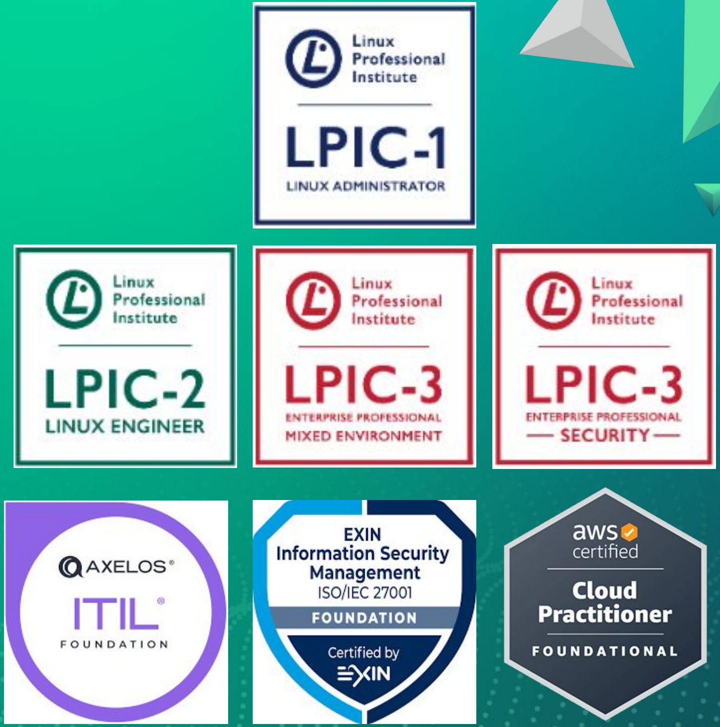
mind the sec /2023

Técnicas de prevenção de ataques e resposta a incidentes em ambientes AWS

mind the sec /2023

Profile

- 24 anos na gestão de times de TI e Segurança da Informação
- Graduação em Ciência da computação com especialização redes e Cloud
- MBA Gestão estratégica de TI pela FGV



mind the sec /2023

Agenda

- Introdução
- Modelo de responsabilidade compartilhada
- Estatísticas de ameaças
- Estudos de caso
  - Medidas de prevenção
  - Respostas a incidentes
- Conclusão

mind the sec /2023

Infraestrutura global

- 245 países
- 32 regiões
- 102 AZs
- +300 serviços

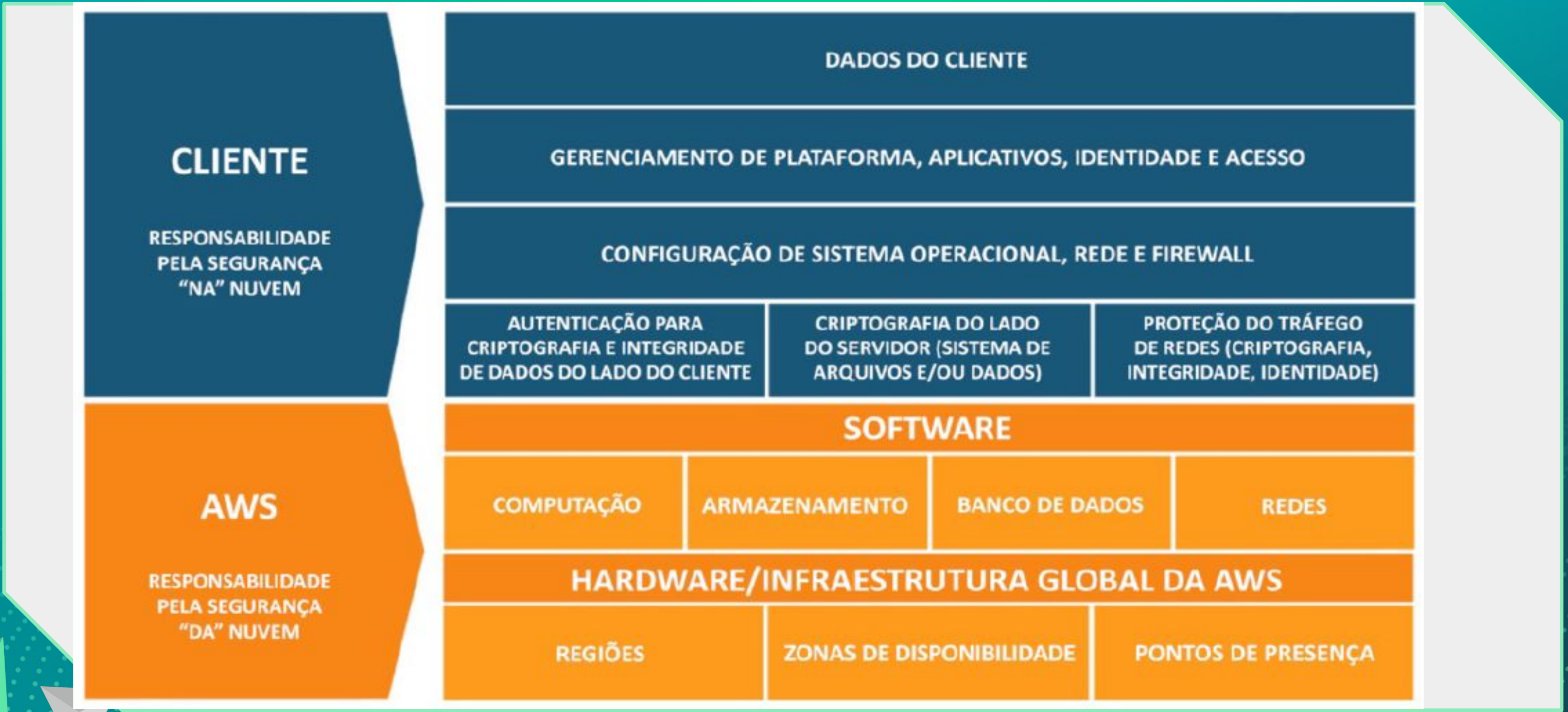
Introdução

- Fornecedores despreparados
- Treinamentos sem foco em segurança
    - Não façam isso em casa!!
- Grande poder computacional em mãos inábeis
    - Prejuízos exponenciais

mind the sec /2023

Modelo de responsabilidade compartilhada

Modelo de Responsabilidade compartilhada



CLIENTE

RESPONSABILIDADE PELA SEGURANÇA "NA" NUVEM

DADOS DO CLIENTE

GERENCIAMENTO DE PLATAFORMA, APLICATIVOS, IDENTIDADE E ACESSO

CONFIGURAÇÃO DE SISTEMA OPERACIONAL, REDE E FIREWALL

AUTENTICAÇÃO PARA CRIPTOGRAFIA E INTEGRIDADE DE DADOS DO LADO DO CLIENTE	CRIPTOGRAFIA DO LADO DO SERVIDOR (SISTEMA DE ARQUIVOS E/OU DADOS)	PROTEÇÃO DO TRÁFEGO DE REDES (CRIPTOGRAFIA, INTEGRIDADE, IDENTIDADE)

AWS

RESPONSABILIDADE PELA SEGURANÇA "DA" NUVEM

SOFTWARE

COMPUTAÇÃO	ARMAZENAMENTO	BANCO DE DADOS	REDES

HARDWARE/INFRAESTRUTURA GLOBAL DA AWS

REGIÕES	ZONAS DE DISPONIBILIDADE	PONTOS DE PRESENÇA

mind the sec /2023

Estatísticas de ameaças

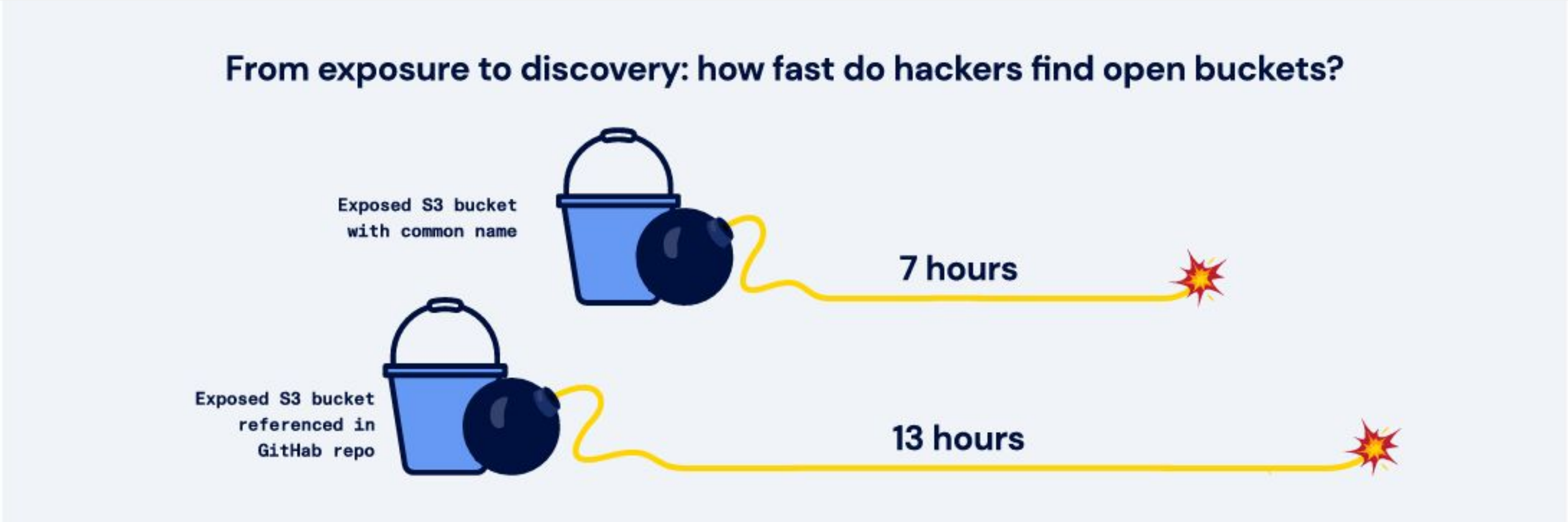
mind the sec /2023

Ameaças

- AWS sofre um quatrilhão de ataques por mês
- 84,1% concedem acessos privilegiados de IAM em imposição de MFA
- 68% contas de terceiros tem acessos administrativos
- 59,4% não aplicam controles básicos de segurança
- 36% das organizações possuem pelo menos um bucket público
  - Um bucket público leva em média de 7 a 13 horas ser acessado por hackers
- 17,4% executam workloads com vulnerabilidades expostos a Internet

Fonte: AWS, Zcaler, DataDog, Wiz

Estatísticas



From exposure to discovery: how fast do hackers find open buckets?

