OpenBIZ

http://www.openbiz.pl

TENABLE SECURITY CENTER CONTINUOUS VIEW

KOMPLEKSOWY POMIAR RYZYKA W SYSTEMACH I SIECIACH.

Główne zagrożenia

Dla sieci i systemów

Ignorowanie zaleceń i norm

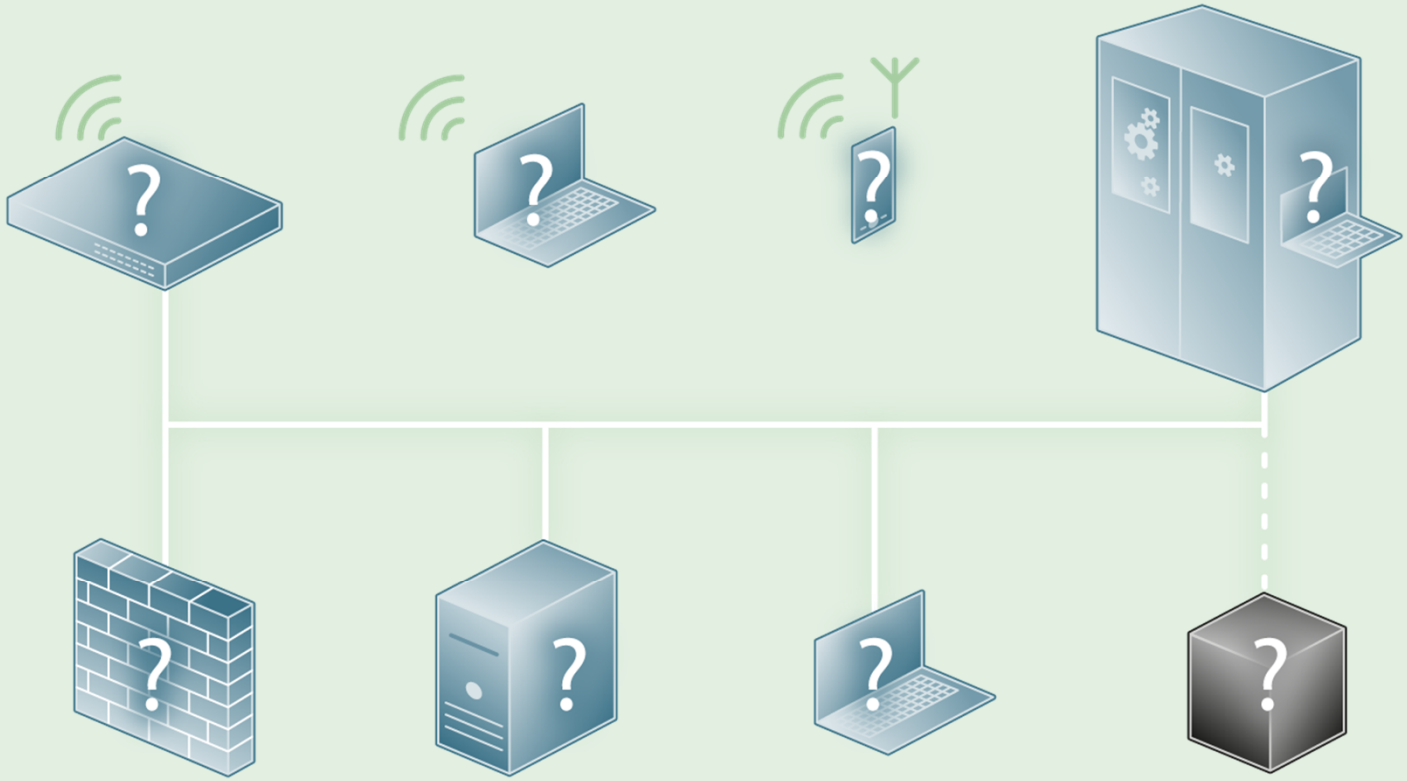
Złośliwe oprogramowanie

Błędy w aplikacjach

Szpiegostwo

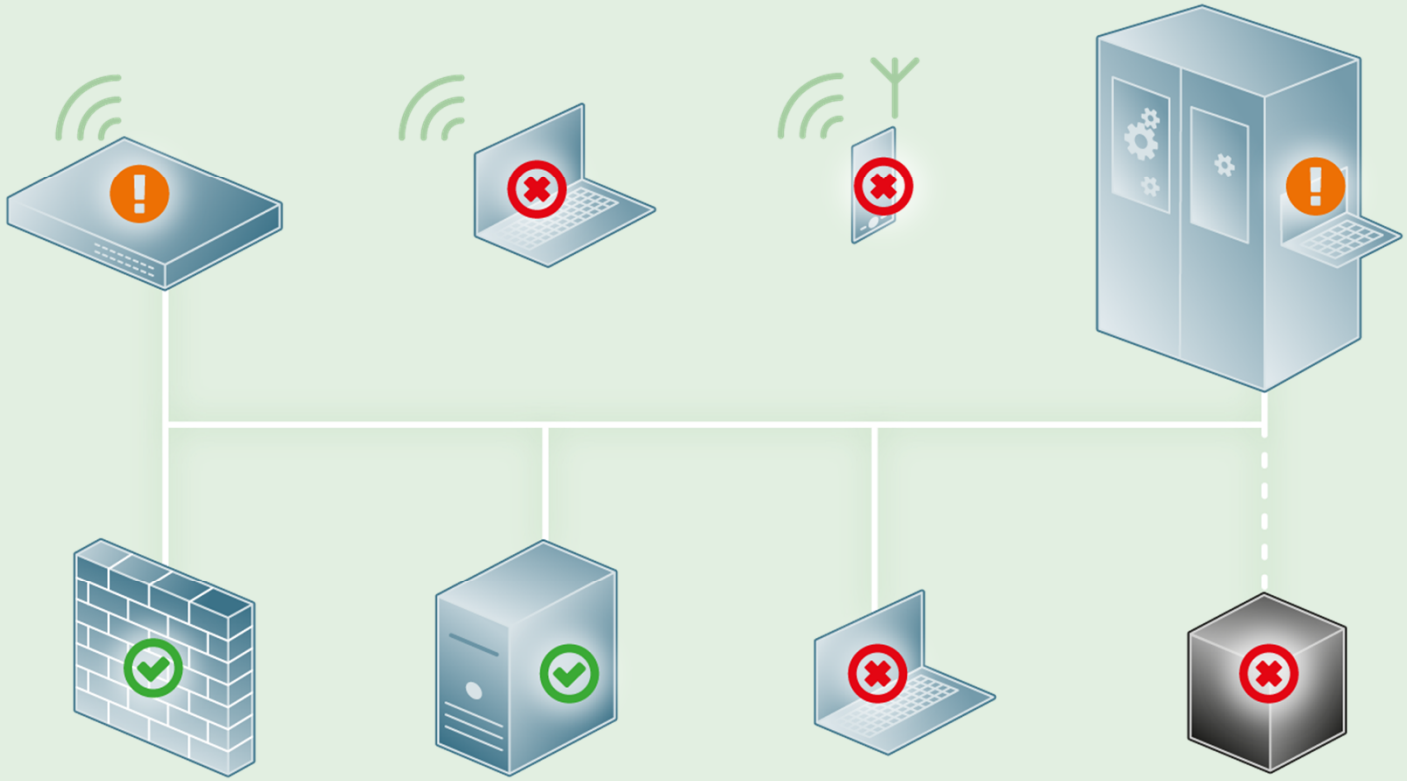
Co się dzieje w sieci?

Co może stanowić zagrożenie dla organizacji?



