esecure | SECURE VISIO

## SOAR

Automation of incident management and response

## NextGen SIEM

Detection of security incidents and threats

# One platform to detect and manage incidents, vulnerabillities and risks

## SecureVisio SOAR

is a specialized Security Orchestration, Automation and Response solution for automating management and response to incidents and improving other security management processes.

**Features and benefits of the solution:**

- Organized work of people - the process of incident management (Workflow) takes place in stages, in accordance with applicable standards (including ISO/IEC 27035)
- Unification of tools - one graphic console contains all the tools and information needed to explain and handle incidents
- Automating people's work - ready-to-use incident scenarios (Playbooks) for many types of incidents
- Integration of tools and data sources - Playbooks automatically launch tools and acquire data from external sources (including Threat Intelligence)
- Business prioritization - incidents are automatically prioritized in relation to the importance for the organization (i.e. supported processes, sensitive information)
- Awareness of business impact of incidents - the incident handling process is carried out with risk awareness (ISO/IEC 27005) and business consequences of security breaches
- Unified vulnerability management - cooperation with Vulnerability Assessment and CVE tools as well as integrated Workflow and Playbook tools for vulnerability management
- Simulation and visualization of threats - analysis of incidents and vulnerabilities is supported by graphical tools simulating attacks and other threats
- Performance metrics with business context - the tools calculate KPIs (key performance indicators) and KRIs (key risk indicators)

## SecureVisio NextGen SIEM

is a new generation Security Information and Event Management solution designed to meet modern security requirements enabling rapid detection of incidents and other threats.

**Features and benefits of the solution:**

- Many detection methods - SIEM correlation rules, behavioral analysis of users and systems (UEBA), Threat Intelligence
- Dynamic SIEM rules - event correlation rules automatically adapt to network and system changes detected using the Auto-Discovery function
- Business context - log analysis in SIEM takes place in the context of the current risk for organizational processes and sensitive information
- Wide scope of analysis - SIEM analyzes security events (logs), current vulnerabilities, Threat Intelligence information and estimated risks
- Event repository - a specialized database for long-term storage and quick search of security events
- Many methods of reading logs - Syslog, e-mail, Windows Event Forwarding, as well as the ability to read logs from databases and flat files
- Graphic parser editor - the predefined set of parsers can be extended with new parsers created with the help of the graphic editor
- Cost effectiveness - licensing is based on the actual number of monitored IT resources with no restrictions on the size of the data analyzed