CASE STUDY

Playtika manages security with 50% fewer resources using Palo Alto Networks Cortex XSOAR

A lack of security visibility, increased complexity of investigations, and alert fatigue were stretching Playtika's lean security operations team to the limit. By standardising on the modern Palo Alto Networks Cortex XSOAR platform as part of a wider security transformation strategy, the leading global gaming company are transforming their security posture and elevating their agility and efficiency. Automation enables security events to be managed using half the amount of people, mean time to respond (MTTR) is reduced by almost 80%, and a Cortex XSOAR chatbot is estimated to save 15% of analysts' time.

IN BRIEF

Customer
Playtika

Organisation Size
34 million monthly active users, 4,000+ employees

Industry
Entertainment

Featured Products and Services
Portfolio of entertainment games

Location
Herzliya, Israel

Challenges

The volume of manual security alerts and tasks delayed response time. There was a lack of consistent response to alerts. The growing complexity of investigations and fragmented security approach delayed response time and increased risk profile.

Requirements

- Complete, connected cybersecurity platform.
- Modern, faster security operations to stay ahead of future threats.
- Reduce security operations tasks and eliminate threats.

Solution

Palo Alto Networks Cortex XSOAR

CHALLENGES

Gaming thrills at every turn

Playtika have been pioneers in the games industry for over a decade, and have more than 34 million monthly active users. The Israeli-based multinational organisation are continually adding innovative games with challenges and thrills at every twist and turn.

Until recently, Playtika were relying on a managed security operations centre (SOC) to support their global cybersecurity operations. The third-party SOC provider – and the two embedded Playtika analysts – were struggling to quickly identify, prioritise, and respond to security incidents. And the problem was getting worse.

Liran Sheinbox, Head of Cyber Security, Playtika, explains, “When our IPO was announced in January 2020, that number tripled. We were too slow to respond to this growing volume of incidents. We also lacked a consistent response. Each time there was a phishing attempt, for example, we would respond in a different way. That fragmented approach delayed our reaction.”

With the gaming industry moving so quickly, change was needed fast. “We wanted a consistent, holistic approach to cybersecurity, using modern technologies like AI and automation to efficiently safeguard the organisation, ” explains Liran.

> The incident meantime to repair took 3.5 hours on average. Part of the reason for this was the SOC set-up. The people in the SOC were the point of integration across different systems – acting as 'swivel-chair' integration – and that slowed us down and invited errors.
>
> **–Liran Sheinbox, Head of Cyber Security, Playtika**

REQUIREMENTS

Reimagine security operations and streamline security operations tasks

Liran and his team identified the need to reimagine security operations – to move away from a traditional manual and reactive approach to an efficient, progressive stance as part of a broader security transformation strategy. Playtika's requirements included:

- A complete, connected cybersecurity platform.
- A modern security operation, enabling better, faster cybersecurity processes to stay ahead of future threats.
- The elimination of threats and a reduction in security operations tasks.
- The unification of threat intelligence aggregation, scoring, and sharing.

SOLUTION

Leader of cybersecurity

Playtika have standardised on the Palo Alto Networks portfolio as part of their enterprise-wide security transformation programme. The comprehensive, connected cybersecurity portfolio helps prevent successful cyberattacks by using an automated approach to deliver consistent security across cloud, network, and applications.

For Playtika, the portfolio spans ML-Powered Next-Generation Firewalls (NGFWs) network security, Prisma Cloud for cloud security posture and cloud workload security, GlobalProtect to safeguard remote working, and the vital component of this security transformation programme, Cortex XSOAR.

> “From my experience, Palo Alto Networks leads the cybersecurity industry. The entire portfolio boasts best-in-class capabilities and frictionless integration – and it’s proven in the market to deliver on its promises.

–Liran Sheinbox, Head of Cyber Security, Playtika

Cortex XSOAR provides modern security orchestration, automation, and response that help Playtika reinvent security operations using artificial intelligence (AI) and automation to detect, investigate, and respond to threats.

The deployment of Cortex XSOAR coincided with the decision to bring the SOC in-house. The SOC now monitors data collected from the ML-Powered NGFWs in the data centre, from thousands of endpoints, and from other sources – leveraging automation and playbooks to transform how the five-strong SOC team manages security operations.

One innovation is the Cortex XSOAR chatbot. If an incident occurs, an automated decision tree determines the subsequent actions, with the chatbot notifying users of progress. Liran explains, “If someone requests a password reset, for instance, the bot asks, ‘Did you request this?’ If they didn’t, a new playbook launches to automate the security process. It’s quick, secure, and doesn’t need any intervention.”

> “XSOAR has been a huge success. Playbook automation, for example, has transformed deployment across a vast number of security use cases.

–Liran Sheinbox, Head of Cyber Security, Playtika

BENEFITS

Operate and innovate at pace

Cortex XSOAR is freeing Playtika to operate and innovate with speed and safety. “Cortex XSOAR supercharges our SOC efficiency,” says Liran.

The benefits of security orchestration include:

- **Doubling SOC productivity**: By liberating resources, Playtika can manage security operations without hiring additional headcount. “Without Cortex XSOAR we’d need twice the number of people we have now to manage events,” says Liran.
- **Decreasing MTTR by 80%**: Intelligent automation and playbooks have reduced MTTR from an average of 3.5 hours to 45 minutes (78%). Teams can manage alerts across all sources, standardise processes with playbooks, and automate responses for any security use case.
- **Automating 50% of incidents**: Within six months of go-live, Cortex XSOAR was automating 50% of the incidents currently logged daily. This percentage is expected to increase in due course, through playbooks and other automation.
- **Saving 15% of analyst time by introducing Chatbot**: XSOAR ingests alerts from threat intelligence sources and orchestrates bot logic via a playbook. “The automated bot shows we are saving up to US$5 million. Although we can’t rely on that figure, the bot is making a huge difference to our productivity. We class the bot as another member of the team; it’s that important,” says Liran.

“Palo Alto Networks Cortex XSOAR enables the art of automation,” says Liran. “The platform provides powerful detections and alerts to drive orchestrated workflows. This ultimately helps us create exciting, compliant video games more quickly and at lower risk.”

> “Without Cortex XSOAR, we’d need twice the number of people we have now to manage events.
>
> **–Liran Sheinbox, Head of Cyber Security, Playtika**

Read the Playtika portfolio story to discover the power of a comprehensive, connected security approach.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com