RIVERSAFE

Living with SIEM

A Customer Story

Phone: +44(0)203 633 2577
Email: sales@riversafe.co.uk
Web: www.riversafe.co.uk

Suite 23, Beaufort Court, Admirals Way, London, E14 9XL

Living with SIEM

THE ORGANISATION

When a global finance organisation with over 25,000 employees makes the strategic decision to consolidate security events and information into an integrated, enterprise-wide log monitoring solution, with the goal of routing high-quality intelligence to its SOC teams, it inevitably needs to make a significant technology investment in a SIEM solution.

Their SIEM platform clearly needs to be a robust and reliable toolset. It forms part of a critical suite of technologies that help them identify security threats, potential vulnerabilities and compromised systems.

Given their much-targeted sector, the organisation faces both a constant background noise of indiscriminate threats like phishing and network port scanning, and also the more persistent, targeted attacks that are likely to find even the smallest weakness in their cyber defences.

Early detection and effective response to both vulnerabilities and compromises are critical in minimizing their impact. Their SIEM tooling provides a consolidated view of all of the cyber security defences, highlighting the important events, and guiding the response to them.

THE CISO'S CHALLENGE

"Any significant failure in our SIEM platform leaves us blind. That's not a situation we can tolerate for very long, and something we need to do everything in our power to avoid.

We knew we'd need a fairly complex platform, processing a large amount of security log data through a couple of tiers and ultimately end up with a huge data lake to analyse.

On top of that, our environment is pretty dynamic, the way we use technology in this business is a significant competitive advantage for us, we are adding new systems all the time, and new threats are a constant.

When we first put the platform in, it was a revelation, that sense of having a complete view of what's going on was brilliant, and the platform was performed well. After 6 to 12 months, I started to get a sense that things were starting to drift. We started to see issues with performance, which we managed to work through, but it cost us some downtime. Then, a year or so later, we discovered a compromise which hadn't been flagged through the SIEM. It turned out the system in question was a relatively new one, and it hadn't yet been onboarded into the event collection.

I was pretty embarrassed to be honest, we'd made a significant investment in the tools, but rendered the investment worth less than it should have been for the sake of sufficient engineering bandwidth. When I looked into it, the engineering team was under strength. A senior member of the team had moved on once the initial implementation was done, and we'd struggled to find a suitable replacement. A couple of other members of the team were focussed on another project at the time."

A Customer Story

THE SOLUTION

Riversafe's Managed Platform Engineering Service provides the necessary expertise, on a proactive and collaborative basis, with a flexible set of deliverables that would need to map well onto the organisation's requirements. They were going to need a service partner with the skills and experience to monitor and maintain their SIEM platform, and flexible pool of resources on hand to help with event source onboarding and platform upgrades.

The core deliverables of Riversafe's service are a great fit organisation's requirements -

- Platform monitoring based on our unique Riversafe Platform Intelligence (RPI) framework drives effective maintenance and fault resolution
- Our team of experts would be on hand around the clock to on deliver event source onboarding, use case implementation and platform upgrades as and when the requirement arose.

> **We are able to focus on the security incident management without needing to worry about the technology platform that underpins it.**

THE OUTCOMES

"Working with the team at Riversafe has changed things for the better in a significant way. The platform has been so much more stable since we started working with them. They keep us informed if they spot anything they need to address, but the whole process is zero effort for us now. We are able to focus on the security incident management without needing to worry about the technology platform that underpins it."

We've also been able to keep the platform itself up to date. Upgrading a toolset this critical is the kind of thing that makes you a little bit nervous, and our own team had been limited to the experience they'd gained running the process once in our test environment. Riversafe had already been through it multiple times, knew all of the steps to make it successful, and were able to fit in with our out of hours change windows.

They've also been incredibly flexible. We initially wanted to retain responsibility for building out the queries and analysis. We had a couple of occasions where we were short of technical resources to do that, and Riversafe were happy to step in and help. That approach worked so well, we've added it into the scope of the service.

Given what we do, we always knew that outsourcing the SOC and incident response wasn't going to suit our organisation, we had kept the platform engineering in house without giving it too much thought. On reflection, handing that task to a team of specialists was something I wish I'd done from day one."

If this story sounds similar to your own, maybe we can help?

Contact Riversafe at **sales@riversafe.co.uk**

RIVERSAFE

ABOUT RIVERSAFE

RiverSafe is a leading cyber security intelligence partner, supporting companies to put security at the heart of business operations & yield actionable business insight. Proudly supporting some of the world's biggest companies -- including Vodafone, Sky and BP.

Our expertise in both cyber solutions and our longstanding technology partnerships gives our customers an advantage over evolving threats. We provide perspective on the status of security infrastructure and remove existing silos to create a unified view of activity and generate better operational outcomes.

For more information please visit:

www.riversafe.co.uk

WHY RIVERSAFE

We offer a comprehensive capability to enable our customers to accelerate time to value, derisk deployment and manage business risks.

- Passionate about customer success
- Flexible, highly skilled resources
- Comprehensive suite of services
- Collaborative
- Proven track record
- Vendor endorsed

GET IN TOUCH

If you would like to find out more about how RiverSafe can help you please get in touch.

Phone: +44(0)203 633 2577
Email: sales@riversafe.co.uk
Web: www.riversafe.co.uk

Suite 23, Beaufort Court, Admirals Way, London, E14 9XL