Stash it Safe

Die Bedeutung von Credential Storage in Vaults im DevOps Prozess

SWISS IT SECURITY
PART OF SWISS IT SECURITY GROUP

JAVA USER GROUP CH

Präsentiert für

Java User Group CH

Zürich, 22.06.2023

Agenda

SWISS IT SECURITY
PART OF SWISS IT SECURITY GROUP

- Kurze (!) Vorstellung
- Credential-Verwaltung im Kontext DevOps
- Repositories are getting breached…
- … and data is being stolen
- How it is happening
- Credential-Security by Design
- Demotime!

Kurze (!) Vorstellung

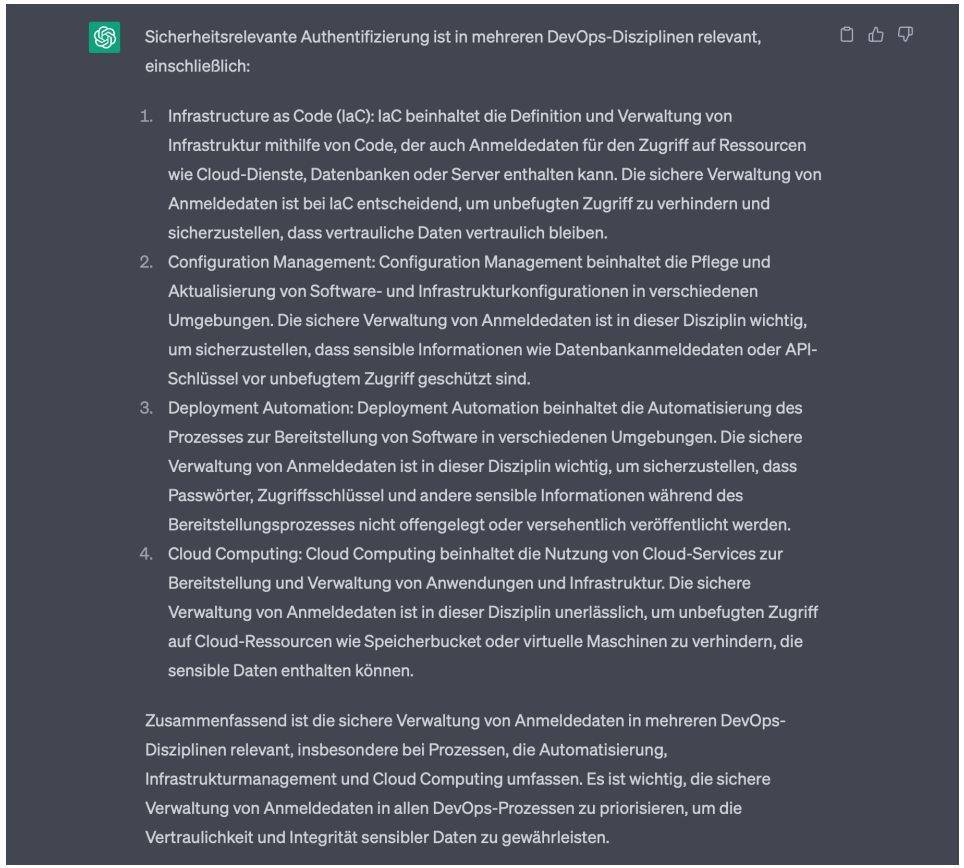
- Stephan Sann
  - Senior IT Security Consultant (PAM) bei der SITS AG
  - CISSP®, CCSP®
  - Java Enthusiast seit 2002
  - LinkedIn: https://www.linkedin.com/in/stephan-sann/

Credential-Verwaltung im Kontext DevOps

SWISS IT SECURITY
PART OF SWISS IT SECURITY GROUP

DevOps Disziplinen

- Continuous Integration (CI)
- Continuous Delivery (CD)
- **Infrastructure as Code (IaC)**
- **Configuration Management**
- **Deployment Automation**
- Monitoring and Logging
- **Cloud Computing**
- Security and Compliance
- Collaboration and Communication
- Agile Development Processes



