

CrowdStrike Falcon

– dlaczego potrzebujesz nowoczesnej
ochrony przed cyberzagrożeniami

Grzegorz Kozak

Senior Key Account Manager
Greeneris

Marcin Czaban

Inżynier Systemowy
Greeneris



Polskie firmy i instytucje na celowniku



07 LIPCA 2022

Coraz częstsze ataki na infrastrukturę krytyczną. Szczególnie wrażliwa jest na nie energetyka

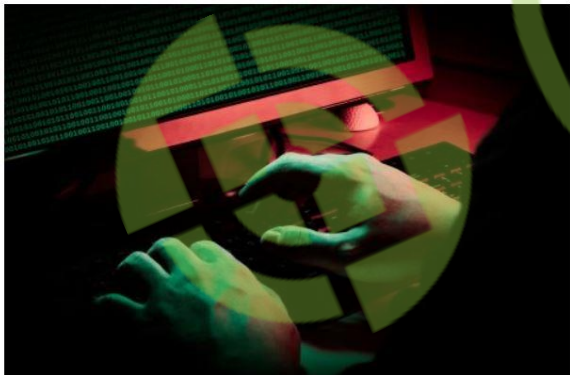
Kategoria: Aktualności

Wojna w Ukrainie zwiększyła skalę cyberzagrożeń, jednak od wielu miesięcy systematycznie podejmowane są ataki na polską sieć. Wiele z nich jest kierowanych z Rosji, a szczególnie narażona jest na nie infrastruktura krytyczna, w tym m.in. energetyka. Ekspert Fundacji Bezpieczna Cyberprzestrzeń

CRN AKTUALNOŚCI WYWIADY I FELIETONY ARTYKUŁY MAGAZYN CRN FORUM KONTAKT

Rekordowa liczba cyberataków na Polskę

Liczba ataków na polskie firmy wzrosła od wakacji o 100 proc



Głównym wektorem ataków są wiadomości e-mail i zaszyfrowane załączniki pdf.

Hakerzy nigdy nie byli tak aktywni jak teraz. Średnio atakowali polskie firmy 2 tys. razy tygodniowo. To wzrost o blisko 100 proc w porównaniu do wakacji br. – ustalił Check Point Research.

Wśród najbardziej zagrożonych branż są sektory użyteczności publicznej, wojskowy, rządowy i finansowy. Hakerzy atakują, by uzyskać dostęp do poufnych danych. Najczęściej dostają się do sieci firmowych za pomocą zdalnego wykonania kodu (w 64 proc. organizacji) oraz ujawnień danych (62 proc.).

EPEC – Elbląskie Przedsiębiorstwo Energetyki Ciepłej – uderzone przez ransomware

28 CZERWCA 2022, 22:06 | W BIEGU | 0 KOMENTARZY

O ataku ransomware raczej nikt nie chce się chwalić – poza zaszyfrowaniem infrastruktury IT często bowiem dochodzi również do wycieku danych.

Tymczasem dość enigmatyczny komunikat można [przeczytać na stronie EPEC](#):

Służby informatyczne EPEC przywracają pracę systemu informatycznego, który w sobotę uległ awarii. Kluczowe systemy w firmie – obsługujące system ciepłowniczy oraz przyjmowanie zgłoszeń do Pogotowia Ciepłowniczego pracują bez zakłóceń.

Klienci mogą mieć jednak kłopot z uzyskaniem od EPEC informacji o kosztach i sposobie rozliczenia.

W przyłączeniu. Informacje te zostały przesłane drogą korespondencji emailowej oraz

z tego, że chodzi po prostu o ransomware.

Elbląskie Przedsiębiorstwo Energetyki Ciepłej oficjalnie stwierdziło, że zostały zaszyfrowane, co uniemożliwiło

pracy. W sieci pojawiły się przypuszczenia, które mają doprowadzić do

Rosyjscy hackerzy wypowiedzieli cyberwojnę Polsce i innym krajom. Bredzą o atakach "rusofobów"

