Whatcha Doin'?

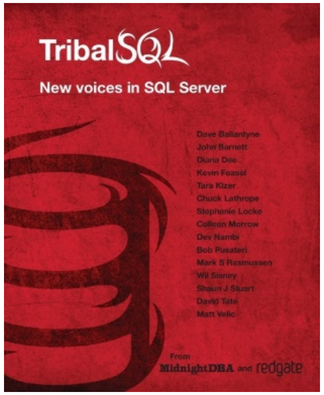
Passive Security for Hostile Environments

Bob Pusateri
Database Administrator
Northwestern University

About Me

SSKS

www.bobpusateri.com



TribalSQL

New voices in SQL Server

Dave Ballantyne
John Barnett
Diana Dee
Kevin Feasel
Tara Kizer
Chuck Lathrope
Stephanie Locke
Colleen Morrow
Dev Nambi
Bob Pusateri
Mark S Rasmussen
Wil Sisney
Shaun J Stuart
David Tate
Matt Velic

From
MidnightDBA and redgate

SQL

@SQLBob

redgate

Friend of Redgate 2015

Microsoft CERTIFIED

Master

EDW

NORTHWESTERN MEDICAL
ENTERPRISE DATA WAREHOUSE

Thank You Sponsors!

Platinum Sponsor

Tintri

SIOS

Gold Sponsor

tegile

Micron

DELL Software

Alliance TECHNOLOGIES

PYRAMID ANALYTICS

idera

Microsoft

Bronze Sponsor

Ntirety®

A DIVISION OF HOSTING

Your feedback is very much appreciated

Who is the best DBA?

- The one you don’t know exists
- Mildly paranoid
- Sense of ownership & responsibility
- Omniscient about DBs entrusted to them

Our Scenario

One or more people have too many rights

- Boss, CEO, “Connected”, etc.
- You don’t trust them
- Nobody can or will say no to them
- You value your job so you won’t either

Our Scenario

They’re a sysadmin!

Can we stop a sysadmin from doing anything?

NO

Our Scenario

sysadmins:

- Can’t be denied anything
- Can undo anything we do

A GAME OF “WHAT IF”?

Goal: Passively Secure Our Instance

Know What’s Going On

- What’s being executed
- Who did it
- When it happened
- Alert DBA(s)

Be Invisible!

- Minimal impact on DB operations
- Record but don’t prevent
- Be as low-profile as possible

Our Toolbelt

- Triggers
- SQL Audit
- Event Notifications
- Extended Events
- Policy-Based Management

Demos

Feature Comparison

	Trigger	Audit	Event Notification	Extended Event
Asynchronous?	No	Yes/No	Yes	Yes
Runs in Transaction?	Yes	No	No	No
Ignores Rollbacks?	Yes	No	Yes	No
Logs Denials?	No	Yes	No	No
Can Instantly Notify?	Yes	No	Yes	No
Works in Standard Edition?	Yes	Server Level Only	Yes	Yes

Questions?

Email: Bob@BobPusateri.com

Twitter: @SQLBob

Resources: www.bobpusateri.com/r/passive

I'm here to help!