

ON TOUR | NETHERLANDS



# Securing the SQL Server Data Platform

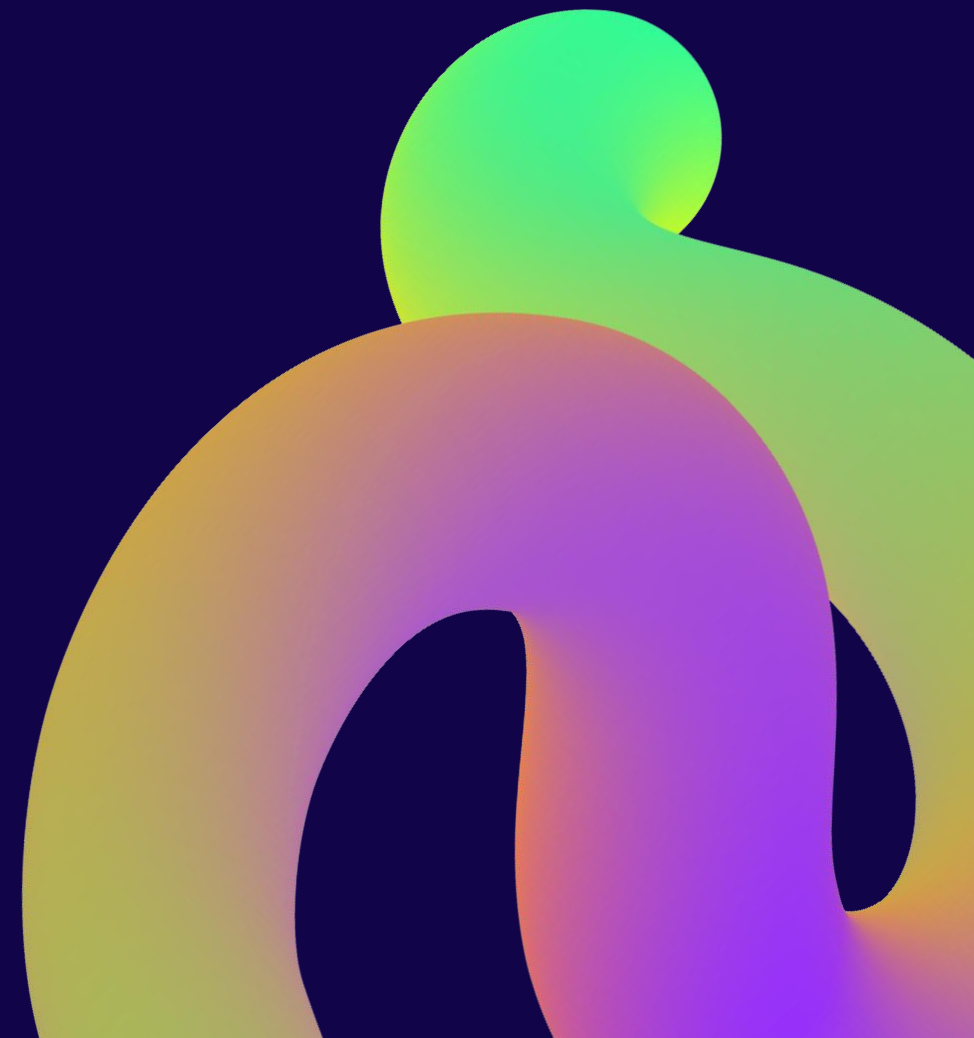
## Defining a security strategy

**Danny de Haan**

He/Him

Solutions Engineer

Redgate Software



# Danny de Haan

He/Him

Solutions Engineer  
Redgate Software



**thatinfradba@pm.me**



**/in/dannydh**



I've been working in IT for nearly 20 years in various roles. With over 15 years of experience with SQL Server, I've always placed a strong emphasis on Security, Risk Management, and Compliance for the SQL Server Data Platform. Ensuring industry best practices and regulatory requirements are followed from an infrastructural point of view.

