sagenso

PREDICT.
REACT.
IMPROVE.

SYNERGIA
LUDZI, WIEDZY
I TECHNOLOGII

Skuteczne systemy cyberbezpieczeństwa

Poznaj Telescope i CyberStudio

sagenso

Wdrożenie i utrzymanie efektywnego procesu zarządzania bezpieczeństwem w całej organizacji

Sagenso tworzy narzędzia, które umożliwiające firmom wdrożenie i utrzymanie efektywnego procesu zarządzania bezpieczeństwem w całej organizacji. Opracowane rozwiązania pokrywają trzy główne obszary ryzyka, w ramach których analizują oraz identyfikują wszelkie zdarzenia potencjalnie świadczące o nadchodzącym zagrożeniu.

Bezpieczeństwo w zakresie:

✓	infrastruktury teleinformatycznej, usług IT oraz urządzeń klienckich
✓	użytkowników systemów informatycznych
✓	procesów w obszarze usług IT

Cyberbezpieczeństwo

Zagadnienia związane z cyberbezpieczeństwem i ochroną zasobów informacyjnych stanowią obecnie jedno z najważniejszych wyzwań dla organizacji na całym świecie. Aby skutecznie budować proces zarządzania ryzykiem w IT i tym samym, skutecznie wspierać realizację celów biznesowych, firmy muszą traktować problem cyberbezpieczeństwa holistycznie, przekrojowo i współzależnie.

Holistycznie

Odpowiedzialność za bezpieczeństwo powinna być świadomością rozwijaną na każdym szczeblu decyzyjnym i operacyjnym.

Przekrojowo

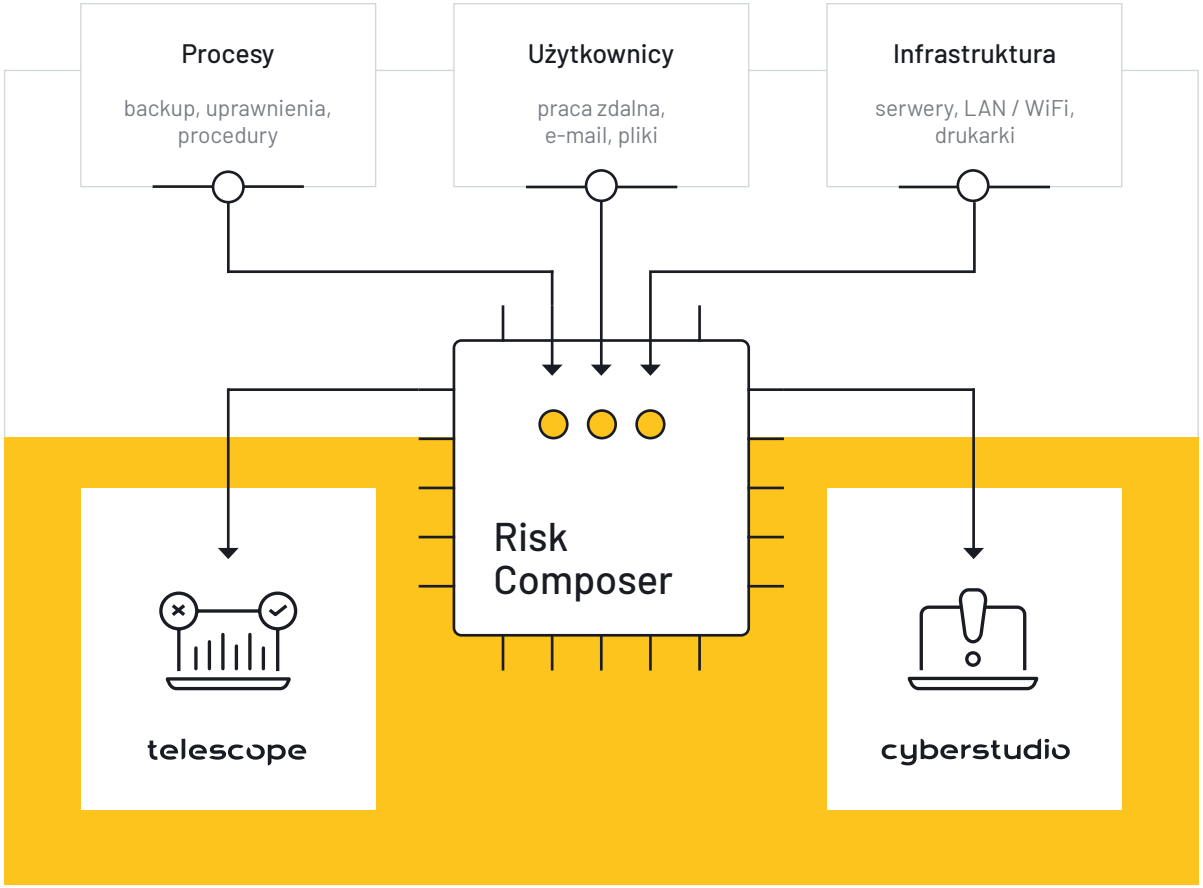
Bezpieczeństwo usług IT nie jest domeną tylko obszaru utrzymania lecz każdego użytkownika w firmie.

