

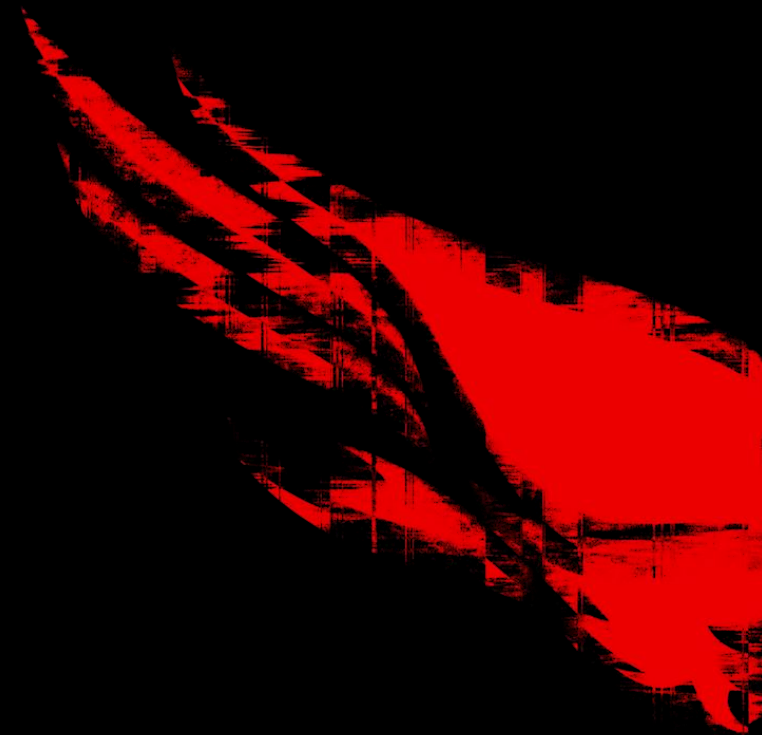


Jak AI i uczenie maszynowe platformy CrowdStrike Falcon zmienia pracę administratora IT?

