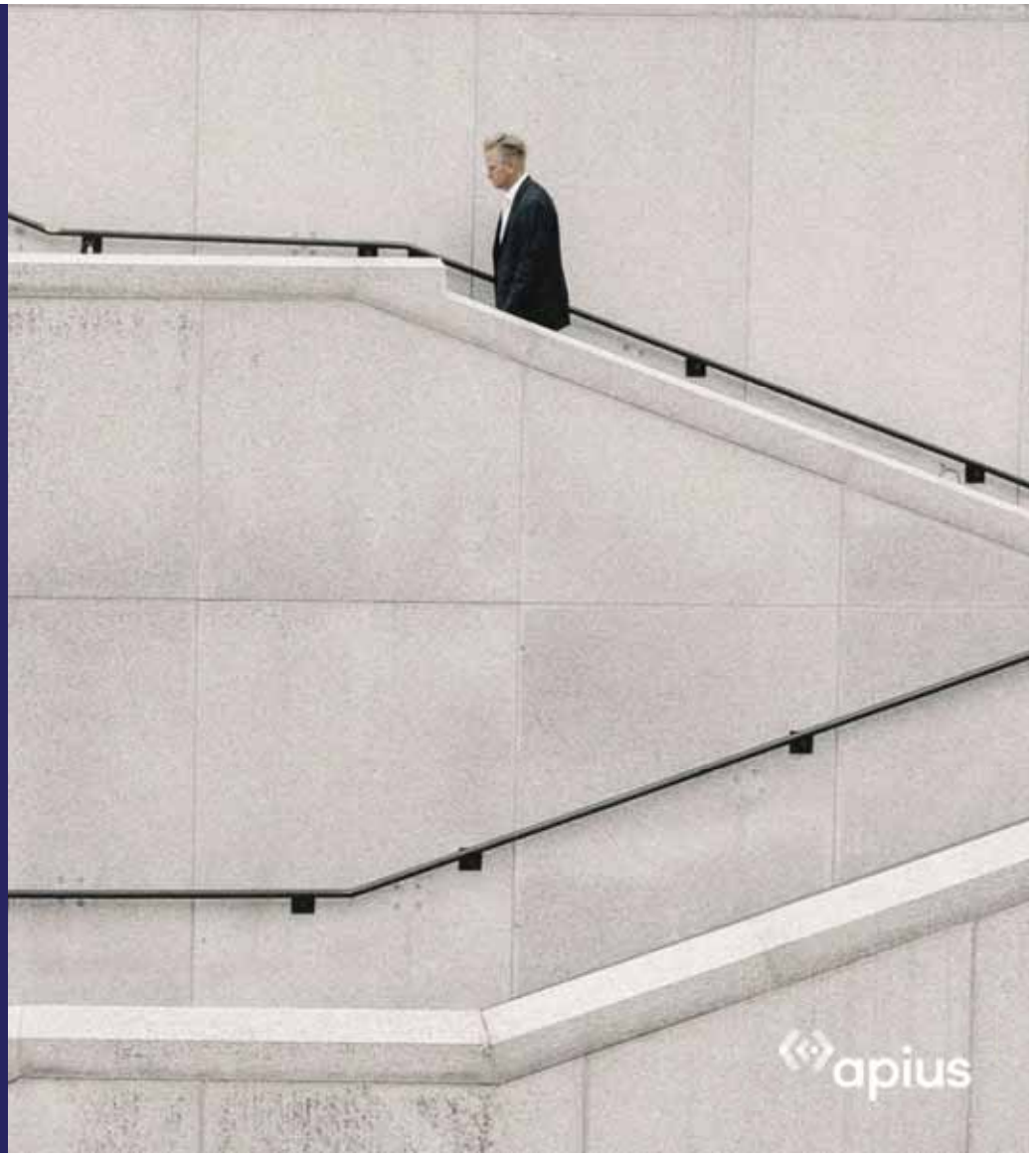