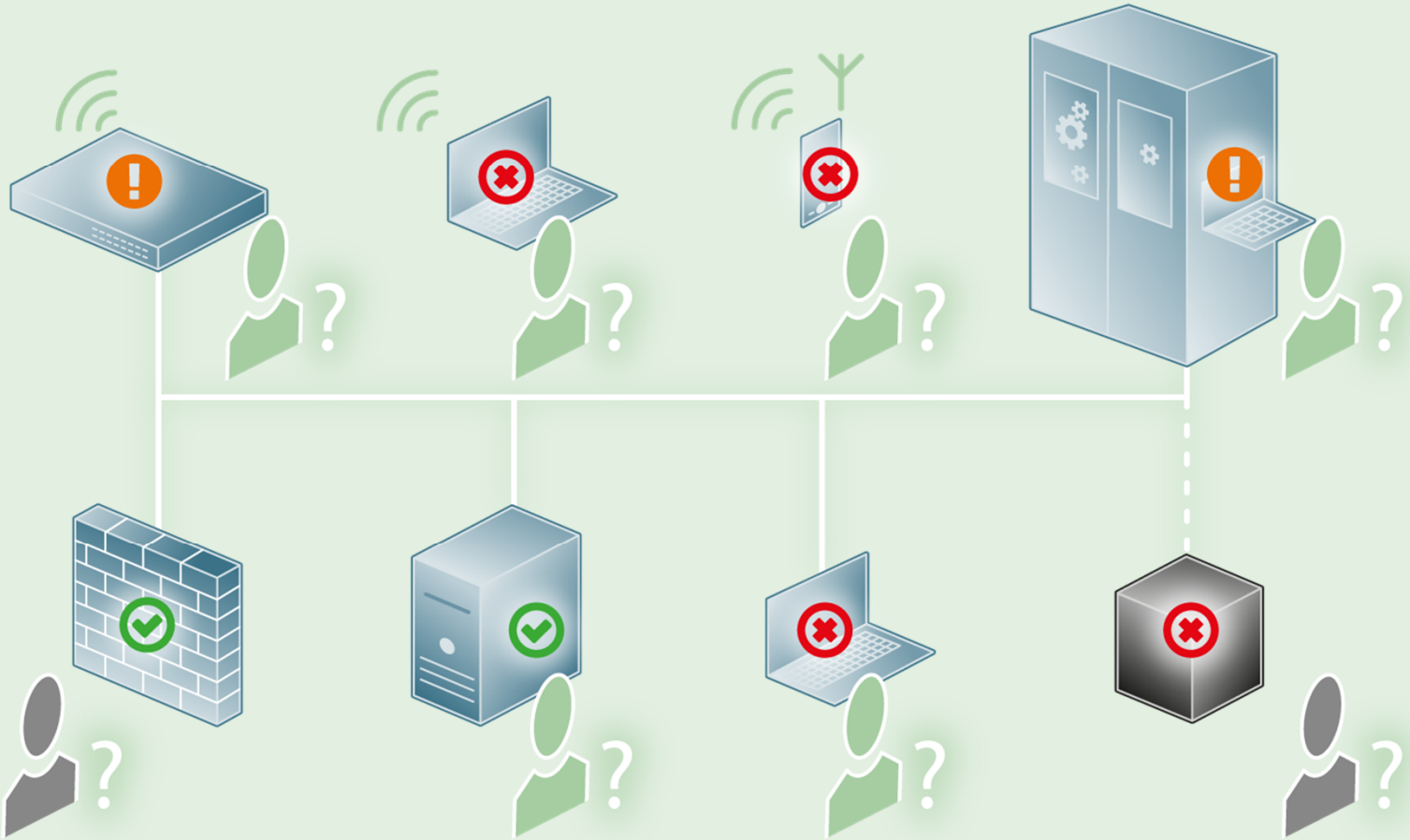
Rzeczywisty stan bezpieczeństwa?

Czy jest nam znany?



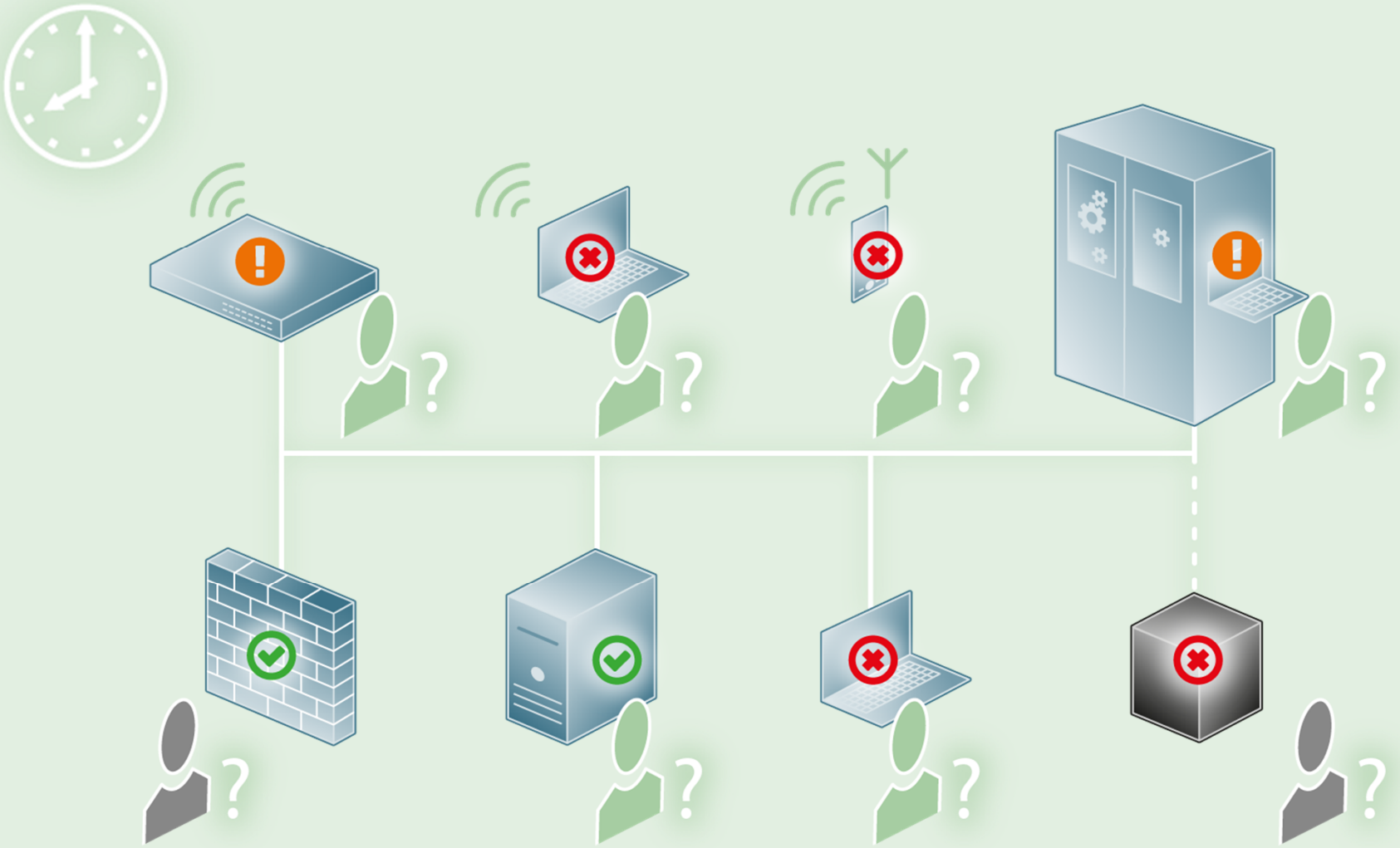
Rzeczywisty stan bezpieczeństwa?

Czy podatności systemów są wykorzystywane?



Rzeczywisty stan bezpieczeństwa?

Jak zmienia się stan bezpieczeństwa w czasie?



