TeleTrusT-Konferenz 2025

Berlin, 02.07.2025

Chancen und Grenzen von KI im Berechtigungsmanagement

Prabhakar Mishra, CyberDesk

Problem

>95%

CyberDesk

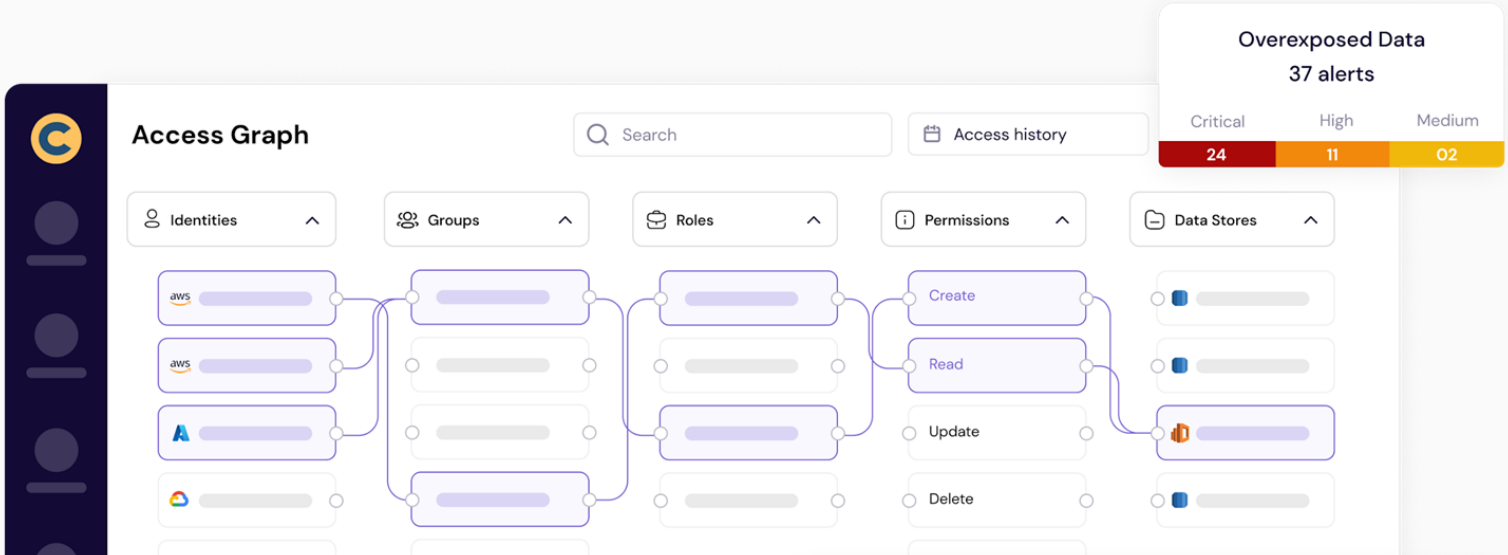
Datenzugriff durch menschliche und nicht-menschliche Identitäten ist unsere größte Schwachstelle.

KI-Agenten machen alles nur noch schlimmer.

Unsere Lösung

CyberDesk

KI ist die Lösung, um granular zu steuern, wer wie auf welche Daten zugreifen kann.



Über uns

Ein Team, ein Ziel: Der Schutz Ihres Datenzugriffs.

Gründer

Dr. Tobias Lieberum

CEO

- Ex McKinsey
- Promotion in Operations Management

Prabhakar Mishra

CTO

- Ex Morgan Stanley, Accenture
- Zertifizierter Cyber-sicherheitsexperte

Team

Cybersicherheitsenthusiasten von

Berater (Auswahl)

Benjamin Bachmann
Director Group InfoSec Bilfinger

Jimmy Heschl
Global Head Digital Sec Red Bull

Martin Jetter
SVP & Chairman EMEA IBM i.R.