Opracował Bartłomiej Pawlak
17.05.2022 19:14

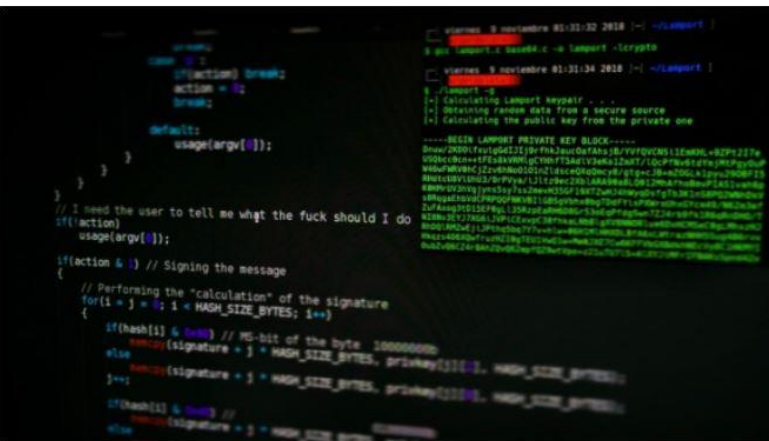
Posłuchaj artykułu

Rosyjska grupa hackerów znana pod nazwą "Killnet" wypowiedziała cyberwojnę Ukrainie i kilku krajom ją wspierającym, w tym Polsce. Hakerzy twierdzą, że muszą "znosić ataki nazistów i rusofobów". Tymczasem sami zaatakowali m.in. włoskie strony internetowe.



Atak DDoS na rządowy serwis – czas na kolejny stopień alarmowy?

2022-11-09



Do pobrania
Czas na kolejny stopień alarmowy (0.02 MB)

- W poniedziałek atak DDoS sparaliżował eZamówienia.
- Niespełna tydzień wcześniej hackerzy zaatakowali Centrum Zdrowia Matki Polki w Łodzi, a 27 października przeprowadzono atak DDoS na serwery Senatu RP.
- Instytucje publiczne były już atakowane przez hackerów od początku roku. W Polsce nadal obowiązuje trzeci stopień alarmowy CHARLIE-CRP. Czy powód do zmartwień mają także firmy?

KLUCZOWE WYZWANIA CYBERBEZPIECZEŃSTWA



**WYRAFINOWANIE
ATAKÓW**



**ZŁOŻONOŚĆ
ROZWIĄZAŃ**



**BRAK
SPECJALISTÓW**



MALWARE
38%

ZATRZYMANIE MALWARE
NIE
WYSTARCZY

MALWARE
THREAT
SOPHISTICATION



HIGH
—
LOW
—
LOW
—
HIGH

HARDER TO PREVENT
& DETECT



PRZESTARZAŁA OCHRONA



CZY WIEDZIAŁEŚ?

80%

WSZYSTKICH NARUSZEŃ
WYKORZYSTUJE
SKOMPROMITOWANE TOŻSAMOŚCI,
A ICH ZIDENTYFIKOWANIE MOŻE
ZAJĄĆ DO 250 DNI¹

1. [2022 CROWDSTRIKE GLOBAL THREAT REPORT](#)

50%

ORGANIZACJI
DOŚWIADCZYŁO ATAKU NA
ACTIVE DIRECTORY W CIĄGU
OSTATNICH DWÓCH LAT²

2. [EMA Research Report - The Rise of Active Directory Exploits](#)

40%

TYCH ATAKÓW ZAKOŃCZYŁO
SIĘ SUKCESEM, PONIEWAŻ
PRZECIWNICY WYKORZYSTALI
BRAK HIGIENY W AD³

3. [EMA Research Report - The Rise of Active Directory Exploits](#)



FAZY ATAKU - PRZETRWAJĄ NAJSZYBSI

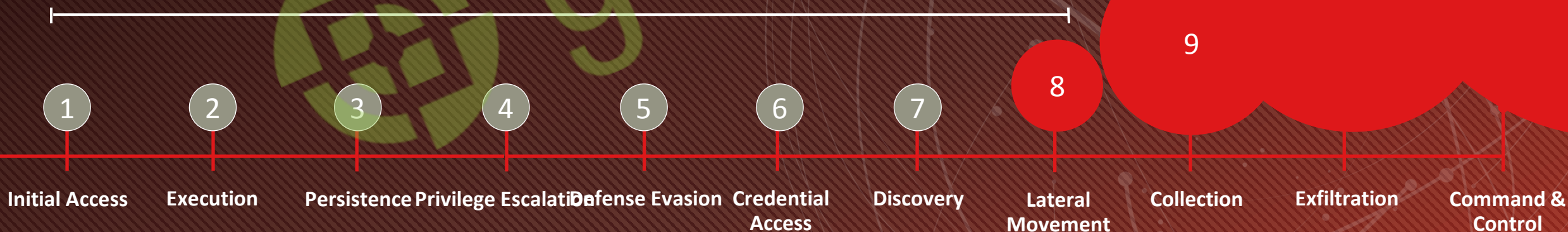
OBROŃCY
MUSZĄ:

