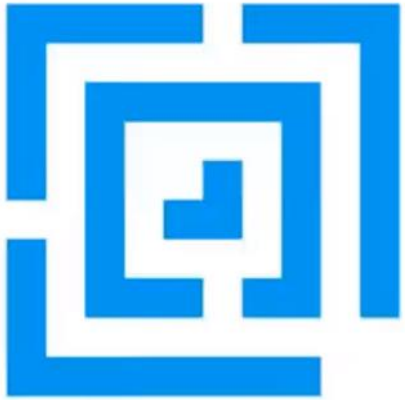
THE DEVELOPER'S CONFERENCE

Reduzindo a superficie de ataques - Secrets Management

Erick Ferreira

Secret Management

THE DEVELOPER'S CONFERENCE



Machine Identity

+

Human Identity

Estado Atual – Ilhas de Segurança

THE DEVELOPER'S CONFERENCE

Ilhas de Segurança

Puppet Hiera

Docker Secrets

AWS IAM

Ansible Vault

Kubernetes Secrets

Azure KMS/IAM

Chef Databags

Google Cloud IAM/KMS

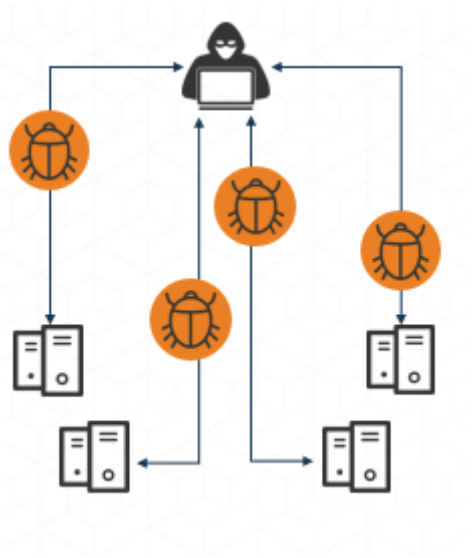
OpenShift Secrets

O poder do privilégio

THE DEVELOPER'S CONFERENCE

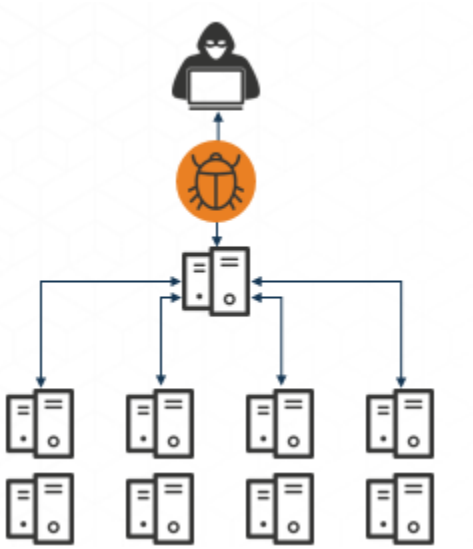
Moda Antiga

"Hack a System"

