Checkmk
Conference

The Fortified Watchtower

How to Set up Checkmk Securely

Ralf Spenneberg
CEO, OpenSource Security GmbH
OpenSource Security

12

Who am I?

Ralf Spenneberg

- Checkmk Gold and Training Partner since 2013
- Strong Security Background

Customers

Security goals of this talk

Authentication

Security begins with authentication

Software Deployment

Our bakery is a software deployment system

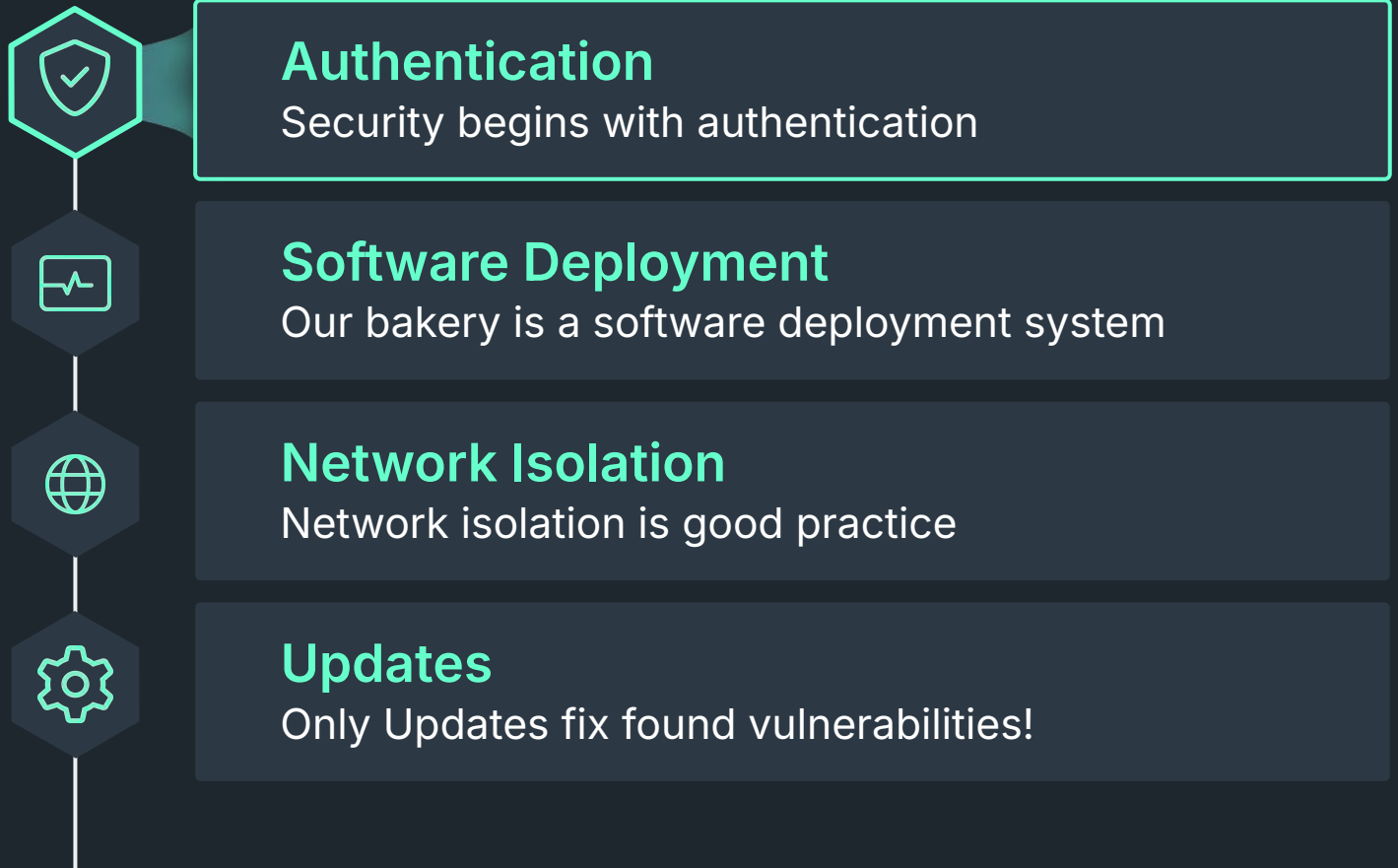
Network Isolation

Network isolation is good practice

Updates

Only Updates fix found vulnerabilities!

Authentication



Authentication
Security begins with authentication

Software Deployment
Our bakery is a software deployment system

Network Isolation
Network isolation is good practice

Updates
Only Updates fix found vulnerabilities!

What do you need for good authentication?

Single-Sign On

SAML

What do you need for good authentication?