Współzależnie

Operacje biznesowe nie są dzisiaj możliwe bez udziału technologii, a z drugiej strony nie powinno się planować inwestycji technologicznych bez zweryfikowanej potrzeby biznesowej.

Risk Composer

Nasze rozwiązania działają w oparciu o autorską technologię **Risk Composer**, za którą stoją algorytmy odpowiadające za ciągłą analizę każdego aspektu bezpieczeństwa w Twojej Organizacji poprzez korelację zdarzeń operacyjnych, procesowych i technologicznych. **Wyniki procesu analitycznego stanowią podstawę do działania Telescope i CyberStudio.**



Architektura rozwiązań

BEZPIECZEŃSTWO I CIĄGŁOŚĆ OPERACYJNA

Wirtualny manager w obszarze zarządzania cyberbezpieczeństwem

telescope

telescope

Telescope to system, który pełni rolę wirtualnego managera w obszarze zarządzania cyberbezpieczeństwem Twojej Organizacji.

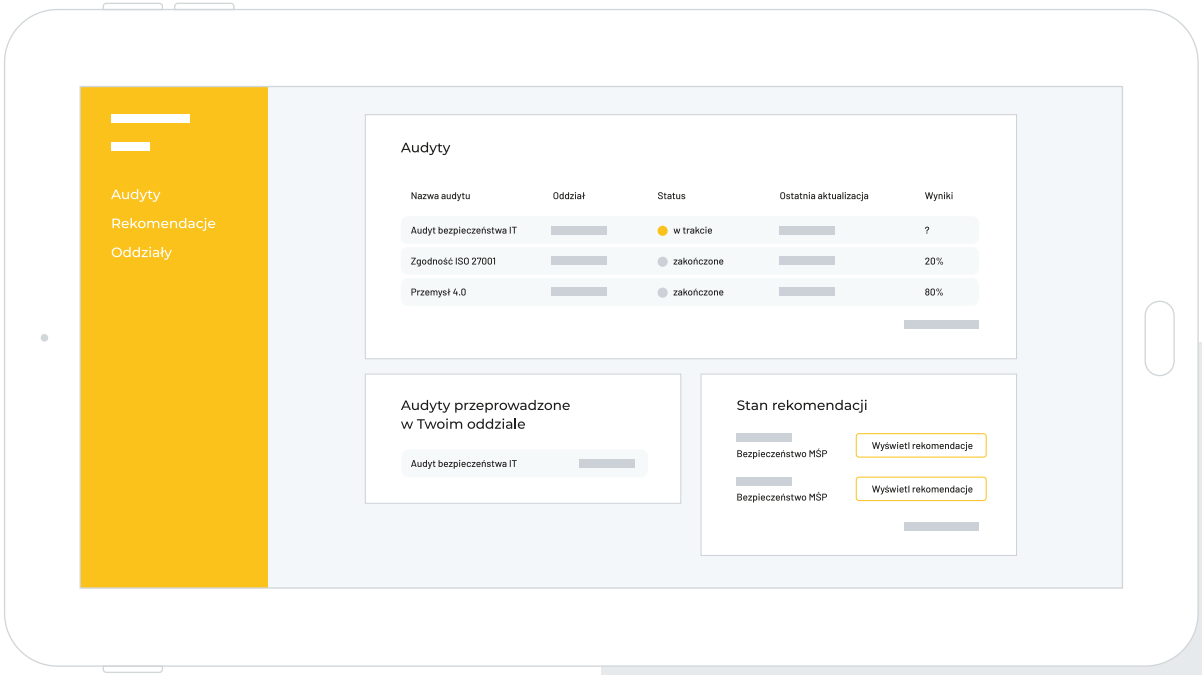
Samodzielnie poprowadzi dialog z wybranymi osobami przechodząc przez wszystkie, często zupełnie nieoczywiste zagadnienia konieczne do zapewnienia właściwej ochrony usług IT.