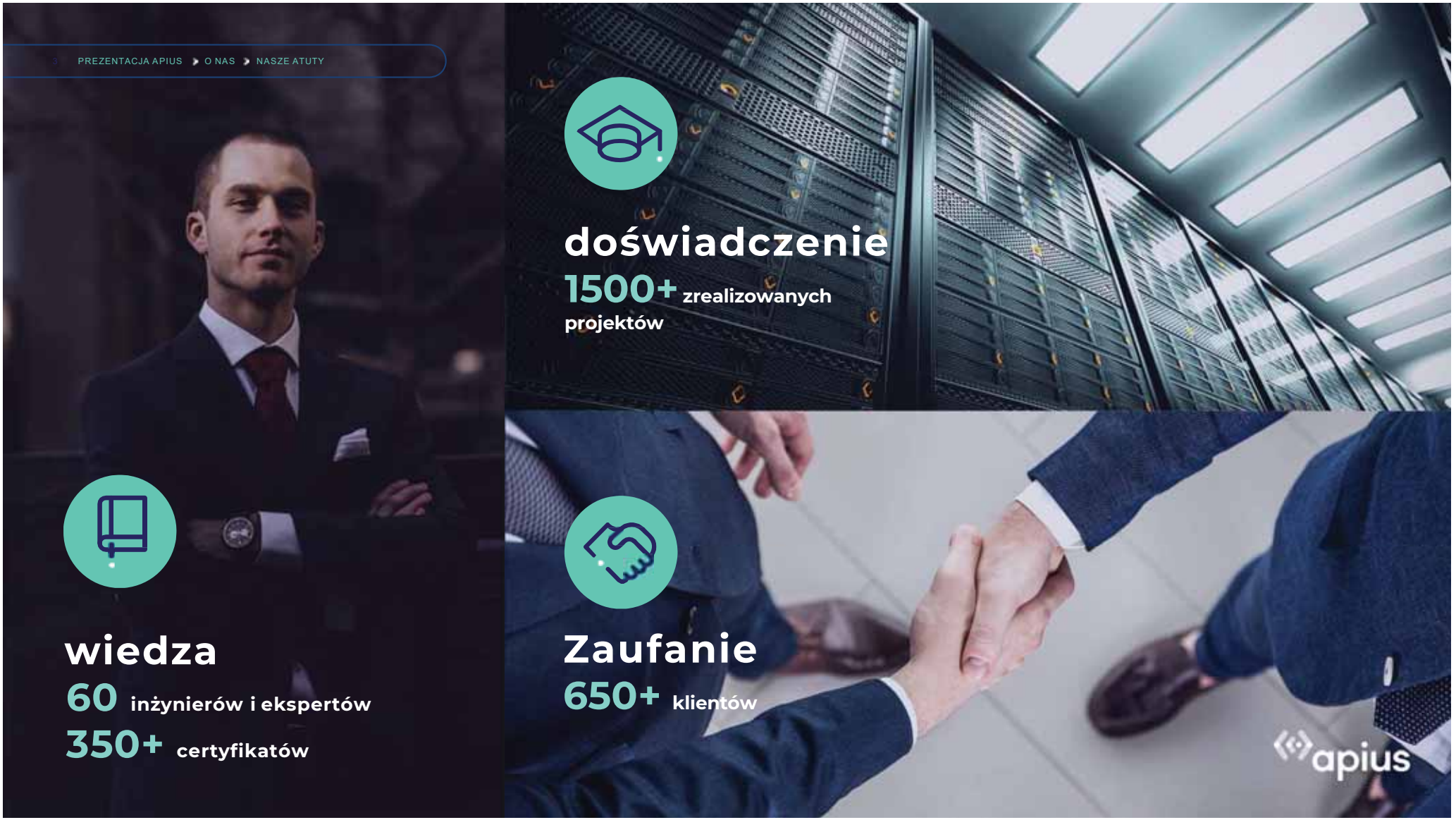