WYKRYĆ W
1min

ZBADAĆ W
10min

ODPOWIEDZIEĆ W
60min

CZAS PRZERWANIA



MITRE ATT&CK PHASE





CROWDSTRIKE POWSTRZYMUJE NARUSZENIA CYBERBEZPIECZEŃSTWA



NOWY STANDARD W OCHRONIE URZĄDZEŃ KOŃCOWYCH

INDUSTRY ANALYSTS

Gartner

"CROWDSTRIKE NAMED A LEADER IN THE 2019 GARTNER MAGIC QUADRANT FOR ENDPOINT PROTECTION AND POSITIONED FURTHEST FOR COMPLETENESS OF VISION"

FORRESTER®

"CROWDSTRIKE IS THE ONLY VENDOR TO BE NAMED A LEADER IN BOTH ENDPOINT SECURITY SUITE AND EDR WAVES"

IDC

"LEADER IN IDC MARKETScape FOR US INCIDENT READINESS, RESPONSE AND RESILIENCY SERVICES"

PRODUCT REVIEWS AND TESTS

AV comparatives

"FALCON CERTIFIED TO REPLACE LEGACY ANTIVIRUS"



SE Labs

"FALCON ACHIEVES AAA RATING IN SE LABS TEST"

MITRE

"MITRE VALIDATES FALCON AGAINST ATT&CK™ FRAMEWORK"



"FIVE STAR RATING AND BEST BUY AWARD"



CUSTOMER INSIGHTS

HIGHEST SCORE OF 4.9/5 IN BOTH EDR AND ENDPOINT PROTECTION PLATFORMS

AWARDS AND RECOGNITION

Winner

NAMED BEST SECURITY COMPANY FOR TWO CONSECUTIVE YEARS



CROWDSTRIKE NAMED CNBC DISRUPTOR FOR TWO CONSECUTIVE YEARS

Forbes

FORBES CLOUD 100 LIST FOR TWO CONSECUTIVE YEARS

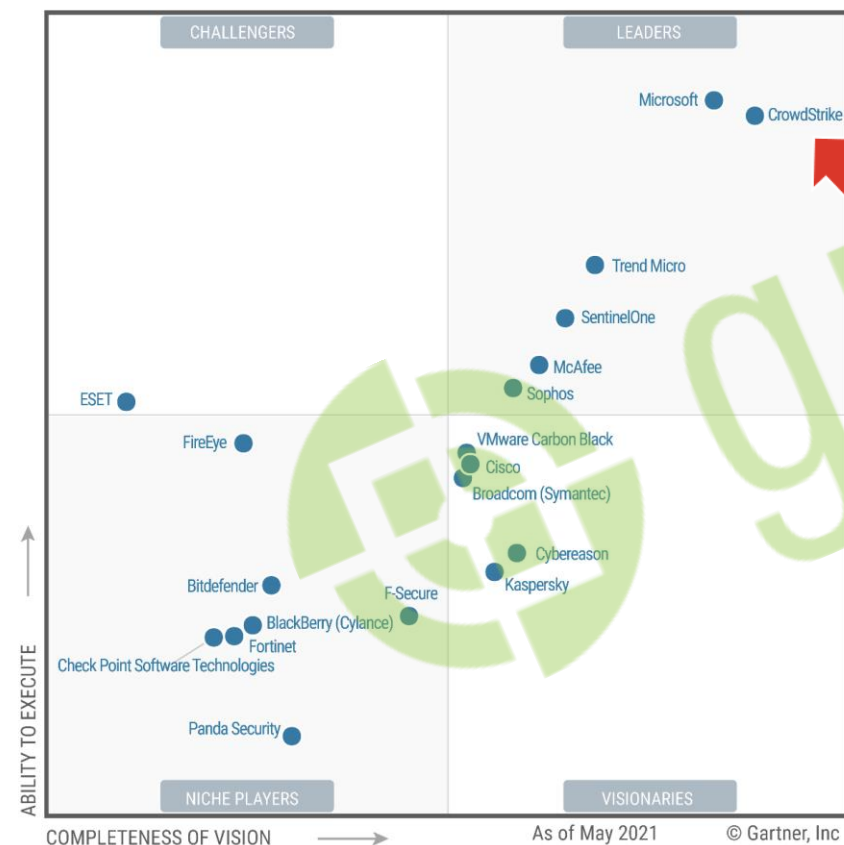
Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose. GARTNER is a registered trademark and the GARTNER PEER INSIGHTS CUSTOMERS' CHOICE badge is a trademark and service mark of Gartner, Inc., and/or its affiliates, and is used herein with permission. All rights reserved. Gartner Peer Insights Customers' Choice constitute the subjective opinions of individual end-user reviews, ratings, and data applied against a documented methodology; they neither represent the views of, nor constitute an endorsement by, Gartner or its affiliates. Gartner Peer Insights 'Voice of the Customer', Endpoint Detection and Response Solutions, 28 February 2019 and Gartner Peer Insights 'Voice of the Customer', Endpoint Protection Platforms, 10 December 2019. <https://www.gartner.com/reviews/customers-choice/endpoint-protection-platforms> and <https://www.gartner.com/reviews/customers-choice/endpoint-detection-and-response-solutions>