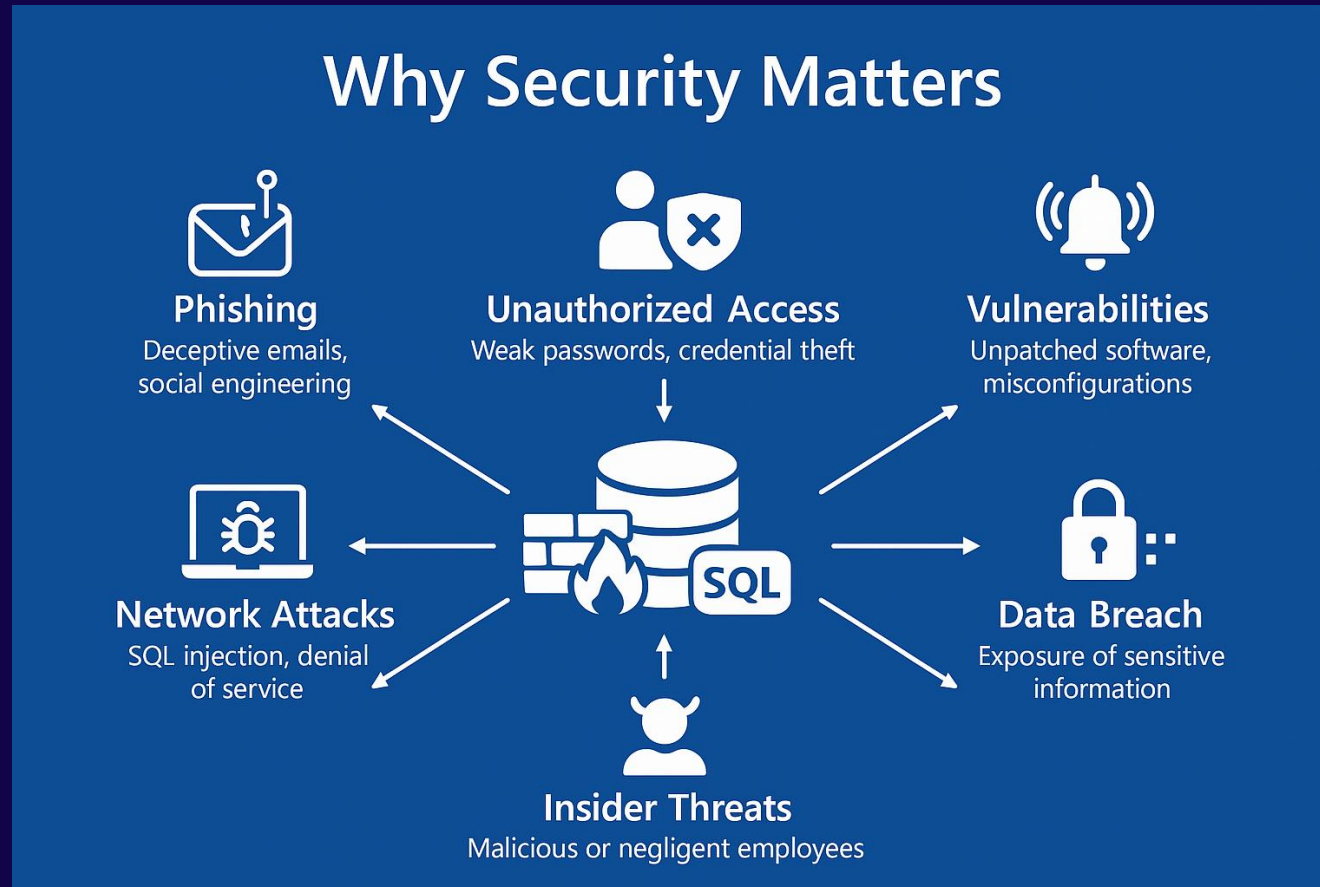
# Session Objectives

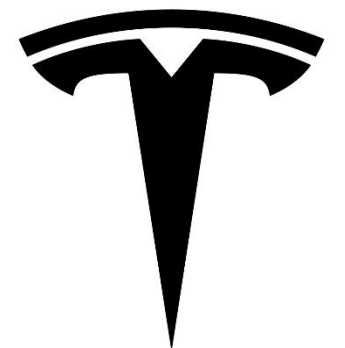
- Understanding the attack surface
- Principle of least privilege
- Monitoring & Auditing
- Defining a strategy

# Schedule

- Building your Security Strategy
- Hardening SQL Server
- Authentication & Authorization
- !! Break !!
- Encrypting SQL Server
- Monitoring, Auditing & Compliance
- Back-up & Recovery Strategies
- Tools & Resources

# Why Security Matters





TESLA



duolingo

cutout.

