



OpenBIZ

<http://www.openbiz.pl>

TENABLE SECURITY CENTER CONTINUOUS VIEW

KOMPLEKSOWY POMIAR RYZYKA
W SYSTEMACH I SIECIACH.

6/21/2017

Security Center Continuous View

Główne zagrożenia

Dla sieci i systemów



Ignorowanie zaleceń i norm



Złośliwe oprogramowanie



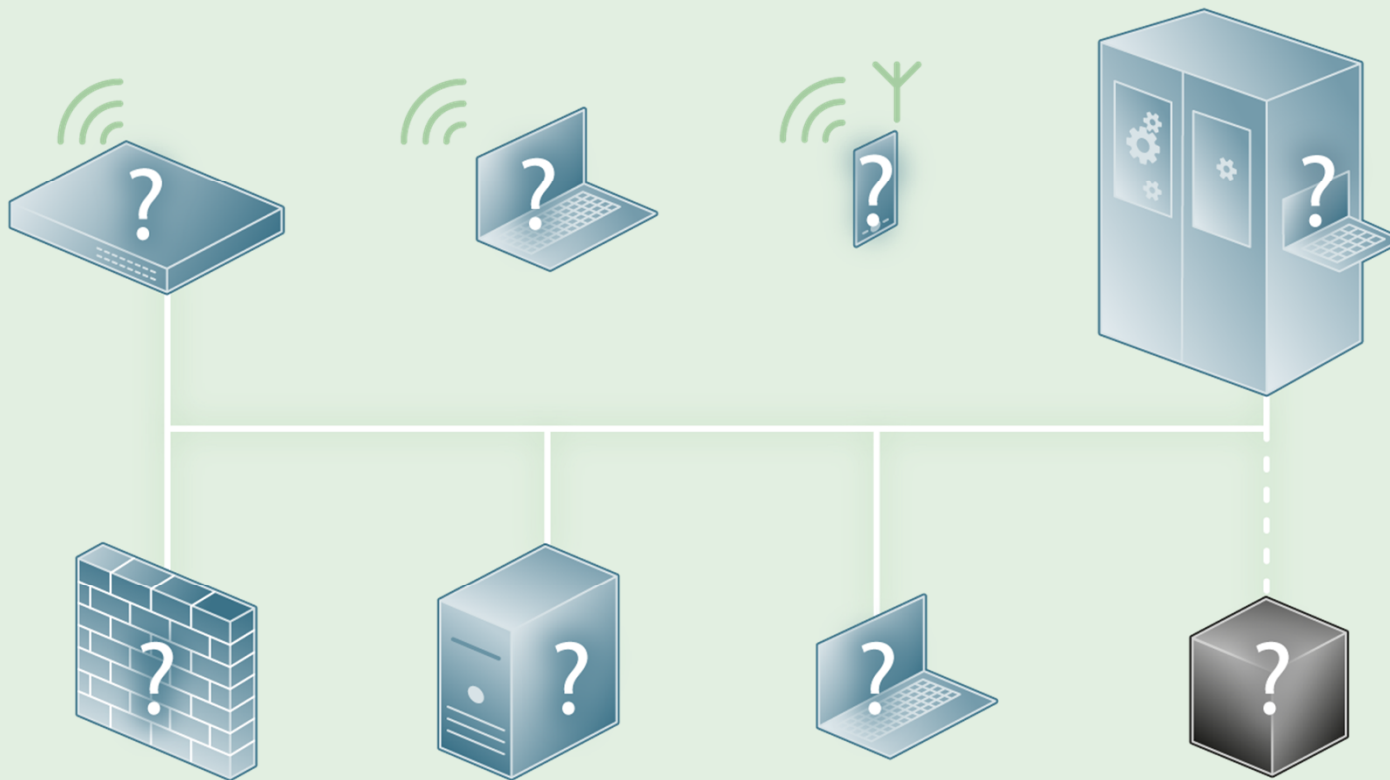
Błędy w aplikacjach



Szpiegostwo

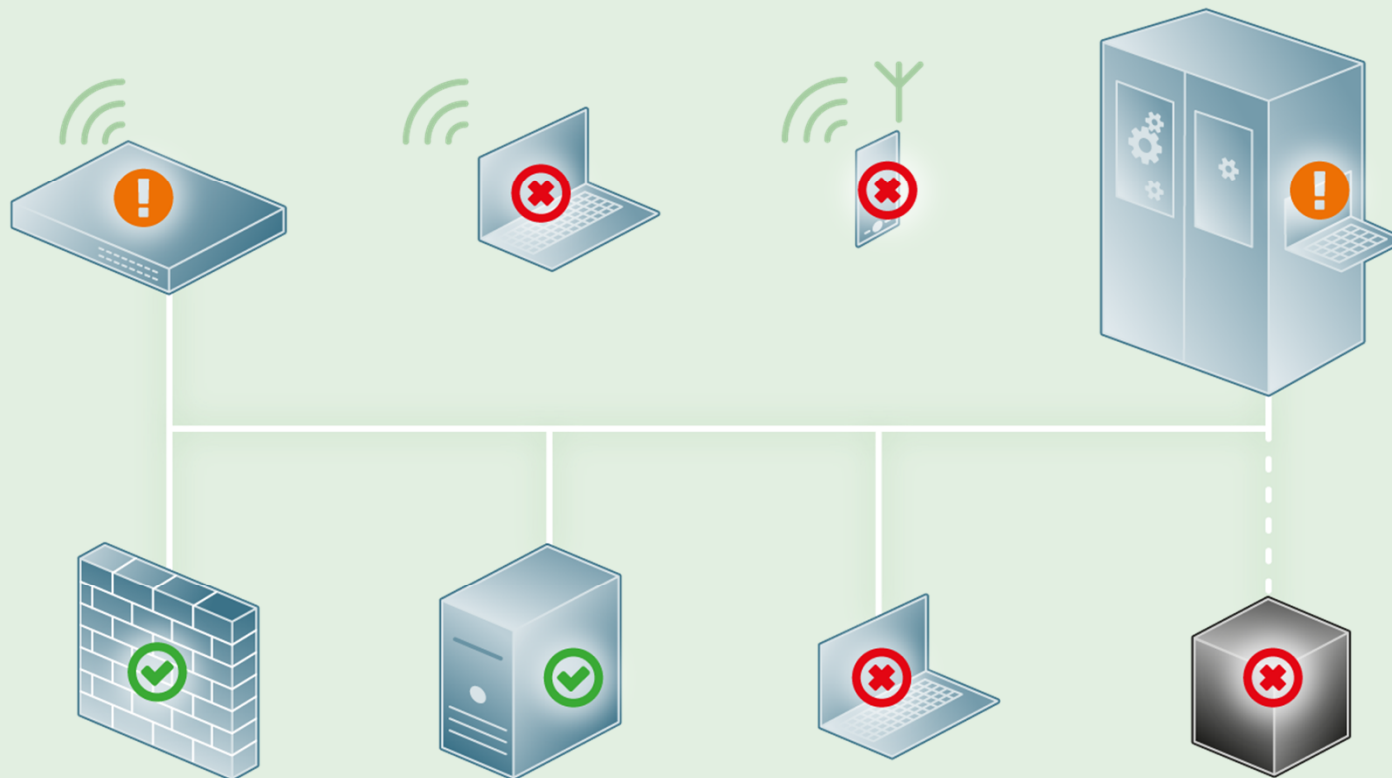
Co się dzieje w sieci?