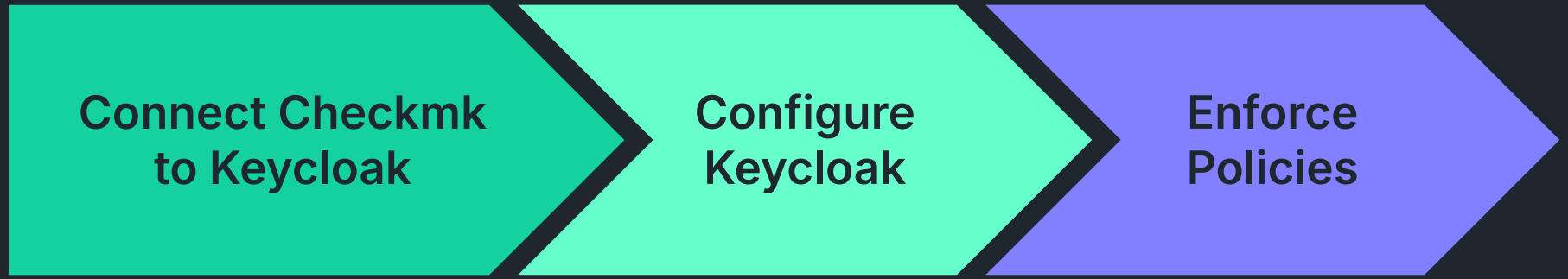
Single-Sign On

SAML

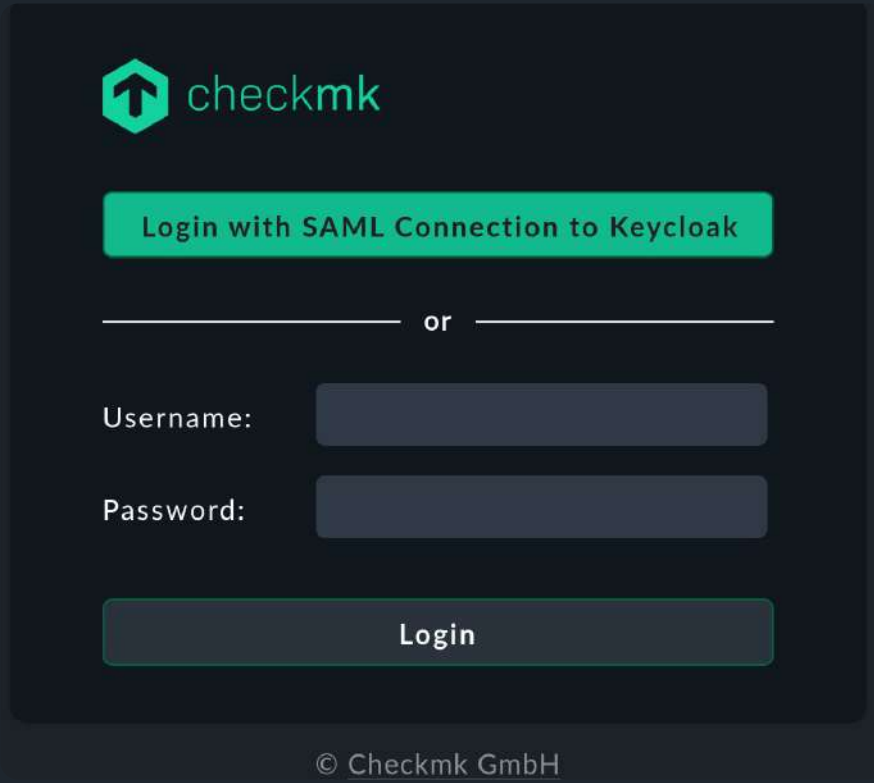
KEYCLOAK

- Open Source Identity and Access Management
- User Federation (LDAP/AD)
- Clustering

