Obrela Security Industries

ArcSight joins forces with Obrela Security Industries to ensure the highest level of resilience against imminent cyber threats encountered by major telecommunications client.

Who is Obrela Security Industries?

Obrela provides the most advanced, comprehensive real-time cyber risk management and early warning services. Using security analytics and sophisticated risk management technology, Obrela dynamically protects its clients by identifying, analysing, predicting, and preventing security threats in real time.

Security Risk in Complex IT and Telecommunications Network

One of Obrela's clients is a major telecommunications company in the Middle East. The company manages and operates telecommunications networks, systems, and infrastructure, maintaining a vast asset inventory across multiple divisions. George Daglas, Chief Operations Officer at Obrela, explains the challenges that threatened their client's security position: "Our client has thousands of employees and a network environment that consists of more than 20,000 assets across multiple divisions. The complexity of the infrastructure represented an extended attack surface, posing many business risks such as service unavailability, consumer trust damage, intellectual capital losses, productivity discrepancies, inability to meet compliance requirements, and remediation costs. Our client needed more visibility in its infrastructure so that it could respond faster to any new threats."

> "The SIEM solution designed and built by Obrela leveraging Micro Focus' (now part of OpenText) next-gen platform and Obrela's Hardcore Content use cases, significantly expanded customer's visibility into activity across its IT and telecom infrastructure. To further enhance the solution's threat detection capabilities, additional ArcSight components have been leveraged and integrated with ArcSight ESM."
>
> **George Daglas**
> Chief Operations Officer
> Obrela Security Industries

Obrela + ArcSight— a Winning Combination

To introduce new monitoring and reporting capabilities for their client, Obrela turned to OpenText™. ArcSight Enterprise Security Manager (ESM) by OpenText includes a sophisticated correlation engine to analyze security logs and provide advanced security analytics to identify threats and risks. To create an effective Security Information and Event Management (SIEM) solution, Obrela combined this with their advanced threat analytics and correlation capabilities. This so called "Hardcore Content" concept

OBRELA
SECURITY INDUSTRIES

At a Glance

Industry

Telecommunications

Location

Middle East

Challenge

Providing highest level of visibility and enhanced threat detection capabilities in a large and complex network environment

Products and Services

ArcSight Enterprise Security Manager (ESM)
ArcSight Interactive Discovery

Critical Success Factors

- 10x increase in MSS coverage, monitoring over 10,000 devices
- 8 million monthly alerts are managed automatically
- Proactive threat identification and mitigation minimizes business disruption
- 250+ user-friendly customized dashboards provide real-time security insight

“ArcSight ESM complements our own security expertise perfectly, enabling us to orchestrate and control all aspects of cyber security through one platform, integrating people, processes, and technology for the benefit of our clients.”

George Daglas
Chief Operations Officer
Obrela Security Industries

Connect with Us
www.opentext.com

gathers content from various internal and external sources into a single platform to analyze and correlate data and identify potential risks for the organization. The team monitors security events, by collecting, aggregating, and normalizing logs enabling faster and more proactive threat discovery and control, before it affects business users. Approximately 200 automated advanced use cases were developed to prioritize incident severity. As a result, on average, eight million alerts are triggered per month, resulting in 2,500 incident cases created automatically, without the need for human involvement.

Obrela’s dedicated team of engineers is responsible for the seamless operation of the solution, by monitoring its performance on an ongoing basis, providing regular maintenance, platform updates and upgrades, and delivering emergency support. Obrela also performs health monitoring services so that any potential issues are diagnosed and mitigated as early as possible. Obrela’s elite team of cyber security experts is also closely involved in the client environment. They provide level 2 and level 3 security support to the onsite team of security analysts during the investigation and mitigation of active security incidents. By preventing and protecting against real or simulated attacks the organization’s security position is maintained and business continuity is ensured.

Full Cyber Security Visibility in Flexible Dashboards

George Daglas comments: “The SIEM solution designed and built by Obrela leveraging Micro Focus’ (now part of OpenText) next-gen platform and Obrela’s Hardcore Content use cases, significantly expanded customer’s visibility into activity across its IT and telecom infrastructure. To further enhance the solution’s threat detection capabilities, additional ArcSight components have been leveraged and integrated with ArcSight ESM.” Specifically, the MSS coverage was increased tenfold reaching more than 10K devices monitored in total.

“ArcSight ESM platform provides a centralized and consolidated view of the full environment. Advanced integration offers security rendering and the appropriate flexibility,” says George Daglas. “Cyber security visibility coverage has increased substantially, and we helped our client’s internal security team with the customization required in such a complex environment. It was crucially important to prevent any service outages and avoid breaching compliance regulations resulting in remediation charges, a challenge to which we responded with the highest efficiency”. Obrela and the client can monitor real-time user activity across the entire environment through specialized daily/weekly/monthly dashboards, leveraging ArcSight’s visualization capabilities. More than 250 customized dashboards have become available to analysts so far and keep increasing according to client’s needs. To build on this, the underlying architecture is designed to be highly scalable, allowing for the ongoing integration of additional log data sources, responding to the client’s evolving requirements.

George Daglas concludes: “It has been helpful to work closely with Micro Focus (now part of OpenText) in finding a fast and effective solution to a very real security threat our client was facing. ArcSight ESM complements our own security expertise perfectly, enabling us to orchestrate and control all aspects of cyber security through one platform, integrating people, processes, and technology for the benefit of our clients.”

768-000020-003 | O | 11/23 | © 2023 Open Text