Ümit Kuşdoğan
CISO ADAC

Matthias Muhlert
CISO Oetker-Gruppe

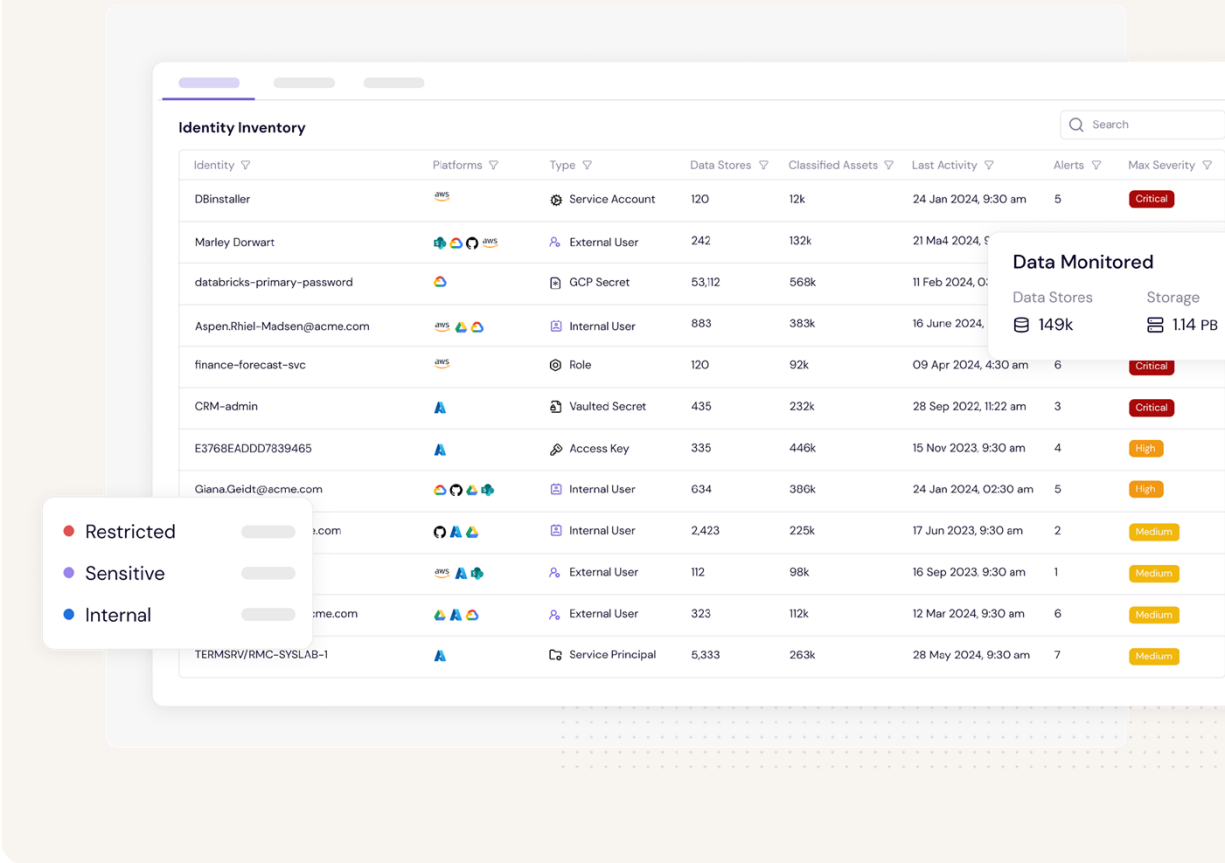
Alexander Zhitenev
Head of IT Security IFCO