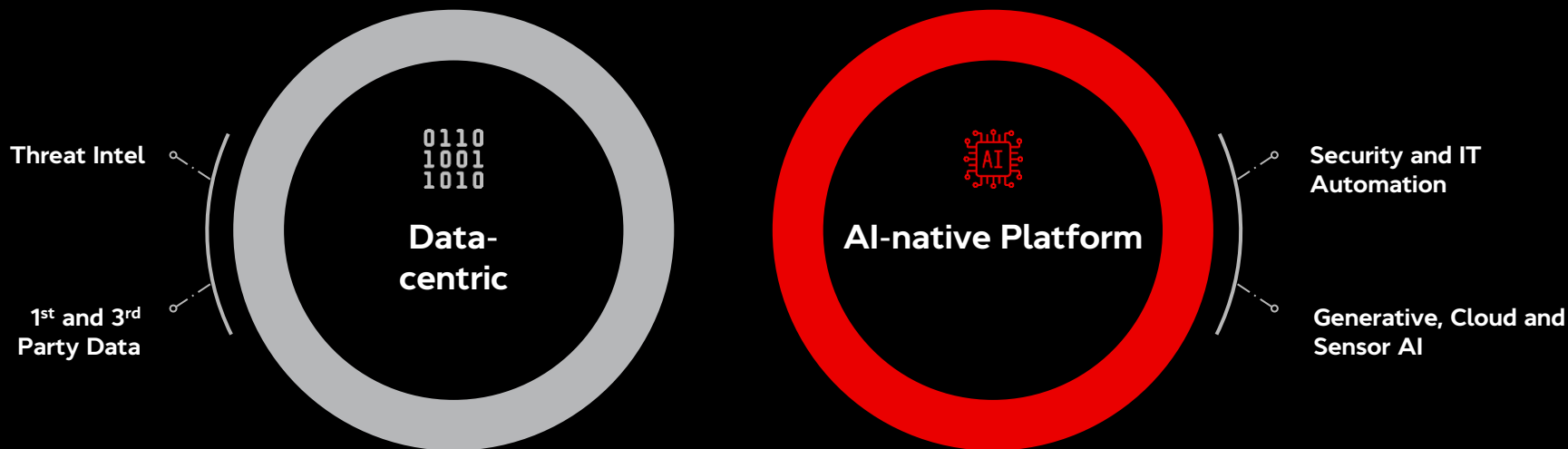


Bartosz Galoch

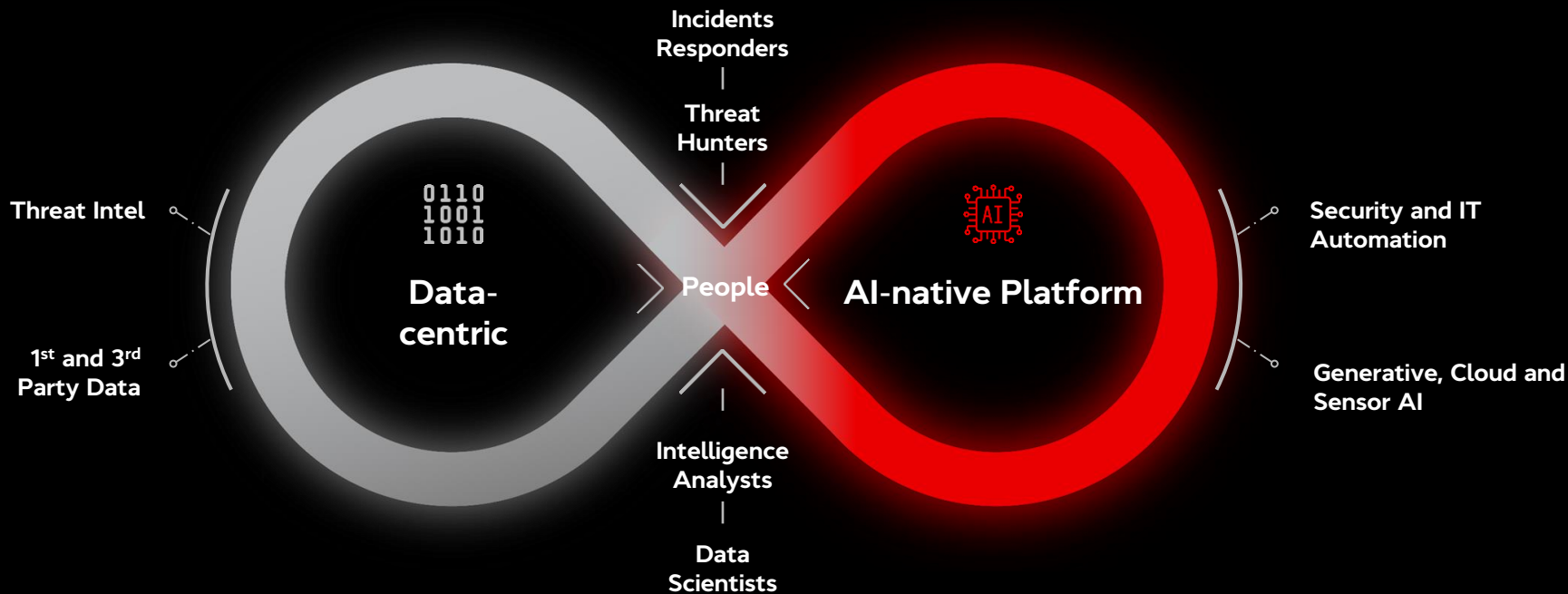
CrowdStrike Product Manager
iIT Distribution Polska



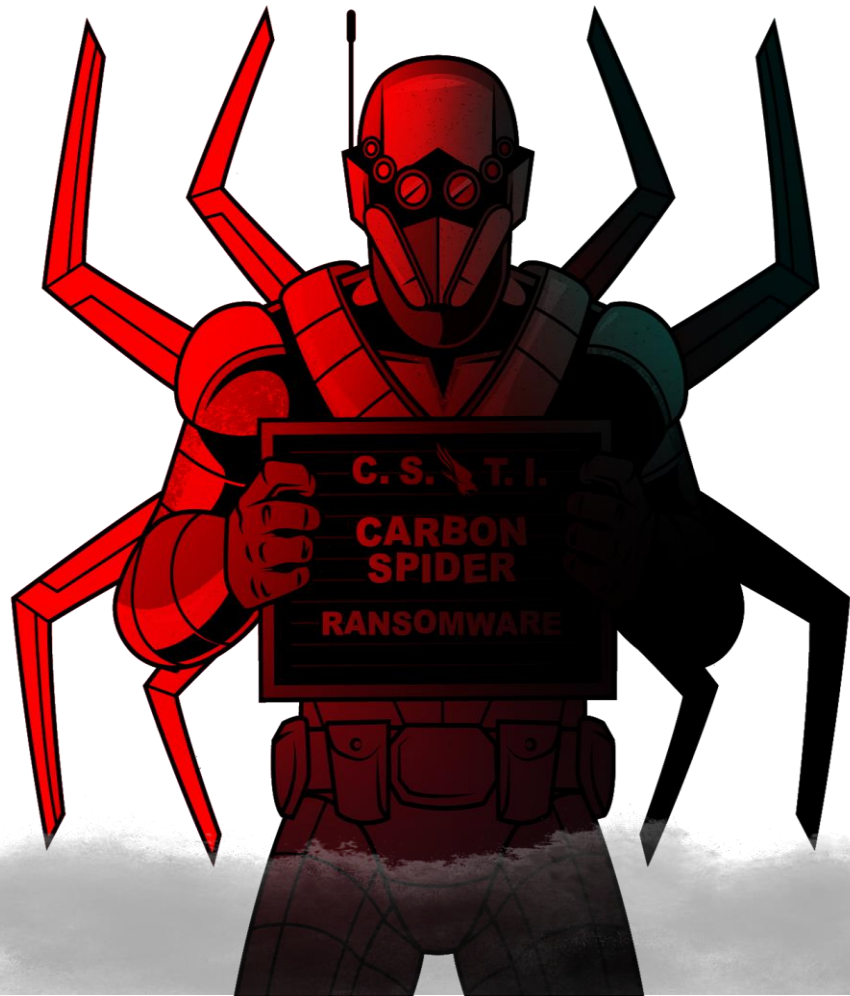
Pionierzy w podejściu do platformy **opartej na danych**



Pionierzy w podejściu do platformy **opartej na danych**



Nie masz problemu
ze złośliwym
oprogramowaniem,
Masz problem
z „**adwersarzami**”.





