SIEM
SEARCHINFORM

SEARCHINFORM EVENT MANAGER

Monitoring and correlating information security events

www.searchinform.com

SEARCHINFORM
INFORMATION SECURITY

1995
entered the IT market

Moscow, Russia
head office

17 offices
worldwide

2000+
clients

1 200 000+
computers protected by SearchInform DLP

2006
released SearchInform Data Leak Prevention system

2010
opened own Training Center

2011
held the first series of the Road Show SearchInform conferences

2014
released TimeInformer - a work time efficiency monitoring solution

2015
earned the resident status in Skolkovo Innovation Center

2016
released SearchInform Event Manager (SIEM)

2017
SearchInform DLP made it to Gartner Magic Quadrant for Enterprise Data Loss Prevention

© 2018 SearchInform LTD

CHALLENGE

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

Most of those systems are sources of valuable data – the object of intense interest for various violators, that's why such systems require exceptional protection.

The company can be endangered both by actions of system administrators (unauthorised assignment of access rights, creation or removal of accounts, disablement of firewall) and by vulnerability of hardware and software through which violators can get access to data.

Any system event is logged (protocoled). But it is impossible to manually track, analyse, and react timely to all events.

SOLUTION

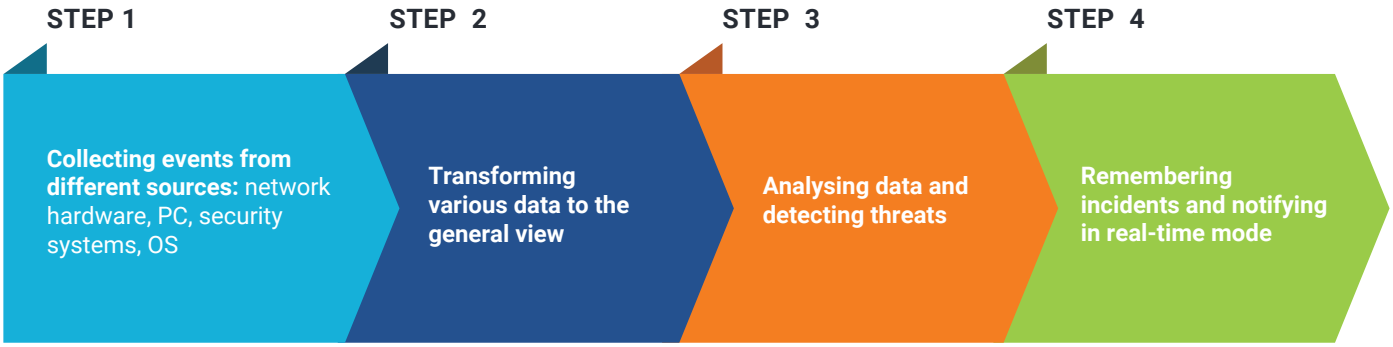
SearchInform Event Manager or SIEM is a system designed for collecting and analysing security events in real-time mode, detecting information security incidents, and reacting to them.

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

SIEM REVEALS:

- Virus epidemics and separate infections
- Attempts to get unauthorised access to sensitive information
- Errors and failures in the information systems operation
- Critical events in the security systems

HOW DOES THE SYSTEM WORK?



It is important to note that SIEM carries out complex audit and detects threats by a complex of events that separately may seem as a non-threat.

CHALLENGES OF MODERN SIEMS

Taking into account all advantages of modern SIEM systems, majority of solutions have the same disadvantages:

1. **Complexity of implementation**

   Vendors and integrators claim the implementation time to be from several months to a year. It will take 5-6 months of system operation in full force to get the first results.

2. **Complexity of operation**

   Most SIEM systems require involvement of highly experienced experts who can write reaction rules, customise sources of events, correct correlation rules, etc. As a result, a company not only pays for the software but also pays a significant amount of money to technical support staff.

3. **Complexity of integration with existing IT infrastructure**

   SIEM system is to be flexible in the integration with existing IT infrastructure, collect and analyse data from various hardware and software. Not every SIEM is capable of that. Besides, vendor must be able to develop a separate connector according to individual needs of a customer. Not every vendor can offer that.