Unterstützt von

CyberDesk

Module

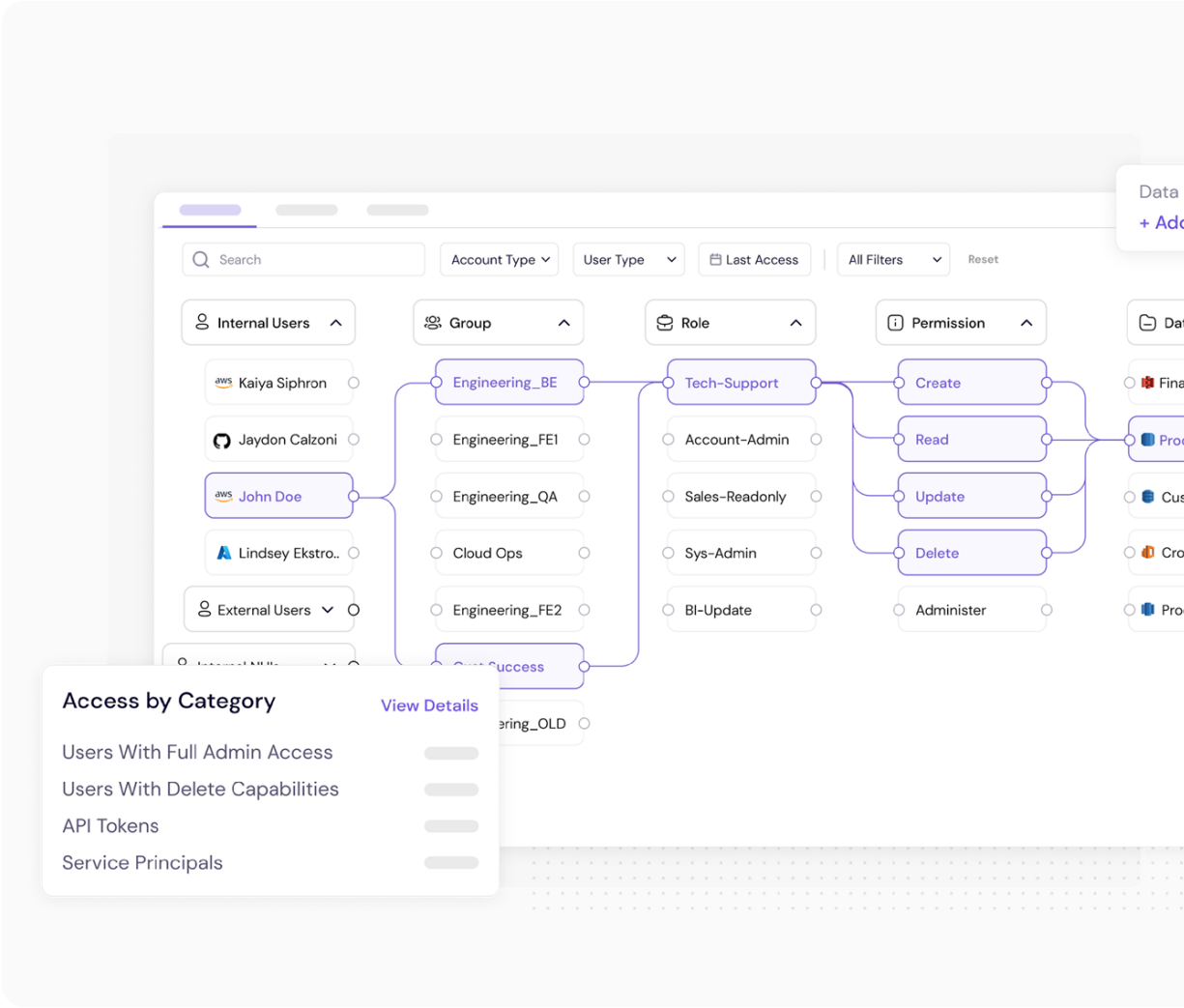
Daten- & Identitäts-inventar



CyberDesk

Module

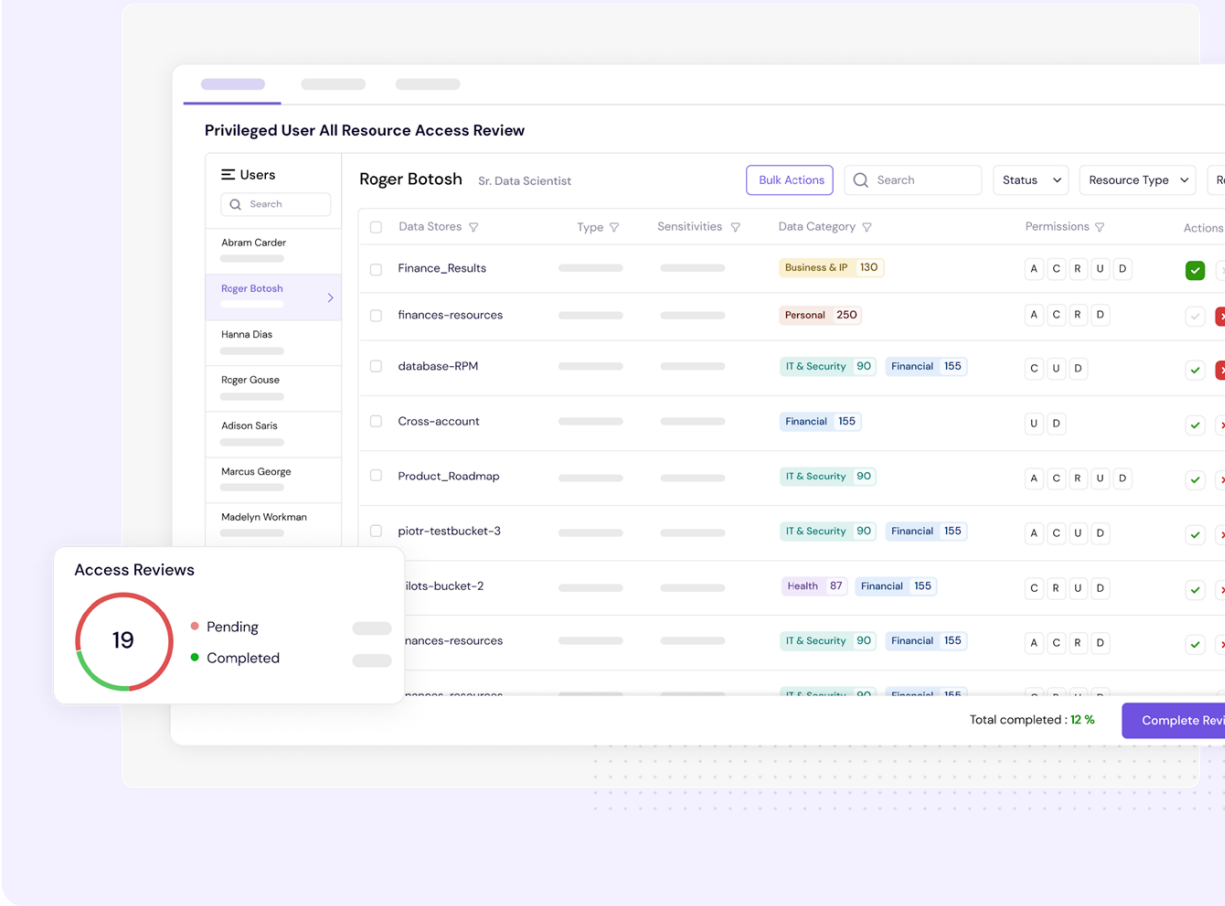
Granularer Berechti-gungsgraph



CyberDesk

Module

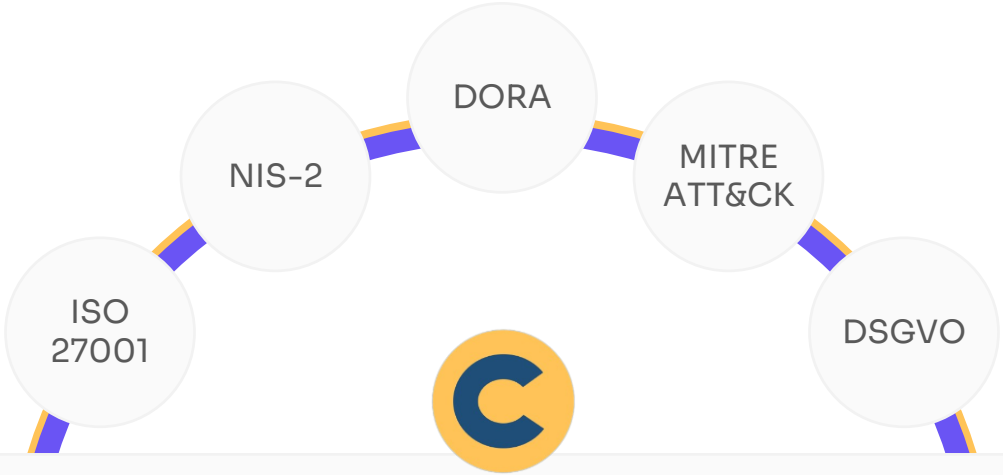
KI-basierte Risiko-behebung



CyberDesk

Integrationen

CyberDesk



CyberDesk Plattform

Standardintegrationen

Identitäts-Provider