System ten samodzielnie analizuje praktyki oraz mechanizmy kontrolne stosowane przez daną organizację i w przypadku zanotowanych nieprawidłowości, rekomenduje gotowe propozycje usprawnień procesowych lub operacyjnych, które po zaakceptowaniu będą monitorowane pod kątem realizacji.

> **Telescope doskonale sprawdzi się także w roli wirtualnego audytora.**

Proces ciągłego audytu

System został zaprojektowany w taki sposób, aby odwzorowywać realny proces audytowy w architekturze najlepszych praktyk rynkowych. W związku z powyższym, proces ten ma charakter niezależnej oceny poziomu bezpieczeństwa usług IT (np. dostawców zewnętrznych), która wymagana jest przez regulacje formalno-prawne (jak np. RODO, NIS2), ale także będzie doceniona przez kadrę zarządzającą dbającą o wykazywanie należytej staranności w rozwoju swojej organizacji. **Wszystko w sposób zautomatyzowany, bezpieczny i obiektywny.**



Telescope to nie tylko skuteczna ochrona, ale także tworzenie kontrolowanych warunków do niezakłóconego wzrostu biznesowego organizacji.

Telescope to:

- ✓ Zautomatyzowana ocena skuteczności praktyk w obszarze zarządzania cyberbezpieczeństwem.
- ✓ Moduł RiskComposer, który analizując potencjalne nieprawidłowości w zakresie zarządzania ryzykiem technologicznym samodzielnie dopasuje propozycje usprawnień organizacyjnych.
- ✓ Moduł analityczny, mający swoje zastosowanie w utrzymywaniu postępu realizacji zaakceptowanych rekomendacji.
- ✓ Moduł nadzorczy, który pozwoli świadomie kreować decyzje biznesowe w oparciu o mapę zagrożeń technologicznych.

NEXT-GEN
CYBERSECURITY
SOLUTIONS

Automatyzacja procesu detekcji i usuwania zagrożeń

cyberstudio

cyberstudio

CyberStudio to zaawansowany system automatyzujący proces detekcji i usuwania zagrożeń w obszarze bezpieczeństwa technologicznego.

Stały monitoring stanu usług IT oraz wszystkich urządzeń w infrastrukturze pozwala na identyfikację wszelkich zdarzeń wskazujących na potencjalne zagrożenie. Następnie, w zależności od zaistniałej sytuacji, system podejmuje działania dostosowane do typu oraz skali niebiezpieczeństwa.