Sicherheitsrelevante Authentifizierung ist in mehreren DevOps-Disziplinen relevant, einschließlich:

1. Infrastructure as Code (IaC): IaC beinhaltet die Definition und Verwaltung von Infrastruktur mithilfe von Code, der auch Anmeldedaten für den Zugriff auf Ressourcen wie Cloud-Dienste, Datenbanken oder Server enthalten kann. Die sichere Verwaltung von Anmeldedaten ist bei IaC entscheidend, um unbefugten Zugriff zu verhindern und sicherzustellen, dass vertrauliche Daten vertraulich bleiben.
2. Configuration Management: Configuration Management beinhaltet die Pflege und Aktualisierung von Software- und Infrastrukturkonfigurationen in verschiedenen Umgebungen. Die sichere Verwaltung von Anmeldedaten ist in dieser Disziplin wichtig, um sicherzustellen, dass sensible Informationen wie Datenbankanmeldedaten oder API-Schlüssel vor unbefugtem Zugriff geschützt sind.
3. Deployment Automation: Deployment Automation beinhaltet die Automatisierung des Prozesses zur Bereitstellung von Software in verschiedenen Umgebungen. Die sichere Verwaltung von Anmeldedaten ist in dieser Disziplin wichtig, um sicherzustellen, dass Passwörter, Zugriffsschlüssel und andere sensible Informationen während des Bereitstellungsprozesses nicht offengelegt oder versehentlich veröffentlicht werden.
4. Cloud Computing: Cloud Computing beinhaltet die Nutzung von Cloud-Services zur Bereitstellung und Verwaltung von Anwendungen und Infrastruktur. Die sichere Verwaltung von Anmeldedaten ist in dieser Disziplin unerlässlich, um unbefugten Zugriff auf Cloud-Ressourcen wie Speicherbucket oder virtuelle Maschinen zu verhindern, die sensible Daten enthalten können.

Zusammenfassend ist die sichere Verwaltung von Anmeldedaten in mehreren DevOps-Disziplinen relevant, insbesondere bei Prozessen, die Automatisierung, Infrastrukturmanagement und Cloud Computing umfassen. Es ist wichtig, die sichere Verwaltung von Anmeldedaten in allen DevOps-Prozessen zu priorisieren, um die Vertraulichkeit und Integrität sensibler Daten zu gewährleisten.

Repositories are getting breached…

SWISS IT SECURITY
PART OF SWISS IT SECURITY GROUP

sec.okta.com/articles/2022/12/okta-code-r

{okta} OKTA HOME

December 21, 2022

Okta Code Repositories

Okta

SUMMARY: In alignment with our core value of transparency, we are sharing context and det
recent security event affecting Okta code repositories. There is no impact to any customers,
HIPAA, FedRAMP or DoD customers. No action is required by customers.

SCOPE: The security event detailed below pertains to Okta Workforce Identity Cloud (WIC) c
repositories. It does not pertain to any Auth0 (Customer Identity Cloud) products.

EVENT: In early December 2022, GitHub alerted Okta about possible suspicious access to C
repositories. Upon investigation, we have concluded that such access was used to copy Okt

www.cybersecuritydive.com/news/slack-tok

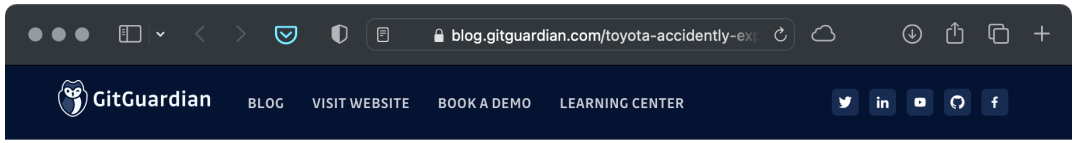
CYBERSECURITY DIVE Deep Dive Library Topics Sign up

