FIREWALL TO ZA MAŁO.

JAK SKUTECZNIE CHRONIĆ URZĘDOWĄ SIEĆ W DOBIE ATAKÓW TYPU APT I RANSOMWARE?

Aleksander Kostuch
Inżynier wsparcia sprzedaży
Aleksander.Kostuch@Stormshield.eu

WYBRANE ATAKI

Hakerzy okrad Malborku. Pra wystarczył jed

I.O., pszl | publikacja: 10.06.2015 | aktualiza

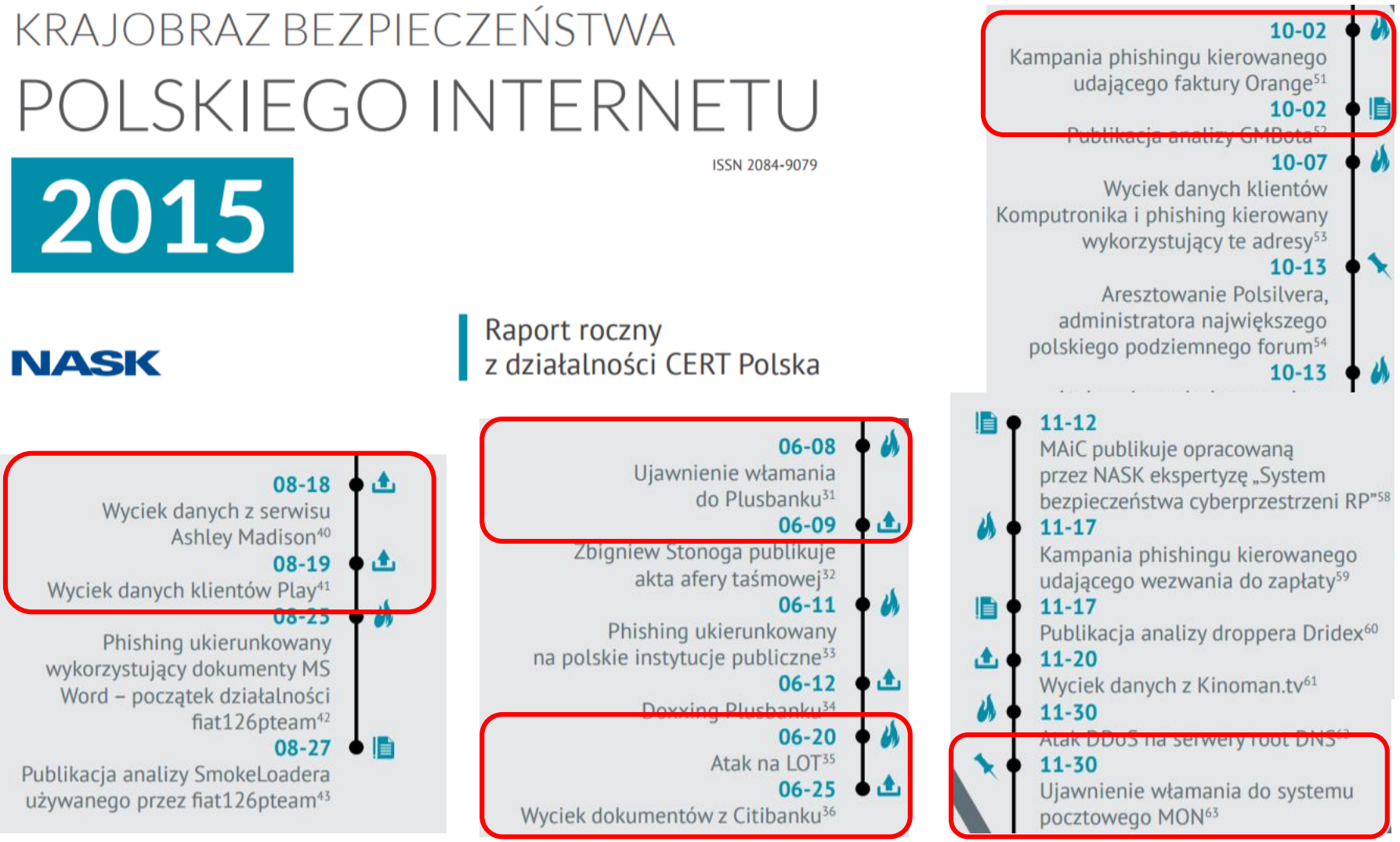
Prokuratura zaznacza, że namierzenie osz

20 tys. zł przelał za pośrednictwe pracowników Powiatowego Urzęd dziwnego, gdyby nie to, że pienią planowano. Urząd padł ofiarą ata prokuratura.

Jabłonna. Władze SZPZOZ o zaszyfrowaniu bazy danych pacjentów

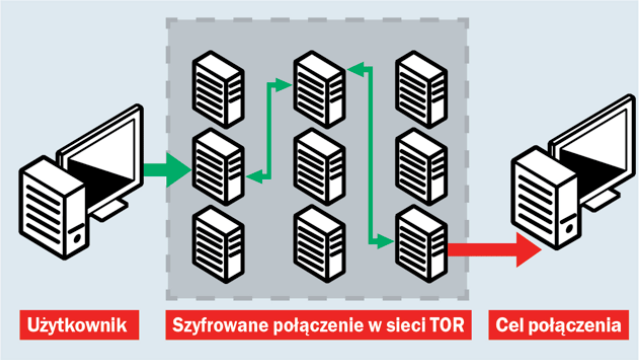
22 Września 2016 | Komentarzy: 3 | Jabłonna | Redakcja

