Teleport Connect 2024

Hardening Infrastructure Security Against SSO Identity Provider Compromise



Francesco Lacerenza

Sr. Security Engineer

Doyensec

whoami?



Application Security
Offensive Engineering

```
$ tsh status

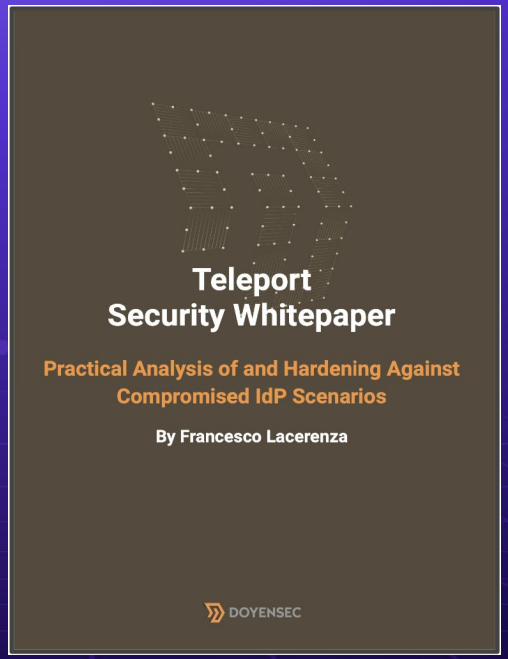
> Company URL: https://doyensec.com
Logged in as: Francesco Lacerenza
Roles: Senior Security Engineer, WebSec & CloudSec Enthusiast
Logins: @lacerenza_fra (on X), francesco-lacerenza (on LinkedIn)
Extensions: Scuba Diving, Running
```

The End We Start From

DOYENSEC | Teleport Connect 2024



Defending against Identity Provider (IdP) Compromise



Practical Analysis of and Hardening Against Compromised IdP Scenarios

Doyensec's Teleport IdP Hardening Checklist

Teleport Connect 2024

DOYENSEC

What is an IdP? Why do we care?

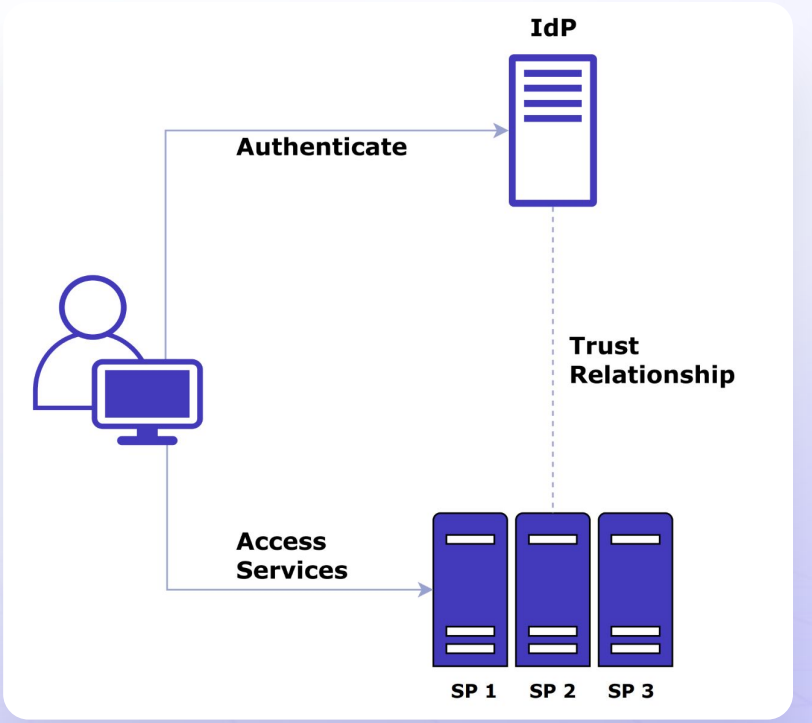
Definition and Service Providers (SP) Relationships

Research Thesis

Federated Identity Actors

DOYENSEC | Teleport Connect 2024

- **Identity Provider (IdP):**
  a service used to manage a pool of users and authenticate them in registered apps called Service Providers
- **Service Providers (SPs):**
  an application or service that relies on an IDP for user authentication



IdP Compromises in the news

DOYENSEC | Teleport Connect 2024

- Okta Breach
  September 28, 2023
  to October 17, 2023
- OneLogin
  May 31, 2017
- etc.