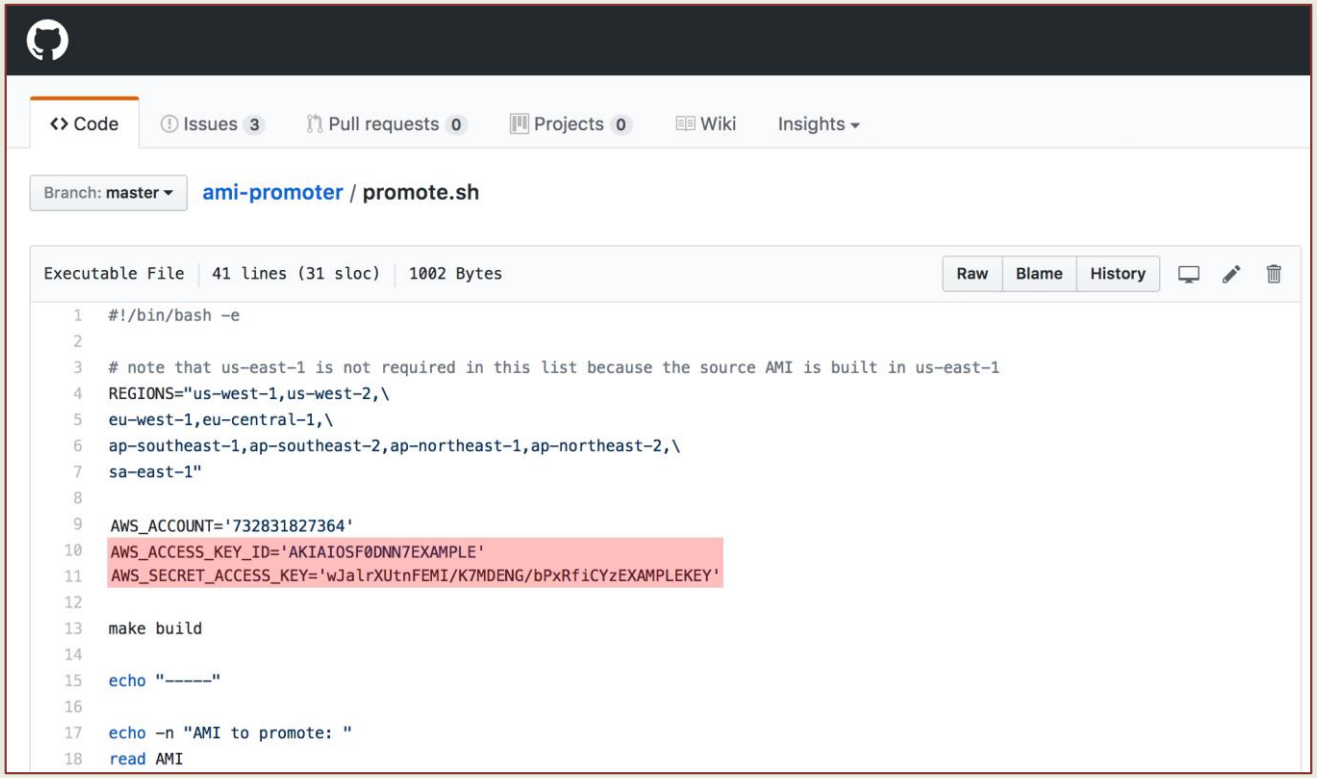


Nova Moda

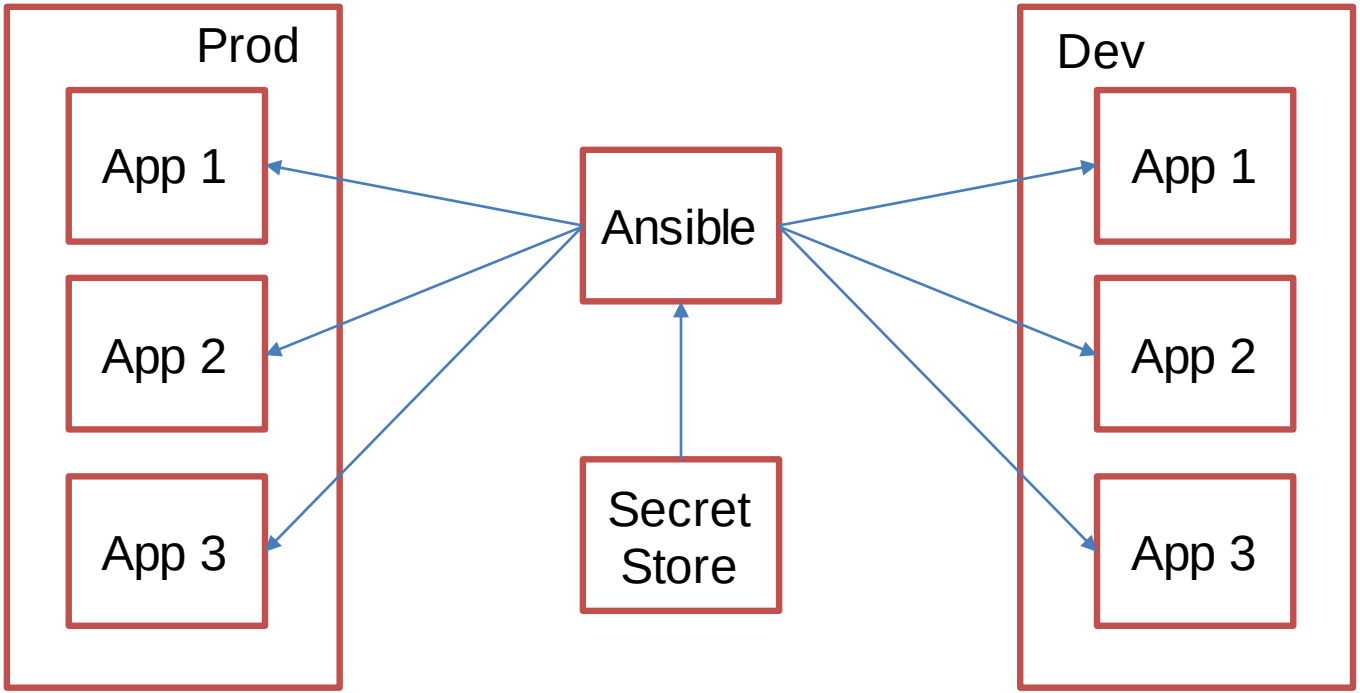
"Hack a Datacenter"



