CREATING AN EFFECTIVE SECURITY OPERATIONS PLATFORM

Michał Ostrowski
Chief Revenue Officer
SecureVisio

Company Information

- Created 14 years ago, Secure Visio had a market debut in 2016.
- The system has been successfully implemented in more than 150 organisations.
- SecureVisio supports cybersecurity teams in public institutions, central and local government and critical infrastructure providers such as telecoms, hospitals, waterworks or power plants, etc.
- SV is a 100% privately owned company with Polish capital
- SecureVisio team currently consists of more than 100 people, 70% of whom are in technical positions (implementation engineers, developers, testers, post-implementation consultants, pre-sales).

What’s your cyber resilience level on a scale 1-10?

1

4

10

secureVISIO

CHALLENGES OF CYBERSECURITY OPERATIONS:

Technology

People

Money

CHALLENGES OF CYBER SECURITY OPERATIONS

TECHNOLOGY:

⚠️ Countless point products, best-of-breed approach, technological debt - results in:

⚠️ Huge amount of data from multiple sources, more alerts

⚠️ Very difficult to find things that really matter

PEOPLE:

⚠️ Attrition rate, investing in people vs losing them

⚠️ Boring, repetitive tasks, no time for self-development

MONEY:

⚠️ Solutions designed for large teams, expensive, complicated, high TCO

⚠️ BAS, TIP – more than the annual budget

How do we help?

SECUREVISIO MISSION:

Simplify security operations and enable effective security risk management to help customers achieve cyber resilience.

How do we do it?

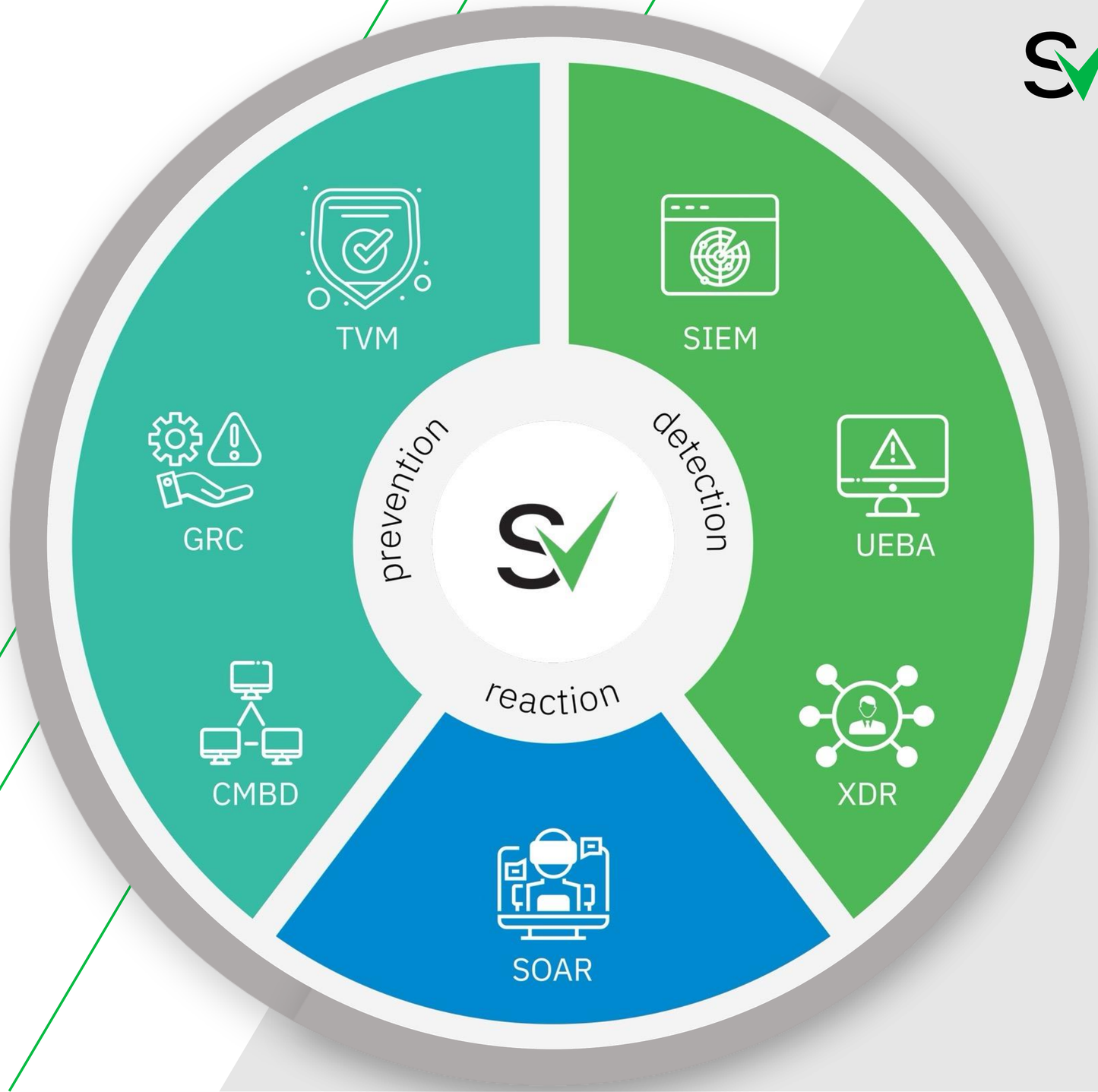
SECUREVISIO ARCHITECTURE COMPONENTS:

- ASSET MANAGEMENT/ CMDB
- IT GRC/ INTEGRATED RISK MANAGEMENT
- THREAT AND VULNERABILITY MANAGEMENT
- RISK-BASED SECURITY AND EVENT MANAGMENT
- USER AND ENTITY BEHAVIOUR ANALYSIS
- EXTENDED DETECTION AND RESPONSE
- SECURITY ORCHESTRATION AUTOMATION AND RESPONSE

One Console

Integrated cybersecurity platform for better prevention, detection & reaction with...

GDPR
ADD ON



Threat Intel Integration with SecureVisio

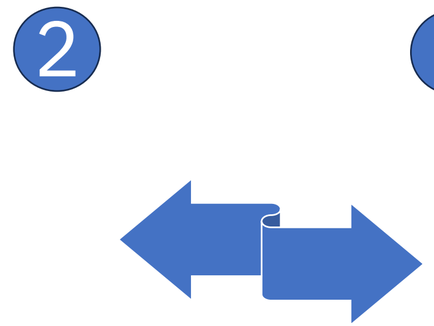
TIP
(Cyber Threat Intel Platform)

Using corporate context sent by SV for IOC feeds profiling

- Vulnerabilities
- Incidents
- Profiled information

Returning information toSecureVisio:

- Profiled and updated IOC feeds,
- TTPs (ie.: CVE)
- Potential incidents and vulnerabilities



SecureVisio™ **SIEM/SOAR**
(Security Management Platform)

Based on AutoDiscovery mechanism, content is sent to TI

Information about the organisation (IP/Domains/key words, services)

Feed consumption:

- Detection and response automation
- Prioritisation of actions

Simplicity and cost

- One console - one data-lake, reduced time to react, ease of use – people can spend more time on other tasks
- SV operates on infrastructures from 50 assets to 60k+ assets
- (Affordable) professional services can help you with implementation and training
- Thanks to one console, shortened implementation time
- Less time spent on integration thanks to one console

Flexibility of deployments

- Fully on premise implementations and operations – we understand that your data sometimes needs to stay inside. Plus MSSP model with multi – tenancy
- Cloud version soon available
- Hybrid models of implementation

USAGE OF AI IN THE SECUREVISIO PLATFORM

- Separate, scalable service (can be installed on selected servers and in different locations)
- Built in the solution and available through all the functional modules of the software (SIEM/UEBA/SOAR).
- Fully customizable
- Wide and fully controlled data range
- Automated sample selection for specific learning profiles – both user and asset related
- Automatically updated knowledge about the organisation
- Integration with external models i.e. Chat GPT, with full anonimisation suport
- Building our proprietary SLM (planned for 2025)

SV CAS (Cybersecurity Advanced Services)

Our expert cybersecurity team offers a comprehensive suite of advanced services to enhance your organization’s security posture.

- CTI – Cyber Threat Intelligence (feed and TIP) focused on EE related threats
- Threat Modelling and Risk Analysis
- Building Cyber Infrastructure
- Compliance Audits
- Cyber Excercises and Scenario-Based Trainings
- Full CTEM framework coverage

DON’T JUST TAKE OUR WORD FOR IT!

wodociągi warszawskie

CEDC

MASPEX

PKP ENERGETYKA

T-Mobile

PGNiG GRUPA ORLEN

OPI PIB

Ministerstwo Spraw Wewnętrznych i Administracji

MIASTO STOŁECZNE WARSZAWA

YGGDRASIL

POZnań

POLSKA GRUPA GÓRNICZA

e·on

PKO Bank Polski

TEM Electronic Components

Sąd Apelacyjny we Wrocławiu

TVP TELEWIZJA POLSKA

OEX E-BUSINESS eCOMMERCE LOGISTICS HUB

POLSKA AGENCJA ŻEGLUGI POWIETRZNEJ
POLISH AIR NAVIGATION SERVICES AGENCY

WOJEWÓDZTWO WARMIŃSKO-MAZURSKIE

TUI

ZARZĄD DRÓG MIEJSKICH

CEZ GROUP

DELPHARM

UMCS
UNIWERSYTET MARII CURIE-SKŁODOWSKIEJ W LUBLINIE

POLITECHNIKA LUBELSKA
LUBLIN UNIVERSITY OF TECHNOLOGY

secureVISIO

THANK YOU!

www.securevisio.com