Co może stanowić zagrożenie dla organizacji?



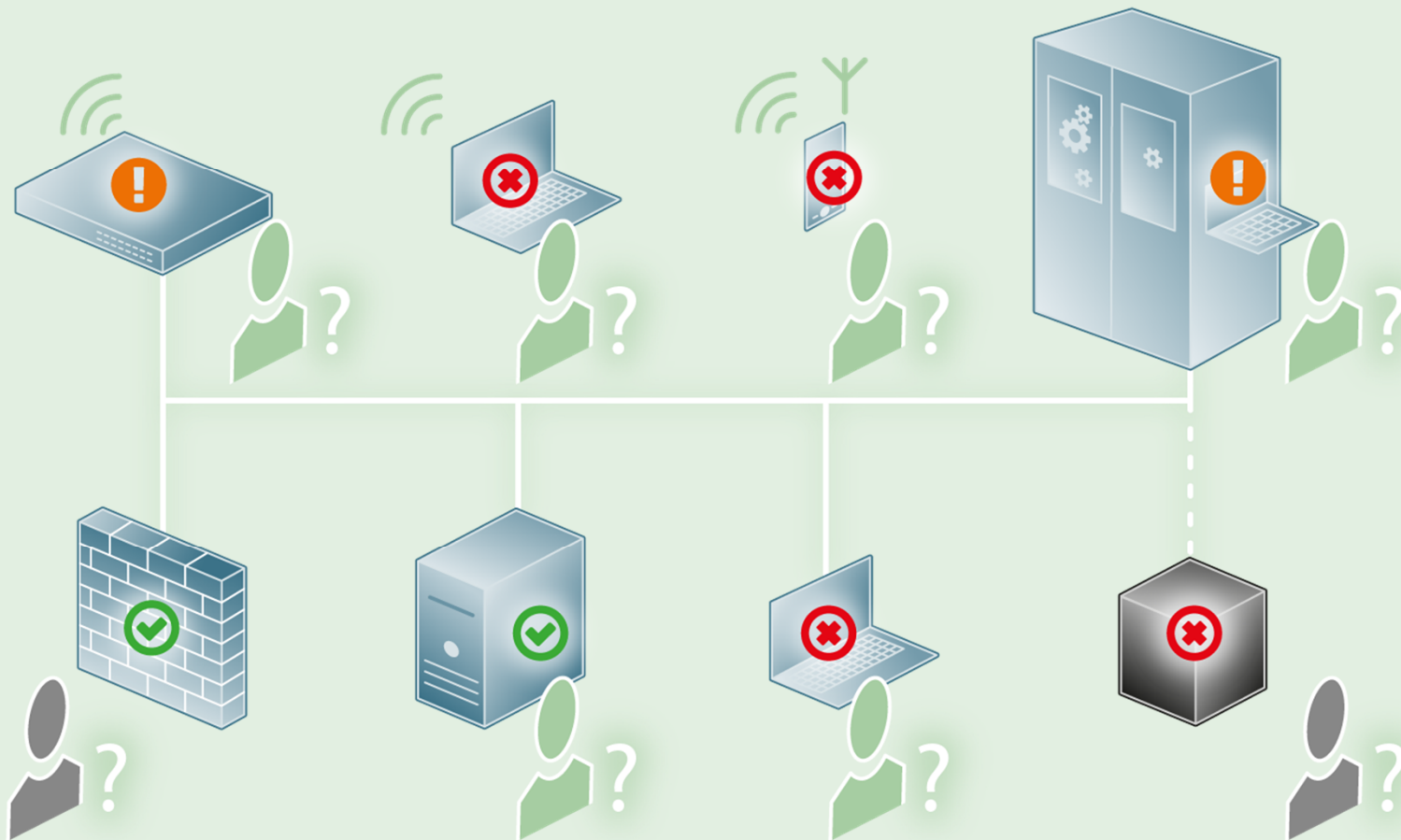
Rzeczywisty stan bezpieczeństwa?

Czy jest nam znany?



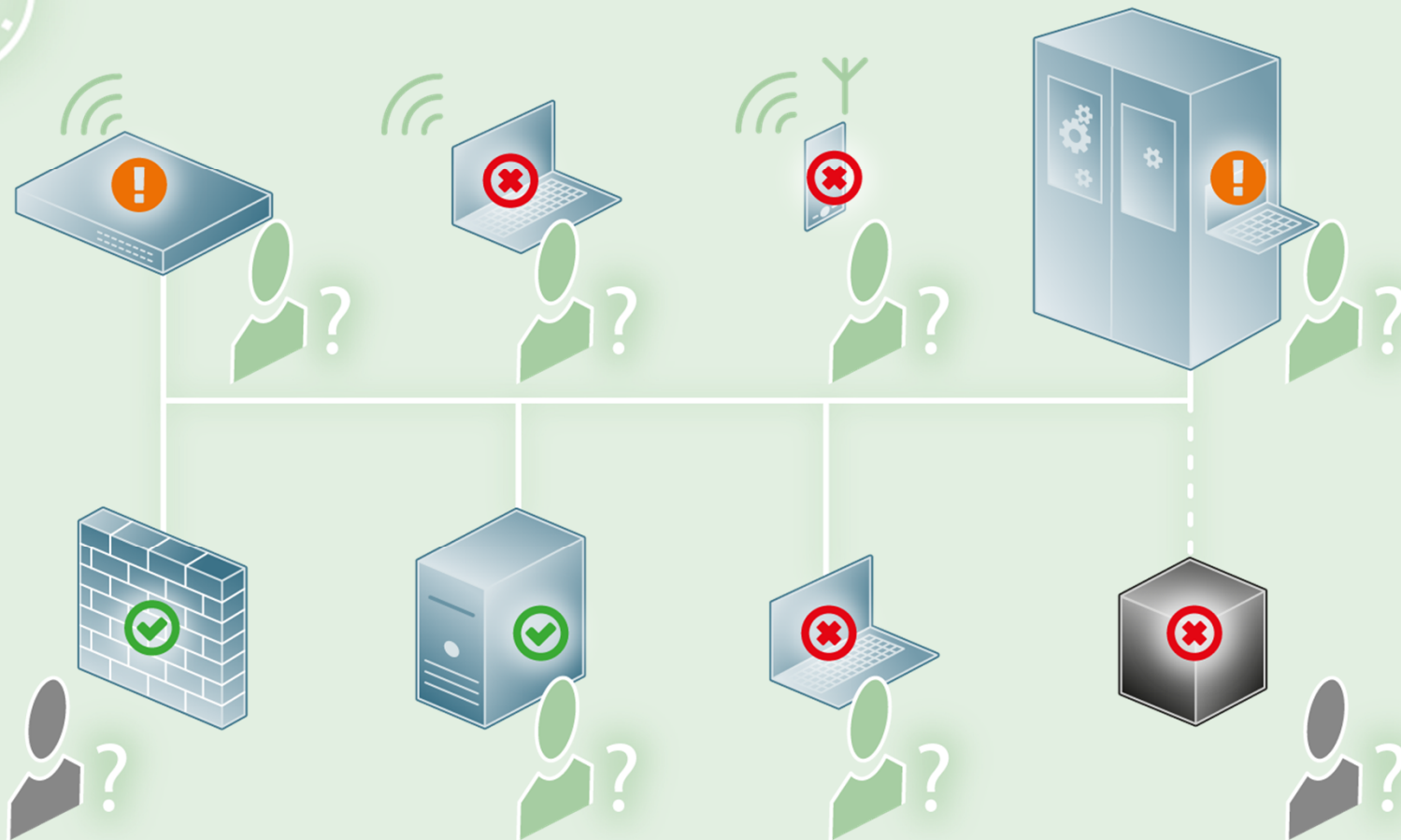
Rzeczywisty stan bezpieczeństwa?