Infra-struktur

SaaS Lösungen

Data Lakes

snowflake

databricks

Sicherheits-lösungen

Kundenspezifisch

Offene API

Filters

millio

Show only highlighted nodes

Graph history

Data Stores: arn:aws:s3:::million-plus-objects

Clear all

Dashboard

Alerts

Access Graph

Inventory

Workflows

Settings

Docs

Logout

Identities Data View

Conditions

Last Activity Date

Storage Type

User Type

Sensitivity

Data Category

User

Service Account

Group

Role

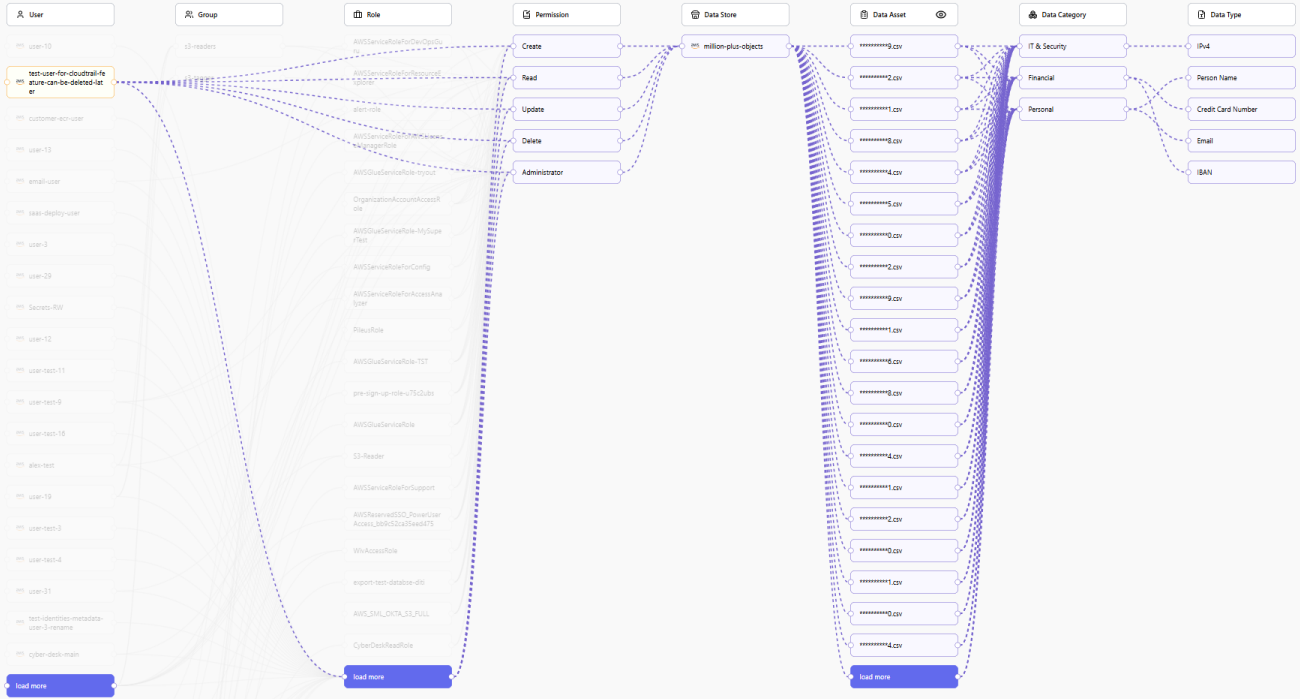
Permission

Data Stores

Search storage

million-plus-objects

Data Asset

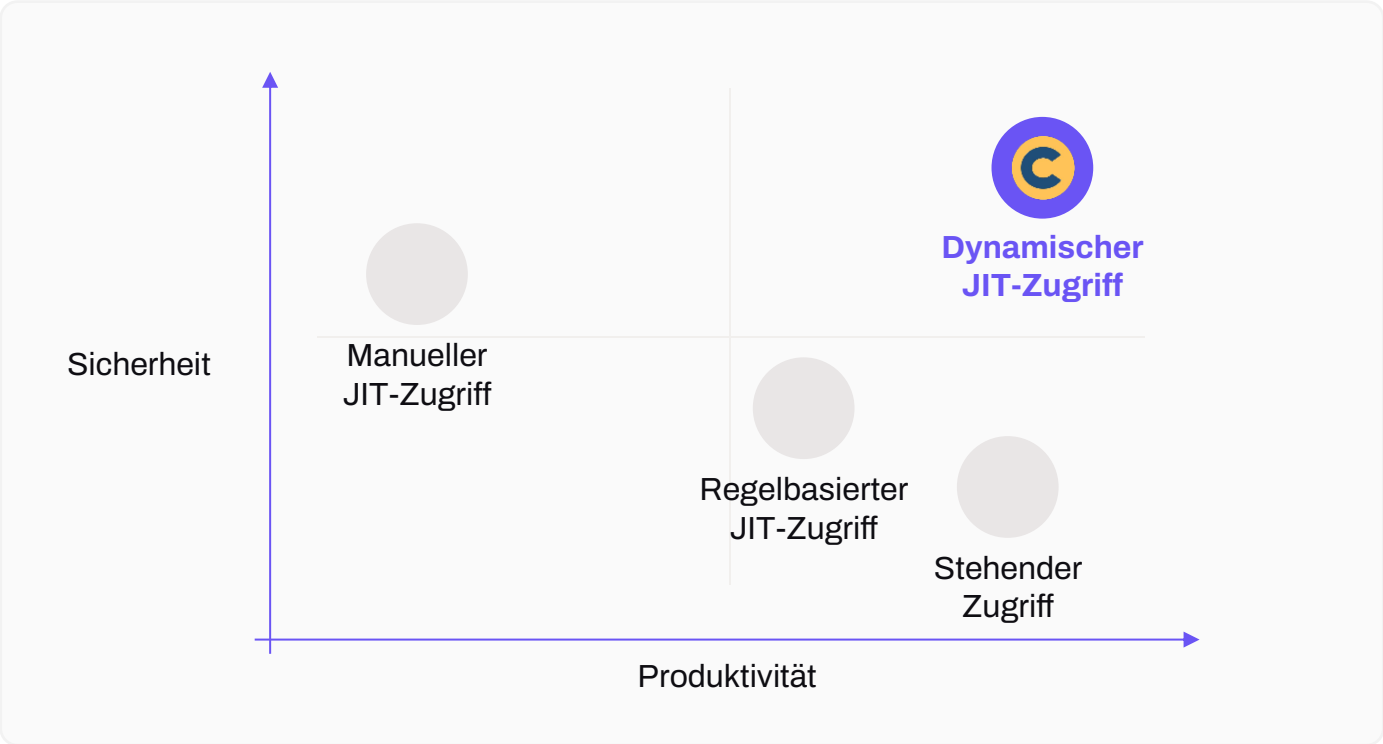


React Flow

Zukunft

CyberDesk

KI ermöglicht Just-in-Time (JIT) Datenzugriff



CyberDesk

Autorisierung trifft Machine Learning

So revolutioniert Machine Learning die Autorisierung:

🚨 Anomalieerkennung

→ Erkennt ungewöhnliche Zugriffsmuster und löst automatisch Warnungen aus

📊 Verhaltensanalyse

→ Lernt typische Nutzeraktivitäten, um Identitätsdiebstahl oder Insider-Bedrohungen frühzeitig zu erkennen

🧑‍🚀 Manipulationserkennung bei Berechtigungen

→ Überwacht Änderungen an Zugriffsrechten in Echtzeit und meldet unautorisierte Zugriffe

🎭 Erkennung von Spoofing & Impersonation

→ Nutzt biometrische und verhaltensbasierte Daten zur Identifikation echter Nutzer

🕹️ Kontextabhängige Zugriffskontrolle

→ Bewertet Standort, Gerät und Zeitpunkt für präzisere Zugriffsentscheidungen

⚠️ Risikobasierte Authentifizierung

→ Dynamische Zugriffsanpassung auf Basis individueller Risikobewertungen

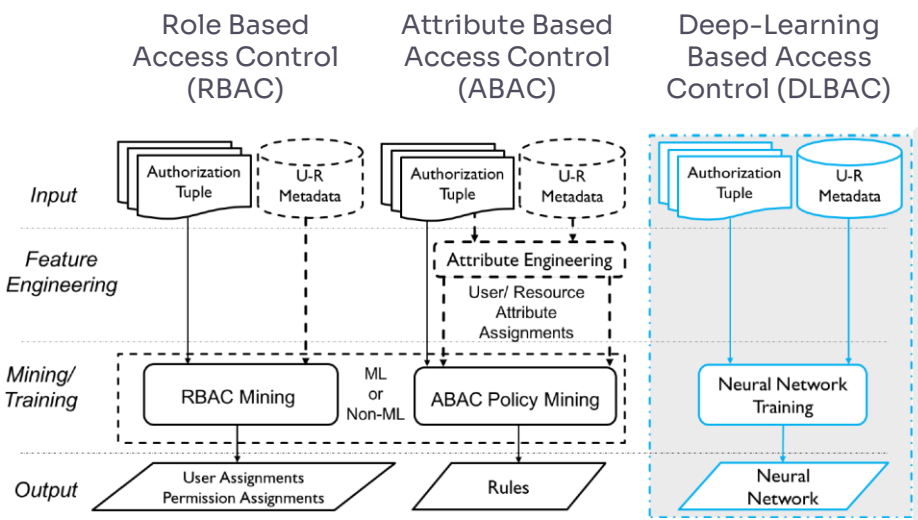
Umsetzung

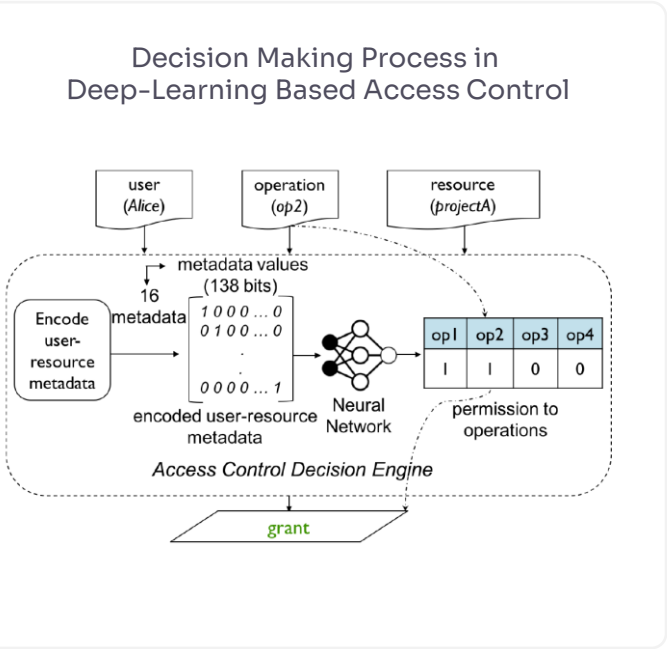
CyberDesk

KI-Mitarbeiter entlasten die IT-Abteilung

CyberDesk

Deep Learning basierte Zugriffskontrolle





POL-02- Finance Department Access Policy

Role-Based Access Permissions

3.1. Junior Financial Analyst
- Responsibilities: Data analysis, financial reporting, expense tracking.
- Access: Read-Only: Transaction logs, summary reports, and financial performance dashboards. No Access: Customer account details, personal information, or transaction authorizations.
- Restrictions: No download capabilities for sensitive data; access limited to view-only dashboards. Access to reports limited to non-personally identifiable information (PII).

3.2. Senior Financial Analyst
- Responsibilities: Comprehensive financial analysis, forecasting, budgeting.
- Access: Read/Write: Budgeting and forecasting tools, aggregated financial reports. Read-Only: General ledger, high-level customer segmentation data (no PII).
- Restrictions: No access to individual transaction data or customer PII. Restricted ability to export sensitive data (subject to audit trail tracking).

