CYREBRO

Deep Visibility & Actionable Security Operations With CYREBRO

New York Hedge Fund
Case Study

The Challenge

- Too Many Security Tools
- The Need to Optimize and Scale
- Lack of Inhouse Cybersecurity Expertise
- No 24/7 Monitoring & Response

About the company

CYREBRO

An alternative capital, US hedge fund established in 2006.

The company is one of the top US hedge funds in the alternative investment space and invests in various public equity markets including financial, telecom, healthcare and industrial companies, on a global scale. They implement long-short investment strategies through qualitative and quantitative analysis methods, generating high returns for its clients. Its high-level investment decisions are made by employing a variety of resources such as public financial statements, Wall Street research and consultants and bankers.

The company maintains a transparent approach and meets all industry best practices.

A few years ago, having an antivirus and firewall solution was the norm within the alternative investment space as well as in other industries. Focusing on “bad actors” or searching for nextgeneration SOC solutions only began when the SCC regulated the alternative investment industry to implement IPS (Intrusion Prevention Detection) platforms. This was a huge transition.

Within two years of implementing several security platforms, the SCC released another regulation for further cybersecurity requirements.

With a vast amount of systems and platforms already in place, optimizing was an enourmous challenge. The customer was in need of in depth assessment of their network security posture and provide them with clear cybersecurity insights. The next stage was to find and implement a SOC solution that could seamlessly integrate with their existing security schemes.

Establishing a security team alongside their existing team of IT professionals was not feasible. It is also important to note that in areas where there is significant reliance on third-party service providers, it was unrealistic to have the company’s IT team, as professional as they were, to conduct in-depth due diligence on the cybersecurity measures implemented by such suppliers.

With a lack of in-house cybersecurity experience, time, and resources, it was imperative to find a complete solution that would fully enhance the company’s security. Having various tools on-hand and detecting alerts and incidents just didn’t cut it anymore.

They needed a cybersecurity solution to give them a high-level, in-depth overview of their current security state, implement a tailored solution and provide the extensive knowledge required to provide real-time action and forensic analysis.

CYREBRO was able to quickly develop a targeted and efficient approach to meeting the company's specific risk profile. As CYREBRO is completely technology agnostic, it provided unbiased capabilities on the different detection and response management systems on hand. Improving the company's visibility into their security posture and what they needed to do to achieve their goals was a huge leap forward.

CYREBRO utilized its next generation Security Operations Platform and technology to provide a thorough viewpoint, making sure nothing was overlooked or mishandled. Following initial assessment of the company's entire security suite and scanning for vulnerabilities throughout the entire development process, the company was found to be at a sophisticated and mature state in terms of systems, but were not scalable.

> *CYREBRO's fully agnostic SOC solution effortlessly integrated with all of our existing systems, a feature we found lacking in other vendors. We were highly impressed by their capabilities and the solution immediately allowed us to ensure scalability with the agility that we needed. At this point, it was unquestionable that even if a breach were to occur, it would be immediately detected before even remotely harming the company's operation or reaching classified data.*

CYREBRO

The Resolution

> *We now have an online security operation platform that not only monitors our entire network environment, but also proactively manages and responds to alerts/threats through forensic analysis. It is the closest to feeling as though we have our own personal SOC. We now have a sense of security that we did not have, before working with CYREBRO. This is priceless as it allows us to focus on our core business operations, while letting the true experts manage our cybersecurity.*

The Result

Bad hackers don't rest, therefore, having full visibility, real-time detection and response to security threats to post-mortem analysis is imperitive. This operation needs to run like a welloiled machine, ready to make decisions and take appropriate actions quickly in a highpressure environment. In order to ensure incidents are managed in the most consistent and efficient way, but at the same time these processes must be flexible enough to be quickly adapted to new technologies or attack methods.

CYREBRO

We are where we envisioned to be and that is a great feeling. We made the right decision in choosing this solution as it provides an enterprise class technology. CYREBRO truly cares about their customers and provide a personal touch, upholding open communication lines along with a proactive approach to our cybersecurity

CYREBRO not only provided a next-generation Security Operations Platform and the professional guidance we needed, but they continue to offer ongoing, unbiased and highly professional input on technologies we explore. They are above and beyond a managed SOC provider, we had access to insights and people with a range of specialist skills, from platform engineering, network and forensic analysts to software developers and threat intelligence researchers. I see them as a true partner.

Company CTO

Eliminated the need to staff an in-house security team 24/7

Strong ROI with enterprise class knowledge and managed detection

Security-by-design mindset and technology to allow rapid scale

The company has full confidence in their security posture. They will continue to evolve with the pace of technological innovation, and now have the confidence of being able to make necessary adjustments to their network as they grow and have the ability to respond to the never resting hackers and cyber threats.

Schedule A Demo