OTUS

Security Information & Event Management

OTUS SIEM

OTUS SIEM is a management system for storing server, application, and network information on a centralized location. OTUS SIEM offers a fast and organized way to access, analyze, and act on your network data. Data analysis, intruder detection, and custom report are some of the many features that are available.

Data search

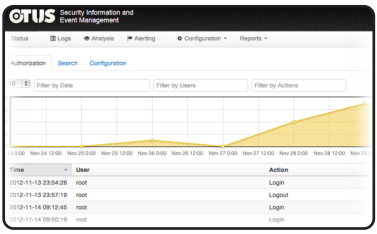
OTUS SIEM offers two search methods. Simple data search makes your original raw data searchable with regular expressions or by an exact string. SQL data search operates on indexed data, which is searchable by creating an easy-to-build SQL-like criteria. By combining the two search methods, it is possible to create rich multiple criteria, allowing you to get the most out of your data.

Why use otus SIEM?

OTUS SIEM makes data analysis and configuration a simple task. Thanks to the auto-detection feature configuration is as simple as pointing a data source to an OTUS SIEM node. Being based on a distributed architecture allows OTUS SIEM to be easily scalable for the smallest to the largest organizations. The indexing feature transforms your raw data into complex data structures, which allows for easier search, analysis, alerting... A dedicated team and almost half a decade of development offers you with a solution that is au-pair with top SIEM products.

Data transformation

OTUS SIEM offers fast and simple access to relevant data. Once the raw data enters the system, an indexer analyzes it, extracts its important components, and stores it in a table form. This allows for a more concentrated search with more meaningful results. OTUS SIEM provides more than 70 integrated indexers from various software and hardware vendors.



OTUS Security Information and Event Management

Data collection

OTUS SIEM collects data with two different fetch methods. The Push fetch method is based on the remote hosts sending data directly to an OTUS SIEM node, with an integrated syslog/snmp/slow tool. Such data sources can be auto detected and configured with the click of a button. The Pull fetch method uses an ssh/ftp/http client to periodically gather data from remote hosts. This fetch methods allows gathering of data from any custom/unsupported system (eg. security card readers).

Security alerting

OTUS SIEM analyzes the collected data in real time, looking for signs of various attacks and other malicious behavior. If such activity is identified an appropriate alert is raised, and a system administrator is promptly notified. Correlated alert rules allow the system to join many single events into a major event, so that the system identifies the root cause of a problem. This leads to a more meaningful and precise notifications to the system administrator. OTUS SIEM comes with many predefined rules to make your systems more secure and threat aware.

Distributed architecture

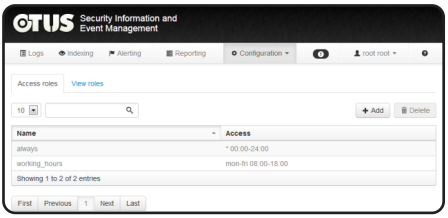
The OTUS SIEM system is based on a distributed architecture, consisting of one or more worker nodes. If an organization requires a higher data throughput, higher EPS (events per second), or more intensive data indexing, additional worker nodes can be added to the system. The architecture is automatically reconfigured resulting in a fast and reliable system. Being based on a distributed architecture allows OTUS SIEM to be easily scalable for the smallest to the largest organizations.

Graphic and tabular reports

OTUS SIEM provides multiple views on the collected data, including graphical and tabular reports. Reports are generated for a specific time interval, eg. last 6 months, last week... The generated reports can be exported in XLS, PDF, and other common formats. A graphic report gives a visual presentation of any measurable parameters (eg. number of security threats per server). A tabular report shows more detailed information about the measurable data (eg. overview of invalid logins per network element). OTUS SIEM comes with a wide range of predefined generic reports, but also provides a way of creating custom reports with the help of a wizard.

Role based access

By using role based access (RBAC) a system administrator can create flexible roles which restrict other users usage of the system. Limiting by data gives users the right to view only part of the stored data (eg: only on a particular server, only on a particular date range...). Limiting by module restricts users from using a particular system component (eg: configuration, indexing, alerting...)



Otus modules

Data retention

A base module that provides a data search. Data can be searched by a plain string, regular expression, data type, and server. Indexed data is searchable by creating an easy-to-build SQL-like criteria. By combining the two search methods, it is possible to create rich multiple criteria, allowing you to get the most out of your data. Similar search results are aggregated into a single entry giving the user a better overview of the results.

OTUS Security Information and Event Management

Configuration

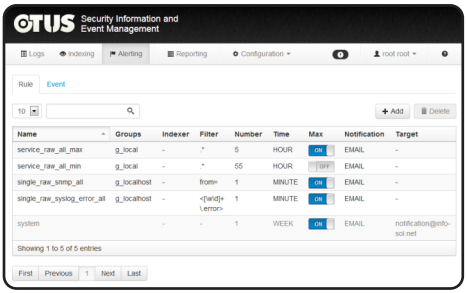
A base module that provides simple configuration for all licensed modules. Thanks to the auto-detection feature configuration is as simple as pointing a data source to an OTUS SIEM node. The system automatically detects the time format used by a particular data source when it first enters the system.

Indexer

A module that analyzes the raw data once it enters the system, extracts its important components, and stores it in a table form. This allows for a more complex and meaningful search of the data. OTUS SIEM provides more than 70 integrated indexers from various software and hardware vendors. The user also has the ability to create custom indexers by using a simple configuration format.

Alerting module

A module that looks for threats and malicious behaviour in your network. By comparing events in your network with a predefined database of known attacks, OTUS SIEM generates alerts as these events are occurring in real time. System administrators are notified about alerts through email, syslog, or snmp.