/ DOWIEDZ SIĘ WIĘCEJ

Zapoznaj się z najważniejszymi funkcjonalnościami systemu CyberStudio

Zarządzanie podatnością

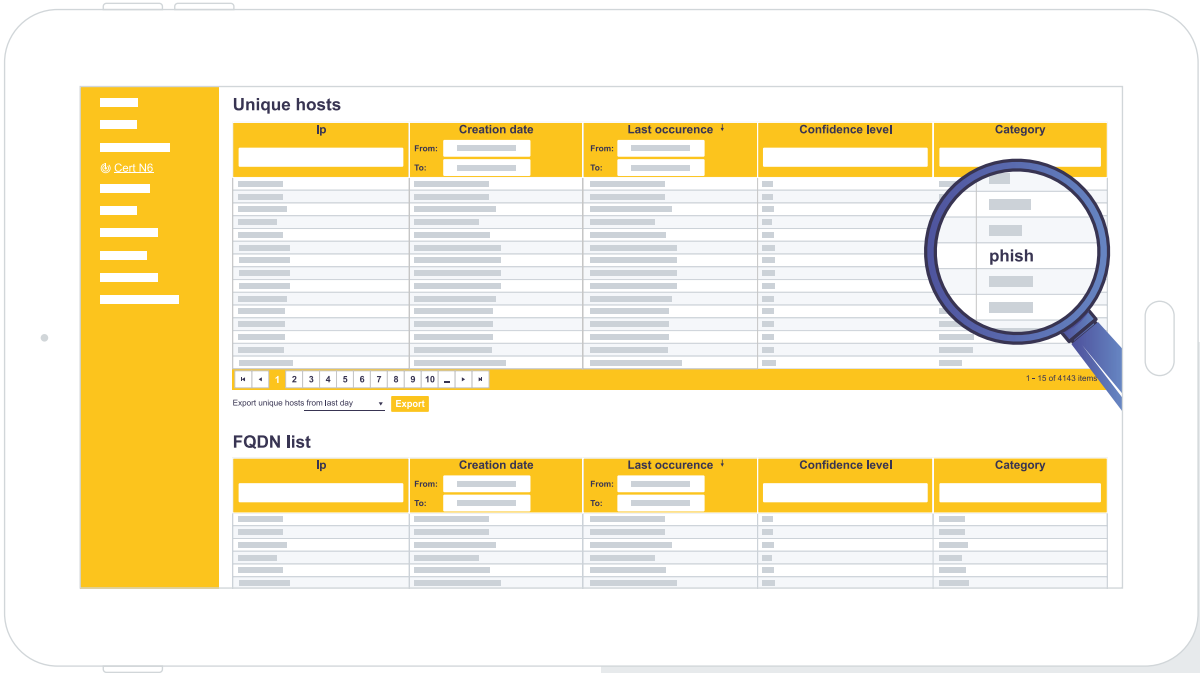
Automatyzacja procesu zarządzania podatnością realizowana jest na dwóch płaszczyznach. Pierwsza dotyczy ciągłego skanowania adresacji dostępnej w sieci wewnętrznej pod kątem identyfikacji hostów z niezweryfikowanym poziomem bezpieczeństwa, które następnie poddawane zostają analizie aktywnych usług, możliwych rozwiązań. Na tym etapie określany jest także podstawowy profil ryzyka. Druga płaszczyzna dotyczy szczegółowego rozpoznania technologicznego, analizy konfiguracji usług i weryfikacji zgodności z wybranym standardem normatywnym. Każda zaobserwowana podatność zostaje objęta procesem klasyfikacji, która uwzględnia m.in. funkcję biznesową danego serwera, punktację CVE czy fakt dostępności narzędzi umożliwiających eksploatację.

Wspólne cechy zarządzania podatnością:

- Monitoring powracających podatności, tj. takich, które zostały przywrócone wraz z odtworzeniem systemu z kopii bezpieczeństwa;
- Monitoring realizacji zadań o wysokim priorytecie;
- Monitoring realizacji skanów podatności infrastruktury IT;
- Monitoring podatności rekomendowanych do usunięcia w pierwszej kolejności;
- Monitoring nowych podatności zgłaszanych przez publiczne źródła danych względem usług funkcjonujących w środowisku informatycznym.