SecurityCenter™ CV
continuous view

Wieloaspektowe monitorowanie zagrożeń

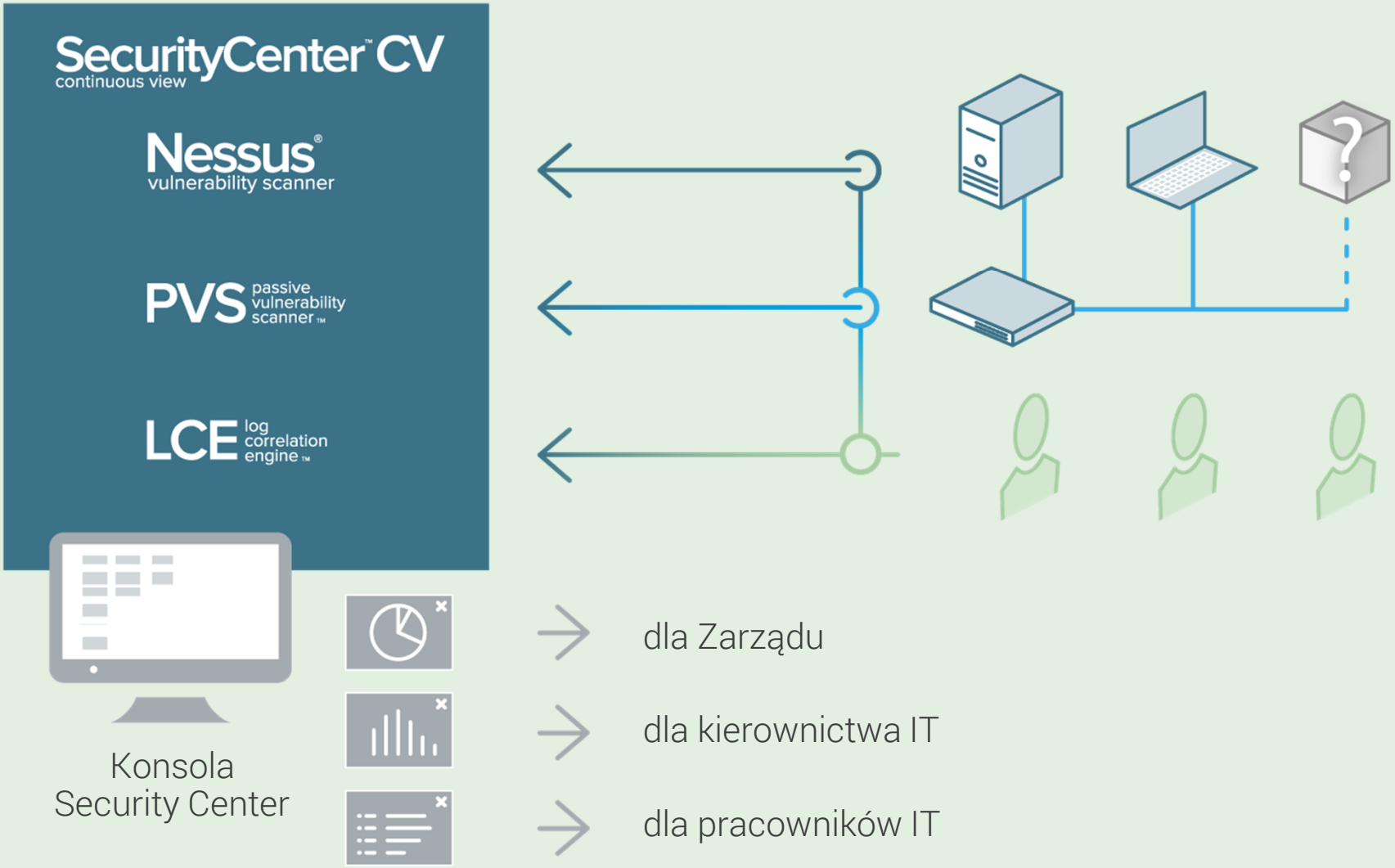
Aktywna analiza bezpieczeństwa

Pasywna analiza bezpieczeństwa

Analiza dzienników i zdarzeń

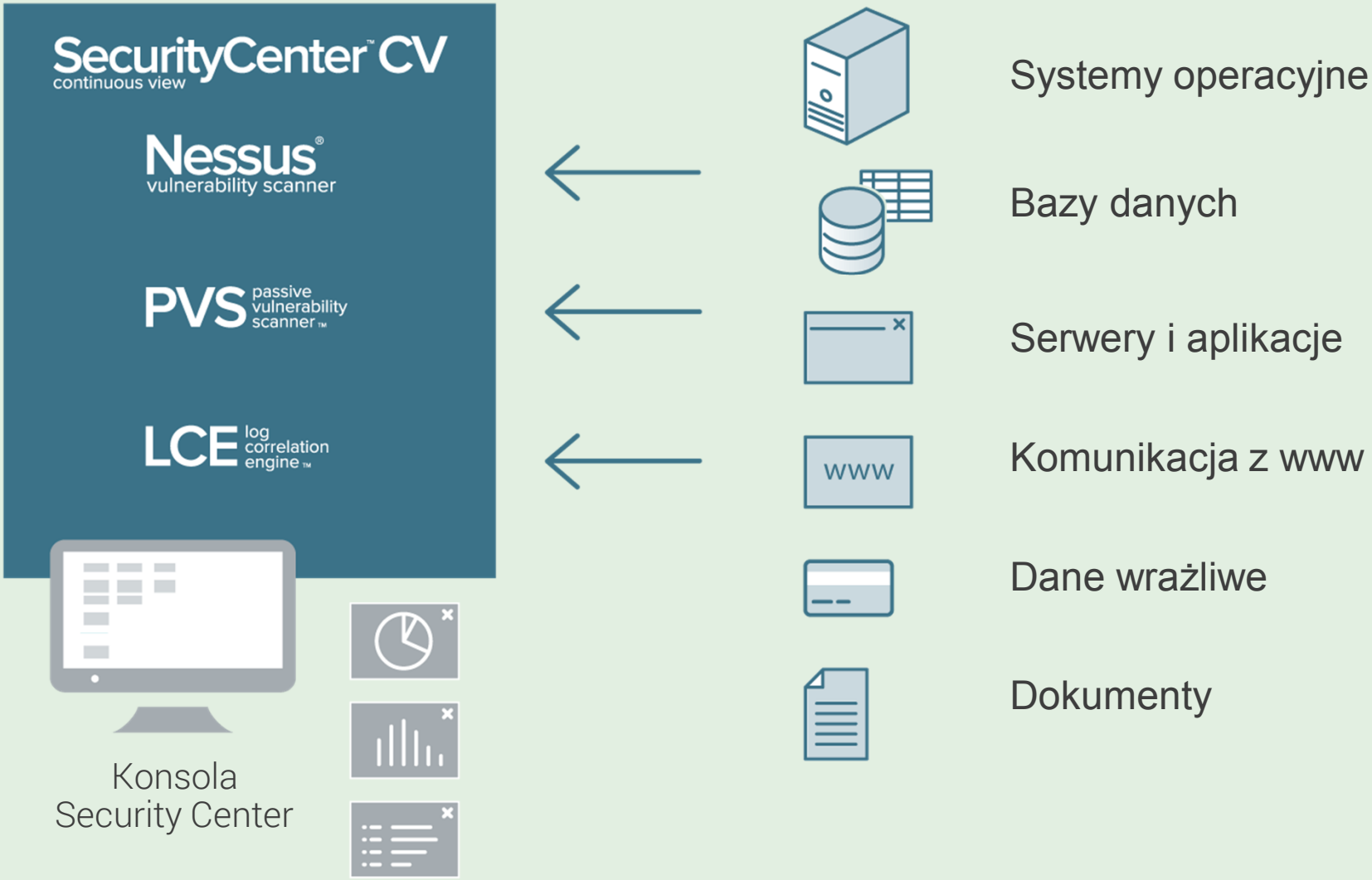
SecurityCenter™ CV
continuous view

Schemat logiczny systemu



SecurityCenter™ CV
continuous view

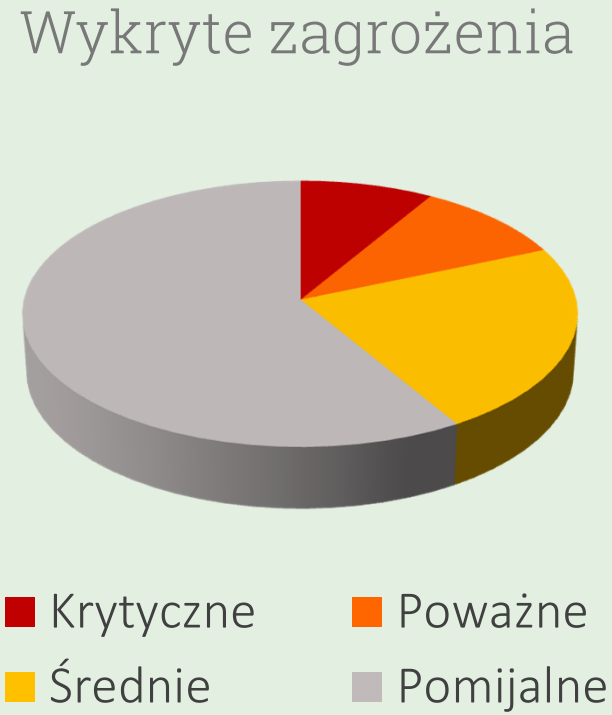
Źródła danych do analizy



Jak widać stan bezpieczeństwa?

Czy możemy je zrozumieć?

Wykryto zagrożenia natury technicznej, technologicznej oraz operacyjnej mające istotny wpływ na poziom bezpieczeństwa instytucji. Zmiany te mają charakter stały, stanowiąc tym samym znaczny czynnik ryzyka dla instytucji. Stwierdzono istnienie zagrożeń dotyczących trzech obszarów działania, związanych z dostawcami, czynnikami zewnętrznymi oraz działaniami pracowników instytucji. Nie da się w pełni określić źródeł ryzyka dla każdego z tych czynników, nie można również określić rzeczywistego poziomu ich wpływu na działanie instytucji. W związku z powyższym sugeruje się znaczne zwiększenie nakładów na wszelkie możliwe obszary związane z bezpieczeństwem systemów teleinformatycznych eksploatowany przez instytucję.



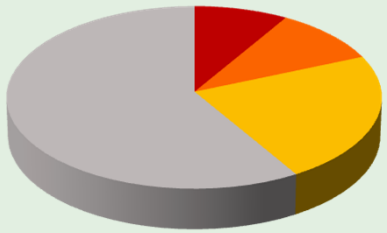
Tak jest.

A tak może być.

SecurityCenter™ CV
continuous view

Agregacja informacji wg poziomu decyzyjnego

Zarządczy



- Krytyczne
- Poważne
- Średnie
- Pomijalne

Kierowniczy

Count	Sever	Name
15	Critical	MS14-080: Cur
8	Critical	MS14-070: Vuli
5	Critical	MS08-067: Mic
2	High	MS06-035: Vur
12	Medium	Microsoft Winc
12	Info	Windows NETB
5	Info	Ethernet Card I

Wykonawczy

MS03-026: Microsoft RPC Interface Buffe

Synopsis:
Arbitrary code can be executed on the remote host.

Description:
The remote version of Windows contains a flaw in th
RemoteActivation() in its RPC interface that could all
execute arbitrary code on the remote host with the
A series of worms (Blaster) are known to exploit this
wild.