DIVE BRIEF

Slack employee tokens stolen, GitHub repository breached

Published Jan. 5, 2023

… and data is being stolen



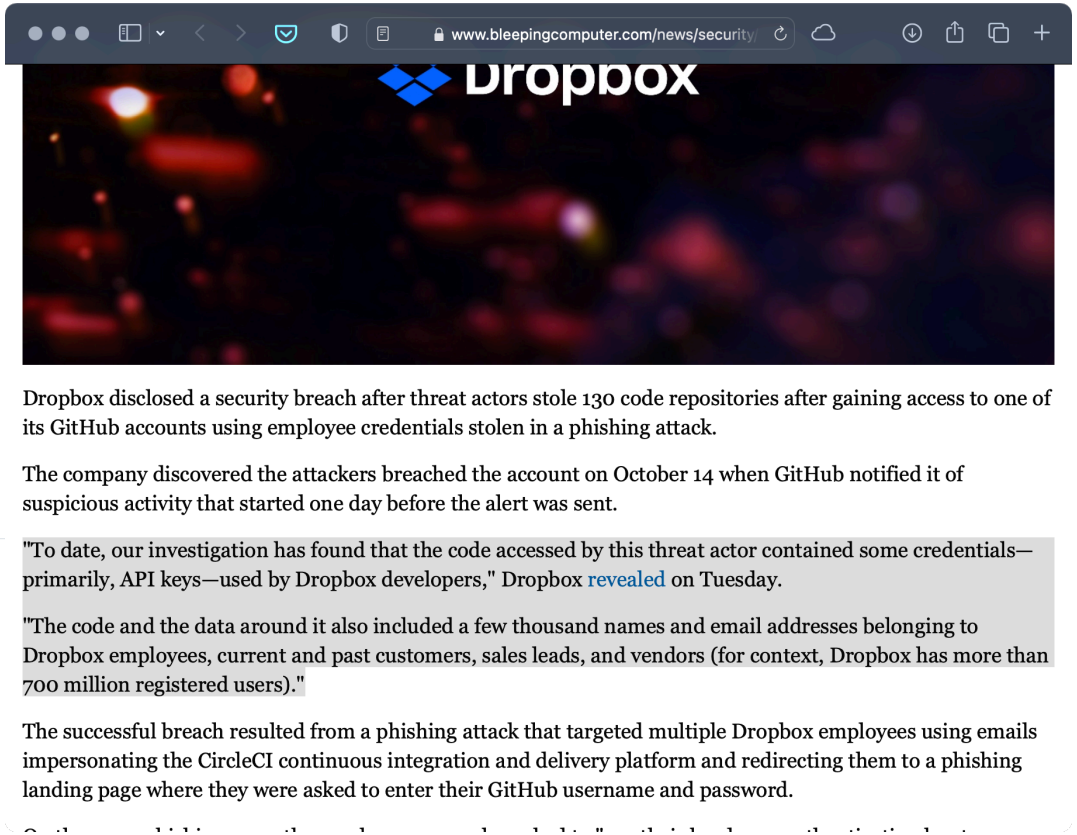
BREACH EXPLAINED

Toyota Suffered a Data Breach by Accidentally Exposing A Secret Key Publicly On GitHub

On October 7th, Toyota revealed a partial copy of their T-Connect source code had been accidentally exposed for 5 years, including access to data for over 290,000 customers.

DWAYNE MCDANIEL
11 OCT 2022 · 4 MIN READ

Share



Dropbox disclosed a security breach after threat actors stole 130 code repositories after gaining access to one of its GitHub accounts using employee credentials stolen in a phishing attack.

