TD SYNNEX

AWS SMB Fraud Defense Workshop

Date	Author	Version
23.09.2023	Piotr Blonkowski	2.0

TD SYNNEX

Agenda

0. Wprowadzenie
1. O atakach słów kilka
2. Otoczenie regulacyjne
3. Zero Trust Architecture on AWS
4. Checklista
5. Hands-On
6. AWS Security Services
7. Ankieta

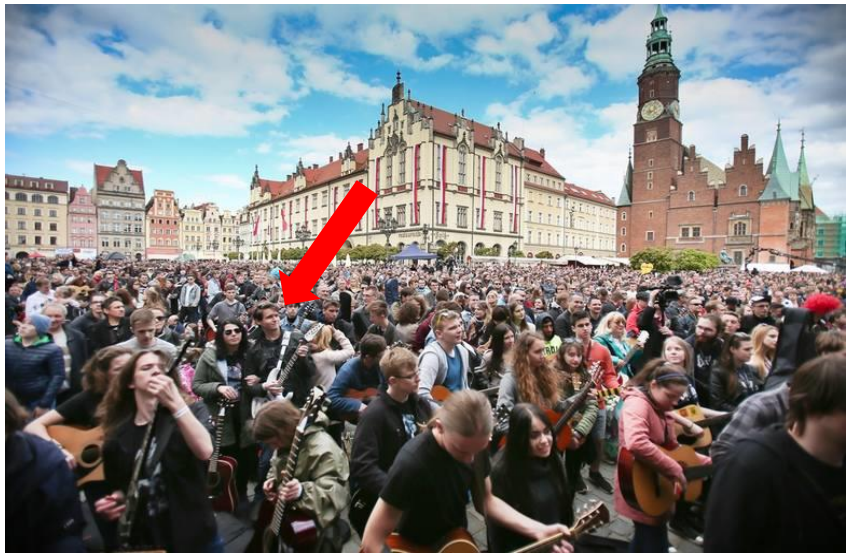
0. Wprowadzenie


AWS
User Groups
Warsaw
23.09.2023, 10:00
Warszawska Wyższa Szkoła Informatyki
Piotr Blonkowski
Cloud Solutions Architect @TD SYNNEX
WARSZTAT:
AWS SMB Fraud Defense
Partners
TD SYNNEX
Warszawska Wyższa Szkoła Informatyki
Hosted by:
Luke Dorosz, AWS Hero
Rafał Mituła, AWS Community Builder

Dziękujemy!

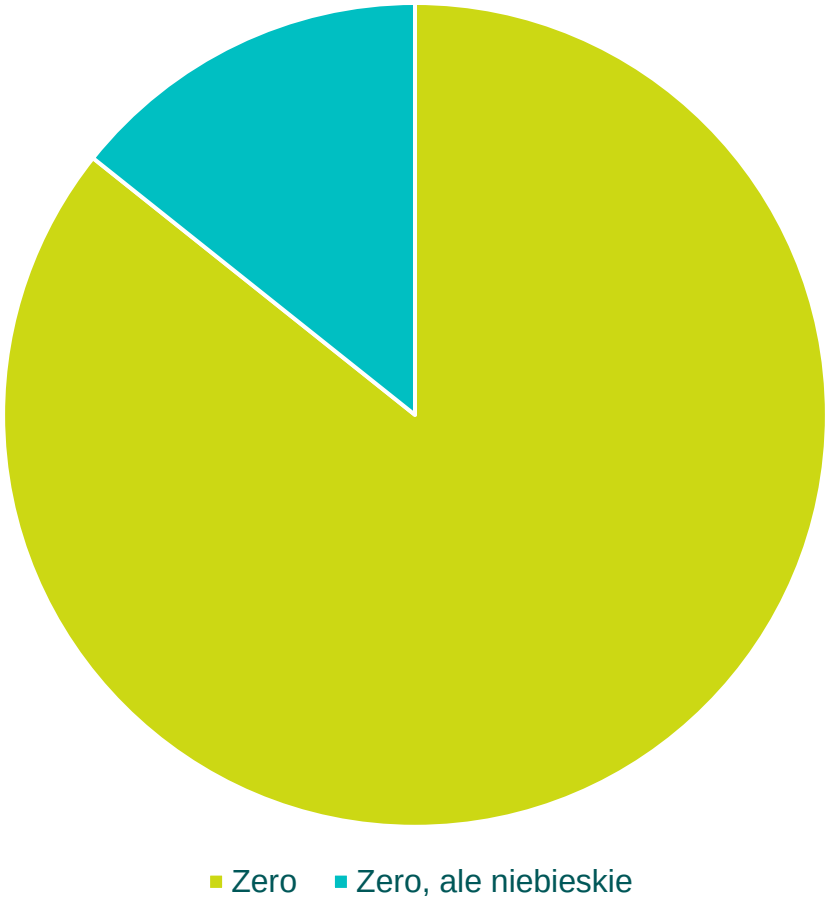
TD SYNNEX

Meet the Trainer



1. O atakach słów kilka

Ile osób jest zainteresowanych danymi statystycznymi na początku prezentacji?



Wprowadzenie do dyskusji

*"Historia każdego większego cyberataku ma tendencję do przechodzenia przez trzy odrębne i rozpoznawalne fazy: **przetrwania**, **dociekania** i **wyrafinowania**, inaczej znane jako fazy "Jak", "Dlaczego" i "Gdzie". Na przykład, pierwsza faza charakteryzuje się pytaniem "**Jak możemy zarobić?**", druga pytaniem "**Dlaczego zarabiamy?**", a trzecia pytaniem "**Gdzie nastąpi kolejny incident?**".*

Zmodyfikowany cytat,
Douglas Addams, Autostopem przez Galaktykę

Dyskusja:
W jaki sposób atakować chmurę publiczną?

Zamawiający informuje, że nie będzie pokrywał kosztów nadmiarowych powstałych na skutek błędów lub ataków hakerskich po stronie Dostawcy chmury lub Wykonawcy. Przygotowywana przez Zamawiającego stosowna zmiana znajduje się Tabeli nr 1 – lista zmian, pod pozycją l.p. 4.

TD SYNNEX

Ile czasu zajęło mi znalezienie szablonu do kopania kryptowalut?

GitHub - mludvig/aws-ethereum-miner: CloudFormation template for mining Ethereum crypto currency on AWS

TD SYNNEX

Czego potrzebuję, żeby zacząć zarabiać?

