Greater network security with SIEM

HENSOLDT Optronics, the market leader in civilian and military sensor solutions, is a global pioneer and innovator in defence and security electronics. The company takes a disruptive approach to developing new products that enable data management, robotics and cybersecurity to combat escalating threats. HENSOLDT employs around 4,300 people and generates annual revenue of €1 billion.

HENSOLDT's diverse portfolio covers all types of defence and security needs, and ensures clients are able to monitor the entire electromagnetic spectrum to a high degree. The company's solutions are deployed on diverse platforms, including helicopters, aircraft, drones, ships, submarines, armoured vehicles and satellites.

Some of the best-known aerospace platforms equipped with HENSOLDT's products are the F-16, Saab Gripen and Dassault Rafale fighter jets, the Eurofighter, the TanDEM-X and EDRS-A satellites, the A400M transport aircraft and various models of helicopter. The company also provides mission-critical equipment for Puma and Leopard armoured vehicles, class 212 and 209 submarines, LCS Freedom class ships used by the US Navy and the German Navy's K130 corvettes.

HENSOLDT
Detect and Protect.

Organisation
HENSOLDT Optronics GmbH

Industry
Insurance and security electronics, warning systems

Employees
4,300

Key impacts
- Achieve comprehensive network visibility
- Provide support for compliance requirements

The challenge

HENSOLDT Optronics was searching for a solution that would create comprehensive visibility for all processes across its network.

Alongside the desire to better protect the firm's own IT infrastructure and critical data, meeting specific compliance requirements was also a high priority. As the company operates in the armaments industry, its products are subject to special legal regulations. HENSOLDT Optronics wanted to enable members of its security team to achieve compliance with these regulations more easily and provide the necessary evidence of compliance without a great deal of effort.

By implementing a new solution, the company also hoped to increase security awareness within the organisation.

> *"Technical brilliance in detection and analysis is only one aspect in the task of evaluating a security intelligence solution. Efficient reporting has a similarly high value."*
>
> - Jochen Scheuerer, IT Director
> HENSOLDT Optronics GmbH

The solution

HENSOLDT began by researching whether an open source solution for log management could provide the services needed. However, inadequate reporting capabilities prompted it to abandon this approach. "Technical brilliance in detection and analysis are not sufficient if excessive effort is needed to prepare the findings in an accurately targeted manner," said Jochen Scheuerer, IT director, HENSOLDT Optronics GmbH.

Thinking Objects, the system integrator that implemented and now operates a new IT security infrastructure for HENSOLDT, recommended the deployment of LogRhythm's SIEM solution. It became clear that a SIEM (security incident and event management) solution was the most logical approach because of its ability to collect the log data from defined systems, while simultaneously detecting rule-based violations of information security and dangerous situations where events extend across several systems in the network. Detection and documentation can therefore be immediate, facilitating both ongoing monitoring and intervention in the event of an attack, while also making it easier to investigate suspicious events afterwards.

HENSOLDT's special set of requirements called for a SIEM system that supports customised implementations for the organisation and industry specific use cases, facilitates forensic investigation, and offers flexible reporting. Operating the system would ideally give IT and security teams the smallest possible workload. LogRhythm's product addressed all of these aspects.

Quick decision

After a proof-of-concept phase of just three days, LogRhythm's platform proved to be an effective solution. Several features stood out:

- Robust functionality compared to competitors' solutions
- High-performance search via 'Pro Advanced Agents' with correlated requests
- Strong reporting functions and an extensive set of adaptable reporting templates – a helpful starting point for audits (e.g. for ISO-27001 and NIST)
- Prefabricated filters and dashboards for systems from well-known technology partners
- Numerous predefined use cases
- Clustering and redundancies to provide strong safeguarding against failures
- Rapid response times when support is needed

Successful introduction, effective operation

The introduction of a SIEM solution confronts both the service provider and its client with the challenge of getting applications to work together to deal with IT-security incidents. Only by achieving this harmony can security intelligence be implemented effectively.

Thinking Objects provided consultancy and concrete suggestions for the client during this phase. "The implementation and launch were facilitated because LogRhythm provided access to a wide spectrum of prefabricated use cases" said Bernd Maier, sales and account manager at Thinking Objects. The integrator incorporated the log sources and adapted the filters, dashboards and alarms. LogRhythm meanwhile, set up a comprehensive reporting system to assure conformity with ISO 27001 and NIST.

"The necessary phase of grappling with our own requirements and risks achieved heightened sensitivity to our security needs – a valuable side-effect," said Jochen Scheuerer.

Operation as a managed service

Thinking Objects now looks after the basic operation of the SIEM system, along with patching, installing updates and fixing bugs. LogRhythm architected the solution to permit a flexible division of labour between the user and implementation partners. In HENSOLDT's case, the services also include regular testing, analysis, evaluation and categorisation of potential IT security risks or vulnerabilities based on LogRhythm dashboards. This reduces the burden on the client's in-house team, with team members provided with precisely the security data to help them accomplish their tasks.

The technical foundation is a hardware appliance located with the client, which reliably achieves the necessary processing capacity. Furthermore, Thinking Objects operates 10 system monitors for HENSOLDT Optronics at Oberkochen, Germany and Irene, South Africa.

The project continues in 2018 with ISO-27001 certification and the inclusion of new areas of infrastructure, including endpoint security, next-generation firewalls and vulnerability management.