sagenso

PREDICT.
REACT.
IMPROVE.

SYNERGY OF PEOPLE, KNOWLEDGE AND TECHNOLOGY

Effective cybersecurity systems

Get to know Telescope and CyberStudio

sagenso

Implementation and maintenance of an effective security management process throughout the entire organization

Sagenso creates tools that enable companies to implement and maintain an effective security management process throughout the entire organization. The developed solutions cover three main areas of risks, within which they analyze and identify any events potentially indicating an imminent threat.

Safety of:

✓	ICT infrastructure, IT services and client devices
✓	IT systems users
✓	IT services processes

Cybersecurity

Cybersecurity and protection of information asset are currently one of the most Important challenges for organizations around the world. In order to efficiently develop the IT risk management process and consequently effectively support the implementation of business goals, companies must approach the cybersecurity problem holistically, cross-sectionally and interdependently.

Holistically

At every decision-making and operational level the awareness of responsibility for safety should be developed.

Cross-sectionally

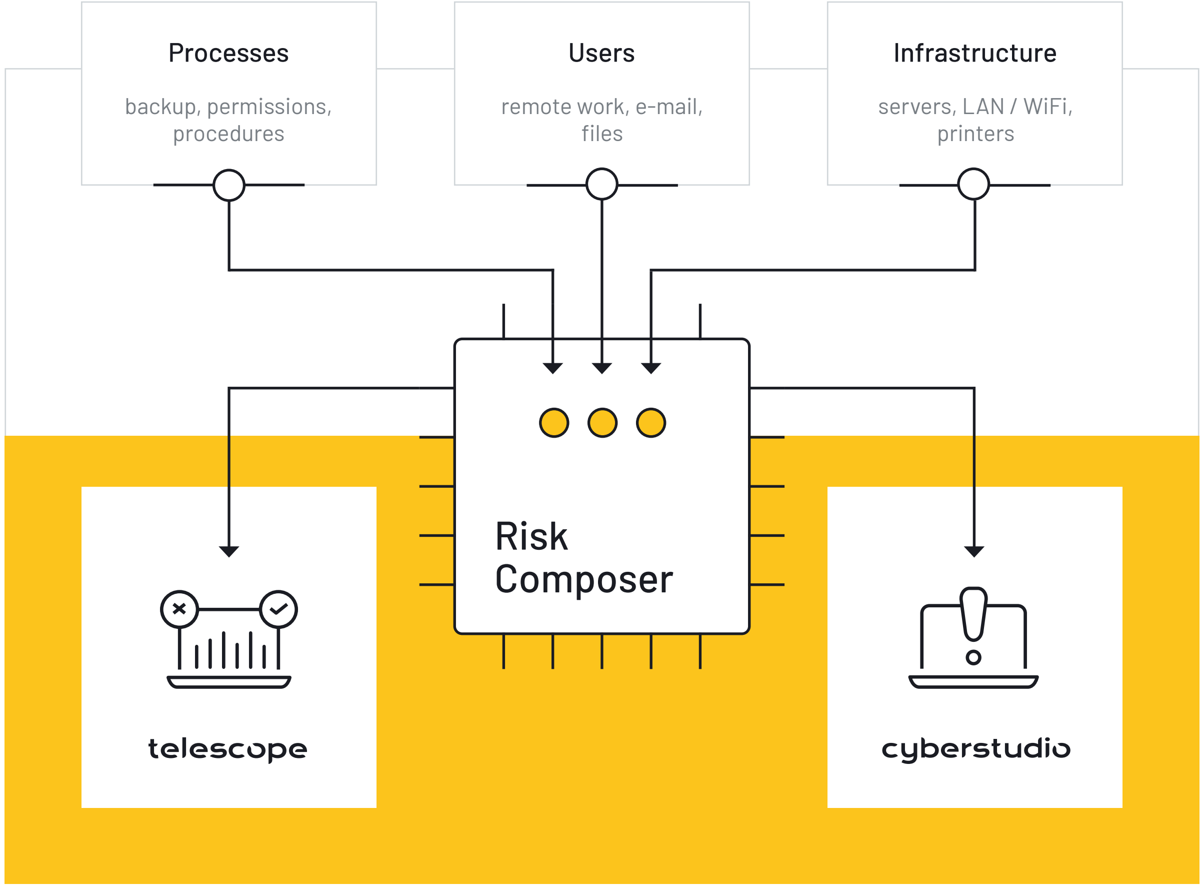
Security of IT services is not the domain of only the maintenance area but of every user in the company.

Interdependently

Business operations today are not possible without technology, and, on the other hand, technological investments should not be planned without a verified business need.