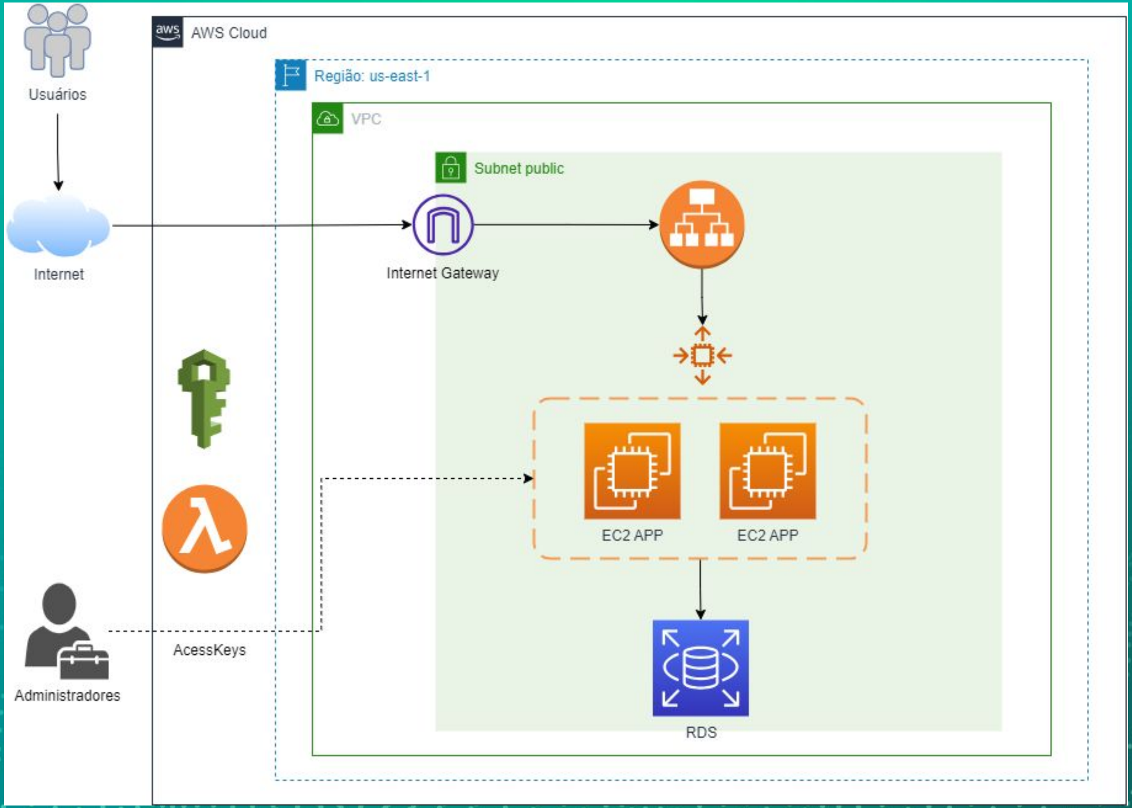
mind the sec /2023

Estudos de caso

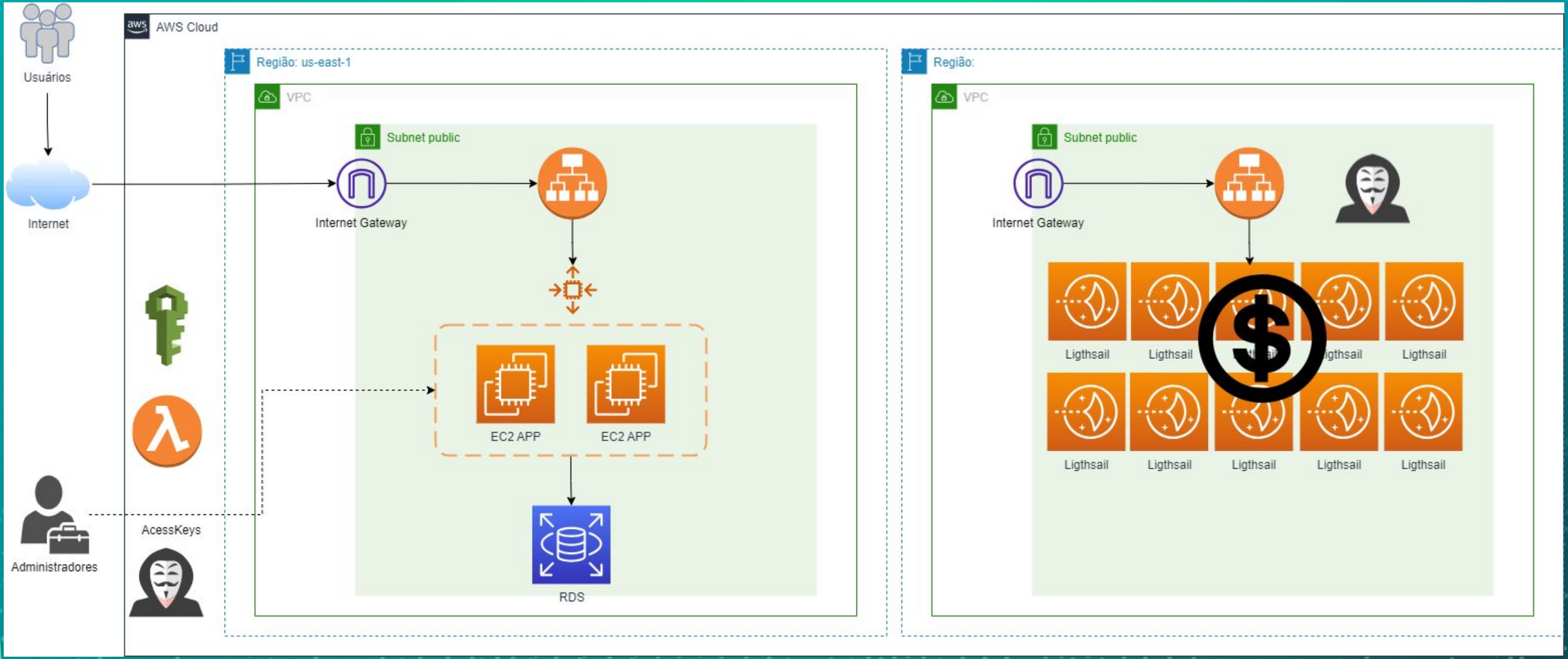
mind the sec /2023

Invasão da Startup

Invasão da Startup



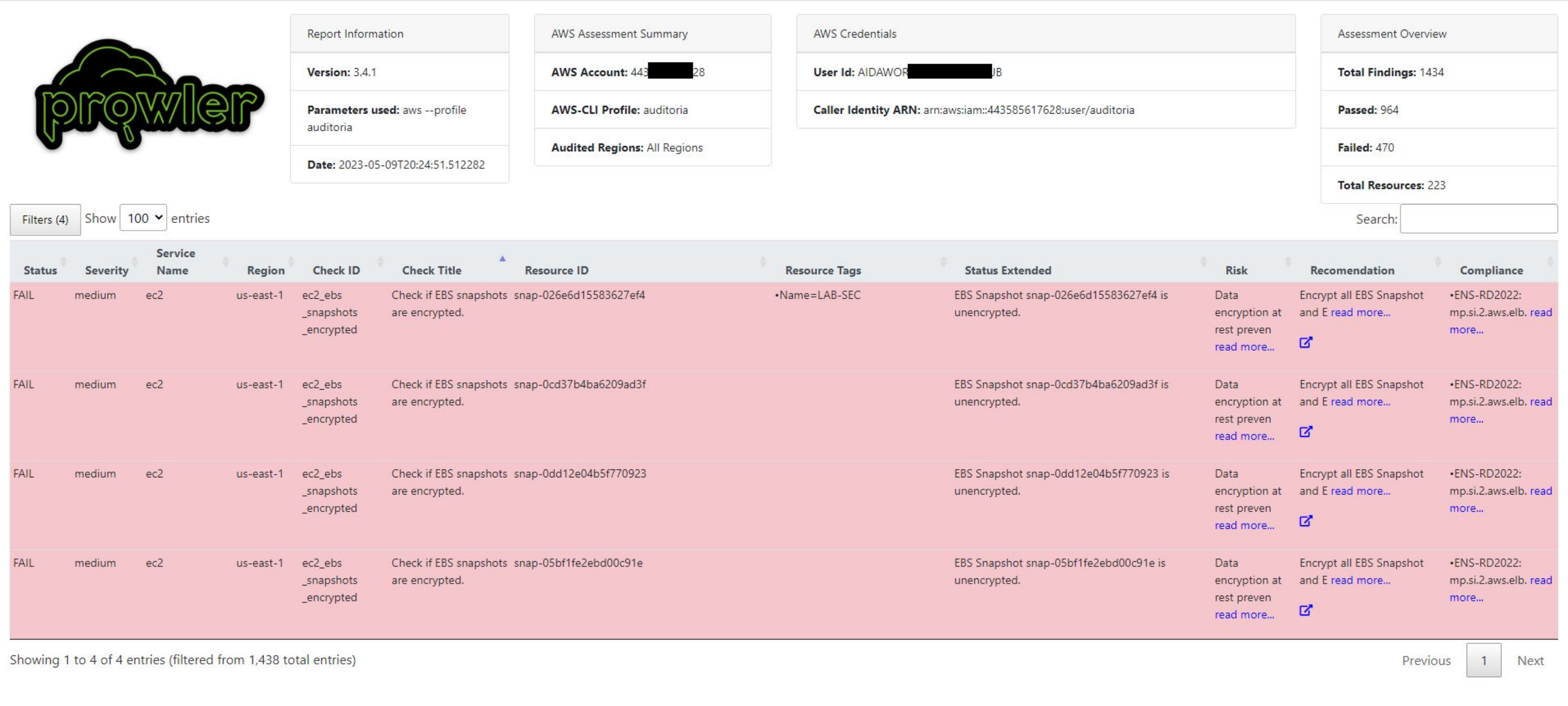
Invasão da Startup



Resposta a incidente

- Identificar
- Conter
- Coletar evidências
- Restaurar/Reparar
- Aplicar ajustes

Identificar origem



Report Information
Version: 3.4.1
Parameters used: aws --profile auditoria
Date: 2023-05-09T20:24:51.512282

AWS Assessment Summary
AWS Account: 443[redacted]28
AWS-CLI Profile: auditoria
Audited Regions: All Regions

AWS Credentials
User Id: AIDAWOR[redacted]B
Caller Identity ARN: arn:aws:iam::443585617628:user/auditoria

Assessment Overview
Total Findings: 1434
Passed: 964
Failed: 470
Total Resources: 223

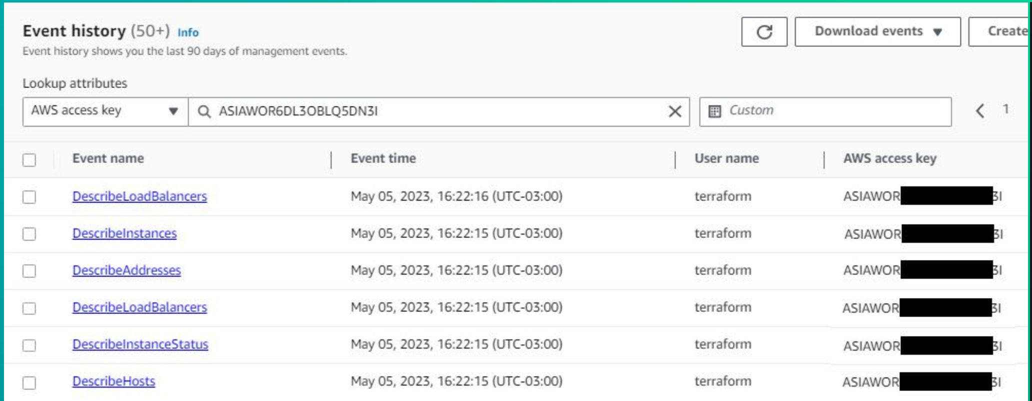
Filters (4) Show 100 entries Search:

Status	Severity	Service Name	Region	Check ID	Check Title	Resource ID	Resource Tags	Status Extended	Risk	Recomendation	Compliance
FAIL	medium	ec2	us-east-1	ec2_ebs_snapshots_encrypted	Check if EBS snapshots are encrypted.	snap-026e6d15583627ef4	•Name=LAB-SEC	EBS Snapshot snap-026e6d15583627ef4 is unencrypted.	Data encryption at rest preven read more...	Encrypt all EBS Snapshot and E read more...	•ENS-RD2022: mp.si.2.aws.elb. read more...
FAIL	medium	ec2	us-east-1	ec2_ebs_snapshots_encrypted	Check if EBS snapshots are encrypted.	snap-0cd37b4ba6209ad3f		EBS Snapshot snap-0cd37b4ba6209ad3f is unencrypted.	Data encryption at rest preven read more...	Encrypt all EBS Snapshot and E read more...	•ENS-RD2022: mp.si.2.aws.elb. read more...
FAIL	medium	ec2	us-east-1	ec2_ebs_snapshots_encrypted	Check if EBS snapshots are encrypted.	snap-0dd12e04b5f770923		EBS Snapshot snap-0dd12e04b5f770923 is unencrypted.	Data encryption at rest preven read more...	Encrypt all EBS Snapshot and E read more...	•ENS-RD2022: mp.si.2.aws.elb. read more...
FAIL	medium	ec2	us-east-1	ec2_ebs_snapshots_encrypted	Check if EBS snapshots are encrypted.	snap-05bf1fe2ebd00c91e		EBS Snapshot snap-05bf1fe2ebd00c91e is unencrypted.	Data encryption at rest preven read more...	Encrypt all EBS Snapshot and E read more...	•ENS-RD2022: mp.si.2.aws.elb. read more...

