacker

**SENSE**

Like a real attacker, the hacker agents search the internet for your exposed assets and open entry points improving your visibility into critical exposures by 10x.

**PLAN**

Hacker agents piece together relationships between assets in order to get ahead of hackers planning their next move.

**ATTACK**

Agents work together to validate whether an attack path is truly exploitable versus theoretical, delivering actionable, proof-backed insights you can trust.


# London Business School

**Key challenges**

- Expanding digital footprint with hundreds of assets across multiple domains, increasing the attack surface.
- Difficulty identifying which risks were critical and prioritizing remediation effectively.
- High-impact, frequently used services (like the scheduling program) exposed, meaning compromise could affect many personnel.

**Hadrian's impact**

- Autonomous agents mapped all external assets, uncovering thousands beyond the initial inventory for full visibility.
- Continuous validation and risk ranking prioritized actionable threats, filtering out noise for efficient remediation.
- High-risk, high-traffic systems were automatically detected and prioritized, enabling immediate remediation and reducing potential impact.

# Let’s Connect

Scan to add me on LinkedIn:

Or email me at:
**gil@hadrian.io**

**Our clients**

McKESSON · NBC · CRÉDIT AGRICOLE · Wendy's · pepsi · amadeus · RITUALS... · DAMEN · VISMA