Czy podatności systemów są wykorzystywane?



Rzeczywisty stan bezpieczeństwa?

Jak zmienia się stan bezpieczeństwa w czasie?



Wieloaspektowe monitorowanie zagrożeń



Aktywna analiza
bezpieczeństwa



Pasywna analiza
bezpieczeństwa

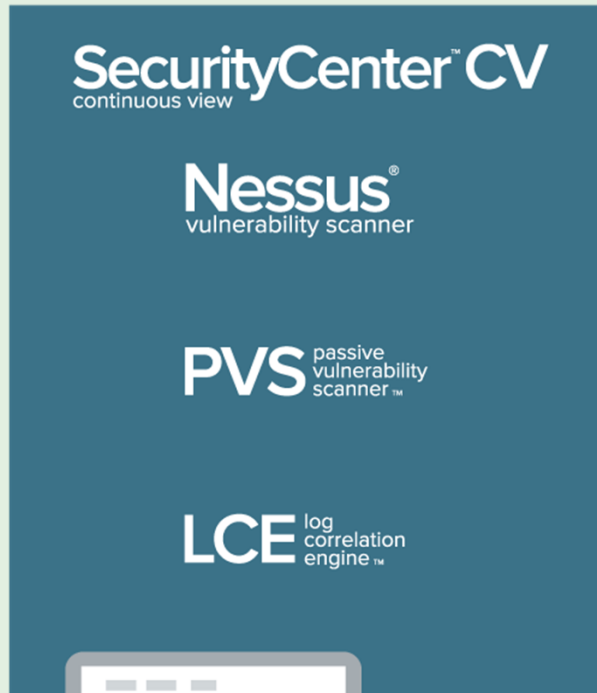


Analiza
dzienników i zdarzeń

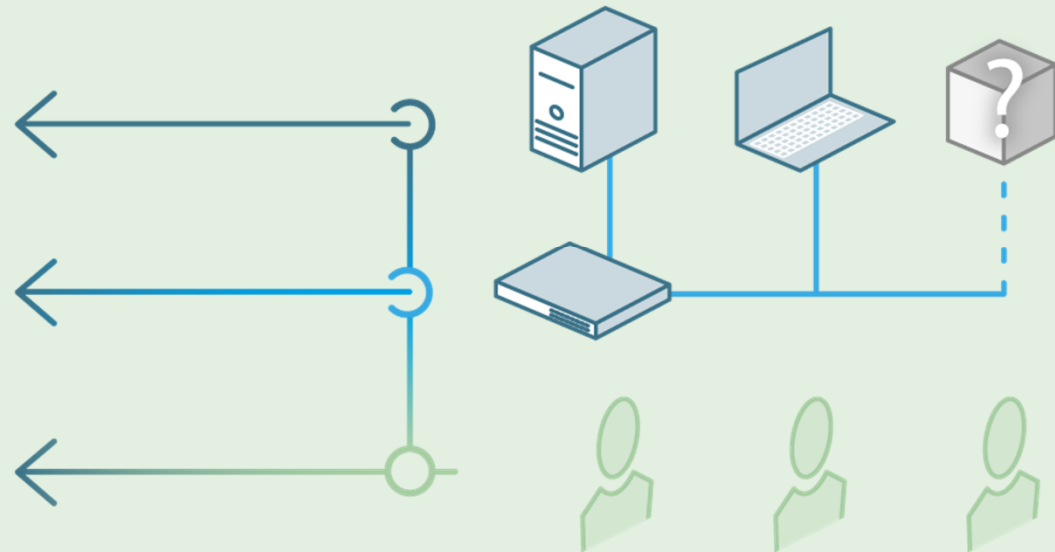
SecurityCenter™ CV

continuous view

Schemat logiczny systemu



Konsola
Security Center



→ dla Zarządu

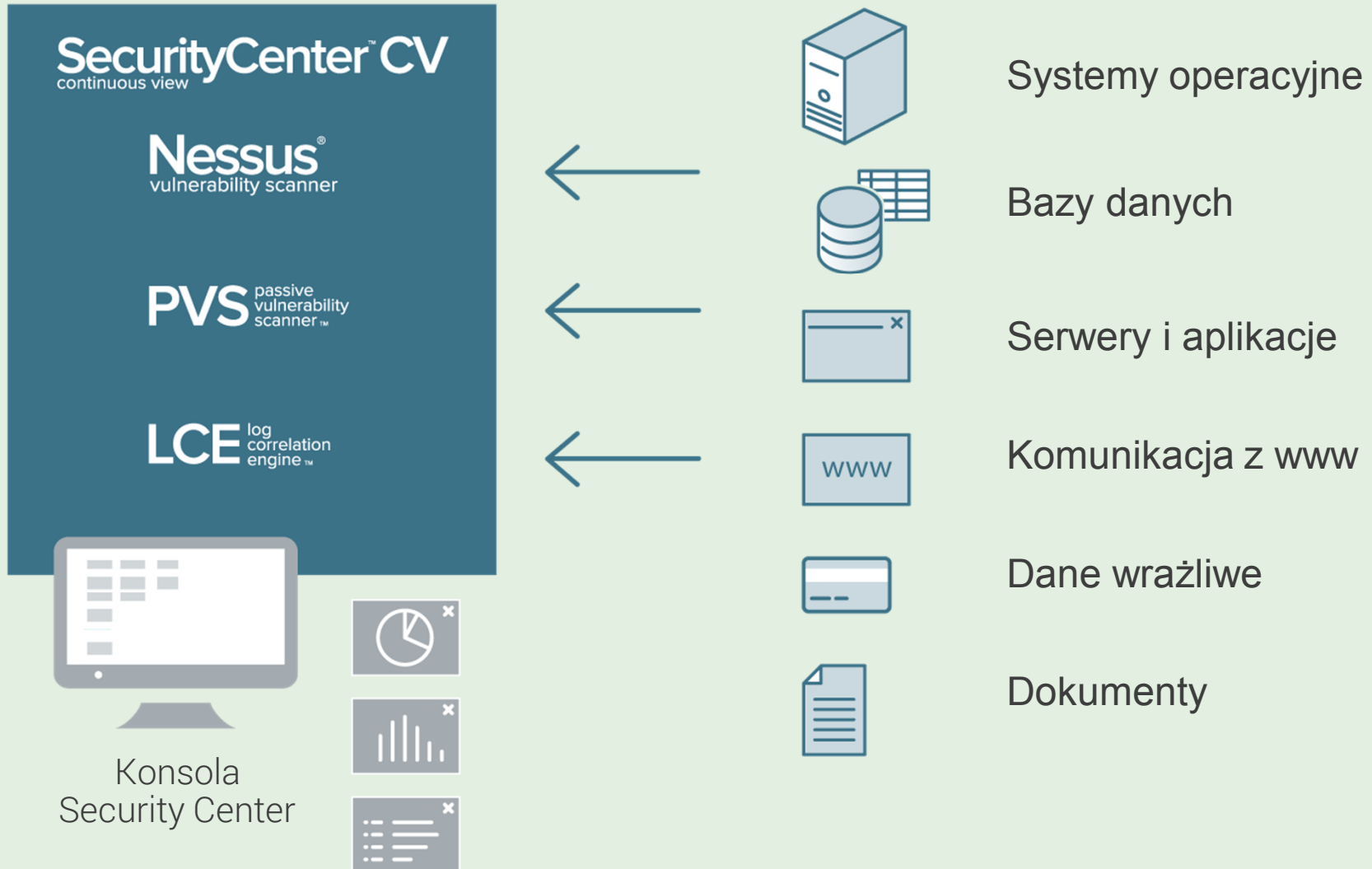
→ dla kierownictwa IT

→ dla pracowników IT

SecurityCenter™ CV

continuous view

Źródła danych do analizy

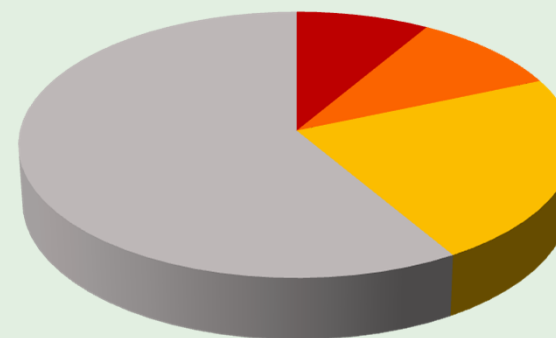


Jak widać stan bezpieczeństwa?

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.

Wykryte zagrożenia



■ Krytyczne

■ Poważne

■ Średnie

■ Pomijalne

Tak jest.