Showing 1 to 4 of 4 entries (filtered from 1,438 total entries)

mind the sec /2023

Identificar origem



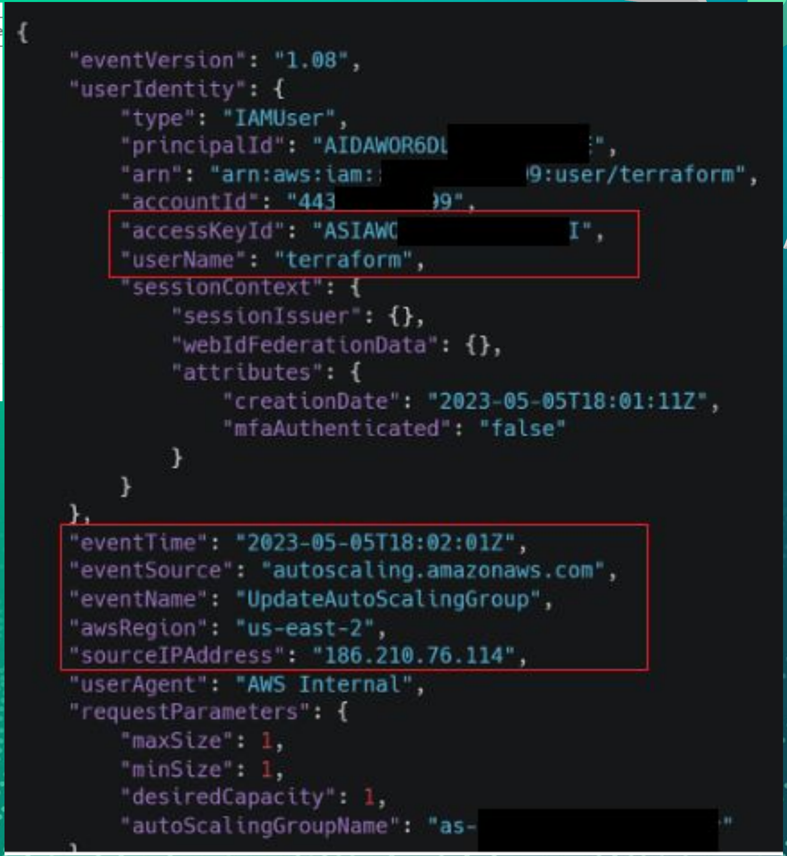
Event history (50+) Info

Event history shows you the last 90 days of management events.

Lookup attributes

AWS access key ▼ | ASIAWOR6DL3OBLQ5DN3I ✕ | Custom | ‹ 1

□	Event name	Event time	User name	AWS access key
□	DescribeLoadBalancers	May 05, 2023, 16:22:16 (UTC-03:00)	terraform	ASIAWOR[redacted]3I
□	DescribeInstances	May 05, 2023, 16:22:15 (UTC-03:00)	terraform	ASIAWOR[redacted]3I
□	DescribeAddresses	May 05, 2023, 16:22:15 (UTC-03:00)	terraform	ASIAWOR[redacted]3I
□	DescribeLoadBalancers	May 05, 2023, 16:22:15 (UTC-03:00)	terraform	ASIAWOR[redacted]3I
□	DescribeInstanceStatus	May 05, 2023, 16:22:15 (UTC-03:00)	terraform	ASIAWOR[redacted]3I
□	DescribeHosts	May 05, 2023, 16:22:15 (UTC-03:00)	terraform	ASIAWOR[redacted]3I



```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAWOR6DL[redacted]",
        "arn": "arn:aws:iam:[redacted]9:user/terraform",
        "accountId": "443[redacted]99",
        "accessKeyId": "ASIAW[redacted]I",
        "userName": "terraform",
        "sessionContext": {
            "sessionIssuer": {},
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-05-05T18:01:11Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-05-05T18:02:01Z",
    "eventSource": "autoscaling.amazonaws.com",
    "eventName": "UpdateAutoScalingGroup",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "186.210.76.114",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "maxSize": 1,
        "minSize": 1,
        "desiredCapacity": 1,
        "autoScalingGroupName": "as-[redacted]"
```

mind the sec /2023

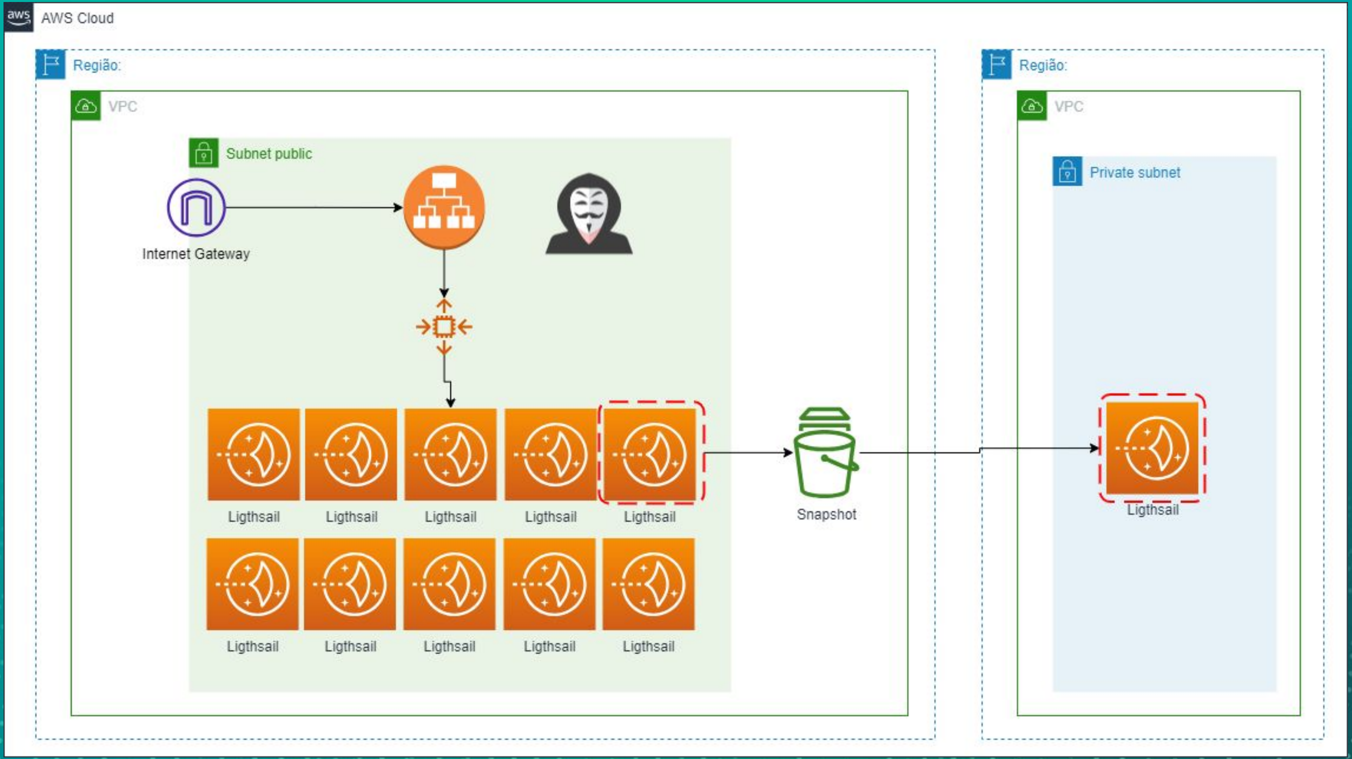
Contenção

- Bloquear acesso de todas AccessKey em uso
  - Ativar *condictions* para restringir o acesso (IP de origem)
  - Realizar rotacionamento gradativo após os devidos ajustes
- Alterar a senha de todos os usuários ativos
  - Ativar MFA
- Gerar novo par de chaves de acesso
- Desativar scripts Lambda

Coletar evidências

- Gerar cópia do histórico do CloudTrail em um bucket protegido
- Preservar instância

Coletar evidências



Reparar/Restaurar

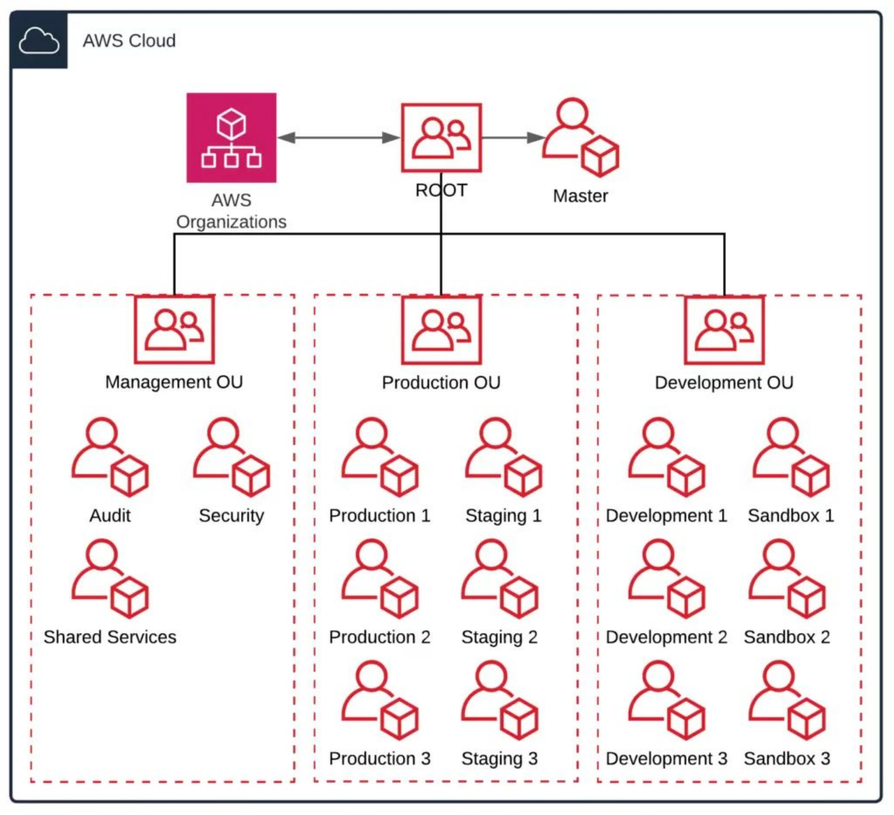
- Excluir/desativar recursos e serviços utilizados pelo atacante
- Restaurar AMIs íntegras
- Restaurar cópias de segurança:
  - Aplicações
  - Bases de dados
- Realizar monitoramento e auditoria do ambiente

