CLIENT CASE STUDY

RÖHLIG-GRINDROD BUILDS VISIBILITY AND TRUST WITH CYSIV SOC-AS-A-SERVICE

CUSTOMER:
Röhlig-Grindrod

INDUSTRY:
Logistics, Freight, and Transportation

LOCATION:
Johannesburg, South Africa

SITUATION:
To maintain customer trust and continue providing smooth logistics services, Röhlig-Grindrod needed a proactive solution to protect sensitive data and company assets from ransomware, malware, and other cybersecurity challenges. These were brought about by the Covid-19 lockdown, which forced further digital innovation and a change in business model.

SOLUTION:
Cysiv SOC-as-a-Service

BENEFITS:

- Faster detection and response of threats
- 24/7 monitoring with access to skilled SOC analysts
- Improved security of cloud-connected systems
- Avoid downtime and customer frustration

OVERVIEW

Röhlig-Grindrod's extensive global network and strategic partnerships with reputable carriers ensures cargos are delivered safely, securely, on time, and to any destination. As an international logistic service company, they offer multimodal solutions encompassing air, sea, road and rail. Furthermore, they support all warehousing, insurance, customs clearing, compliance, supply chain, contract and project logistics needs throughout Africa and across the globe.

The logistics industry is increasingly relying on information and communication technology that puts it on the radar of cybercriminals and opens the door to a broad range of threat vectors that can bring operations to a standstill. With the rising prevalence of attacks against the supply chain, cybersecurity has never been more important for Röhlig-Grindrod, which is why they have chosen to be proactive in their approach to cybersecurity.

"We understand that in such an environment, cyberthreats need to be taken seriously and that simply reacting to a crisis is not the right approach. Businesses must have strong cybersecurity measures in place to detect and respond to threats before they disrupt their operations or compromise their business data," said Mervin Naidoo, Chief Information Officer at Röhlig-Grindrod.

CHALLENGES

The company needed a more proactive approach to strengthening their information security posture. Noted Naidoo, "The last thing you want to be faced with, as an organization, is reacting once the damage has already been done." Their security program began with firewalls and antivirus and expanded to user awareness training and quarterly penetration testing. However, the company needed to add security visibility in order to identify threats in progress and make decisions about hardening their defenses.

"We had to be proactive in determining the vulnerabilities that impact this new working style and cybersecurity had to be a strategic consideration integrated with key areas of work policies."

– Mervin Naidoo, Chief Information Officer at Röhlig-Grindrod.

Two major factors led to Naidoo choosing to work with a partner. First, he realized that they did not have SIEM monitoring expertise in house: Röhlig-Grindrod's core competencies were in moving freight, not operating a SOC. He also acknowledged that a partner could bring a fresh perspective and deeper insights to their security program. "I wanted someone else to mark our work," said Naidoo. "You can't mark your own homework. That was my stance for outsourcing cybersecurity."

Naidoo evaluated proofs-of-concept from three security service providers, including Cysiv, and he was only prepared to select a partner once he felt comfortable enough to trust them with their security posture. Within two weeks of beginning the proof of concept, Naidoo was confident that Cysiv was the right choice.