Lyca  
Mobile



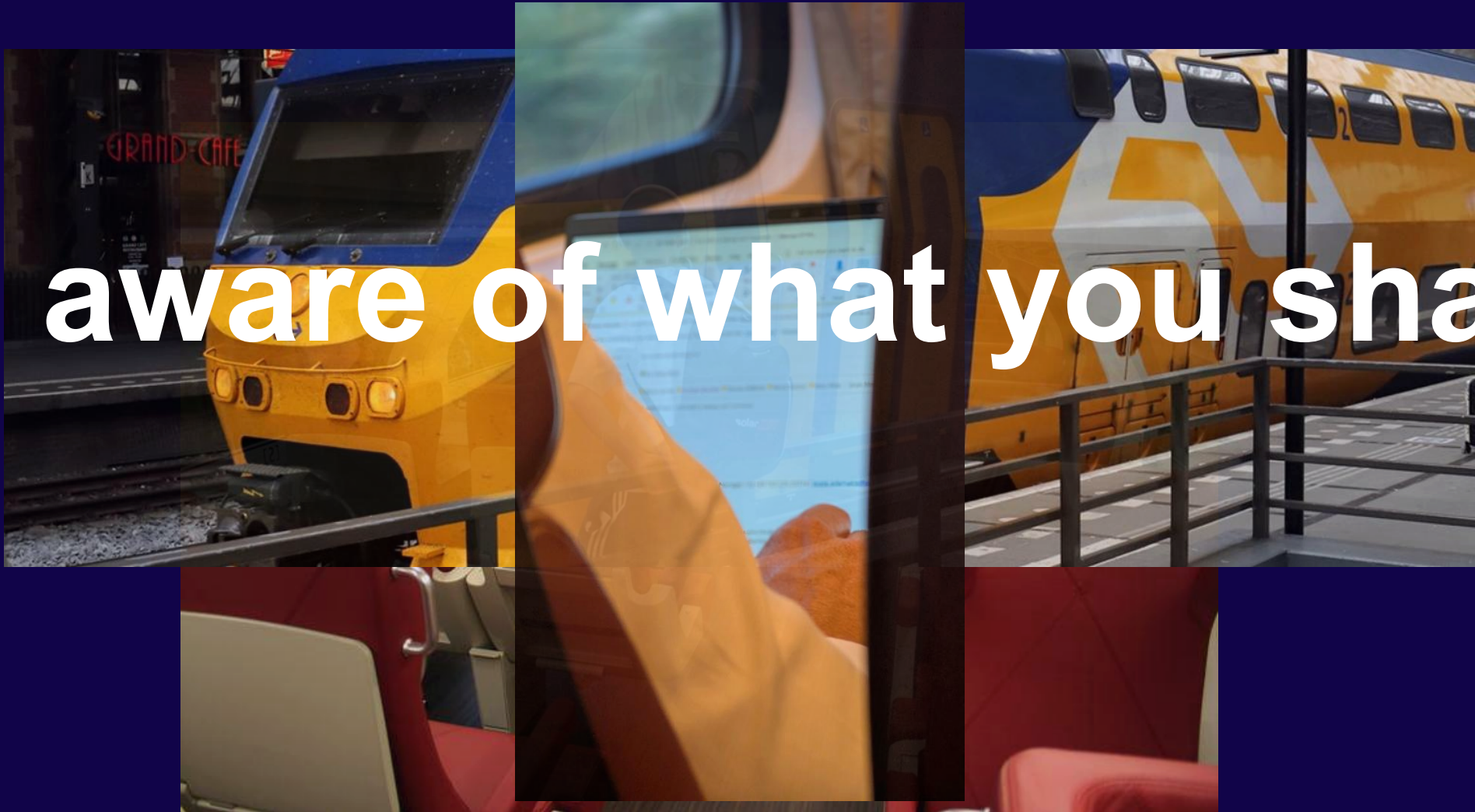
KAI

T Mobile



**“It's not a matter of if, but when...”**

**Be aware of what you share**



# Building your Security Strategy





# Security-First Mentality

- Mindset vs Mentality
- Thinking like an attacker
- 360 degree Security

# Strategy Framework

- Identify
- Assess
- Respond

# Strategy Framework

- CIA triad
  - Confidentiality
  - Integrity
  - Availability
- Risk Tolerance / Appetite

# Human Layer Security

- Training & Education
  - Educate your team
  - Educate your developers
  - Educate your security team
- Social Engineering Defenses

# Hardening SQL Server – Layer by Layer





# Perimeter & Network Layers

- Physical & Digital Security Methods
  - Office building
  - Key Cards
  - Data Center access
  - Firewall
  - VPN Access
  - Network Segmentation
- Who has access to what?

# Endpoint Security

- Antivirus
- EDR
- Patching

# Application Layer

- Design reviews
- (Peer) Code Reviews
- AST
- Pentesting

# Mission-Critical Systems

- HA/DR
- Monitoring pipelines
- Data Availability
- Data Encryption
- RBAC

# Default SQL Server Installation, what's next?

DEMO



# Authentication & Authorization



# Identity Strategy

- Where to store credentials?
- Automation?
- SQL Authentication?