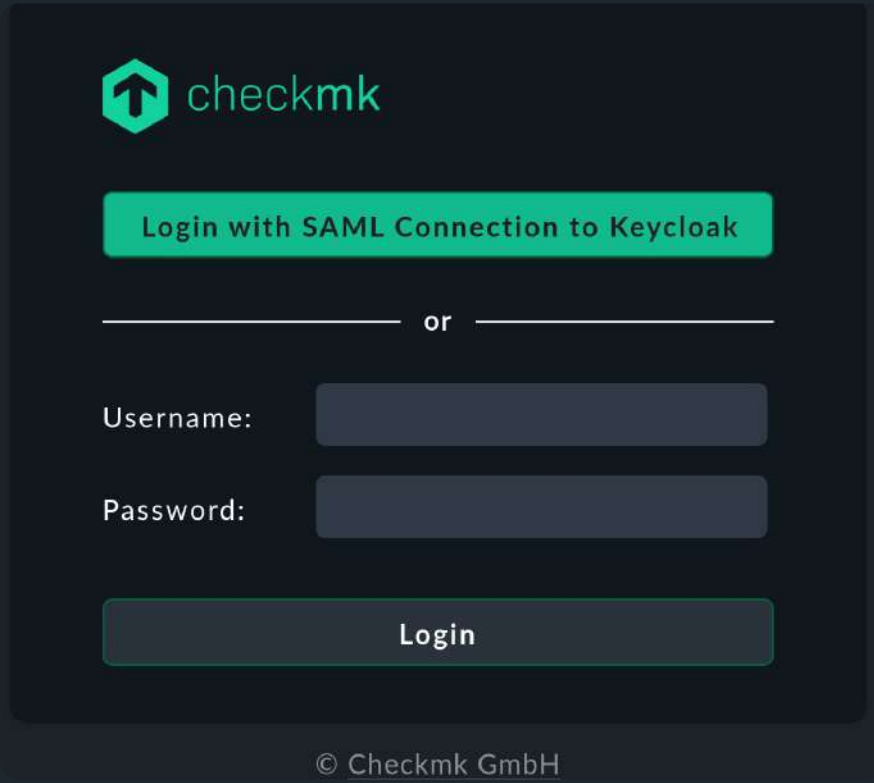
The road to Single-Sign-On



Single-Sign-On in Checkmk



Single-Sign-On in Checkmk



TLS secured access

SAML endpoints must have been registered with Keycloak

Connecting Checkmk to Keycloak

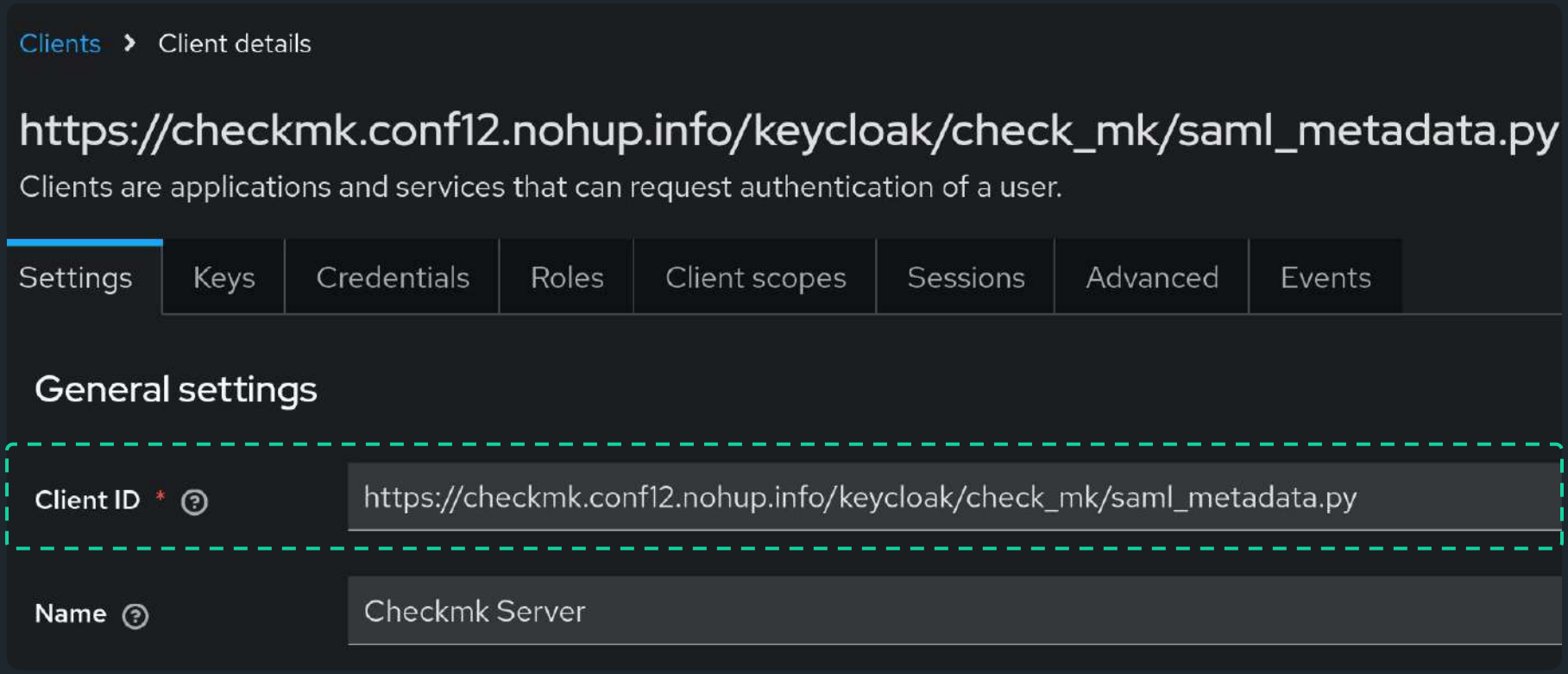
Checkmk service provider metadata (generated automatically)

Entity ID	https://checkmk.conf12.nohup.info/keycloak/check_mk/saml_metadata.py
Metadata endpoint	https://checkmk.conf12.nohup.info/keycloak/check_mk/saml_metadata.py?RelayState=saml
Assertion Consumer Service endpoint	https://checkmk.conf12.nohup.info/keycloak/check_mk/saml_acs.py?acs

