Introduction

Warsaw, 2023-06-22

Esecure Sp. z o.o.
ul. Hoffmanowej 19
35-016 Rzeszów

www.securevisio.com
NIP: 6842590749
REGON: 180539624

Sąd Rejonowy w Rzeszowie
XII Wydział Gospodarczy
KRS: 0000350718

1. GENERAL DESCRIPTION

About SecureVisio

SecureVisio is a 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. Vendor 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.

Company Snapshot	
Industry:	• Enterprise Security • SMB • Security Operations Centers (SOC)
Product:	• SecureVisio Platform, sales from 2016
Customers:	• 4 SOCs (providing security services to customers) • 100+ customers
Location:	• Sales HQ: Warsaw, Poland, R&D: Rzeszów, Poland
Company Milestones:	• 2010 – Company founded • 2012 – EU funding obtained • 2016 – investor attracted • 2017 – commercialization began • 2018 – Acquisition of clients such as: T-Mobile Polska S.A., PKP Energetyka, Warsaw Municipal Water and Sewer Authority (MPWiK Warsaw) • 2020 – acquisition of the City of Warsaw, a prestigious project involving 45,000 terminals • 2021 – acquisition of the Polish Air Navigation Services Agency, a project including implementation of both the SecureVisio system and the Security Operation Center service.

SecureVisio as integrated and complex cybersecurity platform, provides Situational Awareness to SOC organizations (business aware CMDB, Network Mapping and SIEM/ UEBA, BIA, Risk Analysis, Attack Vector Visualization) and Situational Awareness to constituencies (Risk Analysis, BIA, Countermeasures Evaluation). The Solution optimizes IR processes (SOAR with playbooks, automatic escalation, IR process automation, NIST SP 800-61/ISO 27035) and Vulnerability Management processes (BIA and risk-based prioritization, workflow). Additionally, SecureVisio, develops IT security organizations capabilities and value (Playbooks, Knowledge Base).

2. EXPERIENCE AND REFERENCES.

Experience in development and implementation of SecureVisio

As the manufacturer of SecureVisio, Vendor has experience both in terms of system development and implementation. Since the start of commercial sale of the system on the Polish market, SecureVisio has actively participated in implementation process of their software for more than 100 customers.

The effectiveness of cyberthreat detection and response mechanisms has been tested by the biggest and most demanding customers, deriving from both commercial and public sectors. For instance, in the period of time of less than a year, while monitoring activity of more than 34k of users, with data flow of approximately 11k EPS, SecureVisio detected 39 security events (potential security incidents), 7 of which turned out to be false positives.

Such an impressive reduction in the number of false positives given this monitoring scale is deemed possible due to synergy between detection mechanisms and contextual tools found in SecureVisio, but most importantly, is the result of well adjusted and adopted to the client's needs implementation methodology. Vendor has specialized engineer staff that is responsible for the development, testing, implementation, as well as providing training and post-implementation support of SecureVisio - both in terms of system adoption (post-implementation workshops responsible for providing practical knowledge in terms of system usage), as well as reaction to submitted technical issues.

During system's commercialization process, SecureVisio's technical team had an opportunity to verify the system's effectiveness in sectors such as telecommunication, gaming, energy, leasing or government. SecureVisio's SIEM/SOAR have been successfully installed for both smaller, as well as bigger customers, whose network consisted of even thousands of assets requiring constant monitoring. Implementations and configuration work have been conducted in on-premise, hybrid and cloud environments. In case of the latter, SecureVisio has experience in terms of integration with Google Cloud, Sophos, Office 365, Azure Sentinel, Azure Monitor Activity Logs and Azure AD.

SecureVisio: Selected key references (case studies)

Reference no 1

Polish Air Navigation Services Agency (PANSA)

Every day the Polish Air Navigation Services Agency ensures safety of passengers in almost 3000 flights over Poland. The agency oversees and controls one of the biggest airspace in Europe: over 334,000 km2. There are approximately half a million of passengers on board of planes flying over Poland everyday. Polish Air Navigation Services Agency is the only institution in Poland that trains and employs civil air traffic controllers.

Project requirements achieved by SecureVisio:

- Fulfilment of the requirements specified in Polish Domestic Cybersecurity Regulations dated July 5th, 2018
- Continuous risk analysis for cyber threat
- Managing security incidents
- Keeping up-to-date cybersecurity documentation
- Managing vulnerabilities
- Reporting more severe security incidents to The Governmental Computer Security Incident Response Team
- Implementation of personal data protection management (PDP)
- Implementation of a complex tool used by PANSA's SOC consisting of the following components: SIEM/UEBA and SOAR

Why did the Customer choose SecureVisio?
SecureVisio was chosen via competitive bidding. SecureVisio solution fulfilled all the technical requirements defined by the Client. The tool needed to perform the function of Security Information and Event Management (SIEM) such as: collecting logs from systems and devices, aggregating logs in a dedicated repository with a capability of searching them and, based on log analysis, detect security incidents. The tool needed to perform the function of Security Orchestration and Automation Response (SOAR) - one graphical console enabling use of ready-to-use incident handling playbooks working according to a standardized incident handling process (Workflow), equipped with sets of predefined actions that would ensure automation of teams' work and integration of external data sources such as Vulnerability Assessment or Threat Intelligence. Additionally, the delivered solution needed to allow personal data protection for the organization, within the scope of reporting and creating and maintaining the registers legally required by GDPR, as well as cyberthreat analysis. SecureVisio solution was the only one that managed to fulfill the Customer's expectations concerning all-in-one tool with all the previously mentioned functionalities.

Competition

The tender procedure carried out by the Customer concerned both delivery of technological solution, as well as providing Security Operation Center outsourcing.

The solutions offered by the competitors were, among others:
- SPLUNK (SIEM)
- Energy SOAR
- Energy Logserver
- IBM Security QRadar SIEM

SecureVisio Solution fulfilled all Client's expectations and the submitted bid received the highest rating.

Reference no 2

The City of Warsaw

The City of Warsaw is the largest city office in Poland. It consists of City president, City council and 18 districts of the capital city of Poland - the largest Polish city in terms of area and population. The tasks of the office include primarily activities in the field of: city transport, trade, healthcare, culture, sport, education, real estate and many others tasks for over 1,7 million inhabitants of the city.

Project requirements achieved by SecureVisio

- Quick and efficiency incidents detection in all the city network of 22k assets (SIEM);
- Automation and prioritization of cybersecurity incident response (SOAR, Playbook);
- Automation of vulnerability management with business prioritization (SOAR);
- Integration with vulnerability assessment tool (Rapid 7).

Competition

Customer tested SIEM/UEBA solutions, including Exabeam and Splunk but they lacked SOAR features (automation, workflow, playbook), vulnerability management, business awareness and NISD support.

Why did the Customer choose SecureVisio?

- Detection and response for cybersecurity incidents in one tool (SIEM+SOAR)
- Unified management of risk, vulnerabilities and incidents
- Risk analysis and business prioritization of incidents and vulnerabilities
- Electronic documentation of networks and assets with threat modelling
- Automation of human works in incident response process

Reference no 3

Warsaw Municipal Water and Sewer Authority in Warsaw (MPWiK Warsaw)

MPWiK Warsaw every day provides over 350 million liters of clean water to the inhabitants of the Warsaw agglomeration. The company has over 130 years of tradition. It operates over 4,300 km of the water supply network and 4,200 km of the sewage network. The modernized and constantly expanded sewage system provides the residents with comfort and savings.

.

Project requirements achieved by SecureVisio

- Security Operations Center (MPWiK SOC) for business IT systems as well as SCADA/OT systems in critical infrastructure
- Incident management compliant with NISD (Polish Act on the national cybersecurity system)
- Automation of human security management operations (SOAR, Playbook)
- Deep integration with incident detection and vulnerability assessment tools

Competition

Customer evaluated many SOAR and SIEM/UEBA solutions, including IBM and Splunk but they lacked business awareness and NISD support.

.

