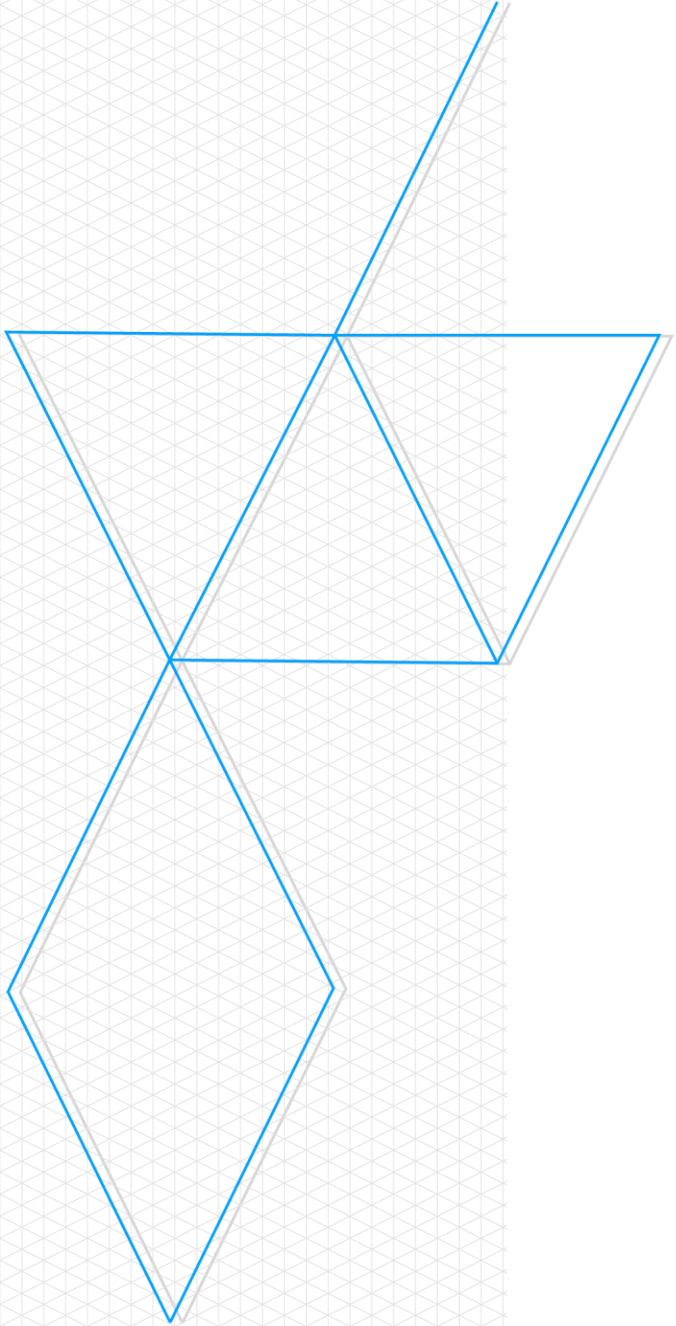
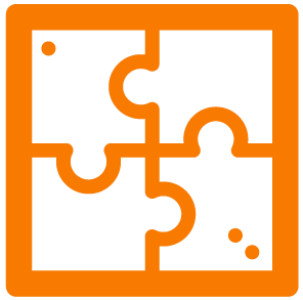




SIEM

SEARCHINFORM

searchinform.com

What business tasks does SIEM solve?

CHALLENGE

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

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

Every system is a source of personal, financial and corporate data that violators aim to obtain.