mind the sec /2023

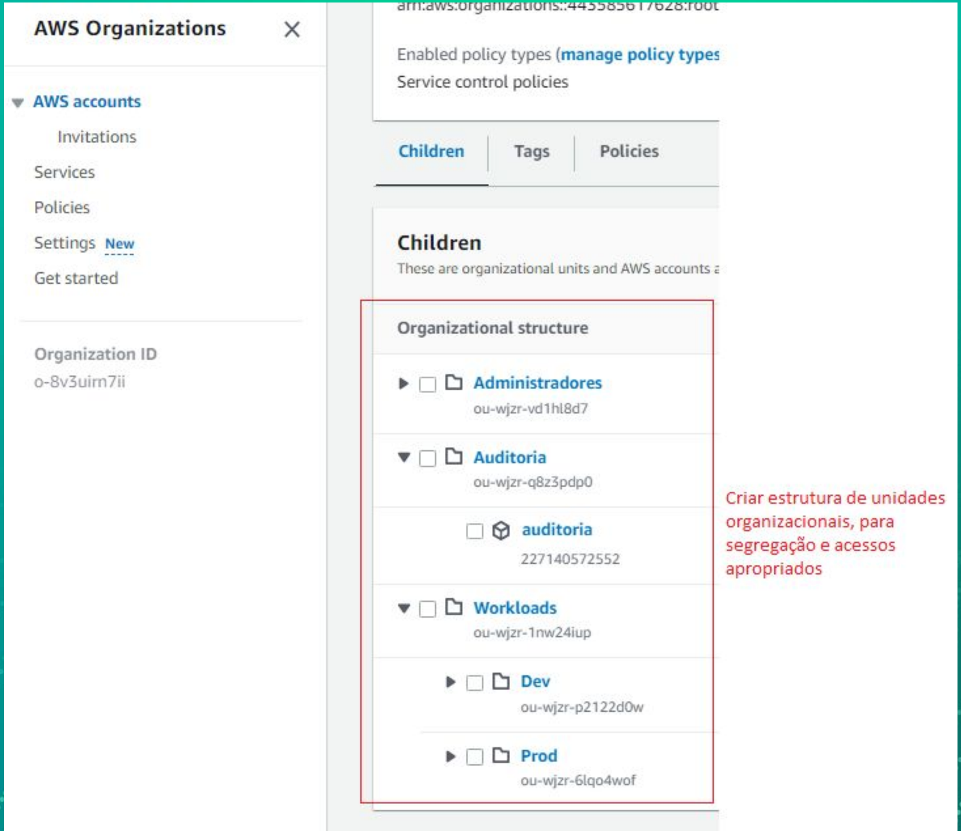
Aplicar ajustes

- Analisar evidências coletadas
- Desativar contas não utilizadas
  - Excluir AccessKeys
- Princípio de privilégio mínimo
- Utilizar Roles (devidamente parametrizadas) ao invés de AccessKey

Aplicar ajustes



Aplicar ajustes



AWS Organizations ✕

- AWS accounts
  - Invitations
- Services
- Policies
- Settings New
- Get started

Organization ID
o-8v3uirn7ii

arn:aws:organizations::443585617628:root

Enabled policy types (manage policy types
Service control policies

Children

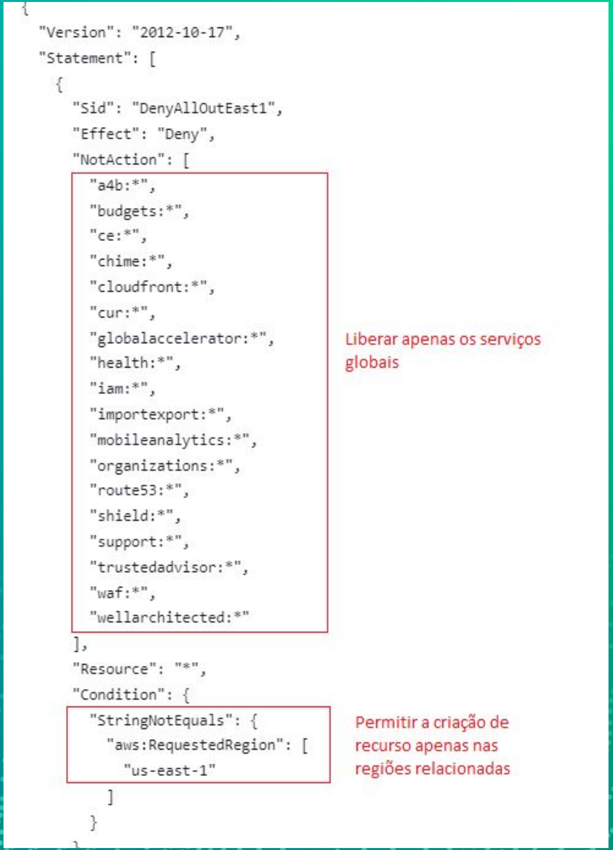
These are organizational units and AWS accounts a

Organizational structure

- ▶ □ Administradores ou-wjzr-vd1hl8d7
- ▼ □ Auditoria ou-wjzr-q8z3pdp0
  - □ auditoria 227140572552
- ▼ □ Workloads ou-wjzr-1nw24iup
  - ▶ □ Dev ou-wjzr-p2122d0w
  - ▶ □ Prod ou-wjzr-6lqo4wof

Criar estrutura de unidades organizacionais, para segregação e acessos apropriados

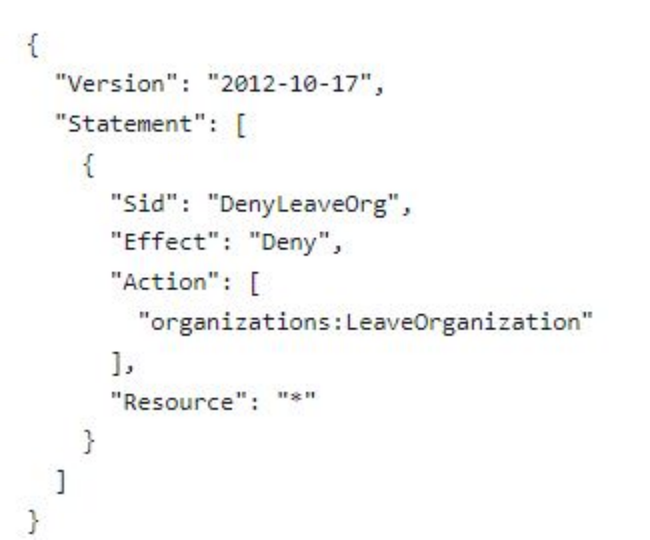
Aplicar ajustes



```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyAllOutEast1",
      "Effect": "Deny",
      "NotAction": [
        "a4b:*",
        "budgets:*",
        "ce:*",
        "chime:*",
        "cloudfront:*",
        "cur:*",
        "globalaccelerator:*",
        "health:*",
        "iam:*",
        "importexport:*",
        "mobileanalytics:*",
        "organizations:*",
        "route53:*",
        "shield:*",
        "support:*",
        "trustedadvisor:*",
        "waf:*",
        "wellarchitected:*"
      ],
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:RequestedRegion": [
            "us-east-1"
          ]
        }
      }
```

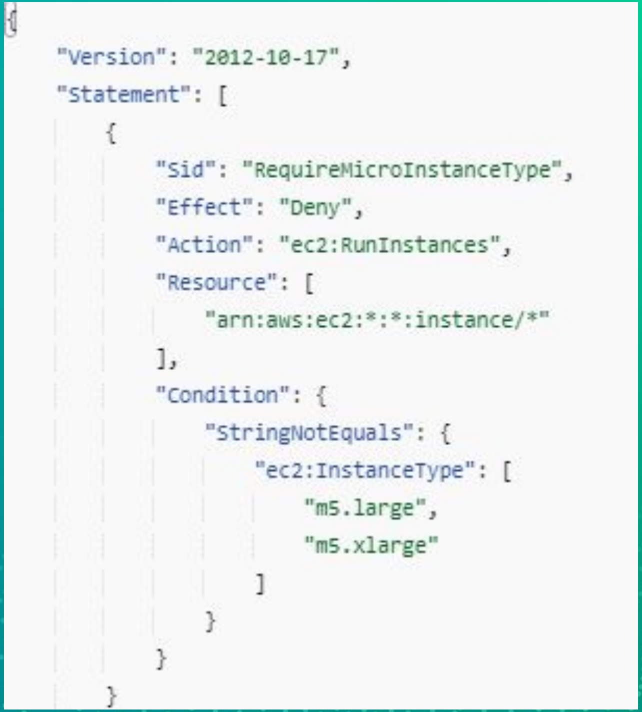
Liberar apenas os serviços globais

Permitir a criação de recurso apenas nas regiões relacionadas

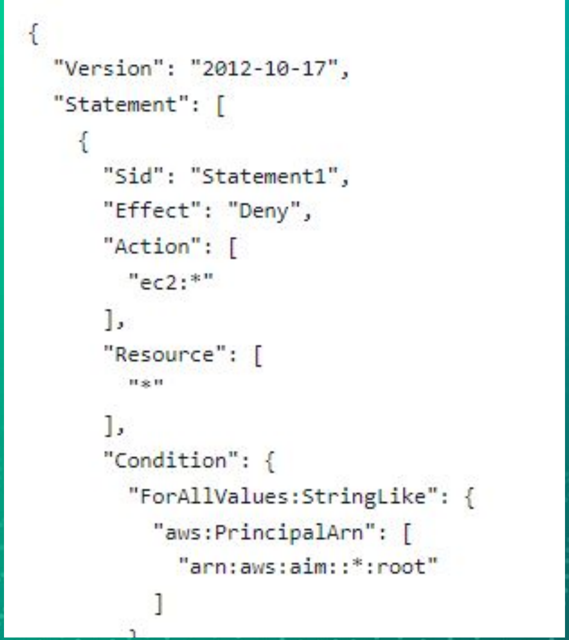


```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyLeaveOrg",
      "Effect": "Deny",
      "Action": [
        "organizations:LeaveOrganization"
      ],
      "Resource": "*"
    }
  ]
}
```

Aplicar ajustes

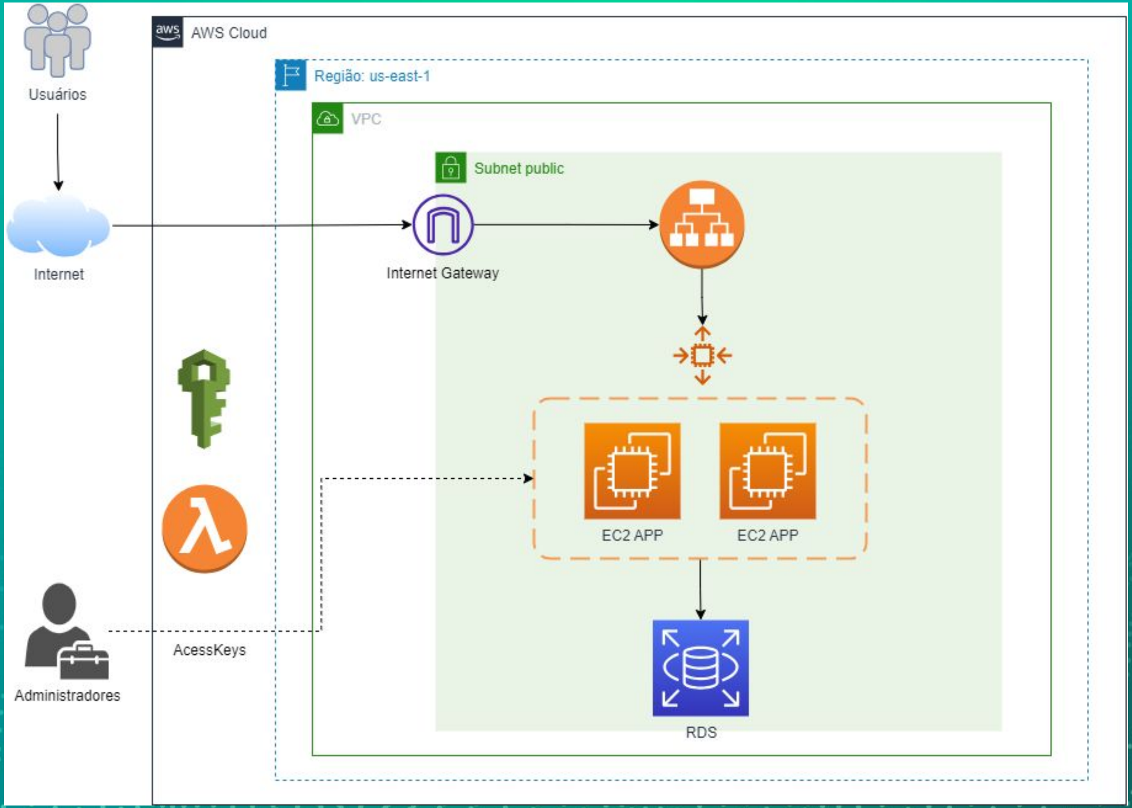


```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "RequireMicroInstanceType",
            "Effect": "Deny",
            "Action": "ec2:RunInstances",
            "Resource": [
                "arn:aws:ec2:*:*:instance/*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ec2:InstanceType": [
                        "m5.large",
                        "m5.xlarge"
                    ]
                }
            }
        }
```