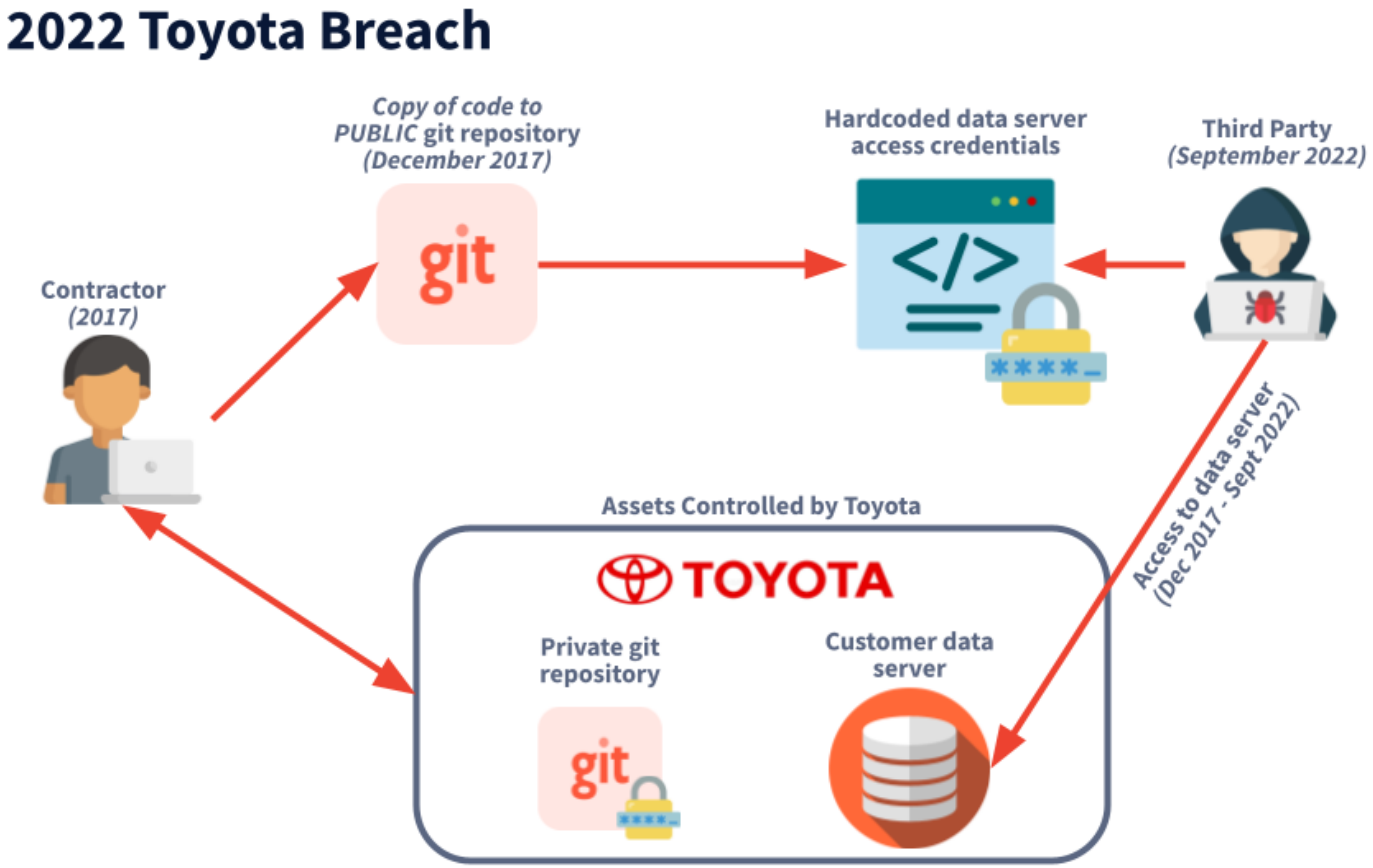
The company discovered the attackers breached the account on October 14 when GitHub notified it of suspicious activity that started one day before the alert was sent.

"To date, our investigation has found that the code accessed by this threat actor contained some credentials—primarily, API keys—used by Dropbox developers," Dropbox revealed on Tuesday.

"The code and the data around it also included a few thousand names and email addresses belonging to Dropbox employees, current and past customers, sales leads, and vendors (for context, Dropbox has more than 700 million registered users)."

