RISK MONITOR

Risk Monitor system represents the innovative employee monitoring concept which comprises DLP, User Activity Monitoring, and SIEM&UEBA elements.

The comprehensive solution against data leak, corporate fraud, toxic behavior within a team, assists you with creating an effective risk management program, facilitates regulatory compliance and investigation processes.

The instruments are created to help information security, internal control and compliance officers, internal auditors, risk managers and human resources specialists perform their tasks and contribute into risk mitigating.

A SECURITY OPERATION CENTER TOOLSET

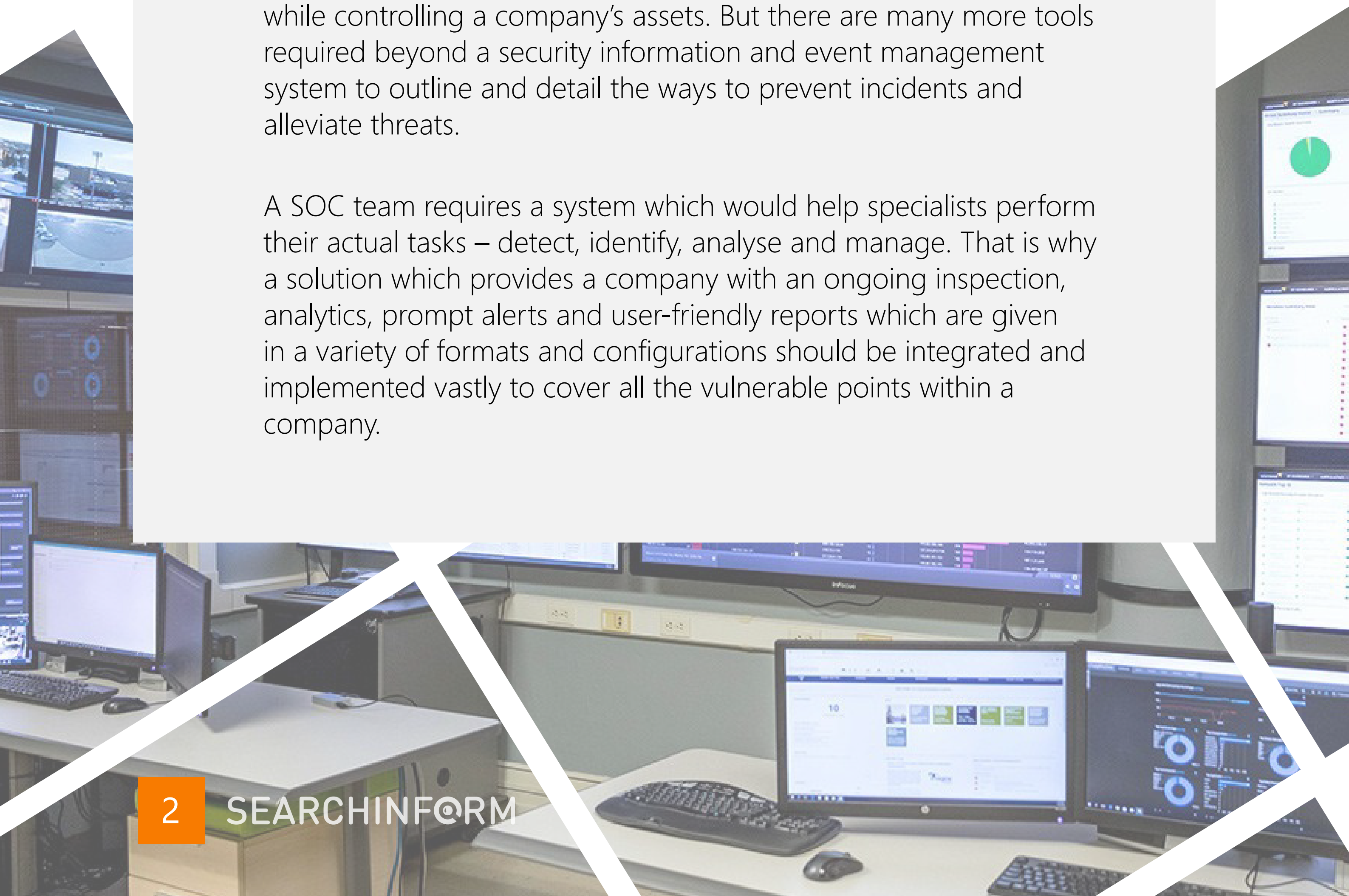
A SOC is a facility that comprises a team responsible for threat detection and security risk mitigation on an ongoing basis.