See also:
http://technet.microsoft.com/en-us/security/bulleti

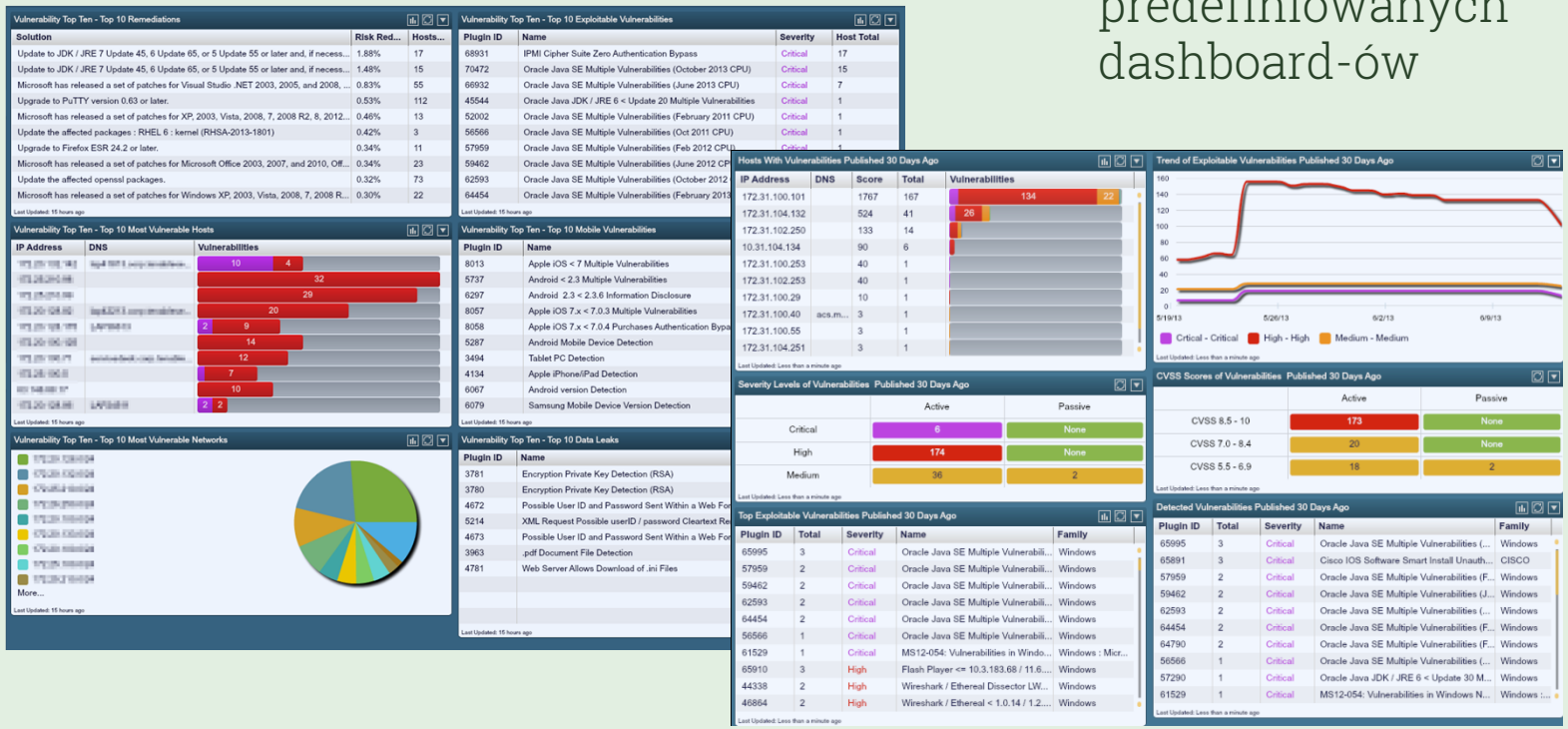
Solution:
Microsoft has released patches for Windows NT, 200

Risk factor :
Critical / CVSS Base Score : 10.0
(CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)
CVSS Temporal Score : 8.3
(CVSS2#E:F/RL:OF/RC:C)

SecurityCenter™ CV
continuous view

Aktywna analiza bezpieczeństwa

Dwa z kilkuset predefiniowanych dashboard-ów

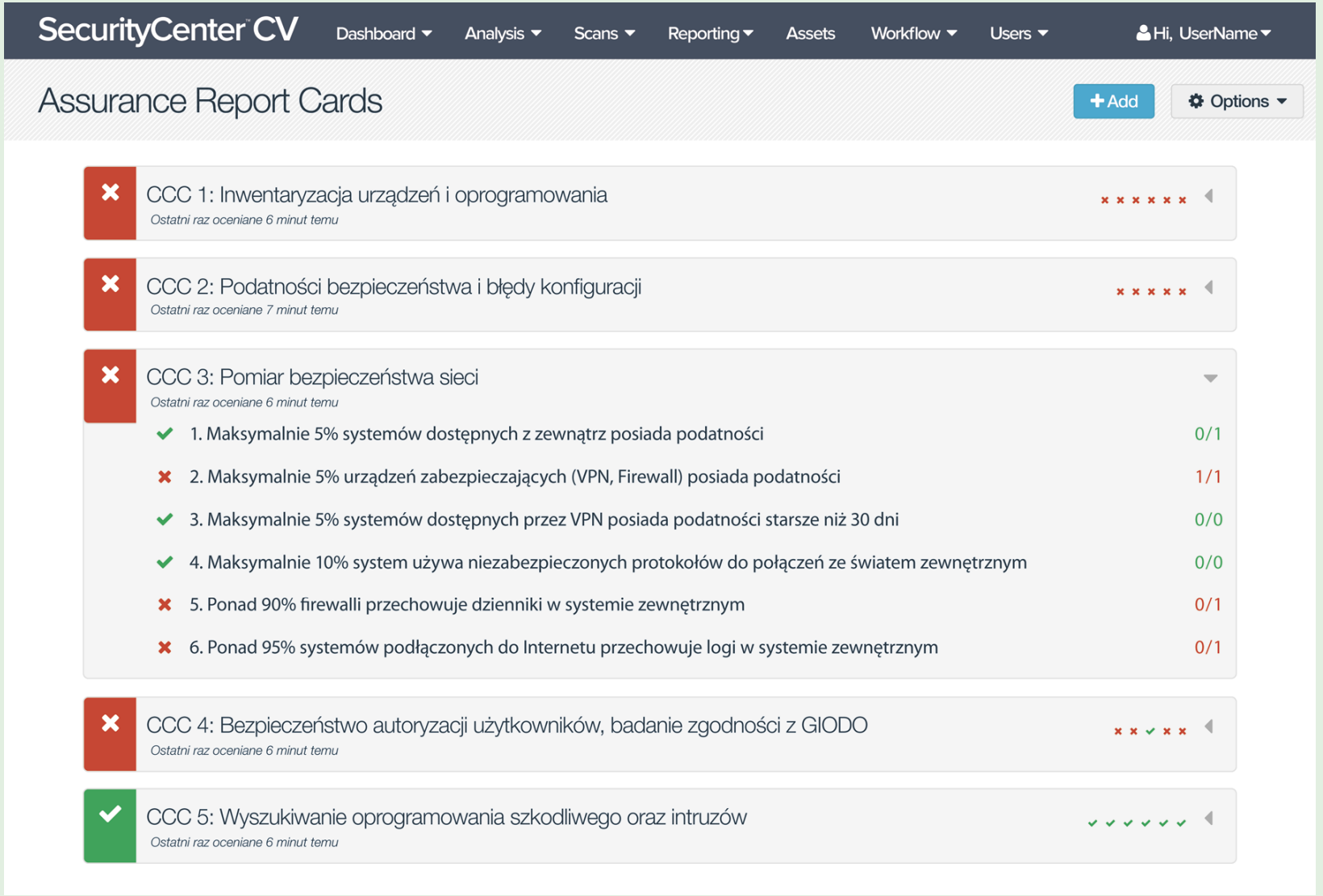


Vulnerability Top Ten

Vulnerabilities Over 30 Days

SecurityCenter™ CV
continuous view

Karty realizacji celów strategicznych



SecurityCenter™ CV
continuous view

Ochrona danych osobowych

SecurityCenter™ CV
continuous view

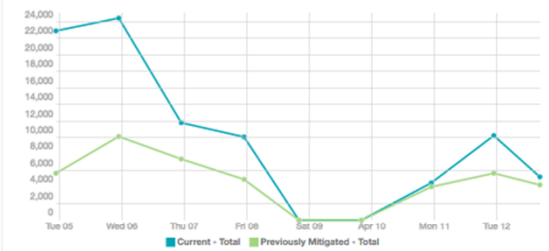
Wskaźniki zarządcze

SecurityCenter Dashboard Analysis Scans Reporting Assets Workflow Users

Executive Vulnerability Metrics

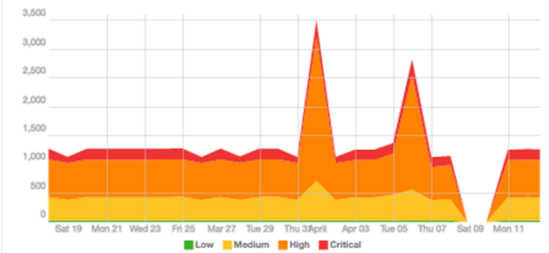
Switch Dashboard Options

Executive Vulnerability Metrics - Vulnerability Trend



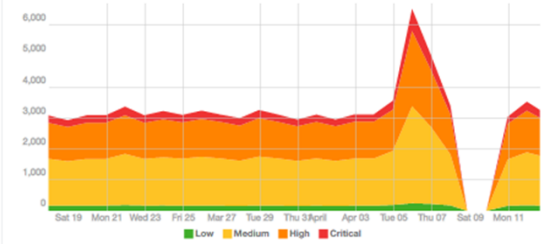
Last Updated: 23 minutes ago

Executive Vulnerability Metrics - 25 Day Trend Windows Vulnerabilities



Last Updated: 1 hour ago

Executive Vulnerability Metrics - 25 Day Trend Linux Vulnerabilities



Last Updated: 1 hour ago

Executive Summary - Vulnerability Age

	New Hosts	Low	Medium	High	Critical
< 7	68	155	1662	1399	628
< 30	461	444	4077	3134	920
< 90	763	1288	6680	3570	1153
> 90	24	158	311	127	38