CyberSecurity
is in our DNA .
apius

o nas

Jesteśmy jednym z największych dostawców rozwiązań cyberbezpieczeństwa w Polsce





wiedza

60 inżynierów i ekspertów

350+ certyfikatów

doświadczenie

1500+ zrealizowanych projektów

Zaufanie

650+ klientów

apius

Partnerzy technologiczni **w obszarze bezpieczeństwa**

apius

Partnerzy technologiczni
w obszarze komunikacji IP oraz usług chmurowych

aruba a Hewlett Packard Enterprise company
ARISTA
cisco
f5
Flowmon Networks
JUNIPER NETWORKS
MICROSENS euromicron group
vmware
netskope
PRISMA BY PALO ALTO NETWORKS
illumio

apius

Czy w mojej organizacji zdarzają się cyberataki?

SUBSKRYBUJ DZIENNIK GAZETA PRAWNA

Większość firm w Polsce odnotowało w 2021 r. przynajmniej jeden cyberatak

18 maja 2022, 11:41

Ten tekst przeczytasz w 2 minuty

Udostępnij Udostępnij

Cyberatak / *ShutterStock*

69 proc. firm w Polsce odnotowało w 2021 r. przynajmniej jeden cyberatak - wynika z badania KPMG. Ponad 2/3 firm

TheStreet INVESTING GO

All Companies Have Been Hacked--Even if They Don't Know It

NATALIE WALTERS • DEC 16, 2016 11:00 AM EST

'There are only two types of organizations: those that know that they've been hacked and those that don't yet know,' Crowdstrike's Dmitri Alperovitch says.

thestreet.com

Dynamic Business

HOME READ WRITE ADVERTISE LEARN

How to improve profit margins by reducing costs - Free white paper

locked

Security

There are two types of companies: Those who know they've been hacked & those who don't

source: https://www.gazetaprawna.pl/wiadomosci/kraj/artykuly/8420387,firmy-w-polsce-2021-r-odnotowany-cyberatak-kpmg-cybezbezpieczenstwo.html
source: https://www.thestreet.com/investing/stocks/all-companies-have-been-hacked-even-if-they-don-t-know-it-13927497
source: https://dynamicbusiness.com/locked/there-are-two-types-of-companies-those-who-know-theyve-been-hacked-those-who-dont.html

apius

Sposoby na Goliata - jak z głową podejść do cyberbezpieczeństwa

Przykłady dobrych praktyk z zakresu cyberbezpieczeństwa sektora publicznego

Apius Technologies S.A.

sales@apius.pl
www.apius.pl

apius

Kim jest Goliat?

- **Hacker?**
- Osoba, która obrała sobie naszą organizacje jako cel ataku, dla:
  - zdobycia reputacji lub renomy
  - korzyści finansowych
- Nasz **były pracownik**, który zna nasze środowisko
- **Szpiegostwo korporacyjne** – zatrudnianie wyspecjalizowanych zespołów, które często latami drenują nasze zasoby danych
- Kradzieże gospodarcze, działalność wywiadowcza, destabilizacja infrastruktury, fake news
- **Sztuczna Inteligencja?**

apius

Co może interesować Goliata w naszej organizacji?

Jakie cyberataki są najczęściej wykorzystywane?

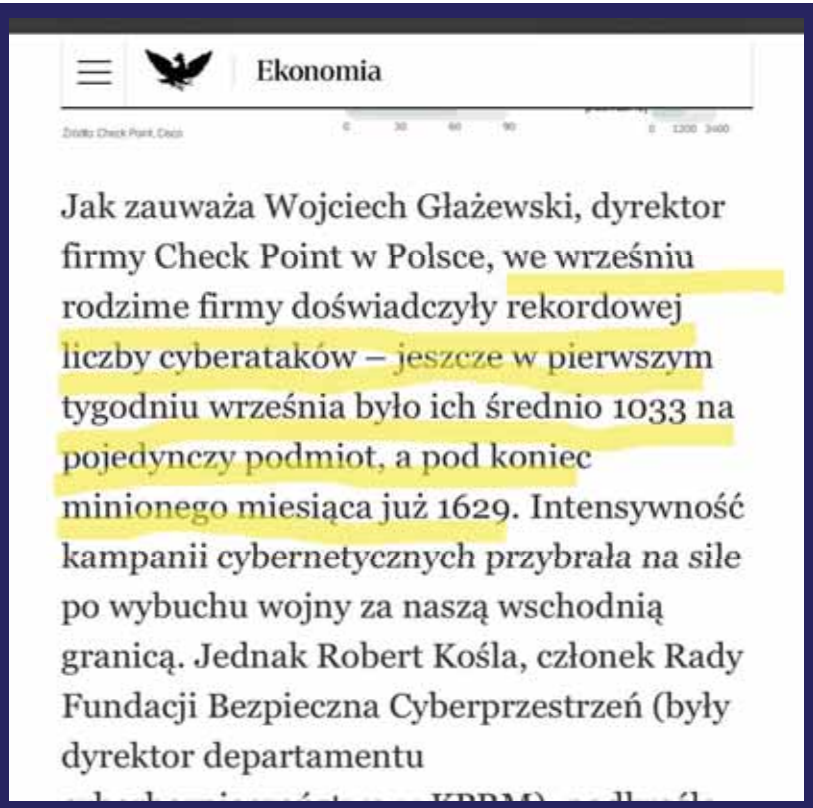
Sukcesywnie każdego roku CERT Polska rejestruje coraz większą liczbę zgłoszeń oraz incydentów cyberbezpieczeństwa. W 2021 r. CERT Polska zarejestrował 116 071 zgłoszeń. Spośród wszystkich zgłoszeń nasi specjaliści wytypowali 65 586, na podstawie których zarejestrowano łącznie **29 483 unikalnych incydentów cyberbezpieczeństwa**.