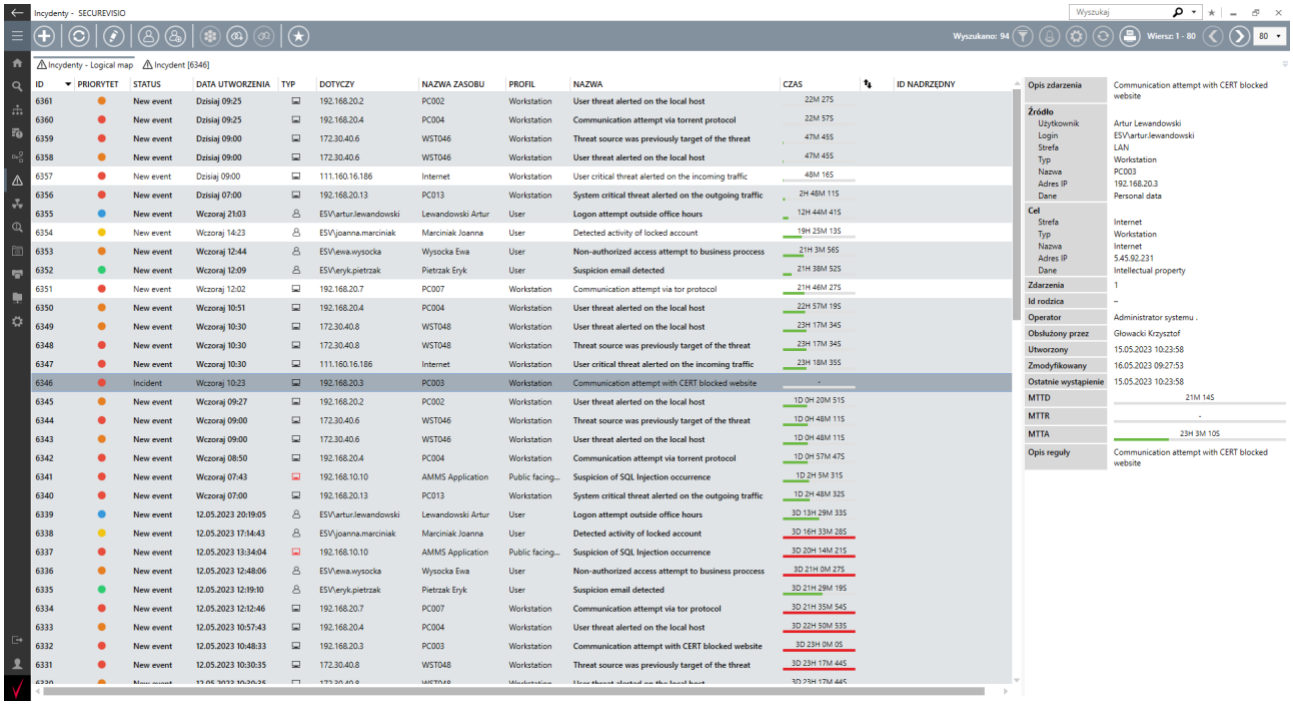
Why did the Customer choose SecureVisio?

- Cost effective SOAR and SIEM/UEBA suitable for SOC of IT and OT/SCADA
- SOAR with one SOC console for incident, vulnerability and risk management
- Automation of human works, incl. incident management with NISD compliance
- Unified platform providing all SOC capabilities, incl. incident detection, incident and vulnerability management, and threat modelling and risk management

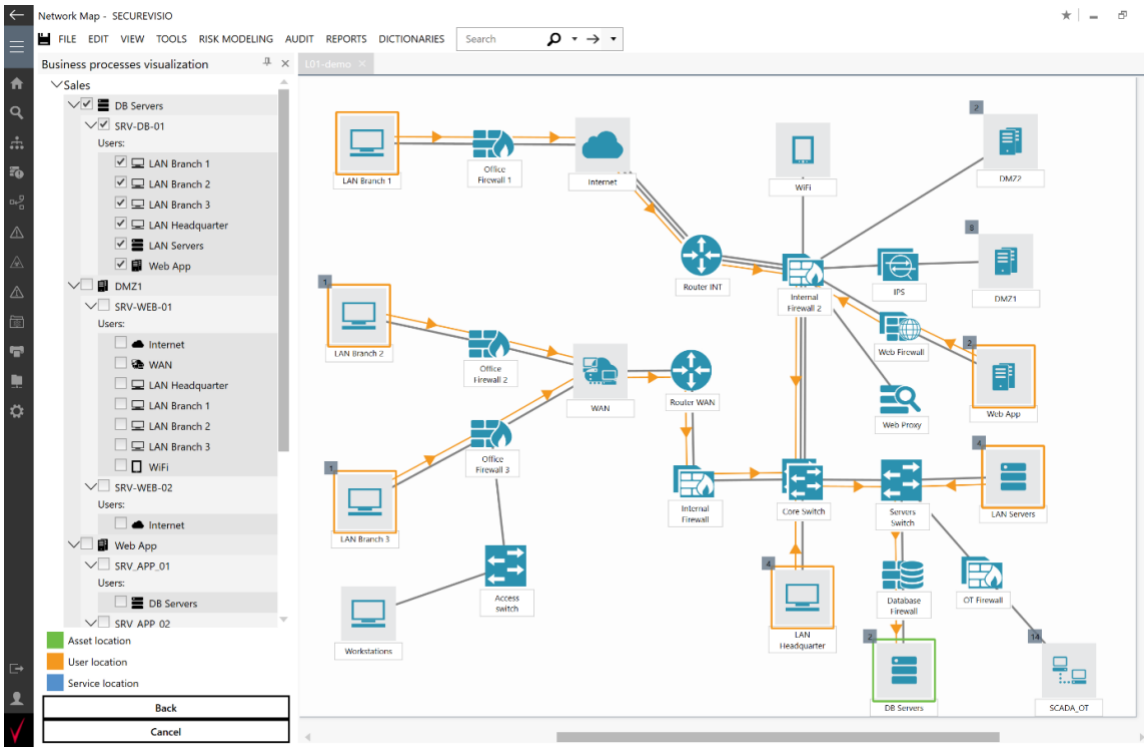
3. TECHNOLOGY DESCRIPTION.

SecureVisio Incident Management Console provides complete set of tools dedicated for incident detection, incident management (based upon an international standard ISO/ IEC 27035), and integrated Business Impact Assessment prioritizing alerts in real time to focus IT security personnel attention on the most important issues.

Security incidents are detected by contextual SIEM/ UEBA supported by Threat Intelligence platform. Unique feature of SecureVisio's SIEM is correlation rules dynamically generated based on the information from Network Map ad IT risk assessment matrix (IT GRC). SIEM correlation rules automatically include the information about new business processes and sensitive data. Thus it can be stated that SecureVisio SIEM understand organisation, it's processes and most significant assets. Additionally, machine learning mechanisms implemented in UEBA module take into account the wider context of the data to be learned, which is enriched with the knowledge of the IT GRC system, which in turn translates into even greater efficiency of both detection and selection of events.