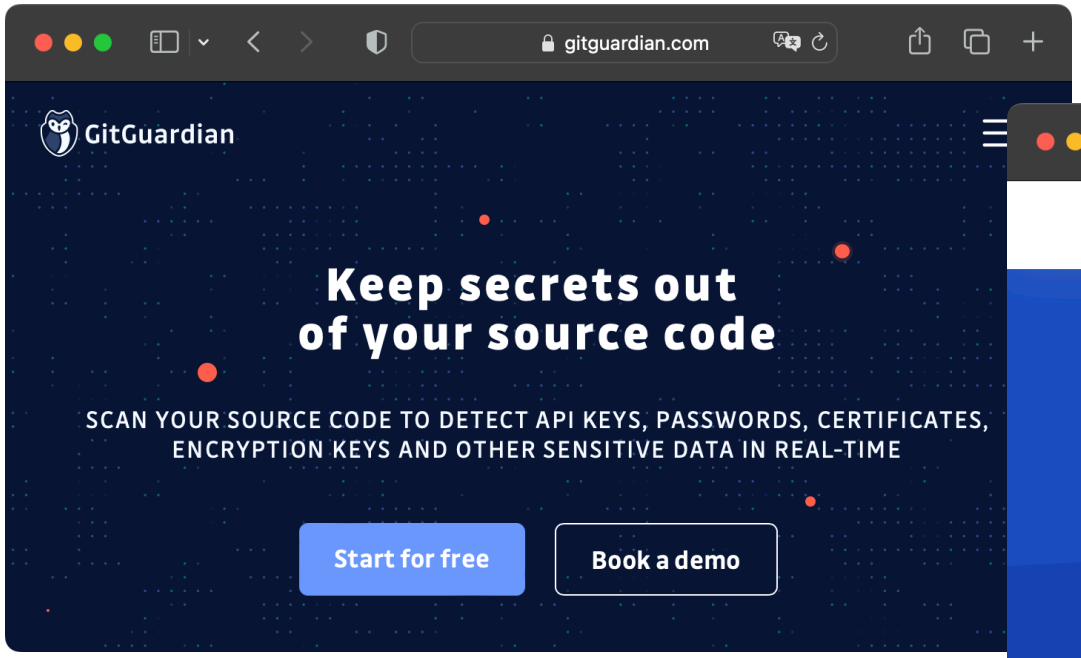
The successful breach resulted from a phishing attack that targeted multiple Dropbox employees using emails impersonating the CircleCI continuous integration and delivery platform and redirecting them to a phishing landing page where they were asked to enter their GitHub username and password.