PUNK
SPIDER

SCATTERED
SPIDER

BITWISE
SPIDER



PUNK
SPIDER

WANDERING
SPIDER

BITWISE
SPIDER



VICE
SPIDER

FANCY
BEAR

WANDERING
SPIDER



ETHEREAL
PANDA



BITWISE
SPIDER



PUNK
SPIDER



BITWISE
SPIDER



VICE
SPIDER



VICE
SPIDER



BITWISE
SPIDER



SILENT
CHOLLIMA



BITWISE
SPIDER



FAMOUS
CHOLLIMA



JACKPOT
PANDA



BITWISE
SPIDER



PULSAR
KITTEN



BITWISE
SPIDER



AQUATIC
PANDA



LABYRINTH
CHOLLIMA



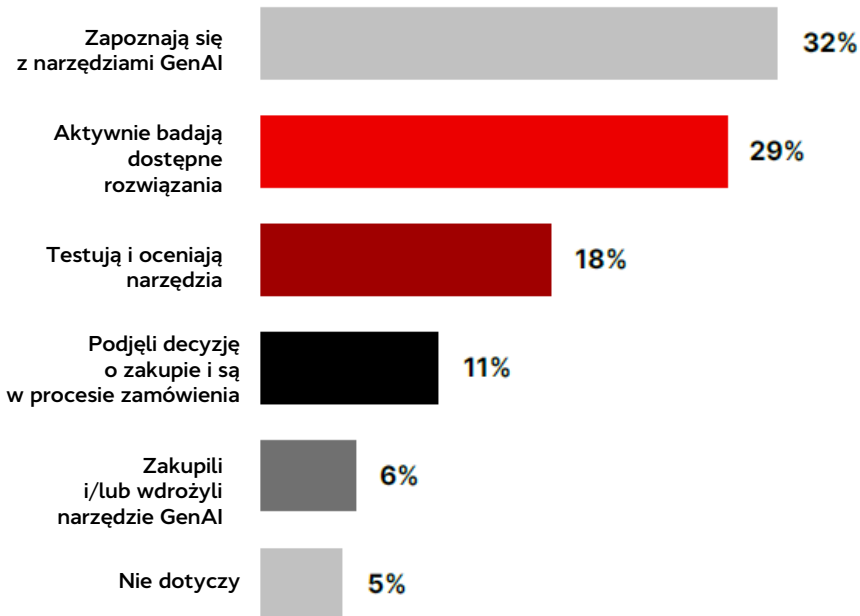
HORDE
PANDA

Badanie: Stan AI w Cyberbezpieczeństwie

CrowdStrike zlecił
przeprowadzenie badania
wśród ponad 1 000
profesjonalistów ds.
cyberbezpieczeństwa,
aby poznać ich opinię
na temat GenAI.



Na jakim etapie zakupu GenAI są profesjonaliści ds. cyberbezpieczeństwa?



Zespoły ds. bezpieczeństwa preferują podejście platformowe

80% respondentów

woli, aby GenAI było dostarczane poprzez platformę cyberbezpieczeństwa, a nie jako pojedyncze narzędzie.

63% respondentów

zmieniłoby dostawcę zabezpieczeń, aby korzystać z GenAI innego dostawcy.

64% respondentów

bada dostępne na rynku narzędzia GenAI lub już je zakupiło.

Zaprojektowana specjalnie dla cyberbezpieczeństwa

76% respondentów

preferuje narzędzia GenAI stworzonych do cyberbezpieczeństwa, zamiast ogólnych rozwiązań AI.

74% respondentów

doświadczyło naruszenia w ciągu ostatnich 12-18 miesięcy, albo obawia się, że mogą być na nie narażeni.

83% respondentów

nie ufa narzędziom, które dostarczają nieodpowiednich lub nieprzemyślanych wskazówek dotyczących bezpieczeństwa.



Najlepsze przepływy pracy związane z bezpieczeństwem dla narzędzi GenAI



Analiza i podsumowanie danych dotyczących zagrożeń



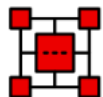
Wspomagana detekcja i analiza



Zautomatyzowana reakcja i/lub wdrożenie przepływu pracy



Pisanie i edytowanie zapytań lub skryptów



Wspomagane zarządzanie lukami w zabezpieczeniach i ich łatanie



Wdrożenie analityków i odpowiadanie na pytania dotyczące funkcjonalności produktu



Umożliwienie zespołom spoza działu bezpieczeństwa (IT, inżynieria itp.) samodzielnego uzyskiwania odpowiedzi na pytania

Wsparcie - nie zastąpienie

Uczestnicy badania są zgodni

GenAI zoptymalizuje pracę analityków, ale nie zastąpi ludzi.