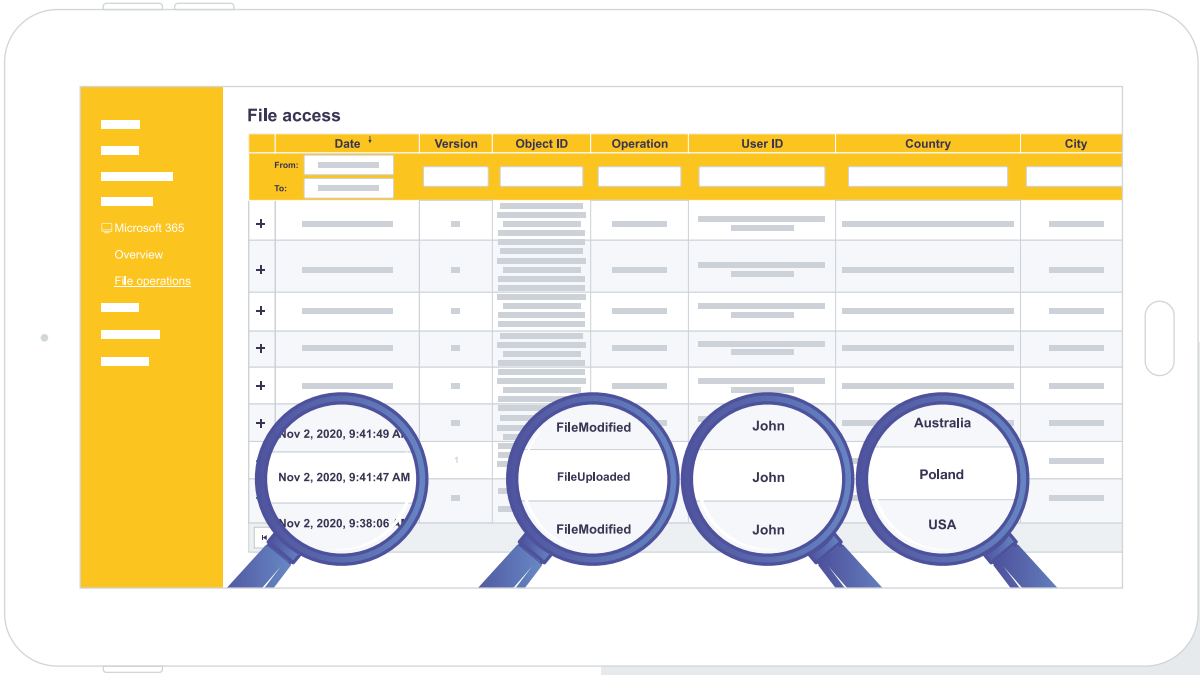
Ochrona komputerów osobistych

Dzięki integracji z platformami **CERT, NASK N6 oraz MISP,** system CyberStudio ma dostęp do informacji o najnowszych atakach kierowanych na pracowników w Twojej Organizacji. Nawet w modelu pracy zdalnej, poza środowiskiem sieci wewnętrznej, jeśli dany użytkownik zostanie poddany próbie nakłonienia do uruchomienia szkodliwej strony internetowej to komponent systemu CyberStudio w postaci agenta instalowanego w systemie operacyjnym zatrzyma komunikację i nie dopuści do dalszej infekcji komputera. Tym samym, ochroni całą Twoją Organizację.



