MICRO FOCUS

Case Study

Security

Obrela

Today's vendor-driven approach to cybersecurity, which continues to add more and more layers, is not sustainable. It is a mathematical certainty that every security model will inevitably fail at least once, regardless of the defense and technology sophistication involved. ArcSight ESM's open architecture enables Obrela to connect its existing data stores, analytics platforms, and other security technologies directly into the SOC, enabling them to decrease response times and confidently offer highly reliable service agreements.

Overview

Imagine you are hosting an intimate dinner party in the dark. Suddenly the lights come on, and you're astonished (and alarmed) to see a large number of dubious-looking strangers sitting at your table along with the invited guests. This sort of unpleasant surprise—which in the security space, translates into sudden awareness of many more internal and external threats than you knew about—is what Obrela Security Industries helps protect its clients from, with the help of the Micro Focus Security ArcSight security information and event management (SIEM) solution.

"ArcSight is a key part of our engineering achievement to collect and analyze structured and unstructured data generating valuable intelligence for new, emerging and advanced security threats giving our clients a unique advantage in predictability, preparation and response."

GEORGE PATSIS
CEO
Obrela Security Industries

Headquartered in London, UK, Obrela Security Industries (O.S.I.) is an enterprise information security service provider, offering an umbrella of security services, products, and intelligence for complex enterprise environments and major domestic and Global 500 corporations, including a major European stock exchange and a multinational financial services company. Obrela's mission is to ensure that its clients' information assets remain safe and available for business; in fact, the company's motto is: "We keep your business in business."

O.S.I. supports large, medium, and small enterprises in the areas of financial services, telecommunications, and government. The ArcSight powerful correlation and analytics engine is a critical element in the advanced intelligence services portfolio that Obrela provides to these clients.

Challenge

Although they have invested in the latest technology, organizations still cannot detect cyber threats during the early stages of the attack lifecycle. The average time to detect and react to cyber breaches today is 240 days. So, businesses need to radically change their mindset and focus on identifying breaches early in the attack lifecycle and responding with the most efficient response strategy. And to do so, they

OBRELA
SECURITY INDUSTRIES

At a Glance

- **Industry**
  Software & Technology
- **Location**
  London, UK
- **Challenge**
  The company needed a powerful, scalable, fully interoperable correlation engine as the foundation for a business that provides advanced intelligence services for complex enterprise environments.
- **Products and Services**
  ArcSight Enterprise Security Manager
- **Success Highlights**
  + Provides a real-time view of security-related activity on systems and networks, enabling clients to stay ahead of cyber criminals
  + Complements defensive security systems by identifying threats early to minimize business impact
  + Offers multi-tenancy, multi-customer support so that different clients can be monitored from the same console
  + Interoperates seamlessly with client infrastructure to ensure rapid integration and immediate results

need to analyze extremely valuable security-related data and metadata that remain unused, fragmented, isolated, and mostly static.

Collecting and analyzing data is crucial for a business-driven cybersecurity model that integrates people, process, and technologies into a comprehensive security program. Enterprises need to protect their constantly changing infrastructure against a constantly moving threat. This is where Obrela comes in. "We make sure our customers can focus on what they do best, their core business, by leveraging our expertise and ArcSight to address their information security needs," says Patsis. "Security is our core business."

Cyber criminals and advanced persistent threats are continuously evolving and becoming increasingly better at circumventing security. It is no longer enough to use technologies that only detect known threats. Enterprises must have the capabilities to hunt for unknown threats in order to detect advanced attacks. Combining real-time correlation with analytics enables SIEM users to tackle today's advanced persistent attacks by detecting both known unknown threats.

Solution

Why would a managed security services provider (MSSP) choose a SIEM solution over another solution as the foundation for its business? For Patsis, the answer is simple: "A SIEM solution can tell you what is happening on your network, on your systems, and in your business on a real-time basis. It is your basic, but powerful tool for security."

This is not necessarily intuitive. "Interestingly, we find that many of our customers have invested all their money into security systems of a defensive nature," Patsis continues. "Of course, this layer of defense is important; but it is mathematically certain that, at some point

in time, the technology of defensive controls will fail. When that happens, will it be possible to understand and visualize the threat early enough, so it can be contained before it gets out of control? A SIEM solution helps us to understand and assess the security state of the enterprise on a real-time basis."

ArcSight has been the SIEM solution of choice for Obrela since the beginning. "We evaluated almost every available product in the market to see how it could fit in a multitenancy, multicustomer, highly complex multivendor environment, and at the same time have the simplest, most efficient, most effective way to operate the system horizontally," recalls Patsis. "Our evaluation was very much in favor of ArcSight."

One of Obrela's primary selection criteria was interoperability. "We believe ArcSight makes the most interoperable solution on the market. Of course, interoperability is crucial for us: When we go to a customer and want to monitor their infrastructure, we can't afford to have problems in understanding what a device says or what an application is doing. We have provided this service to many customers and have never had an issue," says Patsis.

Other key factors included scalability, ease of integration, and raw power. "It is a seamless integration," continues Patsis. "We don't need to install anything on customers' devices or infrastructure, so that helps us complete the integration very quickly. The scalability of the product is excellent; as we grow, we can add hardware and processing power in a predictable manner."

Results

"The power of ArcSight ESM is unmatched and it decreases our response times drastically," declares Patsis. ArcSight saves O.S.I's security analysts' precious time by correlating logs quickly and firing on known rules and conditions. "This means quicker response times and leaves our security professionals more time to hunt for unknown threats."

Customers have varying needs. Some want to invest in the infrastructure, but need someone

> **"The scalability, multitenancy and content authoring capabilities of ArcSight are the most advanced in the market, creating a real competitive advantage when we deal with complex enterprise environments that require increased security vigilance and visibility."**
>
> **GEORGE PATSIS**
> CEO
> Obrela Security Industries

Contact us at:
www.microfocus.com

Like what you read? Share it.

to provide the service; others want to manage everything on their own. Obrela has options available for all different types of customers. Micro Focus and Obrela's partnership allows the latter to sell ArcSight as a service or to sell the product itself.

"We have bought Micro Focus ArcSight and installed it in-house; we use our licenses to monitor devices from client accounts. We also have an agreement to sell the software to clients that require an in-house deployment," Patsis explains.

Obrela provides advanced intelligence—information that can help clients make critical decisions—by providing a complete security picture at any time, any place, for any business. "When we introduce ArcSight into a new account, it is typically like the surprise dinner party," concludes Patsis.

"They thought they were safe, they believed they were able to see everything—then you turn on the light with a new technology, and all of a sudden they see a stranger sitting next to them. With ArcSight, they see the reality of their security situation. Then they can take steps to address it in the most effective way."

Learn more at
software.microfocus.com/arcsight