SecureVisio™ is a modern IT GRC (Governance, Risk management, Compliance) solution designed for any organization, that allows to automate many complex and time-consuming IT security management processes. In practice, at the highest level it is not possible to maintain the safety of all IT systems in an organization. Effective security strategy assumes that people responsible for the security focus their attention on IT systems of critical importance to the organization. SecureVisio™ understands the technical aspects of security, but also knows the business role of the most important IT systems in the organization.

While managing the organization's security, SecureVisio™ knows which business processes are supported by specific IT systems, how important they are to the organization, how important is the data processed by specific IT systems and thanks to IT security expert knowledge and algorithms of the risk management, SecureVisio™ knows the consequences for the organization that follow a security incident in a particular IT system. Usually this knowledge is spread between many people and dozens of often outdated documents. SecureVisio™ is a single system that maintains the information needed to govern IT security of the organization. The main component of SecureVisio™ is an interactive, electronic documentation of networks, systems, and IT security. SecureVisio™ shows the overall picture of the organization’s IT security in technical as well as business areas, and ensures effective security management of IT systems critical for the organization.

SecureVisio’s™ Setup Wizard helps to quickly gather information about the structure of the organization and in the classification of datasets and business processes that are needed to understand the actual requirements for the safety of the organization and for proper decision-making.

- Automation of key processes of IT security management
- Easy in maintenance electronic IT security documentation
- Avoids security breaches within IT systems with critical importance to the organization
- Optimizes the costs of IT security development and maintenance
- Business resilience by focusing on IT systems supporting critical business processes
Automation of key processes of IT security management

SecureVisio™ unique feature that is integrated with electronic documentation is the Business Impact Analysis function, which automatically estimates the consequences of security breaches for an organization. This function is extremely useful in cost-effective IT security planning, security incidents handling as well as complex projects like Business Continuity and Disaster Recovery.

Holistic approach to IT security management improves the risk agility and business resilience. By using SecureVisio™ it is easier for organizations to adjust their risk management procedures to dynamic changes within IT systems that support the organization’s most important operations as well as to improve reliability and high availability of IT services necessary for critical business processes.

The brain of SecureVisio™ is IT security expert knowledgebase used for automatic threat modeling and security auditing. The expert knowledgebase acts as a team of experts from different areas of security. SecureVisio™ maintains the collected by IT security experts and regularly updated information about different types of IT systems and their susceptibilities to various types of attack vectors, information about different types of network safeguards and their effectiveness in preventing different attack vectors, information about effectiveness of local safeguards and lots of other information relevant to IT security management.

SecureVisio™ provides benefits to any organization, regardless of size and industry. It can be used as a standalone IT GRC solution or be integrated with SIEM and used as a platform for building intelligent Security Operations Center (SOC). For the most important IT systems in the organization, SecureVisio™ stores up to date technical and business related information.

SecureVisio™ helps organizations in achieving cost-effectively compliance with the requirements of law and security standards (including ISO-27001, PCI-DSS). Electronic documentation is equipped with graphical wizard that helps to define the organization’s specific security requirements. The requirements may be related to network safeguards, local safeguards and security management tools. Based on the defined requirements SecureVisio™ conducts automatic compliance assessment of the existing or planned security design. When in use, it is possible to tune SecureVisio™ and define new requirements in accordance with actual needs. For people responsible for safety of the organization SecureVisio™ means more control, easier decisionmaking, reduced stress and acceleration of many time-consuming tasks.
Easy in maintenance electronic IT security documentation

The main component of SecureVisio™ is an interactive, electronic documentation of IT security, equipped with graphical tools for editing, searching and analysis of data relevant to the organization’s safety. Business operations of organizations increasingly depend on the information technology. IT systems support the key business processes by storing and processing confidential data. Disruption of IT security translates directly to disruption of organization’s operations.

We are not able to manage the security of IT systems without complete and timely available documentation. We need information about IT systems that recognizes key processes of the organization, how important is data stored and processed in these systems, and what protections should be provided for them. In many organizations this knowledge is spread between many people and dozens of documents. Lack of knowledge leads to errors in the security planning, errors in the incident handling, and a might result in stressful situations for people responsible for the organization’s security.

