Euronext Safeguards Pan-European Trading with Cymulate

Organization

Euronext is the leading Pan-European marketplace, rooted in four centuries of exchanges that are now at the heart of European capital markets. The exchange boasts 1,300 domestic and foreign companies listed for trading, with a combined 3.5 trillion Euro market capitalization.

Euronext's Information Security Department
Euronext's information security department is comprised of multiple teams, including its Security Operation Centre (SOC) team and the Assessment and Exploitation Team. The SOC's main responsibility is to continuously monitor and improve the organization's security posture by managing its incident response, while the Assessment and Exploitation Team is responsible for running vulnerability and red team assessments. The SOC works around the clock and is entrusted monitoring all of Euronext's infrastructure and systems, trading services and platforms, as well as all internal and external users, including the stock exchange service itself.

Business Challenge

The Information Security Department is experienced in developing and running their own homegrown simulations of cyberattacks to test the organization's security posture vis-à-vis specific threats.
Keeping a vigilant eye out for the latest developments in the cybersecurity market, Jorge Ruão, Head of Security Operations Centre at Euronext, sought more efficient ways to prevent and detect cyber attacks.

After implementing new technology, deploying a specific security policy or updating the rule engine of a cybersecurity tool, the teams would run simulations of specific attacks to ensure that they could be blocked, or alternatively, be detected and mitigated.

While the practice of running attack simulations is highly effective, building simulations of specific attacks can be a resource-intensive undertaking, depending on the complexity of a malware strain or its associated variants.

"This is of special concern if time is critical, "says Ruão, "for example, when you are made aware of a new malware campaign exploiting zero-day vulnerabilities that is spreading through the internet."

Challenge
Euronext sought a more efficient and cost-effective way to continuously test its security posture.

Solution
By deploying Cymulate, Euronext can quickly run simulations of the very latest cyber attack, repeatedly and frequently.

Benefits
The team can easily determine the impact of new technology, security controls, and configuration changes on its security stack, while proving the value of business decisions with transparency.

Solution

Commenting about the initial integration, Ruão says, “It was very easy and quick to deploy the solution with satisfactory results." Ruão was impressed by Cymulate’s ease of use and ability to repeatedly run the same battery of assessments to test the organization’s security posture. Using the cyberattack simulation platform removed the need to build and prepare a manual framework to execute those very same tests.
On top of manual penetration testing, red team exercises, and vulnerability assessments performed periodically, Cymulate enables Euronext’s Information Security department to run continuous security tests.

For example, “when there is a new specific threat in the wild, Cymulate incorporates the threat’s indicators of compromise (IoCs) very quickly,” comments Ruão, “and we can immediately see how vulnerable we are to that threat without the need to internally develop a simulation to mimic it." Similarly, if a security tool suddenly proves to be less effective following a configuration change, its settings can be updated and then thoroughly tested against a barrage of simulated cyber attacks.

Having purchased four Cymulate attack modules the year prior, including the Immediate Threat Assessment, Web Gateway, Email and Endpoint modules, Euronext renewed their Cymulate subscription and added the Hopper module to simulate potential lateral movement within the company’s network.

> *I would recommend Cymulate because of its ease of use; it can quickly provide you a window into how vulnerable or how protected your organization is against external threats.*
>
> Jorge Ruão, Head of Security Operations, Euronext

Benefits

Since deploying the solution, both the SOC and Assessment and Exploitation teams use Cymulate together to discover and understand whether current security controls are blocking threats. By using Cymulate, Euronext’s Information Security Department can:

- **Test controls against the latest threats**
  Imminent attacks detected in the wild are simulated by the platform, enabling up-to-date security assessments.
- **Frequently and repeatedly evaluate security controls**
  New technology, configuration changes, or software and hardware updates can be easily tested to see their impact on the organization.
- **Complement homegrown simulations**
  While highly effective, these are resource intensive. Cymulate provides ready-to-use prepackaged threat intelligence-led assessments.
- **Prove the value of business decisions**
  By using Cymulate as a benchmark before deploying new technology, the team can demonstrate the efficacy of new solutions.
- **Understand cyber threats’ modus operandi**
  Discover where in the attack kill chain a potential threat may be successful in circumventing security controls.
- **Provide executive and technical reporting**
  With its automated reports, visibility is provided into how each technology contributes to the organization’s overall security posture.

About Cymulate

Cymulate Extended Security Posture Management solutions enable companies to challenge, assess and optimize their cybersecurity posture against evolving threats, simply and continuously.

Contact us for a live demo, or get started with a free trial

Start Your Free Trial