3.3. Financial Manager
- Responsibilities: Oversee budgeting, audits, and reporting; interact with internal auditors.
- Access: Read/Write: Departmental budgets, audit logs, forecasting applications, and financial reports. Read-Only: Aggregated customer data for financial trend analysis (no individual customer data).
- Restrictions: No direct access to customer PII or individual transaction details. Must route requests for sensitive data through Data Protection Officer (DPO) and obtain manager approval.

3.4. Compliance Officer (Finance)
- Responsibilities: Ensure financial regulatory compliance and audit preparation.
- Access: Read-Only: All financial data necessary for compliance audits, excluding individual customer PII. Restricted Access: Aggregate customer information for compliance reporting, without the ability to drill down to individual accounts.
- Restrictions: No write permissions to any financial records. Must log all access to compliance reports for audit tracking.

3.5. Finance Director
- Responsibilities: Oversee all finance department operations, strategic planning, high-level reporting.
- Access: Read/Write: Access to all financial reports, budgeting tools, forecasting applications, and audit logs. Restricted Access: Customer financial data on an aggregated level only.
- Restrictions: Can access customer data summaries for strategic reporting but cannot view individual customer details. All actions logged and auditable, with dual-authorization for sensitive actions.

Deviations

Group Customer Success — Closed
ID: ABC5143255
Engineering : This permission is not listed in the LP policy for any job title in Finance Department
more

Identity Sarah Miller — Ticket Created
ID: ABC5143255
Engineering : This permission is not listed in the LP policy for any job title in Finance Department
more

Identity John Doe — Open
ID: ABC5143255
Engineering : This permi
for any job title in Financ
Engineering : This permi
for any job title in Financ
less

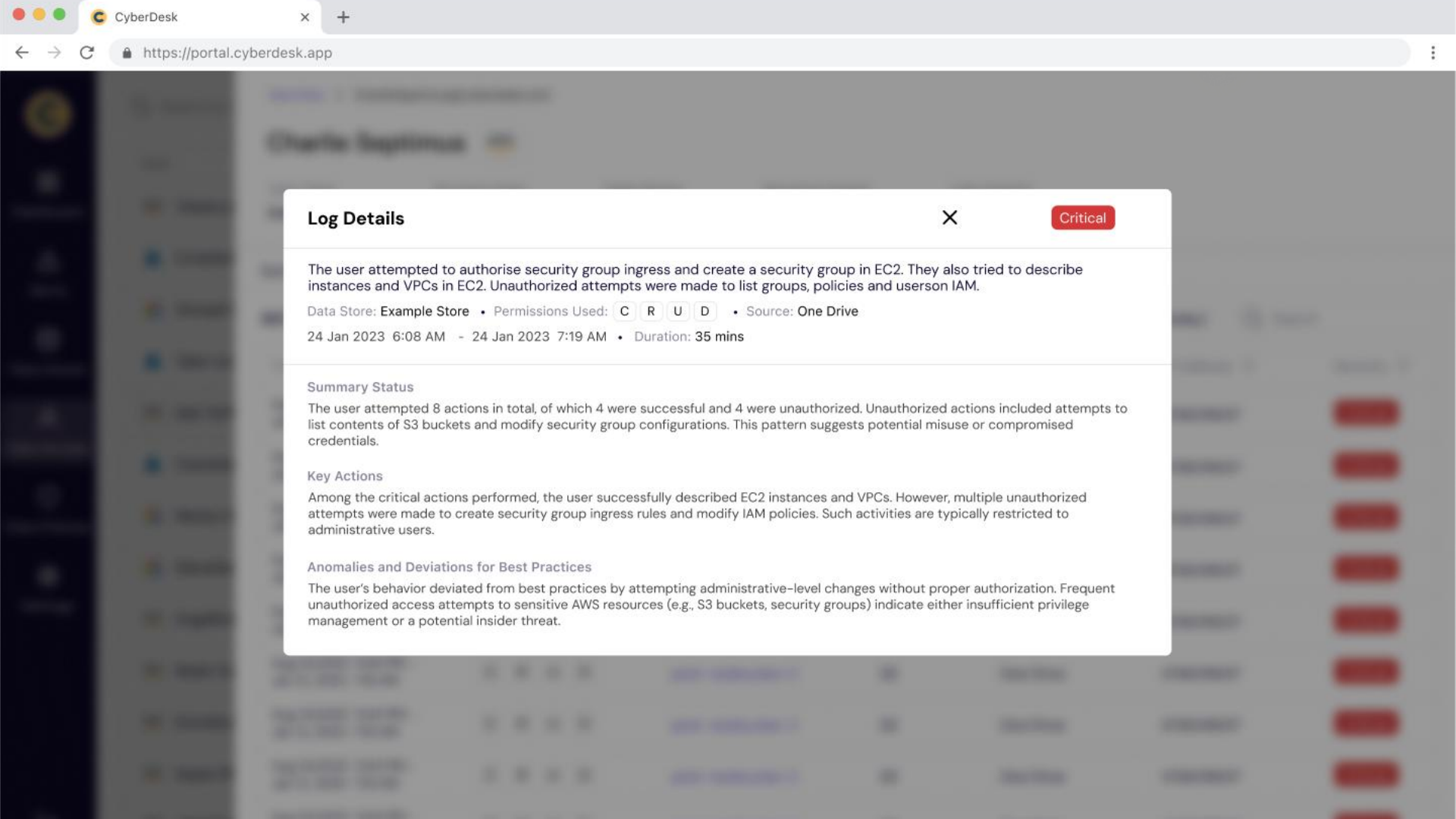
- Create a JIRA ticket
- Notify via email
- Notify via Slack
- Close as Risk Accepted
- Close as False Positive
- Close as Remediated