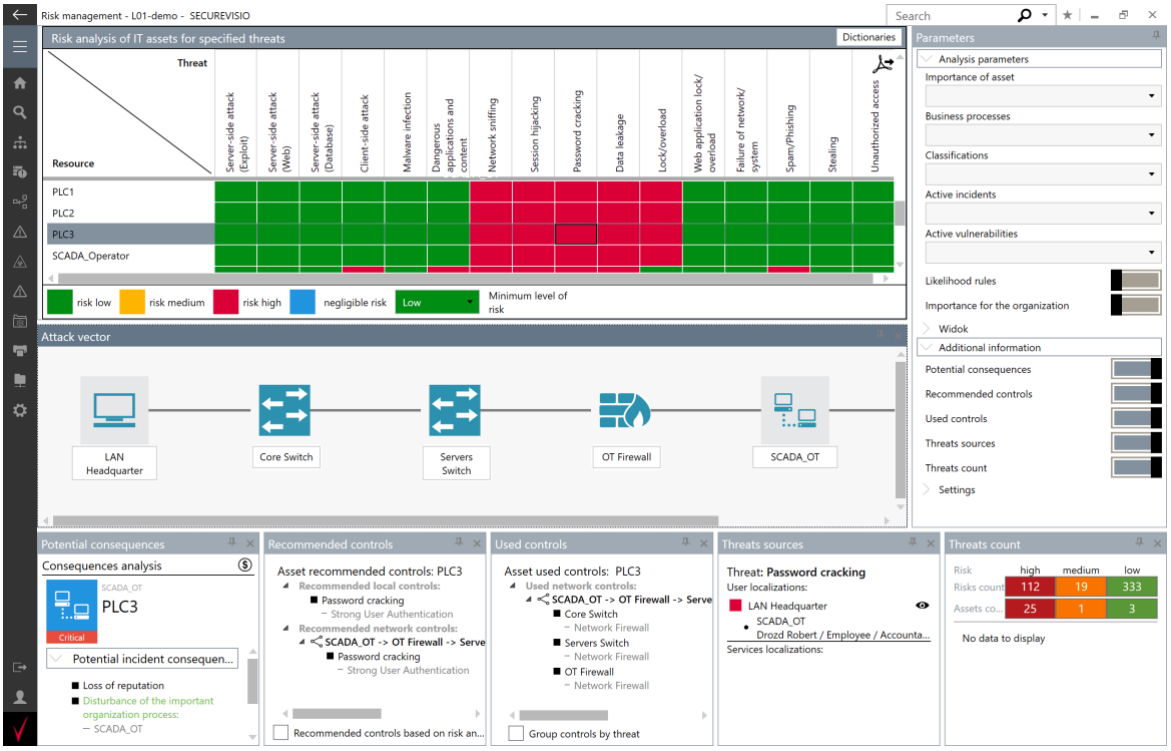
Business prioritization of incidents and vulnerabilities



Visual electronic documentation of networks and assets with threat modelling

SecureVisio Incident Management Console provides SOAR capabilities that allow different technologies to integrate and work together. SecureVisio SOAR is a unified system that in one platform provides many useful tools, including:

- Interactive panel presenting the incidents collected from variety of incident detection systems automatically or on-demand enriched with relevant information retrieved from external data sources like Threat Intelligence
- Workflow defining the tasks and paths of people's works (e.g., incident categorization, triage, analysis, response) that guides and enforces people to conduct defined actions, and provides case management, tracking of status, SLA and useful metrics like mean time to respond (MTTR), and auditing
- Playbook with predefined actions that automate the incident analysis, response and other activities related to incident management, e.g., geolocation lookup on attacker or victim's IP addresses, detonation of suspicious file in anti-malware sandbox, search for suspicious files on endpoints, disconnection of suspicious device from the network, blocking of URL on the safeguards, etc.
- Incident investigation panel to collect and store artefacts of the investigation for current and future analysis and keep historical information of the incidents and notes, and in case of security breach use forensics to perform a detailed analysis of cybercriminals activities
- Collaboration panel that allows the team members to exchange information, coordinate communication with other staff, assign and escalate the cases, coordinate actions and decisions etc. Journaling function records the information about actions taken, including details of the action itself, the person taking the action and when it occurred.
- Dashboards and reports providing summarized information and metrics for different stakeholders like security analysts, managers responsible for incident management teams, and chief information security officers (CISO)



Risk analysis & cybersecurity awareness

Cyber Crisis Management & Prevention with business-orientated SOAR capabilities

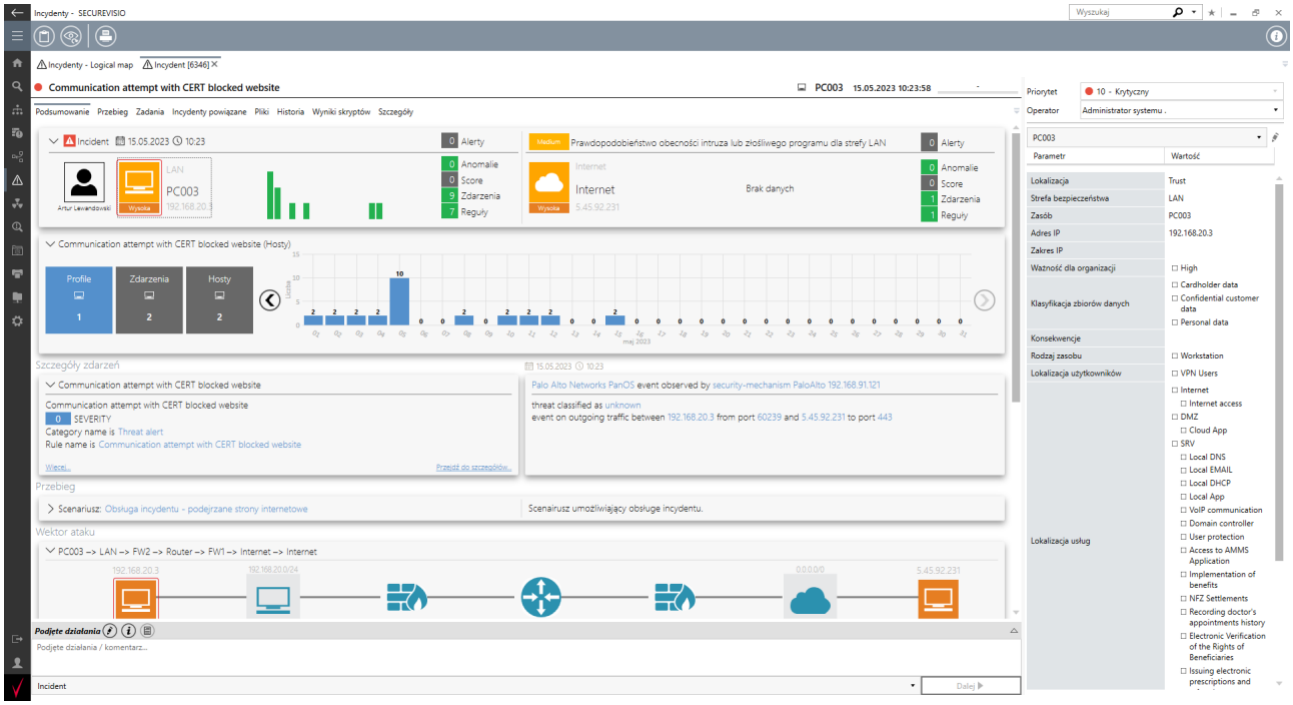
Managers accountable for IT security like CISO, CIO, SOC manager, etc. should be immediately notified in case of new incidents and vulnerabilities that can cause huge business damage, e.g. new vulnerability in a database in financial system. Main goal of IT security – that is protection of the organization's business - is difficult to achieve because the technologies responsible for management of IT security like SIEM, SOAR and vulnerability scanners do not understand the business context of security events.

SecureVisio introduces business awareness into any organization and SOC by integration with existing incident detection systems as well as vulnerability scanners. For the managers accountable for IT security, SecureVisio works as Cyber Crisis Management system.

