SOCWISE

POWERED BY EURO ONE

SOCWISE

YOUR CHALLENGE IS OUR MISSION

socwise.eu

MDR STORY WITH "HAPPY END"

SOCWISE Managed Detect and Response Case Study @ a pharma customer

THE CUSTOMER: MULTINATIONAL MANUFACTURING AND DISTRIBUTION PHARMACEUTICALS COMPANY

IN 2019 suffered a major data breach, which caused production outage, data loss and hundreds of days of out of business hours work for the IT department. Considering the loss and the brand damage, the management called for sufficient countermeasures, hence they were deeply concerned to be hit with a second attack while still remaining to be unable to respond.
They experienced during the attack, that there was not enough data available to examine the attack chain, nor to determine when the attackers had persisted, so they were unable to properly respond.
They also faced the issue that the security specialists in their IT operations team were not trained to handle such an incident.
Furthermore their internal processes were also not sufficient to support their defensive activity. Therefore, after the painful re-installs, restores and resets, they maintained the control and evaluated the lessons learned.

Addressing the challenge

They decided to totally re-design their defense in all aspects such as people, technology and processes. From the technology side they aimed for full visibility over their IT and OT, on-prem and the cloud network. They targeted to build up detection and response capability, so they decided to implement an evolved SIEM system and to organize their own SOC team.
SOCWISE team won the SIEM tender because RSA NetWitness® proved to provide the best visibility over their network be perfectly scalable and flexible to be integrated. Other tools offered good AI however it lacked tailored content and case management. A Multi-vendor solution would have been more expensive and cost more resources.

The SOCWISE team implemented a managed SIEM solution made of RSA NetWitness®Suite, and also developed the detection content and started the operation.
The next challenge for them was that despite their continuous aggressive recruitment activity, they were unable to fill the desired roles, so their SOC team has never came to life. That's why they issued an tenderRfP to provide MDR services, which SOCWISE was appointed for.

PAGE ONE

SOCWISE

POWERED BY EURO ONE

SOCWISE

YOUR CHALLENGE IS OUR MISSION

socwise.eu

Results

The SOCWISE team firstly designed the detailed service model and created the proper incident response plans. After the initial fine tuning the SOC of the customer was finally up and running, with experts from SOCWISE eyes on the glass and consultants to guide the customer through implementing the sophisticated procedures. On a daily basis the SOCWISE team and Customer IT operations team work together like a whole team, let that be content fine tuning, containing a phishing attack or finding and advising the risky users based on the identity behaviour. The service is being provided based on an operational handbook and measured by agreed KPIs.

The customer now feels that they have a complete overview of the internal network events and outbound traffic. Through various examples the SOC team and the platform proved that the well prepared, 100% dedicated and trained team is essential to bring attention to risky changes, unwanted activities while supporting the IT operations.

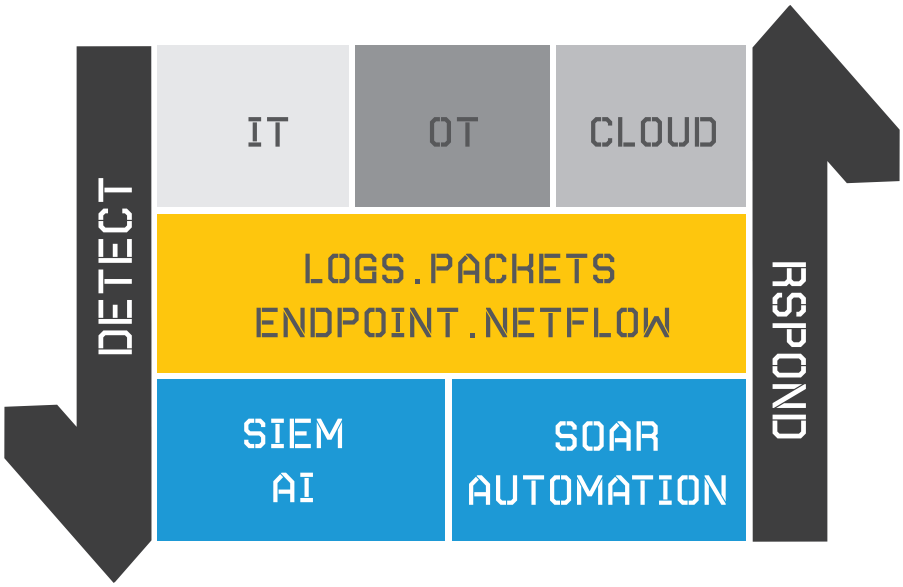
This cooperation enabled the CISO to prove the abilities of his department, reduce the stress on his team and provide the working environment where all of them can work much more comfortably.

Solution overview

SOCWISE managed the detect & response service, which concludes the remote human resources, the experienced consultant know-how and the technology platform.

The development of the SIEM or SOAR content are tailored for the exact business risks and the service is always based on exact needs of the customer.

The NetWitness® platform is a worldwide leading SOC technology, which is still the only platform processing out of the box all logs, network and endpoint data. It performs a multi-level AI analysis and also includes a leading SOAR and a threat intelligence platform.



PAGE TWO