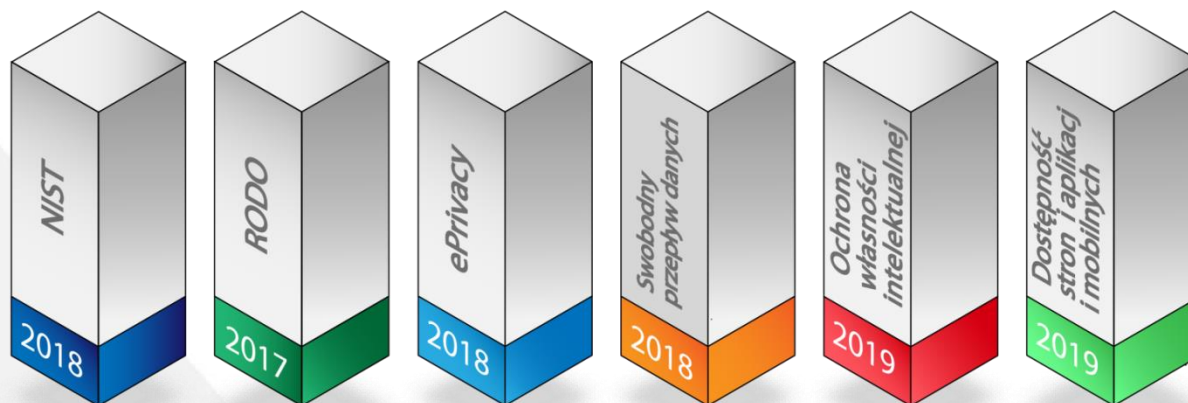


Zaufać drugiej stronie

Jakub Jagielak
Security Business Development Director
Atende S.A.

Fakty i mity

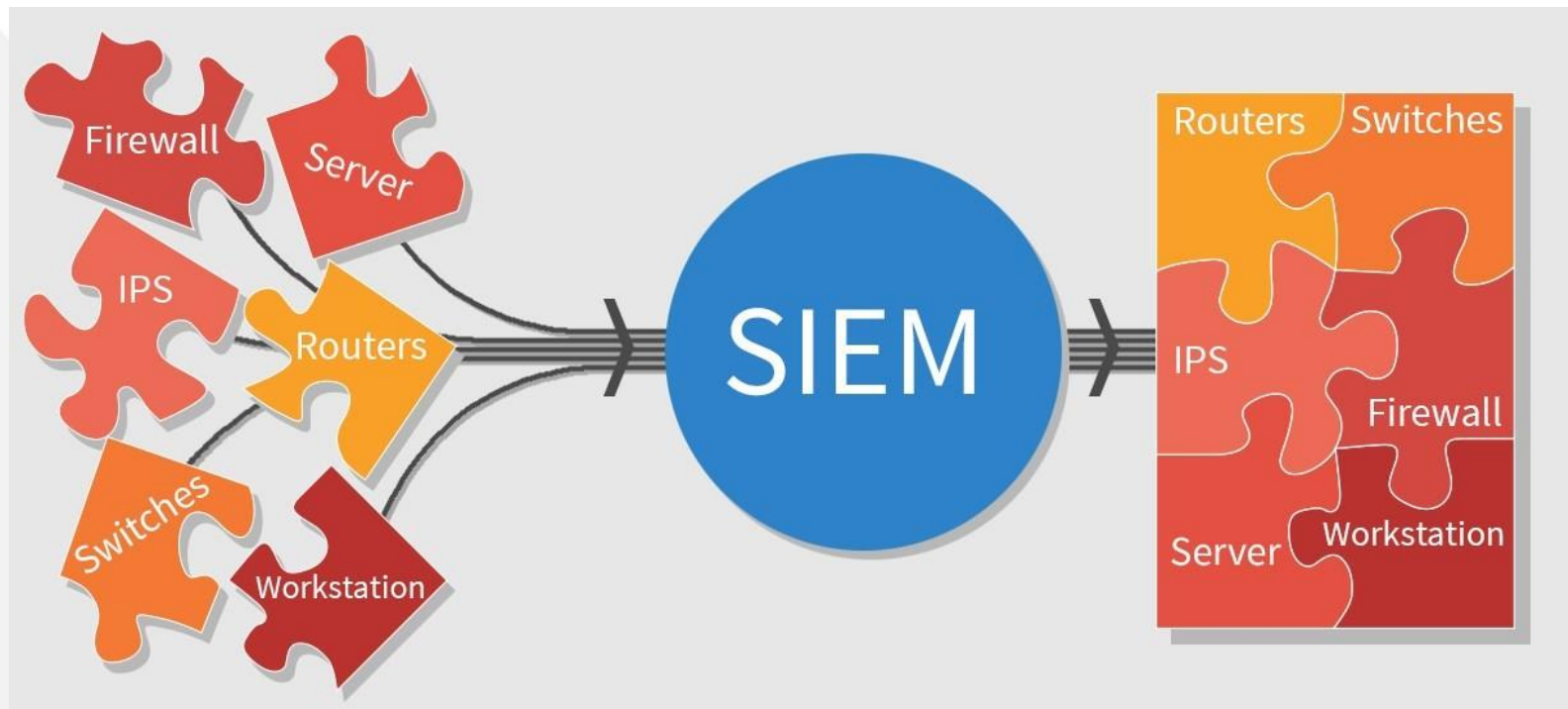
Silne hasło jest wystarczające by czuć się bezpiecznym	Istotne jest podwójne uwierzytelnianie i monitoring
Mały i średni biznes nie jest celem ataku hakerów	Ponad połowa ataków skierowana była na sektor SMB
Tylko wybrane sektory są podatne na ataki hakerskie	Każdy biznes zawierający istotne dane jest narażony na ataki
AntyMalware i AntyWirus zapewniają wysokie bezpieczeństwo	Software nie chroni przed cyberatakami.
zagrożenie bezpieczeństwa cybernetycznego pochodzi z zewnątrz	zagrożenie z wewnątrz jest równie prawdopodobne i trudniejsze do wykrycia