The Question

What can the SP do in order to protect its own service in case of IdP compromise?

The Thesis

Implementing an additional layer of security over the identity provider in place

Teleport Connect 2024

DOYENSEC

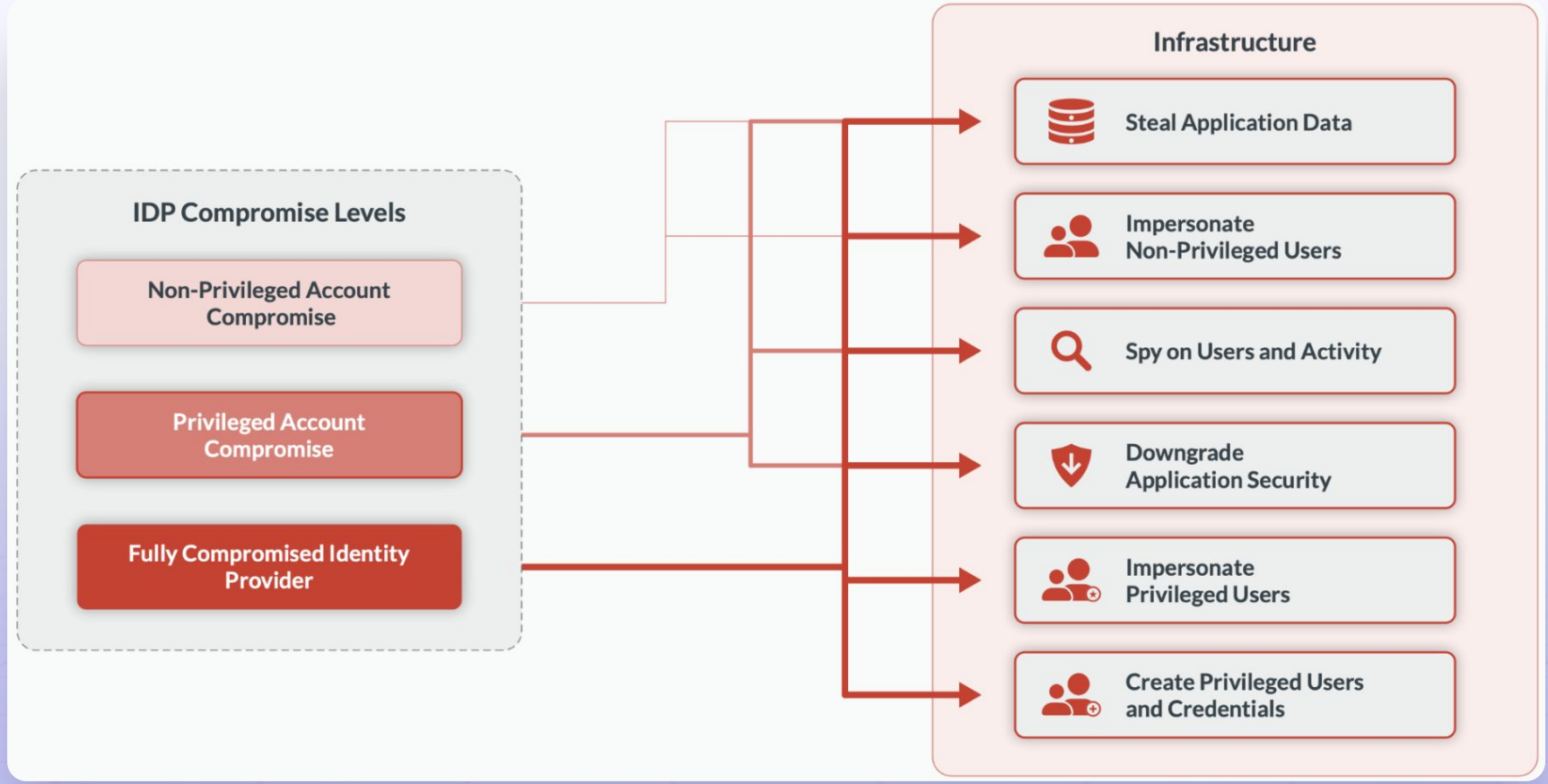
Evaluation Strategy

IdP Levels of Compromise

Threats against the SP

IDP Threat Vector Tree

DOYENSEC | Teleport Connect 2024



Teleport Connect 2024

DOYENSEC

