

RED QUEEN SIGNALS

There used to be a pause between attacks. That pause is gone.

Why every security timeline built on the attacker's breathing room is now a gap.

RED QUEEN CIPHER
Maria How | Cybersecurity + AI + PQC



MY READ

The pause was a control nobody wrote down.

Monthly patching. Alerts triaged in the morning. Systems restored after a quiet day.

All of it assumed an attacker who had to stop and think.

BEFORE THE INTRUSION

Patch to exploit is now modeled as zero.

> “Patch soak time is no longer meaningful.”
>
> Google Project Zero, November 13, 2026

It calls zero patch-to-exploitation time "a reasonable, though imperfect, model of attacker behavior."

MANDIANT M-TRENDS 2026

-7 days

estimated mean time to exploit.

Exploitation routinely starts before a patch is released.

2025 data. It does not single out AI as the cause.

DURING THE INTRUSION

The hesitation is gone.

> “A human threat actor who finds a password has to stop, read, decide and try. These agents did not.”
>
> Eye Security, November 12, 2026

A case at an unnamed European e-commerce company.

BARRACUDA'S OWN INCIDENT

44 hours and it was over before anyone reported it.

About 10 cloud accounts, starting from a key given to a third-party vendor and never retired.

AFTER THE INTRUSION

The quiet day was not a pause.

> “Less than an hour later, the threat actor was back with critical alerts.”
>
> Eye Security, after systems were restored

The quiet spell was "most likely a gap in the threat actor's resources."

THE RED QUEEN, PROPERLY READ

Nobody gets to rest.

Van Valen's 1973 hypothesis, named for Carroll's Red Queen: "the struggle for existence never eases up."

It does not say the fastest wins. Build controls that work without the breather.

DECISIONS FOR THIS QUARTER

Build for no pause.

1. Measure exposure in hours, not patch cycles
2. Retire long-lived and vendor keys
3. Rotate every reachable credential before you restore
4. Report exposure hours to the board

My recommendations, not legal obligations.

SOURCES AND LIMITS

Read the originals.

Google Project Zero, November 13, 2026
Policy and Disclosure: 2026 Edition
projectzero.google

Barracuda, November 11, 2026
Forty-four hours: Anatomy of a machine-speed intrusion
blog.barracuda.com

Eye Security, November 12, 2026
Our AI vs. AI Cyber Battle: Threat Actors at Machine Speed
eye.security

Google Cloud (Mandiant), March 24, 2026
M-Trends 2026: Data, Insights, and Strategies From the Frontlines
cloud.google.com

University of Chicago News, October 20, 2010
Leigh Van Valen, evolutionary theorist and paleobiology pioneer, 1935-2010
news.uchicago.edu

Also consulted: Project Gutenberg. Full register on the article page.

Project Zero calls its model imperfect. Mandiant does not single out AI. The two intrusion accounts are first-hand from the defenders: they illustrate, they do not prove a trend.