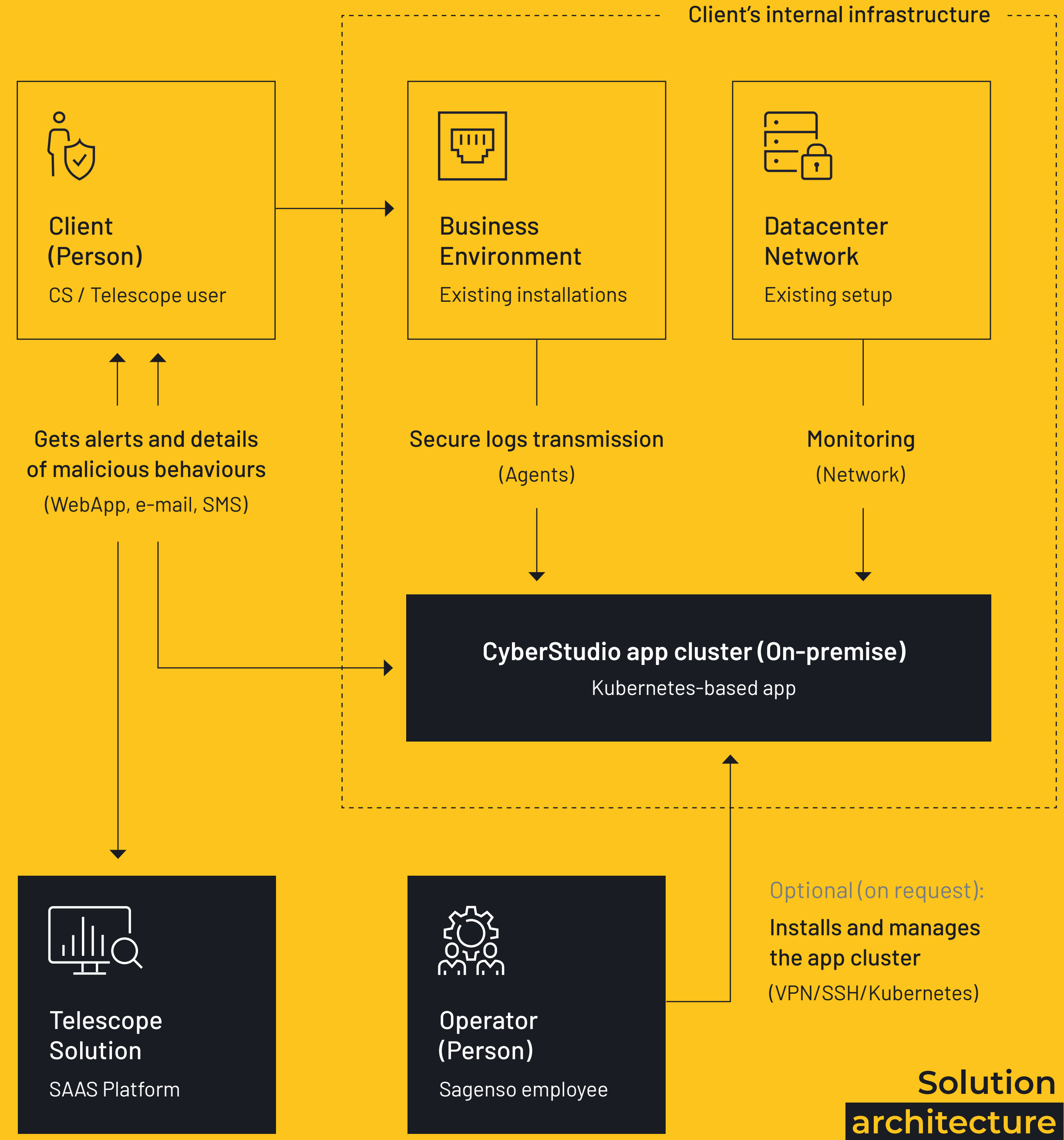
Risk Composer

Our solutions operate on the basis of proprietary **Risk Composer** technology, behind which are the algorithms responsible for continuous analysis of every aspect of security in your organization through the correlation of operational, process and technological events. **The results of the analytical process form the basis for the operation of Telescope and CyberStudio.**



Processes
backup, permissions, procedures
Users
remote work, e-mail, files
Infrastructure
servers, LAN / WiFi, printers
Risk Composer
telescope
cyberstudio

Solution architecture



Client's internal infrastructure

Client (Person)
CS / Telescope user

Business Environment
Existing installations

Datacenter Network
Existing setup

Gets alerts and details of malicious behaviours
(WebApp, e-mail, SMS)

Secure logs transmission
(Agents)

Monitoring
(Network)

CyberStudio app cluster (On-premise)
Kubernetes-based app

Telescope Solution
SAAS Platform

Operator (Person)
Sagenso employee

Optional (on request):
Installs and manages the app cluster
(VPN/SSH/Kubernetes)

#telescope

SECURITY AND OPERATIONAL CONTINUITY

Virtual manager in cybersecurity management

telescope

telescope

Telescope is a system that acts as a virtual manager in the area of cybersecurity management in your organization.

