
SIEM
SEARCHINFORM

WHAT BUSINESS TASKS DOES SIEM SOLVE?

CHALLENGE

IT infrastructure of a contemporary company is a complex mechanism that includes a multitude of corporate systems: Active Directory, CRM, Exchange, antiviruses, etc. Every IT system is a source of financial and corporate data, information about clients and other valuable information that violators aim to obtain.

The company can be endangered both by actions of system administrators (unauthorized granting of access rights, creation or deleting accounts, disabling firewall) and by vulnerability of the products through which violators can get access to company's data.

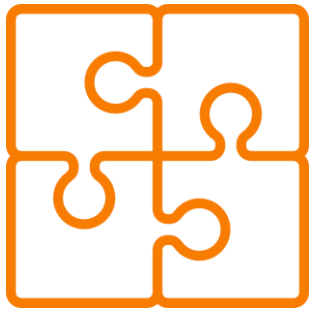
Any event in the system is logged (protocoled). But it is impossible to track, analyze, and react timely to all events without an automatic system.

SOLUTION

SIEM (Security information and event management) is a system designed for collecting and analyzing security events in real-time mode, detecting information security threats, and reacting to them.

SIEM
SEARCHINFORM

WHAT IS SEARCHINFORM SIEM?



SearchInform Event Manager (SIEM) is a system used to collect, monitor, and analyze information security events in real-time mode.

SearchInform SIEM collects information from different sources, analyses it, fixes incidents, and notifies concerned parties about them.

SIEM
SEARCHINFORM

HOW DOES THE SYSTEM WORK?

Sophisticated mechanism of SIEM operation boils down to the following algorithm:

STEP 1

Collecting events from various sources (network hardware, PC, security systems, OS)

STEP 2

Bringing heterogeneous data to a common denominator

STEP 3

Analyzing data and detecting threats

STEP 4

Pinpointing security breaches and sending alerts in real-time mode

SIEM
SEARCHINFORM

WHAT INCIDENTS DOES SIEM DETECT?

- Suspicious user activity.
- Virus epidemics and separate virus infections.
- Attempts to get unauthorized access to confidential information.
- Elevated rights, fraud.
- Errors and failures in information systems work.
- Manipulations with email, databases and other corporate IT resources.

SIEM
SEARCHINFORM

WHAT SOURCES DOES SIEM ANALYZE?

SIEM can gather information almost from every source. The most important thing is delivery of data as different sources can refer to the same event differently.

In order to systematize information, controllers, remote data collection via NetBIOS, RPC, TFTP, FTP protocols, or event sending as SYSLOG are used. For example, **SIEM analyses:**

EVENT LOGS OF SERVERS AND WORKSTATIONS

Used to control access, compliance with information security policies.

ANTIVIRUSES

Information about availability, reliability, and validity of antivirus SW, information about infections, and virus epidemics.

NETWORK ACTIVE EQUIPMENT

Used to control access and network traffic.

FIREWALLS

Information about attacks, malware, etc.

ACCESS CONTROL, AUTHENTICATION

Control of access to information systems and use of rights.

SIEM
SEARCHINFORM

WHAT DOES SEARCHINFORM EVENT MANAGER CONTROL?

SIEM is capable of analyzing data from numerous sources. But there are solutions used in vast majority of companies: Active Directory, antiviruses, Proxy, Exchange, accounting software. They should be supported first of all.

SIEM controls:

- Active Directory domain controllers.
- Access to file resources.
- User activity.
- Exchange mail servers.
- Kaspersky antivirus.
- DBMS (MS SQL).
- Syslog of hardware and applications.
- SearchInform DLP.

Currently under development and testing:

- Network equipment and proxy-server traffic.
- Virtualization environments and terminal servers.
- Email captured via mail server integration.
- Netflow (detecting suspicious network activity, DDoS attacks, etc.)
- Dynamical dashboards.
- More antiviruses, DBMS, and mail servers.

SIEM
SEARCHINFORM

PECULIARITIES OF SEARCHINFORM EVENT MANAGER

One of the key advantages of SearchInform Event Manager is easy implementation and availability for operation right out of the box. The system is supplied with a set of ready-made policies and considers experience and tasks of companies from all business and economic spheres.

The principle of the system operation: taking practical tasks and solving them with SIEM. We have gathered opinions, practices, and needs of SearchInform clients and generated the policies out of all these. The system will be developed in the same way: when there are new sources of data, client will get a set of rules.

SIEM
SEARCHINFORM

EXAMPLES OF PRESET POLICIES OF SEARCHINFORM SIEM

For Active Directory domain controller:

- Temporary renaming of a user account
- Password-guessing
- Multiple accounts on a single computer
- Password set by domain administrator
- Obsolete passwords
- Logon statistics
- One account on multiple computers
- Temporary enablement of account
- Temporary addition of account to group
- Obsolete AD account becoming active
- Temporary assignment of AD permissions
- Creation of temporary user accounts
- Operations on accounts
- Change of membership in critical user groups
- Use of service accounts
- User-initiated event log clearing
- Audit policy change

SIEM
SEARCHINFORM

EXAMPLES OF PRESET POLICIES OF SEARCHINFORM SIEM

For file operations:

- Temporary granting of file/folder permissions
- Access to critical resources
- Large number of users working with a file
- Operations on specific file types
- Statistics of changes of access rights to files/folders

