# SearchInform SIEM

SEARCHINFORM

RISK AND COMPLIANCE MANAGEMENT

## Challenge

Data leaks do not occur all of a sudden, they are always preceded by a number of events. Unfortunately, the significance of such events often becomes evident only post-factum. Whether you missed a user accessing a specific resource or didn’t notice an administrator granting elevated privileges – the problem with such loopholes is in the constantly growing volumes of data that information security officers have to work with.

## Solution

SearchInform SIEM is designed to perform collection and automated analysis of various corporate system events in order to reveal threats and information security breaches.

The complex mechanism of SearchInform SIEM operation boils down to a quite simple algorithm:

- It collects events from different systems (network equipment, software, security tools, OS).
- It structurizes data.
- It analyzes data and reveals threats.
- It detects incidents and notifies about them in real time.

## What SearchInform SIEM Controls

SearchInform SIEM supports the following data sources:

- Active Directory domain controllers
- Windows logs
- Data on file operations
- Data on user activity
- Logs of Exchange and IBM Domino mail servers
- Databases of Kaspersky, Symantec and McAfee antiviruses
- Log files of DBMS (MS SQL, Oracle, PostgreSQL)
- Syslog of hardware and software
- SearchInform RM applications
- Data on operations with external devices
- Syslog of VMware ESXi
- Syslog of Cisco network hardware
- Syslog of FortiGate complex network security hardware
- Syslog of Linux
- Syslog of Apache web server
- Syslog of Postfix mail server
- Syslog of Very Secure FTP Daemon server
- Syslog of Palo Alto and Check Point firewalls
- Syslog of ESET antivirus
- Logs of 1C and Checkweighers

Currently under development and testing:

- Terminal servers
- Netflow and OPSEC support
- Dynamical dashboards
- More antiviruses, DBMSs, and mail servers
- IDS and IPS support

# Software Objectives

## 1. Collecting and processing events from different sources

The sheer number of event sources nowadays is so high that it's impossible to manually control all events in the infrastructure. And this might lead to the following risks:

- Missing a security violation
- Failure to identify details and determine causes (due to event log clearance, etc.)
- Failure to reconstruct events.

And SearchInform SIEM, as an aggregator of information from different devices, solves this problem. The system unifies the data and provides a secure storage for the data.

## 2. Event analysis and incident processing in real time

SearchInform SIEM does not just correlates events, but also evaluates their significance. The system visualizes the information focusing on important and critical events.

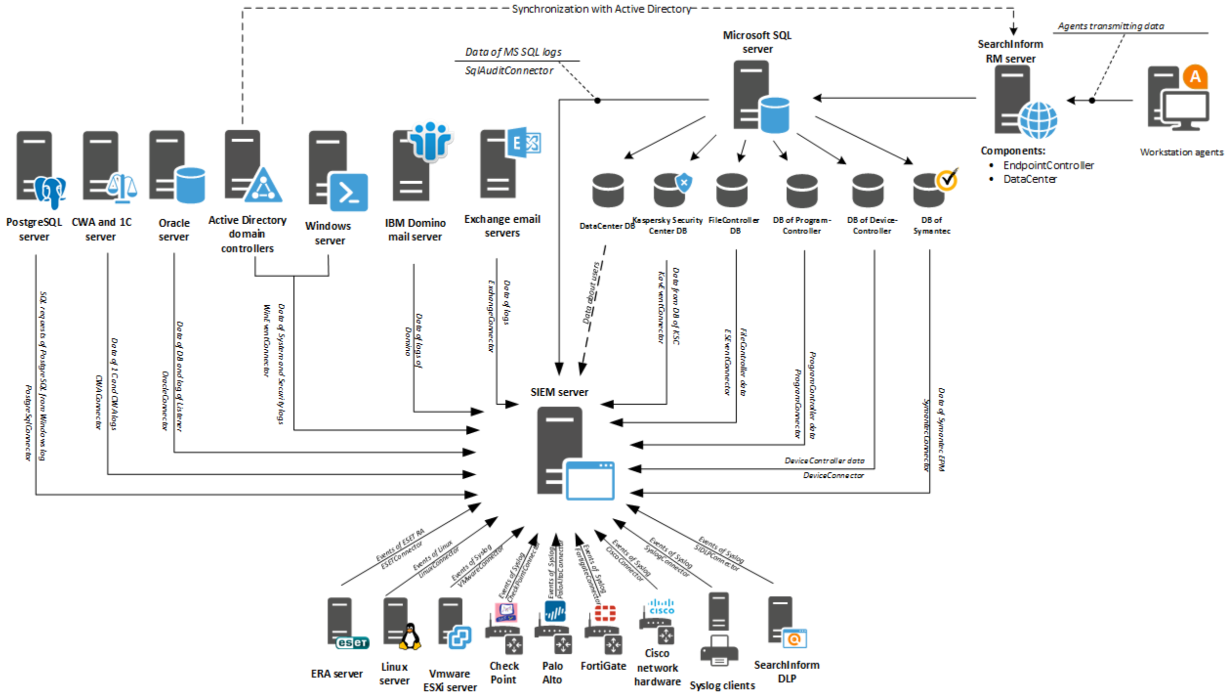
## 3. Correlation and processing based on rules