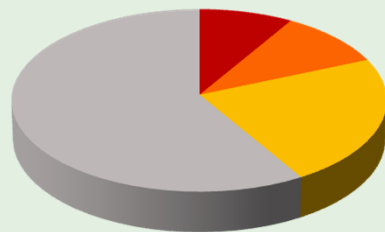
A tak może być.

Agregacja informacji wg poziomu decyzyjnego

Zarządczy

Kierowniczy

Wykonawczy



- Krytyczne
- Poważne
- Średnie
- Pomijalne

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

MS03-026: Microsoft RPC Interface Buffer

Synopsis:

Arbitrary code can be executed on the remote host.

Description:

The remote version of Windows contains a flaw in the RemoteActivation() in its RPC interface that could allow an attacker to execute arbitrary code on the remote host with the same privileges as the user. A series of worms (Blaster) are known to exploit this vulnerability.

See also:

<http://technet.microsoft.com/en-us/security/bulletin>

Solution:

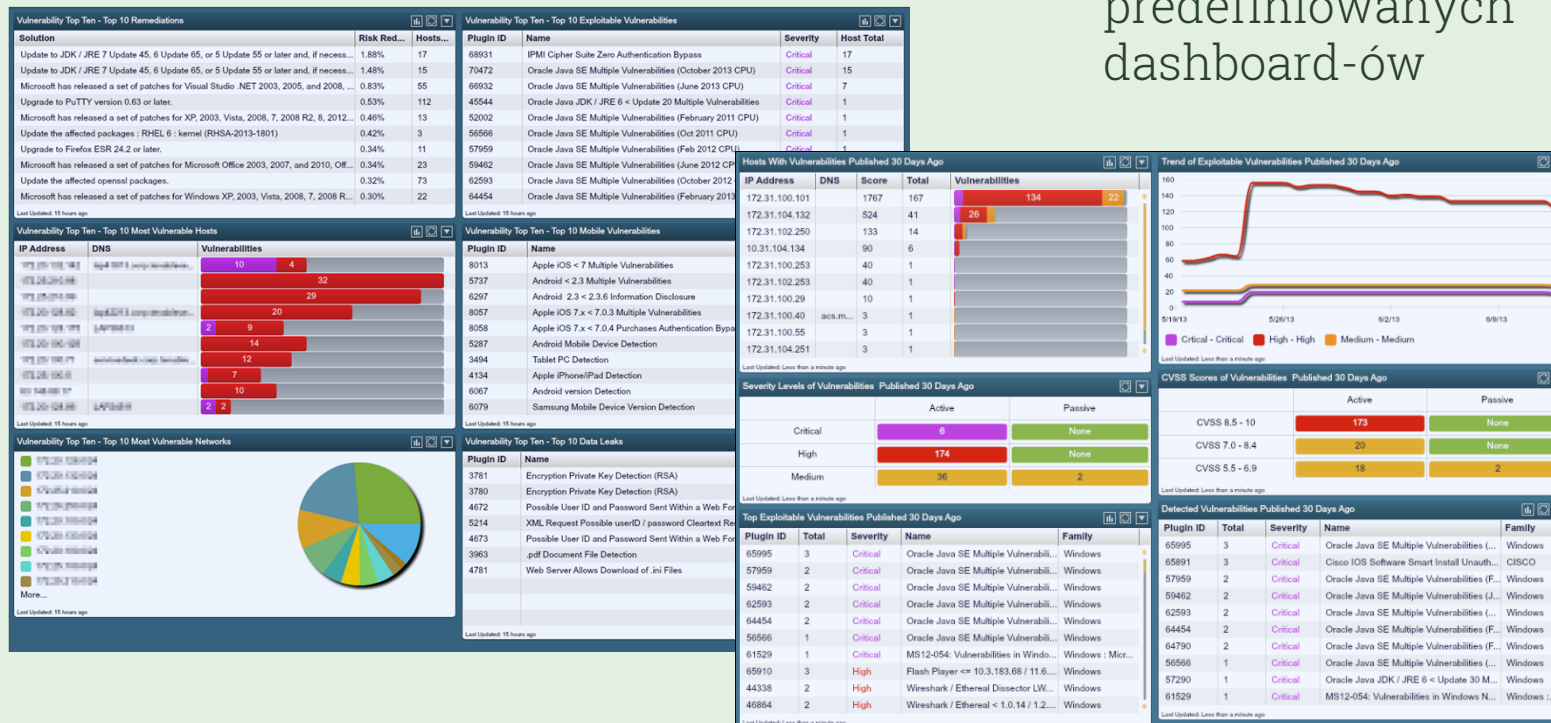
Microsoft has released patches for Windows NT, 2000, and Windows XP.