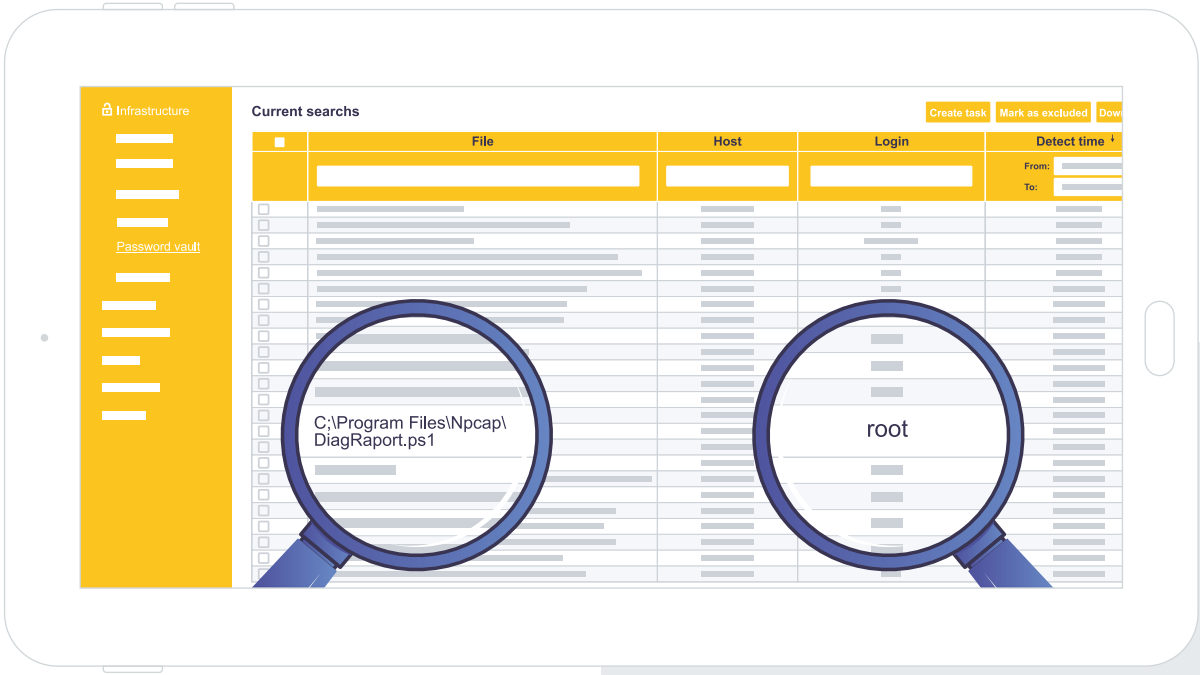
Identyfikacja zagrożeń Insider Threat

Niebezpieczeństwa Insider Threat mają miejsce, gdy (intencjonalnie lub nieintencjonalnie) zagrożeniem staje się użytkownik systemów IT w Twojej organizacji. Na przykład, gdy konto zostaje przejęte przez intruza i zostaje wykorzystane do pobierania wszelkich dostępnych zasobów informacyjnych. Identyfikacja jest realizowana poprzez analizowanie i korelowanie kontekstu zdarzeń obserwowanych w zakresie aktywności kont użytkowników oraz parametrów takich jak np. ilość aktywnych sesji na tym samym loginie, typy oraz źródła aktywnych sesji, metadane urządzeń, uprawnienia, geolokalizacja, aktywności na plikach i folderach.



Password Leaks

W ramach tej funkcjonalności, administratorzy IT otrzymują **narzędzie identyfikujące wszelkie potencjalne skrypty, w których są zapisane dane uwierzytelniające w sposób jawny**. Pozwala to na utrzymanie stałego nadzoru nad środkami bezpieczeństwa kont uprzywilejowanych, a także zależnymi od nich procesami przetwarzania danych, których awaria może zagrozić ciągłości operacyjnej usług IT. Moduł ten dostarcza informację o ujawnionych zbiorach wycieków danych, w których znalazły się loginy pracowników Organizacji. **Dzięki powyższemu, minimalizuje się ryzyko przejęcia kont pracowniczych i tym samym, nieautoryzowanego dostępu do danych wrażliwych**.



Zarządzanie kopiami bezpieczeństwa

Funkcjonalność stanowiąca fundament ochrony Twojej Organizacji. **System CyberStudio zweryfikuje, i jeśli będzie to konieczne, zaproponuje usprawnienia w praktykach generowania i utrzymywania zdatnych do użytku kopii bezpieczeństwa**. Dodatkowo, w ramach monitoringu technologicznego, system CyberStudio będzie weryfikował czy kolejne archiwa powstają zgodnie z zaplanowaną systematyką.