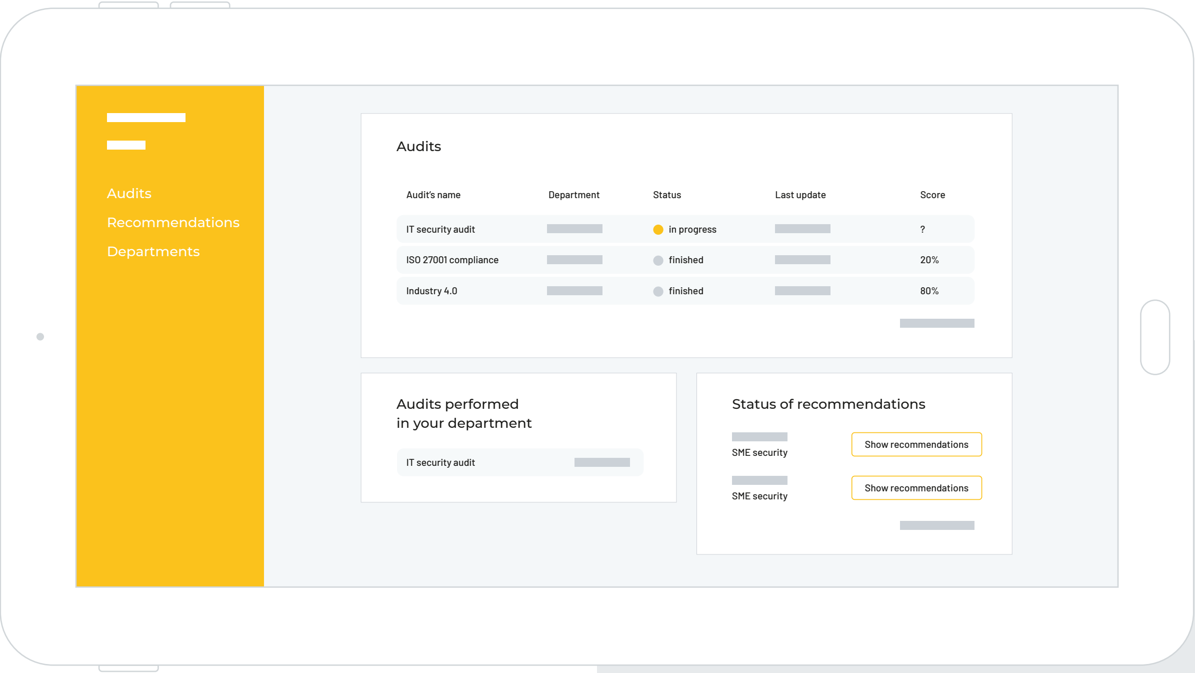
It independently conducts a dialogue with selected people going through every, often completely non-obvious issue necessary to ensure proper protection of IT services.

This system independently analyzes the practices and control mechanisms used by a given organization and in the case of irregularities, recommends proposals for process or operational improvements, which, after acceptance, will be monitored for implementation.

> Telescope will also be perfect in the role of virtual auditor.

Continuous audit process

The system is designed to recreate the real audit process to the best market architecture practices. Therefore, this process is an independent assessment of the level of security of IT services (e.g. external providers), which is required by formal and legal regulations (such as GDPR, NIS2), but will also be appreciated by the management team who care about showing due diligence in the development of their organization. **Everything in an automated, safe and objective way.**



Audits

Audit's name	Department	Status	Last update	Score
IT security audit		● in progress		?
ISO 27001 compliance		● finished		20%
Industry 4.0		● finished		80%

Audits performed in your department

IT security audit

Status of recommendations

SME security

SME security

Telescope provides not only effective protection, but also creates controlled conditions for uninterrupted business growth organization.

Telescope means:

- ✓ Automated assessment of the effectiveness of cybersecurity management practices.
- ✓ The RiskComposer module, which, analyzing potential irregularities in the area of technological risk management, will independently adjust the proposals for organizational improvements.
- ✓ Analytical module, applicable in maintaining the progress of the implementation of accepted recommendations.
- ✓ A supervisory module that will allow you to consciously create business decisions based on the map of technological threats.

#cyberstudio

NEXT-GEN
CYBERSECURITY
SOLUTIONS

Automating the process of detecting and removing threats

cyberstudio

cyberstudio

CyberStudio is an advanced system that automates the process of detecting and removing threats in the area of technological security.

Continuous monitoring of the status of IT services and all devices in the infrastructure allows you to identify any events indicating a potential threat. Then, depending on the situation, the system takes actions adapted to the type and scale of danger.