VIII. Oszustwa komputerowe	**25472**	**86,40%**
Phishing	22575	76,57%
II. Złośliwe oprogramowanie	**2847**	**9,66%**
Niesklasyfikowane	2836	9,62%
V. Włamania	**247**	**0,84%**

https://cert.pl/posts/2022/04/statystyki-obslugi-incydentow-2021/

apius

Tempo wzrostu ilości ataków nie maleje


Ekonomia

Źródło: Check Point, Cisco

Jak zauważa Wojciech Głażewski, dyrektor firmy Check Point w Polsce, we wrześniu rodzime firmy doświadczyły rekordowej liczby cyberataków – jeszcze w pierwszym tygodniu września było ich średnio 1033 na pojedynczy podmiot, a pod koniec minionego miesiąca już 1629. Intensywność kampanii cybernetycznych przybrała na sile po wybuchu wojny za naszą wschodnią granicą. Jednak Robert Kośla, członek Rady Fundacji Bezpieczna Cyberprzestrzeń (były dyrektor departamentu

Check Point podaje, że wykryto próby włamania do 128 organizacji w 42 krajach, również w Polsce. W 29 proc. przypadków były one skuteczne (najczęściej atakowano agencje rządowe, firmy z sektora IT, operatorów krytycznej infrastruktury).

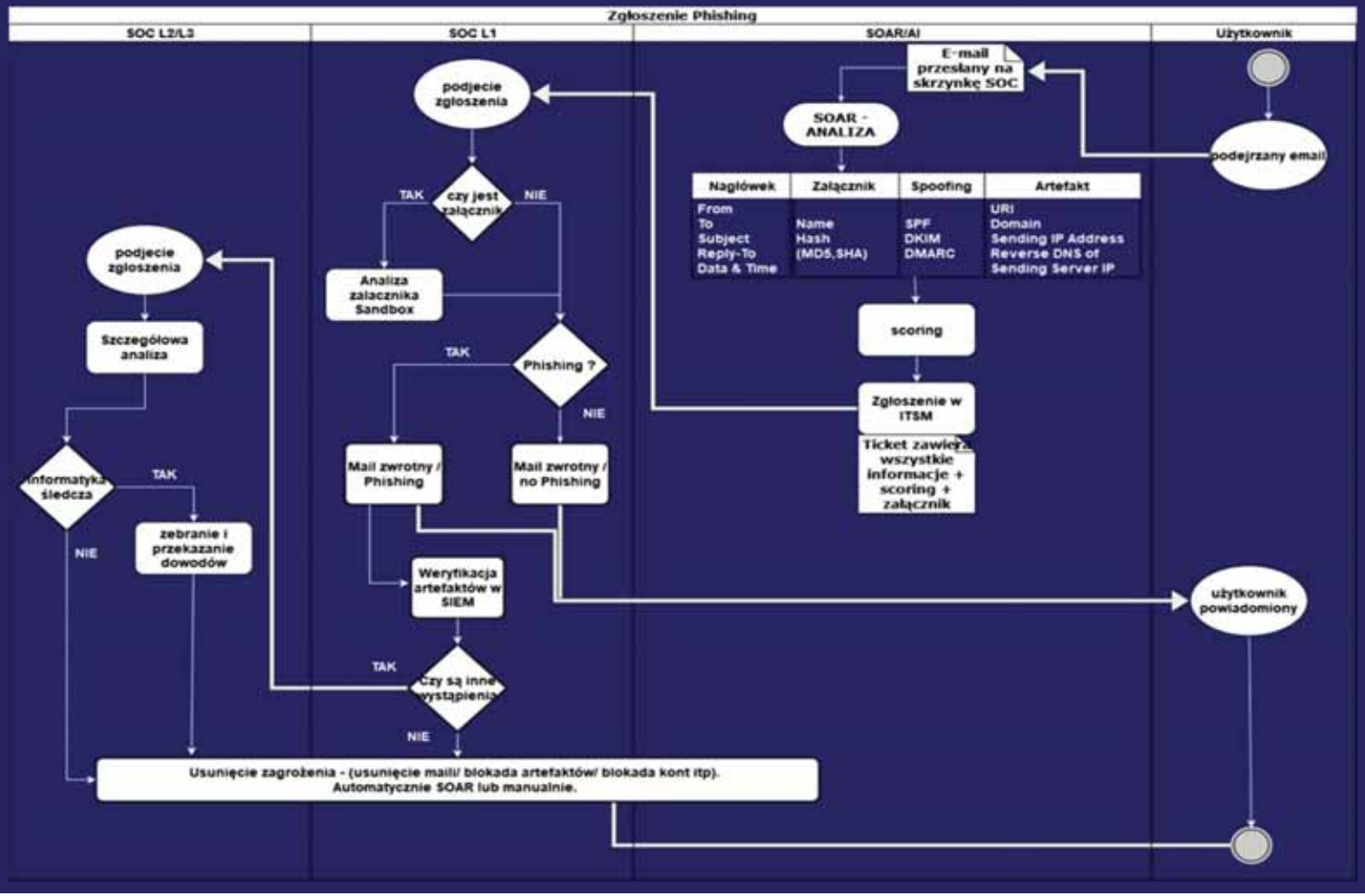
https://www.rp.pl/biznes/art37267811-rekordowa-liczba-hakerskich-uderzen-na-polska-siec

