SearchInform SIEM

SEARCHINFORM

INFORMATION SECURITY

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 SIEM operation boils down to a quite simple algorithm:

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

What SIEM Controls

SearchInform SIEM supports the following sources of data:

- Active Directory domain controllers[1].
- 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.

Software Objectives

1. Collection and processing of 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.

[1] Domain controllers based on Windows Server 2008 R2 or higher are supported.

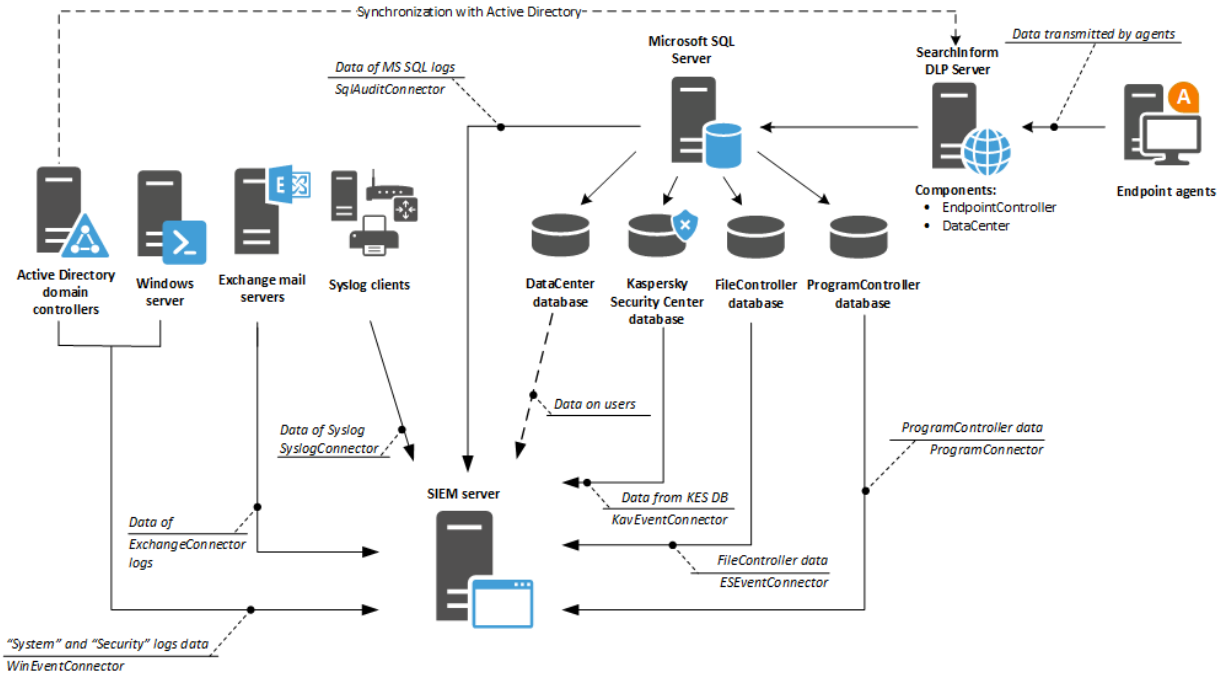
3. Correlation and processing based on rules

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 SIEM server reads the System and Security logs of domain controllers and Windows servers, Exchange mail servers, Kasperky Security Center and MS SQL databases, FileController and ProgramController databases, as well as Syslog events. The SIEM server analyzes 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 specified information security officer.
- The SearchInform 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 SIEM was designed based on requests of our largest clients from different industries.

- **Ready to work 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 products are less demanding in terms of hardware and software requirements.

- **Integrated with SearchInform DLP**

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

System Requirements

	Minimum system requirements (for just the out-of-box set of rules, 1 domain controller)
CPU	2.1 GHz 4-core
RAM	4 GB[2]
Hard drive	from 200 GB[3]
Network card	100 Mbit/s

[2] Custom rule creation requires higher RAM (~15 MB for each new rule).
[3] As events are saved to SIEM database, additional disk space might be required.

Predefined Policies of SearchInform SIEM *

Preset polices for Active Directory domain controller:

- 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.
- 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.
- Granting mail access.
- Owner of mail box was changed.
- Groups of management roles were changed.
- Access to mail box by another user.

Preset policies for user activity:

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

Preset policies 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.
- Other events.
- SearchInfrom DLP events.

* The information is relevant for SIEM 1.5.0.6 released on 30.03.2017.