Attacks & Hardening Guideline

Idp-to-SP mapping with Least Privilege

Attributes Manipulation & Autoprovisioning

Extra Identity Confirmation Layer

Detection & Response

Impersonation Attacks

DOYENSEC | Teleport Connect 2024

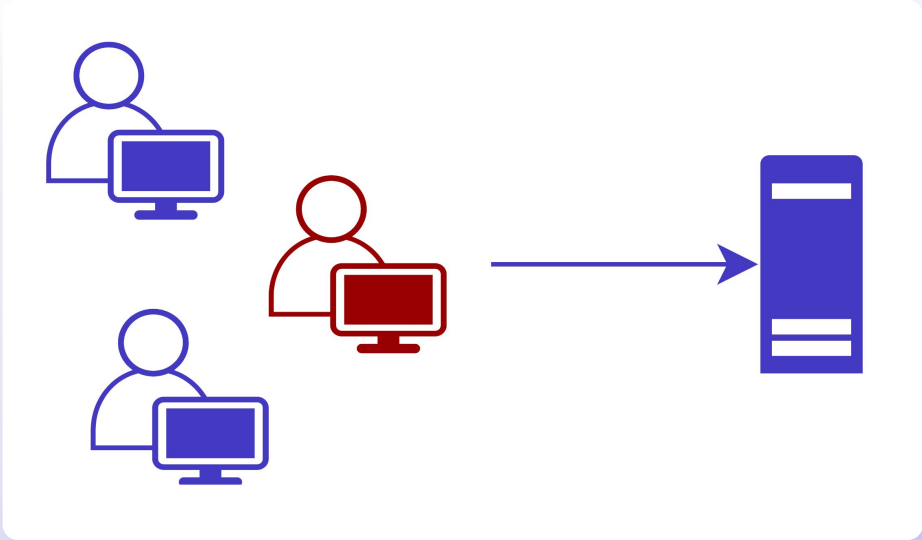
Teleport User Impersonation

In this case, attackers could:

- Impersonate any existing SSO user
- Re-assign users to a specific SSO role-mapping group