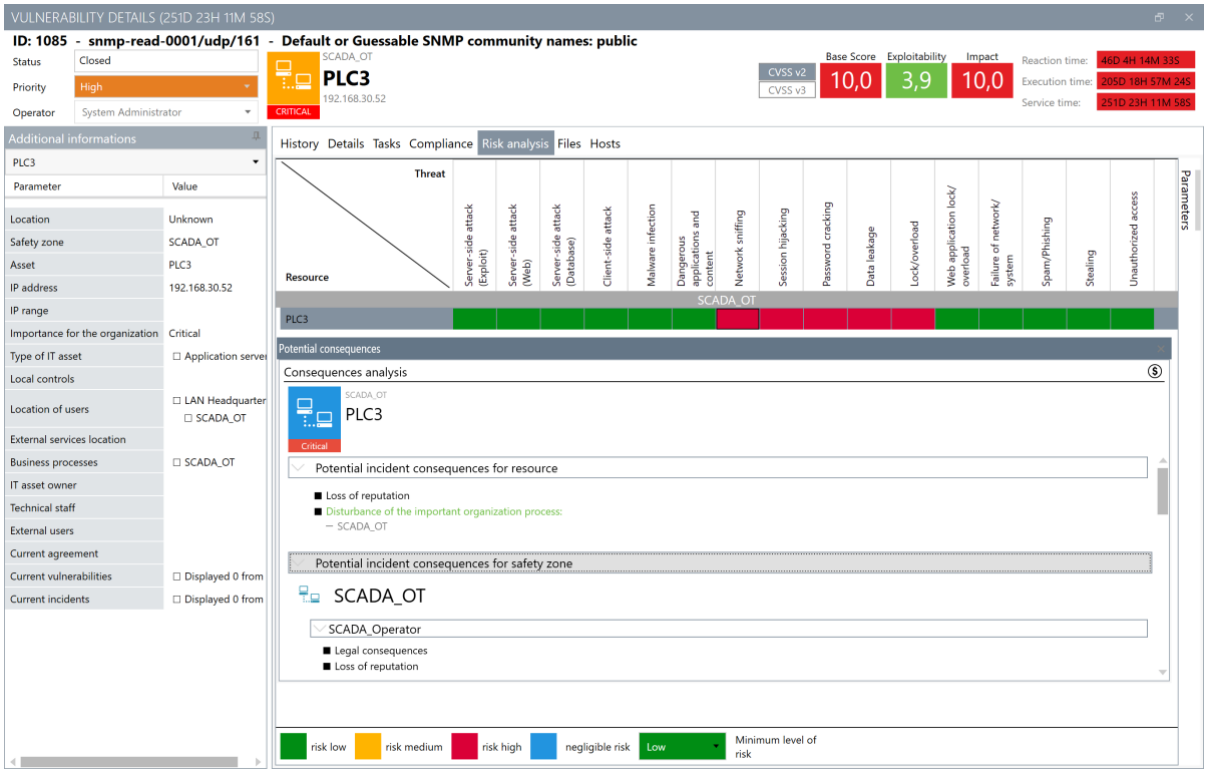
Particularly, the following SecureVisio's features are used to make work of CISO, CIO, SOC managers, etc. more effective:

- SecureVisio in real-time conducts business impact analysis (BIA) and based on potential impact it prioritizes all security alerts and vulnerabilities. It works even for thousands of generated alerts and detected vulnerabilities. People managing IT security focus on the most important events and they will do not overlook the situations that can cause damage to the organization
- SecureVisio automatically supplements the knowledge of people managing IT security with the information required to understand the situation and make proper decisions, i.e. potential business damage and breach costs, new vulnerabilities of the assets, new and historical incidents relevant to the assets, visualized asset data on the network map, etc.

- SecureVisio conducts threat modelling and attack simulations, and based on the results on the Network Map visualizes all potential network paths where cybercriminals can attack the assets critical for the organization



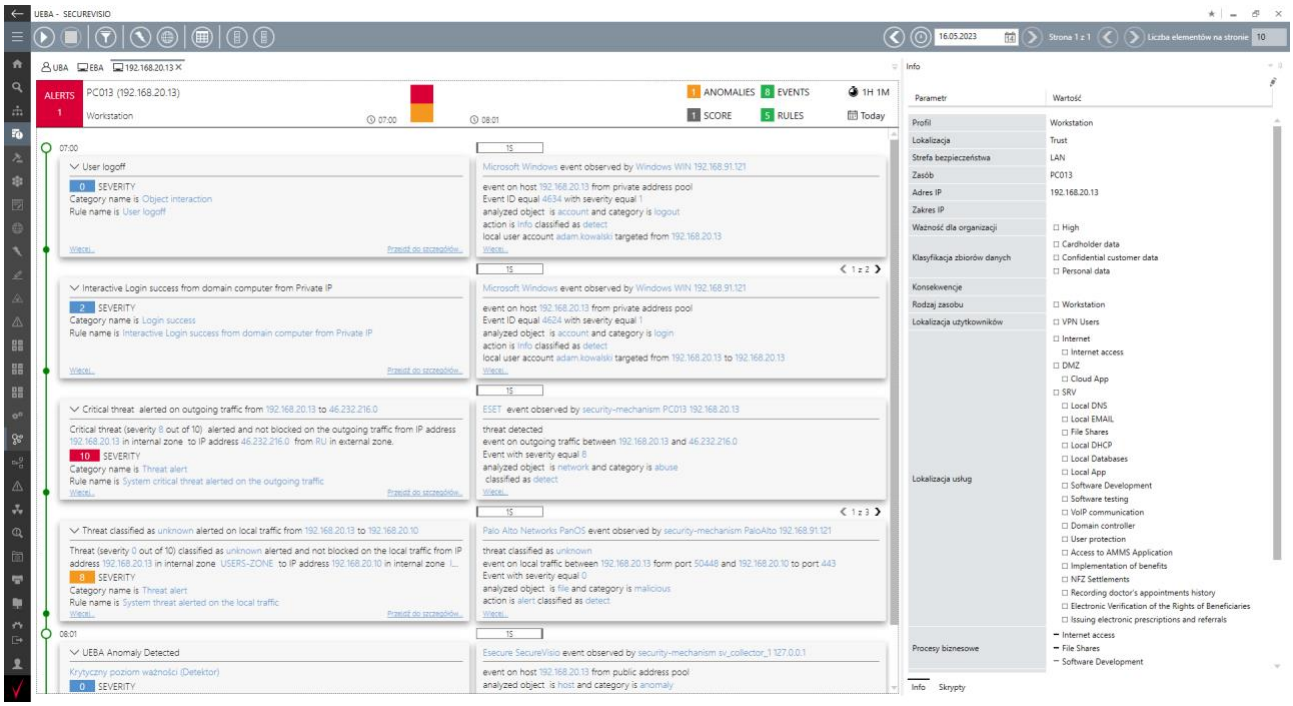
Cybersecurity incident overview with complete business context



Vulnerability overview with complete business context

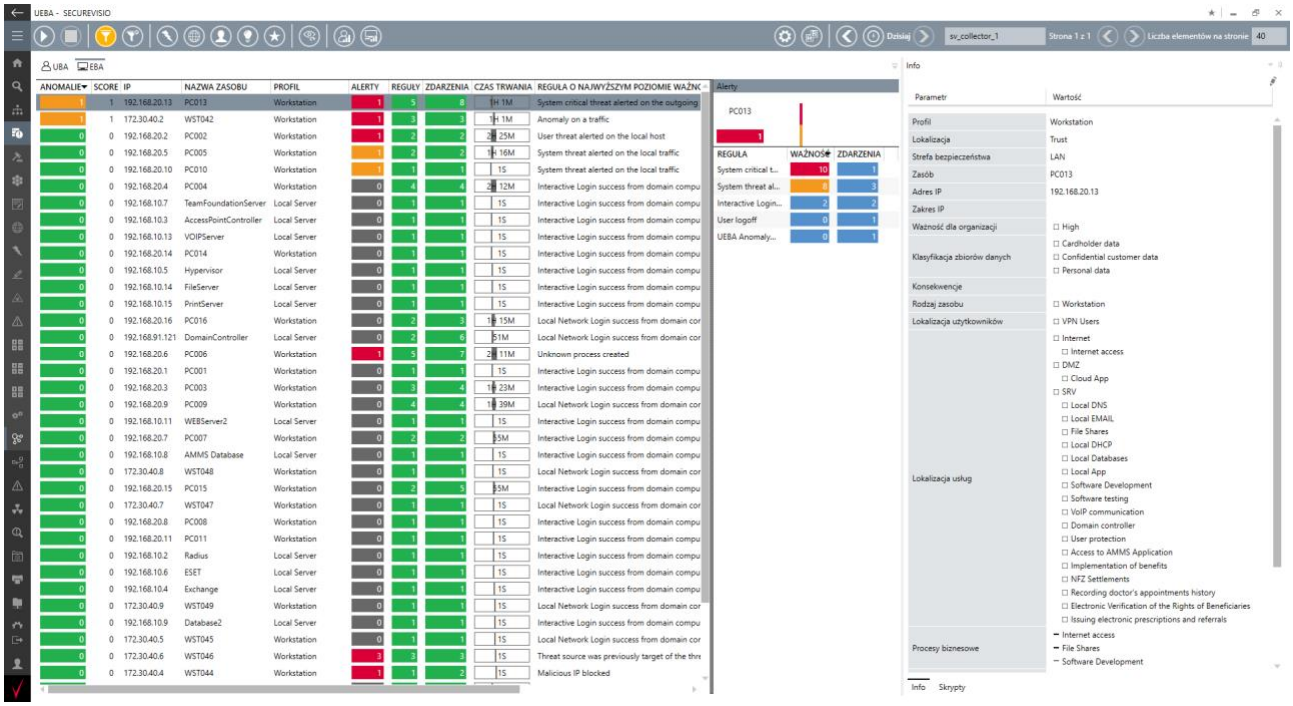
SecureVisio SIEM/UEBA understands business context in real-time. People conducting incident management are supported with dedicated Workflow, Playbook, Dashboard and Reporting tools offering capabilities of SOAR - Security Orchestration, Automation and Response. SecureVisio addresses world cybersecurity trends, i.e. Gartner[1] emphasizes the following main SOAR's benefits and uses:

- Prioritizing security operations activities: Prioritized and managed remediation based on business context is the main target of security operations
- Formalizing triage and incident response: Security operations teams must be consistent in their response to incident and threats. They must also follow best practices, provide an audit trail and be measurable against business objectives
- Automating containment workflows: This offers SOC teams the ability to automate most of the activities to isolate/contain security incidents to be conceived by the human decision for the final steps to finalize the incident response



UEBA Console overview

[1] Innovation Insight for Security Orchestration, Automation and Response, Gartner 2017



UEBA Console overview

Who is SecureVisio useful for?

- Security teams responsible for incidents and vulnerability management and other security operations in IT environments. SecureVisio automatically conduct risk assessment and allow immediately to understand business impact of all detected events (there is no need to spend time in search for this information in IT systems' documentation or consult with business owners of effected IT systems).
- Security architects. SecureVisio uses expert knowledgebase and ISO/IEC 27005 risk management methodology to automatically analyse an effectiveness of protections of IT systems against relevant attack vectors and threats and estimate risk level. SecureVisio uses its expert knowledgebase to recommend the protections that reduce the risks. This function immediately provides useful advice to people responsible for designing IT security. What is important, people understand potential business damage if the risks are realized and security breaches occurred.
- Managers of security team's accountable for effectiveness and quality improvement. SecureVisio calculates business-relevant key performance indicators (KPIs) and key risk indicators (KRIs). These metrics allow to predict new emerging threats to proactively react and improve protection of the most valuable assets.
- Business owners accountable for the protection of IT services and sensitive data.
- Security professionals responsible for support of Business Continuity Planning.

SecureVisio Incident Management Console - criteria for analysis

Facilitate and automate the collection and input of business context	SecureVisio Network Map – visual network picture and asset inventory created automatically using firewall logs received by SecureVisio SIEM module. Network map is based on a mathematical graph that describes IT systems in a technical and business context, as well as visualizes IT systems' network connectivity and safeguards. Network Map describes IT systems supporting important business processes and their location, i.e., logical security architecture describing network connectivity, control layers and security zones. SecureVisio Business Process Wizard – graphical panel to define important business processes using, i.e., process importance to the organization, consequences of security breach, business owner, cost of 1 hour failure, dependent processes, days, and time of operation) and indicate IT systems on the network map that are required for the business processes to operate. If relevant, indicate on network map the location of sensitive date, i.e., PII, intellectual property, cardholder data.
Facilitate and automate the collection and input of technical context	SecureVisio Network Auto-Discovery - in SecureVisio's Network Map the asset inventory and technical context collection is automated with auto-discovery mechanisms that utilize SNMP, CDP, LLDP, WMI as well as IP and port scanning and network flows analysis. SecureVisio Vulnerability Assessment – the vulnerabilities discovered by integrated vulnerability scanner (e.g., OpenVAS, Tenable Tools, Qualys, Rapid 7) and CVE database as well as the indicators of compromise (IoC) received by integrated Threat Intelligence Platform (e.g., MineMeld). SecureVisio Expert Knowledgebase integrated with SecureVisio's Network Map provides IT security expert know-how, including: ● susceptibility of different IT system types to various attack methods (e.g., workstations are more susceptible than servers to client-side exploit attacks) ● effectiveness of different safeguards against various attack methods (e.g., anti-malware can prevent against

	computer viruses and worms but not against network exploit attacks) • likelihood of malware and intruder presence in different types of network zone (e.g., DMZ and guest network segment have high likelihood of malware and intruder presence) The system has a connector that is used to collect logs acquired from Microsoft Azure cloud and which utilizes the Multiconnector interface. Logs can pertain a multiple number of Microsoft products that the user has access to via Azure cloud, such as: Microsoft AZURE Sentinel and Office 365. The SecureVisio Connector periodically establishes connection with the cloud via Azure Log Analytics API and subsequently executes a specific query for a given source, e.g. Azure Active Directory, Office 365, Microsoft Defender for Clouds Apps to filter and download logs in order to parse and correlate them. The system has a connector that is used to collect logs acquired from Sophos Antivirus cloud. The connector establishes connection with Sophos cloud via REST API. It provides a capability to download logs both from Alert and Event categories. The downloaded logs are then correlated with other events taking place within the environment, e.g. events from AZURE.

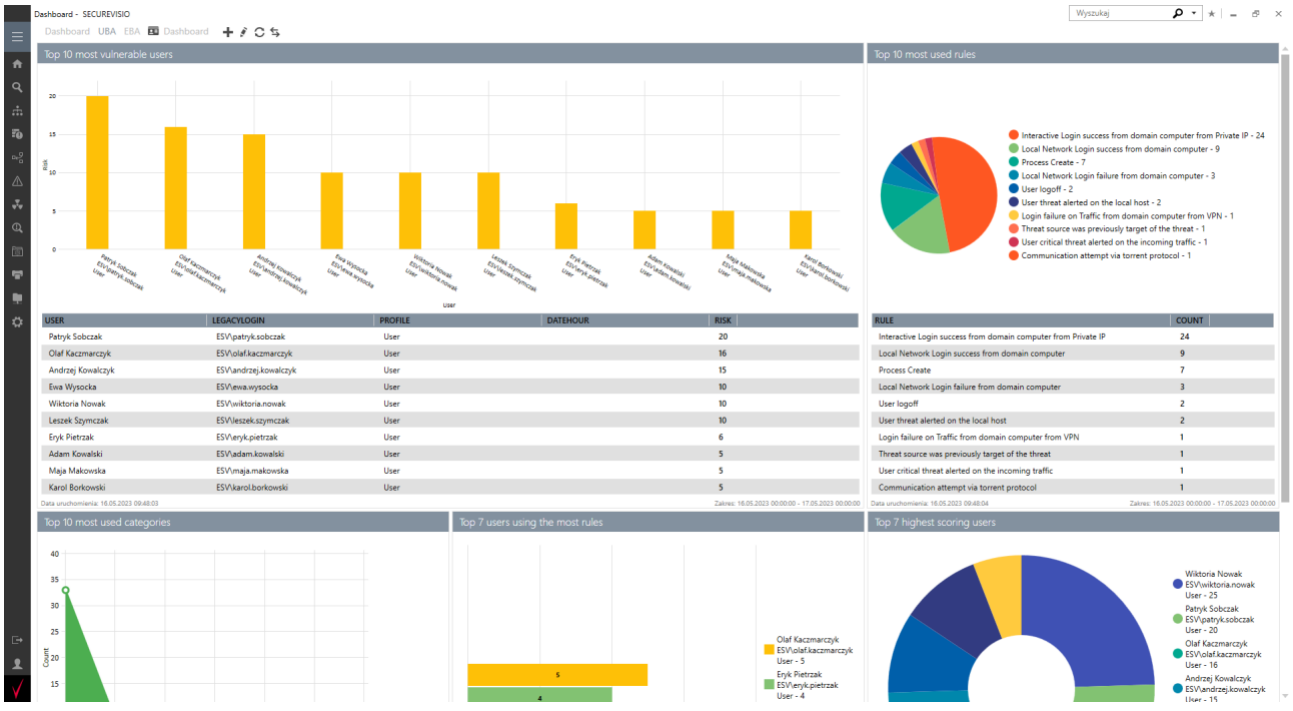
Availability of business and technical context at a low level of data analysis (SIEM, UEBA)	SecureVisio Event Prioritization (part of SIEM and UEBA engines): • Technical priority estimation – severity of the event is estimated in real time based on the information received from the safeguards and Threat Intelligence, and CVSS score received from vulnerability scanner or CVE. • Business priority estimation – criticality of the event is estimated in real time based on sensitivity of data (e.g., intellectual property, financial data) and the importance of business processes supported by the assets affected by incident or vulnerability. The information required for the estimation is maintained in the network map and asset inventory. • Business impact assessment - consequences of the event (i.e., potential business damage) are assessed in real time based on sensitivity of data, the importance of business processes supported by the assets as well as legal consequences (e.g., GDPR). Business impact analysis is conducted also for the assets located in the same security zone as the asset affected by an incident or vulnerability.