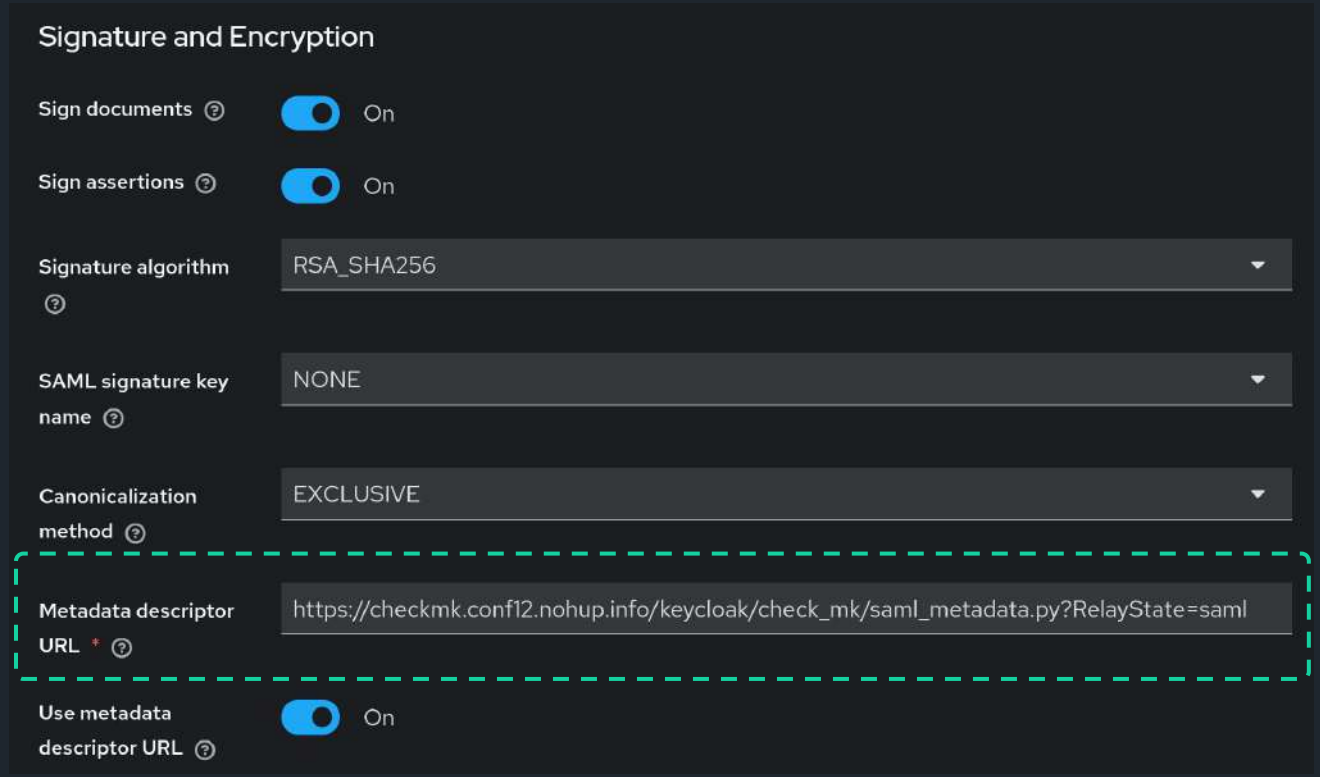
Connection

Identity provider metadata (required)	URL
	https://keycloak.conf12.nohup.info/realms/checkmk_realm/protocol/saml/descriptor
Checkmk server URL (required)	https://checkmk.conf12.nohup.info
Identity provider connection timeout	Connection timeout 12 seconds
	Read timeout 12 seconds