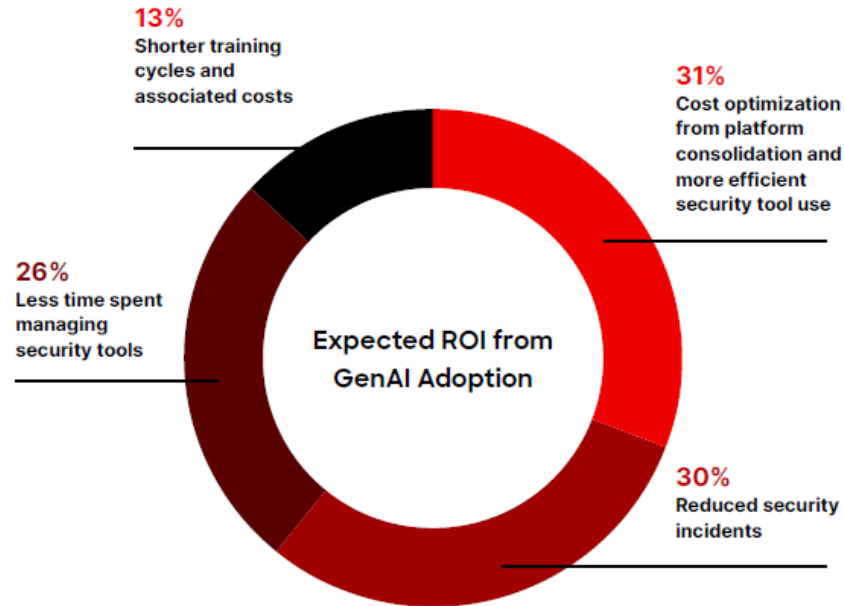
Respondenci postrzegają GenAI jako narzędzie do **poprawy komfortu pracy** analityków.

Najczęściej wskazywane obszary zastosowania GenAI koncentrują się na zwiększeniu produktywności analityków i usprawnieniu analizy danych.

Kluczowy jest **mierzalny** zwrot z inwestycji (ROI)

Najważniejszym aspektem ekonomicznym GenAI nie jest koszt, lecz **możliwość wykazania konkretnego zwrotu z inwestycji**.

Respondenci oczekują stopniowych oszczędności wynikających z **konsolidacji narzędzi w jednej platformie**.





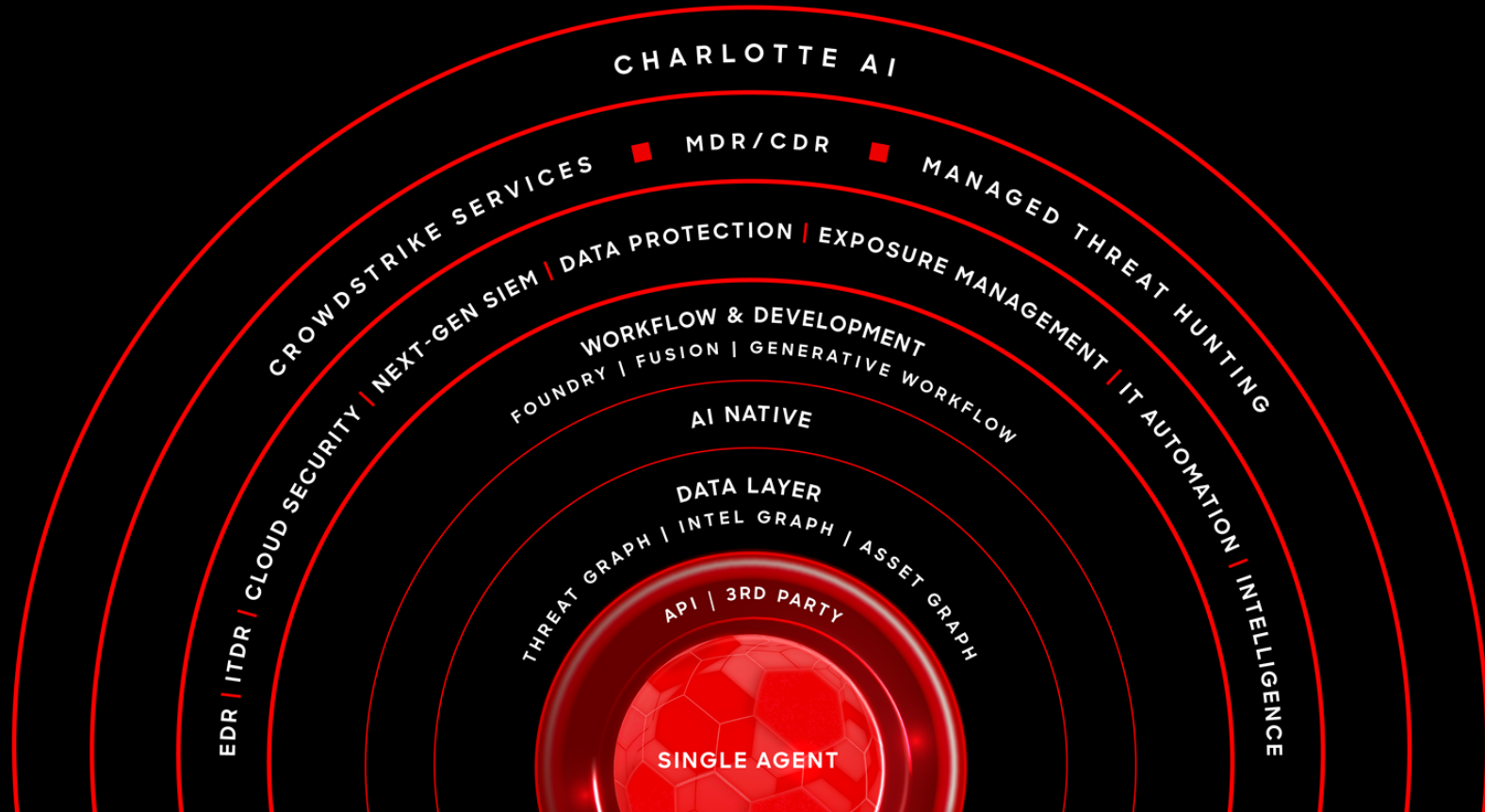
Bezpieczeństwo i prywatność to priorytet