/ LEARN MORE

Familiarize yourself with the most important functionalities of the CyberStudio system ↓

Vulnerability management

Automation of the vulnerability management process is implemented on two levels. The first concerns the continuous scanning of the addressing available in the internal network in terms of identifying hosts with an unverified level of security, which are then analyzed in terms of active services, possible vulnerabilities. At this stage, the basic risk profile is also determined. The second level concerns detailed technological reconnaissance, analysis of service configuration and verification of compliance with the selected normative standard. Each observed vulnerability is covered by a classification process that takes into account, among others, the business function of a given server, CVE scoring or the fact of availability of tools enabling exploitation.

+ Common features of vulnerability management:

Monitoring of recurring vulnerabilities, i.e. those that were restored with the restoration of the system from a backup copy;

Monitoring the implementation of high-priority tasks;

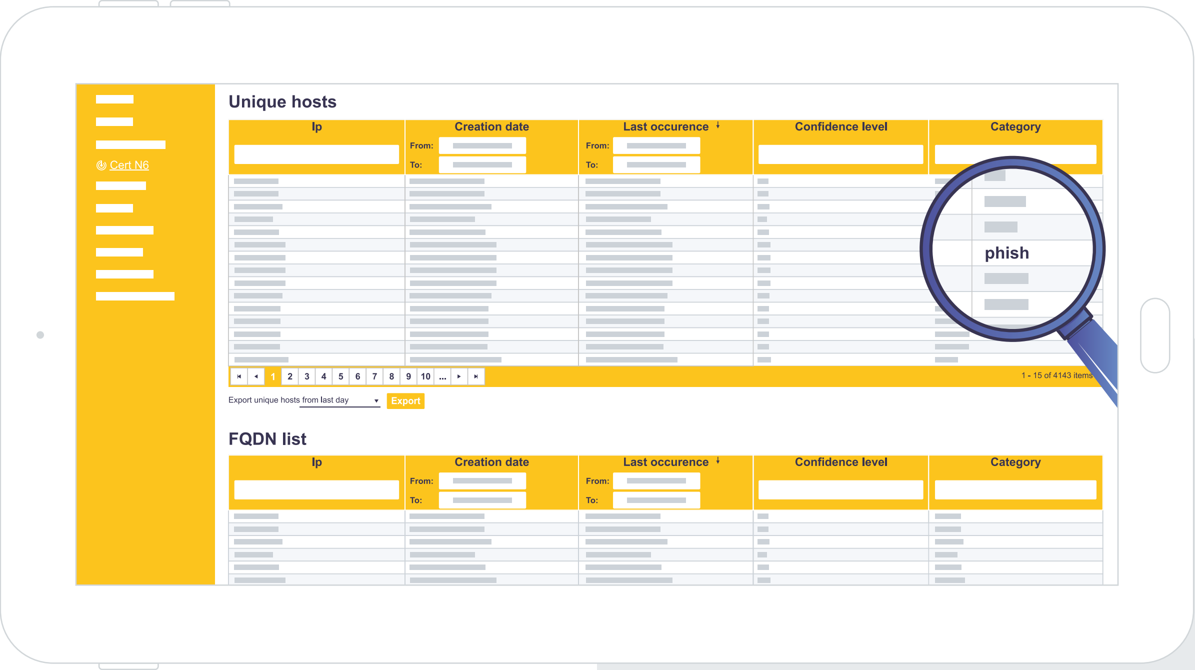
Monitoring the implementation of scans of IT infrastructure vulnerabilities;

Monitoring of vulnerabilities recommended for removal in the first place;

Monitoring of new vulnerabilities reported by public data sources in relation to services operating in the IT environment.

Protection of personal computers

Thanks to integration with **CERT, NASK N6 and MISP** platforms, the CyberStudio system has access to information about the latest attacks targeted at employees in your Organization. Even in the remote work model, outside the internal network environment, if a given user is subjected to an attempt to persuade to start a malicious website, the component of the CyberStudio system in the form of an agent installed in the operating system will stop communication and prevent further infection of the computer. Thus, it will protect your entire Organization.