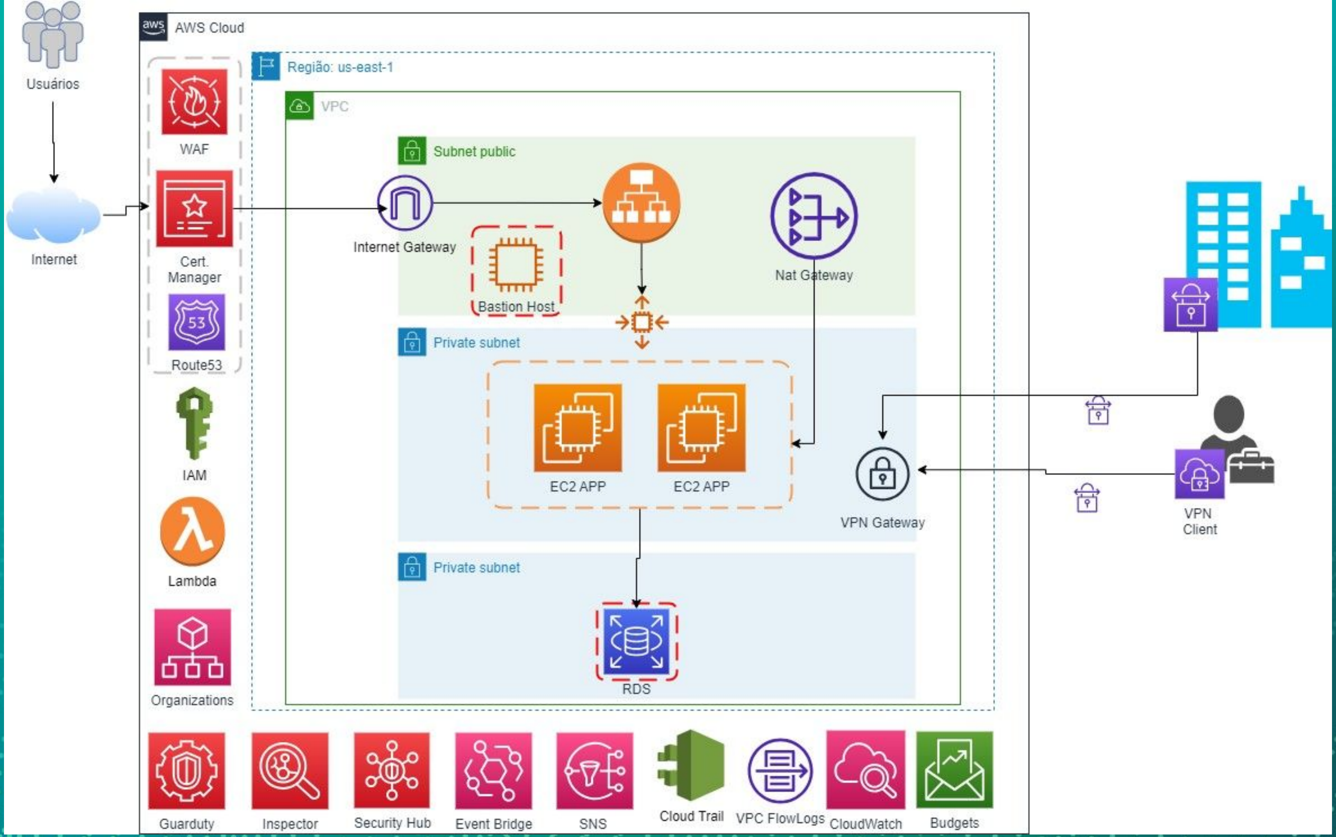


```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Statement1",
      "Effect": "Deny",
      "Action": [
        "ec2:*"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "ForAllValues:StringLike": {
          "aws:PrincipalArn": [
            "arn:aws:aim::*:root"
          ]
```

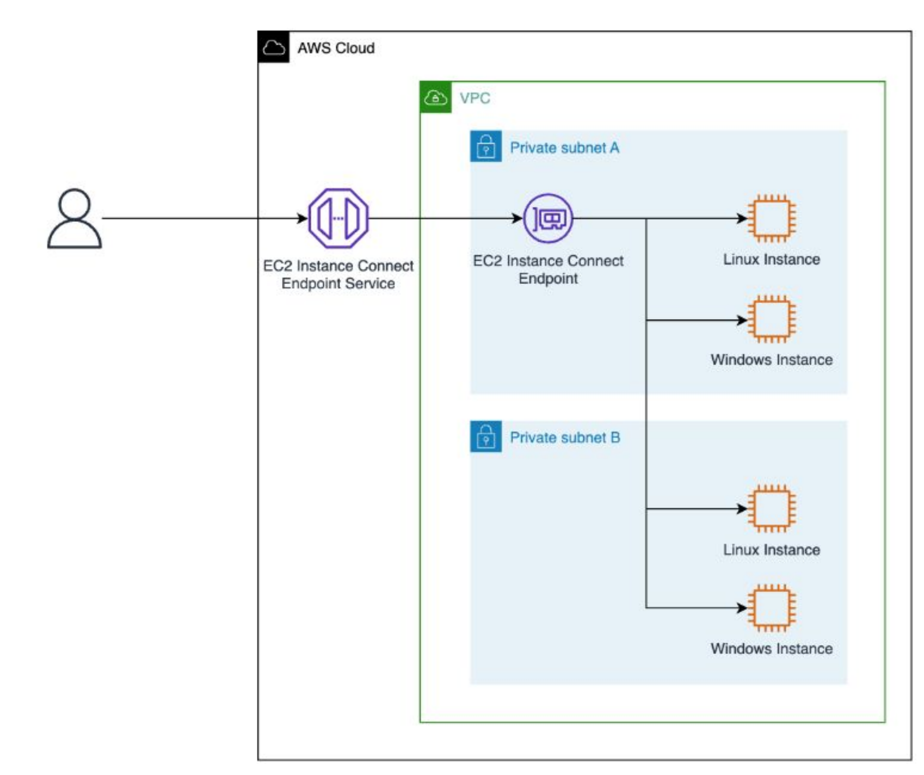
Aplicar ajustes



Aplicar ajustes



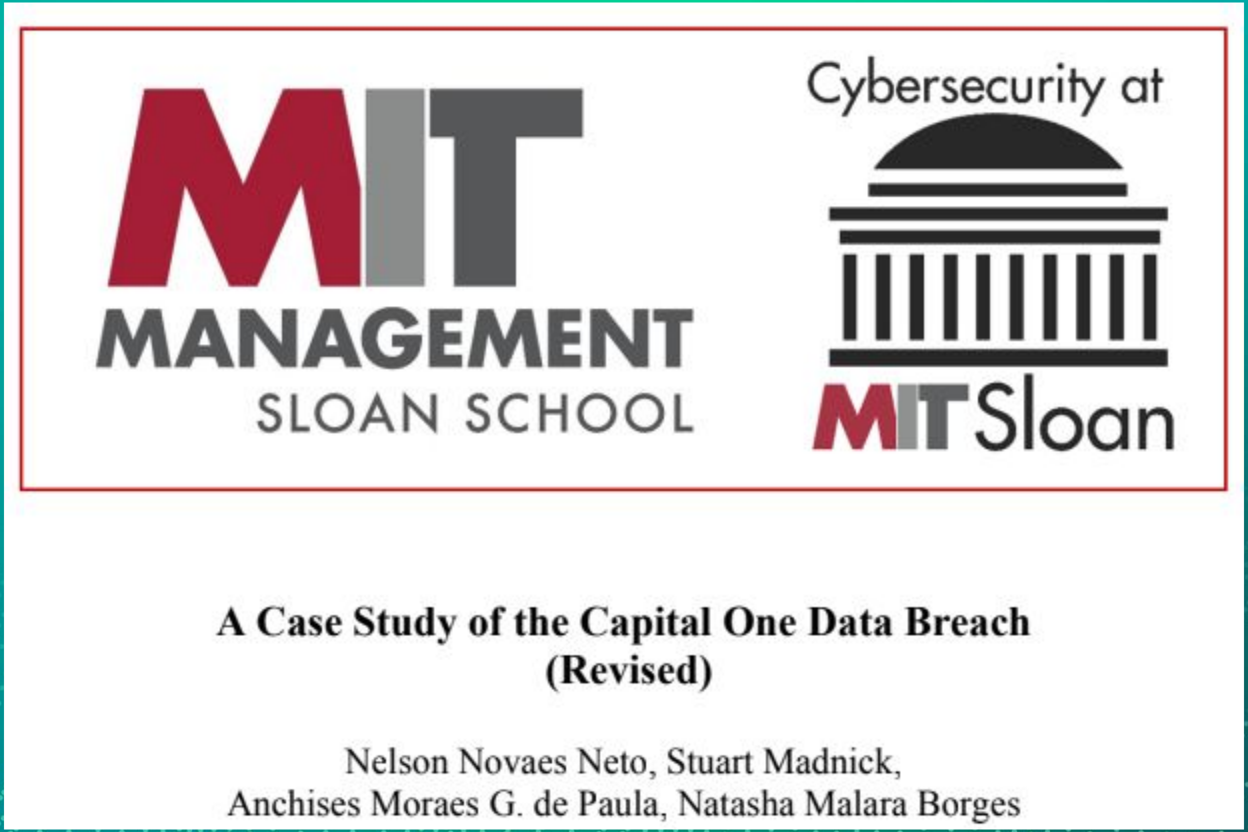
Aplicar ajustes



mind the sec /2023

Roubo de dados CapitalOne

Roubo de dados CapitalOne



MIT MANAGEMENT SLOAN SCHOOL

Cybersecurity at MIT Sloan

A Case Study of the Capital One Data Breach (Revised)