↓

Result: We assume valid Teleport certificates for the mapping in place



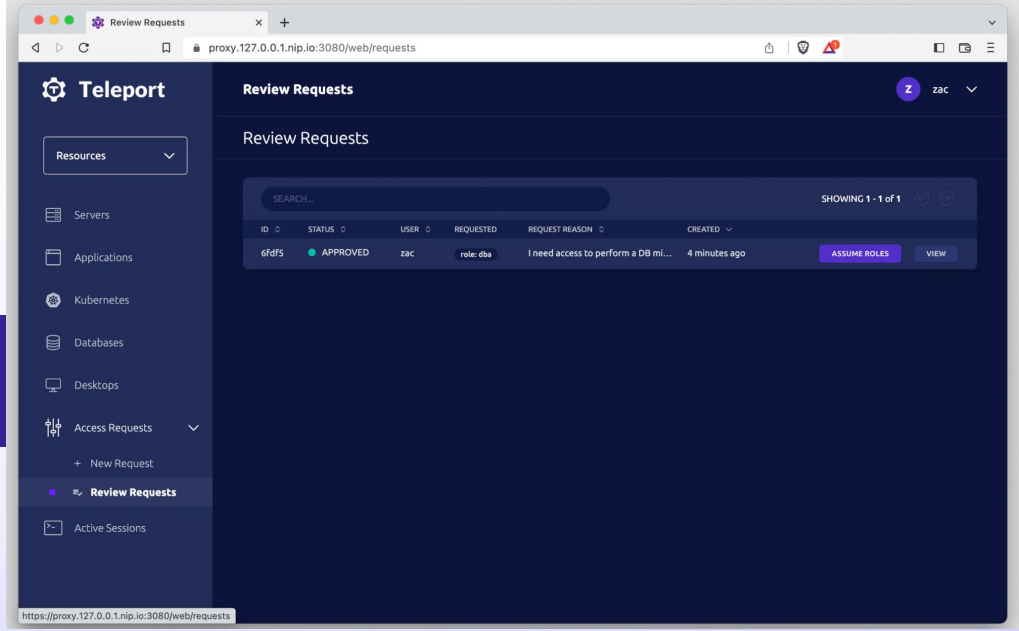
Hardening

Teleport Connect 2024

Access Requests

Just-in-time Access Requests allow Teleport users to request access to a resource or role

