From Checklist-based Pentesting to Autonomous Ethical Hacking:

What Changed for CEGID

ETHIACK
autonomous ethical hacking

cegid

About CEGID

CEGID is a conglomerate of companies headquartered in Lyon, France. They offer dozens of software solutions, often in critical sectors dealing with sensitive data. It goes without saying that cybersecurity is at the top of their list of concerns.

They found great results from implementing Autonomous Ethical Hacking. Here's the full story.

Industry
Information Technology

Headquarters
Lyon, France

Company Size
+5000 people

Protected Attack Surface
+1500 assets

The Problem

André is a SecOps Engineer responsible for all infrastructures and their security in Portugal, Spain and Africa. After 5 years of his team-leading this area of the company, he identified a vital need: they couldn't stick to annual pentests.

His team managed the assets of 21 companies and multiple offices of the group, and he knew that a simple checklist-based pentest done once per year wasn't going to be effective in keeping their customer data safe. Product teams were shipping code every week - **they needed a solution that kept up with these changes.**

They experimented with other tools but quickly ran into a problem: false positives. André mentions "these often came in the thousands" and made it impossible to mitigate any real vulnerabilities.

The Solution

Enter Ethiack. During a casual lunch meeting, an ethical hacker from our talent pool was mentioned. A Proof of Concept (POC) was launched for both Ethiack 1.0 and 2.0, which turned into a contract for both Machine Ethical Hacking and Human Ethical Hacking.

Our Machine Ethical Hacking offering solved their biggest problem: having a 24/7, continuous approach to pentesting that could alert the product teams on vulnerabilities needing to be mitigated.

This finally gave André and the whole cybersecurity team a clear view of their security posture and what was more exposed.

And to complement this, they launched Human Hacking events to test the most critical parts of their infrastructure and if it held up against human ingenuity.

The Outcome

The combined approach yielded great results. While Machine Hacking dealt with easier-to-spot attack vectors, the Human Hacking Events uncovered several critical vulnerabilities that only a skilled hacker could have uncovered.

The fast detection of vulnerabilities and minimal false positive rates (<1%) allowed CEGID's product and security teams to focus more on mitigation and prevention, thus improving their security posture. In the words of André:

> The way Ethiack incorporates EASM with Automated Pentesting has brought us simplicity and proactivity in solving large-scale problems. As a group with so many exposed assets, doing this work manually was simply impossible.
>
> The main transformation was gaining a complete view of our surface, which we previously lacked. What we have publicly exposed, their vulnerabilities, and our impact in the cyberspace.

ethiack.com

Autonomous Ethical Hacking