OVERVIEW

ManoMano is Europe’s leading marketplace for DIY home improvement and gardening online.

Challenge

By the end of 2019, the global ecommerce market reached $3.5 trillion¹, representing 14% of total global retail sales. Today, as consumers are motivated to stay — and shop — at home like never before, these numbers are skyrocketing.

This unprecedented growth has brought unwelcome attention to the e-commerce industry from threat actors who are dialing up distributed denial-of-service attacks (DDoS), credit card fraud, and malware infections. They’re also deploying armies of “bad bots” that are able to test-drive stolen credit card data and credentials, and price-scrape to undercut the competition.

At ManoMano, security is paramount. The organization recognizes that to earn — and keep — public trust, they must vigorously protect their customer and seller data. ManoMano’s CISO Fabien Lemarchand summarizes the security team’s approach in two words, “people” and “offense.”

When Fabien joined ManoMano to build a security team from the ground up, one of his first priorities was implementing a threat intelligence tool that could identify, even anticipate, the next cyber threat to the business and the e-commerce industry at large, while focusing his team's efforts on the threats that matter most.

Solution

Fabien explains, “Our mantra and guiding security pillar is, ‘Know your enemy, find threats, and remediate them with excellence.’ This sums up quite well what we were looking for in a threat intelligence partner.”

Recorded Future checked all of these boxes and more by combining analytics with human expertise to produce elite security intelligence that disrupts adversaries at scale.

Before long, Fabien and the ManoMano team were tapping into Recorded Future for a wide variety of use cases, such as:

- **Pinpointing Looming Phishing Attacks.** By continuously monitoring for typosquat domains, Recorded Future alerts the security team in real time when a fraudulent domain (like a fake check-out page, URL modification, phony PayPal account suspension, etc.) threatens the brand. This enables the team to act quickly, take it down, and prevent future phishing attacks.

¹ https://www.statista.com/study/10653/e-commerce-worldwide-statista-dossier/
CASE STUDY

• Monitoring the Tech Stack for Vulnerabilities. Security intelligence aggregates data from the broadest range and variety of sources to deliver context around newly disclosed vulnerabilities in ManoMano’s existing technologies. This gained significant importance as remote employees became even more reliant on VPN technology and collaboration tools during COVID-19.

• Protecting the Third-Party Ecosystem. ManoMano relies on a large network of suppliers and third-party services like payments, site search, and analytics to enhance its e-commerce platform. Security intelligence delivers an unprecedented, continuous view of their partners’ security risk, driving fast, informed decisions and reducing overall risk to the business.

Results

“Security intelligence is like an Oracle, providing you a clear vision of what is happening on the web, what is happening around your business, and empowering you to focus on the right threats,” says Fabien.

He continues, “Thanks to Recorded Future, we can not only monitor everything occurring on the web, focus on current attacks, and protect our infrastructure, but also adapt ourselves quickly to tackle the new threats. For instance, COVID-19 shifted our priorities: We suddenly needed to harden the security of critical endpoints to enable remote work.”

As ManoMano moves toward a comprehensive security intelligence approach, they plan to expand their use of Recorded Future. This will include integrating elite intelligence with their internal security monitoring infrastructure to enable instant prioritization of alerts, incidents, and vulnerabilities based on real-time risk scores from the world’s most advanced security intelligence platform.

The ManoMano team also put security intelligence to work detecting data and credential leaks on the dark web — a major challenge that many e-commerce companies face. In the wrong hands, this data can be used to compromise business email accounts, breach critical systems, and steal information.

After observing a surge in bad bot activity, Fabien and security software engineer Laurent Delosieres decided to investigate the Genesis Store — a huge underground marketplace that sells bots and associated compromised credentials. Not just anyone can enter the Genesis Store, however — you need an invitation. So, the team used Recorded Future to scour the dark web. Within minutes, ManoMano had the code they needed to unlock access.

“Searching for any internal compromised computers was our first reflex. To our relief, the result was negative, however six of our sellers were compromised. Since our relationships with our sellers are essential, we bought those accounts and informed the respective sellers of their security issues,” recalls Laurent.

About Recorded Future

Recorded Future delivers the world’s most technically advanced security intelligence to disrupt adversaries, empower defenders, and protect organizations. Recorded Future’s proactive and predictive platform provides elite, context-rich, actionable intelligence in real time that’s intuitive and ready for integration across the security ecosystem.