- InstanceTypes
- Hashrate
- CoinName
- WalletAddress
- PricingPlan
- … no i konto AWS ☺

```
Parameters:
  InstanceTypes:
    Description: |
      Instance types to choose from. Can be "*" to use all available, or wildcards e.g. "g4dn.*,g5.*",
      or a list of specific instances e.g. "p3.2xlarge,p3.8xlarge", or an exclusion e.g. "-p4d.*".
      The most cost effective combination of available instances will be used first.
    Type: String
    Default: "*"

  Hashrate:
    Description: |
      Required Ethash hashrate in MH/s. AWS will start the most cost effective available
      instances to achieve this Hashrate.
    Type: Number
    Default: 1000
    MinValue: 0

  CoinName:
    Type: String
    Description: Coin type
    AllowedValues:
    - ETC
    - RVN
    - ERG
    - KAS
    Default: ETC

  WalletAddress:
    Type: String
    Description: Wallet Address (use BTC address regardless of the Coin type)
    Default: "bc1qjlm3kjy87zs6qywmwz2u0ytlde9z4whyzflg38"

  PricingPlan:
    Type: String
    Description: Spot or On-Demand or Both
    AllowedValues:
    - spot
    - ondemand
    - both
    Default: both
```

Jak zdobyć konto AWS?

CyberDefence 24 | ARMIA I SŁUŻBY | POLITYKA I PRAWO | CYBERBEZPIECZEŃSTWO | STREFA SAMSUNG

CYBERBEZPIECZEŃSTWO

#CyberMagazyn: Systemy polskiej administracji pod ostrzałem. Tak atakowali cyberprzestępcy

NIKOLA BOCHYŃSKA
03.06.2023 07:20

DRUKUJ PDF

Fot. Envato

Rok 2022 był wyjątkowo niespokojny w cyberprzestrzeni, także dla podmiotów administracji rządowej czy infrastruktury krytycznej. Zespół CSIRT GOV we wspomnianym okresie otrzymał w sumie 1,234 mln zgłoszeń o potencjalnym incydencie, w tym 21,56 tys. stanowiło realne zdarzenia w cyberprzestrzeni - wskazano w raporcie CSIRT GOV o stanie bezpieczeństwa w cyberprzestrzeni RP na 2022 rok.

9:23
16/9/2022

[AKTUALIZACJA #2] Uber zhackowany!

Autor: redakcja | Tagi: Hacked!, Uber

Ktoś przejął infrastrukturę Ubera. Do sieci wyciekły screeny z wewnętrznych systemów firmy. Atakujący wypowiadał się też korzystając z oficjalnych kont spółki. Wciąż nie wiadomo, jakie dane klientów pozyskano.

Włamanie

Wygląda na to
strony softwar
zhackowana.
obsługi klient

Pierwsze sygn
oficjalnego ko

UBE
vsph
ACC

Potem, przeci
pojawiła się n

Jak doszło do włamania? Usiądźcie...

Jeśli wierzyć opublikowanym screenom z rozmowy z włamywaczem, to atak w tej skali był możliwy ze względu na ...znalezienie skryptu z zahardcodowanymi danymi dostępowymi do infrastruktury:

Tea Pot
last seen just now

ok so basically uber had a network share \\[redacted]ots. the share contained some powershell scripts.

one of the powershell scripts contained the username and password for a admin user in Thycotic (PAM) Using this i was able to extract secrets for all services, DA, DUO, Onelogin, AWS, GSuite 8:05 PM

on an uber IP range? or [redacted] on like GCP or AWS (*.uberinternal) edited 8:06 PM

in Uber intranet 8:07 PM

*.corp.uber.com edited 8:07 PM

How'd you get access to the intranet then? 8:08 PM

SE an employee -> access VPN -> scan intranet? 8:08 PM

yes! 8:08 PM

exactly 8:08 PM

TD SYNNEX

8:30
11/10/2021

Ile kosztuje niewiedza w chmurze? Analiza 5 niepotrzebnie wysokich rachunków

Autor: redakcja | Tagi: ARTYKUŁ SPONSOROWANY, chmura, Google

Home | Events | Offers | Posts | Live | Photos

[redacted]

Mam problem,
stworzyłem sobie konto google cloud i odpaliłem ten rok próbny z budżetem demonstracyjnym który wynosił gdzieś około 1k.
Oczywiście musiałem podpiąć swoją kartę. Korzystałem wczoraj trochę z tego w trakcie nauki i w nocy zablokowało mi konto i przysłało w ch*j wielka kwotę do rozliczenia.
Jak to k*rwa anulować?

Kiedy tworzyłem konto czytałem że dopóki ręcznie nie zezwolę żadne środki nie zostaną ściągnięte z mojego konta.

Niech ktoś pomoże bo jestem w d*pie.

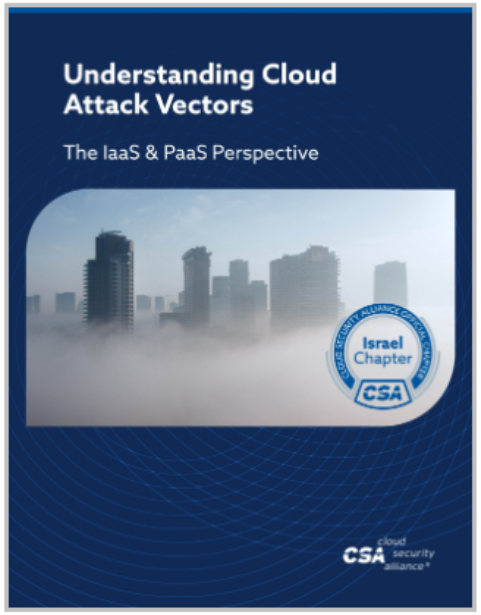
Bieżący miesiąc

1–25 października 2020

Całkowity koszt od początku miesiąca

104 583,66 zł

Cloud Attack Vectors by CSA



Understanding Cloud Attack Vectors

Release Date: 06/06/2023

The goal of the document is to map the various attack vectors that are actually being used during cloud-based attacks in IaaS/PaaS and to map the vectors and their mitigating controls to various resources. The motivation for this document came after we analyzed much research around cloud security and realized that they are listing a combination of risks, threats, attack vectors, vulnerabilities, and concerns. And while there are many risks and threats to IaaS/PaaS platforms and applications, most of the risks are associated with a very specific number of attack vectors.

