

SearchInform Event Manager

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 Event Manager 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 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 SIEM Controls

SIEM supports the following data sources:

- Active Directory domain controllers
- Windows logs
- Data on file operations
- Data on user activity
- Exchange mail servers
- Kaspersky antivirus
- DBMS (MS SQL, Oracle)
- Syslog of hardware and software
- SearchInform DLP applications
- Data on operations with external devices
- VMware ESXi
- Cisco network hardware
- FortiGate complex network security hardware

Currently under development and testing:

- Virtualization environments and 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 Event Manager, 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

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

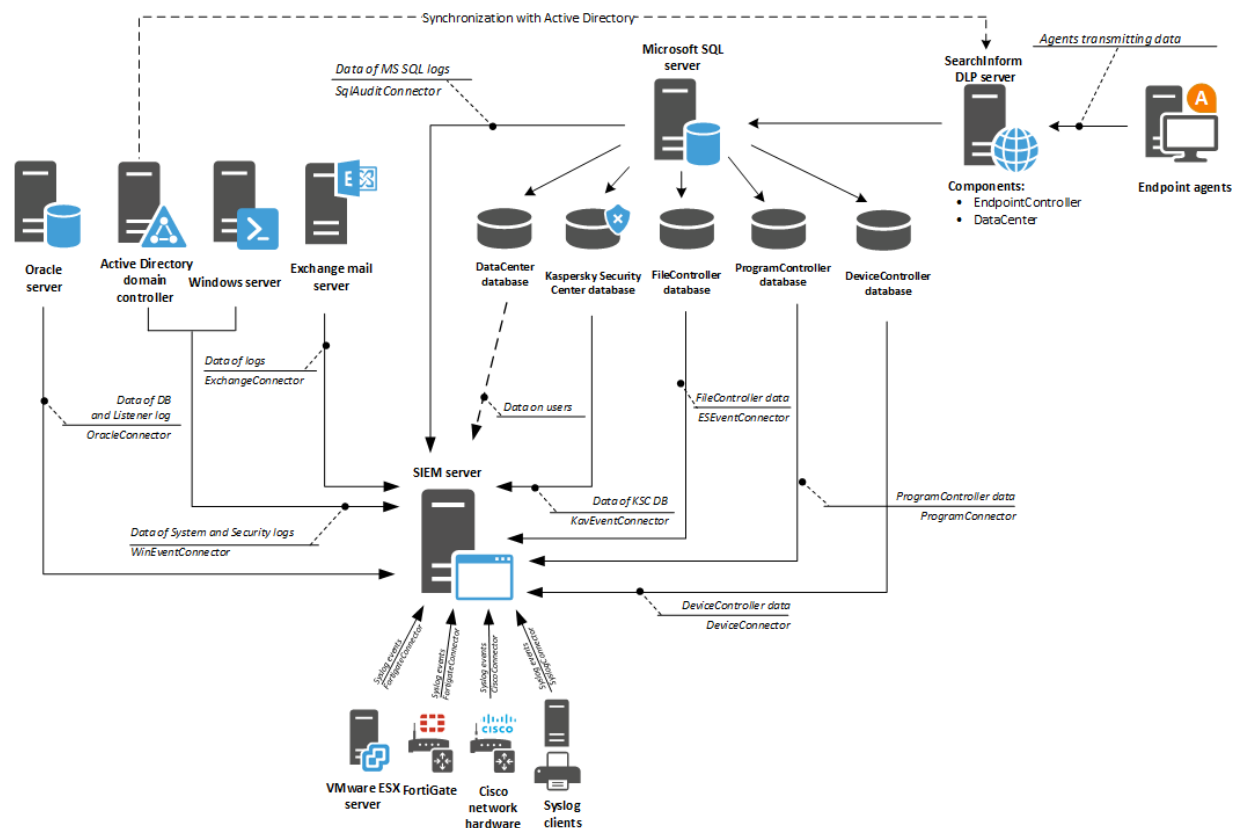
3. Correlation and processing based on rules

A single event is not always indicative of an incident. For example, a single failed login might be just accidental, however, three or more attempts probably indicate a password-guessing attack. To identify really critical events, SearchInform Event Manager 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 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 SIEM management console, you can set up connection to event sources, configure rules and notifications.
- The SIEM server reads the System and Security logs of domain controllers and Windows servers, Exchange mail servers, Kaspersky Security Center, MS SQL, Oracle, FileController, ProgramController, and DeviceController databases, as well as gets events from Syslog clients (VMware ESXi, Cisco network hardware, FortiGate). Then, 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.
- SIEM management console lets you build reports on detected incidents and export selected events to a file.

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 Event Manager was designed based on requests of our largest clients from different industries.

- **Ready to work out of the box**

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**

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 DLP**

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

System Requirements

Minimum system requirements (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 SIEM database, additional disk space might be required.

Preset Policies of SearchInform Event Manager*

Preset policies 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 epidemic 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 DLP 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

* The information is relevant for SIEM 1.10.1.4 released on 29.09.2017.