Identity Sarah Miller
ID: ABC5143255
Engineering : This permi
for any job title in Financ
more

Group Customer Success — Closed
ID: ABC5143255
Engineering : This permission is not listed in the LP policy for any job title in Finance Department
more

Group Customer Success — Closed
ID: ABC5143255
Engineering : This permission is not listed in
for any job title in Finance Department
more

Risk Accepted

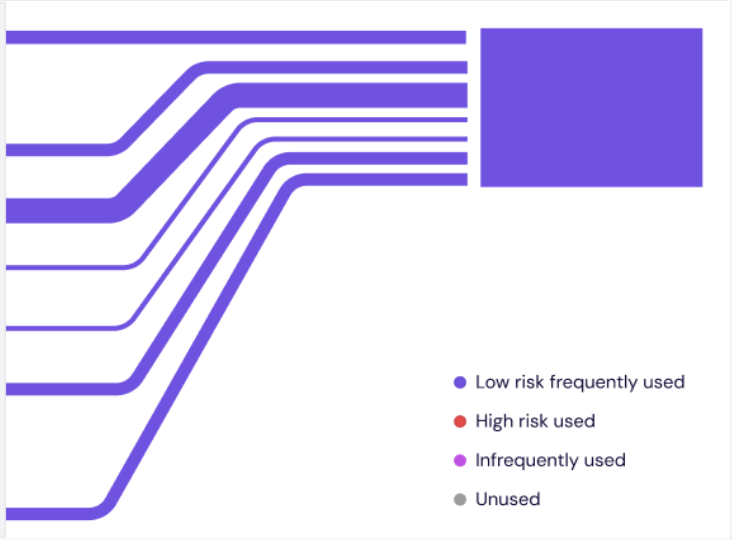

CyberDesk
https://portal.cyberdesk.app
Log Details
Critical
The user attempted to authorise security group ingress and create a security group in EC2. They also tried to describe instances and VPCs in EC2. Unauthorized attempts were made to list groups, policies and userson IAM.
Data Store: Example Store • Permissions Used: C R U D • Source: One Drive
24 Jan 2023 6:08 AM - 24 Jan 2023 7:19 AM • Duration: 35 mins
Summary Status
The user attempted 8 actions in total, of which 4 were successful and 4 were unauthorized. Unauthorized actions included attempts to list contents of S3 buckets and modify security group configurations. This pattern suggests potential misuse or compromised credentials.
Key Actions
Among the critical actions performed, the user successfully described EC2 instances and VPCs. However, multiple unauthorized attempts were made to create security group ingress rules and modify IAM policies. Such activities are typically restricted to administrative users.
Anomalies and Deviations for Best Practices
The user's behavior deviated from best practices by attempting administrative-level changes without proper authorization. Frequent unauthorized access attempts to sensitive AWS resources (e.g., S3 buckets, security groups) indicate either insufficient privilege management or a potential insider threat.

Charlie Septimus

User Type	Platforms	Manager	Data Stores	Sensitive Assets	Last Activity
Internal User	aws Azure GCP	+ Add Manager	134	663	11 Sep 2023 ; 09:54 am

10 Policies | 152 Permissions

Policy	Permissions
EC2-App-Capacity-Update	
EKS Admin	
RDS Admin	
S3 Operator	
CodePipeline Admin	
LB Admin	
DNS Operator	
VPC Admin	
Dynamo DB Admin	




siken Risiken Risiken Risiken Ris
ance Compliance Compliance Com
zen Ineffizienzen Ineffizienzen In

CyberDesk

Vielen Dank

Wir freuen uns, mit Ihnen ins Gespräch zu kommen.

tobias.lieberum@cyberdesk.app

FRAGEN & ANTWORTEN

tobias.lieberum@cyberdesk.app