apius

Na dobrze przygotowany phishing można złapać każdego

apius

Jak powinien wyglądać proces zgłoszenia Phishingu do naszego zespołu Cyberbezpieczeństwa



apius

Dobre Praktyki z Cyberbezpieczeństwa

1. Edukacja pracowników

- **regularne szkolenia** w temacie cyberbezpieczeństwa
- budowanie świadomości o **konsekwencjach dla firmy** w przypadku skutecznego cyberataku
- **budowanie i regularne aktualizowanie procedur** reagowania na podejrzane zdarzenia, a następnie szkolenie

pulsHR.pl

Personnel Service

Zarządzanie » Wiadomości

Cyberbezpieczeństwo mocno kuleje. Błędy pracowników mogą być bardzo kosztowne

jk • 25 lis 2021 15:16

Skomentuj

Jeden na trzech pracowników przyznaje, że w domu mniej przestrzega procedur bezpieczeństwa niż w biurze. Tyle samo przyznaje się do popełnienia „krytycznego" błędu w pracy, a 14 proc. podjęło ryzyko, które wiązało się z poniesieniem kosztów przez ich organizację - takie wnioski płyną z raportu przygotowanego na zlecenie Iron Mountain.

Jedna czwarta pracowników (25 proc.) twierdzi, że padła ofiarą oszustwa lub phishingu - wynika z raportu przygotowanego na zlecenie Iron Mountain. Niestety 34 proc. z nich używa tego samego hasła na wielu platformach, 27 proc. nie blokuje swojego laptopa na czas nieobecności przy biurku, a 18 proc. trzyma swoje hasło zapisane na kartce na biurku.

Source:https://www.pulshr.pl/zarzadzanie/cyberbezpieczenstwo-mocno-kuleje-bledy-pracownikow-moga-byc-bardzo-kosztowne,85921.html

apius

2. Jak optymalnie inwestować w cyberbezpieczeństwo

- Ogłaszanie przetargów publicznych na część rozwiązań cyberbezpieczeństwa to proszenie się o kłopoty
- Kupując systemy/usługi kierujmy się **wiarygodnością dostawcy –** czy nie kupimy rozwiązania, które po zakończeniu umowy może stać się bezużyteczne
- Wybierając rozwiązania cyberbezpieczeństwa zweryfikujmy, **czy będziemy w stanie sami utrzymywać, rekonfigurować i rozwijać system.** W przypadku braku pewności powinniśmy zapewnić sobie odpowiednie wsparcie inżynierskie u dostawcy.
- **Outsourcing inżynierów do rozwiązań zaawansowanych staje się standardem,** ponieważ wyzwaniem jest zbudować i utrzymać kompetencje w firmie.

apius

3. Skorzystajmy z wiedzy praktyków, np.

- Architektura referencyjna systemu teleinformatycznego zgodna z zaleceniami CIS Controls™

apius

3

CIS Controls™

CIS Critical Security Controls

Źródło: Center for Internet Security®
https://www.cisecurity.org/controls/cis-controls-list/

CIS Control 1: Inwentaryzacja i kontrola zasobów firmowych (sprzętowych)

