Case Study

AI-driven cybersecurity for online gaming sites

Online gaming is a favorite pastime for millions, and this operator runs many of the biggest sites and collections of brands in its sector. Action is nonstop, and players have access to a huge selection of games and tournaments. This company has operations in more than a dozen locations across North America, Europe and Asia Pacific.

Online gaming is a big target

Cybersecurity is paramount for gaming sites, and to maintain its competitive advantage, the company must deliver the best experience for gamers, guard its operations and protect its brands.

Gaming companies are lucrative targets for cybercriminals who range from solo actors to organized rings. Nor is the threat only external: Insiders could use privileged access into systems and data for illicit purposes.

Unchecked ransomware can quickly turn into extortion and disruption. An outage or breach can deliver instant material damage to the company's income, customer retention and long-term brand value.

Another potential payout for criminals: The company's gaming software is a market leader, and it must tightly control and protect its intellectual property.

In addition, the company is publicly traded and operates in a highly regulated environment. It must comply with a broad range of requirements, including the Payment Card Industry Data Security Standard (PCI-DSS) and European Union General Data Protection Regulation (GDPR).

Organization

Global online gaming brand

Industry

Online gaming

Challenge

Stay constantly vigilant to threats without staffing 24x7 security operations

Selection criteria

AI threat hunting tool that automatically detects a broad range of threats with a minimal burden on security analysts

Results

- Proactively detect complex, multistage attacks before damage is done
- Focus on the highest-risk threats and reduce an overwhelming volume of security alerts and false positives
- Easily integrate threat detection with big-data analytics and enforcement tools

VECTRA®
Security that thinks®

Constant vigilance

The gaming site wanted to be vigilant about threats and attacks. And it wanted to detect stealthy, in-progress cyberattacks inside its network before damage is done. The security team needed to hunt for threats around the clock without requiring security teams to be present on site 24/7.

At the same time, security analysts were overwhelmed by the volume of alerts – and the inevitable time-wasting false positives – from their security tools, such as security information event management (SIEM), firewalls and other defenses.

Going all-in on AI threat hunting

The security team knew that using AI to hunt for threats would give them an edge, especially against today's organized criminals and highly evasive threats.

"The threat landscape is in rapid and constant flux," says the company's head of information security. "Adopting an approach that detects threat behaviors helps us stay ahead."

AI-based threat hunting can automatically detect hidden and unknown attacks while lifting much of the manual work that consumes security analysts' time and resources.

The tools show their hands

The company set out to evaluate the leading AI-based cybersecurity tools.

After extensive in-house testing of multiple leading AI-based threat detection tools on its production network, it selected the Cognito® the threat detection and response platform from Vectra®.

"During a recent regulatory audit and penetration test, Cognito's performance was simply fantastic, all with zero overhead from my team," says the company's head of information security.

Nonstop threat surveillance

With Cognito, the security team has AI that automates cyberattack detection and response. Cognito proactively exposes advanced cyberattackers that could otherwise spread inside the company's network – from its data center workloads to user devices in two dozen offices around the world.

"Cognito finds things that all of our other security tools miss," says one security analyst.

The online gaming company found that Cognito had a broader range of attacker detections and presented deeper threat evidence and context, compared to other threat detection solutions it tested.

Cognito uses a broad set of data science techniques and machine learning that leverage deep learning and neural networks, enabling Cognito to continuously learn and detect never-beforeseen threats.

With Cognito, the security team has a complete and dynamic view into the complex chain of events that make up multistage attacks. The highest-risk threats are prioritized on Cognito's intuitive user interface and security analysts are alerted.

Cognito added immediate value and was easier to deploy than the other threat detection tools the company tested. With Cognito's open APIs, integration with the company's existing security tools and in-house big-data analytics platform was straightforward.

Hitting the jackpot

Automating threat hunting with Cognito has enabled the online gaming company to hunt threats around-the-clock without increasing staffing. The security team has the constant vigilance it sought. Cognito doesn't eat or sleep, and doesn't need nights and weekends off.

Cognito significantly reduced the time and effort required to identify, understand and resolve cyberattacks. The team's incident response capability is far more agile now. What took hours or days now takes minutes.

With the ability to detect and stop in-progress attacks faster than ever, the company can protect its loyal customers, uphold its brand reputation and maintain the trust of regulators as it seeks to expand in the lucrative online gaming market.

> *"Cognito finds things that all our other security tools miss."*
>
> Security Analyst
> Online gaming company

VECTRA
Security that thinks®

Email info@vectra.ai **Phone** +1 408-326-2020 www.vectra.ai