Link do publikacji

Cloud Attack Vectors by CSA

1: Exploitable Workloads

2: Workloads with Excessive Permissions

3: Unsecured Keys, Credentials, and Application Secrets

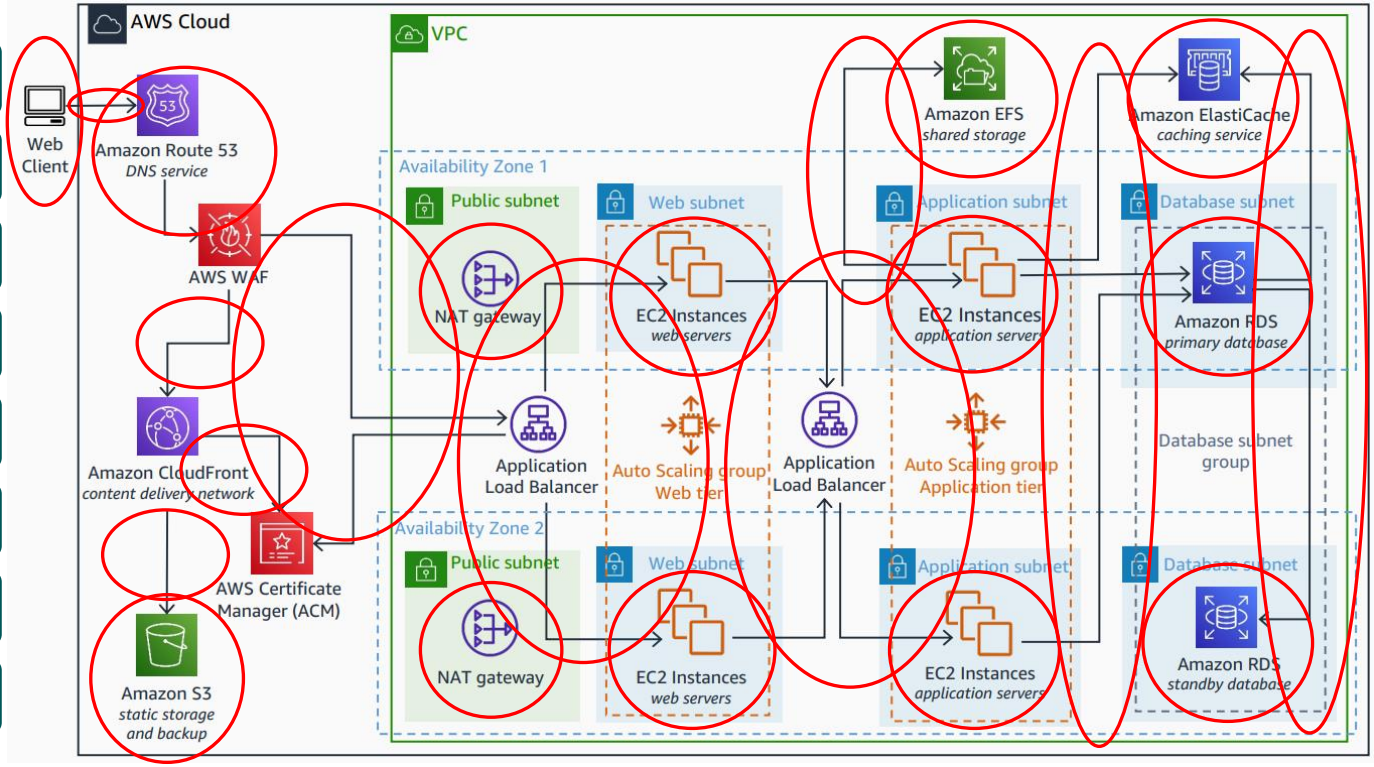
4: Exploitable Authentication or Authorization

5: Unauthorized Access to Object Storage

6: Third-Party Cross-Environment/Account Access

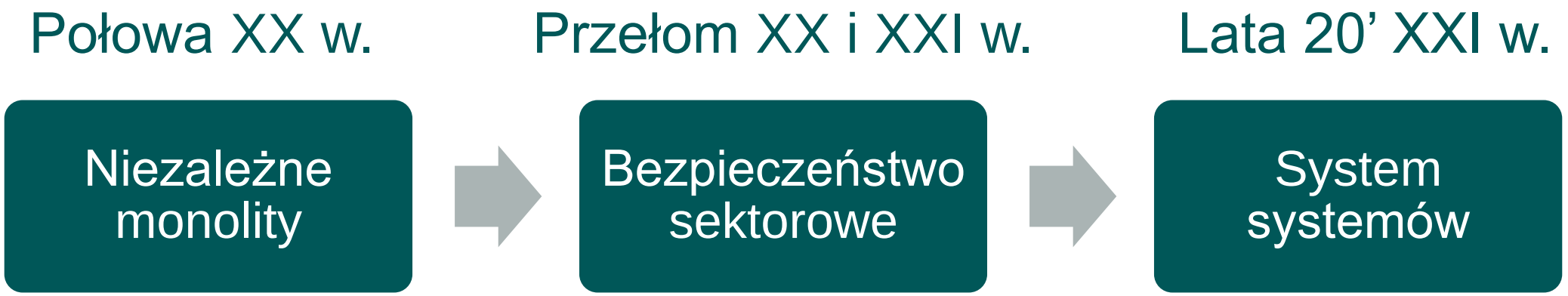
7: Unsecured/Unencrypted Snapshots & Backups