Użytkownicy obawiają się ryzyka związanego z GenAI i **oczekują solidnych zabezpieczeń** oraz **ochrony prywatności** jako kluczowych funkcji.

Największe obawy dotyczą **narażenia danych na dostęp** przez podstawowe duże modele językowe (LLM) oraz potencjalnych ataków na narzędzia GenAI.

87% respondentów wdrożyło już nowe zasady bezpieczeństwa lub opracowuje polityki regulujące wykorzystanie GenAI w ciągu najbliższego roku.

Platforma CrowdStrike Falcon XDR





Zamień godziny pracy w minuty – a nawet **sekundy**

40+ zaoszczędzonych godzin pracy

Średnia liczba godzin zaoszczędzonych tygodniowo dzięki automatyzacji analizy wykrywania za pomocą agentowej AI

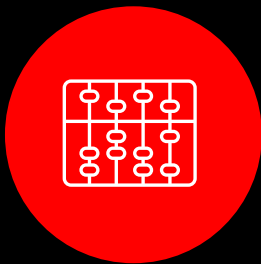
75% szybsze odpowiedzi

Szybsze uzyskiwanie odpowiedzi na pytania dotyczące Twojego środowiska

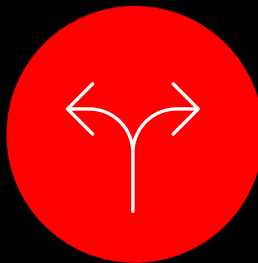
57% szybciej utworzone zapytania

Szybsze tworzenie zapytań, wspierające analityków na każdym poziomie zaawansowania

Ai zbudowane na **najdokładniejszych danych** dotyczących bezpieczeństwa na świecie



**Ponad 2 biliony
zdarzeń dziennie**



**Ponad 180 milionów
decyzji IoA na
sekundę**



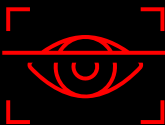
**3x lepsza
priorytetyzacja
podatności dzięki
ExPRT.AI**

Zaprojektowane z myślą o **bezpiecznym** i **odpowiedzialnym** wykorzystaniu zaawansowanej AI



Odpowiedzialność

Korzystaj z zaufanych danych platformy Falcon.



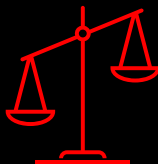
Przejrzystość

Śledź podstawowe źródła z możliwością sprawdzenia szczegółów odpowiedzi.



Prywatność

Zapobiegaj nieautoryzowanemu ujawnieniu danych dzięki kontroli dostępu opartej na rolach.



