Real Time GRC

Digital IT documentation

‘Out-of-the-box’ security expert

Security breach simulation

IT Security translator for business

Vulnerability assessment for business

SOC automation

Adaptive scenarios of incident handling

www.esecure.pl
Which challenges of enterprise security does SecureVisio™ help to overcome

The amount of information present in the area of enterprise security makes risk management very difficult. Companies have limited resources for these tasks and often there is not enough knowledge in order to correlate emerging risks with their impact on business processes. The law acts and official recommendations provide proper guidelines, however it is not an easy matter to implement them in an organization with years of established business practices and processes. This is why in 2010 a number of highly experienced security experts with international practice started to develop a solution that would address these needs. This is how SecureVisio™ came to be.

SecureVisio™ is a modern Real Time GRC solution targeted at organizations of all sizes that allows to automate a large number of complex and time-consuming processes of security management. Making use of our product allows for far better effectiveness in security management and allows to easily meet the law requirements and various security standards (i.e. KNF, PCI-DSS, RODO).

Real Time GRC
(Governance, Risk Management, Compliance)

SecureVisio™ provides real time information by processing alarms received from security products and SIEM systems and automatically analyzing them in relation to both technical and business contexts. Our system is fitted with a security rule editor which can provide a simulation of consequences of potential security breaches (BIA), allows for automatic risk analysis and can correlate any technical parameters with business ones. When an event occurring in a network matches a defined rule the system creates a new security incident or updates an existing one, marks it with appropriate severity and informs appropriate staff members about the event.

Figure 1. SecureVisio™ – Security rule editor
**Digital IT documentation**

The main component of SecureVisio™ is an interactive, digital documentation of the network, IT systems and security devices, fitted with graphical tools for editing, searching and analysis of data important for the security of our organization. The Asset Discovery feature allows for automated detection, recognition and documentation of enterprise’s IT systems.

Figure 2. SecureVisio™ – logical topology map view

**‘Out-of-the-box’ security expert**

The solution helps the user in making decisions in relation to security monitoring and management. This is possible thanks to an expert’s knowledge base implemented in the system that can act as a team of experts from various areas of IT security. This feature provides information about the effectiveness of implemented host and network security measures in preventing different kinds of attacks and breaches. It also provides a lot of other information, important for security management.

**Security breach simulation**

The system implements a functionality of risk simulation that allows to audit security in relation to both discovered and potential attack vectors. This makes it possible to visualize and analyze security vulnerabilities and to present risks and potential consequences of security breaches from the perspective on any single resource.

**IT Security translator for business**

A solution that helps to avoid communication errors while handling security incidents as well as during day-to-day IT tasks.
Vulnerability assessment for business

SecureVisio™ has the capability to identify security vulnerabilities in the IT systems thanks to integration with CVE® database, as well as integration with vulnerability scanners for which it can create and run scanning schedules. Our system automatically analyzes the business importance of IT systems as well as technical information relating to risks (CVSS) thus calculating the priorities for the vulnerable systems.

![Figure 3. SecureVisio™ – List of vulnerabilities](image)

**SOC automation**

SecureVisio™ is always actively monitoring logs and helps with coordinating SOC responses by providing scenarios for handling of security incidents. The integration and correlation of information from SIEM, security systems, vulnerability scanners and CVE database allows for automation of many SOC tasks, thus increasing effectiveness of operations and decreasing the risk of security incidents.

**Adaptive scenarios of incident handling**

SecureVisio™ manages scenarios of security vulnerabilities and security incidents handling. The scenario is run when predefined conditions are met and are build based on a context workflow. As part of security incident handling scenario the users have a number of predefined actions to choose from, such as modification of documentation, sending notifications to staff, change of operator handling the incident, execution of a script or assigning various tasks to users.

**TYPICAL IMPLEMENTATION TIME IS 1 – 3 MONTHS**

**RETURN OF INVESTMENT IN 3 – 6 MONTHS**

**THE BEST SUPPORT – NEW SYSTEM RELEASES AS PART OF SUPPORT PACKAGE**

**EFFECTS VISIBLE ON THE FIRST DAY AFTER THE IMPLEMENTATION**

**COMPETITIVE PRICING ADEQUATE TO THE SIZE OF THE ENTERPRISE AND IMPLEMENTATION COMPLEXITY**

www.esecure.pl