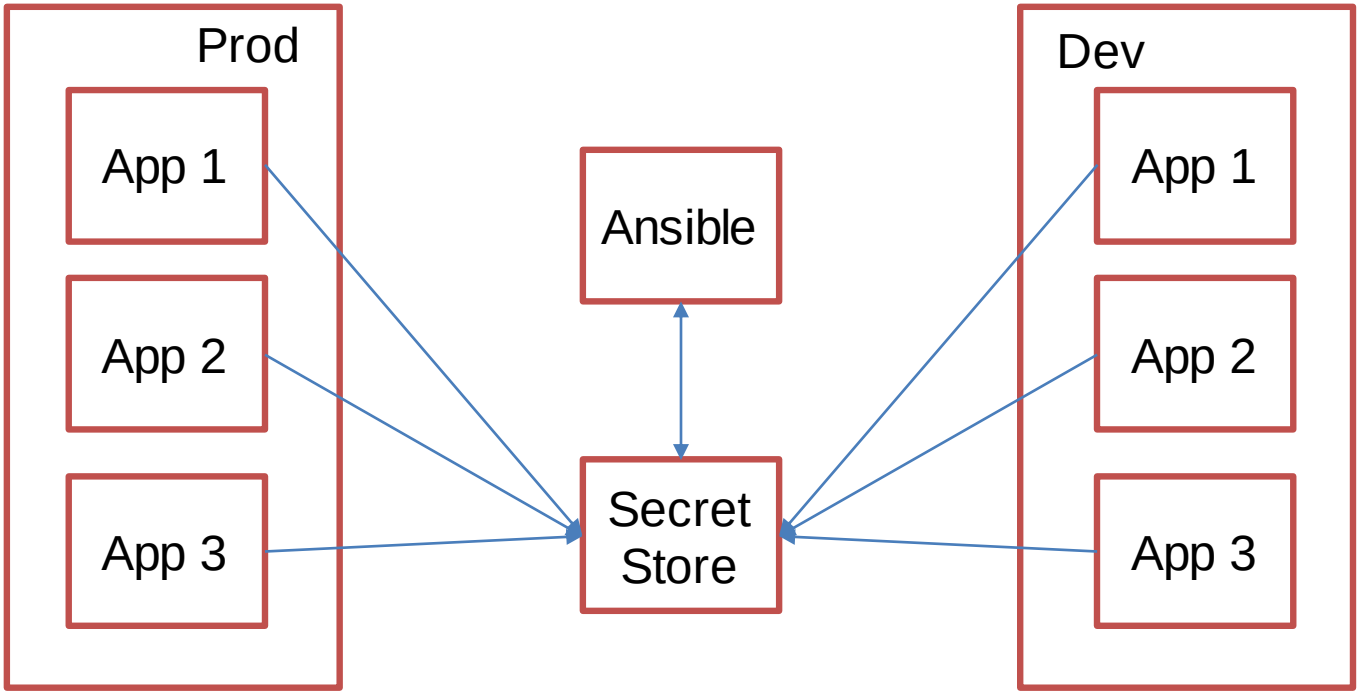
Credencial exposta em domínio público



Abordagem Comum



Abordagem baseada em Identidade



Tem senha no codigo???

THE DEVELOPER'S CONFERENCE

Quando foi a ultima vêz que você alterou uma API Key??

Sua SSH Key?

A senha da Base de dados?

