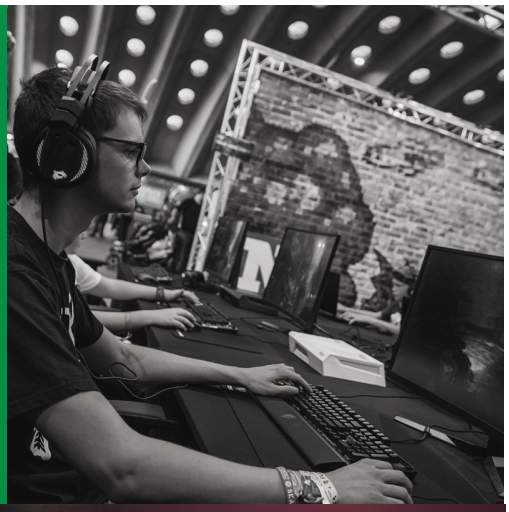
Gaming Case Study

Southern California's premier gaming organization (with 2,000+ slots + favorite table games and luxury hotels and outstanding restaurants) deployed Seceon aiSIEM Platform for comprehensive visibility, proactive threat detection, and automated blocking or containment of threats in real-time.



"We are always focused on offering our customers the best experience and that requires us to deploy our applications and services without friction, but security and a frictionless environment do not normally go hand in hand. When the Seceon platform was suggested we were skeptical and asked for a proof of concept. We were surprised to see its value within days of deployment," said the VP of IT and Cybersecurity at a premium gaming organization.

Our hunt for next-gen security solutions had ended and after a few months of operation, and seeing the value of AI and ML on telemetry ingested from all fall our infrastructure and core systems and applications we were satisfied that we found the solution we needed. I even discussed the platform with my peer group in the industry. He continued, *"Despite evaluating a number of security solutions, including SIEM solutions and behavioral analysis solutions, we could not find any that can be brought together under one umbrella."*
My industry experience and evaluation of many cybersecurity products helped me realize the platform approach taken by Seceon is the right vs. other point solutions in the market.

- VP of IT & Cybersecurity
Premium Gaming Organization

As security breaches and hacks continue to lead global headlines, legacy solutions are no longer able to cope; even with nine security products deployed, our client did not have visibility of all the activities on their network. Multiple products were generating multiple alerts and over 50% of them went un-reviewed due to the volume and history of false positives. Their existing MSSP did not offer any actionable intelligence and had no automation capability. Sophisticated attackers, zero-day attacks, ransomware as a service generated attacks all pose a huge challenge for any organization. Due to the possible rewards, the gaming industry is a prime target for bad actors. One of the biggest challenges for their MSSP was trying to integrate nine point solutions from different vendors, all of which created different IOCs and generated more noise than they could handle or missed major events altogether.

"Seceon's aiSIEM, aiXDR and aiMSSP platform, with its ability to ingest raw logs and flows from various sources, including alerts from existing security products already deployed in the network and endpoint, immediately provided our client with the visibility of all of their assets and their functionality and interactions in real time. It helped us detect some rogue applications and hosts, which were eliminated and improved their cybersecurity posture significantly within two weeks of deployment."

One of the differentiators for Seceon is the ability for automated or push button remediation. Seceon's platform leverages the power of AI/ML and has the ability to respond and contain and eliminate threats in real-time. Most current and legacy security solutions lack this ability.

Due to the ease of integration and correlation of different events Seceon is able to provide comprehensive transparency, context and situational awareness when alerts are escalated. "Seceon's machine learning capability has been key to reducing noise and ensuring that critical alerts get the attention they require," said the VP of IT and Security for Premium Gaming Organization.

Challenges:

- Traditional solutions and services from large vendors could neither combat the increasing sophistication of cyber threats nor could detect between perimeter and endpoint threats to the required level.
- The level of protection afforded by a point solution tech-stack approach adds significant CAPEX and OPEX and never delivers the desired result and causes alert fatigue.
- Integration is the biggest challenge as point solutions from different vendors are not built to communicate with each other, often leading to a miss-match of IOCs and attack forensics.

Solution:

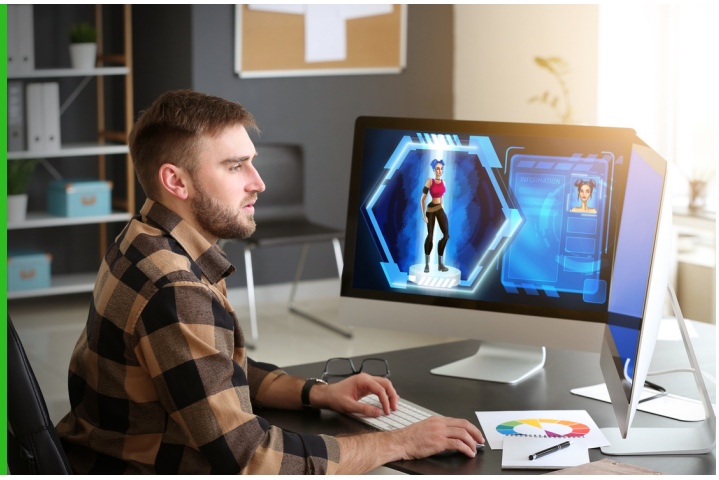
- Analyzes all raw logs, Identity and network traffic, utilizes ML, AI and Dynamic Threat Models to provide "Continuous real-time Monitoring, proactive Detection and auto blocking or quarantine of threats and breaches"
- Single platform eliminates the need for 10+ point solutions like SIEM, UEBA, SOAR, NDR, XDR, NBAD, IDS, Threat Intelligence, ML and AI.

Benefits:

- Increases efficiency of personnel and security team by 89%
- Ease of set-up and integration brings together a variety of seemingly unrelated threat indicators to identify potential issues
- Ability to remediate (contain and eliminate) threats in real-time

"Seceon's machine learning capability has been key to reducing noise and ensuring that critical alerts get the the attention they require."

IT and Cybersecurity Engineer
Premium Gaming Organization



Another advantage of Seceon OTM is the ease of set-up. This case study for a premium gaming organization demonstrated that one businesses possible.

The major use cases to addressed were:

- Real-Time, comprehensive visibility
- Ransomware and malware detection in early stages
- Ability to detect various external and internal threats
- Automated remediation of threats and breaches

Prior to Seceon aiSIEM, the premium gaming organization used nine traditional solutions and services from large market leaders, however, it was always challenging to find a solution that could detect/cover between perimeter and endpoints to the required level of sophistication. The multi-layered approaches recommended by industry experts were rendered ineffective without proper integration between security solutions.

About Seceon

Seceon enables MSPs and MSSPs to reduce cyber threat risks and their security stack complexity while greatly improving their ability to detect and block threats, and breaches at scale. Seceon's Open Threat Management (OTM) platform augments and automates MSP and MSSP security services with our AI and ML-powered aiSIEM, aiXDR and aiMSSP platform. The platform delivers gapless coverage by collecting telemetry from logs, identity management, networks, endpoints, clouds, and applications. It's all enriched and analyzed in real-time by applying threat intelligence, AI and ML models built on behavioral analysis, and correlation engines to create reliable, transparent detections and alerts. Over 300 partners are reselling and/or running high-margin, efficient security services with automated cyber threat remediation and continuous compliance for over 7,500 clients.

Learn more about Seceon aiXDR and

Schedule a Demo www.seceon.com/contact/