Last Updated: 1 hour ago

Executive Vulnerability Metrics - Vulnerability Publication Age

	Low	Medium	High	Critical
< 7	0	0	0	0
< 30	0	1	15	1
< 90	0	67	161	6
> 90	623	2090	1471	552

Last Updated: 1 hour ago

Vulnerability Top Ten - Top 10 Most Vulnerable Hosts

IP Address	DNS	Total	Vulnerabilities
172.26.23.171		45	30
172.26.48.63	win2k.target.tenablesecurity.com	45	32
172.26.48.25	centos6x64.target.tenablesecurity.com	44	31
172.26.0.84		59	53
172.26.48.64	win2k3r2.target.tenablesecurity.com	56	52
172.26.0.42	eng-macmini.lab.tenablesecurity.com	58	55
172.26.0.116	solaris11vm1	18	
172.26.0.68	sunshine.lab.tenablesecurity.com	17	
172.26.0.37	solaris11vm1-sparc.lab.tenablesecurity.co...	16	
172.26.22.197	npw-qa-107.local	37	33

Last Updated: 1 hour ago

Executive Vulnerability Metrics - Patch Publication Age

	Low	Medium	High	Critical
< 7	0	2	12	2
< 30	6	139	130	8
< 90	8	401	423	150
> 90	327	2999	2949	852

Last Updated: 1 hour ago

Executive Vulnerability Metrics - Vulnerability Mitigation

	New Hosts	Low	Medium	High	Critical
< 7	4	123	2289	3506	670
< 30	30	180	3117	3970	830
< 90	61	407	7255	7009	1866
> 90	0	103	1175	933	200

Last Updated: 1 hour ago

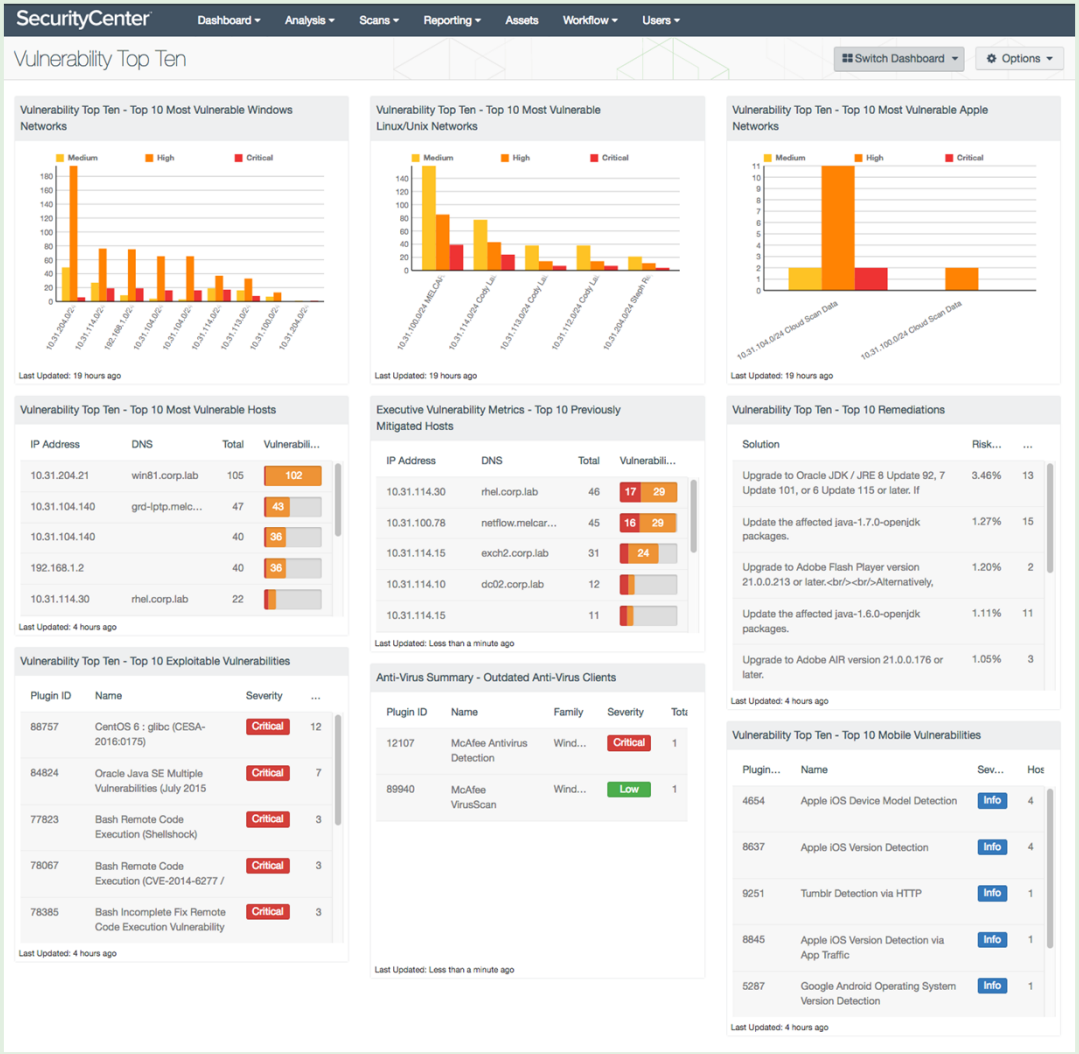
Executive Vulnerability Metrics - Top 10 Previously Mitigated Hosts

IP Address	DNS	Total	Vulnerabilities
172.26.23.171		115	36 79
172.26.48.25	centos6x64.target.tenablesecurity.com	121	34 87
172.26.0.116	solaris11vm1	100	35 65
172.26.0.68	sunshine.lab.tenablesecurity.com	96	31 65
172.26.0.117	bal-lce-001.lab.tenablesecurity.com	72	28 44
172.26.48.99	solaris10.target.tenablesecurity.com	70	28 42
172.26.0.107		81	59
172.26.0.84		110	98
172.26.24.230	ssl-nix.lab.tenablesecurity.com	72	51
172.26.48.27	debian6.target.tenablesecurity.com	89	75

