secureVISIO

SecureVisio - one platform for incident, vulnerability, and risk detection and management.
The system enables organizations to automate and unify core security management operations in a single, integrated platform. This allows them to optimize the time and cost of security operations.
Security managers can then make better decisions, as they have complete information about incidents, vulnerabilities, and associated risks in one place.

SecureVisio addresses the following areas of the security management process:

1

Situational awareness - inventory, mapping, and visualization of IT assets and processes
Building situational awareness of assets, networks, and processes is one of the most important activities in the security management process, both at the strategic and operational levels. SecureVisio features automated passive and active IT asset inventory and network configuration mapping mechanisms. These mechanisms detect systems, network devices, and applications and automatically determines their type and the relationships between them. They also allow you to identify the technical and business processes in which the identified resources or resource groups participate. As part of the inventory process, the system dynamically calculates possible attack vectors and identifies any potential threats. The infrastructure is also analyzed in terms of the security measures applied to the network and endpoints. All results of the inventory module are presented in the form of a visualized, interactive, logical network map. The collected information is used by other system modules:

- It serves as an event correlation parameter;
- It is used to enrich incident context data as part of the incident handling process;
- It is used when selecting scenarios and assigning tasks to service teams; It affects incident priorities;
- It forms the basis of automated cyber threat risk analysis; It influences the prioritization and handling of vulnerabilities;

2

Cyber threat risk analysis
Cyber threat risk analysis is a strategic activity in the security management process. When you are aware of the risks associated with cyber threats, you can apply more effective safeguards. The results generated by the risk analysis process are an important part of situational awareness and affect operational activities such as the incident and vulnerability handling processes. The SecureVisio platform includes mechanisms for automated, dynamic cyber threat risk analysis for processes and resources, based on data collected and continuously updated via the inventory process. Advanced algorithms analyze threat and security matrices, attack vectors, and potential consequences to systems, processes, and data. Contextual risk analysis rules allow risk mechanisms to be tailored to the specific needs of each organization. The analysis results are presented in the graphic risk assessment panel and the graphic network model. They are also an important event correlation parameter and affect incident and vulnerability priorities.

3

SecureVisio SIEM
Collection and storage of event information
SecureVisio is equipped with powerful, advanced mechanisms for collecting and storing event information from the entire IT infrastructure. The system allows you to collect logs via the syslog protocol, Windows Event Forwarding, and API interfaces, and to read data from text files, databases, and even e-mail accounts. It uses a flat file-based database which allows for very high performance. Built-in automatic archiving mechanisms enable long-term, central, or distributed data storage on the disk volume selected by the system administrator.
Analysis and correlation of events
The system is equipped with a constantly updated set of event parsers for handling various data sources. The regex, xml, json, conditional, and subordinate parsing mechanisms, the graphical parser creation interface, and the built-in debugger are powerful tools that can parse and normalize data from any source. The normalization process transforms the collected data into information that can be searched and processed. The system is equipped with automatic event correlation mechanisms and a constantly updated set of correlation rules based on matrices such as MITRE ATT&CK. Its advanced, highly flexible correlation engine offers a unique set of capabilities:

- Create events based on other events;
- Creating incidents based on events;
- Assigning priorities based on context;
- Scoring mechanism dependent on resource profiles;
- Creating and referencing reference arrays;
- Including resources related to incidents (type of resource and its role in the organization, technical and business processes at risk, type of data processed, potential consequences of the incident, attack vectors, risk analysis results) in the context correlation;
- A graphical interface for creating correlation rules.

secureVISIO

4

SecureVisio SOAR

Implementation of a process for handling security incidents and vulnerabilities

The SecureVisio platform includes an advanced SOAR (Security Orchestration Automation and Response) module. This allows you to implement security incident handling processes and procedures in accordance with industry best practices (including ISO- 270035, NIST SP 800-61R2, ENISA, and Carnegie Mellon University). Each potential security incident created by the correlation mechanisms becomes part of a process whereby SecureVisio automatically enriches the data, tracks status, response, and handling times, escalates the incident, explores potential consequences, and provides scenarios for addressing each stage of the analysis and response process.

Automation of analysis and incident response tasks

SecureVisio automatically assigns tasks to SOC team members based on defined parameters and the event context. The workflow follows scenarios customized for each stage of the incident handling process.

Advanced SOAR features include:

- A graphic interface for creating scenarios;
- Action plans broken down into steps and stages;
- Interaction with end users, asking questions and making further steps contingent on the answers;
- Changing the scenario or jumping to another step based on the circumstances;
- Embedded, automatic, or automated system actions within scenarios;
- Multiple scenarios automatically applied depending on status, context, and incident/event parameters;
- Notification of service teams and resource and process owners based on defined parameters such as resource type, processes at risk, resource importance, incident/event priority;
- Notification when the incident/event status changes;
- Notification when the established response and service times are exceeded;
- Response and handling times dependent on incident/event priority.

The incident handling module includes pre-built scenarios and hundreds of actions that enable automatic or automated interactions with external systems as part of the information gathering, pivoting, and incident response processes.

Implementation of a vulnerability management process

The vulnerability management process is one of the most important aspects of security management. That's why SecureVisio includes a module that provides a comprehensive approach to vulnerability handling. The system has integration interfaces with the leading vulnerability scanning solutions. These interfaces allow you to manage the vulnerability scanning process using multiple scanners and to import the results. Within the vulnerability management subsystem, SecureVisio helps facilitate the following tasks:

- Prioritizing vulnerabilities based on contextual data from other modules;
- Automatically assigning tasks to service teams based on context;
- Automatically assigning vulnerability, handling scenarios based on context;
- Automatically notifying service teams, resource owners, and process owners;
- Automatically tracking response and handling times;
- Automatic escalation;
- Enriching vulnerability information with contextual information from other modules.

5

Personal data protection

The Data Protection module assists the organization in handling data processing activities, processing categories, and reporting. The module also allows you to:

- Search IT systems that process personal data and the groups and the categories of data processed there;
- Determine the available technical safeguards against potential threat sources for all IT systems that process personal data;
- Automatically generate a 'Data protection breach report for the supervisory authority', including a determination of possible consequences of a security breach;
- Conduct the data protection impact assessment (risk analysis) in the scope of cybersecurity threats - as required by the GDPR - in a fully automated manner;
- Automatically analyze the risk of loss of data availability, confidentiality, and integrity;
- The information processed within the module provides additional context considered in the handling process.