CERT 2015


KRAJOBRAZ BEZPIECZEŃSTWA
POLSKIEGO INTERNETU
2015
ISSN 2084-9079
NASK
Raport roczny
z działalności CERT Polska
08-18
Wyciek danych z serwisu Ashley Madison[40]
08-19
Wyciek danych klientów Play[41]
08-25
Phishing ukierunkowany wykorzystujący dokumenty MS Word – początek działalności fiat126pteam[42]
08-27
Publikacja analizy SmokeLoadera używanego przez fiat126pteam[43]
06-08
Ujawnienie włamania do Plusbanku[31]
06-09
Zbigniew Stonoga publikuje akta afery taśmowej[32]
06-11
Phishing ukierunkowany na polskie instytucje publiczne[33]
06-12
Doxxing Plusbanku[34]
06-20
Atak na LOT[35]
06-25
Wyciek dokumentów z Citibanku[36]
10-02
Kampania phishingu kierowanego udającego faktury Orange[51]
10-02
Publikacja analizy GMBota[52]
10-07
Wyciek danych klientów Komputronika i phishing kierowany wykorzystujący te adresy[53]
10-13
Aresztowanie Polsilvera, administratora największego polskiego podziemnego forum[54]
10-13
11-12
MAiC publikuje opracowaną przez NASK ekspertyzę „System bezpieczeństwa cyberprzestrzeni RP"[58]
11-17
Kampania phishingu kierowanego udającego wezwania do zapłaty[59]
11-17
Publikacja analizy droppera Dridex[60]
11-20
Wyciek danych z Kinoman.tv[61]
11-30
Atak DDoS na serwery root DNS[62]
11-30
Ujawnienie włamania do systemu pocztowego MON[63]

PRZEGLĄDARKI TOR

The Onion Router



ilustracja: Komputer Świat

- **ANONIMIZACJA**

Pierwszy serwer proxy podmienia przy tym adres IP peceta na własny. Na każdym następnym przystanku oznaczenie zmienia się kolejny raz

- **SZYFROWANIE**

Tor wysyła zaszyfrowane zapytania i adresy IP użytkownika do operatora strony. Każdy serwer proxy w łańcuchu rozszyfrowuje dane poprzedniego proxy i szyfruje je ponownie dla następnego.

- **ZASADA PRZYPADKU**

Co dziesięć minut wybierana jest nowa, przypadkowa droga przez sieć serwerów proxy.

- **OTWARTOŚĆ**

Open Source

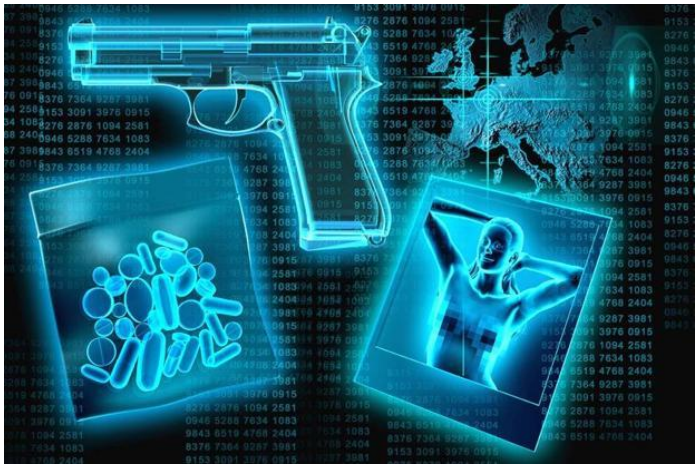
trasowanie cebulowe

Zacieranie cyfrowych śladów w Internecie

DARKNET

- Dysydenci
- Organizacje medialne
- Nielegalne materiały
- Dane dostępowe
- Dane kart kredytowych
- Broń

Płatność: Bitkoiny



ilustracja: https://www.deepdotweb.com/2015/04/15/so-you-want-to-be-a-darknet-drug-lord/

Anonimowa droga przekazywania informacji

WYNAJMĘ HAKERA

- włamania na konto społecznościowe,
- hackowanie scammera,
- odzyskiwanie pieniędzy,
- przywrócenie hasła,
- poprawa stopni w elektronicznym dzienniku,
- sprawdzenie bezpieczeństwa strony internetowej.

Ilustracja:komputerwfirmie.org

- TOR
  - wykupienie profesjonalnej internetowej aplikacji
  - przeprowadzenie własnego ataku z wykorzystaniem ransomware

Korzyści są sprawiedliwie dzielone pomiędzy klienta i sprzedawcę usługi:
Malware as a Service

RANSOM (OKUP) + SOFTWARE = RANSOMWARE

- Przestępcy podszywali się pod powiadomienia wysyłane przez Pocztę Polską
- Link przekierowywał użytkownika na stronę będący złośliwą aplikacją dla systemu Windows lub Android
- Zabezpieczone hasłem pliki zip oraz dokumenty ze złośliwymi makra pobierającymi i instalującymi złośliwe oprogramowanie.
- Program partnerski internetowych kasyn, reklamowanych w spamowych wiadomościach
- Szyfrowanie danych użytkownika dla okupu

CRYPTOWALL/ CONFICKER / CRYPTOLOCKER/ OPFAKE

- Szyfrowania ważnych dla użytkownika plików
- Prosi o zapłacenie grzywny
- .docx, .pdf, .txt, .img, .gif, .mp3, .mp4, .flv

HELP_YOUR_FILES.TXT
HELP_YOUR_FILES.HTML
HELP_YOUR_FILES.PNG

Cannot you find the files you need?
Is the content of the files that you have watched not readable?
It is normal because the files' names, as well as the data in your files have been encrypted.
Congratulations!!!
You have become a part of large community CryptoWall.
[…]
For your attention, the software to decrypt the files (as well as the private key that come fitted with it) is a paid product.

