

Success Story: SIEM/SOC & Intervention Team

“Within 3 months the SIEM/SOC solution became effective including daily/weekly/monthly control reports. Soon after we have connected other complicated systems, the team at Experis Solutions had to invest a lot of effort and innovative thinking to find solutions to complex challenges, which they did successfully. In summary, highly recommended for their expertise level, serviceability and fully cooperative.”

- Shalom Nimny, CIO, Ituran

Challenge

Our customer's company provides value-added location-based vehicle services including vehicle monitoring and recovery, fleet management, mobile asset location and more. With over 2M subscribers using its location-based vehicle services, the company is a leader in the emerging mobility technology field in Israel and Latin America.

The company's response time to alerts, is critical. Their teams must maintain all systems operative at all times. They therefore require top notch cyber security services, operating in as close as possible to 0 response time, from identifying treats to mitigating them.

Solution

To meet these requirements, Experis Solutions offered the customer a SIEM/SOC service based on IBM QRadar. QRadar was carefully configured to match the customer's system architecture and goes through periodic optimization to verify that only relevant alerts will be dealt with to save time. This monitoring and control solution, coupled with Intervention Response service, ensures maximum security to the customer's systems with rapid response time.

The solution has 3 security layers:

- **Tier 1** – SOC team monitors the customers' systems 24/7/365 to identify cyber security events.
- **Tier 2** – Cyber analysts go through the alerts to interrogate and analyze each alert in order to decide on mitigation measures.
- **Tier 3** – Intervention Response team is activated in cases of major cyber events, as decided by the analysts. Such events require experts' intervention, usually involving the customer's IT team.

Results

Experis Solutions has been providing cyber security services to this customer for the past few years, during which we have successfully countered several cyber events. The customer regards us as a trusted advisor, highly professional, with the best experts on the field. We have expanded our services.