4. **High price**

   Some products are so expensive that they are affordable for only very few companies. Moreover, the price includes purchase and services (technical support, customisation services). As a result, only large corporations with millions of dollars of annual turnover can afford a SIEM system.

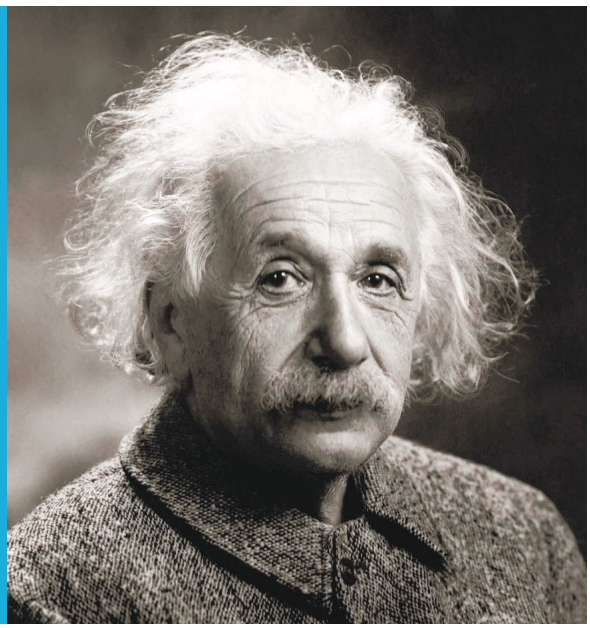
The solution to those challenges is SearchInform Event Manager!

SEARCHINFORM EVENT MANAGER SOLVES PRACTICAL TASKS OF BUSINESS

SearchInform Event Management solution is not just another regular SIEM system that goes down the road paved by other vendors. We see problems and act in the client's environment and do not make simple things look complicated.

SIEM is a software that solves security tasks. This means that any information security expert should be able to easily customise the system, operate it, and timely react to incidents. SearchInform Event Manager does not require programming skills and offers ready-made scripts and event correlation rules.

> *— If you can't explain it simply, you don't understand it well enough.*
>
> *Albert Einstein*



One of the key advantages of the program is simplicity of implementation and possibility of operation right out of the box. The system is supplied with a set of prepared policies and considers experience and tasks of companies from various business and economic spheres.

The principle of the system operation: selecting practical tasks and solving them with SIEM. We have gathered opinions, practices, and needs of SearchInform clients and generated the policies. The system will be developed in the same way: when there are new data sources supported, a client will get a bunch of preset rules.

SIEM can analyse data from many sources. Nevertheless, there are solutions that are employed in the majority of companies, for example, Active Directory, antiviruses, DBMS, mail servers, file storages. They are supported first and foremost.

CASES

PASSWORD GUESSING

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

USER LOGON UNDER SERVICE ACCOUNT

When you use SQL Server, domain account with full access rights to all data bases is created. SIEM notifies if a user logged on with the help of service login and password for SQL Server because there is a great probability of stealing sensitive information from these databases.

UNAUTHORISED 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.

CORRELATION OF UNCONNECTED DATA

There are situations when events, seemingly harmless, all together can pose a great threat. For example, when someone sends the password of a top manager's account. By itself this event will not attract attention, but if further this account accesses critical resources, the system will record the incident.

"GHOST EMPLOYEES" IN THE COMPANY

IT experts can weaken protection of corporate network by being inactive. SIEM will recognise when and if an administrator does not delete accounts of retired employees. For example, a former manager was using login and password to view commercial documents on the network disk. Upon next authorisation, SIEM notices the action on the employee's PC and notifies security department.

AD ACCOUNTS: UNLOCKING, CHANGE OF NAME, 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 notify if it detects such incidents.