AWARIE BANKOMATÓW

- Sieć Bankomatów, podobnie jak w 2013
- IB, rosyjska grupa zajmująca się cyberbezpieczeństwem, przekazała, że problemy z bankomatami, które wystąpiły w Polsce, Holandii, Wielkiej Brytanii, Armenii, Estonii, Rosji i Hiszpanii
- Wypłaty zlecone przez ludzi były księgowane w bankach, jednak bankomaty pieniędzy nie wydawały
- Konkretne bankomaty, wybrane przez hakerów, w tym samym momencie wypłacały pieniądze, które wcześniej powinny wydać użytkownikom

Ilustracja: fotolia (Wprost)

18.11.2016
touchless jackpotting

20.11.2016

SCAM - POPRZEZ CZAT NA FACEBOOKU

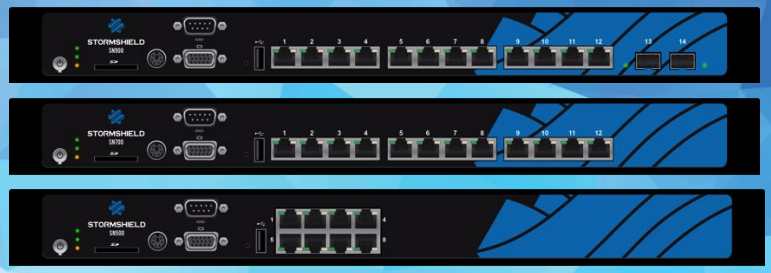
- **Oszustwo** polegające na wzbudzeniu u kogoś zaufania, a następnie wykorzystanie tego zaufania do wyłudzenia pieniędzy
- Jest to plik .svg, który po pobraniu i uruchomieniu w przeglądarce ofiary uruchamia następujący skrypt
- Do zobaczenia filmu potrzebny jest odpowiedni “kodek video”
- Dysk twardy jest szyfrowany

ROZWIĄZANIA OCHRONY DLA KAŻDEJ SIECI

MAŁE ORGANIZACJE, ODDZIAŁY (1-70 UŻYTKOWNIKÓW)

DUŻE SIECI, DATACENTER (700-15 000 UŻYTKOWNIKÓW)

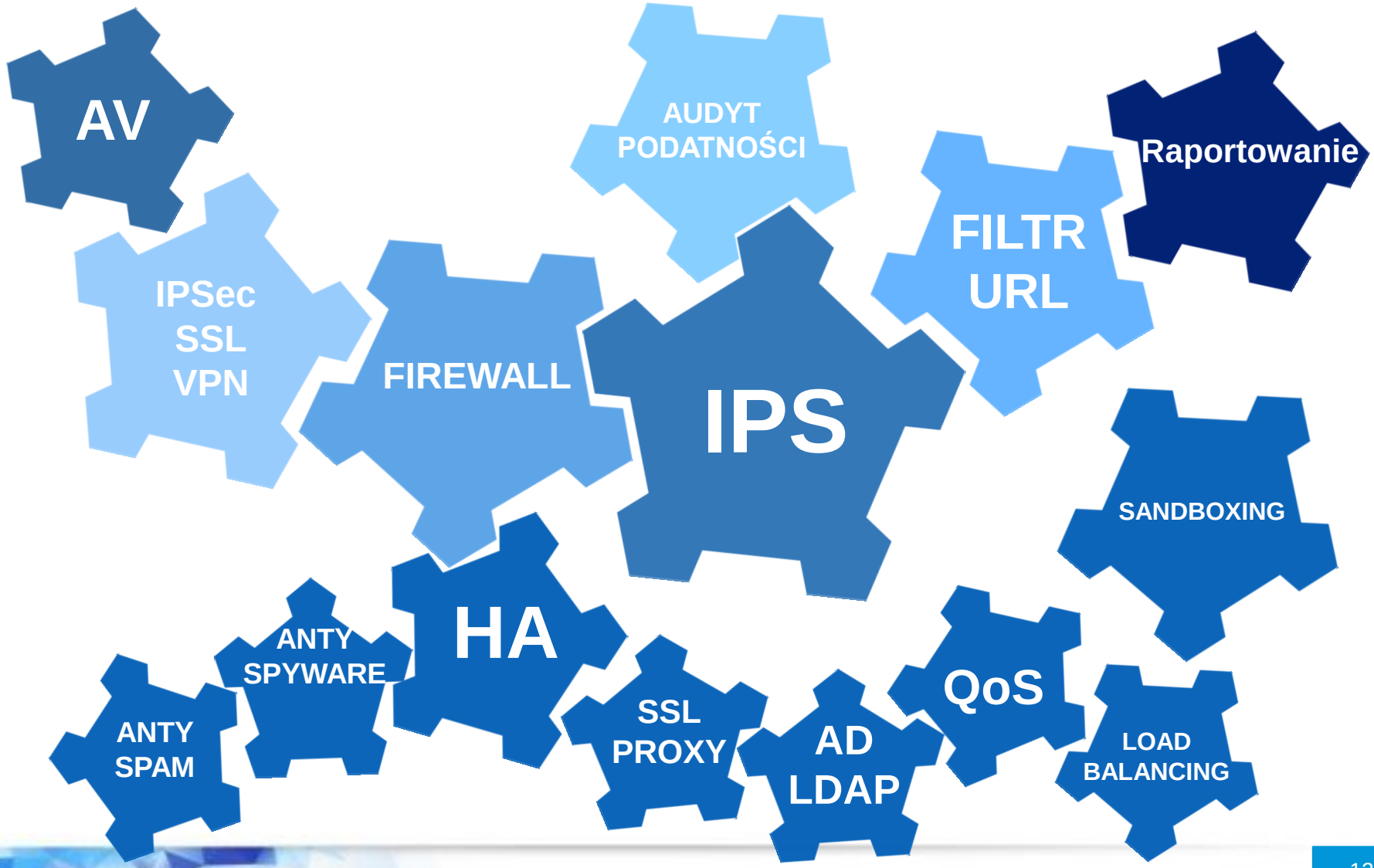
SIECI ŚREDNIEJ WIELKOŚCI (70-700 UŻYTKOWNIKÓW)



