Defensys SOAR

Cybersecurity automation platform for incident monitoring and response

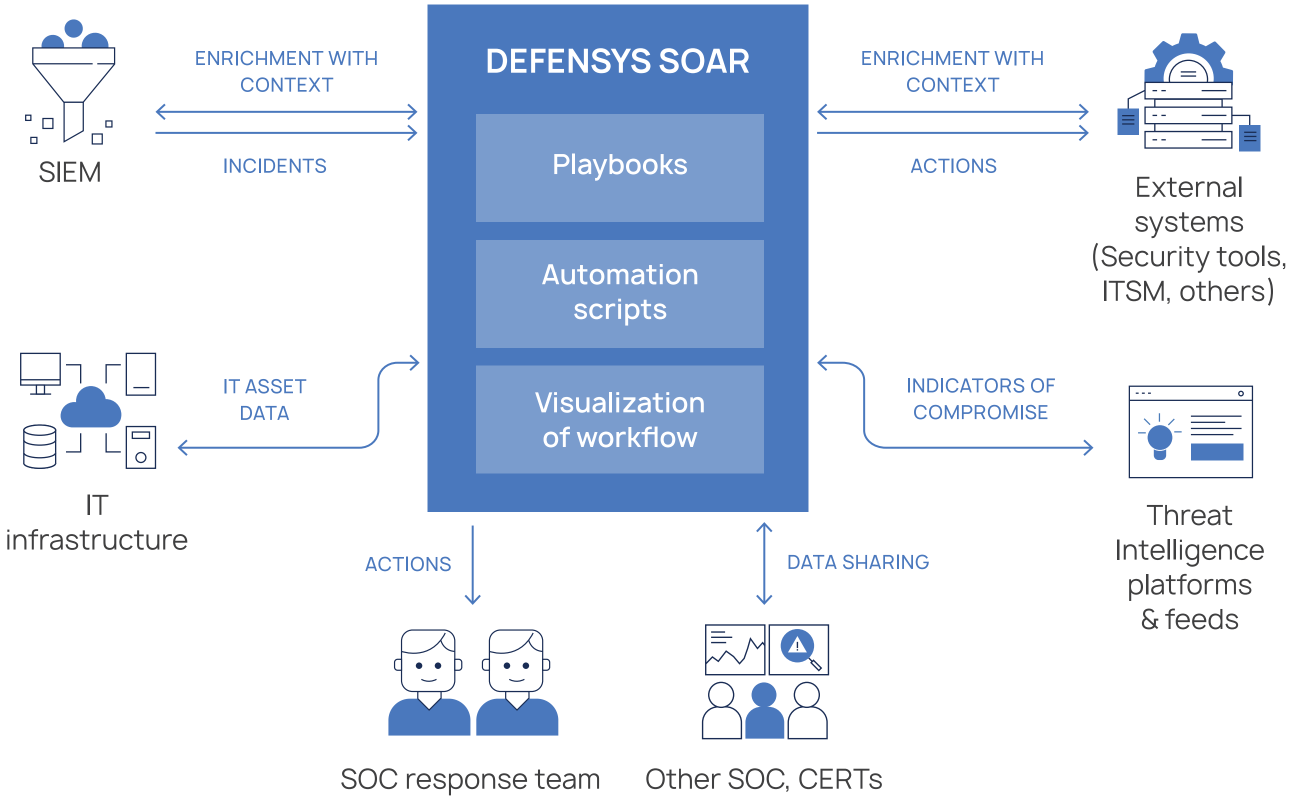
Defensys

Defensys SOAR is a modern incident response platform with the following essential features:

- ✓ Collecting incident data from different sources.
- ✓ Enriching incident data with maximal additional context.
- ✓ Automating routine incident processing and response playbooks.
- ✓ Coordinating SOC teams and members.

SOAR helps your business strengthen cybersecurity resiliency and quickly respond to the most sophisticated transforming threats.

Defensys SOAR functions as a single work console for SOC analysts



SOC analysts benefits

- Significantly reducing the time spent on cyberincident response routine
- Working in a single interface with tracking the cybersecurity status of the infrastructure
- Increasing SOC team efficiency and resiliency
- Automating incident processing routine tasks
- Building efficient interaction between the cybersecurity and IT departments

CISO benefits

- Monitoring of IT infrastructure and its security level
- Automating incident and vulnerability management processes
- Risk mitigation
- Comprehensive risk exposure data, reports and metrics for decision making

Key Features

Collecting data on all incidents in a single response console.

Automating incident response process by running pre-set algorithms and playbooks; ability to adapt the response playbook to meet your company's real-time needs; processing incidents full cycle.

Managing response team and processes, assigning roles, coordinating actions, notification, escalation, planning and control of tasks in a single workspace.

IT assets inventorying and control, vulnerability management, software monitoring; detecting unauthorized software, devices, and external connections; consolidation of infrastructure security statuses.

Multitenancy mode in a single installation: spreading the action of response playbooks and connectors, getting feedback; multiple response playbooks runs.

Integration with SIEM, NGFW, IPS/IDS, vulnerability scanners, antivirus software, DLP, TI services, ITSM/Service Desk, databases and many other sources via universal connectors.

Interaction with any external systems via Connector constructor, obtaining data on incidents and assets.

Orchestration of connected systems, coordinating their interaction within a response playbook, managing the playbooks launch and incident processing.

Information **visualization** on different representation levels, pre-defined set of response metrics, templates and chart builder, pre-installed reports set and report builder, automatic and scheduled reports generation and distribution, export to different formats.

System Benefits

- Flexible adaption to the current IT infrastructure and processes
- Unique integration mechanisms
- Ready-to-use automation scripts
- Incidents prioritization by criticality level
- Dynamic response playbooks and user-friendly graphic editor
- Multitenancy mode

Defensys

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

Cybersecurity Digest:
defensys.com/blog/