Availability of business and technical context during incident handling (SOAR)	SecureVisio Incident Investigation (part of SOAR) • Technical context details – information about incident or vulnerability received from the safeguards, vulnerability scanner as well as external sources like Threat Intelligence • Crime scene – visualization on the network path and security zone where an event occurred. Network map is utilized to show crime scene • Attack vector likelihood – risk estimation for the threats relevant to an affected asset. Estimation is based on the analysis of safeguards available on the network paths to the affected asset. Attack simulator module and expert knowledgebase are utilized for this purpose • Current vulnerabilities – when analysing security alerts (e.g., malware infections) the information about current vulnerabilities of an affected asset is received from vulnerability scanners or CVE SecureVisio Attack Simulator module based on expert knowledgebase and algorithms to find potential attack paths in the network using Dijkstra graph algorithm (i.e., finding the shortest paths between nodes in a graph). SecureVisio Risk Assessment module that automatically estimates the risks based on the algorithm defined in ISO/IEC 27005. Business owners of important assets (e.g., ERP, e-commerce, SCADA, domain controllers, databases containing sensitive data) using Business Process Wizard should specify important business processes, i.e., process importance to the organization, consequences of security breach, business owner, cost of 1-hour failure, dependent processes, days, and time of operation). If relevant, also sensitive data, i.e., PII, intellectual property, cardholder data.

Business-relevant KPIs and KRIs automatically measured	SecureVisio Visualization and Reporting - panel that shows comprehensive picture of the organization's security state relevant to business processes and visualizes technical and business-relevant key performance indicators (KPIs) and key risk indicators (KRIs) to be understandable for non-technical stakeholders. Includes mechanisms for notification of decision makers and business owners of IT systems as well as the reports for compliance with the cybersecurity law requirements. SecureVisio calculates business relevant KPIs and KRIs. These metrics allow to predict new emerging threats to proactively react and improve protection of the most valuable assets. KPIs inform people accountable for IT security about events that have already affected the organization (e.g., number of incidents handled, time from detection to containment/eradication). KRIs show risk trends that can help to better monitor potential future shifts in risk conditions or new emerging risks (e.g., monthly increase of incidents and vulnerabilities related to critical business processes or sensitive data). Thanks to business relevant KPIs and KRIs the business owners of IT systems are aware of security risks, and they are early notified about situations requiring immediate decision and response. KPIs and KRIs are particularly useful for planning the security improvements.

Interactive dashboards

Interactive dashboards

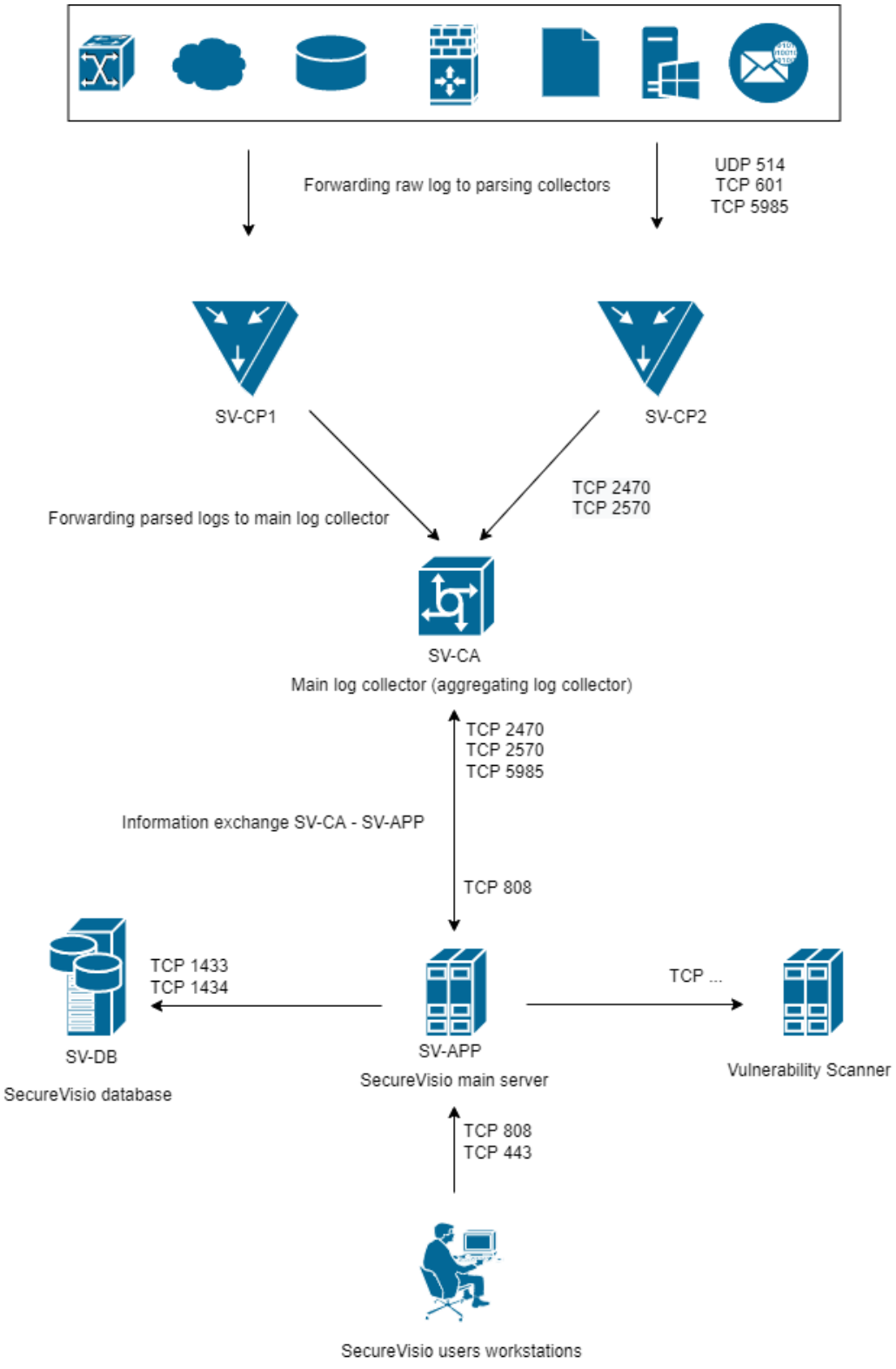


Interactive dashboards

4. THE EXAMPLE OF ARCHITECTURE OF PROPOSED SOLUTION

Proposed architecture for SecureVisio SIEM & SOAR system

Architecture overview



Software to be installed:

Functional server	Quantity	Software type and version
SV application server SV-APP	1	Microsoft Windows Server 2016 or newer
	1	.NET framework version 4.8
	1	SecureVisio SIEM/SOAR Application Server Software
	1	Powershell 7 or newer
SV instance/database server SV-DB	1	Microsoft Windows Server 2016 or newer
	1	Microsoft SQL Server Standard 2016 or newer
	1	NET framework version 4.8
	1	Powershell 7 or newer
SV aggregating collector SV-CA	1	Microsoft Windows Server 2016 or newer
	1	.NET framework version 4.8
	1	SecureVisio Log Collector Server Software
	1	Powershell 7 or newer
SV parsing collector SV-CPx	2	Microsoft Windows Server 2016 or newer
	2	.NET framework version 4.8
	2	SecureVisio Log Forwarder Server Software
	2	Powershell 7 or newer
Software installed on operators' computers(1)	x	SecureVisio GUI Console
	x	.NET framework version 4.8

Required parameters for virtual machines:

Minimal configuration				
SV-APP SV application server	1	vCPU	8	
		RAM	32 GB	
		HDD	Partition 1: 100 GB SSD Partition 2: 50 GB SSD	
		Network interfaces	2 x 1Gb/s Ethernet (min.)	
SV-DB Database server	1	vCPU	4	
		RAM	16 GB	
		HDD	Partition 1: 100 GB SSD Partition 2: 250 GB SSD	
		Network interfaces	1 x 1Gb/s Ethernet (min.)	