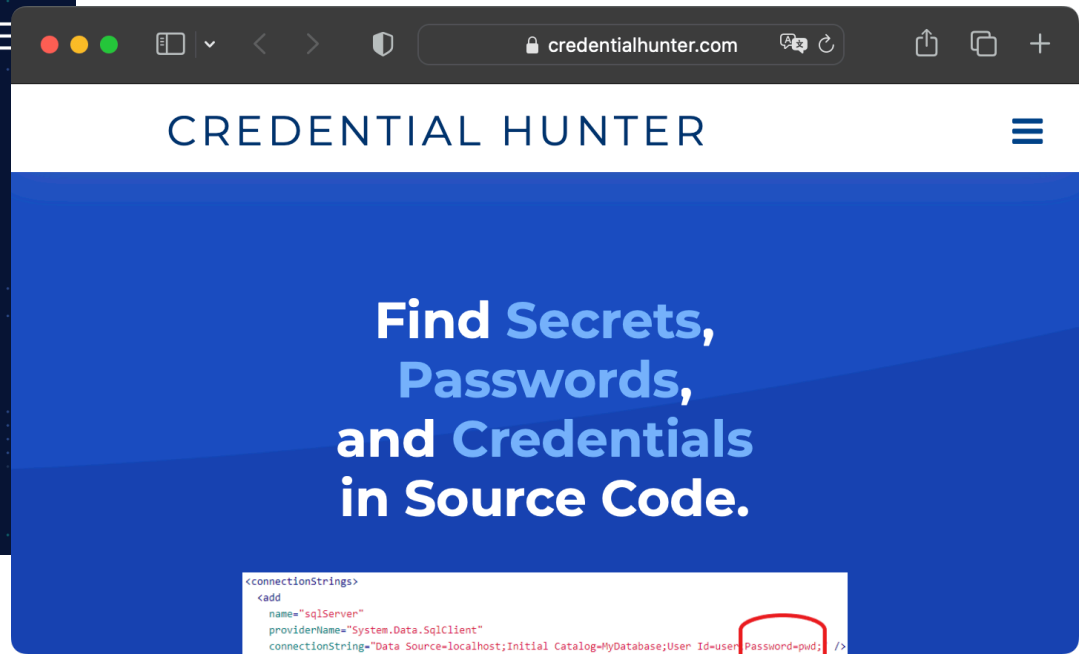
How it is happening

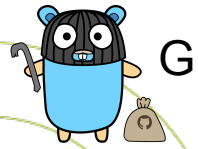


Pro-/Reactive Services & Tools

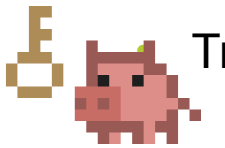
SWISS IT SECURITY
PART OF SWISS IT SECURITY GROUP







Gitrob: https://github.com/michenriksen/gitrob

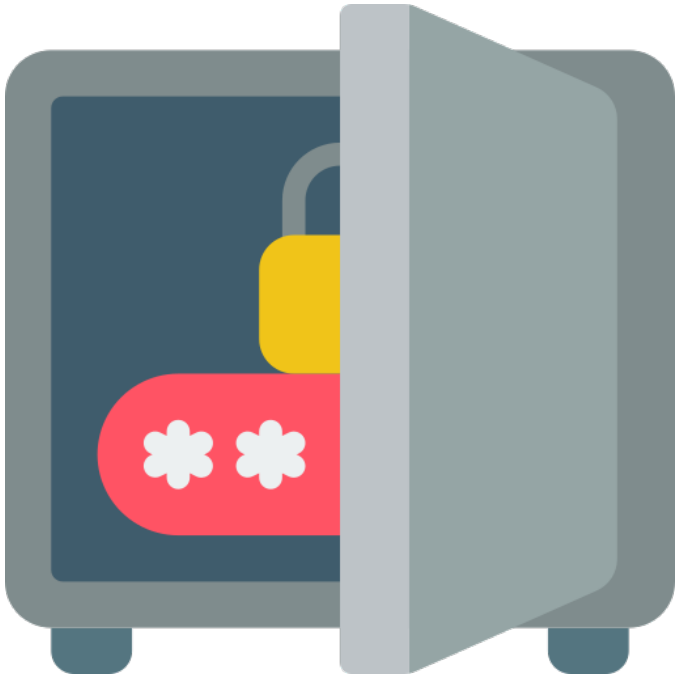


TruffleHog: https://github.com/trufflesecurity/trufflehog

Credential-Security by Design

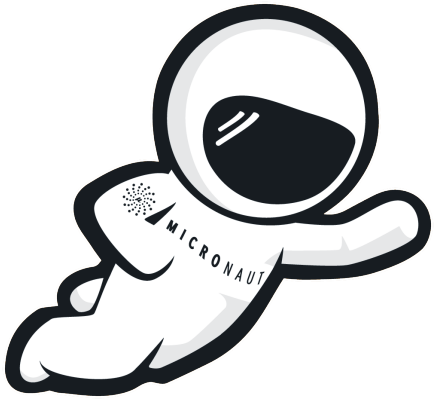
SWISS IT SECURITY
PART OF SWISS IT SECURITY GROUP

- Keine Secrets (Passwörter, Tokens, Keys) im Code oder in Properties-Files
- Sichere Verwahrung von Secrets in digitalen Vaults (verschlüsselt)
- Abfrage via API
- Zugriffskontrolle via Policies



Log in icons created by Smashicons - Flaticon
(https://www.flaticon.com/free-icons/log-in)

Demotime!



MySQL®

SWISS IT SECURITY
PART OF SWISS IT SECURITY GROUP

eclipse

Maven™

HashiCorp Vault

Jenkins

Maven™

Gitea

Demotime!

