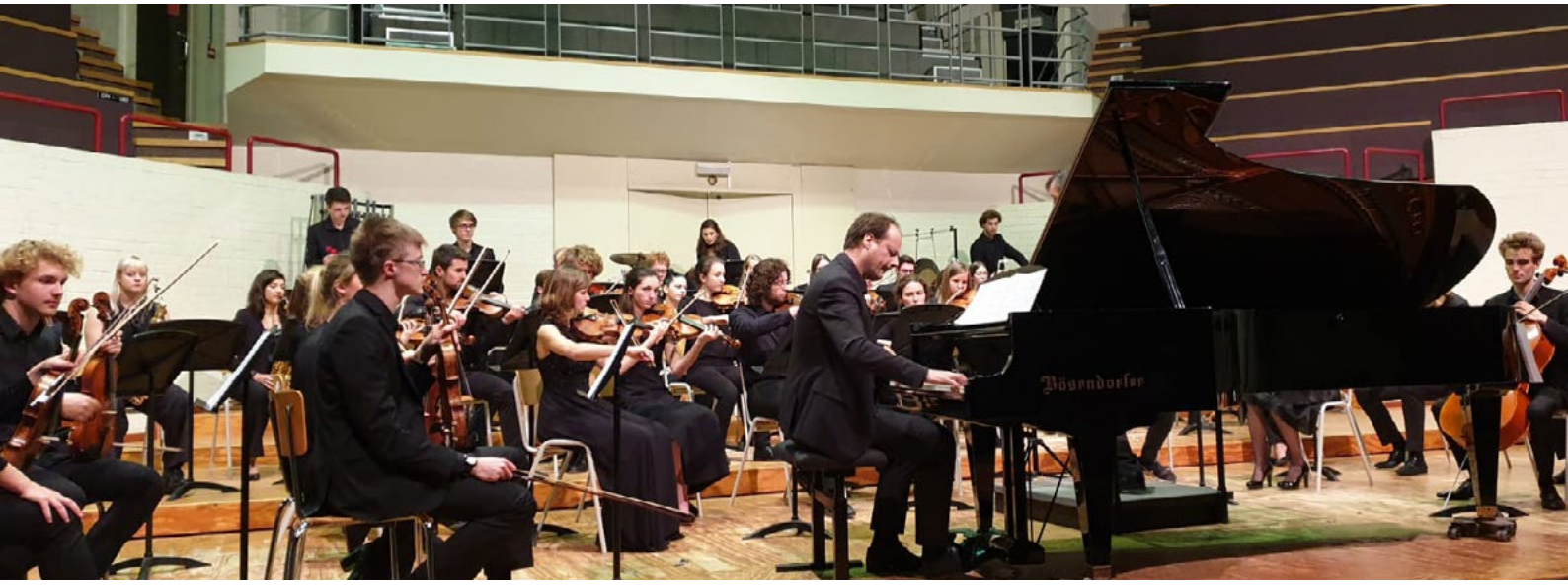
Orange
Cyberdefense

Customer stories

LUCA School of Arts chooses 24/7 Managed Detection & Response services after ransomware attack



At a glance

3,500
Each academic year, all these locations are home to approximately 3.500 students.

700
Arround 700 staff members.

5
Luca School Arts is spread over 5 campuses.

24/7
Luca School Arts is monitored 24/7 by Orange Cyberdefense's control room (CyberSOC)