KNF – Rekomendacja D

- **Wytyczne dotyczące zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego**
- przygotowane przez KNF, które sektor finansowy miał obowiązek wdrożyć do 2016 roku
- Ze zbioru 22 zasad 14 porządkowało wiedzę i praktyki już w bankach wykorzystywane,
- 8 wymagało wprowadzenia fundamentalnych zmian.
- Najtrudniejsze obszary z jakimi przyszło się bankom zmierzyć związane były przede wszystkim z jakością danych oraz operacyjnym reagowaniem na incydenty bezpieczeństwa.





RESCANA DLA KOGO

- Organizacji które mają problemy z oceną ryzyka cybernetycznego swojego i partnerów.
- Z wąskim gardłem w biznesie w onboardingu, fuzjach i przejęciach z ręcznym, długimi i kosztownym audytami bezpieczeństwa.
- Zajęty reagowaniem na zapytania dotyczące ryzyka cybernetycznego firmy.
- Brak pełnego, spójnego i aktualnego śladu internetowego. Trudności z pozyskaniem informacji.
- Zaangażowanych w niekończące się audyty aby spełnić różne standardy regulacyjne.



Nowe i ewoluujące regulacje,
takie jak GDPR, PSD2, wymagają
zarządzania ryzykiem
cybernetycznym firmy i jej
partnerów

Rescana zapewnia automatyczną
ciągłą ocenę, która jest
obiektywna i zgodna z polityką
firmy

Wielokrotne prośby o kontrolę
i ocenę ryzyka firmy
współpracujących i
zewnętrznych dostawców

Rescana umożliwia wymianę
wyników oceny i audytu
pomiędzy organizacjami
współpracującymi

Partnerzy wykazują różne
poziomy dojrzałości swoich
systemów bezpieczeństwa i
często niespójne zgłaszanie
ryzyka

Automatyczne i ciągłe
wykrywanie zasobów firmy
zmniejszające ręczną pracę

COMPANIES

Poker
Champs
Risk Score



Intel Score: 34 Survey
Score: 3

Soccer
Gamble
Risk
Score



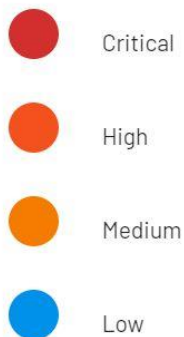
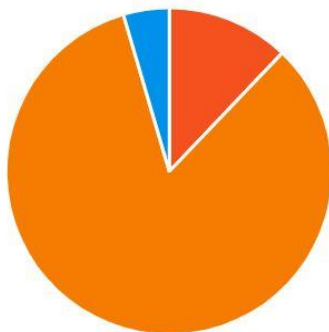
Intel Score: 67 Survey
Score: N/A