SWISS IT SECURITY
PART OF SWISS IT SECURITY GROUP

	DEV	TEST	QUAL	PROD
DB Server	localhost	devops.pamlab.sits	?	?
Account	johndoe	jenkinstest	?	?
Password	**********	**********	**********	**********
Build in	Eclipse	Jenkins	Jenkins	-

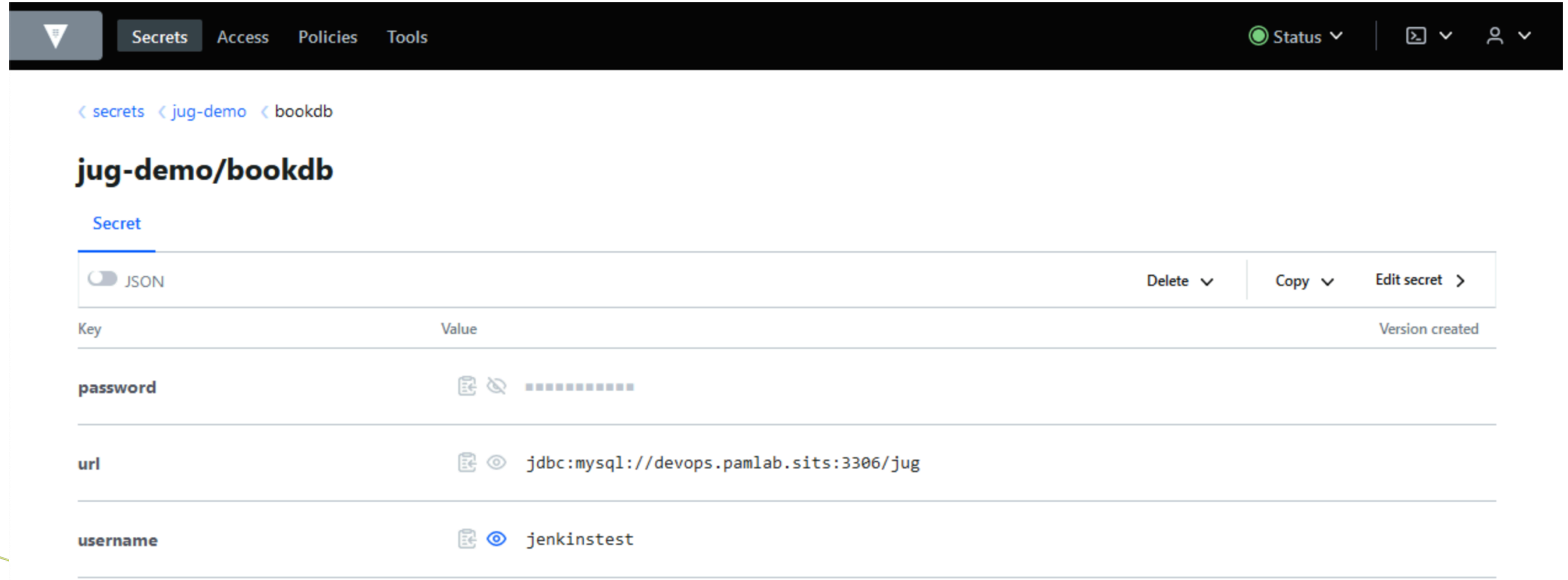
Warum nicht Jenkins Credentials verwenden?

SWISS IT SECURITY
PART OF SWISS IT SECURITY GROUP

- Der Vault kann einfach Credentials rotieren (ggf. Policy-basiert)
- Einfache zentrale Verwaltung von Secrets
- Bei Verwendung von mehreren Jenkins-Controllern kann ein Credential an einem Ort gehalten und allen Jenkins-Controllern verwendet werden