Usable to create an infrastructure with ephemeral admins



Impersonation Attacks

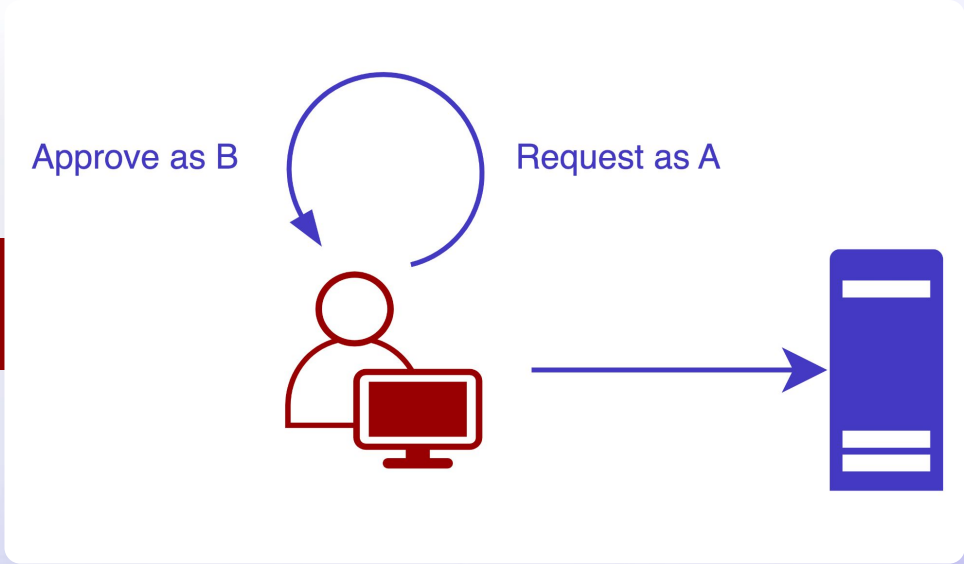
Teleport Connect 2024

Escalation examples

Auto-Approving Access Requests

If Access Request reviewers are SSO users

The attackers could impersonate both the requester and the approver



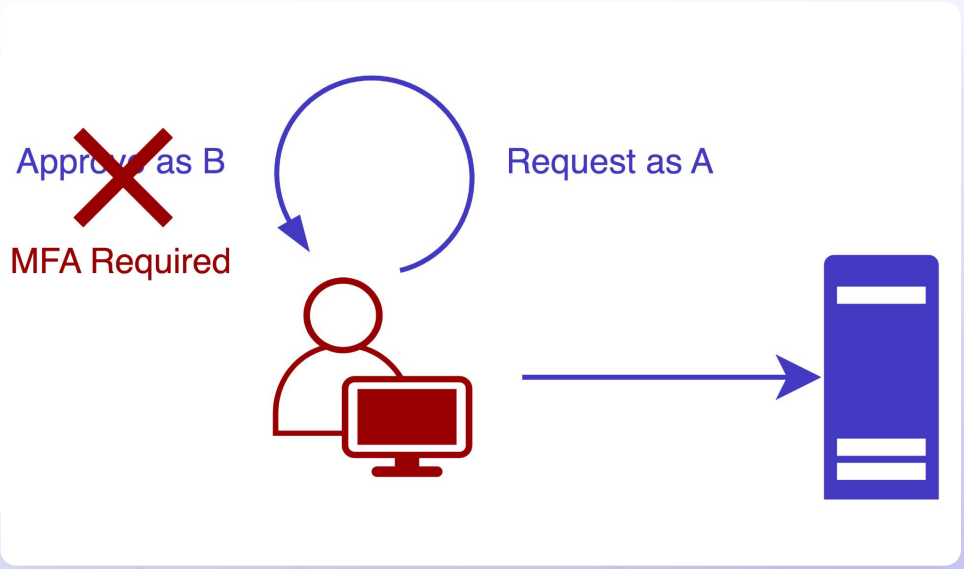
Hardening

Teleport Connect 2024

MFA For Admin Actions

Enforce an additional MFA verification for administrative actions

Prevents cluster-changing actions from impersonated users



Connector Security

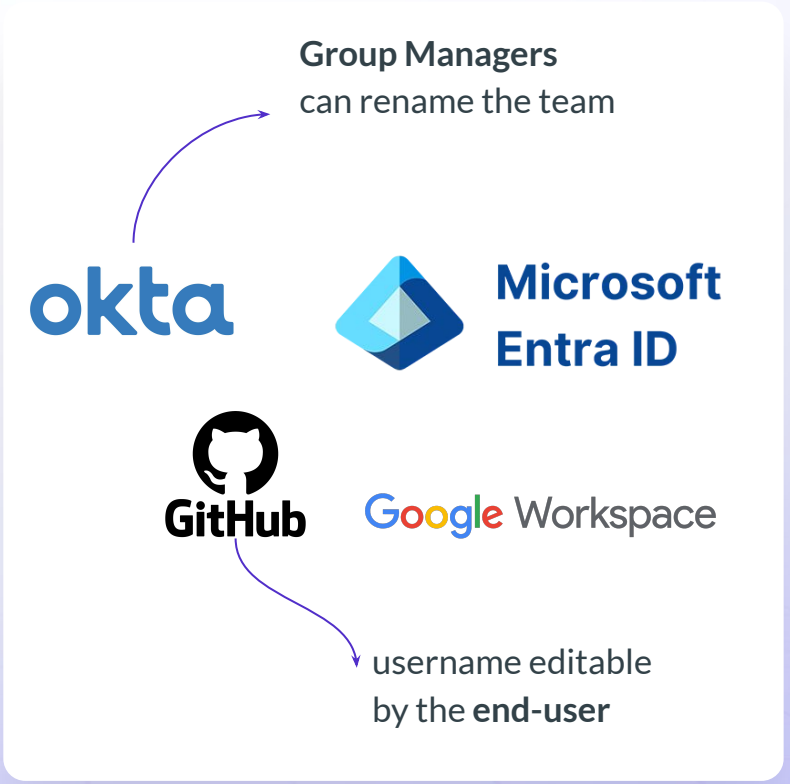
Teleport Connect 2024

Which attributes?