Moduł Task Management

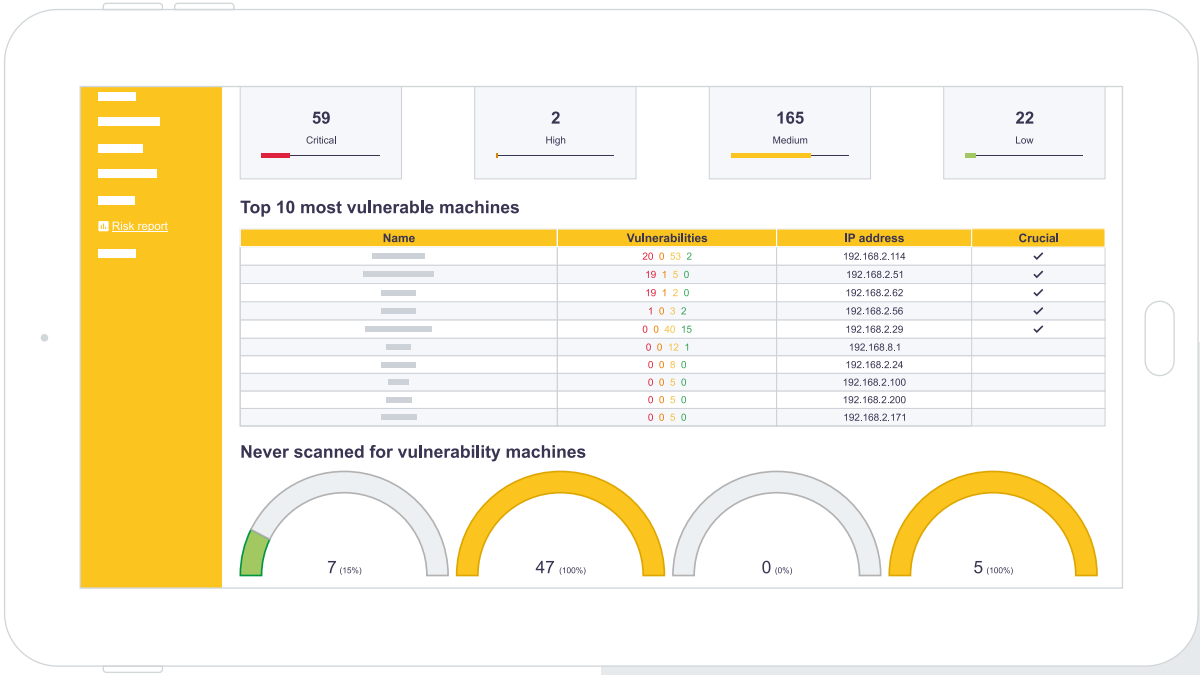
Moduł, którego głównym zastosowaniem jest **utrzymanie ciągłości w procesie zarządzania podatnością technologiczną przez zautomatyzowanie rutynowych czynności wymaganych do zapewnienia bezpieczeństwa Twojej Organizacji**. Zaprojektowany w podobieństwie do innych wiodących systemów typu ServiceDesk, będzie wspierał role odpowiedzialne za utrzymanie infrastruktury IT w organizacji zadań i implementowaniu usprawnień technologicznych. Dodatkowo, moduł ten został wzmocniony logiką monitorującą realizację czynności operacyjnych wymaganych przez praktyki stosowane w Twojej Organizacji.

Przykład

Jeśli dane podatności krytyczne nie zostaną usunięte w zadanym czasie lub nie pojawi się nowa informacja o stanie bezpieczeństwa infrastruktury IT, uruchomiony zostanie automatyczny proces podnoszenia obserwacji do kolejnych osób w strukturach Organizacji. Istotną cechą tej funkcjonalności jest to, że wraz z kolejnym krokiem przekazywania informacji o potencjalnych nieprawidłowościach, system przekształca je z perspektywy głęboko technologicznej na perspektywę procesową i biznesową. Każda osoba zaangażowana w proces zapewnienia bezpieczeństwa w Organizacji będzie mogła precyzyjnie zrozumieć istotę obserwacji oraz dalszy sposób jej adresowania.