A single event is not always indicative of an incident. For example, a single failed logon might be just accidental, however, three or more attempts probably indicate a password-guessing attack. To identify really critical events, SearchInform SIEM uses rules that contain a whole range of conditions and take into account the most diverse scenarios.

## 4. Automated notification and incident management

Automated notifications and incident management enable SearchInform SIEM to fulfill its main purpose: Create conditions for information security officers to rapidly respond to incidents. The solution provides automatic detection of incidents.

# Architecture and Operation Principle



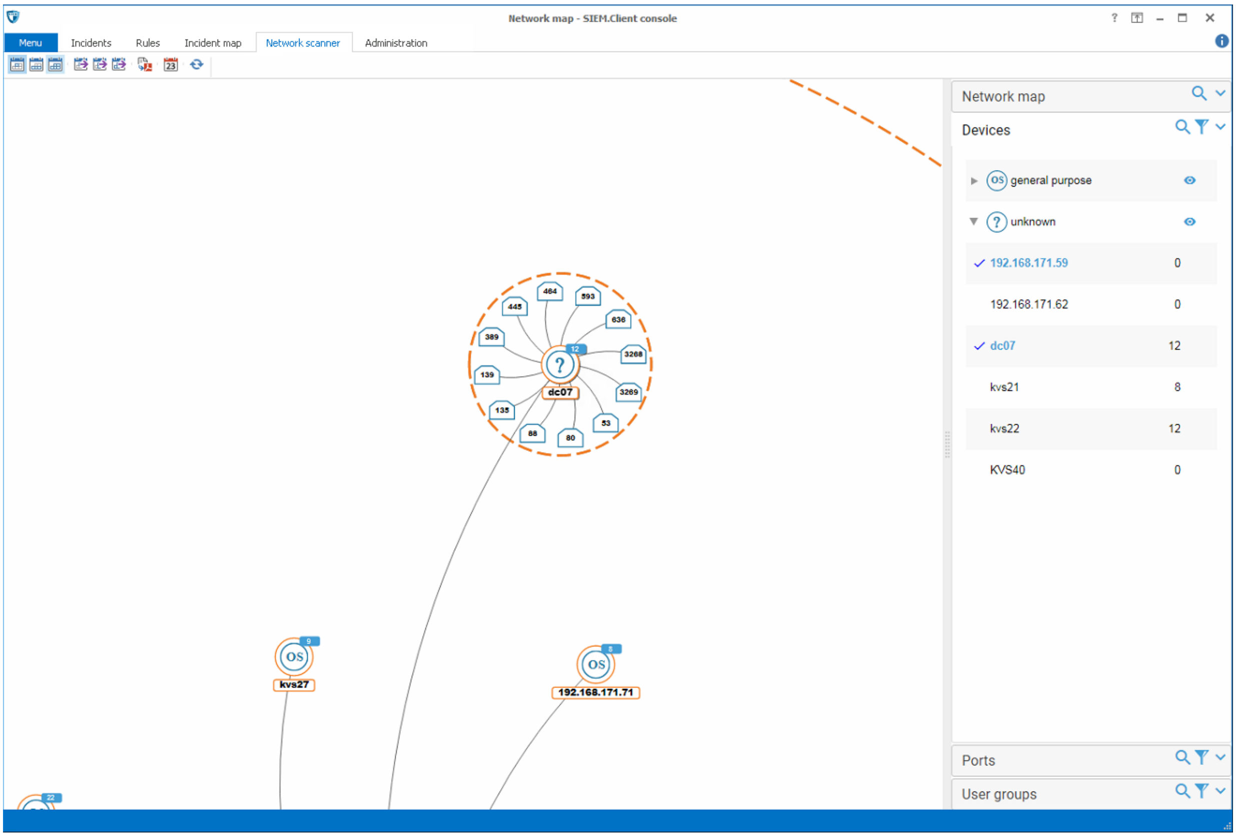
- From the SearchInform SIEM management console, you can set up connection to event sources, configure rules and notifications.
- The connectors collect events of data sources:
  - — Connecting to logs and databases of data sources
  - — Receiving events of Syslog from different hardware.
- The system analyzes in real time the collected data based on configured rules and saves detected incidents to a MongoDB database.
- Upon detection of an incident, the system immediately sends a notification to the information security officer.
- SearchInform SIEM management console lets you build reports on detected incidents and export selected events to a file.