WIRTUALNE URZĄDZENIA I UTM W CHMURZE

11

CO OFERUJEMY - ZABEZPIECZENIA



KIM JESTEŚMY

- Firma francuska, powstała w 1998, w Polsce od 2007
- Producent rozwiązań zabezpieczających do sieci
- Europejskie certyfikaty bezpieczeństwa
- Kilka tysięcy urządzeń wdrożonych w Polsce
- Polski interfejs, dokumentacja i wsparcie

Stormshield

W pełni należy do Airbus Defence and Space Cybersecurity

WYBRANE REFERENCJE W POLSCE

Śląskie.
Pozytywna energia

SZPITAL POWIATOWY
w Limanowej
Imienia Miłosierdzia Bożego

URZĄD PATENTOWY
RZECZYPOSPOLITEJ POLSKIEJ

radom
siła w precyzji

WOD KAN
SKIERNIEWICE

POWIAT
ZGORZELECKI
możliwości bez granic

Regionalny Zarząd
Gospodarki Wodnej
we Wrocławiu
Dbamy o przyszłość naszych wód

KARPACZ

POWIATOWY
URZĄD PRACY
DLA POWIATU NOWOSADECKIEGO

Łomża

SĄD OKRĘGOWY w LEGNICY

WYBRANE REFERENCJE W POLSCE

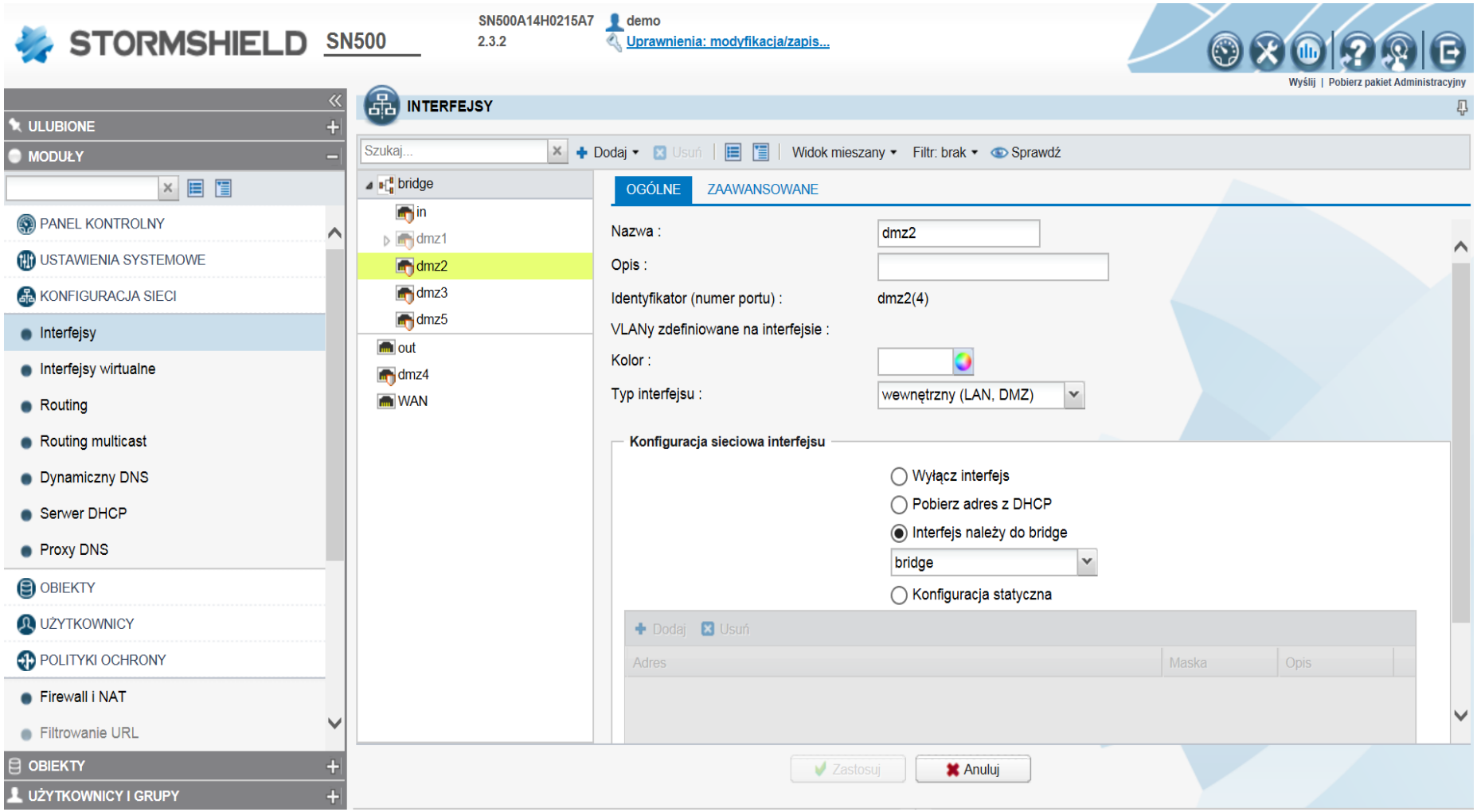
CERTYFIKATY

Vendor	Origin *	CC / cert. country	NATO Restricted	French Qualification	EU Restricted
Astaro/Sophos	UK/US	EAL4+	No	No	No
Check Point	Israel	EAL4+	Yes	No	No
Cisco (ASA)	USA	EAL4+	Yes	No	No
Cyberoam/Sophos	UK/US	EAL4+	No	No	No
Fortinet	USA	EAL4+	No	No	No
Genua	Germany	EAL4+	Only unclassified level	No	No
Juniper	USA	EAL4+	Yes	No	No
Netgear	USA	No	No	No	No
Palo Alto	USA	EAL4+	Yes	No	No
Stonesoft/McAfee	USA	EAL4+	No	Elementary	No
Sonicwall/Dell	USA	EAL4	No	No	No
Watchguard	USA	EAL4+	No (except borderware)	No	No
Stormshield/Airbus DS	FR/GE	EAL4+	Yes	Standard	Yes

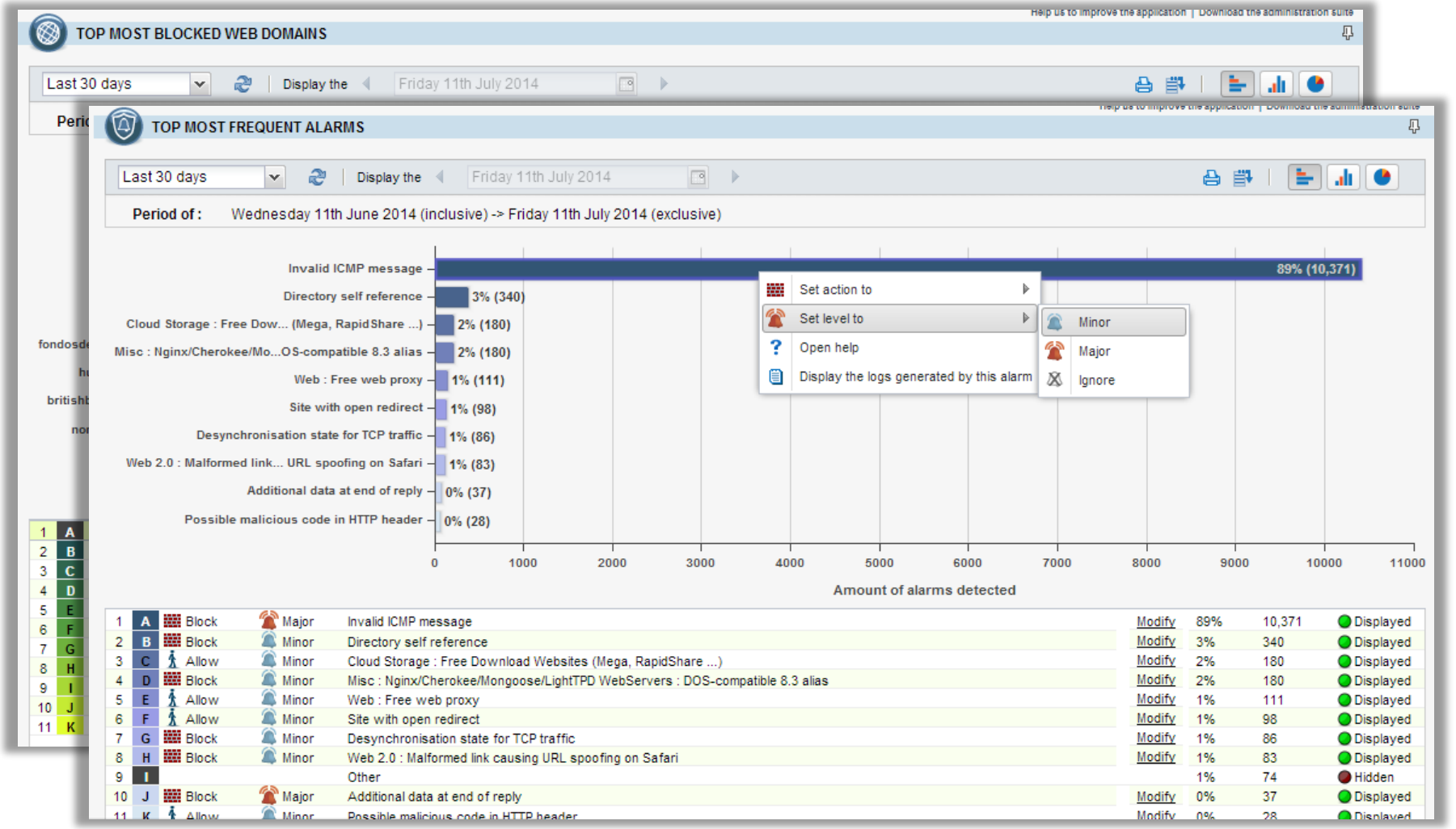
* Origin of the group if the company is a subsidiary.