CIS Control 2: Inwentaryzacja i kontrola zasobów oprogramowania

CIS Control 3: Zabezpieczenie danych

CIS Control 4: Bezpieczna konfiguracja sprzętu i oprogramowania

CIS Control 5: Zarządzanie kont użytkowników

CIS Control 6: Zarządzanie kontroli dostępu

CIS Control 7: Ciągłe zarządzanie podatnościami

CIS Control 8: Zarządzanie logów audytowych

CIS Control 9: Zabezpieczenie poczty elektronicznej i przeglądarek Web

CIS Control 10: Ochrona przed złośliwym oprogramowaniem

CIS Control 11: Zapewnianie zdolności odzyskiwania danych

CIS Control 12: Zarządzanie infrastrukturą sieci

CIS Control 13: Monitorowanie sieci i zabezpieczeń

CIS Control 14: Wdrożenie programu szkoleń i budowania kultury bezpieczeństwa

CIS Control 15: Zarządzanie dostawcami usług

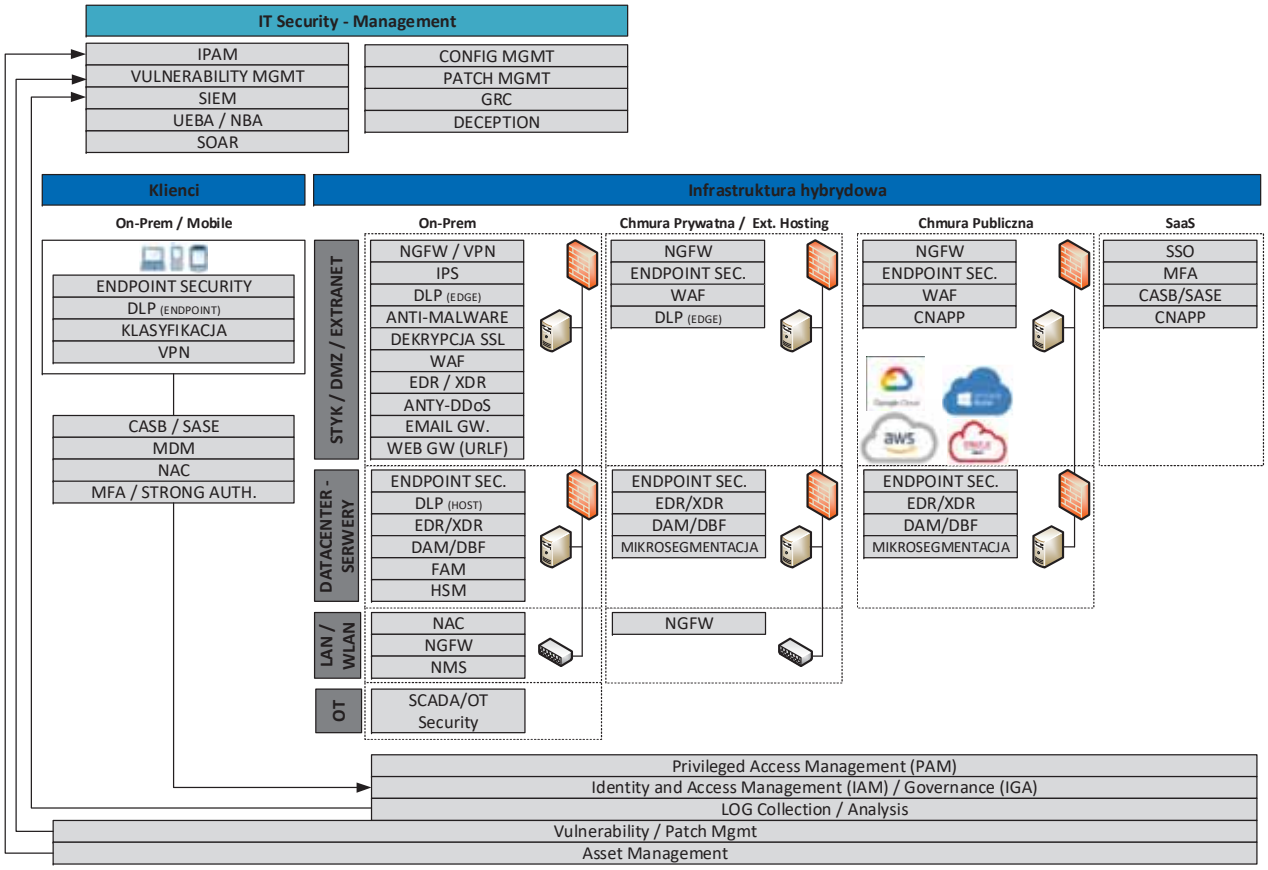
CIS Control 16: Zapewnianie bezpieczeństwa aplikacji

CIS Control 17: Reagowanie i zarządzanie incydentami

CIS Control 18: Testy penetracyjne

apius

ARCHITEKTURA REFERENCYJNA BEZPIECZEŃSTWA



17. REAGOWANIE I ZARZĄDZANIE INCYDENTAMI

ZALECENIA CIS Control 17 TO MUST-HAVE DLA ORGANIZACJI:

- ❑ Posiadających lub budujących SOC
- ❑ Dążących do stworzenia efektywnych procesów zarządzania incydentami lub uporządkowania istniejących
- ❑ Mierzących się z problemem niewystarczającej kadry *Security*, w odniesieniu do liczby incydentów
- ❑ Posiadających dużą ilość rozwiązań / systemów / narzędzi, od których zależy proces obsługi incydentów

REKOMENDACJE CIS W ZAKRESIE ZARZĄDZANIA INCYDENTAMI:

- ❑ STWORZENIE PROCESU OBSŁUGIINCYDENTÓW
- ❑ POWOŁANIE KADRY DO OBSŁUGI
  - ❑ ZBUDOWANIE LITY KONTAKTOWEJ DLA KAŻDEGO Z ETAPÓW PROCESU
  - ❑ PRZYPISANIE RÓL I ODPOWIEDZIALNOŚCI
- ❑ WDROŻENIE RAPORTOWANIA INCYDENTÓW
- ❑ ZAPEWNIENIE MECHANIZMÓW PRACY GRUPOWEJ
- ❑ WDROŻENIE NARZĘDZI DO ANALIZY POST-INCYDENTALNEJ
- ❑ ZDEFINIOWANIE I TUNING WARTOŚCI PROGOWYCH DLA INCYDENTÓW
- ❑ ZAPEWNIENIE NARZĘDZI DO ĆWICZENIA PROCESU ANALIZY INCYDENTÓW

PARTNERZY TECHNOLOGICZNI:

splunk> paloalto NETWORKS smart security apius

CIS Controls™ - 17.

Incident Response Management

SPLUNK ES

SPLUNK PHANTOM

CORTEX XSOAR

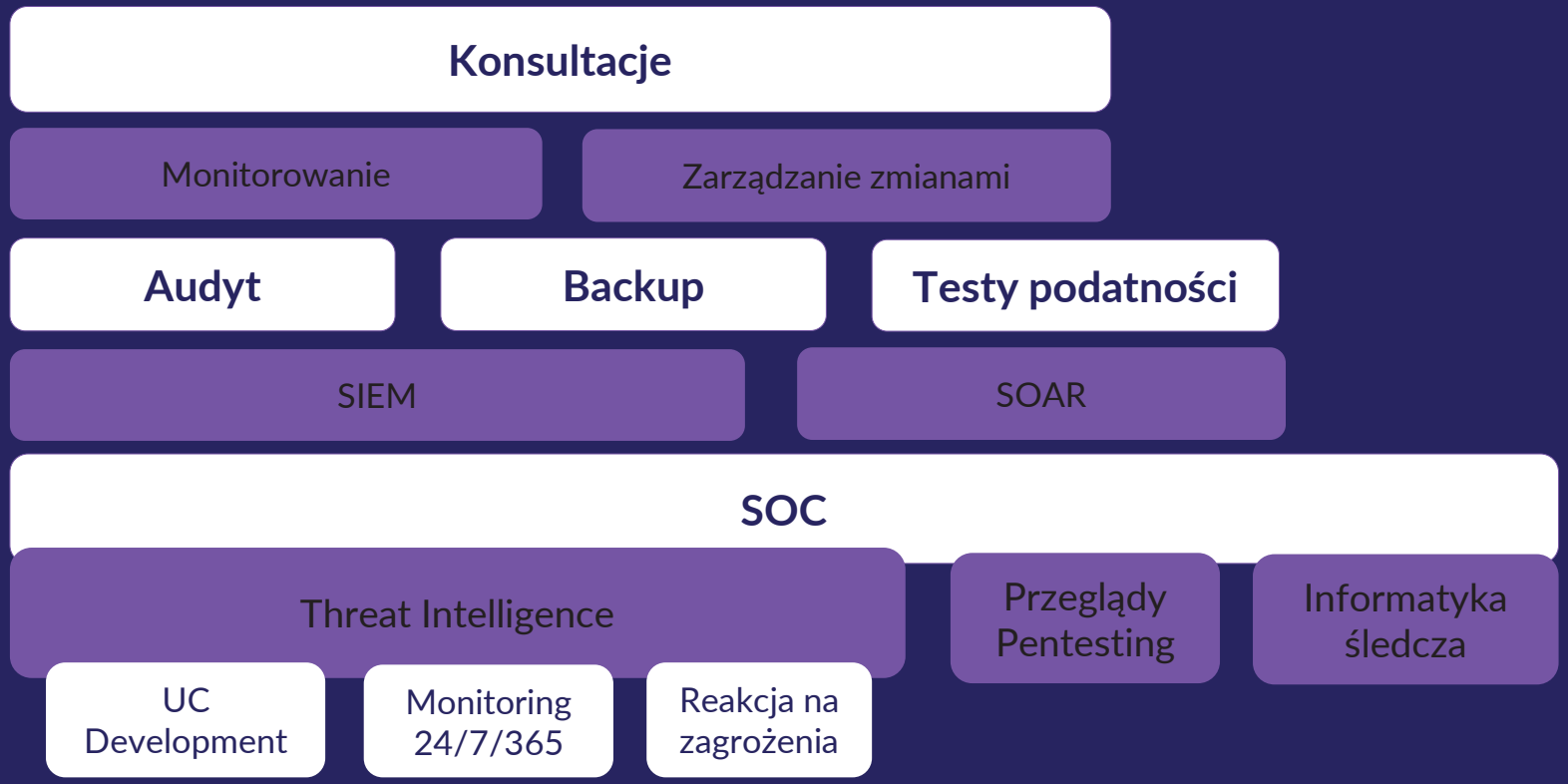
- ❑ Rozwiązanie klasy SIEM, pozycjonowane przez Gartnera wśród Liderów
- ❑ Możliwość analizowania dowolnych danych
- ❑ Nieograniczone możliwości analityczne, dzięki wykorzystaniu jako silnik, platformy Splunk Enterprise (m.in. *Machine-Learning*)
- ❑ Liniowa skalowalność