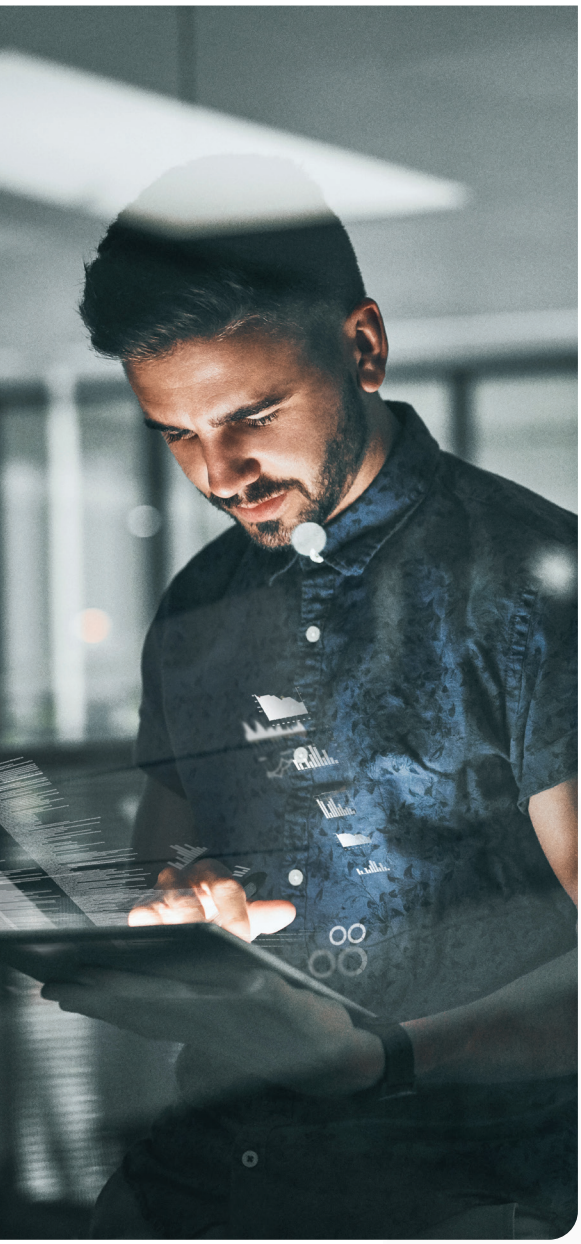
WHY CYSIV

- **Collaborative Partnership**
- **Seamless Onboarding**
- **24/7 Monitoring**
- **Responsive, Communicative Experts**
- **Transparent SIEM Platform**

Röhlig-Grindrod values trust and relationships. That drives the company's logistics work, and that attitude extends into why Cysiv fits so well with their security program. Naidoo explained that one of the major reasons he chose Cysiv SOC-as-a-Service is the customer centricity, relationship management and quick responsiveness of the whole Cysiv team.

Other service providers Naidoo tried had struggled with communication, with tickets sometimes taking over a day to generate a response. On the other hand, when Naidoo and his team wanted additional details on a specific incident or threat, Cysiv was on the case quickly. Typically, within half an hour of investigating a possible threat, Cysiv was on a call with the Röhlig-Grindrod team reviewing the issue. Within an hour, the SOC team knew what had happened and provided a full analysis. Within two hours, the issue was fully resolved.

Naidoo also highly values the Cysiv platform, including its integrated feature set, the dashboard reporting and its transparency. The platform is not a black box. Naidoo wanted to be able to see what Cysiv was doing, and where he stood from a security perspective. With Cysiv's platform there is no guesswork; he can log into it, see the same things that Cysiv's analysts can see, and use that to better inform their decisions.



SOLUTION

Within a week, Röhlig-Grindrod had been onboarded to Cysiv SOC-as-a-Service. Cysiv had expertise working with the solutions they use, and the logs that needed to be ingested. The onboarding process went exactly as planned, without endless back-and-forth calls, typical of many service providers.

Their security data feeds continuously into Cysiv's cloud-native, next-gen SOC-as-a-Service platform. The data is parsed, cleansed, normalized, and enriched, generating telemetry in a common information model (CIM) format. This prepared data builds the foundation for Cysiv's detection, investigation, threat hunting, and incident response capabilities. And it allows Cysiv analysts to monitor for possible threats more effectively 24/7, and investigate and respond in a timely manner, based on the severity level and the service level agreement. Biweekly meetings augment the daily communications between the Cysiv team and the Röhlig-Grindrod team.

RESULTS

Cysiv SOC-as-a-Service has given Röhlig-Grindrod greater visibility into their overall security posture, and enabled them to better manage cyber risk. The technology and reporting has helped build their ability to see the threats against their business, and see how well they are able to defend against attacks. In addition, Cysiv has also given Naidoo and his team confidence that when a threat is detected, they have a trusted partner with the skills and business understanding to respond, and the proper communication practices to keep Naidoo and his team informed.

The customer focus of the Cysiv team also stands out to Naidoo, because of their professional relationship management, regular communication, and quick response when there is a question or a possible security issue.

REQUEST A DEMO

Request a demo of Cysiv SOC-as-a-Service at cysiv.com