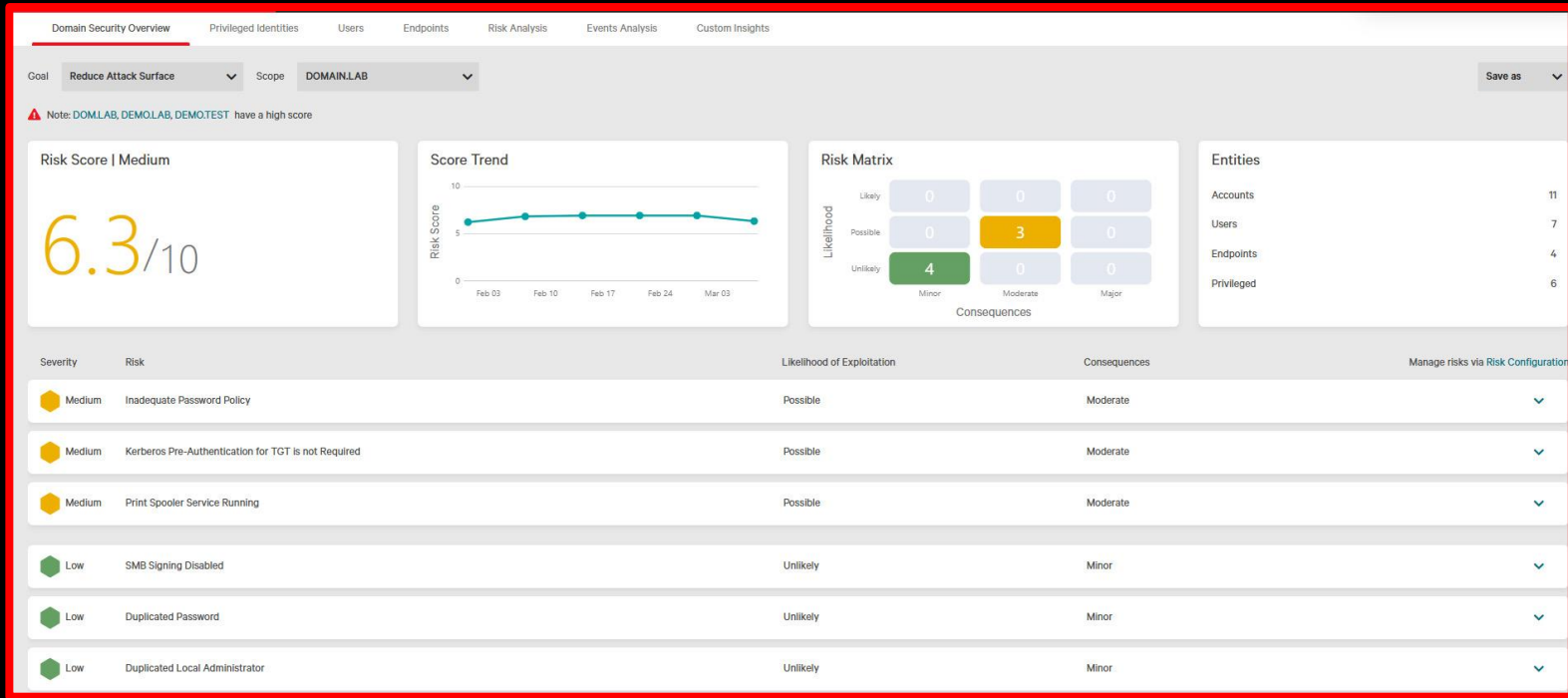
Uczciwość

Bądź pewny, że modele językowe (LLM) nie są trenowane na danych osobowych (PII)



Bezpieczeństwo

Miej pewność, że analitycy sprawdzają i autoryzują wszystkie działania lub skrypty.



SeverityDetect TLNameAttributesAssigned ...ResolutionStatus

Mar. 2, 2025

Command line

"C:\RadioScan\HackRF\sdrsharp-1893\SDRSharp.exe"

File path

\Device\HarddiskVolume3\RadioScan\HackRF\sdrsharp-1893\SDRSharp.exe

State

Local process ID

Not running13916

Hash

be9569c09a73fca44f185fd2187500f732e75916ddf02e1d656bd18c35a75f45

External prevalence

Internal prevalence

Hash action

Associated MD5

LowUnique--8dc083dc85444928de0643f891c1e7

User

DESKTOP-3JGK5M8\HP1

Login type

Logon time

Login server

Login domain

INTERACTIVE - The security principal is logging on interactively.

Feb. 27, 2025 21:04:13

DESKTOP-3JGK5M8

DESKTOP-3JGK5M8

Mar. 2, 2025 09:26:14

Machine Learning via Sensor-based ML

Description

This file meets the machine learning-based on-sensor AV protection's lowest-confidence threshold for malicious files.

Triggering indicator

SHA256 on library/DLL loaded

Associated IOC (SHA256)

be9569c09a73fca44f185fd2187500f732e75916ddf02e1d656bd18c35a75f45

Associated MD5

Global prevalence

Local prevalence

8dc083dc85444928de0643f891c1e7

Low

Unique

Hash action

None

Associated file

\Device\HarddiskVolume3\RadioScan\HackRF\sdrsharp-1893\SDRSharp.exe

670 results (1-20 shown)