Keycloak client configuration

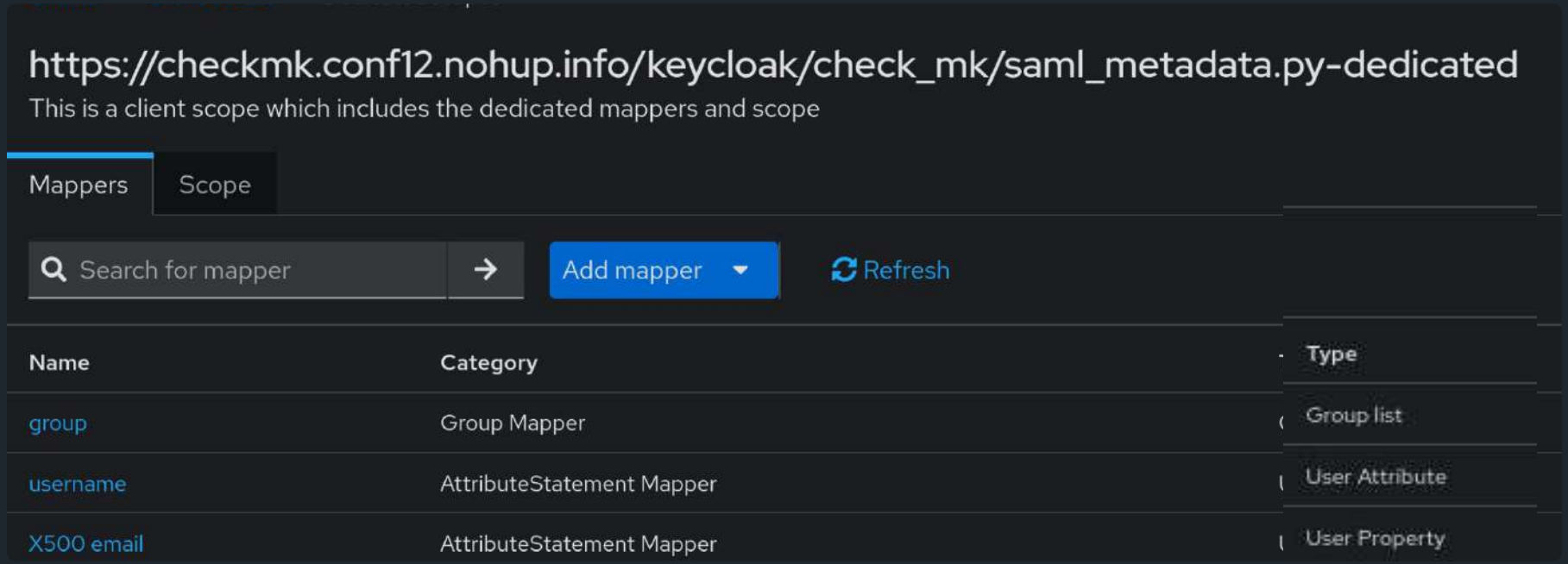


Signature and encryption



Mapping access attributes

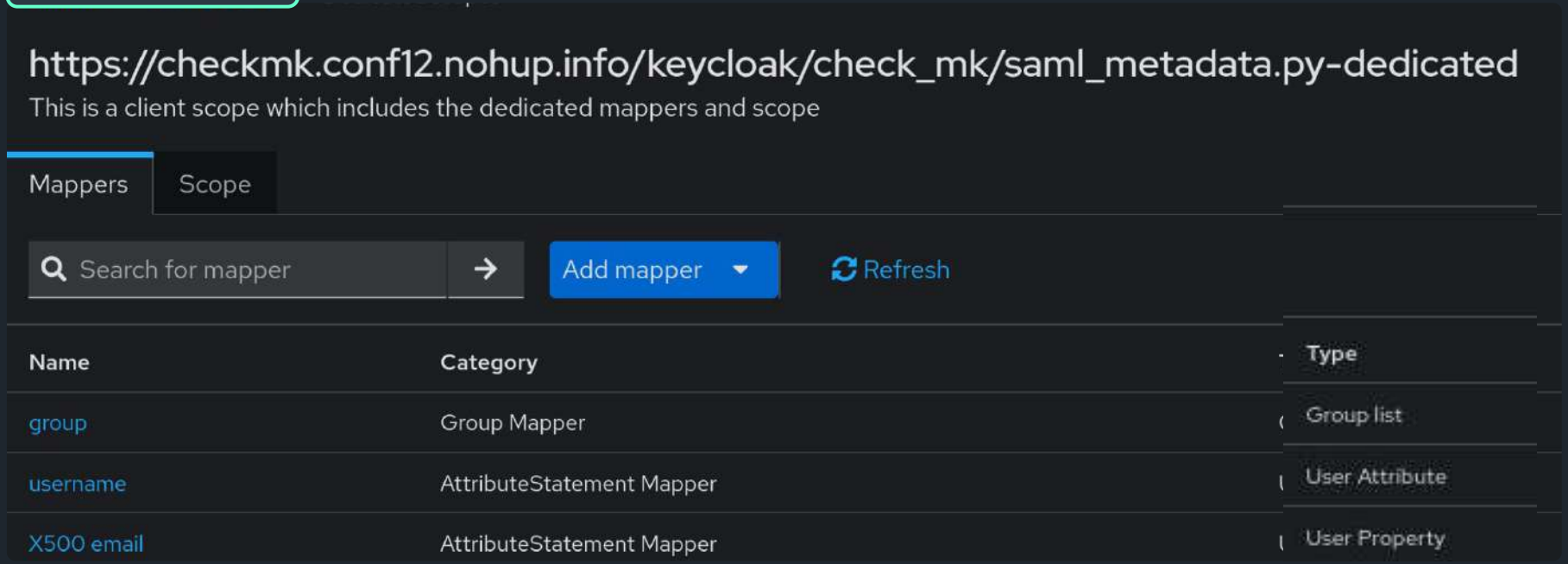
Client Scope



Mapping access attributes

Client Scope

Username



Mapping access attributes

Client Scope

Username

Groups

https://checkmk.conf12.nohup.info/keycloak/check_mk/saml_metadata.py-dedicated