8: Compromised Images



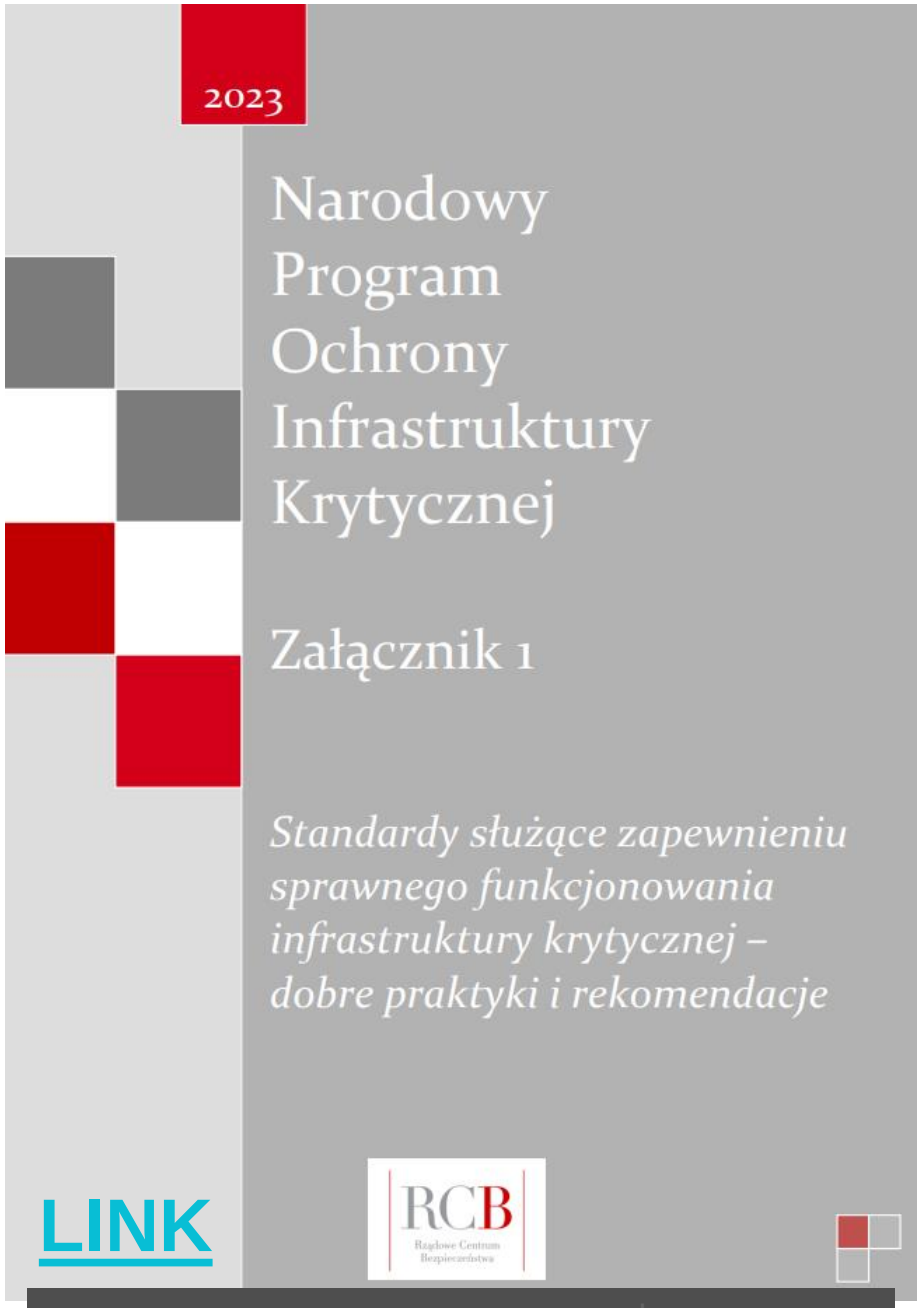
2. Otoczenie regulacyjne

Ewolucja regulacji dot. cyberbezpieczeństwa



Understanding Cybersecurity in the European Union.

1. The NIS 2 Directive
2. The European Cyber Resilience Act
3. The Digital Operational Resilience Act (DORA)
4. The Critical Entities Resilience Directive (CER)
5. The Digital Services Act (DSA)
6. The Digital Markets Act (DMA)
7. The European Health Data Space (EHDS)
8. The European Chips Act
9. The European Data Act
10. The European Data Governance Act (DGA)
11. The Artificial Intelligence Act
12. The European ePrivacy Regulation
13. The European Digital Identity Regulation
14. The European Cyber Defence Policy
15. The Strategic Compass of the European Union
16. The EU Cyber Solidarity Act
17. The EU Cyber Diplomacy Toolbox



LINK

chmur 1/170

2.8. Zapewnienie bezpieczeństwa teleinformatycznego 108

2.8.1. Bezpieczeństwo przetwarzania danych 108
2.8.1.1. Rozwiązania on-premises 108
2.8.1.2. Rozwiązania wykorzystujące przetwarzanie w chmurze obliczeniowej 109
2.8.1.3. Rozwiązania hybrydowe 110
2.8.2. Zasady bezpieczeństwa teleinformatycznego IK 111
2.8.2.1. Poufność, dostępność i integralność informacji 111
2.8.2.2. Rozwiązania organizacyjne, technologiczne, kontraktowe i zasoby ludzkie 112
2.8.2.3. Szkolenia i testy 118
2.8.3. Proces bezpieczeństwa teleinformatycznego 121
2.8.3.1. Strategia Zero Trust 121
2.8.3.2. Modele przetwarzania danych 124
2.8.3.3. Rodzaje zagrożeń 127
2.8.3.4. Współodpowiedzialność za ciągłość procesu 137
2.8.4. Budowanie odporności 139
2.8.4.1. Urządzenia końcowe 140
2.8.4.2. Dane 142
2.8.5. Dostępność systemów i aplikacji. Kopie zapasowe 147
2.8.6. Plan Ewakuacji do Chmury Obliczeniowej 150
2.8.7. Oprogramowanie 156
2.8.8. Infrastruktura 157
2.8.8.1. Sieci i architektura 157
2.8.8.2. Sieci bezprzewodowe 159
2.8.8.3. Monitoring zdarzeń 161
2.8.9. Bezpieczeństwo automatyki przemysłowej 165
2.8.9.1. Bezpieczeństwo sterowników PAC/PLC/RTU i innych urządzeń programowalnych 165
2.8.9.2. Bezpieczeństwo urządzeń HMI 167
2.8.9.3. Bezpieczeństwo przemysłowych sieci sterowania 167
2.8.10. Plany awaryjne i procedury odtworzenia 169
2.8.10.1. Proces tworzenia i doskonalenia planów 169
2.8.10.2. Reakcja na incydenty 171
2.8.11. Wsparcie działań w sytuacjach awaryjnych 175
2.8.11.1. Security Operation Centre 175
2.8.11.2. Współpraca sektorowa 177
2.8.11.3. Zespoły reagowania na incydenty CSiRT 178
2.8.12. Rekomendacje 182

TD SYNNEX

W szczególności:

- **Rozwiązania wykorzystujące przetwarzanie w chmurze obliczeniowej**
- **Rozwiązania hybrydowe**
- **Strategia Zero Trust**
- **Plan Ewakuacji do Chmury Obliczeniowej**
- **Security Operations Center**

3. Zero Trust Architecture on AWS

The fundamental underlying question

*"What are the **optimal patterns** to ensure the **right levels** of **security and availability** for my **systems and data**?"*

