

Gaining Actionable Insights into the threats that matter

RiverSafe helped a multinational telecoms organisation build a new state of the art Global Security Operations Centre (GSOC) in order to gain more actionable insights and visibility into threats. The company had been using traditional security for incident response which included a number of legacy platforms, tools and processes. RiverSafe helped this global enterprise replace all its legacy tools with modern Splunk SIEM software, a PCI platform and SOAR. RiverSafe also introduced Exabeam behaviour analytics to the organisation.

The goal of the GSOC programme was to create a consolidated view of the threat landscape across the globe and provide unprecedented visibility and actionable insight into the threats that required the security team's attention. The Telco provider realised that its business unit-led approach to monitoring was undermining its ability to see what was really going on.

Geographically, the business is very diverse and spread across multiple countries and locations.

Each country or business unit had its own security policies and architecture, resulting in different levels of reporting to the global SOC. The challenge was how to integrate all of these countries/units so that they could use the same processes and tools to provide much-needed visibility to the CISO. The CISO needed consolidated information around how threats and vulnerabilities were being addressed and which countries were being impacted by these.

RiverSafe deployed a team of experts who provided security services to the internal team around best practice for monitoring, user behaviour analytics, PCI compliance, SIEM and SOAR. RiverSafe designed a roadmap for each country, enabling them to deploy the necessary tools in very short timeframes. Additionally, a long-term plan was developed to facilitate all the scalability and agility needed for the future. The project included enabling the organisation to maintain some local security while also giving the global SOC the reporting visibility, processes and assurance it needed.

Partnering with RiverSafe has accelerated the delivery of the first phase of this programme, resulting not only in decreased risk but also reduced costs. RiverSafe was highly responsive and collaborated brilliantly with the in-house team (and other suppliers) to deliver Phase 1 to time and on budget. No surprise then that the Telco is looking to work with RiverSafe on Phase 2.