A security operation center is created within a company to unceasingly monitor and assess the level of corporate security. The center detects, analyses and manages incidents continuously as they occur.

The key point of SOC is to track an organisation's activity inside and outside the perimeter in real time. SOC teams are responsible for employee and customer data control, ensure that hardware and software usage is supervised. A SOC accumulates and processes all the data sent via various communication channels within a corporate network.

The main objective is to detect and monitor every event logged within a network, which makes SIEM an indispensable instrument while controlling a company's assets. But there are many more tools required beyond a security information and event management system to outline and detail the ways to prevent incidents and alleviate threats.

A SOC team requires a system which would help specialists perform their actual tasks – detect, identify, analyse and manage. That is why a solution which provides a company with an ongoing inspection, analytics, prompt alerts and user-friendly reports which are given in a variety of formats and configurations should be integrated and implemented vastly to cover all the vulnerable points within a company.



HOW DOES RISK MONITOR WORK

Besides credit risks, technical errors, natural causes and disasters, the control of which has already been automated and backed by law, there are risks caused by human factor which are frequent, subtle, and require a unique approach.

When an incident occurs companies wish they could have seen the link between a violation and its source, and are willing to learn about what instruments should be used in order to foreknow potential internal risks beforehand.

The software helps you identify employees who can sabotage your business due to malicious activity, or negligence. The system detects employees with debts, gamblers or compulsive gamers, discloses those who spread negative attitudes, are reluctant to perform their tasks, or blackmail their colleagues. Seeing sources of an issue, channels and recipients of communicated information, you can save time on investigation and establish a configurable, receptive and continuous monitoring process.

Works at 3 levels:

- Monitors employee activities and collects all the data from a company's sources, including messengers and social media, before an incident occurs
- Prevents information leakage, encrypts data, supplies you with a wide range of policies, and alerts to any violation of them
- Investigates without a third party involvement – detects violators and those who help them obtain information, including video and voice recording

RISK MONITOR COMPRISES A NUMBER OF ADVANTAGEOUS FUNCTIONS

Control of channels

- IM control with end to end encryption
- web camera recording
- microphone recording with speech to text conversion
- live connection to monitor and microphone
- audit of file system operations
- control of file contents on PC local resources
- audit of installed software and hardware
- capturing user contacts
- worktime audit (active applications and web activities)
- multi-channel data interception, archiving, retrospective investigation

Data analysis

- search for a company seal
- detection of image type (photo/scan)
- text search in audio
- complex queries (several search queries simultaneously)
- complex regular expression search
- similar image search - passports, credit cards, etc.

Reports

- installed/removed software/hardware
- employee work efficiency and productivity
- activities during work time
- absent employees (being late/early)
- time spent on various websites
- time spent in various applications

CASE STUDIES

Two marketing managers, who were dating each other, were working at the marketing department of the same bank and preparing an important campaign to advertise the new bank loans.

When one manager got fired, the other would send messages to the executives asking to hire her back. His request wasn't satisfied, and the discontented marketing specialist decided to leak the campaign details to the former employee he was dating and who would already work for the bank's competitor. She was going to get the marketing campaign so that her bank would release the similar advertisement featuring similar loans and services, stealing the whole idea and hitting the market as originators.

But the specialists began to follow the employee's activity shortly after his emotional talk with the manager. They monitored his communication with his ex-colleague via Skype and prevented the leak.

An employee of a telecommunications company was going to quit his job as he was launching his own app. He would cooperate with two colleagues who notified each other via social media every time they needed to discuss "something". They were gathering during work hours to consider the steps they needed to make to start their application. That is when the specialists responsible for risk mitigation in a company began to track the staffers and enabled microphone recording.

An employee who was to run the business got dismissed whereas the two colleagues were to provide him with confidential information – his access to the server was promptly terminated. They were going to leak him the databases with more than 500,000 accounts the personal data from which would be allegedly used for marketing purposes.

They sent a test email masked as a corporate letter and dispatched to an email address with a company domain – created as a disguise – before sending a second email with a database. The security center identified the offenders before the following letter would be sent. Thanks to the system not only the actual policies violators were detected and fired, but also the initiator of the fraud was neutralised.