- Username (ID)
- Group (Role / Resources Group) etc.

Who could manipulate the attributes?

- IdP Admins
- Group Managers
- Application Managers
- SSO users

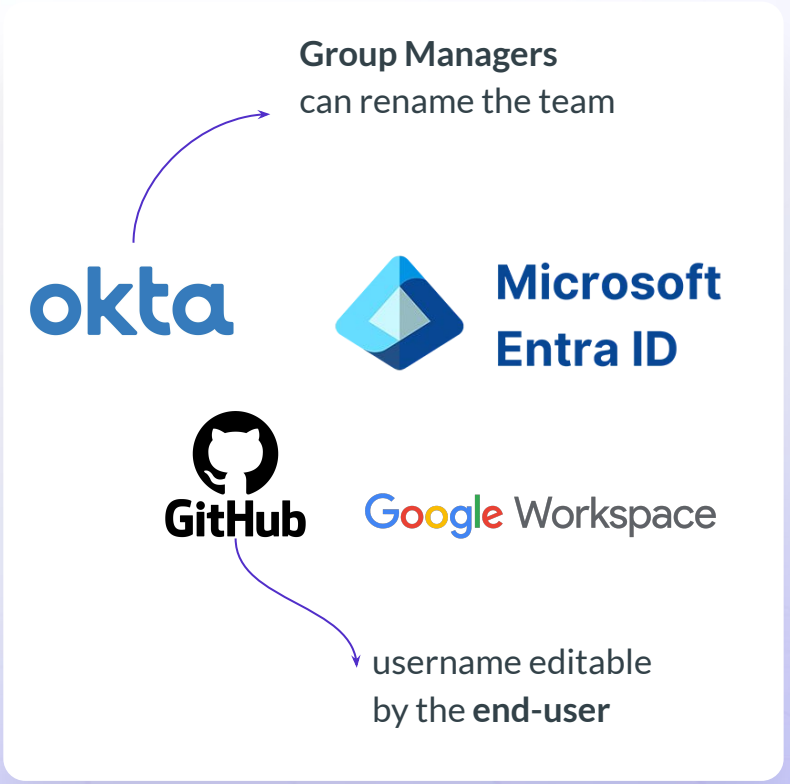


Connector Security

Teleport Connect 2024

Is Autoprovisioning Good or Bad ??

- Convenient user onboarding
- Hard to secure assuming an IdP compromise



Attributes Manipulation Attacks

DOYENSEC | Teleport Connect 2024

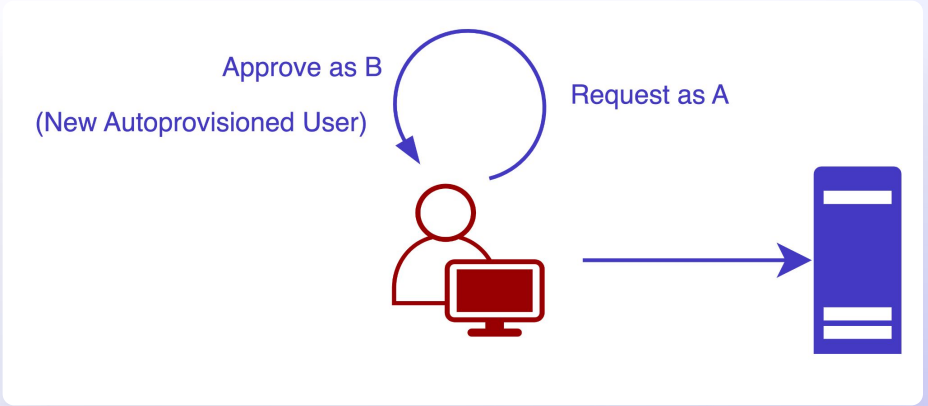
Forced User Automatic provisioning via Username Edit

By changing the ***username***, a new SSO user in Teleport will be provisioned.