Wyróżnienia GARTNER

UZNANIE EKSPERTÓW

Figure 1: Magic Quadrant for Endpoint Protection Platforms



Source: Gartner (May 2021)

UZNANIE KLIENTÓW



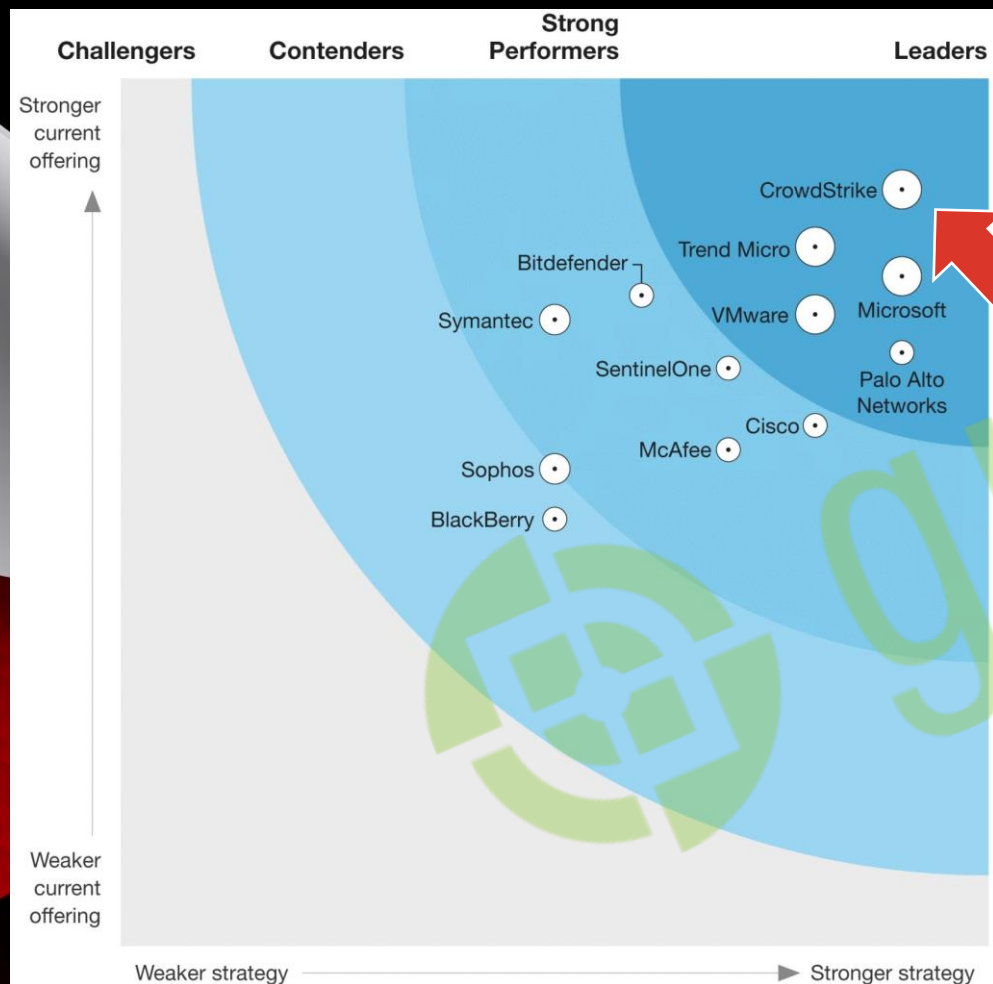
Endpoint Protection Platforms



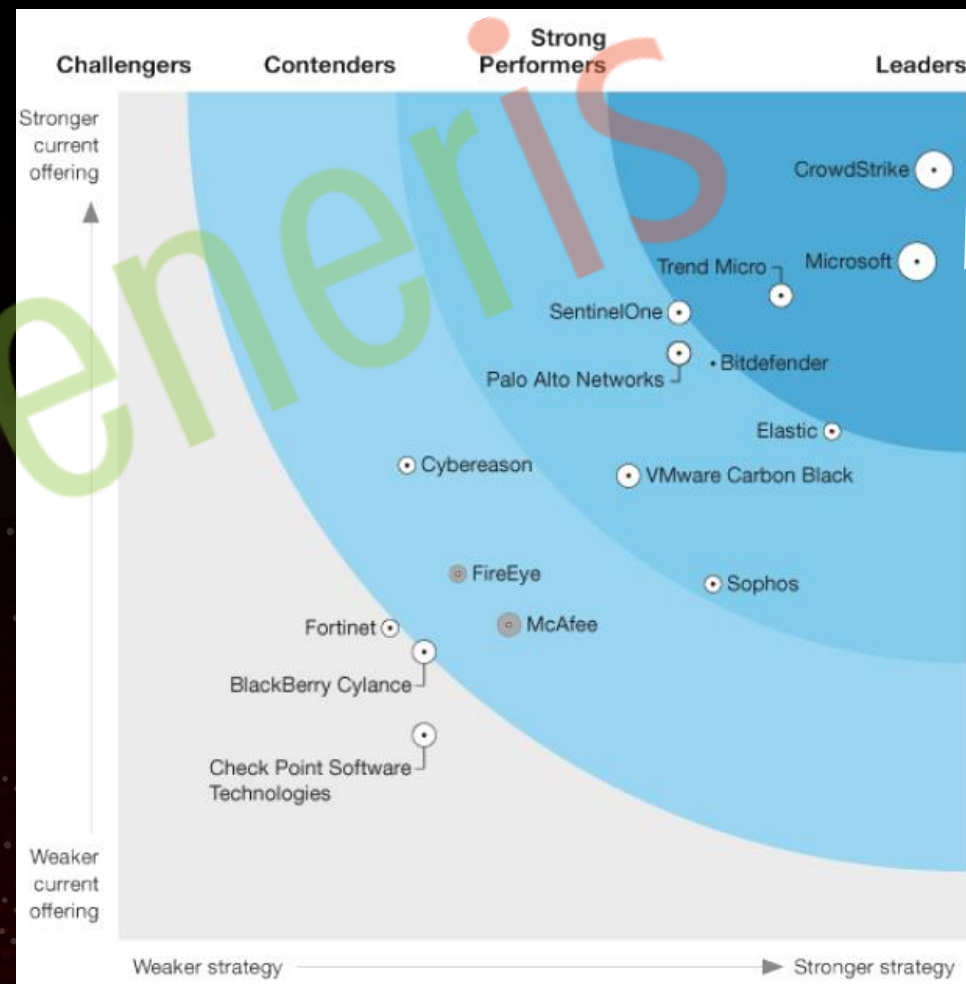
Endpoint Detection and Response Solutions

This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from CrowdStrike. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose. The GARTNER PEER INSIGHTS CUSTOMERS' CHOICE badge is a trademark and service mark of Gartner, Inc., and/or its affiliates, and is used herein with permission. All rights reserved. Gartner Peer Insights Customers' Choice constitute the subjective opinions of individual end-user reviews, ratings, and data applied against a documented methodology; they neither represent the views of, nor constitute an endorsement by, Gartner or its