 Casinoline
Risk Score



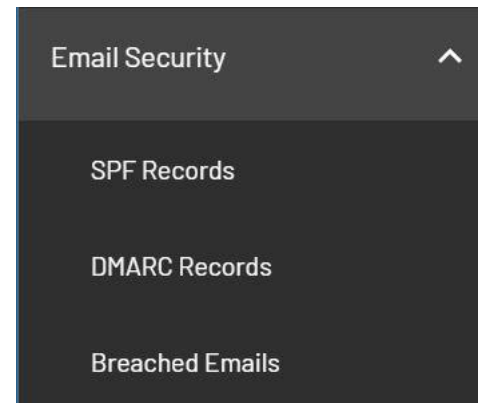
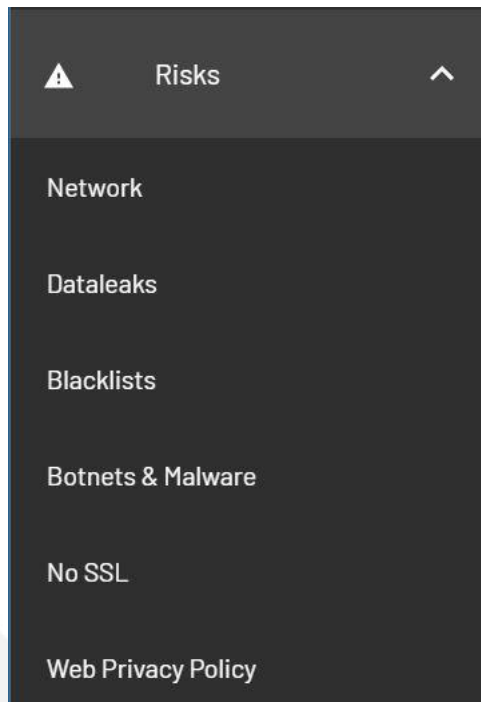
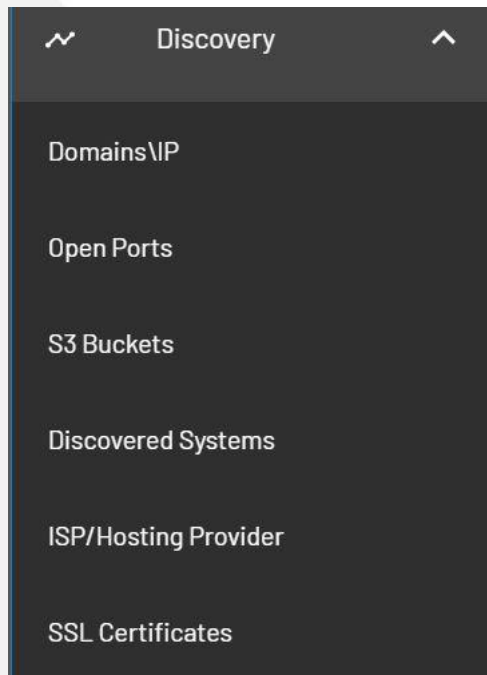
Intel Score: 17 Survey
Score: N/A

CVE SEVERITY



TOP 5 VULNERABLE DOMAINS

interviu.librabank.ro	60
edepozit.librabank.ro	54
transfer.librabank.ro	32
health.casinoclient.bwin.com	28
edesk.librabank.ro	27



