

# Defensys Security Information and Event Management

Centralized cyber security event management






Defensys




**Defensys Security information and Event management (SIEM)** is the main component for creation of cyber security centers. It provides centralized event flow management from all informational systems, helps to timely identify incidents and preserves business integrity.

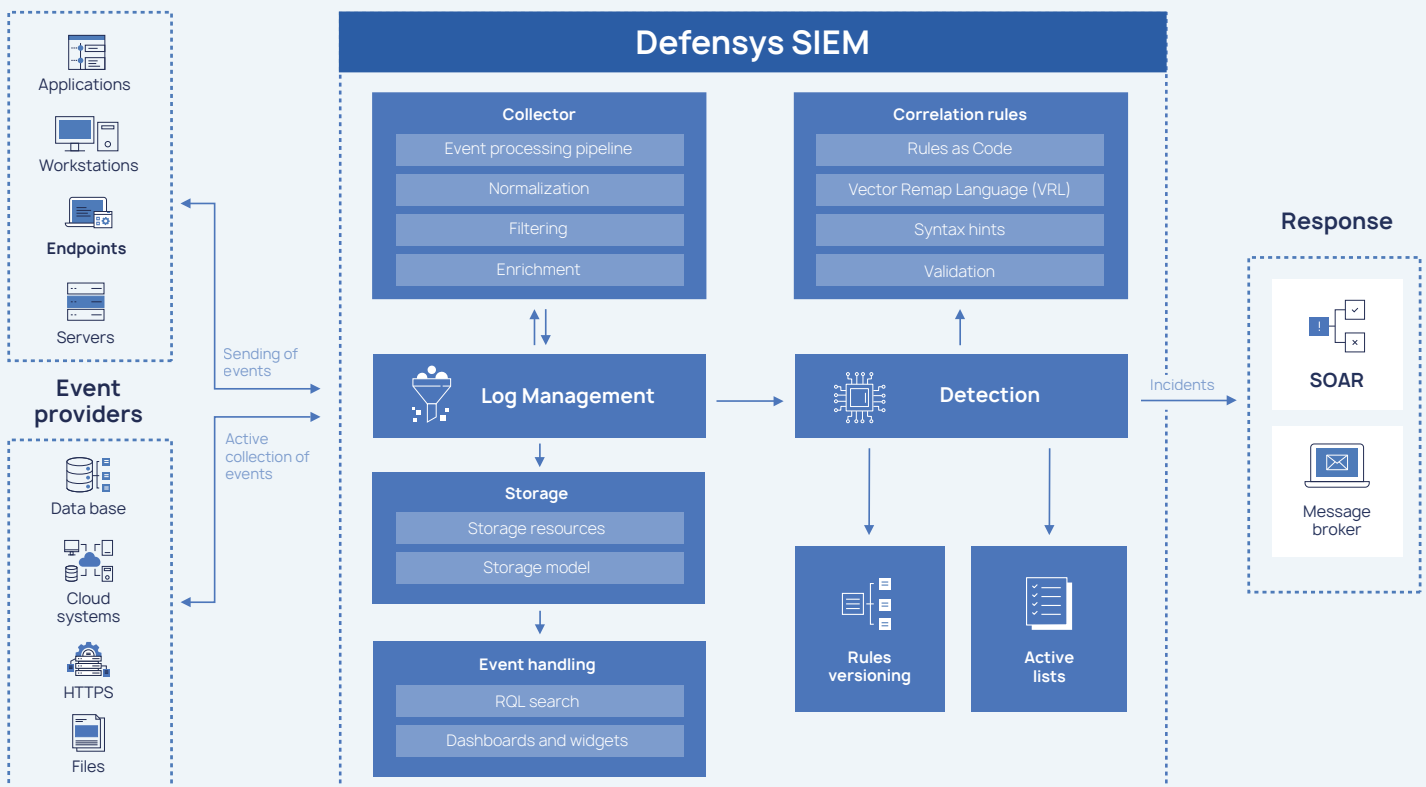
The Defensys SIEM implements a comprehensive approach to event processing that covers all stages of data handling, while helping to optimize company resources.

## Tasks







-  To build an incident detection center
-  To collect and store unique organization's data
-  To reduce the time for connection to new event sources

## Solutions

-  Advanced event collection and correlation rules help to detect incidents in a timely manner
-  Flexible customization of event processing pipelines and event models ensure collection of necessary data
-  Built-in templates and a large list of connectors make possible a quick connection to any event source



## Advantages of the Defensys SIEM

-  **Timely threat detection** through real-time event processing and incident detection
-  **Identification of severe incidents** with advanced correlation rules
-  **Visualization tools for data flow management**
-  **Rational use of resources** through flexible storage settings
-  **Collection of necessary events** using customized data models
-  **Easy scaling** due to architectural features



### Any sources for event collection

Defensys SIEM collects data using an event processing pipeline, which helps to define sources for data collection and connection parameters in a convenient format.

To connect event sources either pre-installed connector templates or users' own templates can be used and afterwards replicated in the Defensys SIEM.



### Single event management center

For the further processing of collected data a graphical constructor has been developed, it allows centralized customization for:

- Reception
- Normalization
- Enrichment
- Events filtering and sending to repositories or to the system for further analysis



### Full-function correlation rules

Properly written correlation rules can detect a wide range of incidents.

Detection rules of the Defensys SIEM represent the concept of "detection as code" with no limitations in logic to detect incidents of different types.

Hints and testing available from the interface help to optimize the process of detection rules preparation. Subsequently, versioning allows users to monitor the state of the created content.



### Flexible storage

To accommodate important events and nonstandard storage needs the Defensys SIEM offers:

Universal data model, that contains a large number of preconfigured fields

A tool for creating custom event models that can be extended without affecting the stored data

Functionality for flexible field customization in the user's event models

The storage metrics system allows users to track storage and database load, set time intervals for different types of storage, and optimize the use of hardware resources.



### Quick events search

The search tool helps to analyze large volumes of collected data:

- When accessing events, users can create queries of any level of complexity using mathematical and logical conditions
- Multi-level filtering of search results, flexible management of filter settings and the ability to add values to filters directly from the event are available to generate a more accurate selection
- Event field statistics helps to identify the most frequently occurring values
- All created queries can be saved, which minimizes the labor costs for analysts when working with data

## Comprehensive protection with the Defensys technologies

Collection	Enrichment			Response
<b>Endpoints</b> <ul style="list-style-type: none"> <li>✓ Events</li> <li>✓ Telemetry</li> </ul>	<b>TDP</b> <ul style="list-style-type: none"> <li>✓ Data from traps and lures</li> <li>✓ Lures identifiers</li> </ul>	<b>UEBA</b> <ul style="list-style-type: none"> <li>✓ Objects' behavior</li> <li>✓ Anomalies</li> </ul>	<b>TIP</b> <ul style="list-style-type: none"> <li>✓ Indicators of compromise (IoC's)</li> </ul>	<b>SOAR</b> <ul style="list-style-type: none"> <li>✓ Incident prevention</li> </ul>



## About Defensys

Defensys is an award-bearing and nationally acknowledged vendor of cybersecurity solutions. Since 2011, we have been fostering government agencies and private-sector companies to confidently withstand modern cyber threats and ensure reliable security management worldwide.

Defensys technologies are embedded in financial, public, oil and gas, energy, metal industry, and other sectors.

✉ [sales@defensys.com](mailto:sales@defensys.com)

⊕ Cybersecurity Digest:  
[defensys.com/blog/](https://defensys.com/blog/)

