SIEM

SEARCHINFORM

What business tasks does SIEM solve?

CHALLENGE

IT infrastructure of a today's company is a complex mechanism that includes a great many of corporate systems:

- Firewall
- Antiviruses
- Applications
- Databases
- OS servers and PCs
- Email servers
- Active Directory
- Network hardware and other hardware

Every system is a source of financial and corporate data, information about clients and other valuable information that violators aim to obtain.

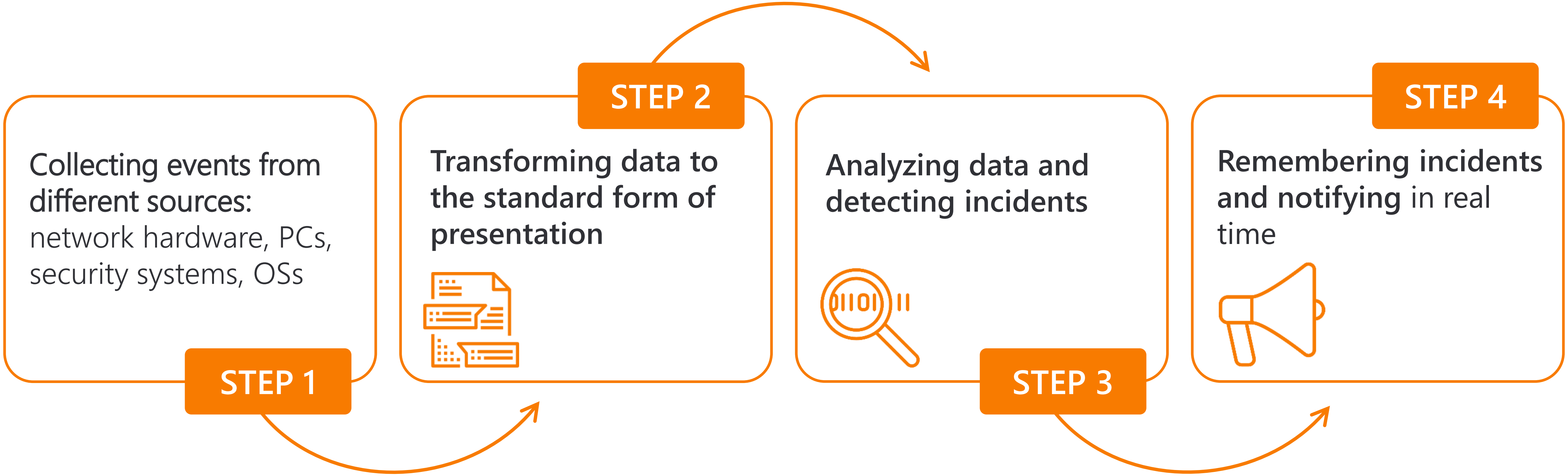
The company can be endangered both by actions of system administrators (unauthorized granting of access rights, creation or deleting accounts, disabling firewall) and by vulnerability of the products through which violators can get access to company's data.

SOLUTION

SIEM (Security information and event management)**:** system for analyzing flow of events, detecting information security incidents, and reacting to them.

SIEM accumulates information from different sources, analyzes it, detects incidents, and notifies about them.

Operating principle of SearchInform Event Manager – in the algorithm:



STEP 1

Collecting events from different sources: network hardware, PCs, security systems, OSs

STEP 2

Transforming data to the standard form of presentation

STEP 3

Analyzing data and detecting incidents

STEP 4

Remembering incidents and notifying in real time

SIEM
SEARCHINFORM

What incidents does SearchInform Event Manager detect?

- **Virus epidemics** and separate virus infections
- **Attempts to get unauthorized access** to confidential information
- **Errors and failures** in information systems operation
- **Critical events** during security system operation

What sources does SearchInform Event Manager analyze?

SIEM can gather information almost from every source. The most important thing is the right delivery of data as different sources can refer to the same event differently. In order to systematize information, connectors to EventLog or Syslog events are used.