## Network Scanner

This functional tab contains data on the number of computers, printers, servers, routers and other devices on the network.

The scanner collects information about network resources such as names, IP and MAC addresses, used ports, OS info and other characteristics of network objects. Detected devices (objects) of network ad open ports are displayed in a visual graph, as well as in the list.

The dashboard allows fast-tracking connections/disconnections of devices on the network.



| | |
|---|---|
| ▶ OS general purpose | |
| ▼ ? unknown | |
| ✓ 192.168.171.59 | 0 |
| 192.168.171.62 | 0 |
| ✓ dc07 | 12 |
| kvs21 | 8 |
| kvs22 | 12 |
| KVS40 | 0 |

## Key Advantages

- **Takes into account the experience of thousands of clients**

  SearchInform supplies ready scenarios which can work efficiently and provide results immediately after the software installation. SearchInform SIEM was designed based on requests of our largest clients from different industries.

- **Ready to function “out of the box”**

  SearchInform SIEM quickly integrates into your system and requires a minimum setup. The solution incorporates predefined universal security policies (the up-to-date list of policies is provided at the bottom of this document).

- **Affordable even for small companies**

  SearchInform SIEM pricing policy and technical support fees are more beneficial for the customer in comparison to other solutions. Besides, SearchInform software products are less demanding in terms of hardware and software requirements.

- **Integrated with SearchInform RM**

  SearchInform SIEM collects, analyzes, and correlates data with SearchInform RM agents or captured network traffic. The SIEM+RM bundle allows revealing tiniest details of an incident.

## System Requirements

| | Minimum system requirements<br>(for 1 out-of-box set of rules, 1 domain controller) |
|---|---|
| CPU | 2.1 GHz 4-core |
| RAM | 4 GB[1] |
| Hard drive | 200 GB[2] |
| Network card | 100 Mbit/s |

[1] Custom rule creation requires higher RAM (~15 MB for each new rule).

[2] As events are saved to SearchInform SIEM database, additional disk space might be required.

# Preset Policies of SearchInform SIEM*

## Preset polices for Active Directory domain controllers

- Temporary renaming of account
- Password-guessing
- Multiple accounts on a single computer
- Password set by domain administrator
- Obsolete passwords
- Logon statistics
- One account on multiple computers
- Password changed by user
- Password guessing
- Non-existent user logon
- Blocked user logon
- 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

## Preset policies 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

## Preset policies 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

## Preset policies for Kaspersky Antivirus

- 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 epidemy detected

## Preset policies for Exchange

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

## Preset policies for user activity

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

## Preset policies for Syslog events

- 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
- Other events

### Preset policies for SearchInform RM applications

- Changes AlertCenter
- Incidents in AlertCenter
- Events of DataCenter

### Preset policies for Device

- 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

### Preset policies for Oracle

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

### Preset policies for VMware

- VMview logon/logout events
- VMware logon/logout events
- Invalid passwords
- Failed logons attempts
- User group/role creation
- User password changed
- User creation/removal
- Snapshots deleted
- VM directories deleted
- Starting/stopping virtual machines
- Virtual machine deleted
- LDAP connection errors
- Hardware overheat