SV-CPx Servers for parsing collectors	2	vCPU	8	Collectors are responsible for parsing and sending parsed events to aggregating collector.
		RAM	32 GB	
		HDD	Partition 1: 100 GB SSD Partition 2: 50 GB SSD	
		Network interfaces	2 x 1Gb/s Ethernet (min.)	
SV-CA Servers for aggregating collectors	1	vCPU	32	Collectors are responsible for aggregation and correlation of events Server needs to be connected to IT asset for log storage This partition 2 has to take advantage of fast and reliable data storage with volume sufficient enough to provide data collection over the required time period. This partition 3 data is dedicated to archived logs.
		RAM	64 GB	
		HDD	Partition 1: 100 GB SSD Partition 2: 2,5TB SSD Partition 3: 2TB SSD	
		Network interfaces	2 x 1Gb/s Ethernet (min.)	

Required disk storage for aggregating collector

There are two types of data storage:

- Online data - uncompressed data supported by all of SV's functionalities. Such data requires high availability data storage (1:2 EPS to IOPS conversion factor)
- Archived data - compressed (10:1) data. Available through archived log browser with basic search capability. This type of data can be stored on slower data storage or even transferred to backup data storage.

For example, with the assumption of average log transfer of 300 GB per month, the estimated amount of necessary disk storage for one aggregating collector:

- Option - 300GB/30 days - retention period and online access up to 90 days
- Monthly requirement for storage space is up to 300GB for raw logs
- Storage space required for raw data retained for 90 days is 900 GB
- After log processing via SecureVisio (parsing, event creation, UEBA feeding data) the required storage space grows twofold. The recommended safe value for disk storage capacity is 2 TB.

Communication port descriptions

The following ports are used on the SV-APP machine:

- Inbound traffic
  - TCP 808 for inbound connections (log collectors and SV client application communication)
  - TCP 443 - SecureVisio (web application)
  - TCP 3389 - RDP remote console
- Outbound traffic
  - TCP 1433, 1434 – communication with the database
  - TCP 2470 - communication with log collectors
  - TCP 2570 - creating internal events
  - TCP 5985 - communication with all collectors (management, updates)
  - TCP 389,636 - Active Directory integration

The following ports are SV- DB used on the database machine:

- Inbound traffic
  - TCP 1433 i 1434 – communication with the database

The following ports are used on the SV-CA machine:

- Inbound traffic
  - TCP 2470 for inbound connections, log collector port (security rules and configuration)
  - TCP 2570 for communication between log collectors (receiving frames from SV-CPx)
  - TCP 5985 - port for management and update - connections initialized from SV server
- Outbound traffic
  - TCP 808 - communication with SV server

The following ports are used on the SV-CPx machine:

- Inbound traffic
  - TCP 5985 - management port, update, WEF - connections initialized from SV server
  - UDP 514, TCP 601 for inbound connections (Syslog protocol) and other ports utilized in the process of receiving and fetching information for data source. Default listening enabled on port UDP 514
- Outbound traffic
  - TCP 2470 for collecting parsers and configuration from Log Collector.
  - TCP 2570 for sending the collected information to Log Collector.

5. ADDITIONAL INFORMATION CONSIDERED TO BE IMPORTANT

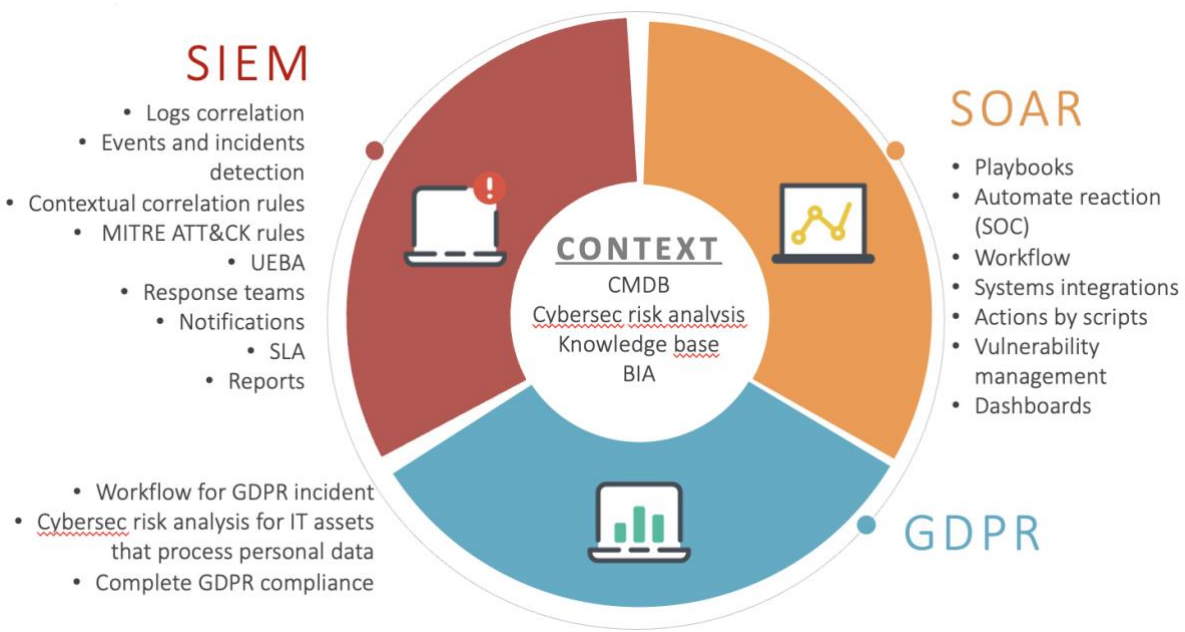
SecureVisio: Complete Security Incident Reaction Platfrom

SecureVisio as an integrated platform that strengthens key strategic, tactical, and operational aspects of cyber security for businesses and organizations. It is the only system on the market that simultaneously implements threat detection and incident handling mechanisms supported by automated resource and process inventories as well as vulnerability management, IT risk analysis and personal data protection.