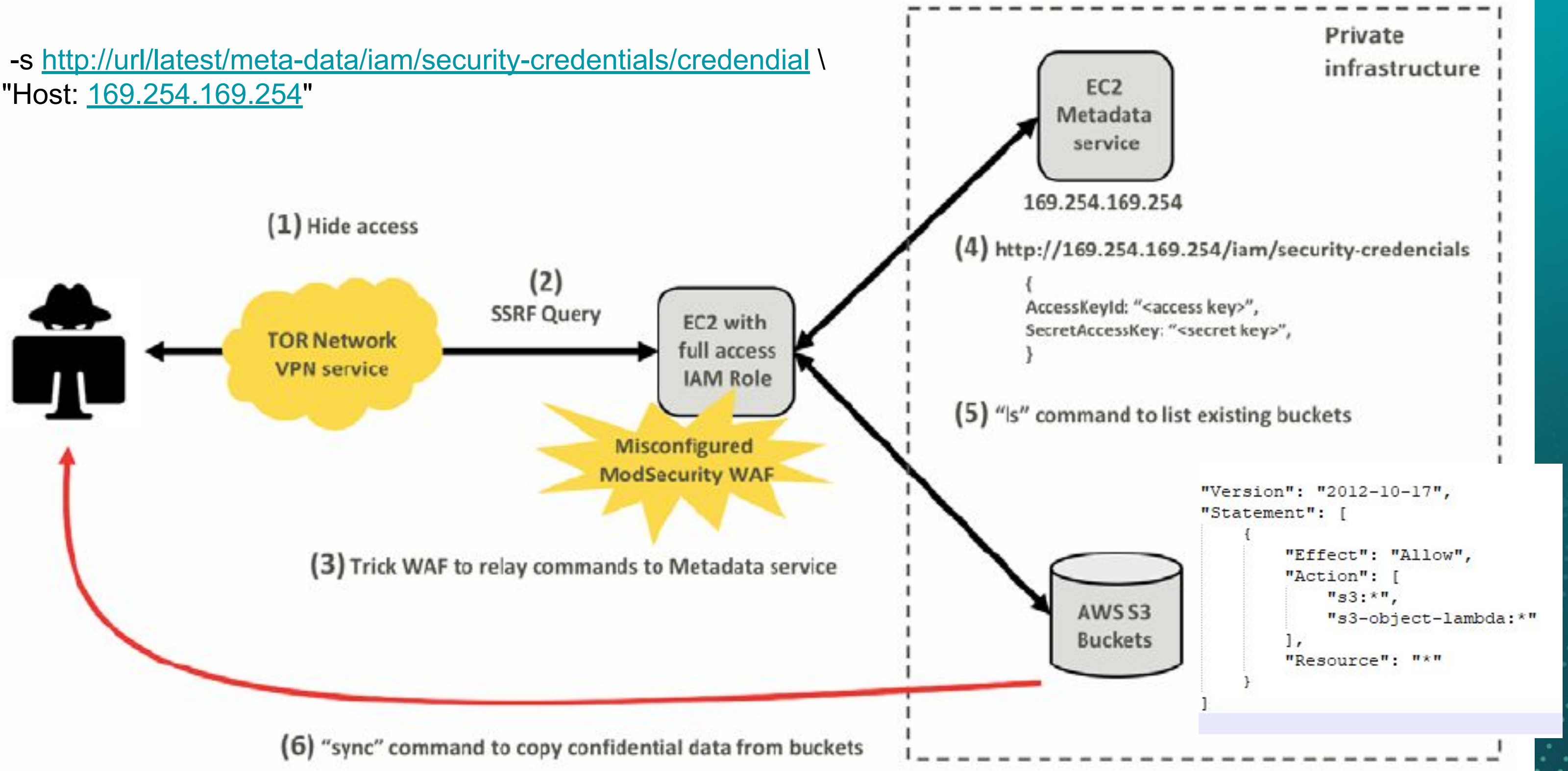
Nelson Novaes Neto, Stuart Madnick,
Anchises Moraes G. de Paula, Natasha Malara Borges

Roubo de dados CapitalOne

- 5º maior banco dos EUA
  - 50.000 colaboradores
  - 85% da equipe de TI formada por engenheiros
- Um dos primeiros bancos a migrar sua infraestrutura para cloud
  - Segmento altamente regulado
  - Balizamento de risco equivalente ao on-premise antes da migração para cloud

Roubo de dados CapitalOne

```
curl -s http://url/latest/meta-data/iam/security-credentials/credendial \
 -H "Host: 169.254.169.254"
```

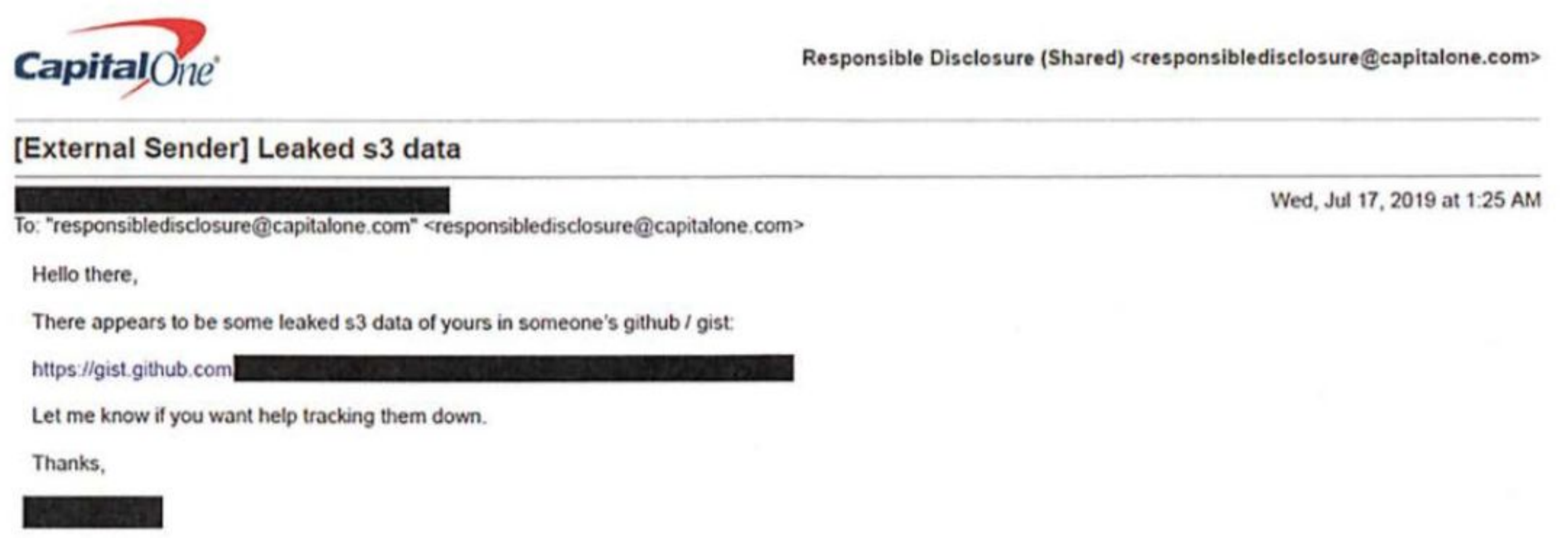

(1) Hide access
TOR Network VPN service
(2) SSRF Query
EC2 with full access IAM Role
Misconfigured ModSecurity WAF
(3) Trick WAF to relay commands to Metadata service
Private infrastructure
EC2 Metadata service
169.254.169.254
(4) http://169.254.169.254/iam/security-credencials
{
AccessKeyId: "<access key>",
SecretAccessKey: "<secret key>",
}
(5) "ls" command to list existing buckets
AWS S3 Buckets
(6) "sync" command to copy confidential data from buckets

```
"Version": "2012-10-17",
"Statement": [
    {
        "Effect": "Allow",
        "Action": [
            "s3:*",
            "s3-object-lambda:*"
        ],
        "Resource": "*"
    }
]
```

Roubo de dados CapitalOne

- Incidente: 22 e 23/03/2019
  - 30 GB de dados de 700 buckets
  - 106 milhões de clientes
    - 100 milhões EUA
    - 6 milhões Canadá
- Nenhum dos sistemas de segurança da organização identificou o ataque

Roubo de dados CapitalOne



Capital One

Responsible Disclosure (Shared) <responsibledisclosure@capitalone.com>

[External Sender] Leaked s3 data

[redacted] Wed, Jul 17, 2019 at 1:25 AM

To: "responsibledisclosure@capitalone.com" <responsibledisclosure@capitalone.com>

Hello there,

There appears to be some leaked s3 data of yours in someone's github / gist:

https://gist.github.com[redacted]

Let me know if you want help tracking them down.

Thanks,

[redacted]

Roubo de dados CapitalOne

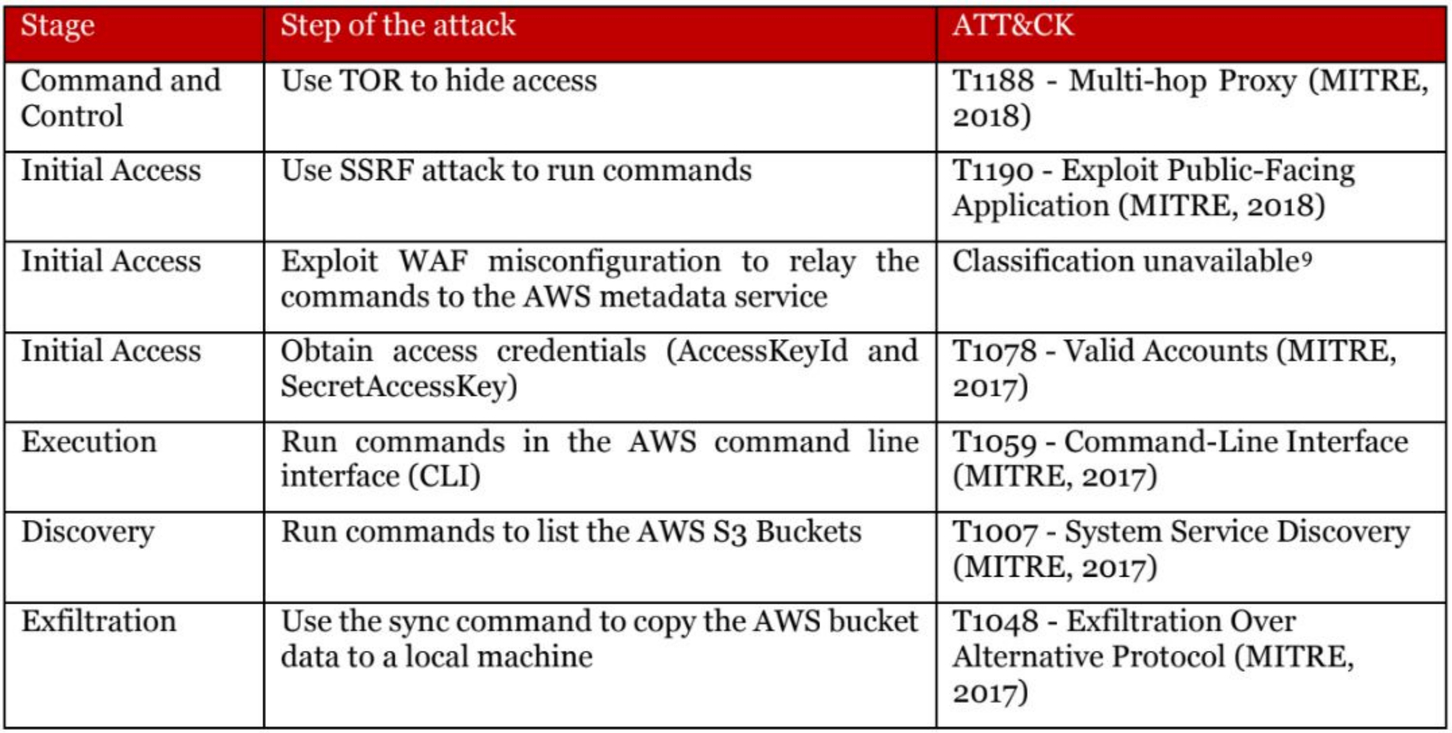
- **Paige Thompson**
  - Ex-colaboradora da AWS
  - Mais de 30 empresas foram afetadas:
    - Agências de governo
    - Grupos de telecomunicações
    - Universidades

mind the sec /2023

Roubo de dados CapitalOne

- **Principais causas do incidente**
  - Falha de configuração do firewall
    - Bloquear tráfego de redes anônimas
    - Ativar regras de proteção contra SSRF
  - Escalação de privilégios
    - Restringir acesso apenas ao bucket necessário
    - Impedir acesso de IPs externos
  - Exfiltração de dados
    - Bloquear tráfego de saída não autorizado
    - Monitorar tráfego de saída de ambiente AWS
    - Utilização de DLP (Data Leak Prevention)