affiliates. <https://www.gartner.com/reviews/customers-choice/endpoint-protection-platforms> and <https://www.gartner.com/reviews/customers-choice/endpoint-detection-and-response-solutions>

FORRESTER WAVES



Forrester Wave for Endpoint Detection and Response, Q1 2020



Forrester Endpoint Detection And Response Providers, Q2 2022

CORAZ WIĘCEJ ORGANIZACJI WYBIERA CROWDSTRIKE



12 of 20

FORTUNE LARGEST GLOBAL
COMPANIES



10 of 20

LARGEST FINANCIAL
INSTITUTIONS



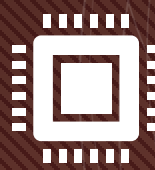
9 of 20

LARGEST HEALTHCARE
PROVIDERS



7 of 10

LARGEST ENERGY
COMPANIES



6 of 10

LARGEST TECHNOLOGY
COMPANIES



5 of 10

LARGEST MEDIA
COMPANIES





CROWDSTRIKE

PIERWSZA NA RYNKU
NATYWNA PLATFORMA
OCHRONY PUNKTÓW
KOŃCOWYCH W CHMURZE

SZTUCZNA INTELIGENCJA ZASILANA PRZEZ THREAT GRAPH

Blokuje znane i nieznane
malware

.....

Działa w sieci i poza
siecią

.....

Nie wymaga
aktualizacji sygnatur

.....