Strongly dependant on US interests

POLSKI INTERFEJS UŻYTKOWNIKA



BEZPŁATNE RAPORTOWANIE



AUDYT PODATNOŚCI

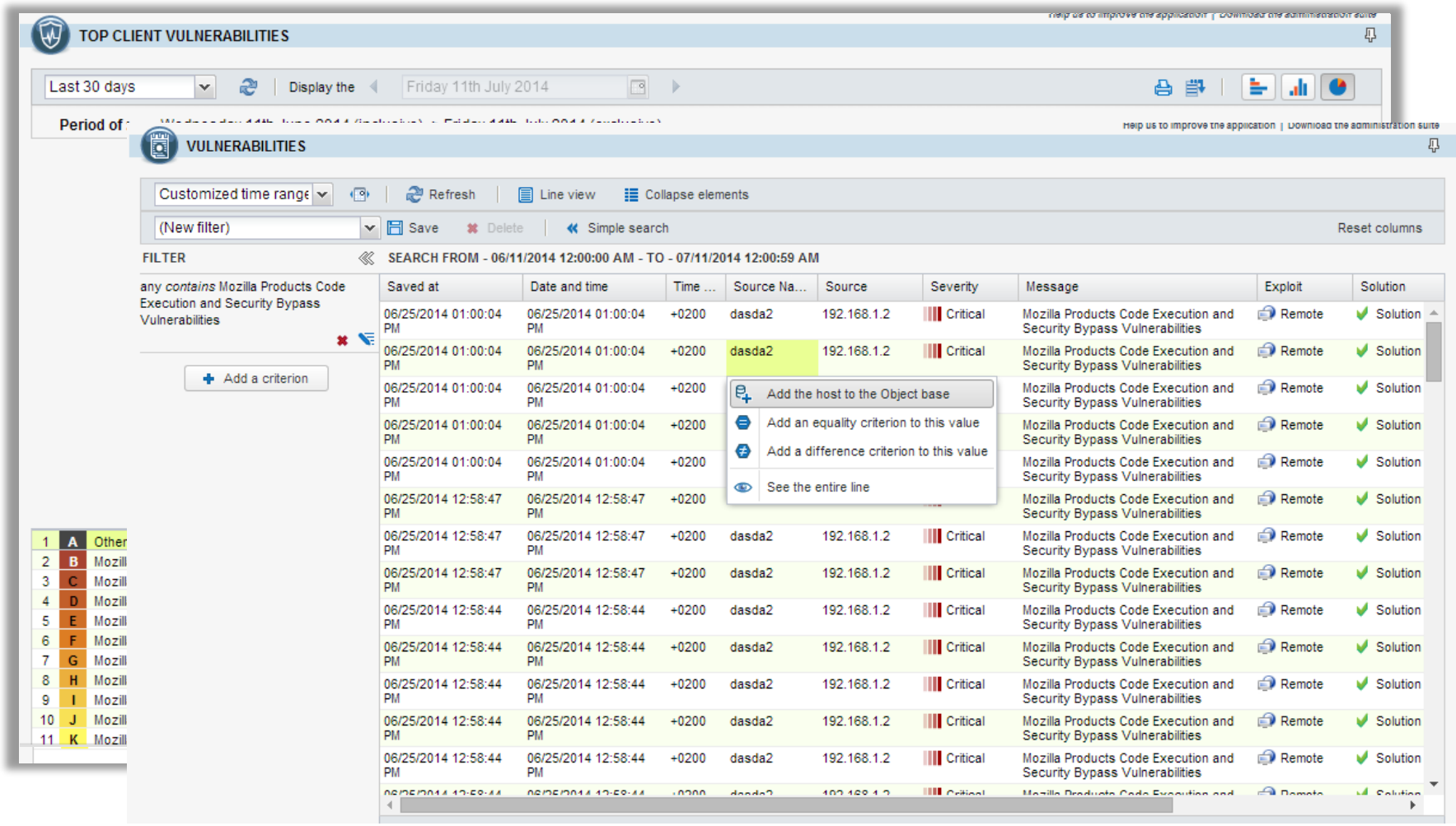