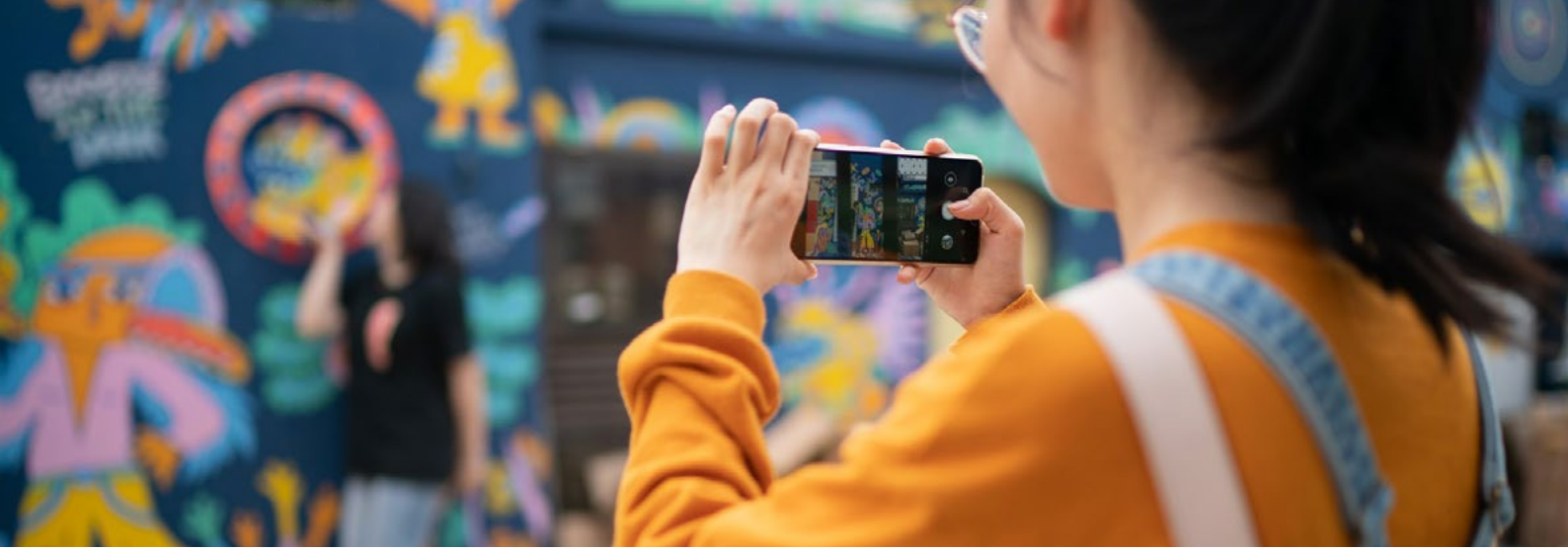
LUCA School of Arts is one of the best-known colleges for art education in Flanders. The institution offers a variety of 30 bachelor's and master's degrees in audiovisual arts and techniques, visual arts, performing arts, and music. LUCA School of Arts is spread over five campuses: C-mine Genk, Lemmensinstituut Leuven, Sint-Lukas Brussels, Sint-Lukas Ghent, and Narafi Brussels. The college is part of the Association KU Leuven. Each academic year, all these locations are home to approximately 3.500 students who are supervised by around 700 members of staff.

Phising mail shuts down school

It is hard to imagine education without technology these days, and certainly not in art education. For instance, there are various programs with a technological approach – think of interior design or film and photography. There is also a lot of digital communication. One of the biggest challenges is the BYOD story. "For students, too, their laptop has become a working tool that they bring along wherever they go. They expect to able to use this device in a secure environment," says Wim Pauwels, responsible for ICT infrastructure at LUCA School of Arts. "Monitoring this multitude of devices and at the same time providing good network facilities has become a security challenge." Especially with the exponential increase in cyberattacks.

As such, educational institutions are no more or less susceptible to cyberattacks than companies. Wim Pauwels: "What makes us more vulnerable, however, is the fact that we have an extremely variable and fragmented user group: thousands of students and hundreds of employees. In addition, we also offer quite a lot of applications."

In March 2020, LUCA School of Arts was hit by a cyberattack. As a result, the IT systems



were unavailable. A rapid intervention was required to get rid of the ransomware on the IT systems. But at the same time, a solution had to be found to avoid similar attacks in the future. “During the first analysis, we noticed that our users replied quite easily to phishing emails and then shared their login details just like that. That was also something to work on,” says Wim Pauwels.

Managed Detection and Response

To avoid such attacks in the future, LUCA School of Arts wanted a solution that had to meet two important criteria. A fast and secure system restart was needed in the short term. And the solution also had to detect and shut down any suspicious activities on the IT systems. Preferably 24/7. “Our internal IT team is too small to monitor all suspicious operations by themselves. So, we absolutely needed a Managed Detection & Response service. Moreover, detecting and monitoring is a very complex matter. We prefer to leave that to real experts.”

Eventually Orange Cyberdefense was chosen. They proposed an endpoint-based managed threat detection service. The managed detection & response service detects and automatically stops suspicious activities to ensure that the attacker cannot continue to move unnoticed in the college IT infrastructure. LUCA School of Arts can also rely on Orange Cyberdefense’s Dutch-speaking control room to intervene manually in exceptional cases.