Nieustanne uczenie
dzięki Threat Graph



AV NOWEJ GENERACJI - FALCON PREVENT



CROWDSTRIKE FALCON
CERTIFIED AS LEGACY
AV REPLACEMENT



WARTOŚĆ BIZNESOWA

Wzmacnia ochronę

Redukuje liczbę incydentów

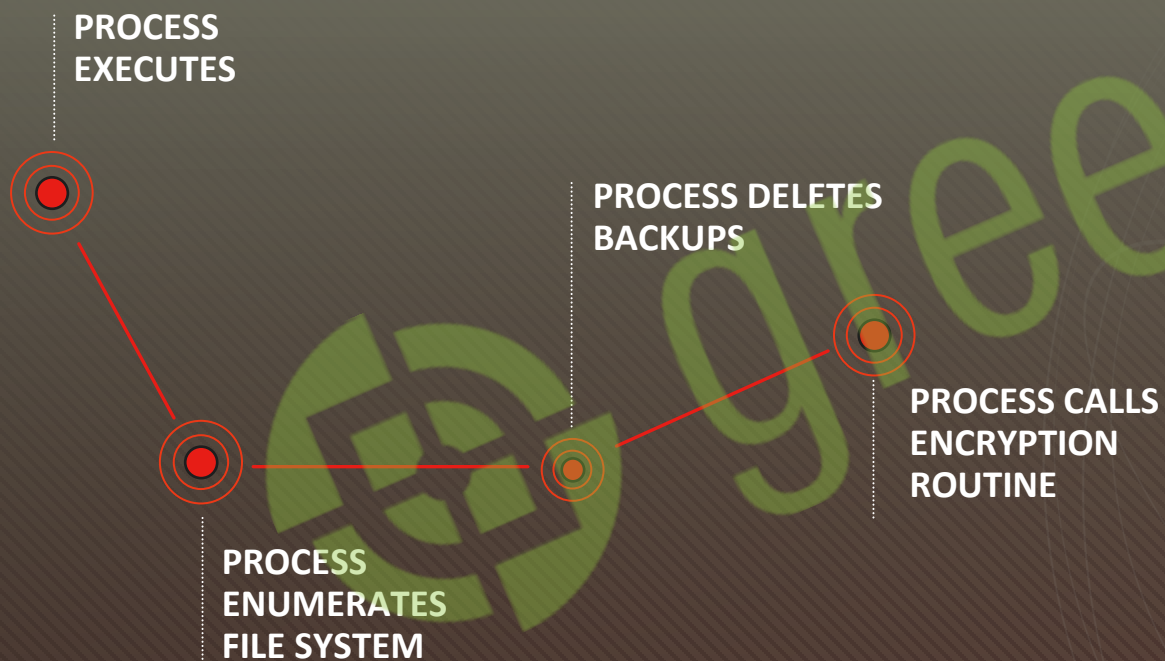
Poprawia produktywność użytkowników –
brak wpływu na użytkownika

Zmniejsza złożoność

Zapewnia wydajność i
skuteczność bezpieczeństwa



INDICATORS OF ATTACK (IOA) – WSKAŹNIKI ATAKU



WSKAŹNIKI ATAKU

Wykonanie kodu, utrwalenie, ukrycie, kontrola poleceń, ruchy boczne

PROAKTYWNE WSKAŹNIKI ATAKU

VS

REAKTYWNE WSKAŹNIKI KOMPROMITACJI

IOCs

Malware, Signatures, Exploits, Vulnerabilities, IP Addresses

ENDPOINT DETECTION AND RESPONSE (EDR) – FALCON INSIGHT

Wyszukiwanie
w czasie
rzeczywistym
oraz z danych
historycznych



Reakcja i
powstrzymywanie
w czasie
rzeczywistym



Nagrywanie
zdarzeń



Połowanie na
zagrożenia



WARTOŚĆ BIZNESOWA

Skraca czas na odpowiedź

Poprawia wydajność SOC

Skraca czas potrzebny na
naprawę

Umacnia umiejętności i
wiedzę

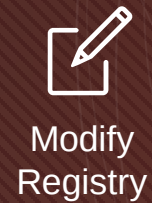
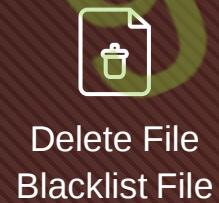
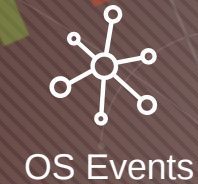
Ogranicza ryzyko