Items per page20

Page 1 of 34

See full detection

Mar. 2, 2025 09:26:14

SDRSharp.exe on DESKTOP-3JGK5M8 by HP1

Edit status

Network contain

Connect to host

No notes from OverWatch

No related adversaries

Status

Process

Workflows

2

Hash

be9569c09a73fca44f185fd2187500f732e75916ddf02e1d656bd18c35a75f45

Activity

Intelligence

IOC Management

Sandbox

CrowdStrike

External prevalence

Internal prevalence

Last seen

LowUnique

Mar. 4, 2025 07:21:20

of hosts

of detections

Hash action

133

No action

History

20h, 21, 2025 13:48:45

6

See more in indicator graph

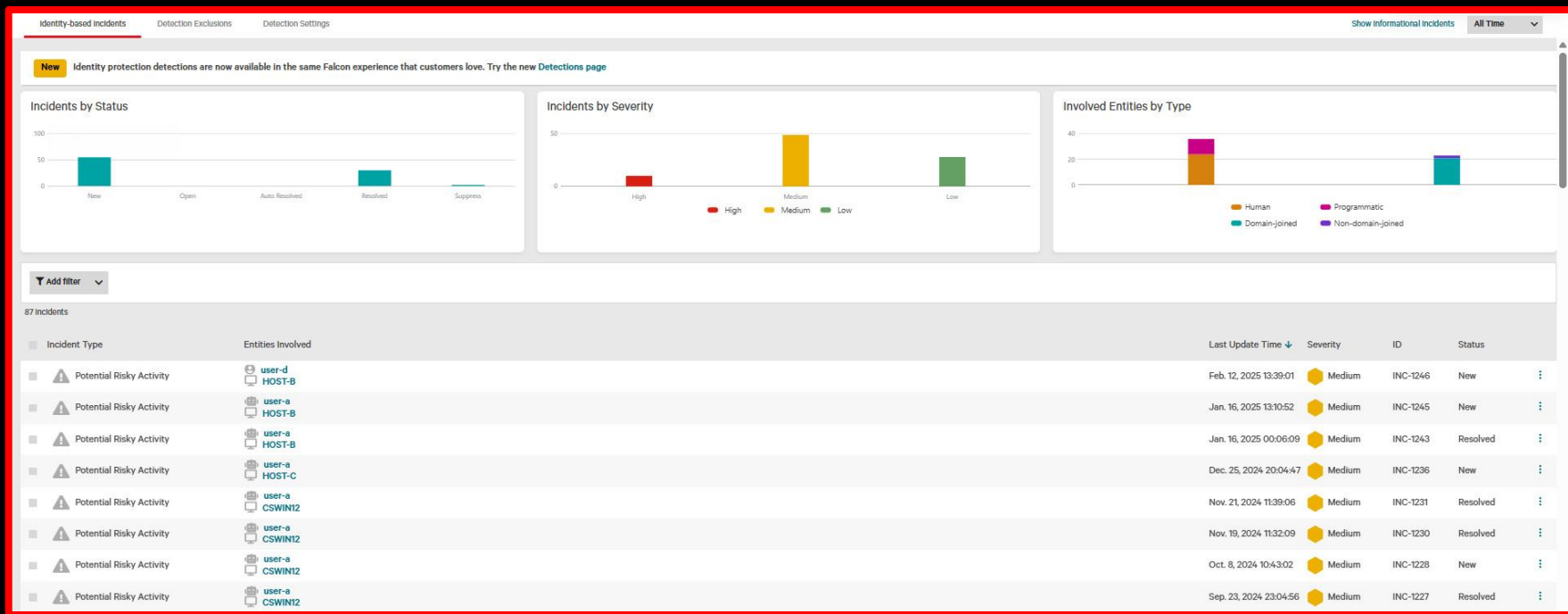
No file

No quarantined files

CROWDSTRIKE

iITD INTELLIGENT
IT DISTRIBUTION

☐	Severity	Detect time	Name	Attributes		Assigned to	Resolution	Status			
Mar. 4, 2025											
☐	Severity Low	Detect time 07:11:50	Process on host Browserupdphenix.exe on DESKTOP-R3GAHNQ by default...	Tactic via technique Malware via PUP	Triggering file Browserupdphenix.exe	Hostname DESKTOP-R3GAHNQ	User name defaultuser0	Assigned to Unassigned	Resolution --	Status New	
☐	Severity Low	Detect time 07:09:24	Process on host dstudio-gui.exe on DESKTOP-R3GAHNQ by defaultuser0	Tactic via technique Malware via PUP	Triggering file dstudio-gui.exe	Hostname DESKTOP-R3GAHNQ	User name defaultuser0	Assigned to Unassigned	Resolution --	Status New	
Mar. 3, 2025											
☐	Severity Low	Detect time 19:00:27	Process on host KMSAuto Net.exe on DESKTOP-6SN9HEN by Татьяна	Tactic via technique Machine Learning via Cloud-based ML	Triggering file MSAuto Net.exe	Hostname DESKTOP-6SN9HEN	User name Татьяна	Assigned to Unassigned	Resolution --	Status New	
☐	Severity Low	Detect time 18:56:48	Process on host utweb.exe on DESKTOP-6SN9HEN by Татьяна		Triggering file web.exe	Hostname DESKTOP-6SN9HEN	User name Татьяна	Assigned to Unassigned	Resolution --	Status New	
☐	Severity Low	Detect time 17:37:55	Process on host L2.exe on DESKTOP-FUTE6B9 by Admin	Tactic via technique Machine Learning via Cloud-based ML	Triggering file L2.exe	Hostname DESKTOP-FUTE6B9	User name Admin	Assigned to Unassigned	Resolution --	Status New	
☐	Severity High	Detect time 08:00:19	Process on host powershell.exe on PERSON3 by 0503	Tactic via technique Malware via Malicious File	Triggering file powershell.exe	Hostname PERSON3	User name 0503	Assigned to Unassigned	Resolution --	Status New	
☐	Severity Low	Detect time 07:25:00	Process on host AAct.exe on DESKTOP-R3GAHNQ by DESKTOP-R3GAHNQ	Tactic via technique Malware via PUP	Triggering file AAct.exe	Hostname DESKTOP-R3GAHNQ	User name DESKTOP-R3GAHNQ\$	Assigned to Unassigned	Resolution --	Status New	
☐	Severity Low	Detect time 07:24:59	Process on host Browserupdphenix.exe on DESKTOP-R3GAHNQ by default...	Tactic via technique Malware via PUP	Triggering file Browserupdphenix.exe	Hostname DESKTOP-R3GAHNQ	User name defaultuser0	Assigned to Unassigned	Resolution --	Status New	
☐	Severity Low	Detect time 07:23:16	Process on host dstudio-gui.exe on DESKTOP-R3GAHNQ by defaultuser0	Tactic via technique Malware via PUP	Triggering file dstudio-gui.exe	Hostname DESKTOP-R3GAHNQ	User name defaultuser0	Assigned to Unassigned	Resolution --	Status New	