:(

Your PC ran into a problem and needs to restart. We're just collecting some error info, and then we'll restart for you.

20% complete

For more information about this issue and possible fixes, visit https://www.windows.com/stopcode

If you call a support person, give them this info:

Stop code: CRITICAL_PROCESS_DIED

Não comprometa a segurança por velocidade

THE DEVELOPER'S CONFERENCE

onelogin

O atacante obeteve acesso a um conjunto de AWS Keys e usou ela para acessar a API do AWS, o banco de dados com todas as informações dos usuários bem como outras chaves.

Vine

Um Hacker acessou o registro de um docker que continha o código completo, API Keys e Secrets da empresa

ASHLEY MADISON.COM

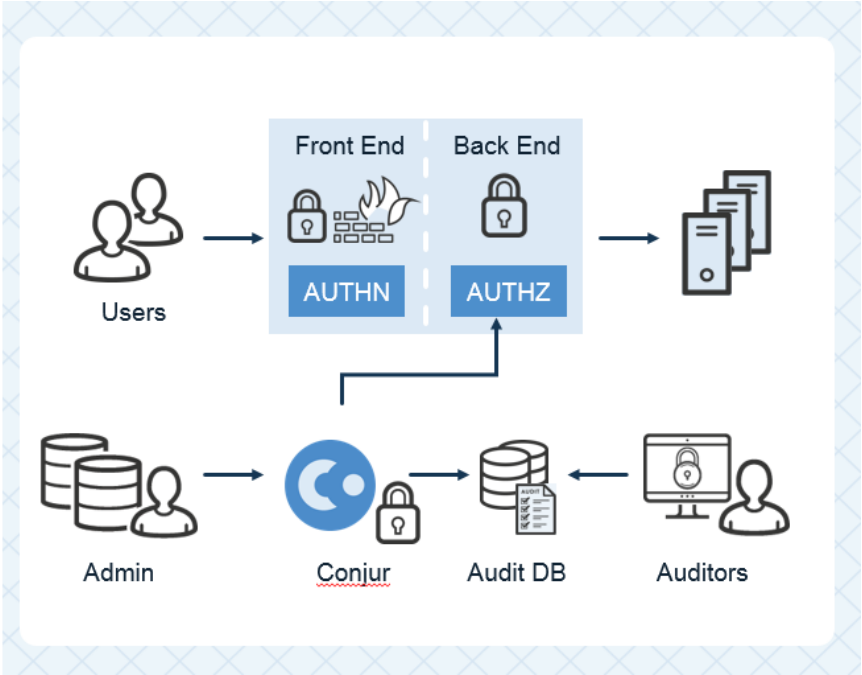
Desenvolvedores armazenaram credenciais no código

Conjur OSS – Open Source

THE DEVELOPER'S CONFERENCE

Conjur Server (Basic)

- Linux Operating System
- PostgreSQL Database
  - Secure Secrets Storage
- HTTPS w/ REST API
  - Authentication, Permissions, Secrets Management, Auditing
- LDAPS Directory Services
  - 3rd Party Integration



Link GitHub https://github.com/cyberark/conjur

Conjur OSS – Open Source

THE DEVELOPER'S CONFERENCE

- Politica baseada em Papéis (Role Based)
- Integração com tecnolgias utilizadas no dia a dia (Puppet, Jenkins, Docker etc)
- Armazenamento seguro de secrets
- Troca de secrets (Pago)

Exemplo de Politica que causa riscos.

THE DEVELOPER'S CONFERENCE

Visual editor | JSON

```
    "Statement": [
        {
            "Sid": "DevOpsPolicy",
            "Effect": "Allow",
            "Action": [
                "iam:CreateInstanceProfile",
                "iam:PassRole",
                "iam:AddRoleToInstanceProfile",
                "ec2.AssociateIamInstanceProfile"

            ],
            "Resource": [
                "arn:aws:iam::*:instance-profile/*",
                "arn:aws:iam::*:role/*",
                "arn:aws:ec2::*:instance/*"
            ]
        }
    ]
}
```

Exemplo de Politica que causa riscos.

SkyArk is a cloud security project with two helpful sub-modules - AWStealth and AWStrace.

Link GitHub: https://github.com/cyberark/SkyArk

THE DEVELOPER'S CONFERENCE

Obrigado!

erickrazr@gmail.com

+55 11 99922-5224