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)

Aktywna analiza bezpieczeństwa

Dwa z kilkuset predefiniowanych dashboard-ów



Vulnerability Top Ten

Vulnerabilities Over 30 Days

Karty realizacji celów strategicznych

SecurityCenter CV Dashboard Analysis Scans Reporting Assets Workflow Users Hi, UserName

Assurance Report Cards

+ Add Options

- CCC 1: Inwentaryzacja urządzeń i oprogramowania**
Ostatni raz oceniane 6 minut temu xxxxxx
- CCC 2: Podatności bezpieczeństwa i błędy konfiguracji**
Ostatni raz oceniane 7 minut temu xxxxxx
- CCC 3: Pomiar bezpieczeństwa sieci**
Ostatni raz oceniane 6 minut temu
 - ✓ 1. Maksymalnie 5% systemów dostępnych z zewnątrz posiada podatności 0/1
 - ✗ 2. Maksymalnie 5% urządzeń zabezpieczających (VPN, Firewall) posiada podatności 1/1
 - ✓ 3. Maksymalnie 5% systemów dostępnych przez VPN posiada podatności starsze niż 30 dni 0/0
 - ✓ 4. Maksymalnie 10% system używa niezabezpieczonych protokołów do połączeń ze światem zewnętrznym 0/0
 - ✗ 5. Ponad 90% firewalli przechowuje dzienniki w systemie zewnętrznym 0/1
 - ✗ 6. Ponad 95% systemów podłączonych do Internetu przechowuje logi w systemie zewnętrznym 0/1
- CCC 4: Bezpieczeństwo autoryzacji użytkowników, badanie zgodności z GIODO**
Ostatni raz oceniane 6 minut temu xxvx
- CCC 5: Wyszukiwanie oprogramowania szkodliwego oraz intruzów**
Ostatni raz oceniane 6 minut temu vvvvv



OB Badanie zgodności z GIODO

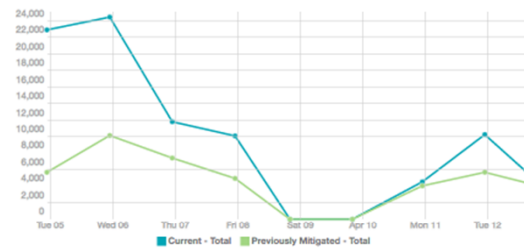
Last Evaluated 20 hours ago

	Systemy muszą posiadać ochronę antywirusową	2 / 4
	Minimalna długość hasła musi wynosić 8 znaków	4 / 4
	Wymóg rotacji haseł	4 / 4
	Hasło musi być zmieniane co 30 dni	4 / 4
	Hasło musi być skomplikowane	4 / 4
	Hasło nie może być przechowywane w postaci jawnej	4 / 4
	Blokada dostępu do konsoli po upłygnięciu okresu nieaktywności.	3 / 4
	System musi odnotowywać każdą operację logowania.	4 / 4
	W systemie nie mogą istnieć konta z przeterminowanymi hasłami	4 / 4
	System musi być chroniony zaporą sieciową	2 / 4

Executive Vulnerability Metrics

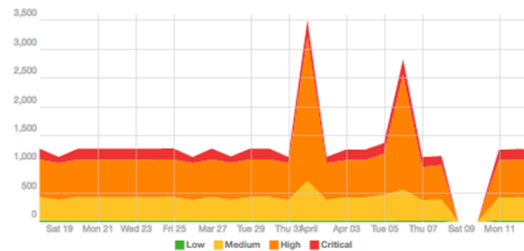
Switch Dashboard Options

Executive Vulnerability Metrics - Vulnerability Trend



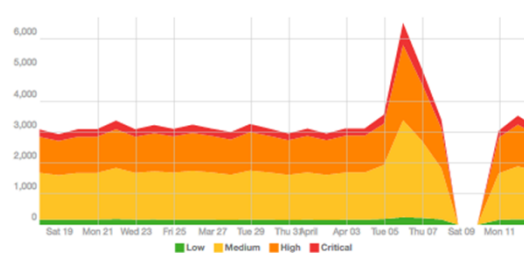
Last Updated: 23 minutes ago

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	90
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-ice-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

TOP 10 podatności w systemach i sieciach

SecurityCenter Dashboard Analysis Scans Reporting Assets Workflow Users

Vulnerability Top Ten

Switch Dashboard Options

Vulnerability Top Ten - Top 10 Most Vulnerable Windows Networks

Last Updated: 19 hours ago

Vulnerability Top Ten - Top 10 Most Vulnerable Linux/Unix Networks

Last Updated: 19 hours ago

Vulnerability Top Ten - Top 10 Most Vulnerable Apple Networks

Last Updated: 19 hours ago

Vulnerability Top Ten - Top 10 Most Vulnerable Hosts

IP Address	DNS	Total	Vulnerability Count
10.31.204.21	wrt81.corp.lab	105	102
10.31.104.140	grd-lptp.melc...	47	43
10.31.104.140		40	36
192.168.1.2		40	36
10.31.114.30	rhel.corp.lab	22	

Last Updated: 4 hours ago

Executive Vulnerability Metrics - Top 10 Previously Mitigated Hosts

IP Address	DNS	Total	Vulnerability Count
10.31.114.30	rhel.corp.lab	46	17 29
10.31.100.78	netflow.melcar...	45	16 29
10.31.114.15	exch2.corp.lab	31	24
10.31.114.10	dc02.corp.lab	12	
10.31.114.15		11	

Last Updated: Less than a minute ago

Vulnerability Top Ten - Top 10 Remediations

Solution	Risk	Count
Upgrade to Oracle JDK / JRE 8 Update 92, 7 Update 101, or 6 Update 115 or later. If	3.46%	13
Update the affected java-1.7.0-openjdk packages.	1.27%	15
Upgrade to Adobe Flash Player version 21.0.0.213 or later.	1.20%	2
Update the affected java-1.6.0-openjdk packages.	1.11%	11
Upgrade to Adobe AIR version 21.0.0.176 or later.	1.05%	3

Last Updated: 4 hours ago

Vulnerability Top Ten - Top 10 Exploitable Vulnerabilities

Plugin ID	Name	Severity	Count
88757	CentOS 6 : glibc (CESA-2016:0175)	Critical	12
84824	Oracle Java SE Multiple Vulnerabilities (July 2015)	Critical	7
77823	Bash Remote Code Execution (Shellshock)	Critical	3
78067	Bash Remote Code Execution (CVE-2014-6277 /	Critical	3
78385	Bash Incomplete Fix Remote Code Execution Vulnerability	Critical	3

Last Updated: 4 hours ago

Anti-Virus Summary - Outdated Anti-Virus Clients

Plugin ID	Name	Family	Severity	Total
12107	McAfee Antivirus Detection	Wind...	Critical	1
89940	McAfee VirusScan	Wind...	Low	1