Being new, no MFA devices will be present, hence allowing MFA checks bypass

↓

Result: Any compromised SSO Identity capable of editing its own username could be abused



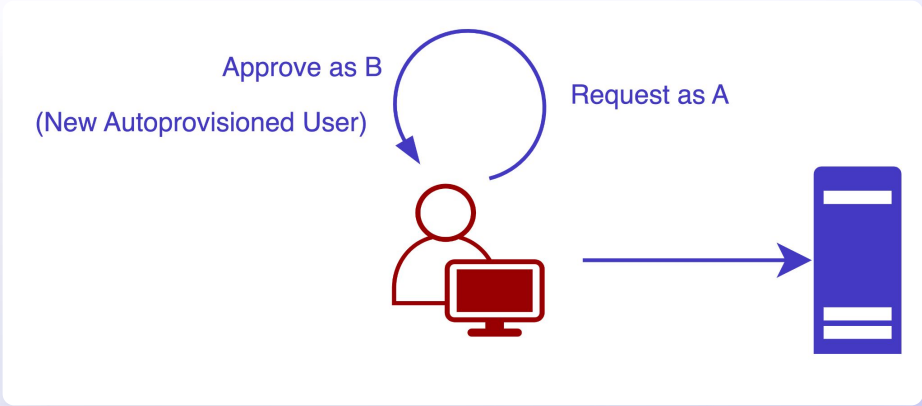
Hardening

DOYENSEC | Teleport Connect 2024

Device Trust

By enforcing it, new SSO users need to perform the first MFA device enrollment from a trusted device