This is a client scope which includes the dedicated mappers and scope

Mappers | Scope

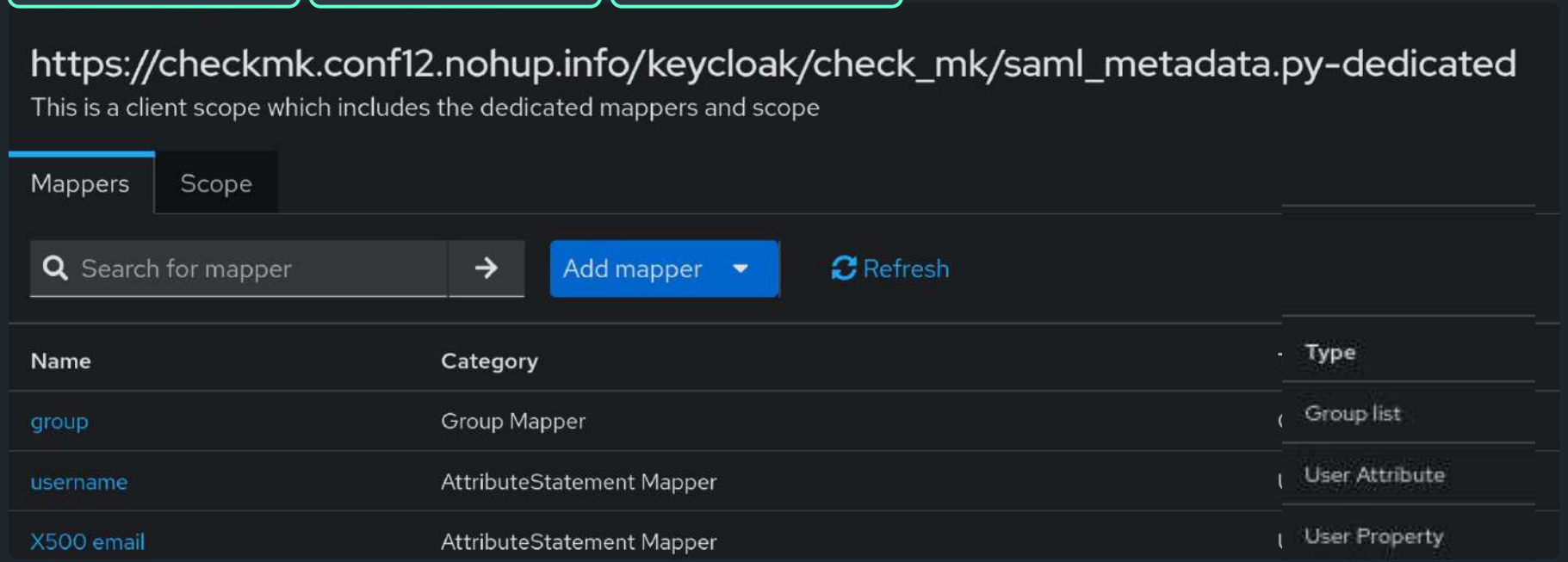
Search for mapper → | Add mapper | Refresh

Name	Category	Type
group	Group Mapper	Group list
username	AttributeStatement Mapper	User Attribute
X500 email	AttributeStatement Mapper	User Property