Zwiększa wydajność i
skuteczność bezpieczeństwa



SILNA ODPOWIEDŹ I REMEDIACJA

COLLECT INFO



TAKE ACTION



JEDEN LEKKI AGENT



40MB	8MB	2MB
Windows	Mac	Linux
installer	Installer	Installer



Architektura oparta na chmurze zapewniająca szybkość i natychmiastową operacjonalizację



Kompatybilny ze wszystkimi istniejącymi rozwiązaniami proxy



Wykorzystanie procesora: 1-2%
Wykorzystanie pamięci: do 60MB
Przepustowość: 5 MB / 24H

Microsoft Windows

64-bit server OSes: Windows Server 2008 R2 SP1 and newer (*including Server 2019*)
64-bit desktop OSes: Windows 7 SP1 and newer (incl 8, 10, Windows 10 IOT Enterprise etc)
32-bit desktop OSes: Windows 7 SP1

Apple OSX

macOS 10.15 Catalina
macOS 10.14 Mojave
macOS 10.13 High Sierra
macOS 10.12 Sierra – support ended 9/30/19

Linux

Amazon Linux 2
Amazon Linux AMI (2018.03, 2017.09, 2017.03)
CentOS (6.7–6.10 7.1–7.7, 8-8.1)
Red Hat Enterprise Linux (6.7–6.10 7.1–7.7, 8-8.1)
SUSE Linux Enterprise (11.4, 12.1–12.5, 15)
Ubuntu (14.04 LTS, 16-AWS, 16.04 LTS, 18-AWS, 18-GCP, 18.04 LTS)
Oracle Linux (6 - UEK 3, 4, 7 - UEK 3, 4, 5)
Coming Soon (End Q1 2020): Debian
Docker Support on Linux



3 PROSTE KROKI DO WDROŻENIA FALCON



Brak konfiguracji
infrastruktury



Bez dostrajania,
pisania reguł



Zainstaluj agenta
Falcon



Sprawdź
instalację



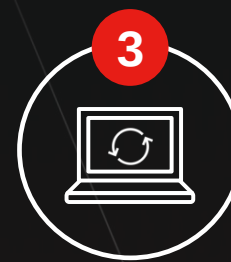
Brak restartu



Brak aktualizacji
sygnatur



Brak skanowania



Usuń starsze
systemy AV

Instytucja finansowa

77,000 AGENTÓW
1 DZIEŃ

Sieć hotelarska

40,000 AGENTÓW
5 DNI

Firma technologiczna

55,000 AGENTÓW 5
DNI

Instytucja finansowa

300,000 AGENTÓW
90 DNI

ROZSZERZ OCHRONĘ STACJI DZIĘKI XDR

JESZCZE LEPSZA DETEKCJA I REAKCJA W CAŁYM ŚRODOWISKU

Zbierz dane



CWPP



Identity



Network



Containers



CASB



Endpoint



Threat Intelligence



Firewall



Web



Email



Cloud



OT/IOT

Wykryj



Parsing



Telemetry
Enrichment



Map to
Schema



Cross-
Correlation



Analytics



Alert
Prioritization

Skoreluj



Triage and Decisioning



Automated Workflows



Unified Hunting and
Investigation



Surgical Response



Scheduled Searches and
Custom Detections



CURRENT TECHNOLOGY PARTNERSHIP LANDSCAPE

SECURITY OPERATIONS

SIEM / UEBA

splunk> sumo logic exabeam IBM Security
 LogRhythm ArcSight Intelligence SEURONIX DEVO
 RAPID panther

SOAR

servicenow splunk> SWIMLANE IBM Security
 LogRhythm Simplify DFLABS Red Hat
 DEMISTO SYNCRITY D3 SECURITY tines ThreatConnect

THREAT INTEL

ANOMALI ATTACK IQ Centripetal EclecticIQ
 CounterFlow cybersixgill DOMAINTOOLS Hunters. INTSIGHTS
 Defend Forward.
 RISKIQ Silobreaker TRU/STAR ThreatConnect
 Threat STOP OPSWAT VIRUSTOTAL

CLOUD, NETWORK
& INFRASTRUCTUREENDPOINT &
NETWORK
SECURITY

AIRLOCK DIGITAL aruba
 a Hewlett Packard
 Enterprise company
 AWAKE The NDR Security Division of
 ARISTA corelight DARKTRACE
 ExtraHop IronNet NOPSEC
 THREAT WARRIOR

EMAIL & WEB
SECURITY

proofpoint mimecast VECTRA
 FORESCOUT Attivo NETWORKS. SAFEGUARD
 CYBER
 PERCEPTION POINT illusive ACALVIO