Przykładowy raport

Domains with SPF Records

DOMAIN	SUBDOMAIN	SPF
examplesoccergambles.fr	none	v=spf1 ip4:10.XXX.XXX.XXX ip4:195.XX.XXX.0/24 mx include:spf-gib2-others.socexamplepp.com include:spf-gci.socexamplepp.com include:spf-vie.socexamplepp.com -all
casinogamblesexample	none	v=spf1 ip4:10.XXX.XXX.XXX /24 a mx -all
examplesoccergambles.com	none	v=spf1 ip4:10.XXX.XXX.XXX ip4:195.XX.XXX.0/24 mx include:spf-gib2-others.socexamplepp.com include:spf-gci.socexamplepp.com include:spf-vie.socexamplepp.com -all
casinogamblesoccerexample.net	none	No Records Found
examplesoccergambles.es	none	v=spf1 ip4:10.XXX.XXX.XXX ip4:193.XXX.XXX.XXX ip4:193.XXX.XXX.XXX ip4:93.XXX.XXX.XXX/24 ip4:293.XXX.XXX.XXX ip4:93.XXX.XXX.XXX/24 mx include:spf-gib2
examplesoccergambles.gr	none	v=spf1 ip4:10.XXX.XXX.XXX ip4:195.XX.XXX.0/24 mx include:spf-gib2-others.socexamplepp.com include:spf-gci.socexamplepp.com include:spf-vie.socexamplepp.com -all

Przykładowy raport

DISCOVERED SYSTEMS

Discovered Systems found on the network.

Domain	Subdomain	IP Address	Port	Product
examplesocccergambles.fr	api.examplesocccergambles.fr	193.XXX.XXX.XXX	80	Microsoft HTTPAPI httpd
examplesocccergambles.fr	api.examplesocccergambles.fr	193.XXX.XXX.XXX	80	Microsoft IIS httpd
examplesocccergambles.fr	simg.examplesocccergambles.fr	193.XXX.XXX.XXX	443	Omniure DC
examplesocccergambles.fr	promos.examplesocccergambles.fr	193.XXX.XXX.XXX	80	Microsoft IIS httpd
examplesocccergambles.fr	promos.examplesocccergambles.fr	193.XXX.XXX.XXX	443	Microsoft IIS httpd
examplesocccergambles.fr	promos.examplesocccergambles.fr	193.XXX.XXX.XXX	80	Microsoft IIS httpd
examplesocccergambles.fr	promos.examplesocccergambles.fr	193.XXX.XXX.XXX	443	Microsoft IIS httpd
examplesocccergambles.fr	www.examplesocccergambles.fr	193.XXX.XXX.XXX	80	Microsoft HTTPAPI httpd

Przykładowy raport

VULNERABLE IPS					
Vulnerable IPs on the network					
DOMAINS	IP	CPE	CVE	CVE SCORE	CVE SUMMARY
fun.soccerexampleg.ro	185.XX.XXX.XXX	apache http_server 2.2.15	CVE-2011-3192	7.8	The byterange filter in the Apache HTTP Server 1.3.x, 2.0.x through 2.0.64, and 2.2.x through 2.2.19 allows remote attackers to cause a denial of service (memory and CPU consumption) via a Range header that expresses multiple overlapping ranges, as exploited in the wild in August 2011, a different vulnerability than CVE-2007-0086. The byterange filter in the Apache HTTP Server 1.3.x, 2.0.x through 2.0.64, and 2.2.x through 2.2.19 allows remote attackers to cause a denial of service (memory and CPU consumption) via a Range header that expresses multiple overlapping ranges, as exploited in the wild in August 2011, a different vulnerability than CVE-2007-0086.

Przykładowy raport

BLACKLISTS

Some of the domains for found in various blacklists, this can sometimes indicate a compromised IP address/domain/MX record that is being used for spreading spam in malware.

Domain	IP Address	Blacklists for IP Address	MX Records	Blacklist for MX Records	NS Records	Blacklists for NS Records
hi.soccerexampleg.ro	119.XXX.XXX.X XX	None	mail.soccere xampleg.ro	MARTENSON -DED, LISINGE-DED	ns.rsoccerexa mpleg.ro, ns2.resoccerex ampleg.ro	None
occerexampleg.be	119.XXX.XXX.X XX	None	mail.soccere xampleg.ro	MARTENSON -DED, LISINGE-DED	ns.rsoccerexa mpleg.ro, ns2.resoccerex ampleg.ro	None
occerexampleg.fr	119.XXX.XXX.X XX	None	mail.soccere xampleg.ro	MARTENSON -DED, LISINGE-DED	ns.rsoccerexa mpleg.ro, ns2.resoccerex ampleg.ro	None

Dziękuję za uwagę.

jakub.jagielak@atende.pl