TD SYNNEX

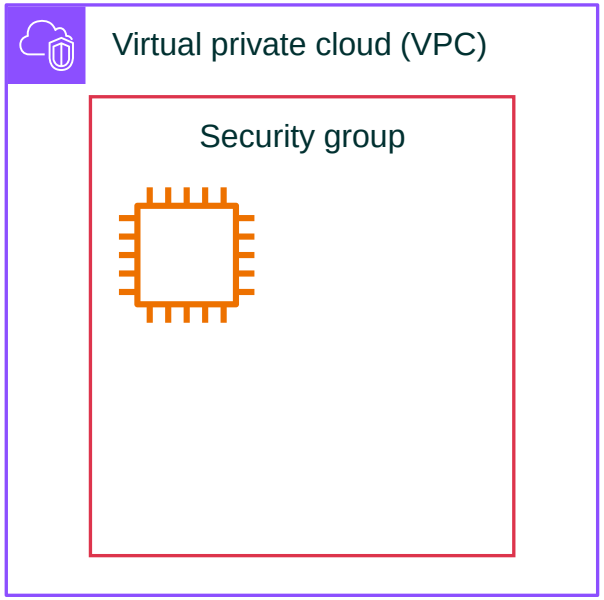
Zero Trust Defined

*A conceptual **security model** and associated set of **mechanisms** that focus on providing security controls around digital assets that **do not solely or fundamentally depend** on traditional network controls or network perimeters*

Muzeum sztuki - balans

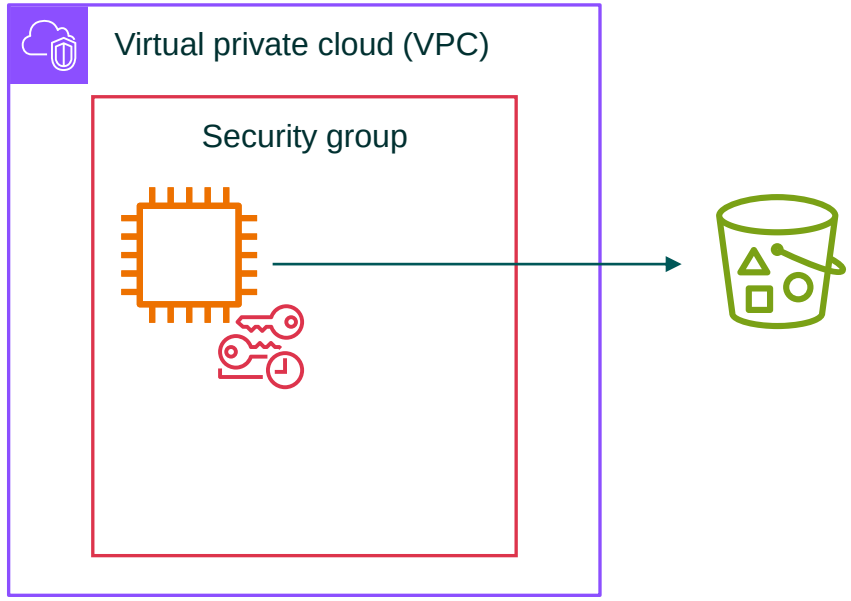
Guiding Principle #1 – Avoid a binary choice

Identity-centric approach **OR** Network-centric approach



Guiding Principle #1 – Avoid a binary choice

Identity-centric approach **AND** Network-centric approach



TD SYNNEX

Guiding Principle #2 – Focus on use cases

Machine-to-machine

Human-to-application

Digital transformation

Same: Technical principles

Different: Organizational objectives

Focus: Problems we're trying to solve

Avoid: Getting mired in low value discussions

Guiding Principle #3 – One size doesn’t fit all

Do: Apply in accordance with the value of the systems being protected

Don’t: Issue inflexible mandates

Opinie ☺ :

1 • Share Best Newest Oldest

mgrennan

a year ago

Classic endless dribble from AWS using AWS wank words with out saying anything.

0 0 Reply • Share ›

Matt Erdogdu

3 years ago

Thanks for this detailed explanation of the Zero Trust concept in AWS.

0 0 Reply • Share ›

TD SYNNEX

Zero Trust Architecture Principles

- AWS Artifact
- AWS CloudTrail
- Amazon CloudWatch
- AWS Config
- Amazon GuardDuty
- AWS Identity and Access Management
- AWS Key Management Service
- AWS Secrets Manager
- AWS Security Hub
- Amazon Virtual Private Cloud

Verify and authenticate

Least privilege access

Micro-segmentation

Continuous monitoring and analytics

Automation and orchestration

AWS re:Invent 2022 - Zero Trust: Enough talk, let's build better security (SEC405) - YouTube

4. Checklista

TD SYNNEX

AWS Startup Security Baseline

Securing your account

Securing your account overview

- ACCT.01 – Set account-level contacts to valid email distribution lists
- ACCT.02 – Restrict use of the root user
- ACCT.03 – Configure console access for each user
- ACCT.04 – Assign permissions
- ACCT.05 – Require multi-factor authentication (MFA) to log in
- ACCT.06 – Enforce a password policy
- ACCT.07 – Deliver CloudTrail logs to a protected S3 bucket
- ACCT.08 – Prevent public access to private S3 buckets
- ACCT.09 – Delete unused VPCs, subnets, and security groups
- ACCT.10 – Configure AWS Budgets to monitor your spending
- ACCT.11 – Enable and respond to GuardDuty notifications
- ACCT.12 – Monitor for and resolve high-risk issues by using Trusted Advisor

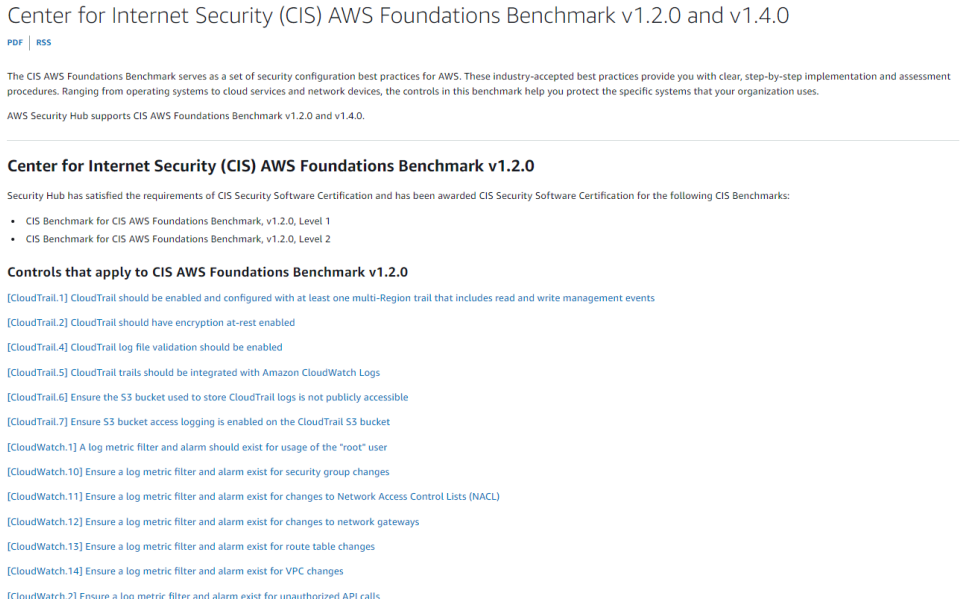
Securing your account - AWS Prescriptive Guidance (amazon.com)