SecureVisio™ providers easy-to-maintain electronic documentation of networks, systems and IT protections. Electronic documentation requires only minimum information necessary to manage security of IT systems critical for the organization. Logical security architecture presents data about major network safeguards and their security mechanisms as well as description of security zones and the most important IT systems located in these zones. If necessary, the administrators can add new parameters and links to external documents. IT security expert knowledgebase and risk assessment algorithms, that are integrated with the documentation module, help in making difficult decisions and cost-effective security planning. Documentation of SecureVisio™ describes a logical architecture of IT security and, if necessary, may also contain detailed diagrams of physical networks where the network engineers specify the parameters of the links, switches, routers and other network elements. Asset Discovery toolset provides automatic detection, identification and documentation of IT systems.

With SecureVisio™ people responsible for the organization’s safety have complete IT systems documentation containing technical and business related information in a single system. One of unique features of SecureVisio™ is a built-in documentation module and interactive toolset for threat modeling and security auditing. These mechanisms allow for quick identification of threat sources, automatic analysis of the network paths between IT systems, automatic analysis of existing network, local safeguards and security management tools as well as analysis of critical business processes in scope of Single Point of Failure detection (i.e. determining the network, system and security elements that do not have redundancy).

Electronic documentation can be exported on demand to printable form (PDF). Report Wizard allows to define additional documents with selected aspects of IT and security systems. Using electronic documentation and its tools makes it easier to conduct complex security projects in cost-effective manner, such as DLP and BCP. For example, SecureVisio™ provides tools for flexible classification of datasets and determination of network location of sensitive data (e.g. intellectual property, personally identifiable information, financial data). This significantly speeds up implementation of DLP projects and increases the likelihood of success. Tools that automate the processes of Business Impact Analysis support the implementation of the most difficult stage of BCP project, which is the assessment of an impact of incidents on the business of the organization.

- Electronic documentation equipped with dedicated tools for defining logical IT security architecture and detailed physical network diagrams
- Asset Discovery provides automatic detection, identification and documentation of IT systems
- Graphical tools for editing and searching of security, network and IT system elements as well as the reports wizard
- Cost-effective security development assisted by IT security expert knowledgebase with automatic risk assessment and threat modeling functions
- Agile risk management and cost-effective security development in dynamic IT environments
Avoids security breaches within IT systems with critical importance to the organization

The main problem of vulnerability management is the fact that organizations are not able to remove all vulnerabilities. A realistic security strategy assumes that we should quickly identify and remove vulnerabilities in IT systems critical for the organization to avoid serious consequences. We should focus our attention on the vulnerabilities in the most important IT systems.

Security incidents take place using existing vulnerabilities in IT systems. Every day dozens of new vulnerabilities are detected - in operating systems, applications, databases, software, and mobile devices. When scanning a network of an organization using Vulnerability Assessment tools, we are informed about a very large number of vulnerabilities in IT systems. Often the number of all found vulnerabilities goes to thousands. These vulnerabilities, whose exploitation by criminals or malicious programs can lead to serious consequences for the organization.

SecureVisio™ uses various sources to read the information about new vulnerabilities. Then, based on knowledge about the roles of IT systems in the organization, SecureVisio™ selects and prioritizes the vulnerabilities. People responsible for IT security are only informed about the vulnerabilities whose exploitation could have a high impact on the organization’s business. Thanks to quick identification of the vulnerabilities in the IT systems supporting major business operations and processing sensitive data it is possible to avoid incidents in the IT systems of critical importance for the organization.

In order to identify vulnerabilities, SecureVisio™ connects with Common Vulnerabilities and Exposures™ (CVE™) database and reads the information about newly discovered vulnerabilities of various elements of IT systems. The number of vulnerabilities is high. SecureVisio™ filters the data from CVE database based on their severity to the organization and presents only the vulnerabilities that require urgent consultation with IT staff and business owners.

When an organization uses Vulnerability Assessment tools, it is possible to integrate them with SecureVisio™. A report generated by a vulnerability scanner is analyzed by SecureVisio™ in order to select the most dangerous vulnerabilities in terms of the organization’s operations. This allows organizations to effectively manage vulnerabilities and avoid incidents in the most important IT systems.

IT security expert knowledgebase enables SecureVisio™ to automatically audit the design of network security in scope of the detection of critical business processes that do not have adequate protection. Thanks to this feature, it is possible to focus the attention on IT systems that perform the most important tasks for the organization. Managers making decisions about IT security development have quick and easy access to detailed reports about legal and business consequences of security incidents in different IT systems. The organization’s spending on IT security is justified by legal and business reasons.

SecureVisio™ threat modeling tools enable simulation of various types of failures. For example, we can simulate a failure of a physical server. SecureVisio™ immediately informs us which IT systems are not available as a result of this failure, and which business processes supported by these IT systems are disrupted. Similarly, we can simulate failures of network and security devices, and based on this information easily decide if the risks are acceptable for the organization.