Mapping access attributes

Client Scope

Username | Groups | E-mail



Mapping access attributes

Client Scope

Username	Groups	E-mail	Complex Mappers via Javascript

https://checkmk.conf12.nohup.info/keycloak/check_mk/saml_metadata.py-dedicated

This is a client scope which includes the dedicated mappers and scope

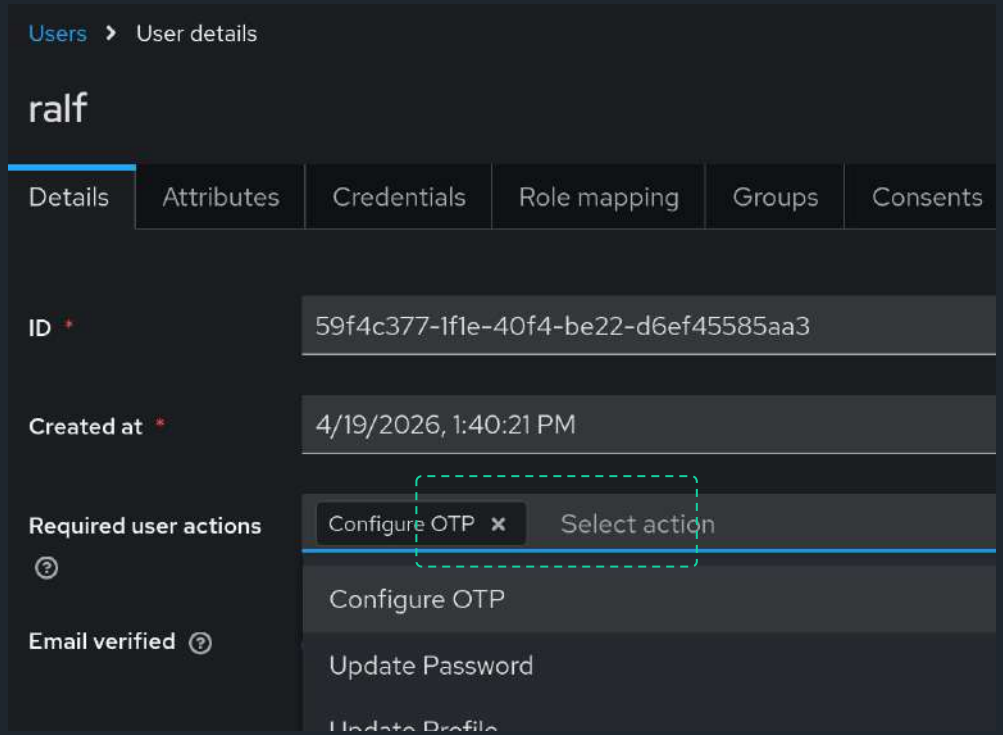
Mappers | Scope

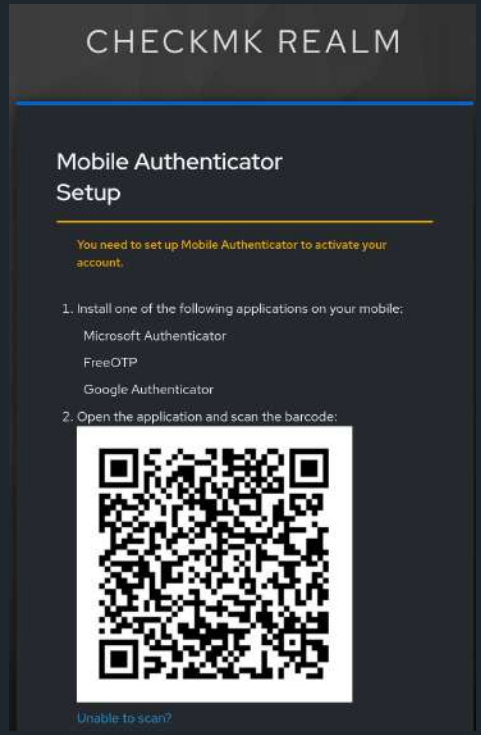
Search for mapper | Add mapper | Refresh

Name	Category	Type
group	Group Mapper	Group list
username	AttributeStatement Mapper	User Attribute
X500 email	AttributeStatement Mapper	User Property