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

SIEM
SEARCHINFORM

Operating principle of SearchInform SIEM is its algorithm:

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

STEP 1

STEP 2

Analyzing data and making correlations,
detecting incidents

Remembering incidents and notifying
in real time

STEP 3

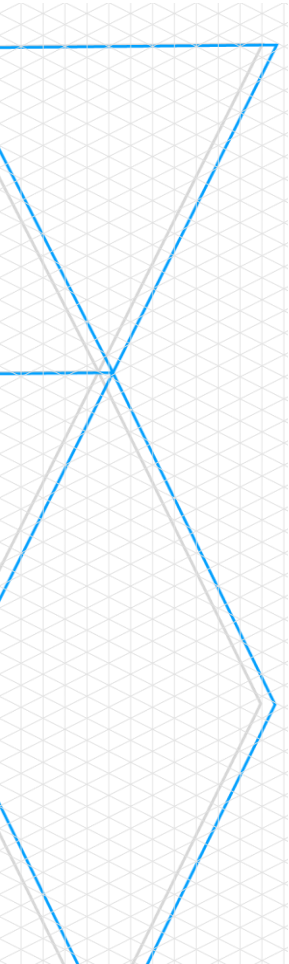
SIEM
SEARCHINFORM

What incidents does SearchInform SIEM detect?

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

What sources does SearchInform SIEM analyze?

SIEM can gather information almost from every source:



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

Information system access rights control

ANTIVIRUSES

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

VIRTUALIZATION ENVIRONMENTS

Virtual machines creation, usage, and deletion control

SIEM
SEARCHINFORM

What does SearchInform SIEM control?

SIEM
SEARCHINFORM

- Active Directory domain controllers
- EventLog
- Email servers (MS Exchange, Postfix, IBM Domino)
- Antiviruses (Kaspersky, Symantec, McAfee, ESET)
- DBMS (MS SQL, Oracle, PostgreSQL)
- Syslog of hardware (server, routers, printers, etc.) and applications
- SearchInform DLP (user activity, access to file resources, file operations on connected devices)
- Cisco, Palo Alto, and Check Point network hardware
- VMware ESXi;
- FortiGate devices for complex network security
- Apache HTTP servers
- Vsftpd FTP servers
- Linux server and workstations
- Checkweighers
- Dynamic dashboards

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

Under development and testing

Highlights of SearchInform SIEM

One of the key advantages of SearchInform SIEM is easy implementation and capability to be deployed as an out-of-the-box solution. The system is supplied with a set of ready-made policies and takes into account 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 is developed in the same way: when there are new data sources, client gets 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
- Other events

SearchInform DLP events

- Incidents and changes in AlertCenter
- Grant access rights for a file/folder
- Critical resource access
- Copying to removable devices
- File execution from removable devices
- User activity during the off-hours

EXAMPLES OF PRESET POLICIES

Active Directory domain controllers

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

DBMS (MS SQL, Oracle, PostgreSQL)

- Temporary creation of accounts
- Temporary activation of accounts
- Statistical changes in access rights
- Successful/unsuccessful logon attempts
- User password change
- Listener events
- User authentication errors
- Errors in operation

EXAMPLES OF PRESET POLICIES

Email servers (Exchange, IBM Domino)

- Access to the mailbox by another user
- New owner of the mailbox
- Granting mail access
- Audit policy change
- Change of critical roles and other events

Virtualization environments (VMware)

- VMview and Vmware logon/logout events
- Invalid passwords
- Failed logon attempts
- User group creation
- User password change
- User creation/removal
- Removal of Snapshots, etc.

EXAMPLES OF PRESET POLICIES

AD monitoring

- Scheduled AD structure snapshots taking
- Control of all attribute changes
- Control of AD objects adding/removing
- Capability to compare any two AD snapshots to each other, detecting all attribute changes, adding/removing AD objects

Linux servers and workstations

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

EXAMPLES OF PRESET POLICIES

Devices (Fortigate, Palo Alto, Check Point, CWA, Cisco)

- Logon/logout events
- Cooling system failure
- Logon with elevated rights
- System errors
- Event logs of System, Threat, Authetication, Traffic, VoIP, etc.
- Event logs of AntiSpam, AntiVirus, AntiBot, IPS, Threat Emulation, etc.