Last Updated: 7 minutes ago

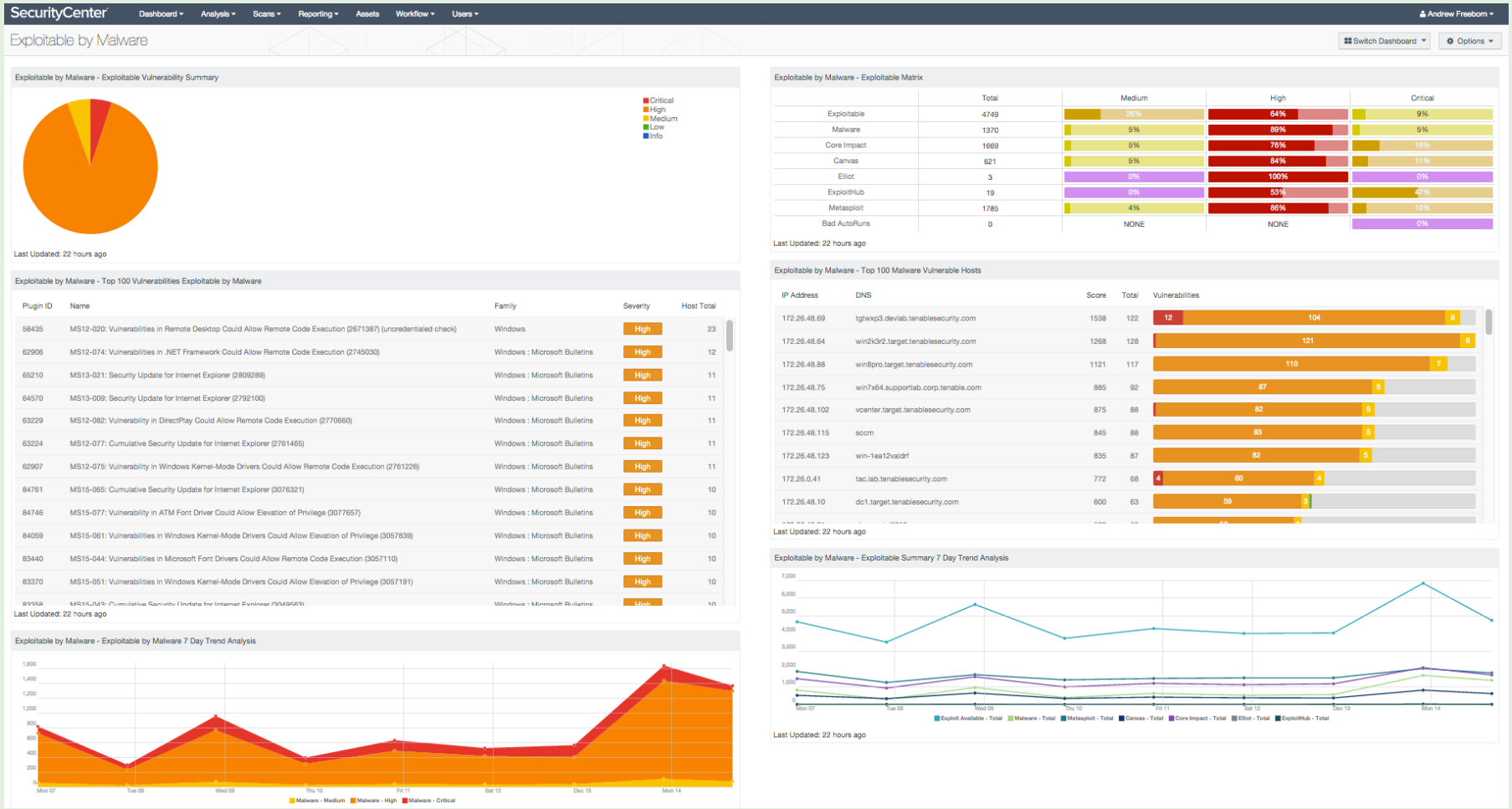
SecurityCenter™ CV
continuous view

TOP 10 podatności w systemach i sieciach



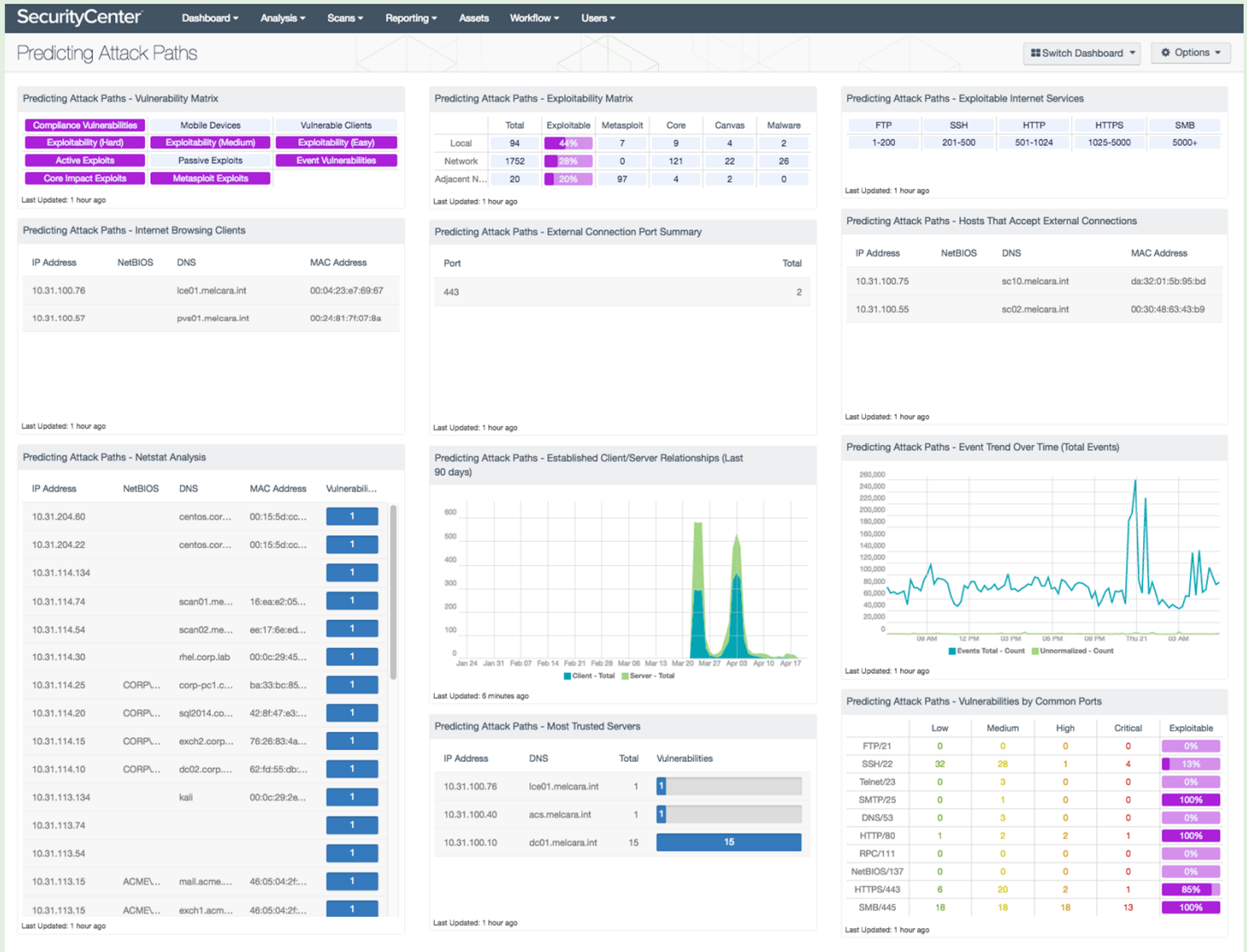
SecurityCenter™ CV
continuous view

Wektory ataku dla Malware



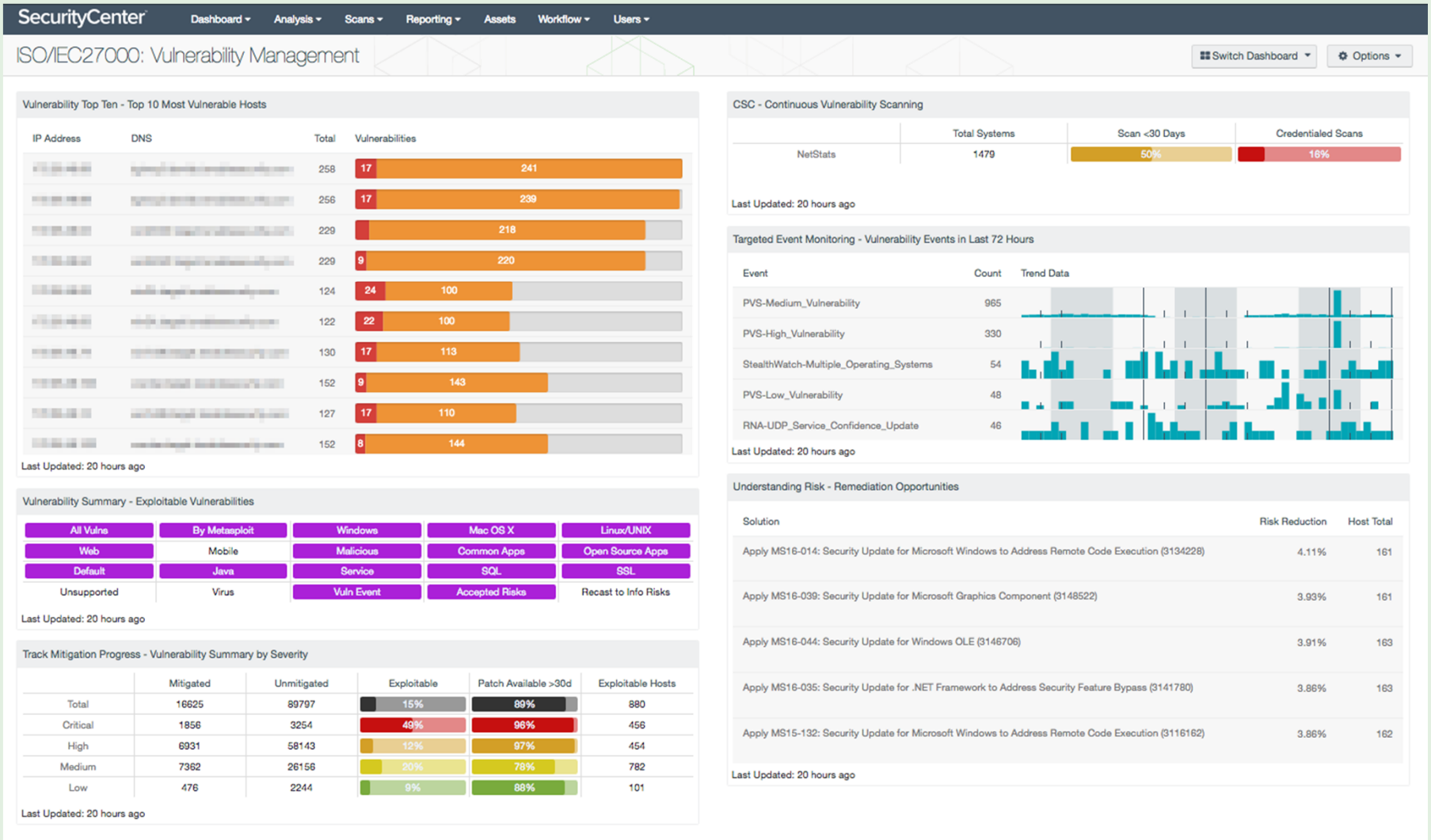
SecurityCenter™ CV
continuous view

Wykryte wektory ataku



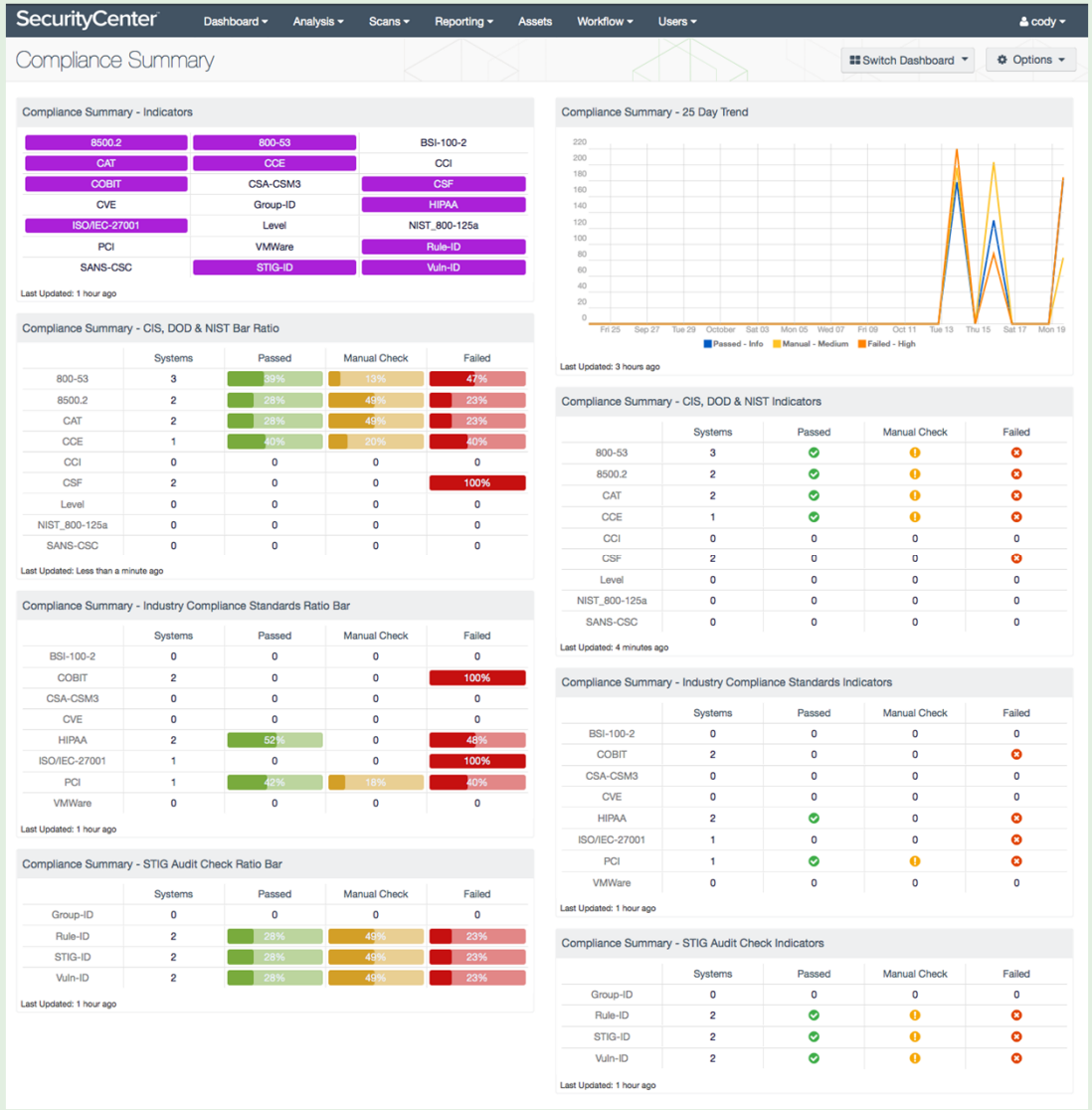
SecurityCenter™ CV
continuous view

Widok dla ISO/IEC27000



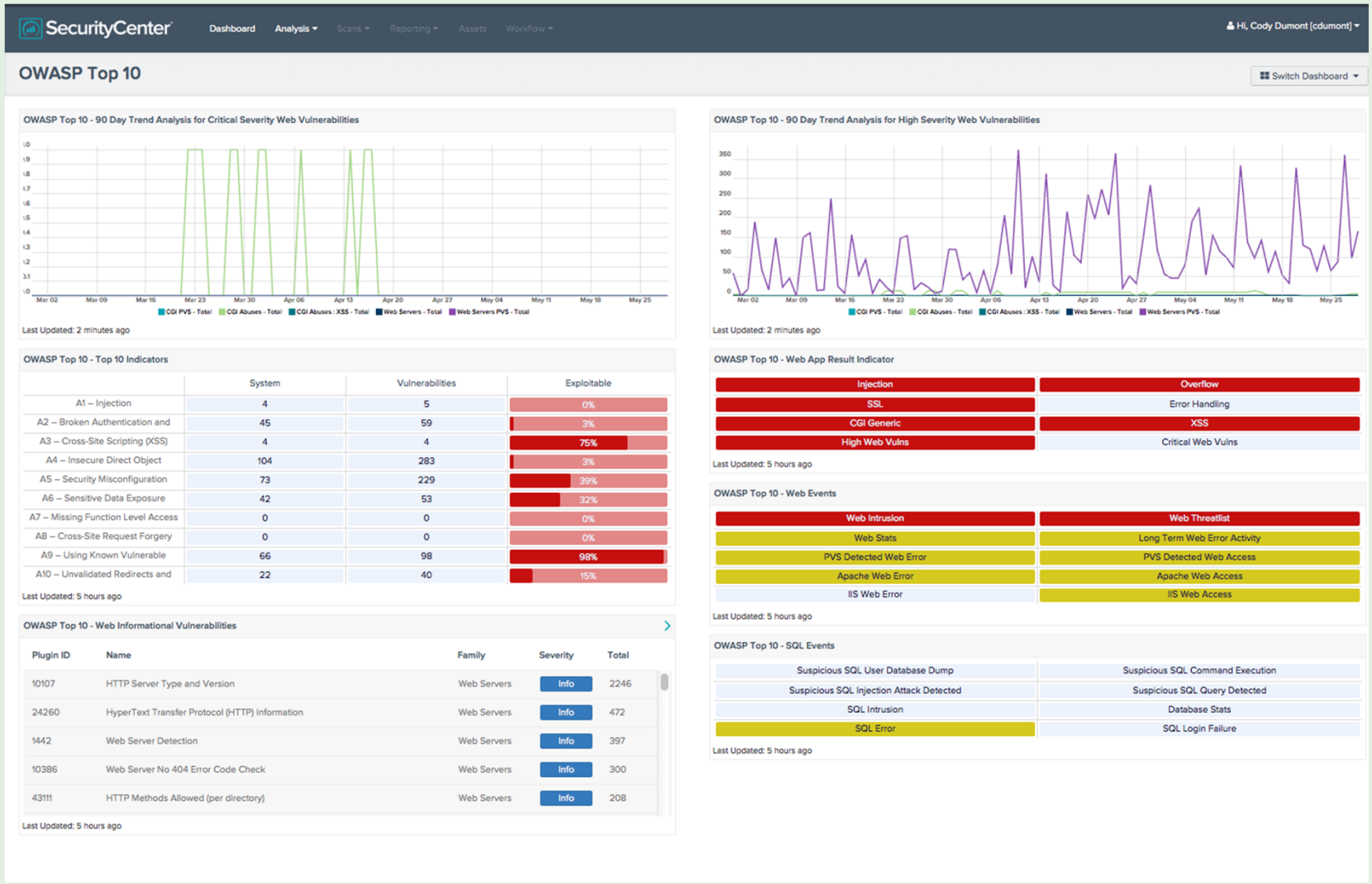
SecurityCenter™ CV
continuous view

Widok dla PCI DSS



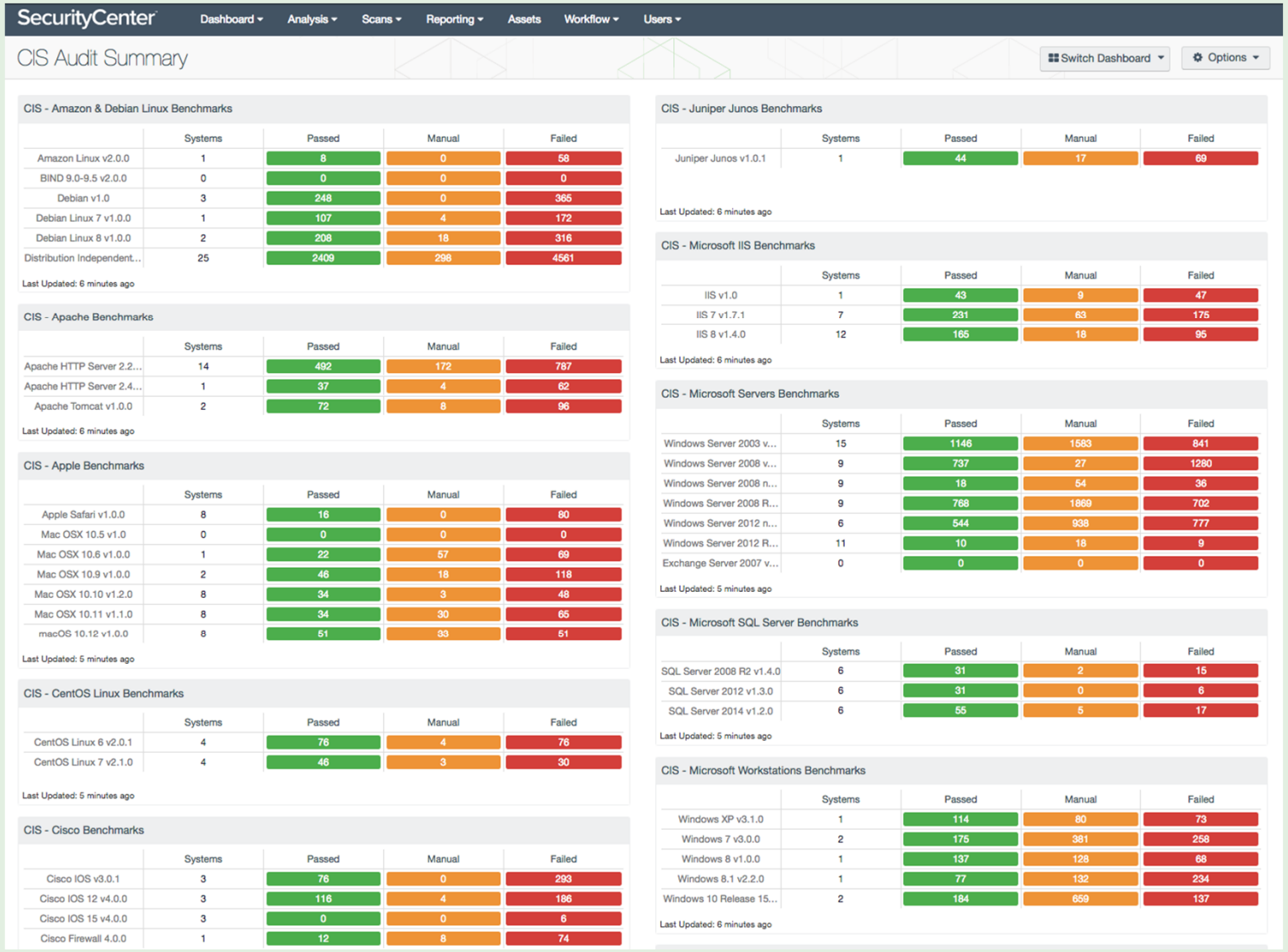
SecurityCenter™ CV
continuous view

OWASP Top 10



SecurityCenter™ CV
continuous view

Zgodność z normami CIS



SecurityCenter™ CV
continuous view

Aktywna analiza bezpieczeństwa

