SUCCESS STORY

flare

# How EDHEC Protects 10,000 Students from External Cyber Threats Through a Proactive Approach

### The Customer

Founded 120 years ago, EDHEC is a business school with research centers and chairs supporting:

- 10,000 students
- 60,000 alumni benefitting from digital services
- 800 staff members

When 10,000 students use personal computers with varying levels of digital hygiene to access academic systems, credential compromise becomes inevitable. For EDHEC, the question was not whether student accounts would be targeted by infostealer malware, but rather how quickly the security team could detect and respond to leaks before attackers could exploit them.

## Challenge: Accounting for Varying Levels of Digital Hygiene for 10,000 Students

EDHEC operates an open and interconnected digital environment where protecting sensitive data is critical, including:

- students' personal information (GDPR)
- financial data
- professors' academic research
- employee information

In an academic environment where students use personal computers with varying levels of digital hygiene, student accounts represent a significant attack surface for the school.

When Sandy Rosada joined EDHEC four years ago as CISO, the IT department prioritized the protection of servers and infrastructure. However, proactive threat detection was lacking. The school had no visibility into its external attack surface, including discussions about EDHEC on malicious websites, data leaks on the dark web and Telegram, etc.

# Implementation: Detecting Infostealer Malware Targeting Students

While Sandy was searching for a Threat Exposure Management (TEM) solution, Flare stood out from the competition by providing direct access to the platform rather than sending reports, allowing EDHEC to immediately see results. Axel Vahé, recruited as a Cybersecurity Officer, actively contributed to the deployment of the solution.

From the POC onward, Sandy's team continued to see the ROI. The EDHEC team discovered numerous events, including compromised student accounts and leaks present on the dark web and Telegram. Analysis revealed that students were targeted by infostealer malware, often unknowingly, following the installation of malicious programs embedded in cracked software, particularly video games.

Onboarding went smoothly. The quality of support allowed EDHEC's security team, made up of only two people, to deploy the tool within one month, including configuring events to reduce noise. The platform proved to be intuitive and required no additional training or special skills to get started. To better integrate into their existing workflows, Flare was configured to send notifications via Microsoft Teams and email reports for events deemed critical.

# Benefits: Strengthening Proactive and Protective Actions

EDHEC moved from a reactive approach to a proactive approach and significantly increased the number of protective actions.

## Neutralizing Compromised Credentials Before Exploitation

> **Infostealer malware is such a pressing threat for our students, and the ability to react quickly is a must. Being alerted of a leak before an actual compromise and changing the passwords is priceless for the safety of our students and school.**
>
> **- Axel Vahé, Cybersecurity Officer, EDHEC**

During a technical support session with a student, EDHEC's security team discovered that the student's academic and personal credentials (including their family's) had been compromised by an infostealer. The infection was traced back to the unsanctioned download of a video game, a common vector for this type of malware. With Flare, the IT department found that these credentials were already being sold on the dark web. Passwords were immediately changed before an attacker could exploit them.

According to the Verizon DBIR, exposed credentials are exploited within a median of two days. With Flare, their detection and remediation can be carried out within minutes, well before any exploitation attempt.

## Taking Preventative Measures for Future Phishing Campaigns

Flare detected domain names resembling EDHEC's, in preparation for a future phishing campaign targeting payment fraud. This early visibility allowed the team to take preventive measures before the campaign was even launched.

By mitigating EDHEC's external threats, the IT department enables the school to fulfill its mission of protecting not only the institution and its employees, but also its students, without needing to control their personal devices.

# Forward Look: Training the First Line of Defense and Remediating Faster

In the future, EDHEC is focusing on two key initiatives: strengthening student awareness efforts and automating remediation workflows. Automation will allow faster responses by instantly blocking compromised accounts, even outside working hours.

To support these objectives, the IT department is evaluating the additional capabilities offered by Flare.