Antiviruses (Kaspersky, McAfee, ESET, Symantec)

- Antivirus self-protection disabled
- Virus detected
- Virus epidemic detected
- Network attack detected
- Antivirus protection components disabled
- Computer in critical state
- Failure to perform an administrative management task
- Antivirus license not found
- Potentially harmful software detected

EXAMPLES OF PRESET POLICIES

Apache web servers

- Authentication failed
- User not found
- Wrong password
- Invalid authorization scheme
- Client denied by server configuration
- Unknown encryption algorithm
- Error: Invalid Nonce
- Other errors

Vsftpd FTP servers

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

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

ADVANTAGES
of SearchInform SIEM

EASY IMPLEMENTATION

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

EASY DEPLOYMENT

SIEM deployment and implementation process does not require any programming skills. Any expert will be able to customize SIEM. There is no need to create scripts and write event correlation rules because the solution is supplied with a set of versatile policies. And SearchInform Deployment Department will help you configure individual policies.

SIEM
SEARCHINFORM

ADVANTAGES
of SearchInform SIEM

FOR MEDIUM AND SMALL-SIZED BUSINESS

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

EXPERIENCE OF MANY CLIENTS

We have studied the experience of our biggest clients, identified general needs and best practices to employ them in SearchInform SIEM.

SIEM
SEARCHINFORM

ADVANTAGES
of SearchInform SIEM

SYMBIOSIS OF SEARCHINFROM SIEM AND SEARCHINFORM DLP

The simultaneous operation of SearchInform SIEM and SearchInform DLP fortifies a company's information security program. SIEM detects abnormal behavior and the way the access to information is gained. SearchInform DLP analyzes communication channels. The combination of the two systems enables you to investigate any incident properly and get evidence.