SecureVisio™ allows organizations to automate many complex security management processes, such as: the vulnerability management and mapping of vulnerabilities to IT systems that have critical importance for the organization; automatic assessment of the impact of incidents for the organization; the risk assessment of IT systems and business processes as well as security assessment of planned IT systems changes, and many other complex and time-consuming activities. Thanks to SecureVisio™, the people responsible for safety of the organization always have up to date and complete information and specialized tools that make their work less stressful and reduce errors when making difficult decisions.
Optimizing the costs of IT security development and maintenance

To be cost-effective IT security should be developed based on the results of risk analysis. Main task of IT security is to ensure the continuity of important business processes, protect sensitive data, as well as to achieve compliance with the requirements of law, standards, agreements and other regulations. Lack of knowledge in this area leads to wrong decisions and unjustified spending on IT security.

Integrated with electronic documentation, an automatic risk assessment function estimates and shows the security status of all important IT systems in the organization. The risk assessment method implemented in SecureVisio™ assesses at high accuracy level risks related to all attack vectors used by cyber-criminals. This approach simplifies the risk mitigation process as the security engineers responsible for designing IT security accurately know what attack vectors do not have adequate countermeasures.

SecureVisio™ allows quick determination of Single Point of Failure elements in scope of the IT systems that have critical importance for the organization. For this purpose SecureVisio™ analyzes all network paths from the users’ locations to the locations of servers providing IT services and determines the elements that do not have redundancy. SecureVisio™ tools automate many complex and timeconsuming activities. This enables work-time optimization and stress reduction of people responsible for IT security management.

Security incidents often take place during changes and modernization of IT systems. For example, incidents occur when new IT services are made accessible to the users on the Internet without ensuring adequate security measures. Changes in IT systems often mean huge stress for people responsible for the organization’s safety. SecureVisio™ provides dedicated tools that help organizations in safe and costeffective implementation of IT systems’ changes in regards to the network security architecture. Using the expert knowledgebase SecureVisio™ tools automatically analyze the correctness of new design of the network security architecture and assess compliance of changes with standards and requirements of the organization.

SecureVisio™ reduces risks connected with IT system changes and makes sure that spending for IT security is justified by the organization’s business requirements.
Business resilience trough focus on IT systems supporting critical business processes

Cyber-criminals use more and more sophisticated attack vectors and evasion techniques to bypass the safeguards protecting the most valuable assets of organization. A realistic security strategy assumes that organizations will not be able to avoid all security incidents. People responsible for the organization’s safety should focus on effective detection of incidents in IT systems which play a key role in the organization and should be prepared to quickly restore critical business processes affected by these incidents.

SecureVisio™ adds intelligence and business context to technical safeguards improving the organization’s business resilience. Technical controls (e.g. firewalls, IPS, etc.) and management tools (e.g. SIEM) generate a large number of logs and alarms that indicate occurrence of the security incidents. Thanks to integration with electronic documentation Business Impact Analysis function, SecureVisio™ performs automatic estimation of the consequences of incidents for the organization’s operations.

Technical safeguards inform us about the IP addresses of IT systems which are victims of the incidents. To investigate and properly handle the incidents we also need to know their business context. SecureVisio™ automatically retrieves IP addresses of incident victims and immediately provides necessary information and recommendations - if we should expect legal consequences, whether the organization could lose confidential data, whether the organization’s critical business processes could be disrupted, or if as a result of this incident the organization could suffer reputation damage. Knowledge about the consequences of incidents is absolutely necessary to prepare an appropriate corrective action plan. Automating the process of incident handling is possible through SecureVisio™ integration with SIEM systems and other technical security technologies, e.g. Next-Generation Firewalls, Intrusion Prevention Systems, Anti-Malware Sandboxing, etc. SecureVisio™ is equipped with Syslog Universal Parser, using which it can read logs and alarms from various systems like SIEM and other information sources about IT security incidents.

SecureVisio™ complements the technical information with intelligence and business context. Thanks to SecureVisio™, in a case of an incident we can quickly determine who is the business owner of IT system and who is responsible for its technical administration. This is important in order to conduct quick and correct handling of such incidents. SecureVisio™ can alert the personnel responsible for the incidents handling in real time and provide them with all of the necessary technical and business related information. SecureVisio™ enables organizations to quickly restore continuity of critical business processes affected by incidents.

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, Poland
tel.: +48 17 779 62 46

R&D Office
Aleje Jerozolimskie 162 A
02-342 Warsaw, Poland

www.esecure.pl