

SecureVisio™ Technical Specification

Modern IT Governance, Risk management, and Compliance (GRC) solution equipped with an electronic documentation of IT systems, as well as integrated Incident Management, Threat Modelling, Security Auditing and Business Impact Analysis tools. SecureVisio™ can act as an independent IT GRC solution in an organization or as an intelligent platform to build a Security Operations Center (SOC).



Main components:

- Electronic documentation of IT systems
- Knowledgebase of IT security experts
- Threat modeling tools
- Security auditing tools
- Automated risk assessment tools
- Business Impact Analysis tools
- Failure simulation tools
- Journal of security incidents
- SIEM and network safeguards integration module
- Vulnerability Assessment integration module
- CVE® database integration module
- Reporting and alerting module

Electronic documentation of IT systems

- IT GRC Setup Wizard
- Technical and business parameters
- Graphical tools for documentation editing and searching
- Automatic detection of IT systems (System Discovery)
- Logical architecture of IT security (security devices and zones, layers of protection)
- Diagrams of physical network (connections, switches, routers, etc.)
- Attaching external documents
- Defining custom parameters
- Users and roles management

Knowledgebase of IT security experts

- Best practices for security design
- Best practices for security auditing
- Effectiveness matrix of network safeguards
- Effectiveness matrix of local safeguards
- Methodology of risk assessment

Threat modeling tools

- Determine threat sources of an IT system
- Show IT system's protections against potential threat sources
- Show the most exposed IT systems
- Show location of particular data category
- Show scope and consequences of a security incident
- Show network areas outside the organization
- Show protections against specific threat source
- Show location of particular system type
- Show systems with particular local safeguards
- Show security management tools for security devices
- Show security management tools for important IT systems

Automated risk assessment tools

- Focused on IT systems of critical importance to the organization
- Map IT systems to business processes
- Importance of business processes
- Algorithm of business risk analysis
- Summary table of risks of all major IT systems

Business Impact Analysis tools

- Automatic estimation of legal and business consequences of an incident
- Automatic estimation of IT systems' value for the organization
- Threats specific to IT systems

Security Audit tools

- Show exposed IT systems of critical business importance
- Show important IT systems vulnerable to failures
- Show IT systems of high risk level
- IT systems risk analysis for specific threats
- Built-in security audit templates (e.g. PCI-DSS)
- Custom security requirements wizard: network safeguards requirements, local safeguards requirements, security management tools requirements

Vulnerability Assessment integration module

- Import and analysis of vulnerability scanners' reports (including Nessus™, Rapid7 Nexpose™)
- Selection of vulnerabilities based on importance to the organization

CVE® database integration module

- Automatic import of new vulnerabilities from CVE database
- CVE compliant specification of important IT systems (OS, software)
- Selection of vulnerabilities based on importance to the organization

Technical specification

- Virtual Appliance – VMware ESX, VMware Player
- GUI: dedicated application installed in Microsoft Windows 7, 8, 8.1 and 10; Web console supported in Microsoft Internet Explorer 9, 10, 11 and Firefox 4x

Failure simulation tools

- Linking physical and logical network elements
- Identification of Single Point of Failure
- Activation/deactivation of network elements and IT systems
- Show disrupted business processes

SIEM and network safeguards integration module

- Logs and alerts analysis of SIEM, firewall, IPS and other safeguards (Syslog)
- Incident identification in IT systems of critical importance to the organization
- Firewall logs selection based on IT systems importance to the organization

Reporting and alerting module

- Critical vulnerabilities report
- Critical incidents report
- Custom reports wizard
- Email notifications
- Interactive calendar
- Export to printable form (PDF)

Journal of security incidents

- Incident registration form (manual description)
- Automatic processing of security alerts (Syslog Universal Parser)

Licensing

- Based on the number of important IT systems and the number of devices on network maps
- License extension - Threat Modeling functions, Security Audit functions

About eSecure:

Private company founded in 2010 as an initiative of the business and IT security experts who understood that an automation of IT security management would be the only way to achieve the organization's safety in dynamically growing, business-driven IT world. eSECURE provides enterprises with the ability to avoid security breaches within IT systems with critical importance to the organization, optimize the costs of IT security development and maintenance, and add intelligence and business context to technical safeguards improving the organization's risk agility and business resilience.

Headquarters

ul. Hoffmanowej 19
35-016 Rzeszów
tel.: +48 17 779 62 46

R&D Office

Aleje Jerozolimskie 162 A
02-342 Warszawa, Poland

www.securevisio.com