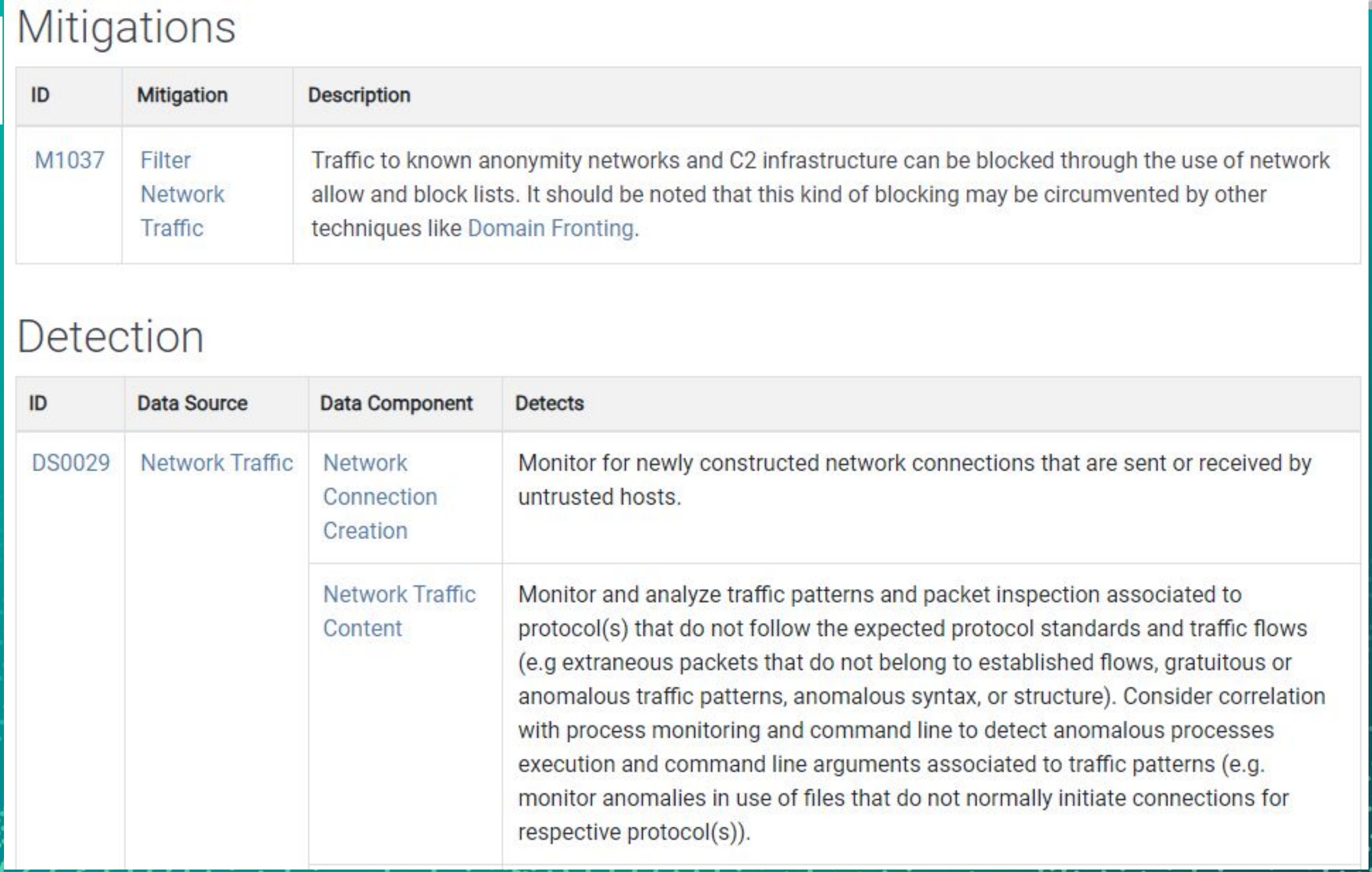
Roubo de dados CapitalOne



Stage	Step of the attack	ATT&CK
Command and Control	Use TOR to hide access	T1188 - Multi-hop Proxy (MITRE, 2018)
Initial Access	Use SSRF attack to run commands	T1190 - Exploit Public-Facing Application (MITRE, 2018)
Initial Access	Exploit WAF misconfiguration to relay the commands to the AWS metadata service	Classification unavailable[9]
Initial Access	Obtain access credentials (AccessKeyId and SecretAccessKey)	T1078 - Valid Accounts (MITRE, 2017)
Execution	Run commands in the AWS command line interface (CLI)	T1059 - Command-Line Interface (MITRE, 2017)
Discovery	Run commands to list the AWS S3 Buckets	T1007 - System Service Discovery (MITRE, 2017)
Exfiltration	Use the sync command to copy the AWS bucket data to a local machine	T1048 - Exfiltration Over Alternative Protocol (MITRE, 2017)

Roubo de dados CapitalOne

T1090.3
Multi-hop Proxy



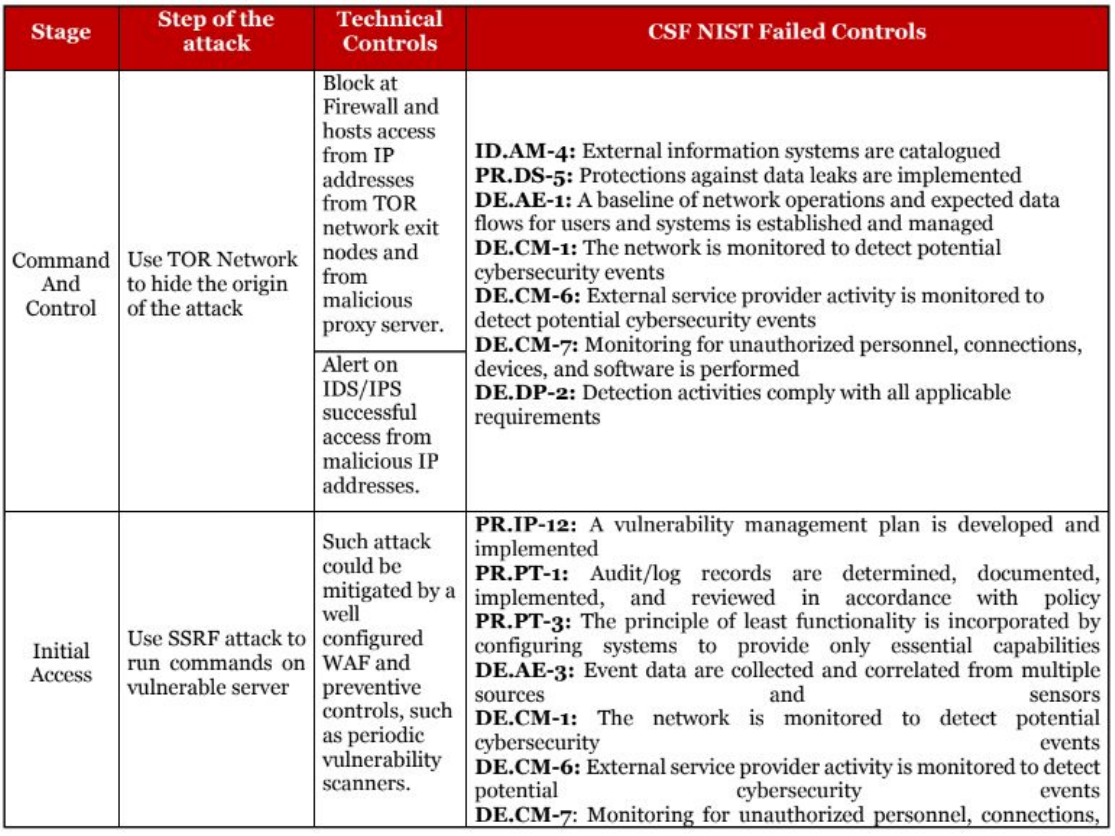
Mitigations

ID	Mitigation	Description
M1037	Filter Network Traffic	Traffic to known anonymity networks and C2 infrastructure can be blocked through the use of network allow and block lists. It should be noted that this kind of blocking may be circumvented by other techniques like Domain Fronting.

Detection

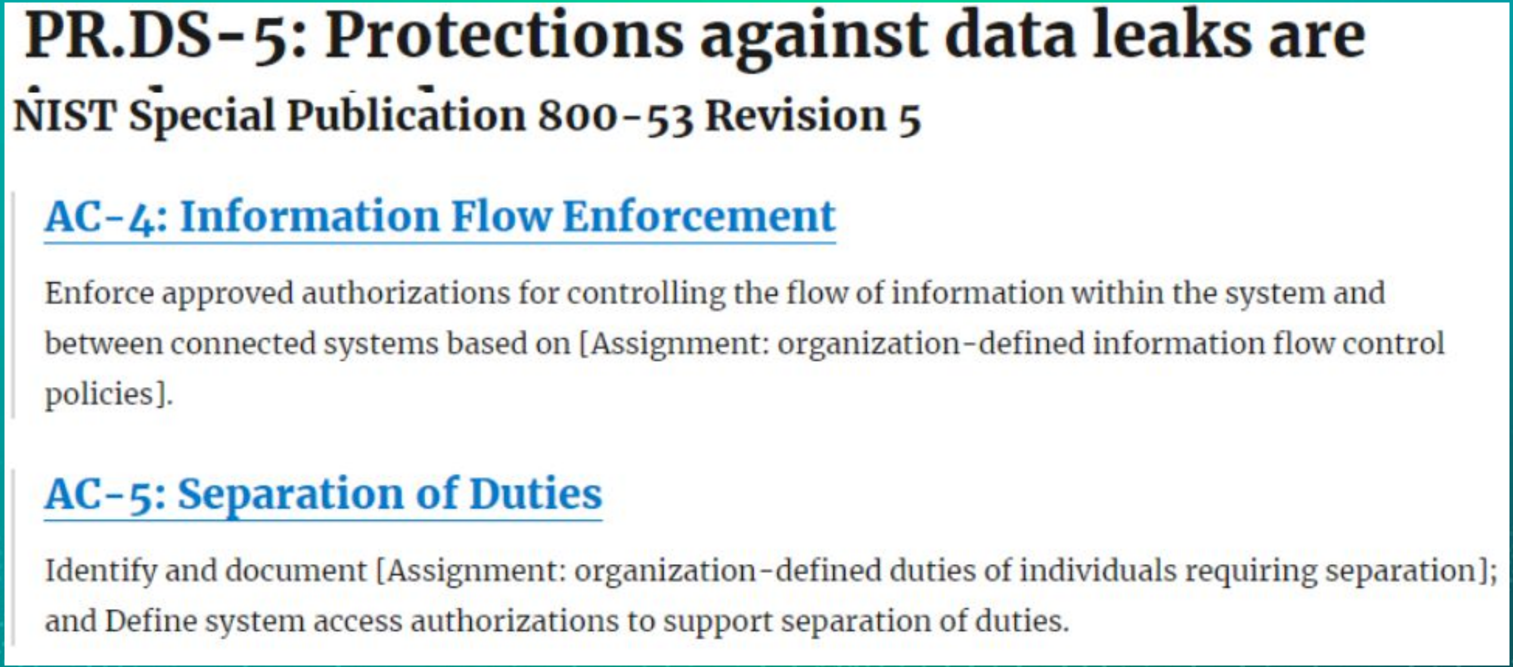
ID	Data Source	Data Component	Detects
DS0029	Network Traffic	Network Connection Creation	Monitor for newly constructed network connections that are sent or received by untrusted hosts.
		Network Traffic Content	Monitor and analyze traffic patterns and packet inspection associated to protocol(s) that do not follow the expected protocol standards and traffic flows (e.g extraneous packets that do not belong to established flows, gratuitous or anomalous traffic patterns, anomalous syntax, or structure). Consider correlation with process monitoring and command line to detect anomalous processes execution and command line arguments associated to traffic patterns (e.g. monitor anomalies in use of files that do not normally initiate connections for respective protocol(s)).