TD SYNNEX

CIS Amazon Web Services Foundations Benchmark

CIS Amazon Web Services Foundations Benchmark

AWS Documentation



Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0 and v1.4.0

PDF | RSS

The CIS AWS Foundations Benchmark serves as a set of security configuration best practices for AWS. These industry-accepted best practices provide you with clear, step-by-step implementation and assessment procedures. Ranging from operating systems to cloud services and network devices, the controls in this benchmark help you protect the specific systems that your organization uses.

AWS Security Hub supports CIS AWS Foundations Benchmark v1.2.0 and v1.4.0.

Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0

Security Hub has satisfied the requirements of CIS Security Software Certification and has been awarded CIS Security Software Certification for the following CIS Benchmarks:

- CIS Benchmark for CIS AWS Foundations Benchmark, v1.2.0, Level 1
- CIS Benchmark for CIS AWS Foundations Benchmark, v1.2.0, Level 2

Controls that apply to CIS AWS Foundations Benchmark v1.2.0

[CloudTrail.1] CloudTrail should be enabled and configured with at least one multi-Region trail that includes read and write management events

[CloudTrail.2] CloudTrail should have encryption at-rest enabled

[CloudTrail.4] CloudTrail log file validation should be enabled

[CloudTrail.5] CloudTrail trails should be integrated with Amazon CloudWatch Logs

[CloudTrail.6] Ensure the S3 bucket used to store CloudTrail logs is not publicly accessible

[CloudTrail.7] Ensure S3 bucket access logging is enabled on the CloudTrail S3 bucket

[CloudWatch.1] A log metric filter and alarm should exist for usage of the "root" user

[CloudWatch.10] Ensure a log metric filter and alarm exist for security group changes

[CloudWatch.11] Ensure a log metric filter and alarm exist for changes to Network Access Control Lists (NACL)

[CloudWatch.12] Ensure a log metric filter and alarm exist for changes to network gateways

[CloudWatch.13] Ensure a log metric filter and alarm exist for route table changes

[CloudWatch.14] Ensure a log metric filter and alarm exist for VPC changes

[CloudWatch.2] Ensure a log metric filter and alarm exist for unauthorized API calls

Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0 and v1.4.0 - AWS Security Hub (amazon.com)

AWS Security Hub wspiera CIS v1.2.0 i v1.4.0

CIS Benchmark

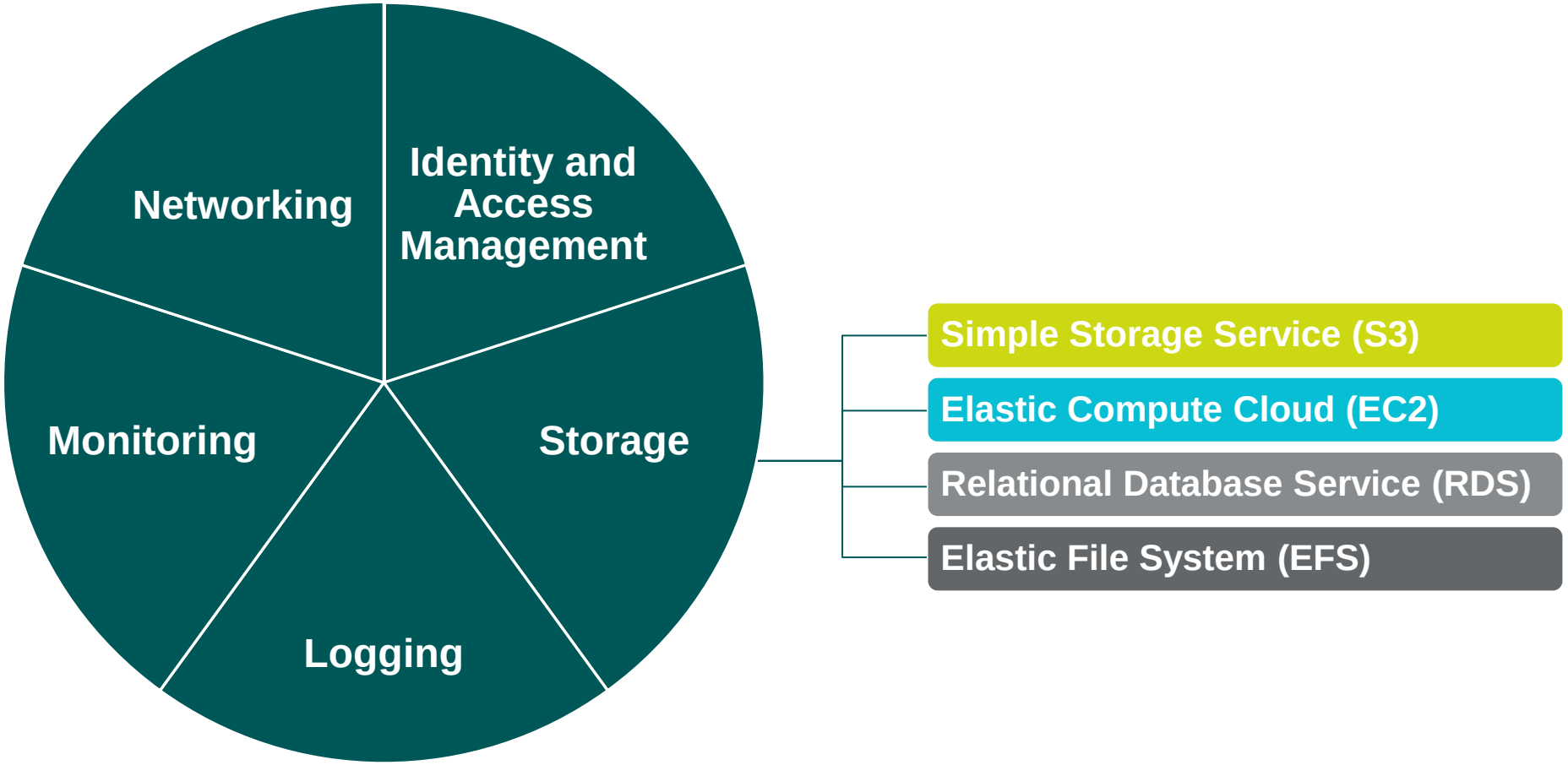
CIS Center for Internet Security®

CIS Benchmarks™

CIS Amazon Web Services Benchmarks (cisecurity.org)

v2.0.0 – 06-28-2023

Sekcje benchmarku CIS



5. Hands-on

https://github.com/IT-flavoured/AUGP_SMBFraudDefenseLabs

ACCT.01 – Set account-level contacts to valid email distribution lists

Hands-on:

- Ensure that your ***Root Account Email*** is valid to avoid losing access to your account
- Add ***Alternate Contacts*** so that your teams are accurately notified
- Add ***Security Challenge Questions***

CIS Amazon Web Services Foundation Benchmark:

- 1.1. Maintain current contact details (Manual)
- 1.2. Ensure security contact information is registered (Manual)
- 1.3. Ensure security questions are registered in the AWS account (Manual)

ACCT.02 – Restrict use of the root user

ACCT.05 – Require multi-factor authentication (MFA) to log in

ACCT.03 – Configure console access for each user

Dyskusja:

Break Glass Account in AWS

TD SYNNEX

Tasks that require root user credentials

- Change your account settings
- Restore IAM user permissions
- Activate IAM access to the Billing and Cost Management console
- View certain tax invoices
- Close your AWS account
- Register as a seller in the Reserved Instance Marketplace
- Configure an Amazon S3 bucket to enable MFA
- Edit or delete Amazon SQS resource policy that denies all principals
- Edit or delete Amazon S3 bucket policy that denies all principals
- Sign up for AWS GovCloud (US)
- Request AWS GovCloud (US) account root user access keys from AWS Support
- Recovery of AWS Key Management Service key in case of emergency (through AWS Support)

TD SYNNEX

ACCT.03 – Configure console access for each user

- IAM (standalone)
  - Users: long term credentials
  - Groups
  - Roles: short-term credentials, uses STS
    - EC2 instance Roles
    - Service Roles
    - Cross Account roles
  - Policies
    - AWS Managed
    - Customer Managed
    - Inline Policies
  - Resource Based Policies

- IAM Identity Center
  - One login (single sign-on) for all your:
    - AWS accounts in AWS Organizations
    - Business cloud applications
    - SAML 2.0-enabled applications
    - EC2 Windows Instances
  - Built-in identity store + 3rd party
  - Multi-Account Permissions
  - Application Assignments
  - Atribute-Based Access Control (ABAC)

TD SYNNEX

IAM Security Tools

- IAM Credentials Report (account-level)
  - A report that lists all your account's users and the status of their various credentials
- IAM Access Advisor (user-level)
  - Access advisor shows the service permissions granted to user and when those services were last accessed
  - You can use this information to revise your policies

TD SYNNEX

ACCT.04 – Assign permissions

- Link technology to the business – f.e. HR onboarding/offboarding process
- Manage permissions using groups
- Minimum privilege rule
- Blocking usage of AWS Regions
- Lock out the rarely used EC2 instance types:
  - GPU
  - CPU
  - AWS Nitro SSD Disks

Dyskusja:

W jaki sposób organizować strukturę użytkowników i grup?

ACCT.05 – Require multi-factor authentication (MFA) to log in

CIS Amazon Web Services Foundation Benchmark:

- 1.4 Ensure no 'root' user account access key exists (Automated)
- 1.5 Ensure MFA is enabled for the 'root' user account (Automated)
- 1.10 Ensure multi-factor authentication (MFA) is enabled for all IAM users that have a console password (Automated)
- 1.11 Do not setup access keys during initial user setup for all IAM users that have a console password (Manual)
- 1.13 Ensure there is only one active access key available for any single IAM user (Automated)
- 1.14 Ensure access keys are rotated every 90 days or less (Automated)

Dyskusja:

Ile kosztuje wdrożenie darmowego MFA?

ACCT.06 – Enforce a password policy

Dyskusja:

Aktualne trendy dotyczące polityki haseł.

CIS Amazon Web Services Foundation Benchmark:

- 1.8 Ensure IAM password policy requires minimum length of 14 or greater (Automated)
- 1.9 Ensure IAM password policy prevents password reuse (Automated)

TD SYNNEX

ACCT.07 – Deliver CloudTrail logs to a protected S3 bucket

CIS Amazon Web Services Foundation Benchmark:

- 3.1 Ensure CloudTrail is enabled in all regions (Automated)
- 3.2 Ensure CloudTrail log file validation is enabled (Automated)
- 3.4 Ensure CloudTrail trails are integrated with CloudWatch Logs (Automated)
- 3.7 Ensure CloudTrail logs are encrypted at rest using KMS CMKs (Automated)

ACCT.08 – Prevent public access to private S3 buckets

CIS Amazon Web Services Foundation Benchmark:

- 3.3 Ensure the S3 bucket used to store CloudTrail logs is not publicly accessible (Automated)
- 3.6 Ensure S3 bucket access logging is enabled on the CloudTrail S3 bucket (Automated)

Logging in AWS

- To help compliance requirements, AWS provides many service-specific security and audit logs
- Service Logs include:
  - CloudTrail trails – trace all API calls
  - Config Rules – for config & compliance over time
  - CloudWatch Logs – for full data retention
  - VPC Flow Logs – IP traffic within your VPC
  - ELB Access Log – metadata of requests made to your load balancers
  - CloudFront Logs – web distribution access logs
  - WAF Logs – full logging of all requests analyzed by the service
- Logs can be analyzed using AWS Athena if they’re stored in S3
- You should encrypt logs in S3, control access using IAM & Bucket Policies, MFA
- Move Logs to Glacier for cost savings

