solarwinds

Data Security and Privacy Techniques for Modern Databases

Thomas LaRock, Head Geek™, SolarWinds®

SOLISYON
www.solisyon.de

Zötler Bier
natürlich, sympathisch, frisch

DATAmasterminds

POWER BI SENTINEL
Documentation · Data Lineage · Change Tracking · Backup

ROSEN
empowered by technology

HEDDA.IO

SentryOne®

redgate

SHOP APOTHEKE
EUROPE

dbWatch
DATABASE CONTROL

Why Are You Here?

You have data, and databases

You want to secure that data

You have no idea how to get started

Thomas LaRock

Head Geek, SolarWinds

Over 20 years experience in roles including programmer, developer, analyst, and DBA.

Enjoys working with data, probably too much to be healthy, really.

Microsoft CERTIFIED Master

Microsoft MVP Most Valuable Professional

vmware vEXPERT

@SQLRockstar

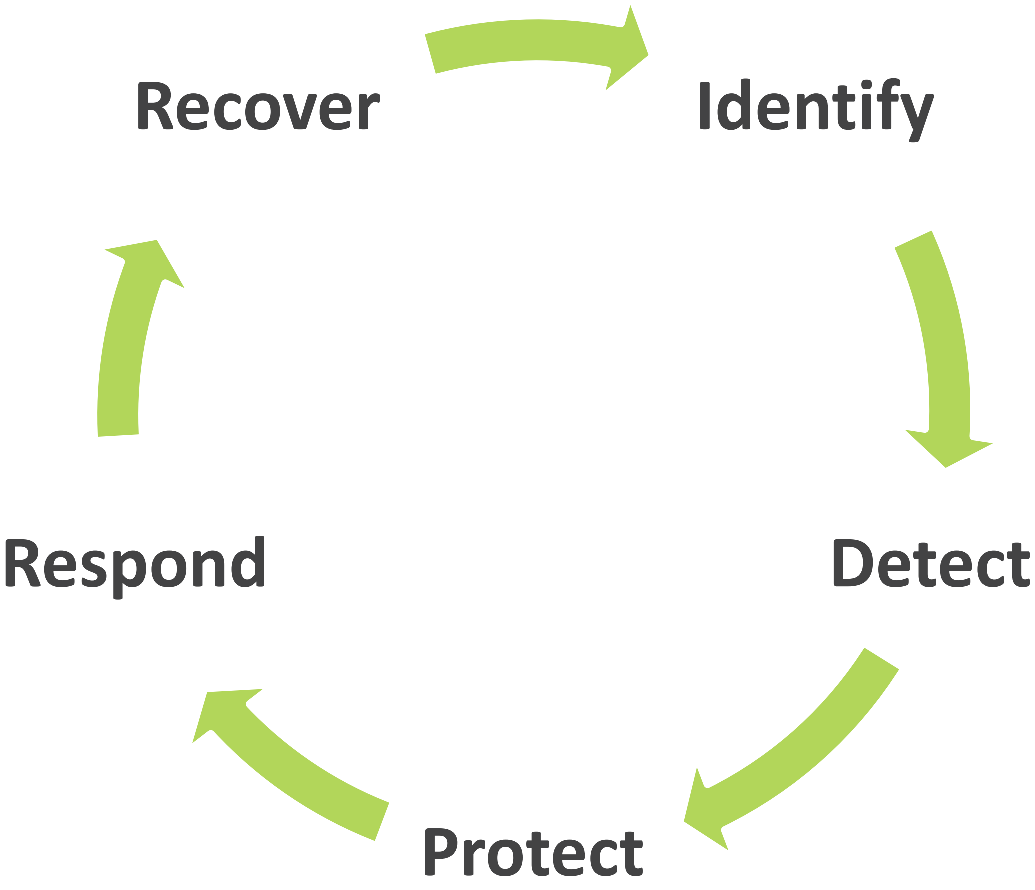
facebook.com/thomas.larock

linkedin.com/in/SQLRockstar

thomaslarock.com/blog

@solarwinds

NIST Cybersecurity Framework



Agenda

1 **Identify**

2 Detect

3 Protect

4 Respond

5 Recover

Agenda

1 Identify

2 Detect

3 Protect

4 Respond

5 Recover

Agenda

1 Identify

2 Detect

3 Protect

4 Respond

5 Recover

Agenda

1 Identify

2 Detect

3 Protect

4 Respond

5 Recover

Agenda

1 Identify

2 Detect

3 Protect

4 Respond

5 Recover

Identify

Data Management

Risk Assessment

Azure® Data Catalog

Data Discovery and Classification

Vulnerability Assessment

DEMO

Protect

Data security

Access control

Information protection

Data at rest

Data in use

Data in motion

It’s the data circle of life.

Data at Rest

Database files

Additional app files

Database backups

Transparent Data Encryption

Backup Encryption

Bitlocker

Data in Use

Excel®

PowerBI

Access control

Row Level Security

Dynamic Data Masking

Data in Motion

Transmit data across network

Secure Sockets Layer (SSL)

Always Encrypted

DEMO

Detect

Timely discovery of events

SQL Server® Audit

SQL Injection

Anomalous Access

Data Exfiltration

DEMO

Respond

Response plan

Containment

Mitigation

Continuous improvements

Penetration testing

Red Team

Blue Team

Red Team/Blue Team

Red Team

Assign specific task

Identify vulnerabilities in the PPT (People, Processes, Technology)

Blue Team

Review logs (SIEM)

Threat intelligence

Network traffic flow analysis

Recover

If you can’t recover, you can’t keep your job

RPO/RTO

Consider how you refresh dev/test from production

Don’t recover malware!

Agenda

1 Identify

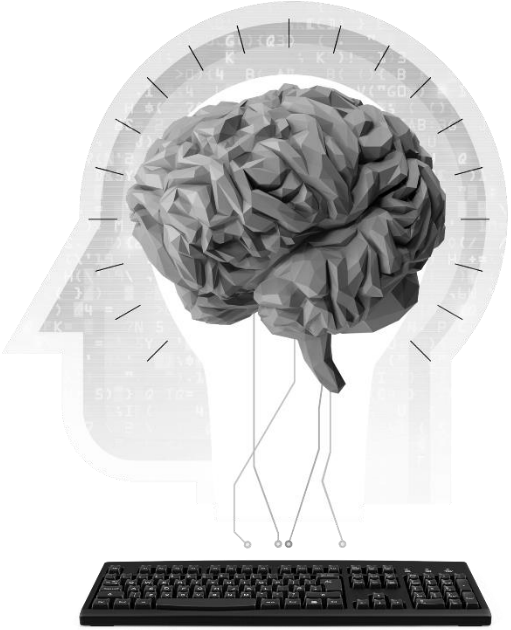
2 Detect

3 Protect

4 Respond

5 Recover

Q&A



THANK YOU!

For More Information

slrwinds.com/NIST-Framework

slrwinds.com/DataCatalog

slrwinds.com/DataDiscoveryClassification

slrwinds.com/VulnerabilityAssessment

slrwinds.com/TDE

slrwinds.com/BackupEncryption

slrwinds.com/RLS

slrwinds.com/DDM

slrwinds.com/AlwaysEncrypted

slrwinds.com/SQLAudit

slrwinds.com/SQL-ThreatDetect

slrwinds.com/SQLMAP

Session Feedback Day 2

http://bit.ly/DataGrillen2019Day2

Event Feedback

http://bit.ly/DataGrillen2019Event