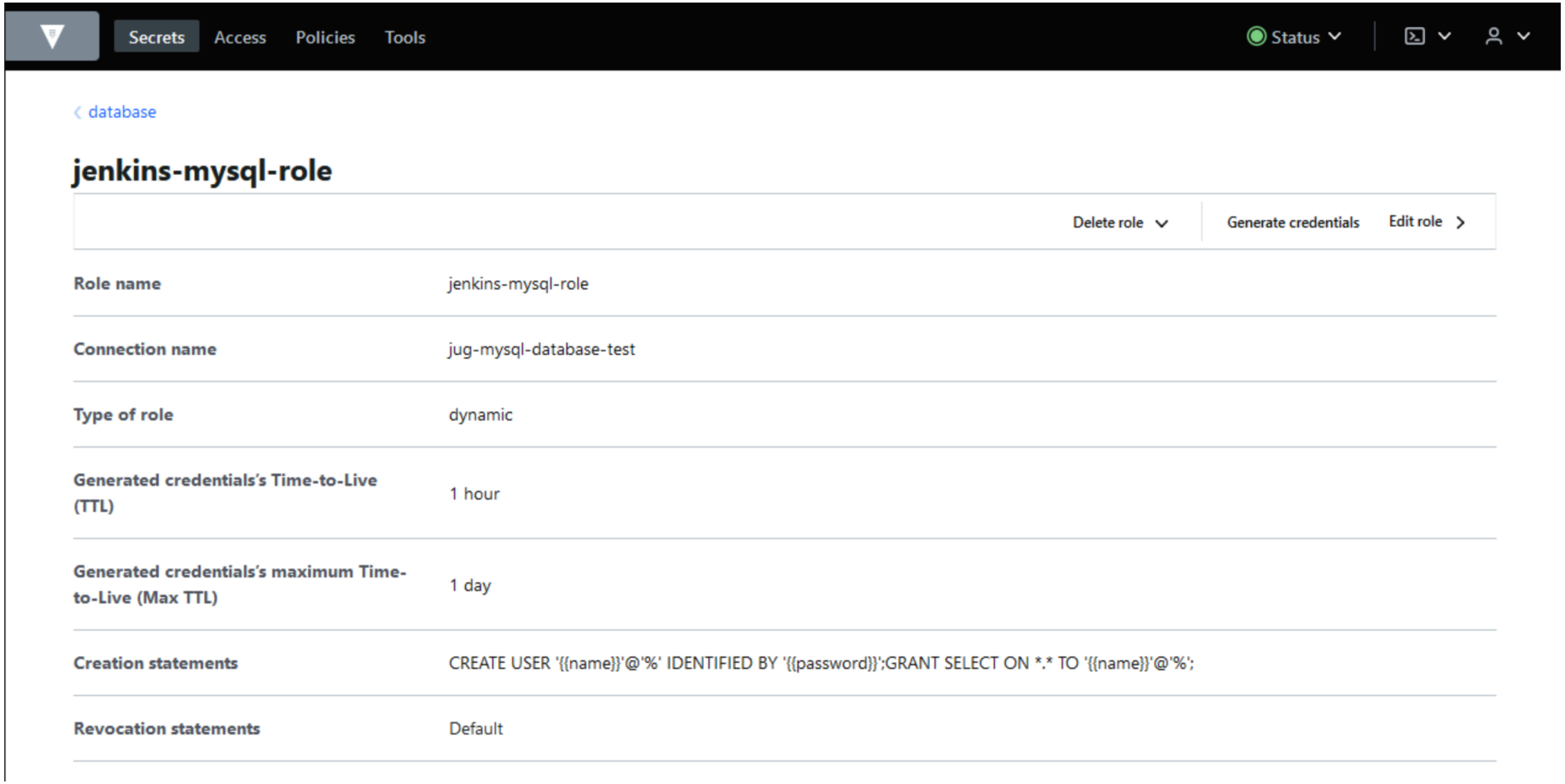
Key/Value Secrets Engine

SWISS IT SECURITY
PART OF SWISS IT SECURITY GROUP



Database Secrets Engine

SWISS IT SECURITY
PART OF SWISS IT SECURITY GROUP



Fragen?

Herzlichen Dank für Ihre Aufmerksamkeit!

SWISS IT SECURITY
PART OF SWISS IT SECURITY GROUP

Ihre Ansprechperson

Swiss IT Security AG
Stephan Sann
Senior PAM Consultant

stephan.sann@sits.ch
www.sits.ch