The benefits

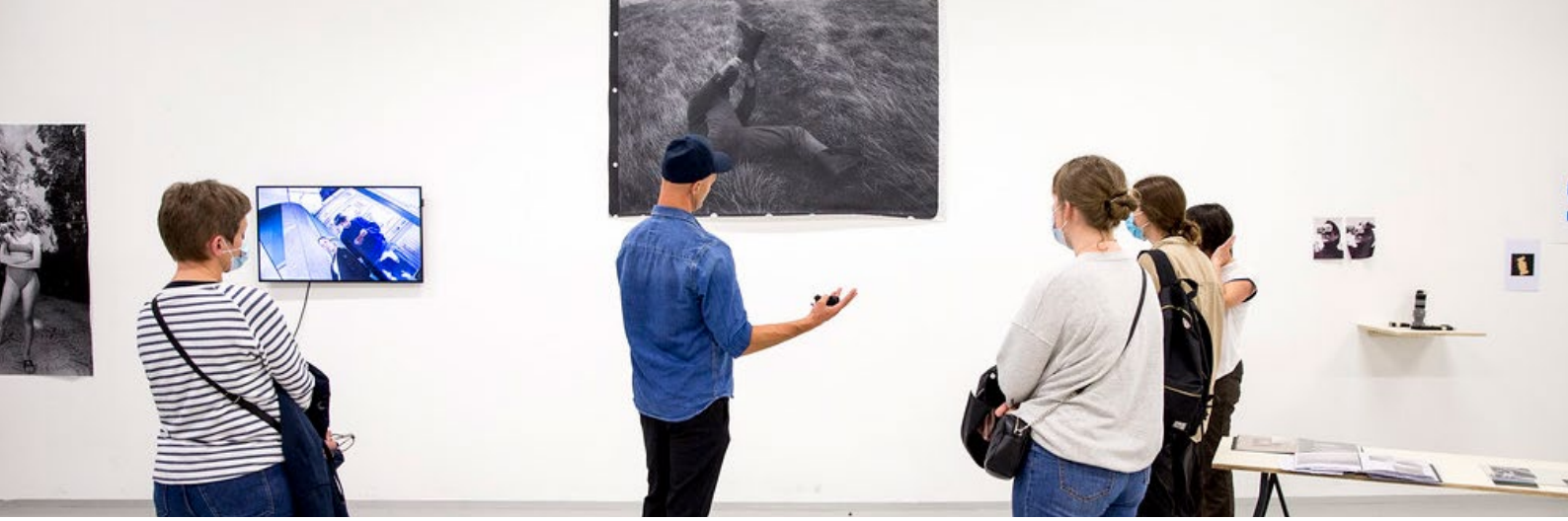
The main advantage of the solution is operational reliability. Wim Pauwels: “We have now seen that a cyberattack can shut down a college or any organization. This Managed Threat Detection enables us to respond directly to suspicious activities on an enduser’s device.”

A second benefit is the professional approach of Orange Cyberdefense. The combination of their expertise and speed ensured that the service could be activated quickly. “Two weeks after the ransomware attack, we could start deploying the endpoint detection and response software. And after just one month, our IT infrastructure was already monitored 24/7 by Orange Cyberdefense’s control room (CyberSOC). The local presence of Orange Cyberdefense is a great added value. The fact that CyberSOC is Dutch-speaking, facilitated communication even more,” explains Wim Pauwels.

Result

At the moment, the college has been completely restarted. More than 600 software agents of the endpoint detection and response solution have been installed on end-users’ devices and on the school’s servers. All these devices are thus monitored and secured 24/7. The college can

> “For the IT team, the managed detection & response service means good night’s sleep and peace of mind.”
>
> **Wim Pauwels | Responsible for ICT infrastructure at LUCA School of Arts**



also continue to provide all applications in a user-friendly environment. Wim Pauwels: “The service activation happened about six months ago. In the past four months alone, an average of about three suspicious incidents was detected each month. The service sees them, and Orange Cyberdefense’s control room notifies us immediately if they are indeed dangerous operations.”

The managed detection and response service responds appropriately to detections. Orange Cyberdefense quickly determines the risk and possible impact. The detections by the software are a solid base, but Orange Cyberdefense also relies on its own analysis and knowledge to provide an adequate assessment. The importance of a security analyst should not be underestimated when making the right choice.

The future

The next step in LUCA’s story is to increase security awareness and to raise awareness among users. LUCA School of Arts still sees users clicking on phishing emails and revealing their login and password. Wim Pauwels: “Since the attack of last spring, we had another phishing attack this summer. Several users have clicked on the link, fortunately, without negative consequences for our IT environment. Thanks to the solution and professionalism of Orange Cyberdefense. But it shows once again that we need to continuously raise awareness among our users to recognize and block such emails. For this, we will probably reach out to other services of Orange Cyberdefense,” concludes Wim Pauwels.

- Perfect solution to mitigate risks in a short period of time.
- Secure environment: the managed detection & response service automatically detects suspicious operations and responds in an appropriate way.
- CyberSOC: 24/7 monitoring, analysis and alerting gives the small IT team the required security.

About Orange Cyberdefense

Orange Cyberdefense is the expert cybersecurity business unit of the Orange Group. As Europe’s go-to security provider, we strive to build a safer digital society.

We are a threat research and intelligence-driven security provider offering unparalleled access to current and emerging threats.

Orange Cyberdefense retains a 25+ year track record in information security, 250+ researchers and analysts 16 SOCs, 10 CyberSOCs and 4 CERTs distributed across the world and sales and services support in 160 countries. We are proud to say we can offer global protection with local expertise and support our customers throughout the entire threat lifecycle.