Roubo de dados CapitalOne



Stage	Step of the attack	Technical Controls	CSF NIST Failed Controls
Command And Control	Use TOR Network to hide the origin of the attack	Block at Firewall and hosts access from IP addresses from TOR network exit nodes and from malicious proxy server. Alert on IDS/IPS successful access from malicious IP addresses.	**ID.AM-4:** External information systems are catalogued **PR.DS-5:** Protections against data leaks are implemented **DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed **DE.CM-1:** The network is monitored to detect potential cybersecurity events **DE.CM-6:** External service provider activity is monitored to detect potential cybersecurity events **DE.CM-7:** Monitoring for unauthorized personnel, connections, devices, and software is performed **DE.DP-2:** Detection activities comply with all applicable requirements
Initial Access	Use SSRF attack to run commands on vulnerable server	Such attack could be mitigated by a well configured WAF and preventive controls, such as periodic vulnerability scanners.	**PR.IP-12:** A vulnerability management plan is developed and implemented **PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy **PR.PT-3:** The principle of least functionality is incorporated by configuring systems to provide only essential capabilities **DE.AE-3:** Event data are collected and correlated from multiple sources and sensors **DE.CM-1:** The network is monitored to detect potential cybersecurity events **DE.CM-6:** External service provider activity is monitored to detect potential cybersecurity events **DE.CM-7**: Monitoring for unauthorized personnel, connections,

Roubo de dados CapitalOne



PR.DS-5: Protections against data leaks are

NIST Special Publication 800-53 Revision 5

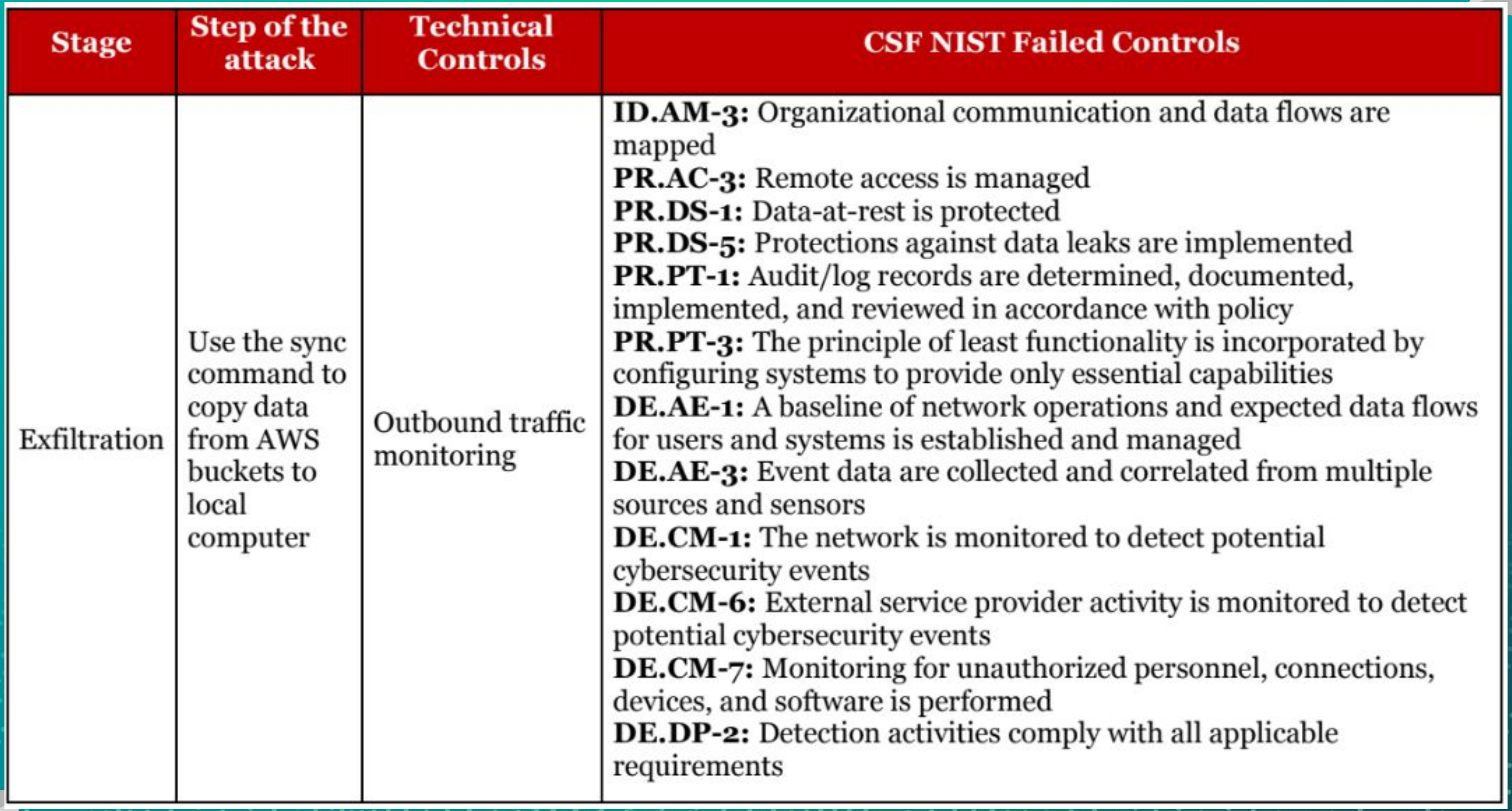
AC-4: Information Flow Enforcement

Enforce approved authorizations for controlling the flow of information within the system and between connected systems based on [Assignment: organization-defined information flow control policies].

AC-5: Separation of Duties

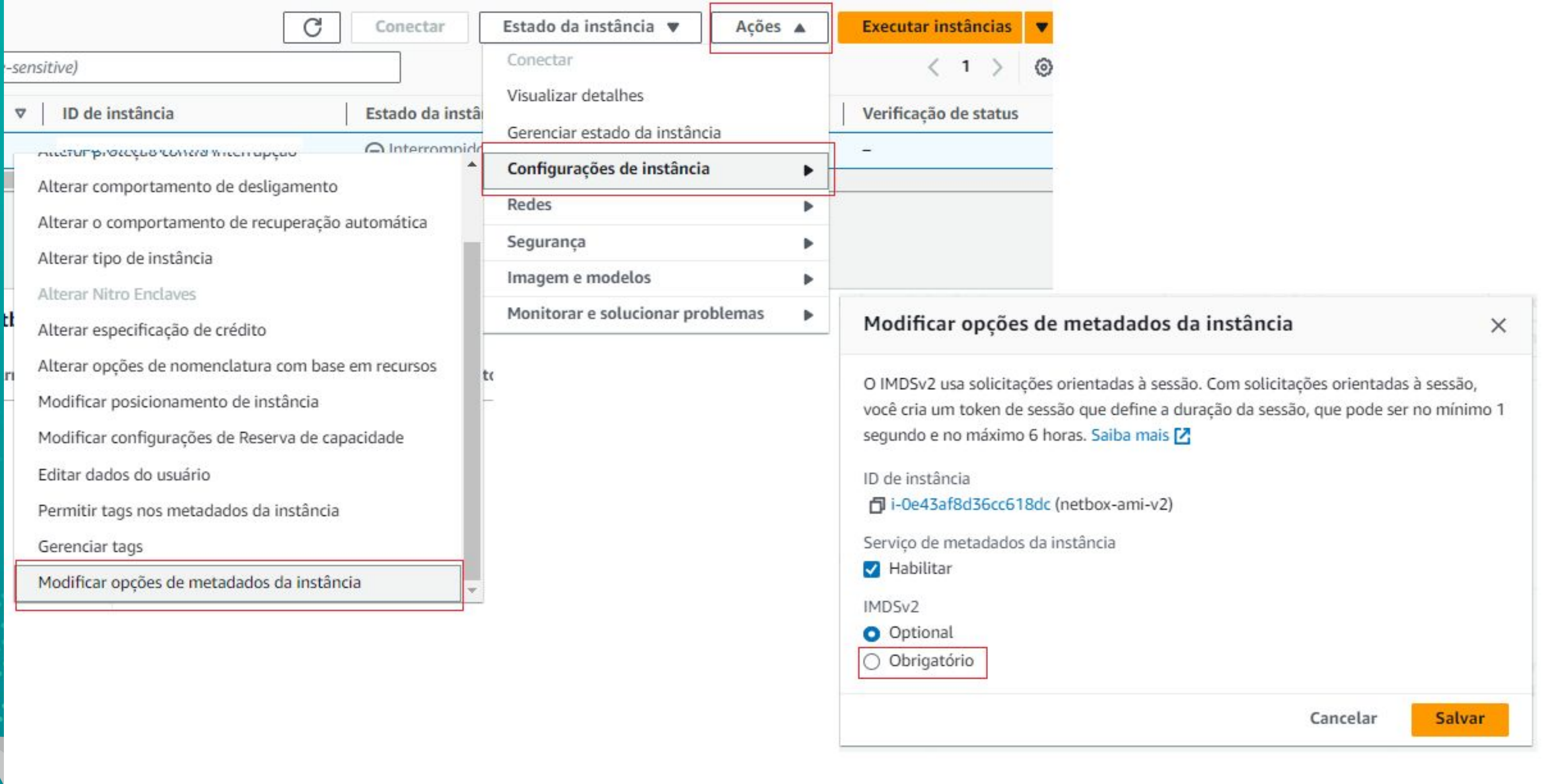
Identify and document [Assignment: organization-defined duties of individuals requiring separation]; and Define system access authorizations to support separation of duties.

Roubo de dados CapitalOne



Stage	Step of the attack	Technical Controls	CSF NIST Failed Controls
Exfiltration	Use the sync command to copy data from AWS buckets to local computer	Outbound traffic monitoring	**ID.AM-3:** Organizational communication and data flows are mapped **PR.AC-3:** Remote access is managed **PR.DS-1:** Data-at-rest is protected **PR.DS-5:** Protections against data leaks are implemented **PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy **PR.PT-3:** The principle of least functionality is incorporated by configuring systems to provide only essential capabilities **DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed **DE.AE-3:** Event data are collected and correlated from multiple sources and sensors **DE.CM-1:** The network is monitored to detect potential cybersecurity events **DE.CM-6:** External service provider activity is monitored to detect potential cybersecurity events **DE.CM-7:** Monitoring for unauthorized personnel, connections, devices, and software is performed **DE.DP-2:** Detection activities comply with all applicable requirements

Habilitar Metadata v2


Conectar
Estado da instância ▼
Ações ▲
Executar instâncias ▼
-sensitive)
ID de instância
Estado da instâ
Verificação de status
Interrompid
Alterar proteção contra interrupção
Alterar comportamento de desligamento
Alterar o comportamento de recuperação automática
Alterar tipo de instância
Alterar Nitro Enclaves
Alterar especificação de crédito
Alterar opções de nomenclatura com base em recursos
Modificar posicionamento de instância
Modificar configurações de Reserva de capacidade
Editar dados do usuário
Permitir tags nos metadados da instância
Gerenciar tags
Modificar opções de metadados da instância
Conectar
Visualizar detalhes
Gerenciar estado da instância
Configurações de instância ▶
Redes ▶
Segurança ▶
Imagem e modelos ▶
Monitorar e solucionar problemas ▶

Modificar opções de metadados da instância

O IMDSv2 usa solicitações orientadas à sessão. Com solicitações orientadas à sessão, você cria um token de sessão que define a duração da sessão, que pode ser no mínimo 1 segundo e no máximo 6 horas. Saiba mais

ID de instância

i-0e43af8d36cc618dc (netbox-ami-v2)

Serviço de metadados da instância

☑ Habilitar

IMDSv2

● Optional

○ Obrigatório

Cancelar | Salvar

Conclusão

Conclusão

- **Medidas de prevenção:**
  - Entender o cenário antes de iniciar a migração/deploy
  - Utilizar frameworks para validação da estrutura de segurança:
    - MITRE ATT&CK
    - NIST
  - Realizar pentest/auditoria regularmente
    - Elaborar plano de resposta a incidentes
  - Configurar alertas de atividades suspeitas
  - Manter inventário atualizado e documentado
  - Segurança camadas (Firewall, SG, VPCs, Auditoria)
  - Bloquear recursos não utilizados
  - Não utilizar a conta root
  - Aplicar princípio do mínimo privilégio (contas, roles, serviços)
  - Não utilizar configurações default (Metadata v2)

mind the sec /2023

Obrigado

O preço da paz é a eterna vigilância

John Philpot Curran

mind the sec /2023

Pedro Borges

pedroeborges@gmail.com

in /pedroborgescio