# Role-Based Access Control

- Administrative tasks
- Applicational tasks

# Authentication & Authorization

DEMO

ON TOUR | NETHERLANDS

 **PASS**

**BREAK**



# Encrypting SQL Server



# Encryption in Transit

- Transport Layer Security
- Certificates
- SQL Server Fallback Certificate

# Encryption at Rest

- Transparent Data Encryption
- OS Compromise
- Read-only access?

# In-Memory Encryption

- Always Encrypted
- Client-side encryption

# Keys & Secrets Management

- Key rotation?
- Certificate rotation?
- Password Management?



# Encrypting SQL Server

DEMO

# Monitoring, Auditing & Compliance



# SQL Audit & Extended Events

- Change tracking
- Anomaly detection
- Hack attempts

# Compliance Mapping

- GDPR / ISO / HIPAA / ...
- PCI DSS
- CIS Benchmark
- STIG
- TBA...

# Reporting

- Uniform
- Ease of mind
- Compliancy rates
- Always 100%?
- Building a baseline

# Monitoring, Auditing & Compliance

DEMO

# Back-up & Recovery Strategies





# Back-up Planning

- Recovery Models
- Snapshot back-ups
- Back-up schedules

# Back-up Tiering

- 3 Tier Back-up Model
  - Tier 0
  - Tier 1
  - Tier 2
  - Tier 3

# Recovery Scenario's

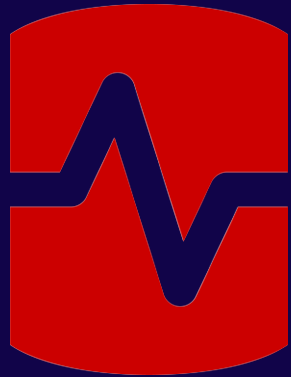
- Recovery Point Objectives
- Recovery Time Objectives
- Recover from which tier?