Unique hosts

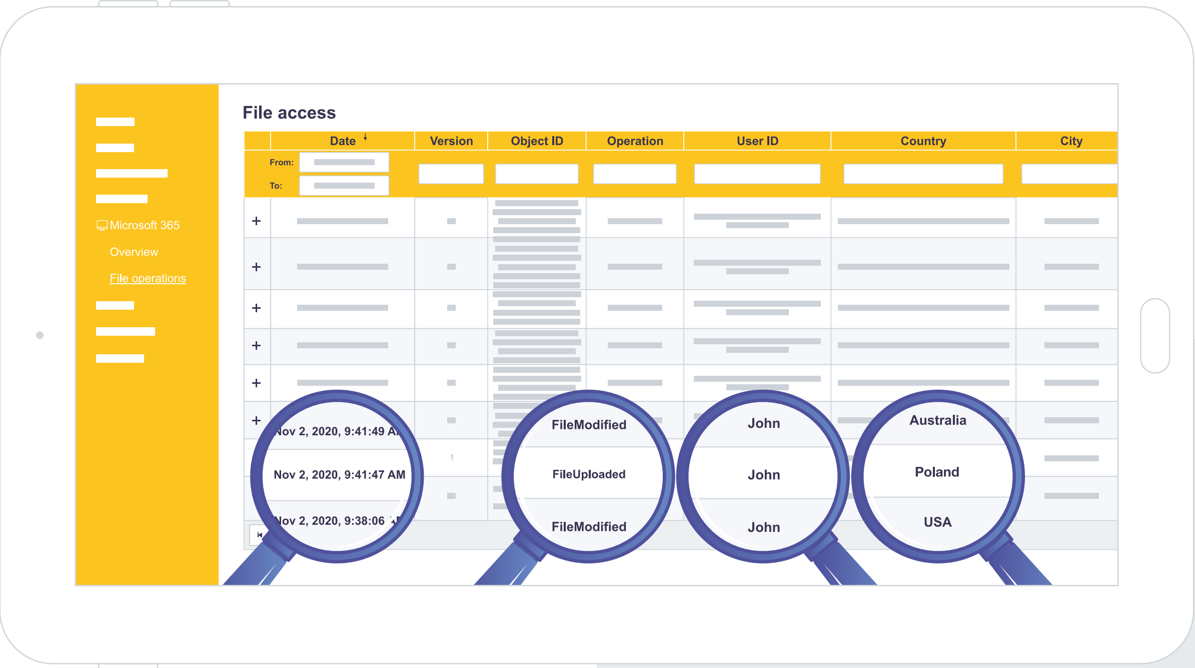
Ip	Creation date	Last occurence ↓	Confidence level	Category
	From: To:	From: To:		

FQDN list

Ip	Creation date	Last occurence ↓	Confidence level	Category
	From: To:	From: To:		

Insider Threat risks identification

Insider Threats occur when (intentionally or unintentionally) a user of IT systems becomes a threat in your organization. For example, when an account is taken over by an intruder and is used to retrieve any available information resources. This is done by analyzing and correlating the context of observed events in terms of user account activity and parameters such as the number of active sessions on the same login, types and sources of active sessions, device metadata, permissions, geolocation, activities on files and folders.

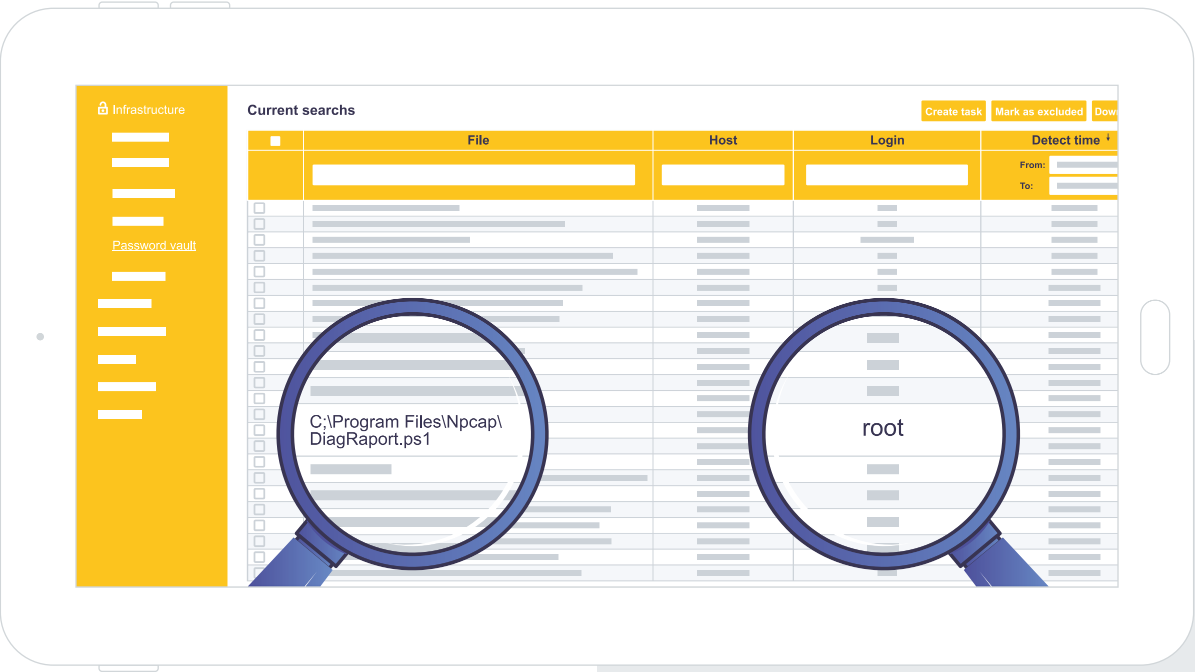


File access

	Date	Version	Object ID	Operation	User ID	Country	City
	From: To:						
+							
+							
+							
+							
+							
+	Nov 2, 2020, 9:41:49 A			FileModified	John	Australia	
	Nov 2, 2020, 9:41:47 AM	1		FileUploaded	John	Poland	
	Nov 2, 2020, 9:38:06			FileModified	John	USA	