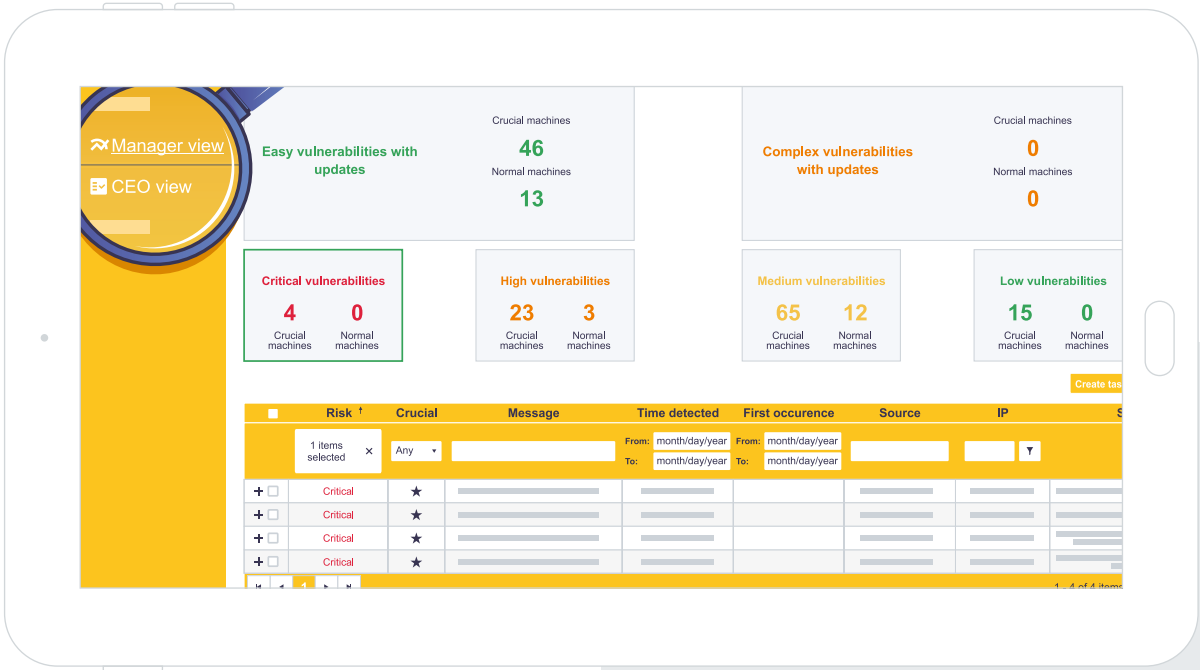
Moduł raportowy

Moduł raportowy, który w wybranym przez Ciebie czasie podsumuje najistotniejsze informacje o ilości i skali podatności środowiska IT, profilu ryzyk najbardziej zagrożonych hostów czy nawet czasochłonności jaką cały proces wdrażania usprawnień pochłania. **Utrzymanie aktualnego stanu wiedzy o poziomie bezpieczeństwa technologicznego oraz potencjalnych zagrożeniach jest niezbędne do zapewnienia właściwej ochrony** Twojej Organizacji, ale także do umożliwienia kontrolowanego wzrostu biznesowego.



Predefiniowane profile użytkowników

Bezpieczeństwo IT ma wymiar biznesowy, a w wielu obszarach wykracza poza warstwę technologiczną. To sprawia, że zaangażowanie kadry kierowniczej w proces doskonalenia całej Organizacji jest kluczowy. Wśród podstawowych profili możemy wyróżnić rolę bezpośrednio odpowiedzialną za administrację i wdrażanie usprawnień technologicznych (np. Administrator, dostawca usług IT), rolę organizacyjnie odpowiedzialną za obszar IT (np. Kierownik IT), rolę właściciela biznesowego (np. Zarząd). **Każda z predefiniowanych ról charakteryzuje się innym zakresem prezentowanych informacji oraz zakresem uprawnień w parametryzacji systemu CyberStudio**.



Moduł informacji zarządczej

Rozwiązanie CyberStudio **automatycznie monitoruje i raportuje wskaźniki efektywności** procesów w obszarze zarządzania cyberbezpieczeństwem.

Wskaźniki obejmują, m.in.:

- Stan zagrożeń o charakterystyce wysokiego priorytetu;
- Efektywność realizacji zadań;
- Stan kopii bezpieczeństwa;
- Status poziomu bezpieczeństwa infrastruktury IT;
- Efektywność procesu usuwania zagrożeń technologicznych (np. podatności).

Wystarczy raz określić wartości dostosowane do charakterystyki biznesowej Organizacji by mieć **stały dostęp do informacji** prezentującej czy wszystkie mechanizmy kontrolne działają efektywnie.

Zobacz różnicę

	Przed – Prewencja			W trakcie – Monitorowanie			Po – Minimalizowanie skutków ataku		
	Analiza	Rekomendacje usprawnień	Implementacja rozwiązań	Monitoring incydentów	Reagowanie na incydent	Plan naprawczy	Konsultacje z ekspertami	Ograniczenie skutków incydentu	Aktualizacja planu strategicznego
INFRASTRUKTURA IT									
Sagenso	✓	✓	✓	✓	✓	✓	✓	✓	✓
Antywirus	✗	✓	✗	✓	✓	✓	✗	✗	✗
Firewall	✓	✓	✗	✓	✓	✗	✗	✗	✗
SIEM	✓	✓	✗	✓	✗	✗	✗	✗	✗
SOC	✓	✓	✓	✓	✓	✓	✓	✓	✓
ZARZĄDZANIE BEZPIECZEŃSTWEM IT									
Sagenso	✓	✓	✓	✓	✓	✓	✓	✓	✓
Antywirus	✗	✗	✗	✗	✗	✗	✗	✗	✗
Firewall	✗	✗	✗	✗	✗	✗	✗	✗	✗
SIEM	✗	✗	✗	✗	✗	✗	✗	✗	✗
SOC	✗	✗	✗	✗	✗	✗	✗	✗	✗