Prevents MFA restrictions bypass via autoprovisioning



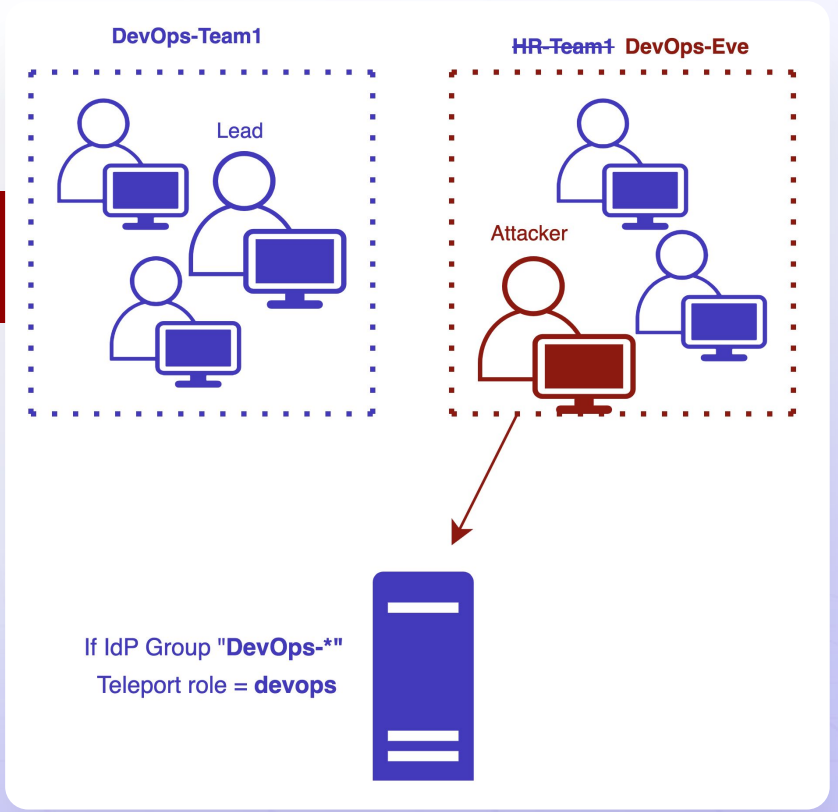
Attributes Manipulation Attacks

DOYENSEC | Teleport Connect 2024

Roles Mapping Matching

The rename operation can be exploited to match a privileged role rule

Exploitable by IdP Admins and group managers to change the role assignment



Hardening

DOYENSEC | Teleport Connect 2024

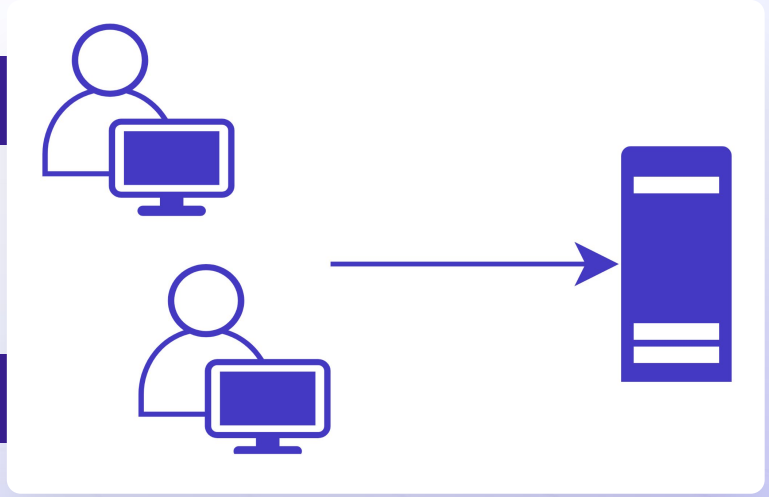
Secure Connector Definition

The username field (IdP-side) mapped as Teleport identity is non-editable and unique

Further secures against autoprovisioning attacks

The Teleport SSO Connector applies fixed string matching to map roles

Prevents role-mapping matching attacks



Extra Identity Confirmation Layer

DOYENSEC | Teleport Connect 2024

Device Trust is configured.
New SSO users need to perform the first MFA device enrollment from a trusted device



Per-session MFA is applied cluster-wide to restrict access to various resources with MFA devices



WebAuthn is forced as second factor to avoid OTP-related attacks



MFA for Administrative Actions is active.
Cluster-changing operations are secured

Detection & Response

DOYENSEC | Teleport Connect 2024

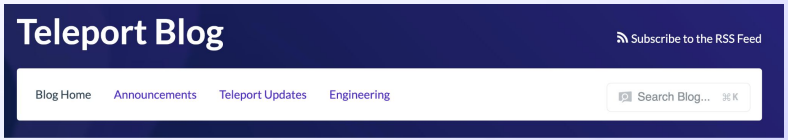
Listen to the valuable events emitted by Teleport

Define a Threat Detection & Response plan leveraging useful features like:

- **Moderated Sessions**
- **Auth Connector Management**
- **Locking**
- **Access Monitoring**

Read the Docs & Blog!

Wanna learn more?



- How To Detect Compromised Identities
- Effective Identity Threat Response

Teleport Connect 2024

DOYENSEC

Conclusions

Can the Service Provider (Teleport) defend itself?

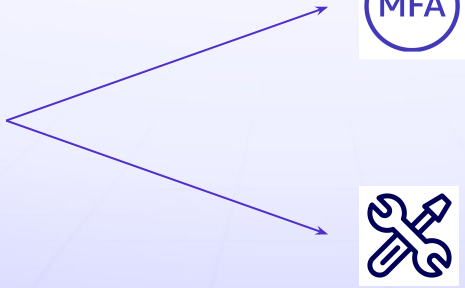
Can Teleport (SP) defend itself against SSO Compromise?

DOYENSEC | Teleport Connect 2024

Not by default.

In federated identities, SPs blindly trust the Identity Provider as a core principle

We can prevent the game-over scenario and restrict the blast radius with



Extra Confirmation Layer to prevent dangerous actions from compromised identities

Proper settings at the connector and cluster level secured against attributes manipulation



Teleport
Connect 2024



DOYENSEC

Fin

Questions & Thoughts?