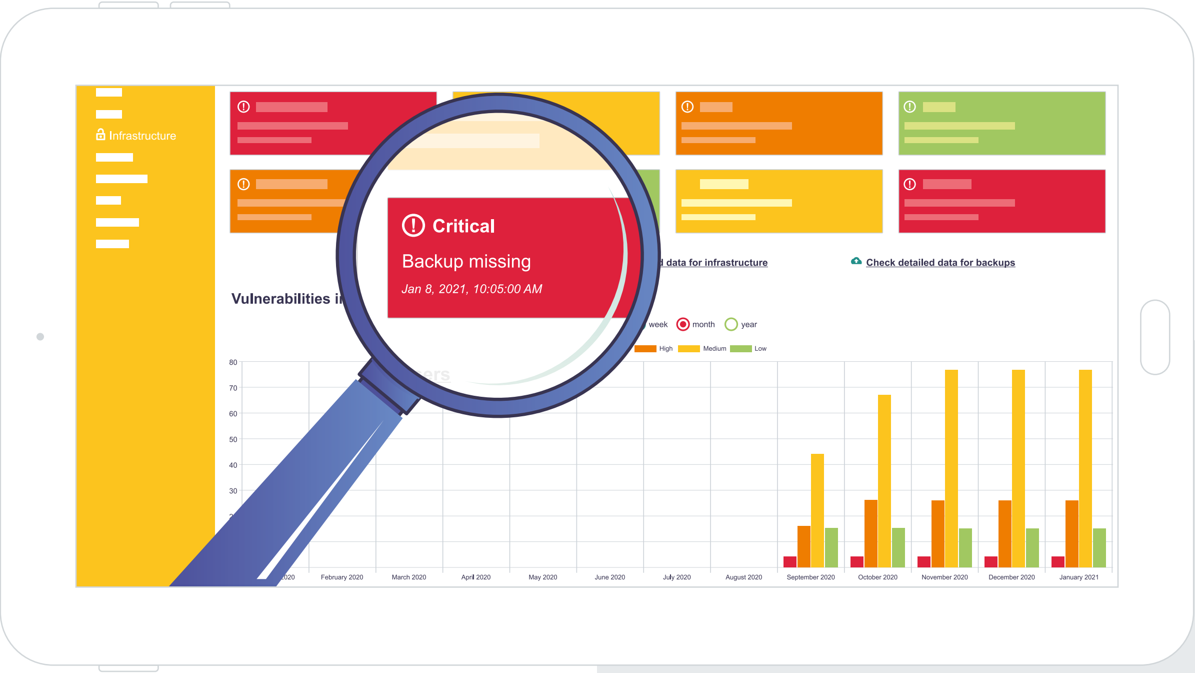
Password Leaks

As part of this functionality, IT administrators receive a **tool to identify any potential scripts, in whose credentials are written explicitly**. This allows you to maintain constant supervision over the security measures of privileged accounts, as well as data processing procedures dependent on them, the failure of which may threaten the operational continuity of IT services. This module provides information about the disclosed data leak files, which included the logins of the Organization's employees. **Thanks to the above, the risk of taking over employee accounts and thus unauthorized access to sensitive data is minimized**.



Backup management

Functionality fundamental for the protection of your organization. **The CyberStudio system will verify and, if necessary, propose improvements in the practices of generating and maintaining usable backup copies.** In addition, as part of technological monitoring, the CyberStudio system will verify whether subsequent archives are created in accordance with the planned schedule.