BRAK WPŁYWU NA WYDAJNOŚĆ SIECI

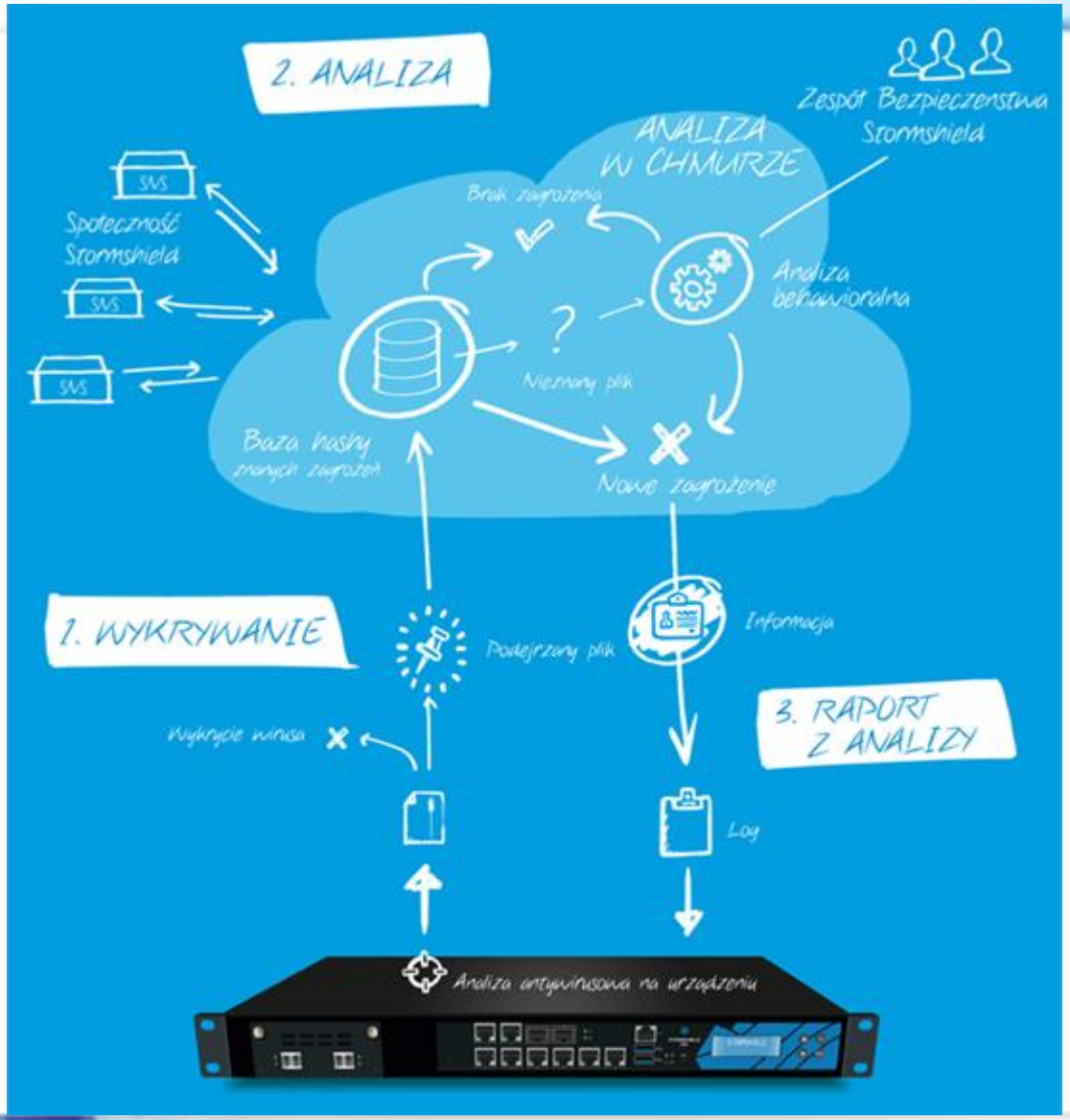
WYSZUKIWANIE SŁABYCH PUNKTÓW
STANOWIĄCYCH ZAGROŻENIA