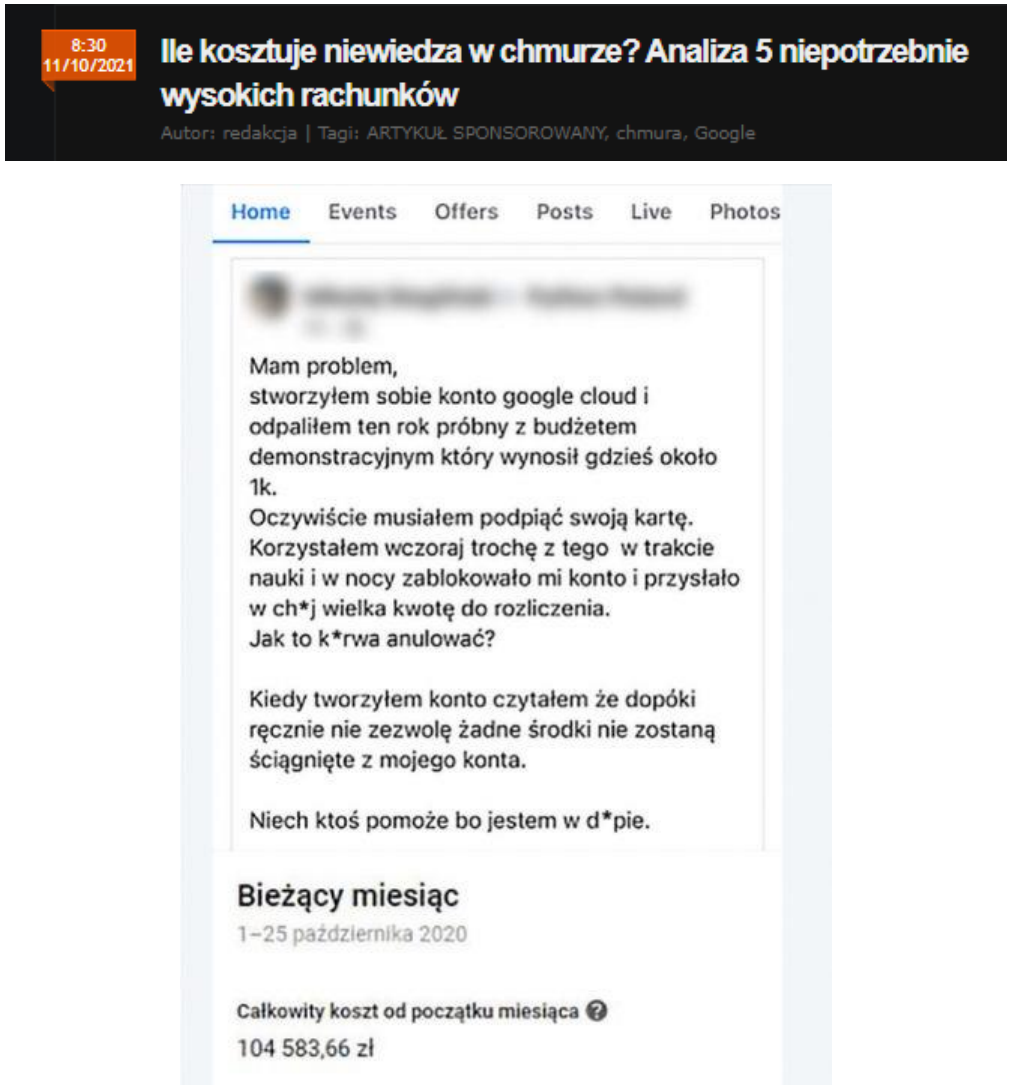
TD SYNNEX

ACCT.09 – Delete unused VPCs, subnets, and security groups

Dyskusja:

Ile kosztuje puste konto AWS?

ACCT.10 – Configure AWS Budgets to monitor your spending



ACCT.11 – Enable and respond to GuardDuty notifications

Amazon GuardDuty:

- Intelligent Threat discovery to protect your AWS Account
- Uses Machine Learning algorithms, anomaly detection, 3rd party data
- One click to enable (30 day trial), no need to install software
- Input data includes:
  - CloudTrail Events Logs – unusual API calls, unauthorized deployments
    - CloudTrail Management Event – create VPC subnet, create trail, …
    - CloudTrail S3 Data Events – get object, list object, delete object, …
  - VPC Flow Logs – unusual internal traffic, unusual IP address
  - DNS Logs – compromised EC2 instances sending encoded data within DNS queries
  - Optional Features – EKS Audit Logs, RDS & Aurora, EBS, Lambda, S3 Data Events…
- Can setup EventBridge rules to be notified in case of findings
- EventBridge rules can target AWS Lambda or SNS
- Can protect against CryptoCurrency attacks (has a dedicated “finding” for it)

ACCT.12 – Monitor for and resolve high-risk issues by using Trusted Advisor

AWS Trusted Advisor:

- No need to install anything – high level AWS account assessment
- Analyze your AWS accounts and provides recommendation on 5 categories:
  - **Cost optimization**
  - **Performance**
  - **Security**
  - **Fault tolerance**
  - **Service limits**

- Basic & Developer Support plan: 7 core checks
- Business & Enterprise Support plan: Full Checks

6. AWS Security Services

Honorable mentions

Single slide: AWS Shield

- AWS Shield Standard:
  - Free service that is activated for every AWS customer
  - Provides protection from attacks such as SYN/UDP Floods, Reflection attacks and other L3/L4 attacks

- AWS Shield Advanced:
  - Optional DDoS mitigation services ($3000 per month per organization)
  - Protect against more sophisticated attacks on Amazon EC2, Elastic Load Balancing (ELB), Amazon CloudFront, AWS Global Accelerator, and Route 53
  - 24/7 access to AWS DDoS response team (DRP
  - Protect against higher fees during usage spikes due to DDoS

Single slide: AWS Web Application Firewall

- Protects your web application from common web exploits (L7)
- Deploy on Application Load Balancer, API Gateway, CloudFront
- Define Web ACL (Web Access Control List):
  - Rules can include IP addresses, HTTP headers, HTTP body, or URI strings
  - Protects from common attack – SQL injection and Cross-Site Scripting (XSS)
  - Size constraints, geo-match (block countries)
  - Rate-based rules (to count occurrences of events) – for DDoS protection

TD SYNNEX

Single slide: Amazon Inspector

- Automated Security Assessments
- For EC2 instances
  - Leveraging the AWS System Manager (SSM) agent
  - Analyze against unintended network accessibility
  - Analyze the running OS against known vulnerabilities
- For Container Images push to Amazon ECR
  - Assessment of Container Images as they are pushed
- For Lambda Functions
  - Identifies software vulnerabilities in function code and package dependencies
  - Assessment of functions as thy are deployed
- Reporting & integration with AWS Security Hub
- Send findings to Amazon Event Bridge

7. Ankieta

TD SYNNEX

Ocena szkolenia - "Warsztat AWS - SMB Fraud Defense"

TD SYNNEX

Skontaktuj się z polskim zespołem AWS w TD SYNNEX!

pl-aws@tdsynnex.com

Date	Author	Version
23.09.2023	Piotr Blonkowski	2.0