Examples of preset policies of SearchInform Event Manager

FOR MAIL SERVERS

- Access to email by a non-owner
- Change of email owner
- Granting access to email
- Audit policy change
- Change of critical roles

FOR FILE OPERATIONS

- Access to critical resources
- Temporary assignment of file access rights
- Temporary assignment of folder access rights
- Large number of users working with a file
- Operation with specific file types

FOR DBMS

- Change of password by a DB admin
- Temporary addition of a login to the role
- Temporary creation of a login
- Temporary assignment of access to a DB object
- Temporary enablement of a login
- Temporary change of the name of a login

FOR ACTIVE DIRECTORY DOMAIN CONTROLLERS

- Temporary account renaming
- Password guessing and obsolete passwords
- Temporary account enablement/addition
- Control of obsolete AD accounts
- Temporary assignment of AD access rights
- One account on multiple computers

FOR SYSLOG

- Custom Syslog rules
- Kernel events
- User-level events
- Mail systems events
- System daemons events
- Security and authorization events
- Internal Syslog events

FOR LINUX SERVERS AND WORKSTATIONS

- Logon of an unknown user
- Logon with elevated rights
- Change of logon GUI
- Logon failure
- SSH logon/logout events
- Starting/stopping session
- Failed attempts of SSH access

USER ACTIVITY

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

FOR CONNECTED DEVICES

- Copying to a removable device
- Copying too many files to a removable device
- Operations with executables on devices
- File execution from removable device
- Copying big volume of data to a removable device

FOR CISCO

- Logon/logout events
- Logon under built-in account
- Logon with elevated rights
- Errors operating the system
- Power errors
- Failure of cooling system
- DHCP errors
- Routing errors
- Double router ID is detected
- WiFi authorization failure

FOR VIRTUALISATION ENVIRONMENTS

- VWview logon/logout events
- VWware start/stop events
- Wrong passwords
- Failed logon attempts
- Creation of user groups
- Change of user password
- Creation/deletion of users
- Deletion of snapshots

FOR ANTIVIRUSES

- Self-protection of antivirus is off
- Virus detected
- Epidemics is detected
- Network attack detected
- Critical status of a computer
- Administration task was not fulfilled
- No license for antivirus
- Potential malware

And 100+ policies that are used in various combinations. The list of connectors and rules is continuously extended.

SearchInform DLP sends SIEM all most important events for prompt response: policies violations and technical statuses of components.

Advantages of SearchInform Event Manager

EASY IMPLEMENTATION

SearchInform Event Manager does not require any preconfiguration. Preset security policies are based on a set of typical tasks that SearchInform clients solve on a regular basis. SIEM provides first analytical results right out of the box.

EASY OPERATION

SIEM operation does not require any programming skills. Any user will manage to set up user configuration. The solution is supplied with a set of ready-made rules which removes the necessity to create scripts, develop event correlation rules.

FOR MEDIUM AND SMALL SIZED BUSINESS

SIEM has low hardware/software requirements and reasonable price policy even for small sized business. The solution is implemented quickly and requires minimum customization.

CONDITIONS FOR COMPREHENSIVE INCIDNET MANAGEMENT

SIEM permanently accesses event sources and processes new events even before entering the system. Thus security experts have time to quickly and effectively react to threats and manage related risks.

EXPERIENCE OF MANY CLIENTS

We have studied experience of our largest client companies, and systemized general demands and best practices in order to employ them in SearchInform Event Manager.

SYMBIOSIS OF SIEM AND DLP

Simultaneous operation of SearchInform Event Manager and SearchInform Data Loss Prevention significantly strengthens company's information security. SIEM detects abnormal behavior and shows how access to information was gained. The combination of the two systems enables investigating any incident properly and collecting evidence base.

CONTACTS

BELARUS
Phone: +375 29 649 77 79
E-mail: ab@searchinform.ru

BENELUX
Phone: +31 6 44 78 62 93
E-mail: benelux@searchinform.com

BRAZIL
Phones: + 55 11 43 80 19 13
+ 55 11 98973 2037
E-mail: v.prestes@searchinform.com

EMEA
Phone: +44 0 20 7043 7152
E-mail: sy@searchinform.com

KAZAKHSTAN
Phones: +7 727 222 17 95
+7 495 721 84 06, ext. 137
E-mail: d.stelchenko@searchinform.ru

LATAM
Phones: +54 11 5984 2618
+54 911 5158 8557
E-mail: r.martinez@searchinform.com

RUSSIA
Phones: +7 495 721 84 06
+7 499 703 04 57
E-mail: info@searchinform.ru

UK
Phone: +44 0 20 3808 4340
E-mail: uk@searchinform.com