Last Updated: Less than a minute ago

Vulnerability Top Ten - Top 10 Mobile Vulnerabilities

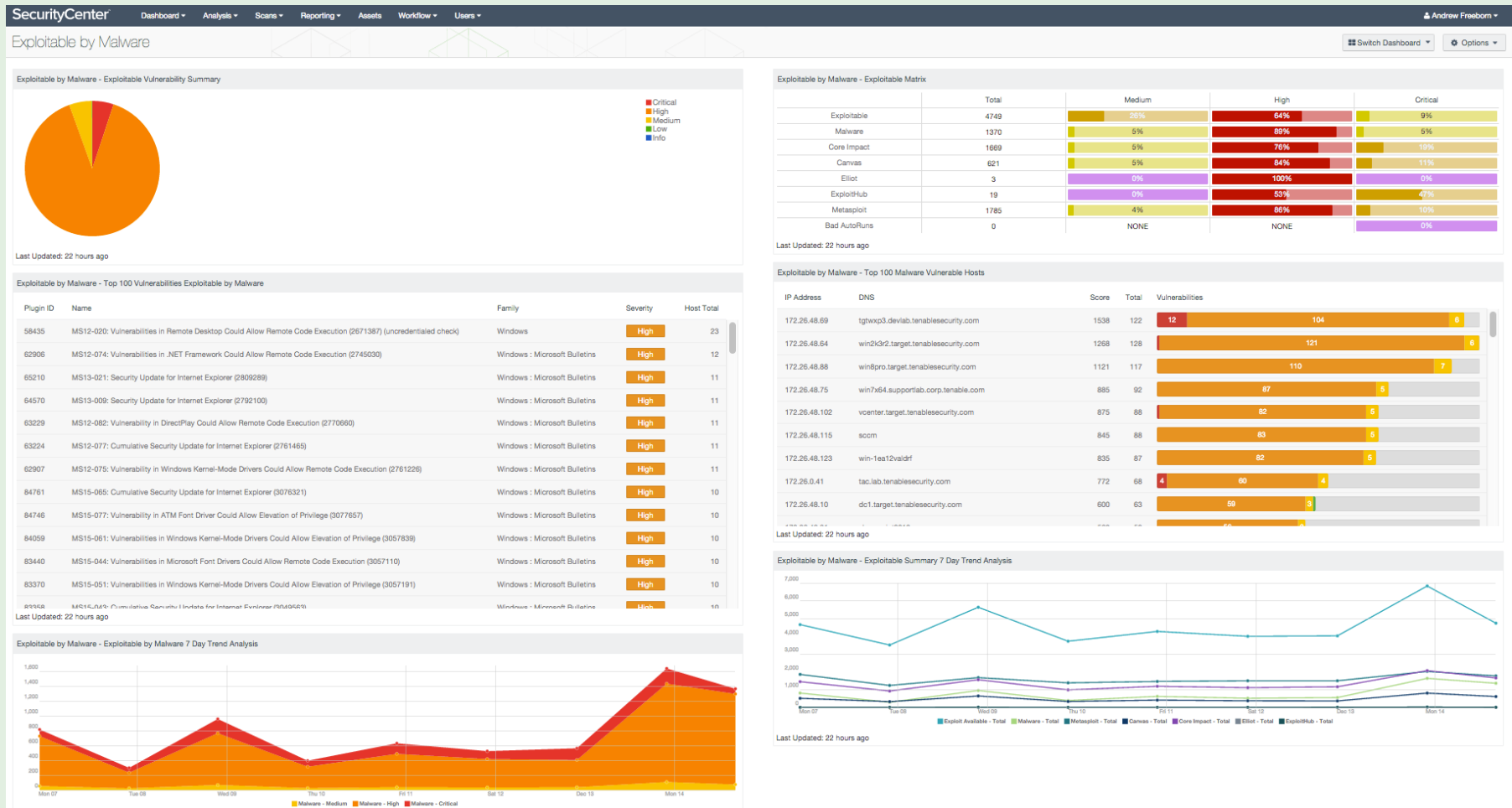
Plugin ID	Name	Severity	Count
4654	Apple iOS Device Model Detection	Info	4
8637	Apple iOS Version Detection	Info	4
9251	Tumblr Detection via HTTP	Info	1
8845	Apple iOS Version Detection via App Traffic	Info	1
5287	Google Android Operating System Version Detection	Info	1

Last Updated: 4 hours ago

SecurityCenter™ CV

continuous view

Wektory ataku dla Malware



Wykryte wektory ataku

SecurityCenter Dashboard Analysis Scans Reporting Assets Workflow Users

Predicting Attack Paths

Switch Dashboard Options

Predicting Attack Paths - Vulnerability Matrix

Compliance Vulnerabilities	Mobile Devices	Vulnerable Clients
Exploitability (Hard)	Exploitability (Medium)	Exploitability (Easy)
Active Exploits	Passive Exploits	Event Vulnerabilities
Core Impact Exploits	Metasploit Exploits	

Last Updated: 1 hour ago

Predicting Attack Paths - Exploitability Matrix

	Total	Exploitable	Metasploit	Core	Canvas	Malware
Local	94	44%	7	9	4	2
Network	1752	98%	0	121	22	26
Adjacent N...	20	20%	97	4	2	0

Last Updated: 1 hour ago

Predicting Attack Paths - Exploitable Internet Services

FTP	SSH	HTTP	HTTPS	SMB
1-200	201-500	501-1024	1025-5000	5000+

Last Updated: 1 hour ago

Predicting Attack Paths - Internet Browsing Clients

IP Address	NetBIOS	DNS	MAC Address
10.31.100.76		lce01.melcara.int	00:04:23:e7:69:67
10.31.100.57		pvs01.melcara.int	00:24:81:7f:07:8a

Last Updated: 1 hour ago

Predicting Attack Paths - External Connection Port Summary

Port	Total
443	2

Last Updated: 1 hour ago

Predicting Attack Paths - Hosts That Accept External Connections

IP Address	NetBIOS	DNS	MAC Address
10.31.100.75		sc10.melcara.int	da:32:01:5b:95:bd
10.31.100.55		sc02.melcara.int	00:30:48:63:43:b9

Last Updated: 1 hour ago

Predicting Attack Paths - Netstat Analysis

IP Address	NetBIOS	DNS	MAC Address	Vulnerabili...
10.31.204.60		centos.cor...	00:15:5d:cc...	1
10.31.204.22		centos.cor...	00:15:5d:cc...	1
10.31.114.134				1
10.31.114.74		scan01.me...	16:ea:e2:05...	1
10.31.114.54		scan02.me...	ee:17:6e:ed...	1
10.31.114.30		rhel.corp.lab	00:0c:29:45...	1
10.31.114.25	CORPL...	corp-pc1.c...	ba:33:bc:85...	1
10.31.114.20	CORPL...	sq12014.co...	42:8f:47:e3...	1
10.31.114.15	CORPL...	exch2.corp...	76:26:83:4a...	1
10.31.114.10	CORPL...	dc02.corp...	62:fd:55:db...	1
10.31.113.134		kali	00:0c:29:2e...	1
10.31.113.74				1
10.31.113.54				1
10.31.113.15	ACMEV...	mail.acme...	46:05:04:2f...	1
10.31.113.15	ACMEV...	exch1.acm...	46:05:04:2f...	1

Last Updated: 1 hour ago

Predicting Attack Paths - Established Client/Server Relationships (Last 90 days)

Last Updated: 6 minutes ago

Predicting Attack Paths - Event Trend Over Time (Total Events)

Last Updated: 1 hour ago

Predicting Attack Paths - Most Trusted Servers

IP Address	DNS	Total	Vulnerabilities
10.31.100.76	lce01.melcara.int	1	1
10.31.100.40	acs.melcara.int	1	1
10.31.100.10	dc01.melcara.int	15	15