- ❑ Uporządkowanie procesów monitorowania incydentów
- ❑ Orkiestracja - skrócenie czasu reakcji / czasu obsługi incydentu
- ❑ Automatyzacja akcji w systemach podłączonych
  - ❑ np. Windows / Exchange / Sandboxy / itp.
- ❑ Automatyczna ekstrakcja artefaktów (np. URLe czy załączniki z maili)

apius

Nasz produkt – Smart SOC

Model współpracy



dla kogo pracujemy?

Pracujemy w 17 krajach na świecie

i w kraju dla wielu sektorów, obsługując zarówno klientów korporacyjnych jak i średnie przedsiębiorstwa.

Doradzamy organizacjom z pierwszej setki największych firm w Polsce.

finanse

apius

nowe technologie

allegro
CANAL+
emitel
EXATEL
FOTOJOKER.pl
grape up
{inittec;}
interia
morele
NOVOMATIC Technologies Poland
orange
PayU
PLAY
plus
SCHIBSTED MEDIA GROUP
TECHLAND
T-Mobile

apius

sektor publiczny

AGH
Główny Urząd Miar
GUS
Kancelaria Prezesa Rady Ministrów
KNF Komisja Nadzoru Finansowego
Kraków
Lubelskie
Lublin
Miasto Stołeczne Warszawa
Ministerstwo Cyfryzacji
Ministerstwo Infrastruktury
Ministerstwo Inwestycji i Rozwoju
Ministerstwo Przedsiębiorczości i Technologii
NFZ
Olsztyn
Policja
Sąd Rejonowy w Ostrołęce
Uniwersytet Ekonomiczny we Wrocławiu
Uniwersytet Jagielloński w Krakowie
UMCS
Uniwersytet Rolniczy
Zamość
ZUS

apius

energetyka i przemysł

AmRest
CANPACK
EDF
Enea
Energa
FARMACOL
GAZ system
innogy
Lufthansa Systems
MASPEX
polpharma
PGE
POLSKA SPÓŁKA GAZOWNICTWA
Selvita
SKANSKA
stokrotka
TAURON POLSKA ENERGIA
TF Kable
VOLKSWAGEN

apius

medycyna

CENTRUM MEDYCZNE
IM. BITWY WARSZAWSKIEJ 1920 ROKU

Krakowski Szpital Specjalistyczny im. Jana Pawła II

Narodowy Instytut Onkologii
im. Marii Skłodowskiej-Curie
Państwowy Instytut Badawczy

NFZ
Narodowy Fundusz Zdrowia

polpharma

Regionalny Szpital Specjalistyczny

SPECJALISTYCZNY SZPITAL

Szpital Specjalistyczny im. dr Józefa Babińskiego SPZOZ Kraków

RYDYGIER

Szpital Specjalistyczny

Szpital Uniwersytecki w Krakowie

Świętokrzyskie Centrum Onkologii

Uniwersytecki Dziecięcy Szpital Kliniczny im. L. Zamenhofa w Białymstoku

UNIWERSYTET MEDYCZNY W LUBLINIE

apius

Dziękuję za uwagę!

Skontaktuj się z nami

sales@apius.pl
www.apius.pl