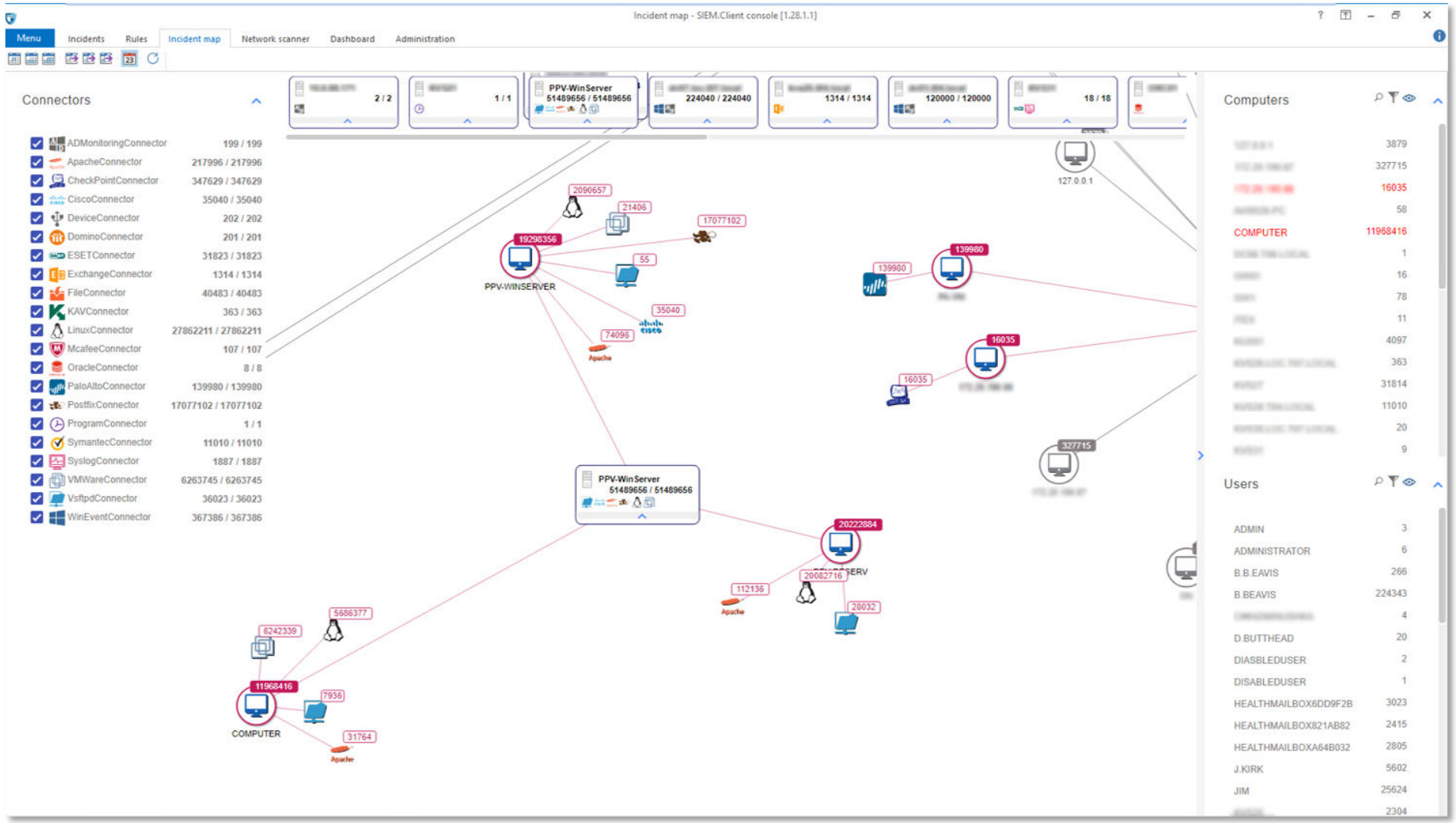
SIMPLE LICENSING SYSTEM

The number of licenses depends on the number of users/equipment units.

SIEM
SEARCHINFORM

GRAPH OF INCIDENTS

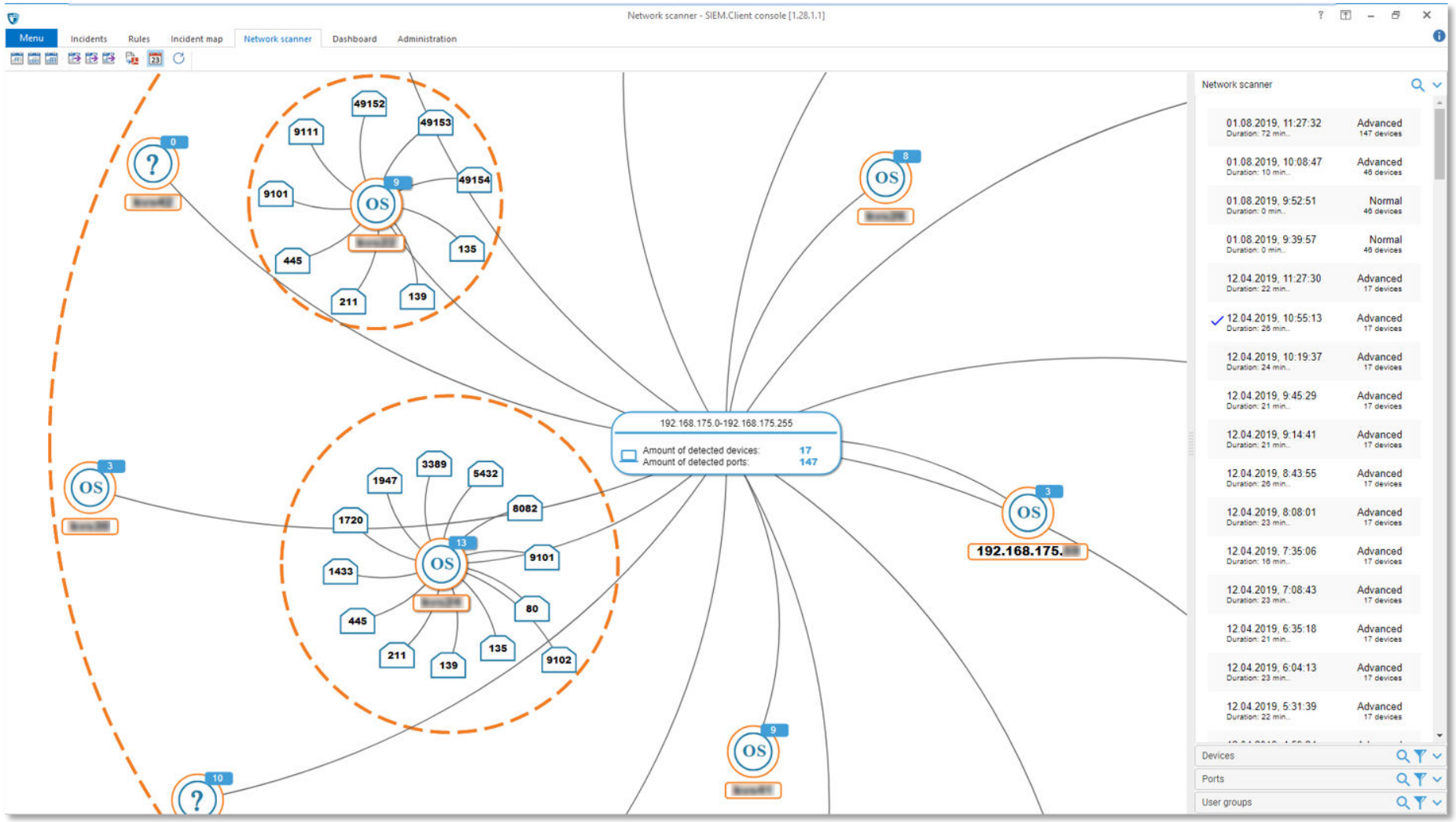
The graph of incidents is an interactive map displaying elements of IT infrastructure and users, detected incidents and detailed description of them.