Last Updated: 1 hour ago

Predicting Attack Paths - Vulnerabilities by Common Ports

	Low	Medium	High	Critical	Exploitable
FTP/21	0	0	0	0	0%
SSH/22	32	28	1	4	13%
Telnet/23	0	3	0	0	0%
SMTP/25	0	1	0	0	100%
DNS/53	0	3	0	0	0%
HTTP/80	1	2	2	1	100%
RPC/111	0	0	0	0	0%
NetBIOS/137	0	0	0	0	0%
HTTPS/443	6	20	2	1	85%
SMB/445	18	18	18	13	100%

Last Updated: 1 hour ago

Vulnerability Top Ten - Top 10 Most Vulnerable Hosts

IP Address	DNS	Total	Vulnerabilities
192.168.1.10	server1.example.com	258	17 / 241
192.168.1.11	server2.example.com	256	17 / 239
192.168.1.12	server3.example.com	229	9 / 218
192.168.1.13	server4.example.com	229	9 / 220
192.168.1.14	server5.example.com	124	24 / 100
192.168.1.15	server6.example.com	122	22 / 100
192.168.1.16	server7.example.com	130	17 / 113
192.168.1.17	server8.example.com	152	9 / 143
192.168.1.18	server9.example.com	127	17 / 110
192.168.1.19	server10.example.com	152	8 / 144

Last Updated: 20 hours ago

Vulnerability Summary - Exploitable Vulnerabilities

All Vulns	By Metasploit	Windows	Mac OS X	Linux/UNIX
Web	Mobile	Malicious	Common Apps	Open Source Apps
Default	Java	Service	SQL	SSL
Unsupported	Virus	Vuln Event	Accepted Risks	Recast to Info Risks

Last Updated: 20 hours ago

Track Mitigation Progress - Vulnerability Summary by Severity

	Mitigated	Unmitigated	Exploitable	Patch Available >30d	Exploitable Hosts
Total	16625	89797	15%	89%	880
Critical	1856	3254	49%	96%	456
High	6931	58143	12%	97%	454
Medium	7362	26156	20%	78%	782
Low	476	2244	9%	88%	101

Last Updated: 20 hours ago

CSC - Continuous Vulnerability Scanning

	Total Systems	Scan <30 Days	Credentialed Scans
NetStats	1479	50%	16%

Last Updated: 20 hours ago

Targeted Event Monitoring - Vulnerability Events in Last 72 Hours

Event	Count	Trend Data
PVS-Medium_Vulnerability	965	
PVS-High_Vulnerability	330	
StealthWatch-Multiple_Operating_Systems	54	
PVS-Low_Vulnerability	48	
RNA-UDP_Service_Confidence_Update	46	

Last Updated: 20 hours ago

Understanding Risk - Remediation Opportunities

Solution	Risk Reduction	Host Total
Apply MS16-014: Security Update for Microsoft Windows to Address Remote Code Execution (3134228)	4.11%	161
Apply MS16-039: Security Update for Microsoft Graphics Component (3148522)	3.93%	161
Apply MS16-044: Security Update for Windows OLE (3146706)	3.91%	163
Apply MS16-035: Security Update for .NET Framework to Address Security Feature Bypass (3141780)	3.86%	163
Apply MS15-132: Security Update for Microsoft Windows to Address Remote Code Execution (3116162)	3.86%	162

Last Updated: 20 hours ago

SecurityCenter Dashboard Analysis Scans Reporting Assets Workflow Users cody

Compliance Summary

Switch Dashboard Options

Compliance Summary - Indicators

8500.2	800-53	BSI-100-2
CAT	CCE	CCI
COBIT	CSA-CSM3	CSF
CVE	Group-ID	HIPAA
ISO/IEC-27001	Level	NIST_800-125a
PCI	VMWare	Rule-ID
SANS-CSC	STIG-ID	Vuln-ID

Last Updated: 1 hour ago

Compliance Summary - 25 Day Trend

Last Updated: 3 hours ago

Compliance Summary - CIS, DOD & NIST Bar Ratio

	Systems	Passed	Manual Check	Failed
800-53	3	33%	13%	47%
8500.2	2	28%	49%	23%
CAT	2	28%	49%	23%
CCE	1	40%	20%	40%
CCI	0	0	0	0
CSF	2	0	0	100%
Level	0	0	0	0
NIST_800-125a	0	0	0	0
SANS-CSC	0	0	0	0

Last Updated: Less than a minute ago

Compliance Summary - CIS, DOD & NIST Indicators

	Systems	Passed	Manual Check	Failed
800-53	3	✓	!	✗
8500.2	2	✓	!	✗
CAT	2	✓	!	✗
CCE	1	✓	!	✗
CCI	0	0	0	0
CSF	2	0	0	✗
Level	0	0	0	0
NIST_800-125a	0	0	0	0
SANS-CSC	0	0	0	0

Last Updated: 4 minutes ago

Compliance Summary - Industry Compliance Standards Ratio Bar

	Systems	Passed	Manual Check	Failed
BSI-100-2	0	0	0	0
COBIT	2	0	0	100%
CSA-CSM3	0	0	0	0
CVE	0	0	0	0
HIPAA	2	52%	0	48%
ISO/IEC-27001	1	0	0	100%
PCI	1	42%	18%	40%
VMWare	0	0	0	0

Last Updated: 1 hour ago

Compliance Summary - Industry Compliance Standards Indicators

	Systems	Passed	Manual Check	Failed
BSI-100-2	0	0	0	0
COBIT	2	0	0	✗
CSA-CSM3	0	0	0	0
CVE	0	0	0	0
HIPAA	2	✓	0	✗
ISO/IEC-27001	1	0	0	✗
PCI	1	✓	!	✗
VMWare	0	0	0	0

Last Updated: 1 hour ago

Compliance Summary - STIG Audit Check Ratio Bar

	Systems	Passed	Manual Check	Failed
Group-ID	0	0	0	0
Rule-ID	2	28%	49%	23%
STIG-ID	2	28%	49%	23%
Vuln-ID	2	28%	49%	23%

Last Updated: 1 hour ago

Compliance Summary - STIG Audit Check Indicators

	Systems	Passed	Manual Check	Failed
Group-ID	0	0	0	0
Rule-ID	2	✓	!	✗
STIG-ID	2	✓	!	✗
Vuln-ID	2	✓	!	✗

Last Updated: 1 hour ago

OWASP Top 10

SecurityCenter
Hi, Cody Dumont [cdumont]

Dashboard Analysis Scans Reporting Assets Workflow

OWASP Top 10

Switch Dashboard

OWASP Top 10 - 90 Day Trend Analysis for Critical Severity Web Vulnerabilities

Last Updated: 2 minutes ago

OWASP Top 10 - 90 Day Trend Analysis for High Severity Web Vulnerabilities

Last Updated: 2 minutes ago

OWASP Top 10 - Top 10 Indicators

	System	Vulnerabilities	Exploitable
A1 - Injection	4	5	0%
A2 - Broken Authentication and	45	59	3%
A3 - Cross-Site Scripting (XSS)	4	4	75%
A4 - Insecure Direct Object	104	283	3%
A5 - Security Misconfiguration	73	229	39%
A6 - Sensitive Data Exposure	42	53	32%
A7 - Missing Function Level Access	0	0	0%
A8 - Cross-Site Request Forgery	0	0	0%
A9 - Using Known Vulnerable	66	98	98%
A10 - Unvalidated Redirects and	22	40	15%

