FORTSCALE

Playtech Secures Sensitive Customer Data with Fortscale User Behavior Analytics

AT A GLANCE

The Need
Secure sensitive customer data against stealthy user-based threats

The Challenge
Generate accurate alerts from huge volumes of log data with minimum false positives

The Solution
Fortscale's User Behavior Analytics

Why Fortscale
Proven user behavior analytics based on advanced machine learning and user profiling algorithms

The Results
Better visibility of user behavior, faster time to remediation, enhanced ROI from SOC team

Background

Founded in 1999, Playtech is a world leader in the online gaming industry and has more than 3,600 employees located in 12 countries. Its infrastructure powers a wide range of gaming applications, live sports betting, and mobile and social gaming – supporting millions of users worldwide.

As an industry leader, Playtech builds its business reputation upon protecting the strict confidentiality of its customers' financial and personal data, as required by international regulatory bodies. Accordingly, it treats this sensitive customer information as its crown jewels.

Playtech's growth has been achieved through multiple acquisitions and integrations with leading gaming providers and operators. To support its diverse operations, Playtech operates dozens of segregated production environments and uses multiple security systems.

The Challenge:

Turning Big Data Analytics into User Intelligence

Realizing that traditional SIEM systems and signature-based tools are not enough to mitigate sophisticated cyber attacks, Playtech invested a significant effort in deploying one of the industry's leading SIEM solutions to address this need. This complex deployment involved a large customization effort, which was both long and expensive.

However, when it came to discovering stealthy user-based threats, Playtech found that it still needed a better way to help its investigators filter out the false alarms from the real threats. Playtech collects huge volumes of log and event data from hundreds of sources. And it had a brand new security analytics system in place to help its analysts sift through this data and detect abnormal behavior. The real challenge – as it turned out – was finding a way to generate smarter alerts with a low false positive rate. After a bit of research, Playtech reached the conclusion that machine learning algorithms, which profile user behavior across multiple dimensions, would help its analysts discover and mitigate user-based threats quickly and with minimum false positives. Enter Fortscale.

> “Playtech’s analysts were able to quickly understand root cause and disconnect the ‘compromised’ computer from the network, before any damage was caused.”

The Solution:

Fortscale User Behavior Analytics

With these requirements in mind, the customer decided to evaluate Fortscale’s User Behavior Analytics solution. Fortscale’s advanced machine learning algorithms were exactly what it needed to complement Splunk and the skills of its own in-house security team. In addition, the fact that these algorithms run on Hadoop allowed the customer to leverage its existing Hadoop big data cluster.

Moreover, Fortscale seamlessly connects to the customer’s Splunk environment, retrieves the log data associated with user login activities, and generates insights into abnormal and suspicious user behaviors for immediate investigation by analysts. Fortscale also sessionizes the data, giving each event a broader user context. Based on the customer’s specific requirements, Fortscale also built 5-10 custom tailored reports to address scenarios related to the company’s proprietary system and data environment.

The first stage of the evaluation was a two-week pilot, whose objective was to examine the ability of Fortscale’s machine-learning algorithms to discover a set of known user-based threats. Not only did Fortscale identify all known threats, it also discovered some unknown scenarios worthy of investigation.

Buoyed by these outstanding results, the customer decided to proceed with full system deployment. This included preparing the system to handle live streams of data from Splunk, as well as building user profiles over a longer time period based on historical data in order to improve algorithm accuracy.

In addition to its machine-learning algorithms, Fortscale’s system comes with a set of core analyst reports, designed to help analysts identify and investigate common security scenarios (e.g., geo-hopping, VPN exfiltration). Each report includes a dedicated set of tables, widgets, and visualizations that make it easy for analysts to view all information relevant to a given scenario.

FORTSCALE

ABOUT FORTSCALE

Fortscale combines expertise from the Israeli Defense Force, big data analytics, and advanced machine learning to rapidly detect and eliminate insider threats to enterprise information and assets.

Backed by Intel Capital and Blumberg Capital. Named a finalist in the 2015 RSA® "Innovation Sandbox" competition. Trusted by a growing number of the Fortune 2000. Fortscale provides the tools to neutralize insider threats faster, more easily, and far more effectively than any other solution available.

www.fortscale.com

The Results:

Better Visibility and Faster Time to Remediation

Playtech is using Fortscale's solution to increase the productivity of its SOC analysts. In one investigation scenario that did not result in any damage, an analyst checked the system and saw that one user was ranked as "suspicious" after his machine had tried to access an unusual number of workstations in one hour. The user was not even aware of this behavior.

Using Fortscale and its own forensics tools, Playtech was able to view the full scope of user activity, i.e., no anomalies in VPN activity and only internal authentications. The investigator discovered the reason for multiple authentications was an EXE file on the user's machine, running authentication attempts to multiple network destinations. It turned out that this user was using a Torrent client to download software and accidentally downloaded a malicious EXE file, which was silently installed on his machine. In this ultimately harmless incident, the offender was a sloppy user; however, this same scenario could easily have indicated a dangerous type of lateral movement by a malicious intruder.

Based on Fortscale's user intelligence, Playtech's analysts were able to quickly understand the root cause and disconnect the compromised computer from the network before any damage was caused. Then, its forensics experts were able to delete the EXE file, make sure any other remnants of the file were gone, and send a copy of EXE file to a sterile lab environment for further investigation of its capabilities.

Learn more about using user behavioral analytics to mitigate security threats from malicious or rogue employees and external hackers operating inside your network. Visit **www.fortscale.com.**