SUGEROWANIE SPOSOBU ROZWIĄZANIA
WYKRYTYCH PODATNOŚCI

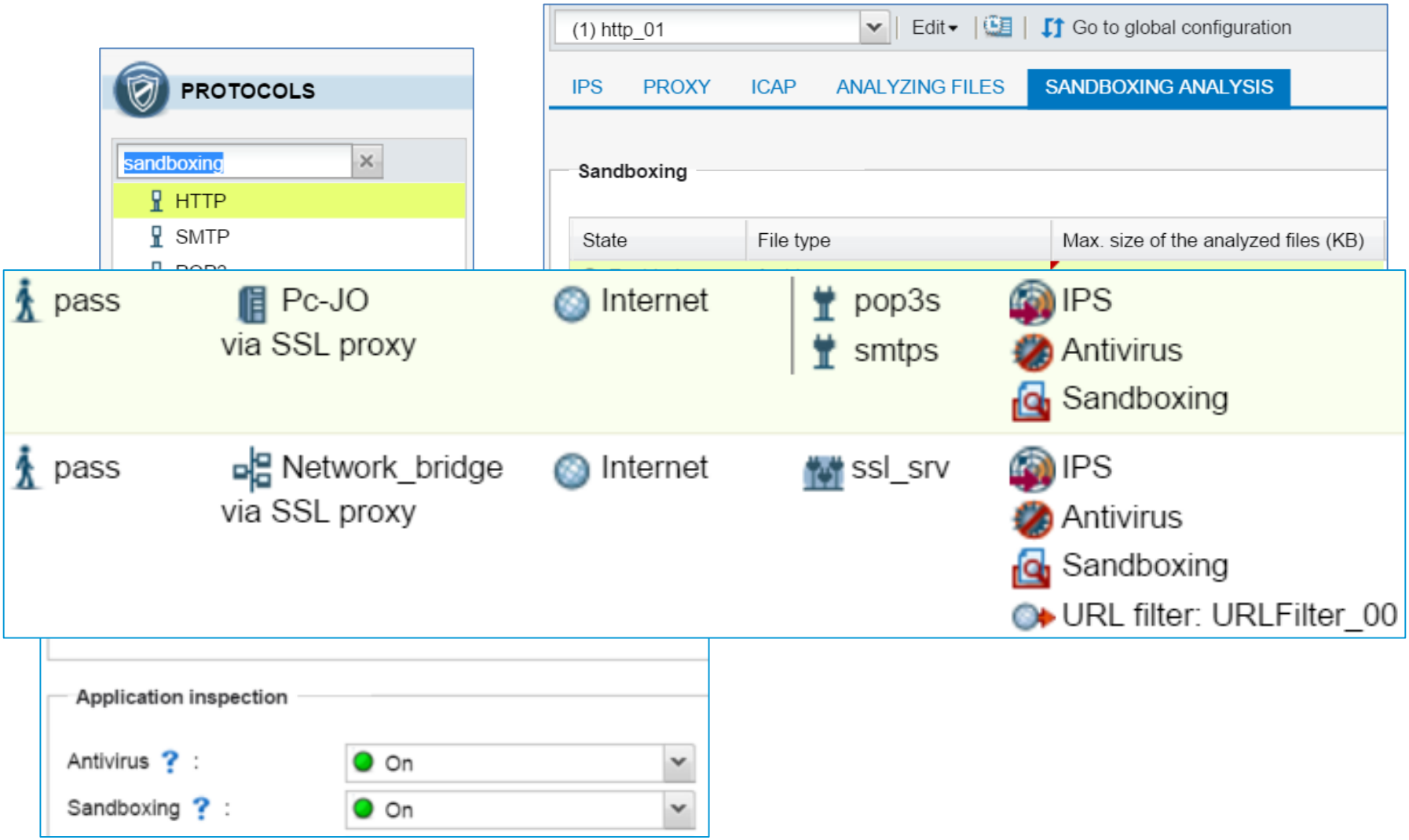
WYKRYWANIE NIEDOZWOLONEGO RUCHU

ANALIZA RYZYKA




2. ANALIZA
Zespół Bezpieczeństwa Stormshield
ANALIZA W CHMURZE
Społeczność Stormshield
SNS
SNS
SNS
Brak zagrożenia
Analiza behawioralna
?
Nieznany plik
Baza hashy znanych zagrożeń
Nowe zagrożenie
1. WYKRYWANIE
Podejrzany plik
Informacja
3. RAPORT Z ANALIZY
Wykrycie wirusa
Log
Analiza antywirusowa na urządzeniu

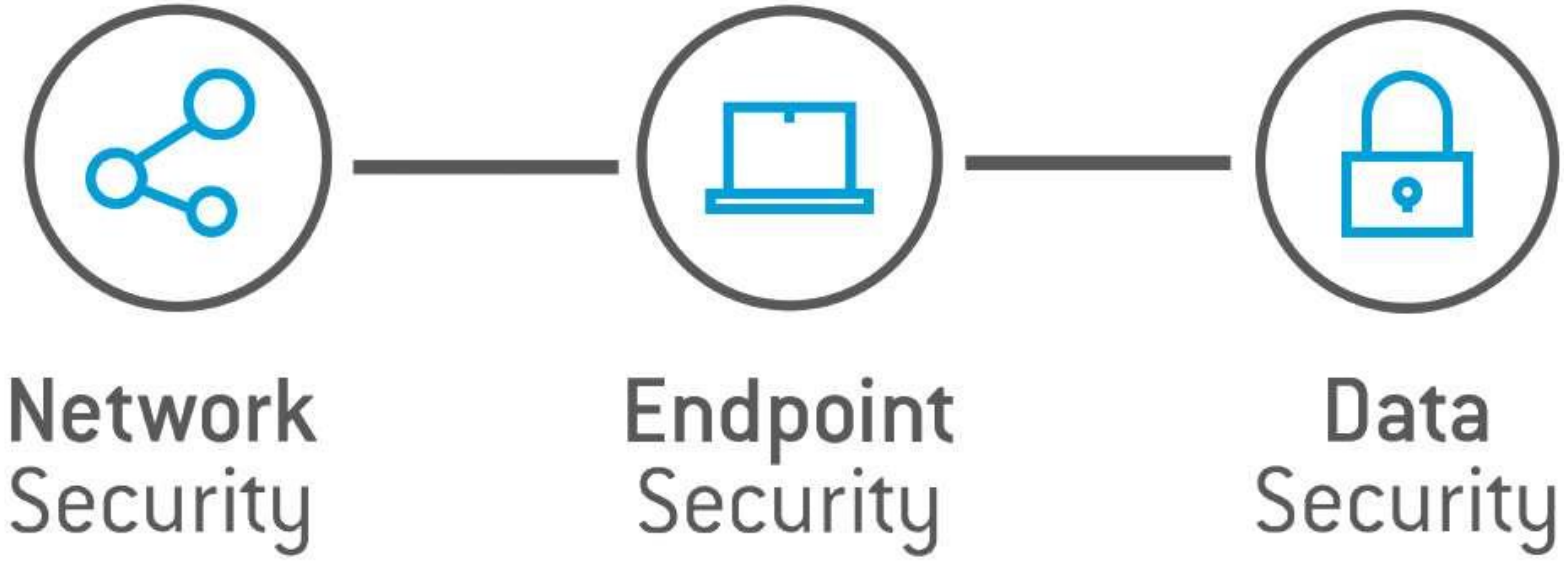
KONFIGURACJA



CO OFERUJEMY:

- Najszybszy IPS z firewall’em na rynku
- Polskie: interfejs użytkownika, wsparcie techniczne i dokumentacja
- 2 moduły raportujące oraz filtr www w cenie serwisu podstawowego
- Po wygaśnięciu licencji moduły nadal działają
- Bezagentowy skaner podatności w sieci

PRODUKTY DO OCHRONY



ZAPRASZAMY DO KONTAKTU

ALEKSANDER.KOSTUCH@STORMSHIELD.EU