For example, **SearchInform Event Manager analyses:**

EVENT LOGS OF SERVERS AND WORKSTATIONS

Used to control access, compliance with information security policies.

NETWORK ACTIVE EQUIPMENT

Used to control access and network traffic, detect attacks, notify about errors and network statuses.

ACCESS CONTROL, AUTHENTICATION

Control of access to information systems and use of rights.

ANTIVIRUSES

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

What does SearchInform Event Manager control?

- Active Directory domain controllers
- EventLog;
- File resources
- User activity
- Email servers (MS Exchange, Postfix)
- Antiviruses (Kaspersky, Symantec)
- DBMS (MS SQL, Oracle)
- Syslog of hardware (server, routers, printers, etc.) and applications
- File operations on connected devices
- SearchInform DLP
- Cisco network hardware
- FortiGate complex network security hardware
- VMware ESXi
- Apache HTTP servers
- Vsftpd FTP servers
- Linux server and workstations
- Checkweighers

- NetFlow and OPSEC support
- Dynamical dashboards
- More antiviruses, DBMS and email servers
- IDS and IPS support

Under development and testing

SIEM
SEARCHINFORM

Highlights of SearchInform Event Manager

One of the key advantages of SIEM is easy implementation and capability to work “out of 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, experience, and needs of SearchInform clients and “shaped” them in the policies. The system will be developed in the same way: when there are new data sources, client will get a set of rules.

EXAMPLES OF PRESET POLICIES

Syslog

- Custom Syslog rules
- Kernel events
- User-level events
- Mail systems events
- System daemons events
- Security and authorization events, etc.

SearchInform DLP events

- Incidents and changes in AlertCenter
- DataCenter events

User activity

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

EXAMPLES OF PRESET POLICIES

Active Directory domain controllers

- Temporary renaming of account
- Password guessing and obsolete passwords
- Temporary enablement/addition of account
- Control of obsolete AD accounts
- Temporary assignment of AD permissions
- One account on multiple computers, etc.

File resources

- 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

EXAMPLES OF PRESET POLICIES

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

Oracle

- Failed logins attempts
- Successful logins attempts
- User or role creation
- User or role removal
- User locked/unlocked
- User password changed
- Listener log, etc.

EXAMPLES OF PRESET POLICIES

Email servers

- Access to mail box by another user
- Owner of mail box was changed
- Granting mail access
- Change of audit policy
- Change of critical roles and other events

Devices

- Copying to removable device
- Operations with executables on devices
- File execution from removable device
- Copying too many files to removable device
- Copying much data to removable device

EXAMPLES OF PRESET POLICIES

Virtualization environments

- VMware logon/logout events
- Invalid passwords
- Failed logons attempts
- User group creation
- User password changed
- User creation/removal
- Snapshots deleted, etc.

Linux servers and workstations

- Logon of unknown user
- Logon with elevated rights
- Shell changed
- Authentication failed
- Multiple authentication failures
- SSH login/logout events
- Opened/closed sessions
- SSH access failed, etc.

EXAMPLES OF PRESET POLICIES

CISCO

- Console logon events
- Built-in user account logon
- Logon with elevated rights
- System errors
- Power supply errors
- Cooling system failure
- DHCP errors
- Routing errors
- Double router ID detected
- Wi-Fi authentication errors

Antiviruses

- Software execution blocked by antivirus self-protection
- Antivirus self-protection disabled.
- Antivirus protection components disabled
- Computer in critical state
- Potentially harmful software detected
- Failure to perform an administrative management task
- Antivirus license not found
- Change of membership in the administrator group
- Blocked and infected programs
- Virus epidemic detected

EXAMPLES OF PRESET POLICIES

Apache web servers

- Authentication failed
- User not found
- Wrong password
- Wrong authorization scheme is used
- Client denied by server config
- Unknown encryption algorithm
- Invalid Nonce, etc.

