SUCCESS STORY

flare

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

The Customer

Founded 120 years ago, EDHEC Business School is a research and higher education institute serving:

- 10,000 students and growing across five campuses in the world
- 60,000 alumni with ongoing services
- 800 staff members

When 10,000 students use personal computers with varying levels of digital hygiene to access academic systems, compromised credentials become inevitable. For EDHEC Business School, the question wasn't if student accounts would be targeted by infostealer malware—but how quickly the Information Systems department could detect and respond to leaks before attackers could exploit them.

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

EDHEC manages an open and interconnected digital environment where protecting sensitive data without stifling academic excellence is crucial:

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

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

When Sandy Rosada joined EDHEC four years ago as CISO, the team was focused on protecting the servers and infrastructure. But proactive threat detection was missing, and the school had no visibility into its external attack surface, particularly regarding discussions about EDHEC on malicious sites or data leaks on the dark web and Telegram.

Implementation: Responding Quickly to Student Credential Leaks from Infostealer Malware

As Sandy searched for a Threat Exposure Management (TEM) solution, Flare differentiated itself from the competition by providing direct platform access instead of simple reports. EDHEC immediately saw results and value. Axel Vahé, who was recruited as the Cybersecurity Project Manager, contributed to the deployment of the solution.

From the POC onward, the team continued to see the ROI. Numerous events have been discovered, 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 cybersecurity 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: Boost Proactive, Protective Actions

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

Stopping Potential Leaked Credential Purchase Before it Happens

> **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 Project Manager, 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 security team detected that these credentials were already for sale on the dark web, and immediately changed them before an attacker exploited them.

According to the 2025 Verizon DBIR, attackers typically exploit exposed credentials within two days. EDHEC's security team was able to validate and remediate these compromised credentials before attackers could exploit them.

Taking Preventative Measures for Future Phishing Campaigns

In addition, the security team 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.

EDHEC's security team neutralizes external threats before they reach the institution, its employees, or its students. This approach protects the community without restricting personal devices or interfering with academic research and learning.

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

Next, EDHEC is pursuing two priorities: automating remediation workflows and expanding student security awareness. Automated workflows will block compromised accounts immediately, even outside business hours, while targeted education campaigns reduce risky student behavior at the source. To support these objectives, the security leaders are evaluating the additional capabilities offered by Flare.