### Preset policies for 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
- Buffer overflow
- Commands input
- Write term/write memory commands
- Change of configuration
- ACL events
- Attack detected
- Blocked DNS requests
- Denied connections
- Lost or incomplete connections
- TeamViewer events

### Preset policies for Fortigate

- Anomaly log events
- App log events
- AV log events
- DLP log events
- Email log events
- Event log events
- GTP log events
- IPS log events
- Traffic log events
- VoIP log events
- WAF log events
- Web log events

### Preset policies for Linux

- User not in sudoers group
- Elevated logon
- Shell changed
- Authentication failed
- ROOT console login
- Login/logout events
- Opened/closed sessions
- Access failed
- Multiple authentication failures
- Wrong password
- Logon denied

- No identification string received
- Invalid user
- Connect refused
- Reverse mapping for address failed
- User creation failed
- User default group changed
- User lock/unlock
- User UID changed
- User added/deleted from group
- User renamed
- User's home directory changed
- User created/deleted
- User changed
- User changed password
- DNS zone transfer denied
- DNS query denied
- No reverse name for sender IP
- Session opened/closed
- Cron tasks replacement
- Command log
- User deleted from crontab
- Command log
- Sudo commands
- Password policy changed
- Low disk space
- DHCP events
- Segmentation fault
- Shadow events
- User group created/deleted
- Resource pool changed
- MySQL client authentication failed
- Custom Linux rule
- All other Linux events

### Preset policies for Postfix events

- Sender verification error
- Receiver domain name not found
- SSL connection error
- Connection lost after AUTH command
- Multiple errors after AUTH command
- Address resolution error
- Sender's host name not found
- Relay access denied
- Unknown connect to SMTP port

- Max connection rate statistics
- Authentication failed
- Unknown user events
- Attempt to send mail to nonexistent domain
- Connection from unknown source

### Preset policies for Apache events

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

### Preset policies for Very Secure FTP Daemon events

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

### Preset policies for checkweigher events

- Login at non-working time
- Updating of the committed document
- Creating of document at non-working time
- An abrupt change in weight

### Preset policies for Symantec events

- Virus detected
- Epidemy detected
- Network and Exploit attack detected
- Selected remediation log
- Scan log
- Agent system log
- Symantec notification log

### Preset policies for Palo Alto events

- Traffic log events
- Threat log events
- Config log events
- System log events
- Hip-match log events
- UserID log events
- Tunnel Inspection log events
- Authentication log events
- Correlated log events

Preset policies for Check Point events

- Identity Awareness events
- Endpoint Security On Demand events
- SecureClient and Edge events
- IPS events
- AntiVirus events
- AntiBot and AntiMalware events
- Threat Emulation events
- AntiSpam events
- URL Filtering events
- Application Control events
- DLP events
- SmartDashboard events
- Custom Check Point event
- All other Check Point events

Preset policies for McAfee events

- McAfee malware detected
- McAfee spyware detected
- McAfee unwanted programs detected
- McAfee other threats detected
- McAfee epidemy detected
- McAfee task log
- McAfee audit log
- Computers with installed agents (Systems)

Preset policies for ESET

- Audit events
- Firewall events
- HIPS events
- Detected threats
- Re-infection detected
- Epidemic detected

- Enterprise Inspector events
- Custom ESET rule
- All other ESET events

### Preset policies for IBM Domino

- Mail tracking center vents
- Mail journal events
- Mail routing events
- WEB logon statistics
- HTTP request errors
- Domino account lockout
- Domino password guessing
- HTTP traffic
- Creating certificates
- Security events
- Domino monitoring
- Miscellaneous events

### Preset policies for 1C

- Change to a posted document
- Change in ACL configuration registers
- Change in the composition of the role
- Change to the role list
- Change in user ACL
- Change in user administration right
- Login in non-working hours
- New user creation
- Change in user privileged mode
- Privileged mode usage
- Change to the role list of user
- Logon of absent user

### Preset policies for PostgreSQL

- Create user or role
- Drop user or role
- Event of enabling of user
- Event of disabling of user
- Rename user or role
- Alter role
- Grant permission to user
- Revoke permissions
- User authentication error
- Errors when working with PostgreSQL

* The information is relevant for SearchInform SIEM 1.24.0.4 released on 20.12.2018.