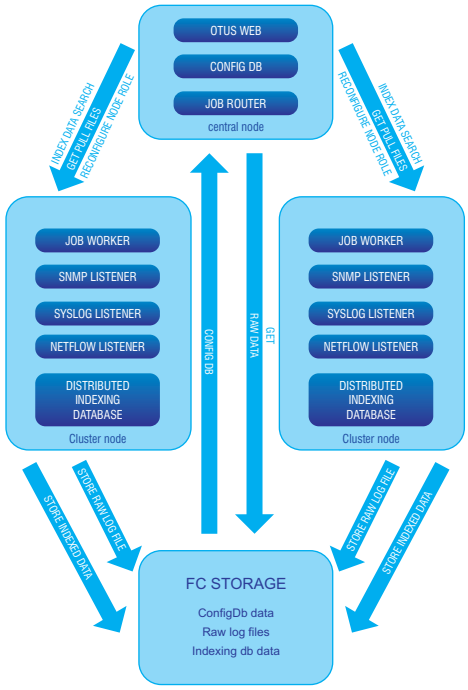
User

A module for managing users and roles. Users can be authenticated from an internal database or by connecting to an Active Directory. User are authorized by their assigned roles, which can limit the users usage in a variety of ways: viewing data only on a certain group of servers, viewing data only on a certain date range, access time to the system, configuration level …

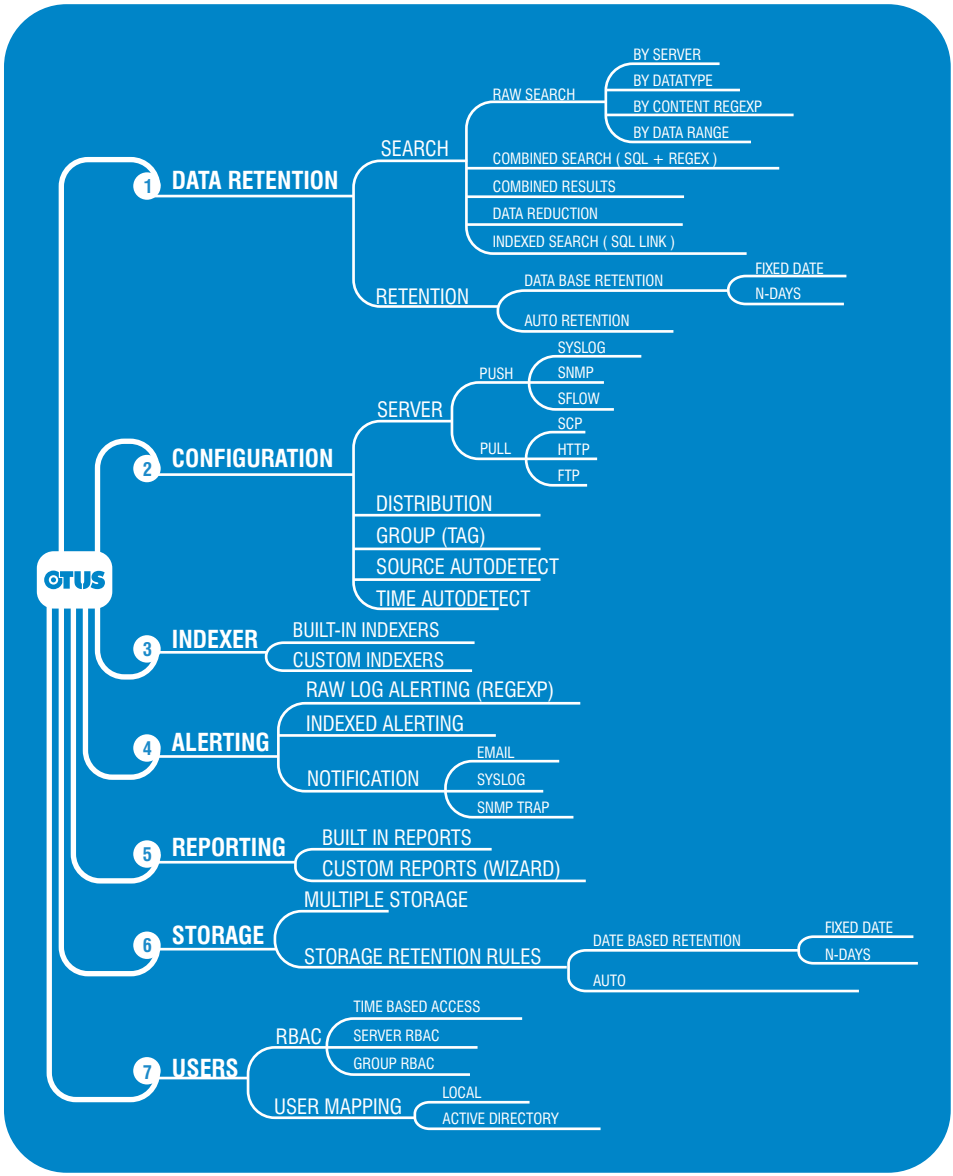
Storage module

A module for managing storage node rules. By creating multiple storage node rules a system administrator can define what data is saved on which storage node. In addition to this a storage node rules defines for how long this data must be kept in the system. Multiple storage modes can be defined: keeping only the last n days of data, keeping data over a fixed date range, or clearing the oldest data when maximum storage space is reached.

Otus architecture



OTUS Security Information and Event Management



Croatia

Infosol d.o.o.
Taborska 31
Zagreb, Croatia

sales@info-sol.net
www.info-sol.net

International

BitSteer technologies
hello@bitsteer.com

www.bitsteer.com
www.youtube.com/user/bitsteer