# Tools & Resources



# Built-in Tools

- SQL Vulnerability Assessment
- Defender for SQL\*



redgate  
Monitor

DEMO

# Wrap Up





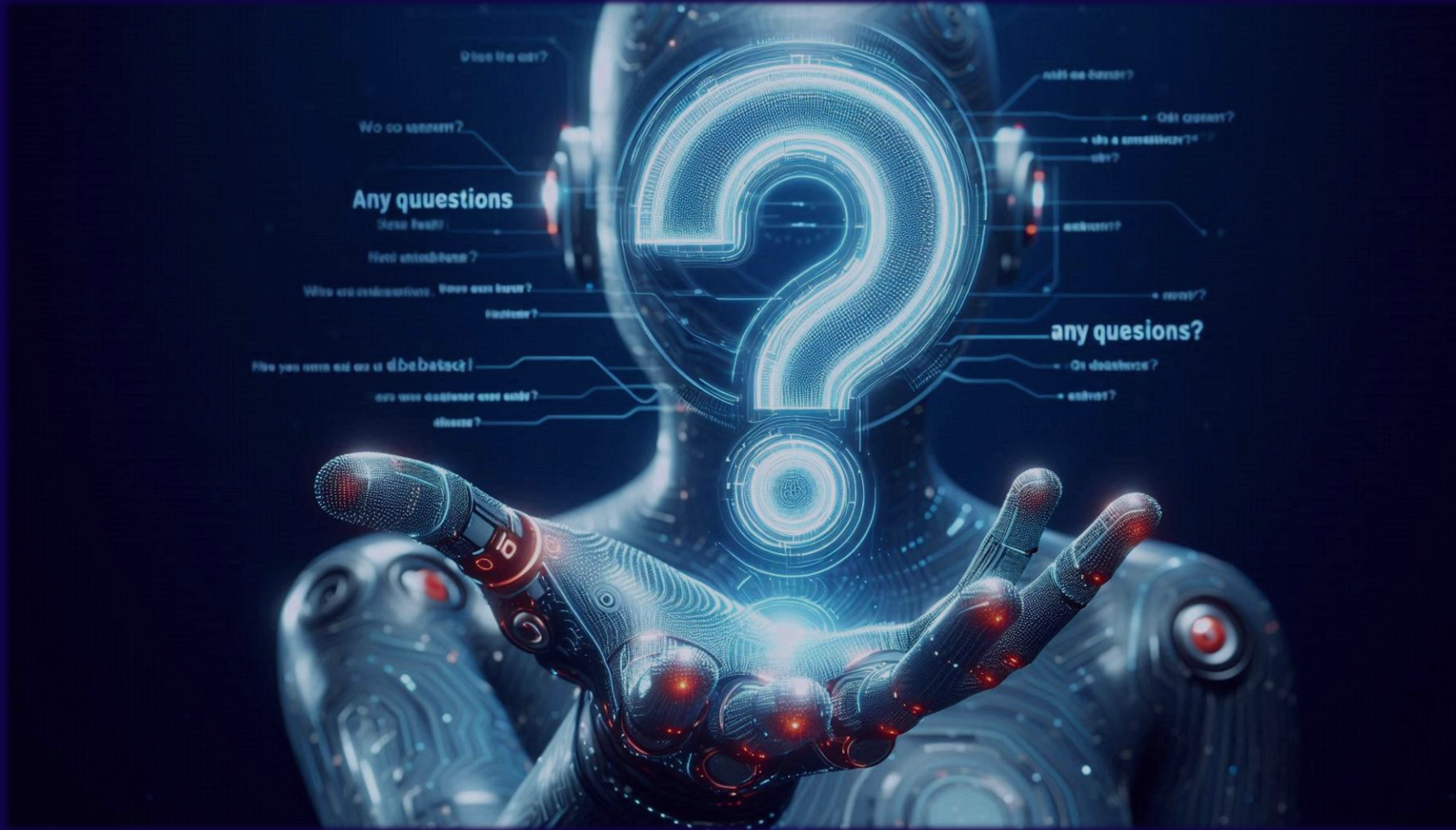
# Summary / Takeaways

- Security aspects of SQL Server
- Monitoring & Auditing
- Principle of least privilege
- Back-up & Recovery
- Tools & Resources

# Next steps...

- Goal setting
- Strategies
- Design
- Assess
- Continuously Improve!

## Q&A



# Your feedback is important to us



**Evaluate this session at:**

[passdatacommunitysummit.com/evaluations-nl](https://passdatacommunitysummit.com/evaluations-nl)

# Thank you

Enjoy the rest of the event!

**Danny de Haan**

 [thatinfradba@pm.me](mailto:thatinfradba@pm.me)

 [/in/dannydh](https://www.linkedin.com/in/dannydh)