Vsftpd FTP servers

- Client connection to FTP
- File download from FTP
- File creation/deletion on FTP
- Directory creation/deletion on FTP

And **100+ more policies** used in different combinations. The list of connectors and rules is continuously extended.

ADVANTAGES of SearchInform Event Manager

EASY IMPLEMENTATION

SIEM does not require any pre-setting. Preset security policies are based on a number of typical tasks that SearchInform clients solve. SIEM provides first results of analysis "out of box".

EASY OPERATION

SIEM operation does not require any programming skills. Any expert will be able to customize SIEM. The solution is supplied with a set of versatile policies without any need to create scripts and write event correlation rules. And SearchInform Deployment Department will help configure individual policies.

ADVANTAGES of SearchInform Event Manager

FOR MEDIUM AND SMALL-SIZED BUSINESS

SearchInform Event Manager has low hardware software requirements The solution is integrated fast and requires minimum customization.
The price depends on the number: the more licenses are, the less price is.

EXPERIENCE OF MANY CLIENTS

We have studied experience of our biggest clients, found out general demands and best practices to employ them in SearchInform Event Manager.

SIEM
SEARCHINFORM

ADVANTAGES of SearchInform Event Manager

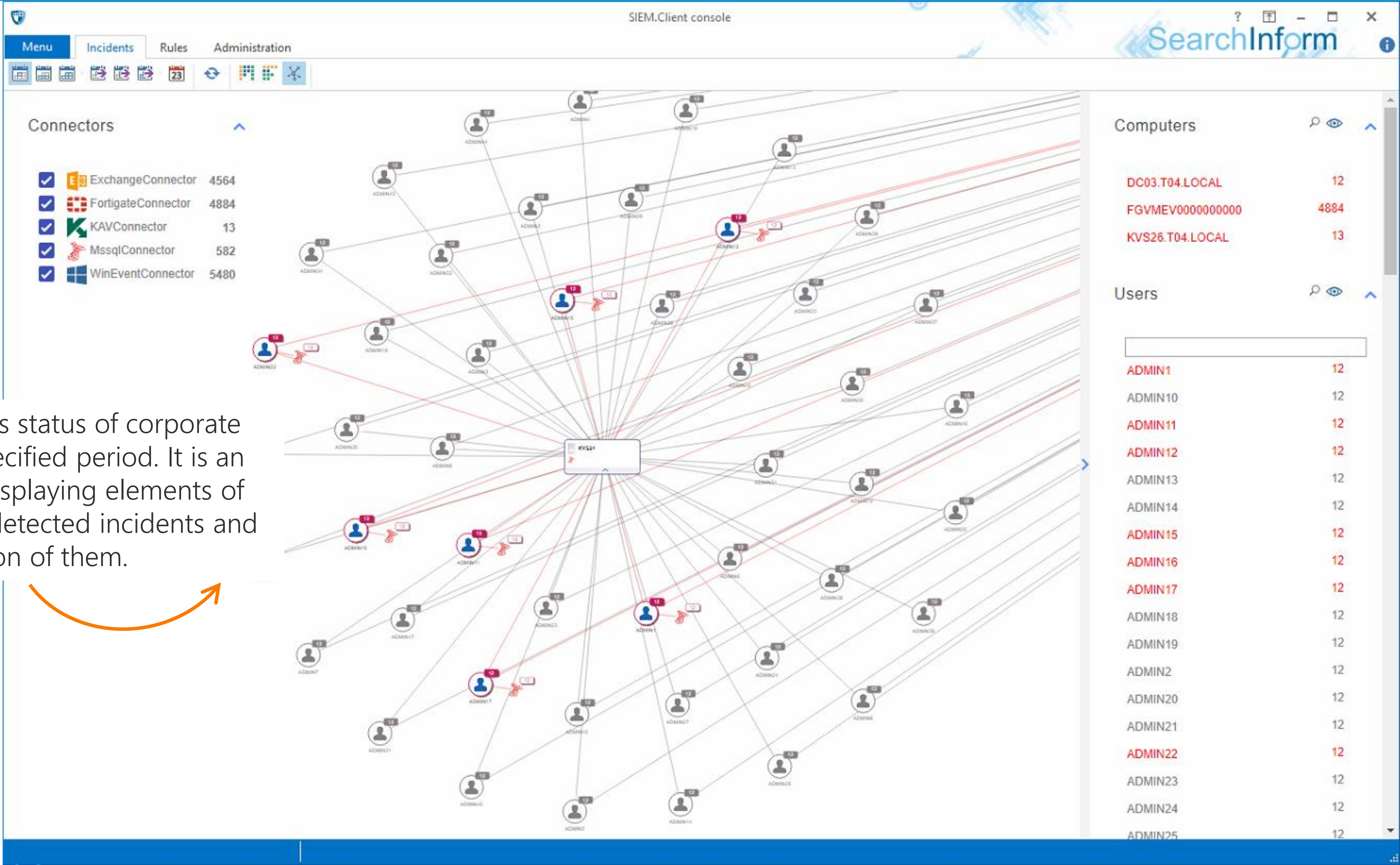
SYMBIOSIS OF SEARCHINFROM EVENT MANAGER AND SEARCHINFORM DLP

The simultaneous operation of SearchInform Event Manager and SearchInform DLP strengthens significantly company's information security. SIEM detects wrong behavior and how the access to information was gained. SearchInform DLP analyzes all communication. The combination of the two systems enables you to investigate any incident properly and get evidence.

ALL PRERQUISITES FOR PROPER INCIDENT MANAGEMENT

SIEM constantly accesses event sources and processes new events upon the system login already. Security officer gets some time to promptly react to a threat and maintain security sustainability.