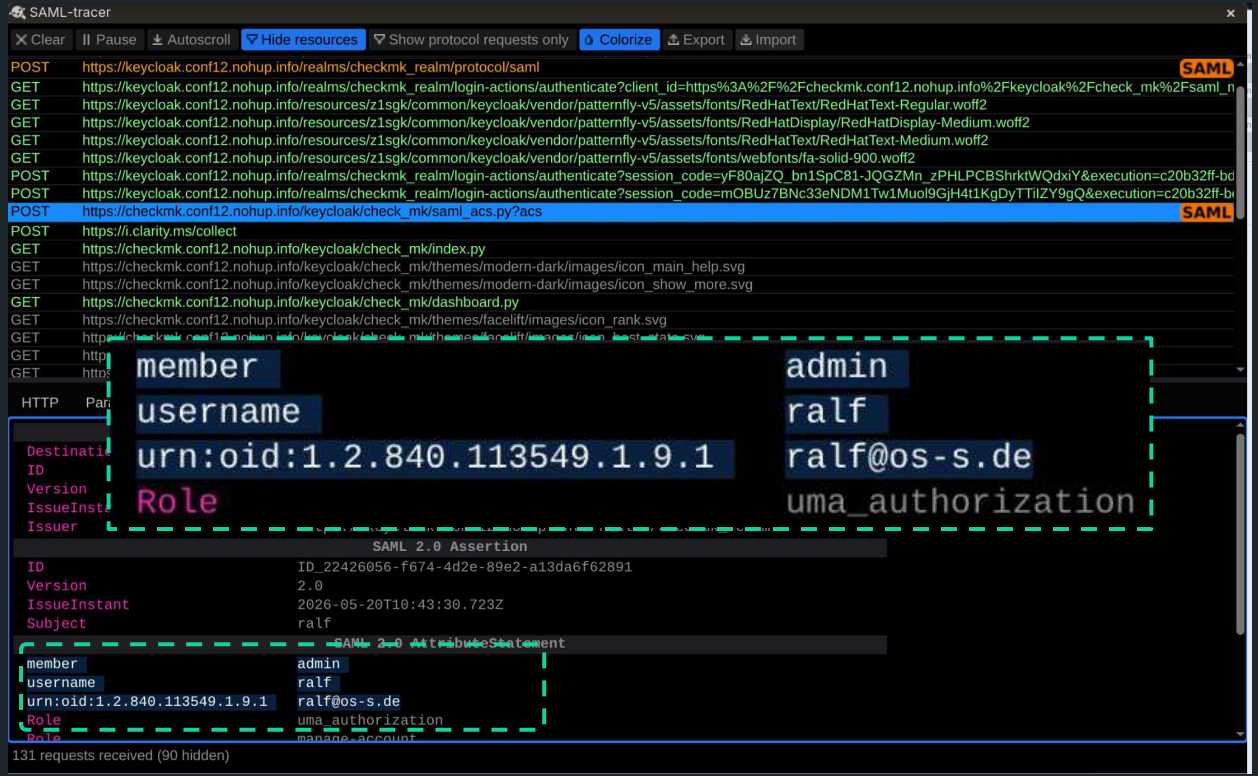
Enforce global MFA with Keycloak

Per realm or user

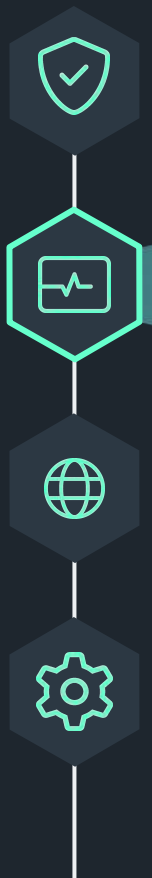




Troubleshooting with SAML Tracer browser plugin



Software deployment



Authentication
Security begins with authentication

Software Deployment
Our bakery is a software deployment system

Network Isolation
Network isolation is good practice

Updates
Only Updates fix found vulnerabilities!

Bakery

Great for supply chain attacks!

Automated

Software deployment

Successful attacks
are catastrophic

Bakery

Great for supply chain attacks!

Automated

Software deployment

Successful attacks are catastrophic

You are responsible for the integrity of the agent package!

Signing only protects these files during storage and for the transport over the network.

The files used to build the agent are not protected.

Hardening the Bakery

Harden the CMK Server

Console Access

- Root only for Updates
  - Use site user

Web Access

- SSO and MFA
  - Ensure trusted users

Checkmk

Bakery

- Non-root agent
- Separate signature keys
- HTTPS

Additional

- Monitor ~/local and MKPs
- File Integrity Monitor

Network isolation

Authentication
Security begins with authentication

Software Deployment
Our bakery is a software deployment system

Network Isolation
Network isolation is good practice

Updates
Only Updates fix found vulnerabilities!

Network isolation

VLANs

Put Servers on
separate VLANs

Network isolation

VLANs

Put Servers on separate VLANs

Users

Restrict the synced Users

Remove the automation user if not needed

Network isolation

VLANs

Put Servers on separate VLANs

Users

Restrict the synced Users

Remove the automation user if not needed

Connections

Central to Remote (Livestatus, Distributed Setup, MQTT etc.)

Remote to Central (Agent Bakery)

Use TLS

Updates

Authentication
Security begins with authentication

Software Deployment
Our bakery is a software deployment system

Network Isolation
Network isolation is good practice

Updates
Only Updates fix found vulnerabilities!

Checkmk vulnerabilities

33 CVEs

2024

1 high (CVSS 4.0)

23 CVEs

2025

5 high (CVSS 4.0)

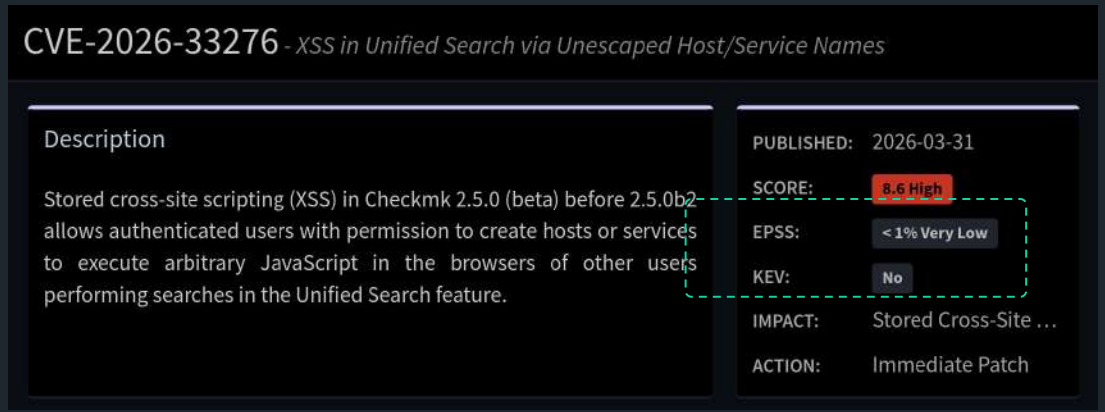
14 CVEs

2026

6 high (CVSS 4.0)

Install updates !

- https://thl-cmk.hopto.org/checkmk/checkmk/checkmk_update
- Risk based prioritization
  - Known Exploit Vulnerability (KEV)
  - Exploitability (EPSS)
    - Exploit Prediction Scoring System (EPSS) is a data-driven machine-learning model that estimates the probability that a published CVE will be exploited in the wild in the next 30 days
- Contextual analysis
  - Feature used?



Goals accomplished

Authentication

Security begins with authentication

Software Deployment

Our bakery is a software deployment system

Network Isolation

Network isolation is good practice

Updates

Only Updates fix found vulnerabilities!

Checkmk Conference #12