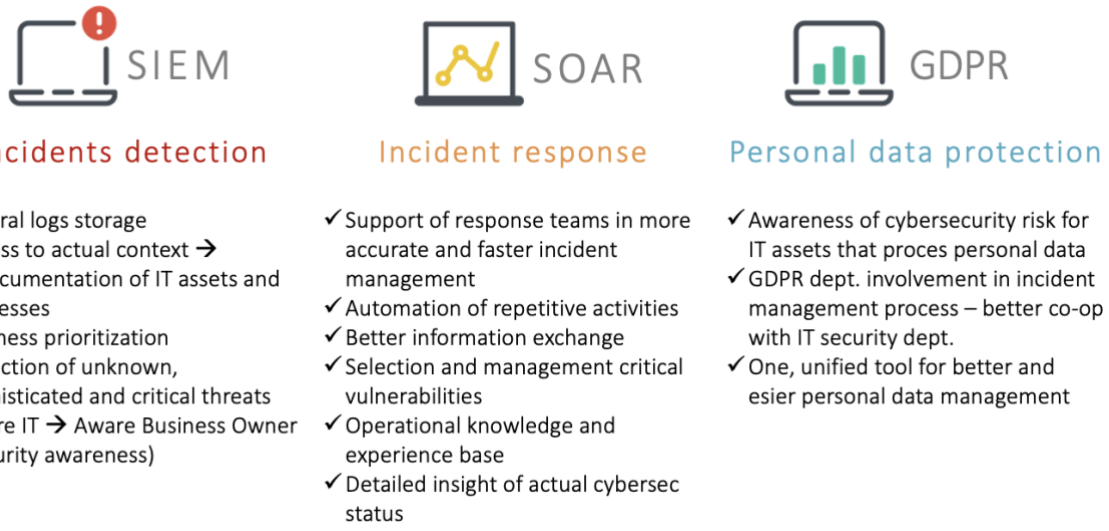
It contains following tools (functionalities):

- Configuration Management Data Base (CMDB)
- IT Governance, Risk Management & Compliance (IT GRC)
- Contextual (business aware) Security Information and Event Management (SIEM)
- User and Entity Behavior Analysis (UEBA)
- Security Orchestration, Automation and Response (SOAR)
- Threat and Vulnerability Management (TVM)
- Personal Data Protection AddOn (GDPR)

Above mentioned tools are incorporated within 3 modules of SecureVisio. Each module shares IT GRC and CMDB functionalities.



Selected benefits of each module:



IT asset management and risk assessment as a foundation of business aware SIEM and SOAR

Building situational awareness of resources, networks, and processes is one of the most important strategic and operational aspects of the security management process. SecureVisio is equipped with automated active and passive IT inventory and network mapping mechanisms. These mechanisms detects systems, network devices and applications, determining their type and the relationships between them. The inventory mechanisms also identify technical and business processes. As part of the inventory process, the system dynamically calculates potential attack vectors and identifies possible threats. IT infrastructure is also analyzed in terms of the security measures applied in the network and at endpoints. The results of the inventory process are displayed as an interactive, visual network map. The collected information is then used by other system modules:

- As parameters in the event correlation process (SIEM/ UEBA);
- To enrich incident contexts in the incident handling process (SIEM/ UEBA and SOAR);
- To help select scenarios and assigning tasks to service teams (SOAR);
- To help assign incident priorities (SIEM);
- As the basis for automated security risk analysis (IT GRC);
- To adapt and implement vulnerability prioritization and handling processes (TVM).

Second strategic element of the security management process in SecureVisio is CyberThreat risk analysis. Awareness of the risks associated with cyber security threats will help you apply effective security measures. The results of the risk analysis process are an important element of situational awareness and affect operational activities such as incident and vulnerability handling processes. The SecureVisio platform includes mechanisms for automatic, dynamic analysis of processes and resources, based on data

constantly collected and updated as part of the inventory process. Advanced analytical algorithms include threat and security matrices, attack vectors, and potential consequences for systems, processes, and data. Contextual risk analysis rules allow adaptation of risk mechanisms to the specific needs of each organization. Analysis results are presented in a graphical risk assessment panel and in a graphical network model. The results are also an important event correlation parameter and affect the incident and vulnerability prioritization processes.

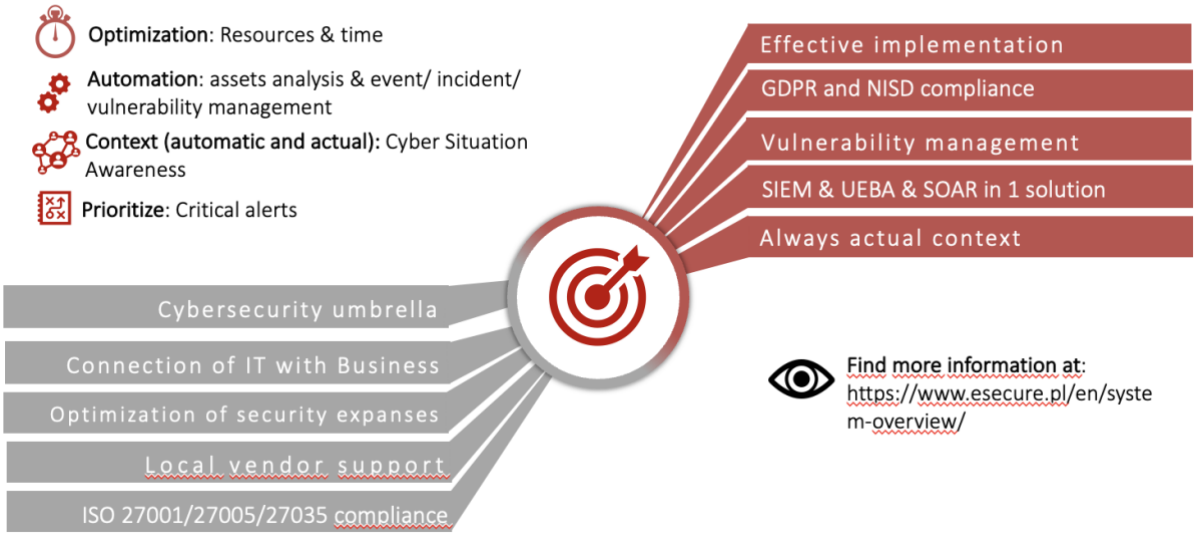
Incidents prioritization and reducing false-positives

SecureVisio allows prioritatization of security events, security incidents and vulnerabilities, while also taking into consideration the company's character. Due to the latter, it is possible to identify events requiring immediate handling, as well as those which handling can be postponed or even omitted entirely.

If the alarm which is sent from the external source has a high priority, it does not necessarily translate to a real threat for the organization. For instance, when Next-Generation Firewall (NGFW) identifies database threat on the basis of the signature, SecureVisio will determine whether the IT asset being the target of such threat actually has such a database at all. In case when the database is not installed on this IT asset, despite the high technical priority assigned by the NGFW, SecureVisio will decrease the event's priority or automatically discard it, treating it as false positive.

SecureVisio has automatic threat assessment functionality that allows it to assess likelihood of threat materialization. For every threat, an attack vector is analyzed, as well as present local and network safeguards, security zone's threat level from which the attack has been registered, vulnerabilities of the attacked IT asset or attacked IT asset type.

The above approach results in high SIEM effectiveness level which is impossible to attain by other competing SIEM systems that do not have IT GRC module.



Key advantages of SecureVisio Platform

Offered technical support & customer care

SecureVisio provides flexible and client-oriented approach in terms of clients' needs. It pertains both individual implementation, including all requirements such as connecting non-standard log sources, preparation of specific integration in terms of response playbooks or system fine-tuning as part contextual mechanisms (cyberthreat risk analysis/e-documentation - CMDB). The receptiveness towards cooperation is reflected in product roadmap which takes into consideration new functionalities and features suggested by end-users. The vast majority of features that SecureVisio can boast has been implemented on the basis of our clients' proposals and opinions.

SecureVisio SIEM & SOAR Cloud Support

SecureVisio supports the current market requirements allowing for implementations tailored to the customer's requirements, including the possibility of installation in various configurations, allowing for the maximum adaptation of the product to the market. The flexibility of the installation allows for the optimization of costs related to the place and method of data processing and ensuring business continuity optimized for the needs of the organization.

The product can be installed directly at the customer (onPremise) and in the cloud. There are also various mixed options that allow the use of reliability options (HA) and the separation of functional components of the system between different clouds or between the onPremise location and the cloud.

SecureVisio has built-in connectors (pre-built connectors) that download logs from cloud services (alerts) and logs of user and resource activity (Assets). If, as a result of the analysis, SecureVisio detects a threat, it can automatically perform actions via cloud services as a response to detected threats (and orchestrate actions back to the cloud services for threat response automation).

SecureVisio fully supports hybrid distributed installation and that is why, starting from version 4.0 , is segmented into different modules, namely:

- Parsing Collector
- Log Collector
- Event Collector
- Machine Learning Collector
- SIEM Collector
- Application Server
- Database Server
- GUI/Web Client

- Automation Agent

Each one from the above modules can be installed in any cloud-based environment or on-premise, which in turn allows for maximum flexibility and cost effectiveness of the solution.