Critical

Backup missing

Jan 8, 2021, 10:05:00 AM

Task management module

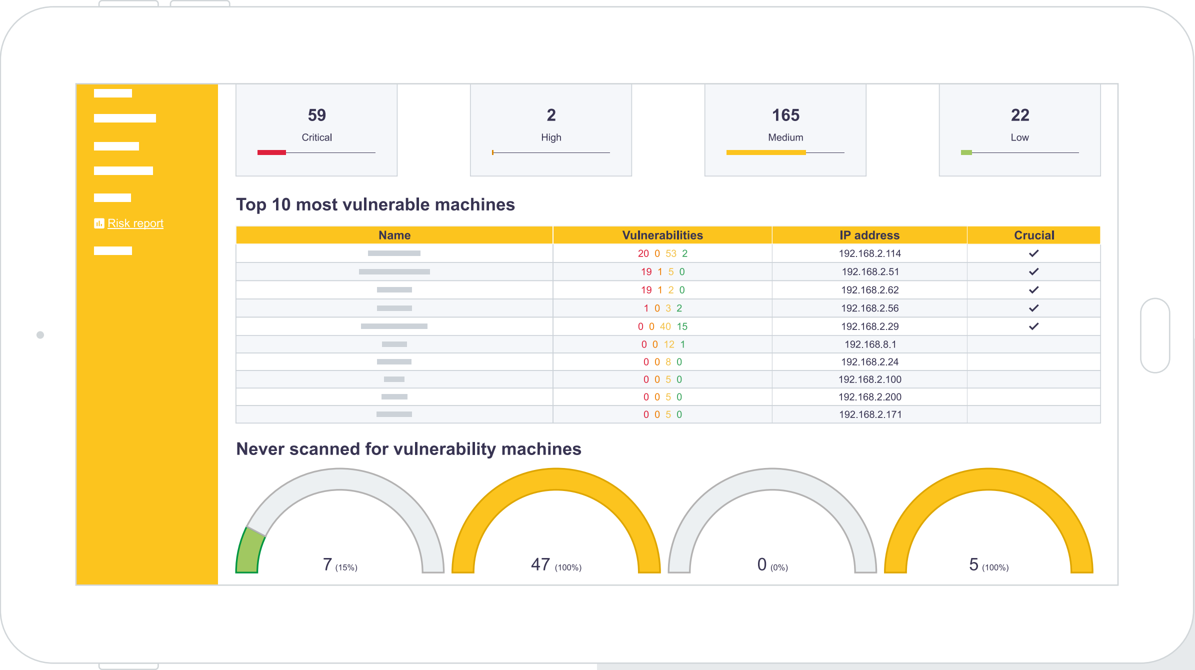
Module whose main application is to **maintain continuity in the process of managing technological vulnerabilities by automating routine activities required to ensure the security of your Organization**. Designed similarly to other leading ServiceDesk-type systems, it will support roles responsible for maintaining IT infrastructure in the organization of tasks and the implementation of technological improvements. In addition, this module has been strengthened with logic monitoring the implementation of operational activities required by the practices used in your organization.

Example

If the critical vulnerability data is not removed within a given time or there is no new information about the security status of the IT infrastructure, an automatic process of raising observations to subsequent people in the Organization's structures will be launched. An important feature of this functionality is that with the next step of providing information about potential irregularities, the system transforms them from a deeply technological perspective into a process and business perspective. Each person involved in the process of ensuring security in the Organization will be able to precisely understand the essence of the observation and the further way of addressing it.

Reporting module

Reporting module, on your preferred time, summarizes the most important information about quantity and scale of vulnerability of the IT environment, the risk profile of the most vulnerable hosts or even the time-consuming nature that the entire process of implementing improvements consumes. **Maintaining the up-to-date state of knowledge about the level of technological security and potential threats is necessary to ensure proper protection** of your organization, but also to enable controlled business growth.