Last Updated: 5 hours ago

OWASP Top 10 - Web Informational Vulnerabilities

Plugin ID	Name	Family	Severity	Total
10107	HTTP Server Type and Version	Web Servers	Info	2246
24260	HyperText Transfer Protocol (HTTP) Information	Web Servers	Info	472
1442	Web Server Detection	Web Servers	Info	397
10386	Web Server No 404 Error Code Check	Web Servers	Info	300
43111	HTTP Methods Allowed (per directory)	Web Servers	Info	208

Last Updated: 5 hours ago

OWASP Top 10 - Web App Result Indicator

Injection	Overflow
SSL	Error Handling
CGI Generic	XSS
High Web Vulns	Critical Web Vulns

Last Updated: 5 hours ago

OWASP Top 10 - Web Events

Web Intrusion	Web Threatlist
Web Stats	Long Term Web Error Activity
PVS Detected Web Error	PVS Detected Web Access
Apache Web Error	Apache Web Access
IIS Web Error	IIS Web Access

Last Updated: 5 hours ago

OWASP Top 10 - SQL Events

Suspicious SQL User Database Dump	Suspicious SQL Command Execution
Suspicious SQL Injection Attack Detected	Suspicious SQL Query Detected
SQL Intrusion	Database Stats
SQL Error	SQL Login Failure

Last Updated: 5 hours ago

Zgodność z normami CIS

SecurityCenter Dashboard Analysis Scans Reporting Assets Workflow Users

CIS Audit Summary Switch Dashboard Options

CIS - Amazon & Debian Linux Benchmarks

	Systems	Passed	Manual	Failed
Amazon Linux v2.0.0	1	8	0	58
BIND 9.0-9.5 v2.0.0	0	0	0	0
Debian v1.0	3	248	0	365
Debian Linux 7 v1.0.0	1	107	4	172
Debian Linux 8 v1.0.0	2	208	18	316
Distribution Independent...	25	2409	298	4561

Last Updated: 6 minutes ago

CIS - Apache Benchmarks

	Systems	Passed	Manual	Failed
Apache HTTP Server 2.2...	14	492	172	787
Apache HTTP Server 2.4...	1	37	4	62
Apache Tomcat v1.0.0	2	72	8	96

Last Updated: 6 minutes ago

CIS - Apple Benchmarks

	Systems	Passed	Manual	Failed
Apple Safari v1.0.0	8	16	0	80
Mac OSX 10.5 v1.0	0	0	0	0
Mac OSX 10.6 v1.0.0	1	22	57	69
Mac OSX 10.9 v1.0.0	2	46	18	118
Mac OSX 10.10 v1.2.0	8	34	3	48
Mac OSX 10.11 v1.1.0	8	34	30	65
macOS 10.12 v1.0.0	8	51	93	51

Last Updated: 5 minutes ago

CIS - CentOS Linux Benchmarks

	Systems	Passed	Manual	Failed
CentOS Linux 6 v2.0.1	4	76	4	76
CentOS Linux 7 v2.1.0	4	46	3	30

Last Updated: 5 minutes ago

CIS - Cisco Benchmarks

	Systems	Passed	Manual	Failed
Cisco IOS v3.0.1	3	76	0	293
Cisco IOS 12 v4.0.0	3	116	4	186
Cisco IOS 15 v4.0.0	3	0	0	6
Cisco Firewall 4.0.0	1	12	8	74

CIS - Juniper Junos Benchmarks

	Systems	Passed	Manual	Failed
Juniper Junos v1.0.1	1	44	17	69

Last Updated: 6 minutes ago

CIS - Microsoft IIS Benchmarks

	Systems	Passed	Manual	Failed
IIS v1.0	1	43	9	47
IIS 7 v1.7.1	7	231	63	175
IIS 8 v1.4.0	12	165	16	95

Last Updated: 6 minutes ago

CIS - Microsoft Servers Benchmarks

	Systems	Passed	Manual	Failed
Windows Server 2003 v...	15	1146	1583	841
Windows Server 2008 v...	9	737	27	1280
Windows Server 2008 n...	9	18	54	36
Windows Server 2008 R...	9	768	1869	702
Windows Server 2012 n...	6	544	938	777
Windows Server 2012 R...	11	10	16	9
Exchange Server 2007 v...	0	0	0	0

Last Updated: 5 minutes ago

CIS - Microsoft SQL Server Benchmarks

	Systems	Passed	Manual	Failed
SQL Server 2008 R2 v1.4.0	6	31	2	15
SQL Server 2012 v1.3.0	6	31	0	6
SQL Server 2014 v1.2.0	6	55	5	17

Last Updated: 5 minutes ago

CIS - Microsoft Workstations Benchmarks

	Systems	Passed	Manual	Failed
Windows XP v3.1.0	1	114	80	73
Windows 7 v3.0.0	2	175	381	258
Windows 8 v1.0.0	1	137	126	68
Windows 8.1 v2.2.0	1	77	132	234
Windows 10 Release 15...	2	184	659	137

Last Updated: 6 minutes ago

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

Przykład synergii – detekcja danych wrażliwych

Potential Sensitive Information (Active Scanning)

Copyright [FTP]	Copyright [SMB]	Copyright [HTTP]	Office Files [SMB]
Office Files [HTTP]	SMB Shares	USB Drives	NFS Exports
P2P Sharing	Databases		

Last Updated: Less than a minute ago

Systems with Sensitive Data

IP Address	NetBIOS	DNS	Total
172.31.100.11	UNKNOWN\DC02		30
172.26.22.195	UNKNOWN\AUDITORACLE		226
172.26.22.150			16
172.26.22.127			254
172.26.22.100	UNKNOWN\RESEARCH3		1
172.26.22.63	UNKNOWN\AUDIT-WINDOWSXP		174
172.26.0.19			45
172.26.0.15			1
10.31.254.254		portal.redhat.com	471
10.31.104.253			471

Last Updated: Less than a minute ago

Asset Sensitive Data Audits and Results

Sensitive Docs	Exploitable Vulns	Recent Scan
!	✘	✔

Last Updated: Less than a minute ago

Sensitive Data Last 25 Days

Last Updated: Less than a minute ago

Sensitive Data Types

Plugin ID	Name	Severity	Total
1002804	RedHat/CentOS 6 is not installed on target	Medium	1
1002803	RHEL-06-000525 - Auditing must be enabled at b...	Medium	7
1002802	RHEL-06-000524 - The system must provide aut...	Medium	7
1002801	RHEL-06-000521 - The mail system must forwar...	Medium	7
1002800	RHEL-06-000505 - OS must conduct backups of ...	Medium	7
1002799	RHEL-06-000504 - OS must conduct backups of ...	Medium	7
1002798	RHEL-06-000356 - System must require admin a...	Medium	7
1002797	RHEL-06-000349 - System must require the use ...	Medium	7
1002796	RHEL-06-000339 - The SSH daemon must restri...	High	7
1002795	RHEL-06-000338- TFTP daemon must operate i...	High	7

Last Updated: Less than a minute ago

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, GIDODO, 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>



DZIĘKUJĘ ZA UWAGĘ

tenable@openbiz.pl