For MS SQL:

- Temporary creation of MS SQL accounts.
- Temporary enablement of MS SQL accounts
- Statistic changes of access rights to MS SQL
- Temporary inclusion of users in DB security role
- SQL account password set by DB administrator
- Temporary renaming of MS SQL account

SIEM
SEARCHINFORM

EXAMPLES OF PRESET POLICIES OF SEARCHINFORM SIEM

For Kaspersky Antivirus:

- Software execution blocked by antivirus self-protection
- Antivirus self-protection disabled
- Antivirus protection components disabled
- Failure to perform an administrative management task
- Change of membership in the administrator group
- Blocked and infected programs
- Virus outbreak detected

For Exchange:

- Change of audit parameters of administrator
- Change of management roles
- Granting mail access
- Owner of mail box was changed
- Groups of management roles were changed
- Access to mail box by another user

For user activity:

- Activity out of working hours
- Long-absent user activity

SIEM
SEARCHINFORM

EXAMPLES OF PRESET POLICIES OF SEARCHINFORM SIEM

For Syslog:

- Custom Syslog rules
- Kernel events
- User-level events
- Mail systems events
- System daemons events
- Security and authorization events
- Internal Syslog events
- Line printer subsystems events
- Network news subsystems events
- UUCP subsystems events
- Clock daemons events
- FTP daemons events
- NTP subsystems events
- Log audit events
- Log alert events
- Scheduling daemon events
- SearchInform DLP events

SIEM
SEARCHINFORM

ADVANTAGES OF SEARCHINFORM EVENT MANAGER

EASY IMPLEMENTATION

1 SearchInform SIEM does not require intensive preliminary configuration. Preset security policies are based on a selection of common tasks that SearchInform clients have to tackle. SearchInform SIEM provides immediate results of analysis right out of box.

FOR MEDIUM AND SMALL-SIZED BUSINESS

3 SearchInform SIEM has low hardware and software requirements and reasonable price even for small-sized business. The solution is easy to integrate and requires minimum customization.

EASY OPERATION

2 Operation complexity of greater part of SIEMs demands the involvement of highly experienced and expensive experts. SearchInform SIEM is supplied with a set of prebuilt policies, embodying the experience and the challenges of real-life businesses from all major verticals. The system undergoes constant improvement based on the feedback from business, and all the users benefit from the updates.

SIEM
SEARCHINFORM

ADVANTAGES OF SEARCHINFORM EVENT MANAGER

EXPERIENCE OF OVER 1000 CLIENTS

4 We have studied the experience of our clients, figured common needs and best practices in order to implement them in SearchInform Event Manager.

SYMBIOSIS OF SIEM AND DLP

5 Simultaneous operation of SIEM and SearchInform DLP significantly strengthens company's information security. SIEM detects the abnormal behavior and shows the patterns of access to information. DLP evaluates the contents of all communications. Such combination of both systems provides for proper investigations and collection of thorough evidence.

SIEM
SEARCHINFORM

CASES

Password guessing

SIEM will notify security department about multiple attempts to guess passwords to employees' accounts on one or several PC.

Entry using service account

When you use SQL Server, domain account with full access rights to all data bases is created. SIEM notifies if, with the help of service login and password for SQL Server, a user logged in because there is a great probability of stealing sensitive information from these bases.

Unauthorized access to corporate e-mail

Administrator of mail server can reconfigure the system to get access to e-mail of top manager or other employee. SIEM will timely react to the incident and notify information security department.

SIEM
SEARCHINFORM

CASES

AD accounts: deactivation, change of name, and simple password

To steal data, unblocked accounts of retired employees are used. Employees who have not changed password for long or gave it to someone else are also at risk. Besides, administrator can temporarily rename someone's account and give network access to intruders.

Correlation of unconnected data

There are situations when events, seemingly harmless, all together can pose great threat. For example, when someone sends password of top manager's account. By itself, this event will not attract attention but, if further this account accesses critical resources, the system will record the incident.

SIEM
SEARCHINFORM

CASES

“Ghost employees” in the company

IT experts can weaken protection of corporate network by being inactive. SIEM will recognize when and if administrator does not delete accounts of retired employees. For example, a former manager was using login and password to view commercial documents on the network disk. Upon next authorization, SIEM noticed the action on the employee’s PC and notified security department.

Detection of “unusual” incidents

One savvy employee was trying to copy client base in an unusual manner. This employee’s own account did not have rights to obtain data from CRM. The employee created a new DBMS account and tried to get information directly from database. One of the SIEM policies controlled access of new accounts to the database, so the system immediately notified security officers about the violation.

SIEM
SEARCHINFORM

SEARCHINFORM TODAY

- Over **1.700** customers in **12** countries
- Over **11** years on the DLP market, **21** years in the IT industry
- SearchInform DLP monitors over **1.000.000** PCs
- Experienced deployment and support team
- In-house Training Center

GAZPROM SUKHOI En+ GROUP LUKOIL OIL COMPANY MTS RTSoft tools and automation systems

SEARCHINFORM
INFORMATION SECURITY

Incident is detected.
It’s time to investigate.

START YOUR FREE TRIAL TODAY!

SEARCHINFORM
INFORMATION SECURITY