GRAPH OF INCIDENTS



Connectors

☑	ExchangeConnector	4564
☑	FortigateConnector	4884
☑	KAVConnector	13
☑	MssqlConnector	582
☑	WinEventConnector	5480

Computers

DC03.T04.LOCAL	12
FGVMEV0000000000	4884
KVS26.T04.LOCAL	13

Users

ADMIN1	12
ADMIN10	12
ADMIN11	12
ADMIN12	12
ADMIN13	12
ADMIN14	12
ADMIN15	12
ADMIN16	12
ADMIN17	12
ADMIN18	12
ADMIN19	12
ADMIN2	12
ADMIN20	12
ADMIN21	12
ADMIN22	12
ADMIN23	12
ADMIN24	12
ADMIN25	12

The graph displays status of corporate system for the specified period. It is an interactive map displaying elements of IT infrastructure, detected incidents and detailed description of them.

SIEM
SEARCHINFORM

SearchInform Event Manager: CASES

PASSWORD GUESSING

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

USER LOGIN UNDER 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 EMAIL

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

SearchInform Event Manager: CASES

AD ACCOUNTS: DEACTIVATION, CHANGE OF NAME, AND SIMPLE PASSWORD

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. SIEM will inform if it detects such incidents.

CORRELATION OF UNRELATED 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 mark the incident.

SearchInform Event Manager: CASES

GHOST EMPLOYEES IN THE COMPANY

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

DETECTION OF UNUSUAL VIOLATIONS

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.

SearchInform today

17 offices worldwide

11 years in DLP market
22 years in IT

2000+ clients
in 17 countries worldwide

1 200 000+ PCs controlled with SearchInform software

In 2017, SearchInform DLP was included in **the Gartner Magic Quadrant**

23 criminal cases won by clients against insiders

SEARCHINFORM
RISK AND COMPLIANCE MANAGEMENT

Incident is detected.

Time to investigate. Start your free trial today!

+7 (495) 721-84-06
info@searchinform.ru
searchinform.com

SEARCHINFORM
RISK AND COMPLIANCE MANAGEMENT