Add filter

87 incidents

Incident Type	Entities Involved	Last Update Time	Severity	ID	Status
Potential Risky Activity	user-d HOST-B	Feb. 12, 2025 13:39:01	Medium	INC-1246	New
Potential Risky Activity	user-a HOST-B	Jan. 16, 2025 13:10:52	Medium	INC-1245	New
Potential Risky Activity	user-a HOST-B	Jan. 16, 2025 00:06:09	Medium	INC-1243	Resolved
Potential Risky Activity	user-a HOST-C	Dec. 25, 2024 20:04:47	Medium	INC-1236	New
Potential Risky Activity	user-a CSWIN12	Nov. 21, 2024 11:39:06	Medium	INC-1231	Resolved
Potential Risky Activity	user-a CSWIN12	Nov. 19, 2024 11:32:09	Medium	INC-1230	Resolved
Potential Risky Activity	user-a CSWIN12	Oct. 8, 2024 10:43:02	Medium	INC-1228	New
Potential Risky Activity	user-a CSWIN12	Sep. 23, 2024 23:04:56	Medium	INC-1227	Resolved

Possible Compromised Domain New High

Type Change

Jan. 17, 2024 17:04:19

Incident type changed from Potential Risky Activity to Possible Compromised Domain

Suspicious domain replication

Jan. 18, 2024 02:59:59

Tactic & technique: [Credential Access](#) via DCSync

Technique ID: T1003.006

Domain replication was executed from 192.168.1.2 by DC-01

More

Anomalous RPC (ZeroLogon)

Acknowledge & trust

Jan. 18, 2024 02:54:59

Tactic & technique: [Lateral Movement](#) via Exploitation of Remote Services (ZeroLogon)

Technique ID: T1210

An unusual NetServerAuthenticate3 DCE/RPC request was performed from 192.168.1.2 on DC-01. This DCE/RPC fits the pattern of ZeroLogon (CVE-2020-1472) exploit.

More

Involved Endpoints (1)

192.168.1.2

Latest Activity

Never

Comments

Add your note about this incident

Add comment

Recommendations

1 Contact the account owner to investigate activity

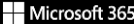
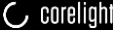
2 This operation is common among cloud syncing software like Entra Connector

3 If this is not an approved action assume the domain was compromised, consider changing the password of all the domain users

4 Review activity of users that associate with the suspected infected endpoint

5 Look over the account activity in recent time

Integracja z zewnętrznymi narzędziami

Identity/SSO	Web security (SWG)	Cloud access security broker (CASB)	 Falcon The Definitive AI-Native Cybersecurity Platform	Email	Network detection & response (NDR)	Firewall
   	  	 		    	  VECTRA 	  



CrowdStrike Marketplace

Search a product, company, and more...



Rozwiązania CrowdStrike cieszą się **światowym** **uznaniem** m.in.:

Gartner®

FROST &
SULLIVAN

IDC

FORRESTER®

SC awards

Gartner
peer insights™



Figure 1: Magic Quadrant for Endpoint Protection Platforms



CROWDSTRIKE

iITD INTELLIGENT
IT DISTRIBUTION

CROWDSTRIKE zaufali:



61 ze 100

pośród firm na liście Fortune 100

37 ze 100

w rankingu największych globalnych firm

13 z 20

w rankingu największych banków

5 z 10

w rankingu największych dostawców
w sektorze opieki zdrowotnej

7 z 10

w rankingu największych rozwiązań
w branży energetycznej



CrowdStrike 2025 Global Threat Report



51 sekund

wyniósł najkrótszy czas
przetamania zabezpieczeń

48 minut

- to średni czas przetwarzania
zabezpieczeń przez adversarzy

79% włamań

było wolnych od złośliwego
oprogramowania

52% wykrytych luk

w 2024 roku to ataki mające na celu
zdobycie pierwszego punktu wejścia
do sieci organizacji

O 442%

wrosła ilość oszustw telefonicznych
wykorzystujących inżynierię społeczną

35% incydentów

ransomware było związanych z przejęciem
kont użytkowników chmurowych
i wykorzystaniem ich do dalszych ataków.

O 150%

wzrosła aktywności grup cyberprzestępczych
powiązanych z Chinami



Dziękuję

Bartosz Galoch
CrowdStrike
Product Manager



b.galoch@iit-d.pl
+48 662 910 762