Vulnerability Top Ten - Top 10 Remediations

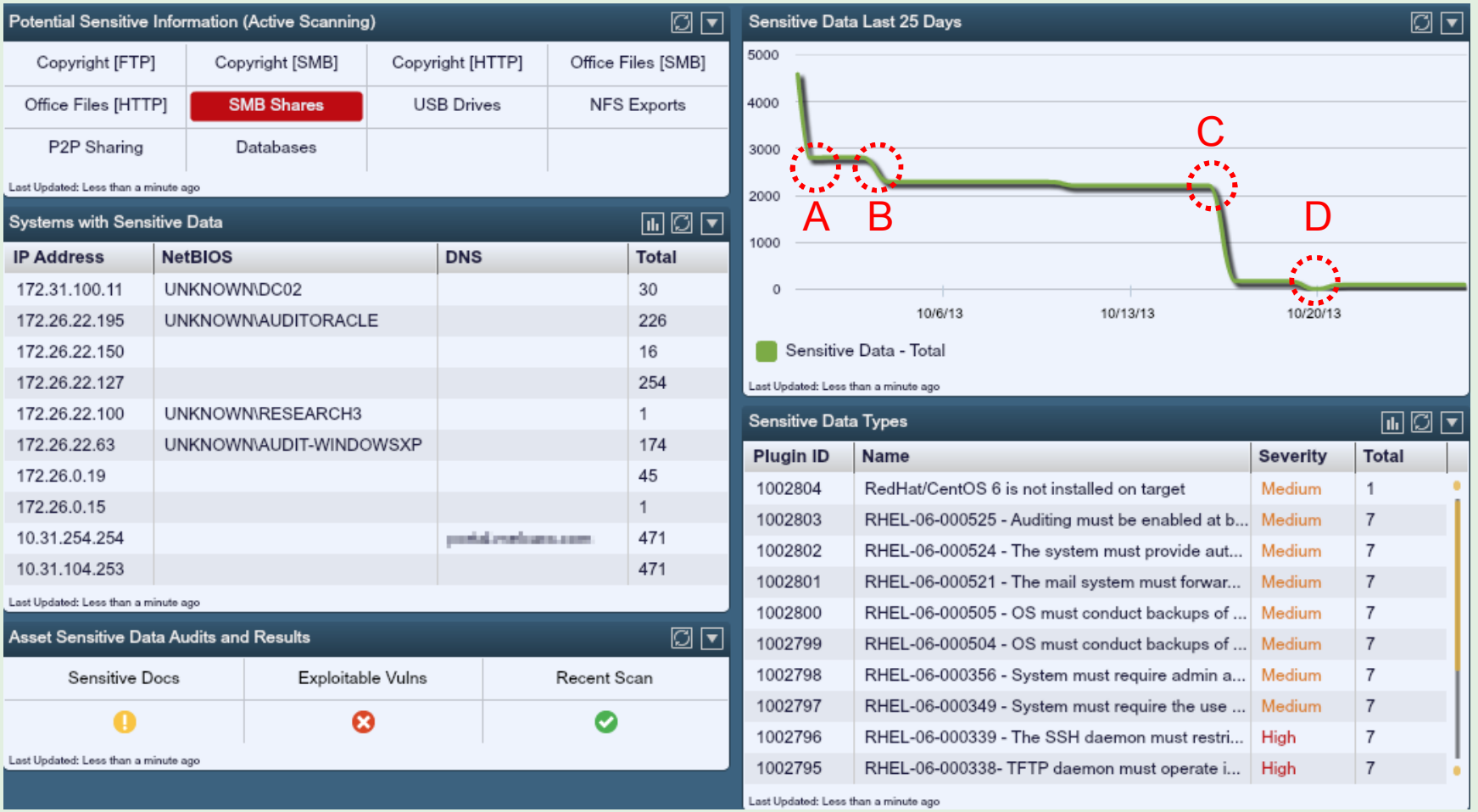
Solution	Risk Red...	Hosts...
Update to JDK / JRE 7 Update 45, 6 Update 65, or 5 Update 55 or later and, if necess...	1.88%	17
Update to JDK / JRE 7 Update 45, 6 Update 65, or 5 Update 55 or later and, if necess...	1.48%	15
Microsoft has released a set of patches for Visual Studio .NET 2003, 2005, and 2008, ...	0.83%	55
Upgrade to PuTTY version 0.63 or later.	0.53%	112
Microsoft has released a set of patches for XP, 2003, Vista, 2008, 7, 2008 R2, 8, 2012...	0.46%	13
Update the affected packages : RHEL 6 : kernel (RHSA-2013-1801)	0.42%	3
Upgrade to Firefox ESR 24.2 or later.	0.34%	11
Microsoft has released a set of patches for Microsoft Office 2003, 2007, and 2010, Off...	0.34%	23
Update the affected openssl packages.	0.32%	73
Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, 2008 R...	0.30%	22

Last Updated: 15 hours ago

Ocena możliwości redukcji ryzyka

SecurityCenter™ CV
continuous view

Przykład synergii – detekcja danych wrażliwych



SecurityCenter™ CV
continuous view

Badanie zgodności systemów

Weryfikacja konfiguracji systemów, stacji roboczych, serwerów oraz urządzeń

Własne, dedykowane polityki bezpieczeństwa

Badanie zgodności systemów z wieloma standardami (PCI DSS, CIS, FIPS, DISA, CERT, GIODO, KNF)

Generacja „wsadu” dla audytu wewnętrznego, raportów dla Rady Nadzorczej i Zarządu, BION

Wsparcie przy sporach z outsourcerami

Automatyczna identyfikacja zasobów

OpenBIZ

http://www.openbiz.pl

tenable

GOLD PARTNER

DZIĘKUJĘ ZA UWAGĘ

tenable@openbiz.pl