59 Critical

2 High

165 Medium

22 Low

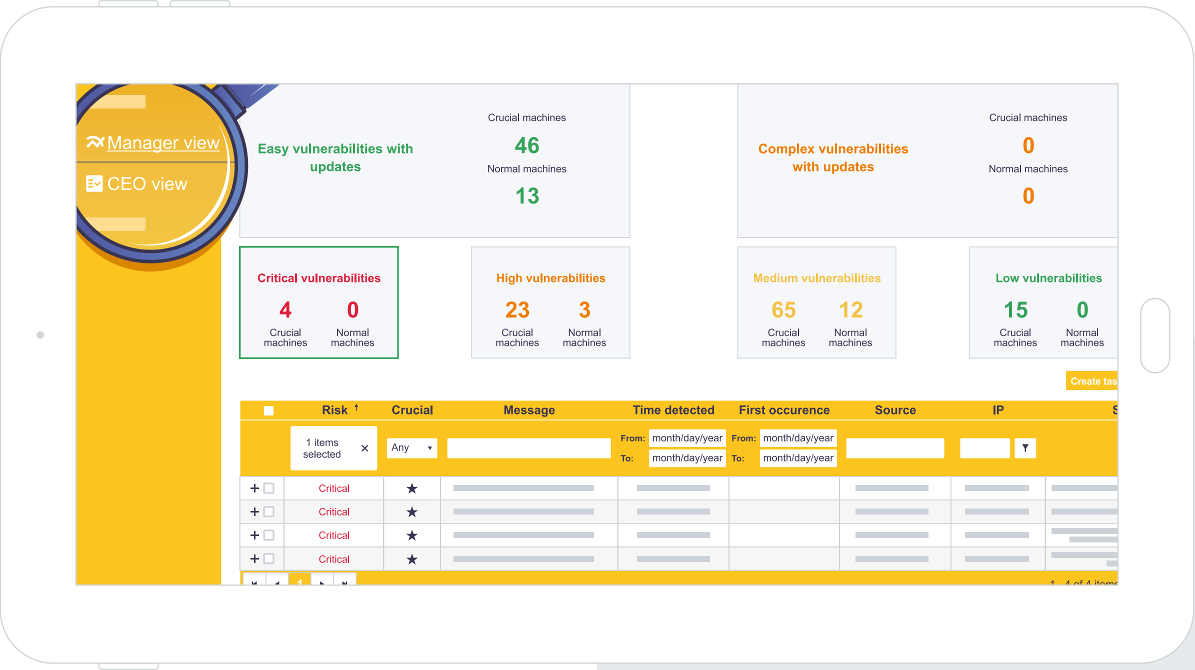
Top 10 most vulnerable machines

Name	Vulnerabilities	IP address	Crucial
	20 0 53 2	192.168.2.114	✓
	19 1 5 0	192.168.2.51	✓
	19 1 2 0	192.168.2.62	✓
	1 0 3 2	192.168.2.56	✓
	0 0 40 15	192.168.2.29	✓
	0 0 12 1	192.168.8.1	
	0 0 8 0	192.168.2.24	
	0 0 5 0	192.168.2.100	
	0 0 5 0	192.168.2.200	
	0 0 5 0	192.168.2.171	

Never scanned for vulnerability machines

Predefined user profiles

IT security has a business nature and in many areas goes beyond the technological layer. This makes the involvement of the management staff in the process of improving the entire Organization crucial. Among the basic profiles, we can distinguish a role directly responsible for the administration and implementation of technological improvements (e.g. Administrator, IT service provider), an organizational role responsible for the IT area (e.g. IT Manager), the role of a business owner (e.g. Management team). **Each of the predefined roles is characterized by a different scope of presented information and the scope of permissions in the parameterization of the CyberStudio system.**



Easy vulnerabilities with updates — Crucial machines 46, Normal machines 13

Complex vulnerabilities with updates — Crucial machines 0, Normal machines 0

Critical vulnerabilities — 4 Crucial machines, 0 Normal machines

High vulnerabilities — 23 Crucial machines, 3 Normal machines

Medium vulnerabilities — 65 Crucial machines, 12 Normal machines

Low vulnerabilities — 15 Crucial machines, 0 Normal machines

□	Risk ↑	Crucial	Message	Time detected	First occurence	Source	IP	S
	1 items selected ×	Any ▾		From: month/day/year To: month/day/year	From: month/day/year To: month/day/year			
+ □	Critical	★						
+ □	Critical	★						
+ □	Critical	★						
+ □	Critical	★						

Management information module

CyberStudio Solution **automatically monitors and reports key performance indicators** of processes in the cybersecurity management area.

Indicators include, among others:

- A high-priority hazard status;
- Efficiency of tasks;
- Backup status;
- IT infrastructure security level status;
- Effectiveness of the process of removing technological threats (vulnerabilities).

It is enough to once determine the values adapted to the business characteristics of the Organization to have **constant access to information** presenting whether all control mechanisms work effectively.

See the difference

	Before Prevention			During Monitoring			After Minimizing the effects of an attack		
	Analysis	Improvements recommendations	Solution implementation	Incidents monitoring	Incident reaction	Repair plan	Consultations with experts	Minimizing the effects of the incident	Updates to the strategic plan
IT INFRASTRUCTURE									
Sagenso	✓	✓	✓	✓	✓	✓	✓	✓	✓
Antywirus	✗	✓	✗	✓	✓	✓	✗	✗	✗
Firewall	✓	✓	✗	✓	✓	✗	✗	✗	✗
SIEM	✓	✓	✗	✓	✗	✗	✗	✗	✗
SOC	✓	✓	✓	✓	✓	✓	✓	✓	✓
IT SECURITY MANAGEMENT									
Sagenso	✓	✓	✓	✓	✓	✓	✓	✓	✓
Antywirus	✗	✗	✗	✗	✗	✗	✗	✗	✗
Firewall	✗	✗	✗	✗	✗	✗	✗	✗	✗
SIEM	✗	✗	✗	✗	✗	✗	✗	✗	✗
SOC	✗	✗	✗	✗	✗	✗	✗	✗	✗

sagenso

cyberstudio telescope

Warsaw	Varso II, Chmielna 73
Rzeszów	Pl. Jana Kilińskiego 2

SECURITY
IS YOUR
CHOICE

Contact us

phone:	+48 509 191 862
email:	kontakt@sagenso.com

sagenso.com