SIEM
SEARCHINFORM

Network scanner

The network scanner takes a scheduled snapshot of network assets and determines their number, IP addresses, type, OS, open ports, etc. Provides you with the graphics to control the status of the company's IT infrastructure.



SIEM
SEARCHINFORM

SearchInform SIEM: CASES

PASSWORD GUESSING

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

USER LOG IN 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 credentials 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 a mail server can reconfigure the system to get access to email of a top manager or other employee. SIEM will promptly react to the incident and notify information security department.

SIEM
SEARCHINFORM

SearchInform SIEM: CASES

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

Employees who do not change passwords for a long time or give it to someone else are also at risk. Besides, an administrator can temporarily rename someone's account and give network access to intruders. SIEM will inform you if it detects such incidents.

CORRELATION OF UNRELATED DATA

There are situations when events, seemingly harmless, together can pose great threat. For example, when someone sends a password to a top manager's account. This event will not attract attention but, if later this account accesses critical resources, the system will alert to the incident.

SIEM
SEARCHINFORM

SearchInform SIEM: CASES

GHOST EMPLOYEES IN A COMPANY

IT experts can weaken protection of a corporate network by being inactive. SIEM will notice when and if an administrator does not delete accounts of fired employees. For example, a former manager used username and password to view commercial documents on the network disk. During next authorization episode, 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. The employee's account did not have rights to obtain data from CRM. The employee created a new DBMS account and tried to get information directly from the database. One of the SIEM policies managed the access of new accounts to the database, and the system immediately notified specialists about the violation.

SEARCHINFORM TODAY

17 branch offices worldwide

13 years in RM market,
24 years in IT

More than 2 500+ clients in 17 countries

More than
1 500 000+ PC
are guarded by the
SearchInform products

In 2017 the SearchInform solution was recognized by Gartner

25 criminal trials against insiders have been won by clients

SIEM
SEARCHINFORM

Incident is detected.
Time to investigate.

SEARCHINFORM
RISK AND COMPLIANCE MANAGEMENT

+44 0 20 3808 4340
order@searchinform.com