CLOUD
SECURITY

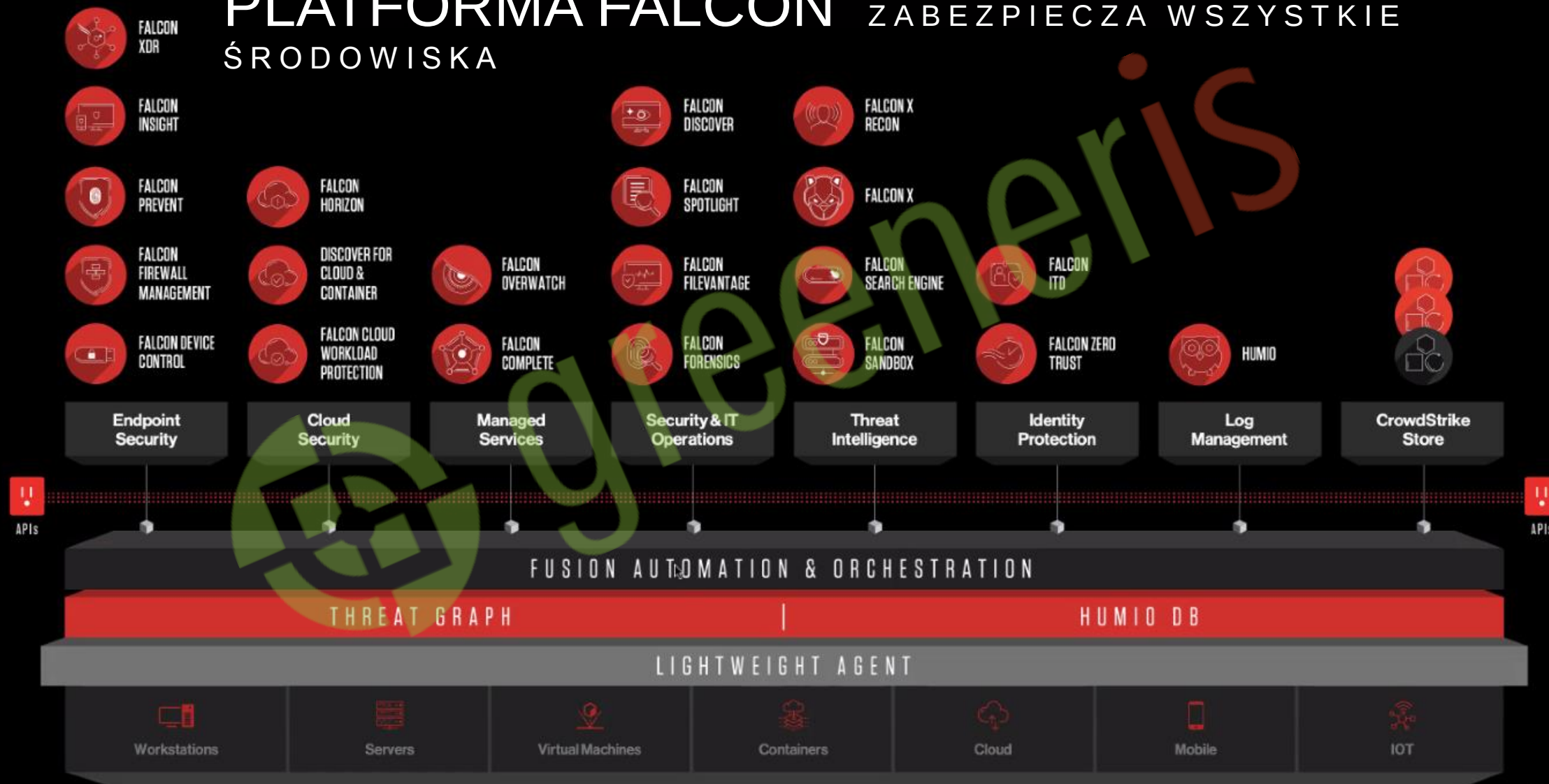
zscaler netskope Akamai TRUEFORT
 okta CLOUDFLARE OBSIDIAN DcControl.

ICS/IOT

ARMIS. DRAGOS FORESCOUT
 CLAROTY MEDIGATE CROWDSTRIKE
 alliances

PLATFORMA FALCON

ZABEZPIECZA WSZYSTKIE ŚRODOWISKA



Zapraszamy na kolejne webinaria i warsztaty on-line

Informacje o zbliżających się webinarach będziemy publikowali na naszej stronie
www: konferencje.greeneris.com oraz w social mediach.



Zapraszamy do śledzenia naszego profilu na Facebooku lub LinkedIn.





greeneris

www.greeneris.com