CASE STUDY

8TH BIGGEST TELCO IN THE WORLD

Certificates, SSH keys & PAM managed
in one single platform

SITUATION

Complex and huge telecommunication network with more 100k devices distributed geographically;

3 huge geographic distributed data center with ssh keys, certificates, and local passwords;

Ghost SSH Keys and certificates in many IT devices on premises and on cloud;

PROBLEM

With no clear policy, machine identities are been created without governance makes it almost impossible to have control of this identities and access.

It is impossible to create a security control center for machines identities and have a clear visibility of this identities.

This allow ghost identities and security attack vector that can be exploited.

SOLUTION

We've **deployed senhasegura platform to manage the lifecycle of machine identities** with high availability and disaster recovery over 3 distributed datacenters;

We **scan and discover all privileged credentials, ssh keys, certificate** with senhasegura's discovery trough more then 10.000 devices, multiple Cas.

Automated identities rotation and renew for Credentials, SSH Keys, Certificates.

RESULTS

The project is still under deployment but the costumer already had:

Centralized view of ssh keys, credentials and certificates.

Lifecycle management for ssh keys and certificates.

Reduction of ghost ssh keys and unused credentials.

Reduction of application outages due to certificate expiration.

REQUEST A TRIAL DEMONSTRATION AND DISCOVER THE BENEFITS OF SENHASEGURA FOR YOUR COMPANY

REQUEST DEMO