



Göteborgs  
Stad

# Risk management in ICS

Rikard Bodfors, CIO Gothenburg Sustainable waste and water

Info class: Public



# Who am I?

- CISA
- CISSP
- ISACA Thomas Fitzgerald award
- SANS Lethal Forensicator
- Säkerhetspodcasten
- >20 years in the business
- Protocol nerd



...or simply your average “Corporate suit IT-manager”

# We deliver human rights!

- We provide more than 600 000 persons in western Sweden with fresh, healthy and tasty water 365 days a year 24 hours a day.
- We also take care of waste collection, reuse and recycling



**Who are you?**





Göteborgs  
Stad

# A quick baseline

To make sure we're on the same page

# IT v/s OT?





# Why is security in OT crappy?





Göteborgs  
Stad

# Threats risks and risk management

Know your enemy, know yourself....



# Who am I up against?



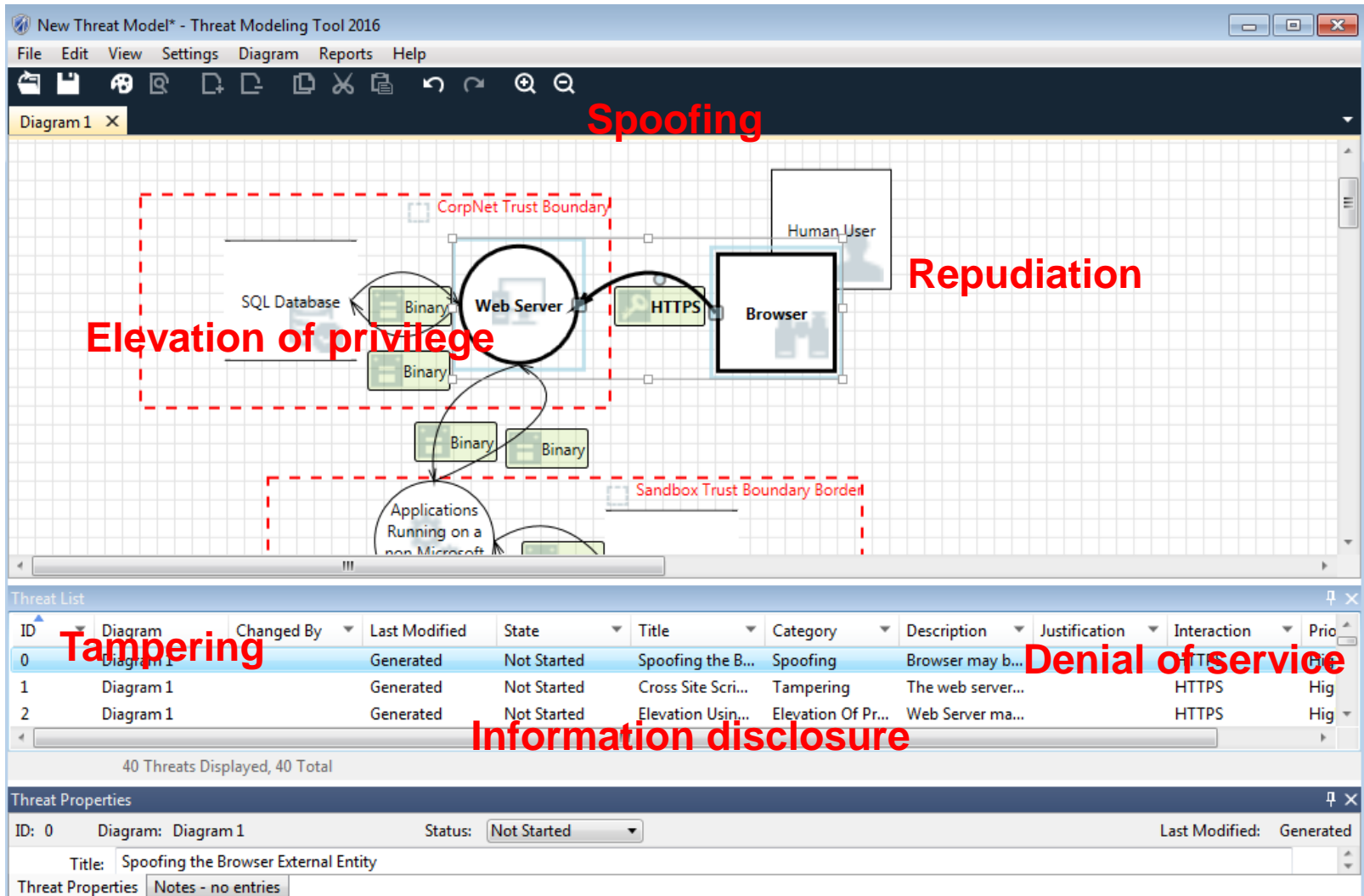
**I can protect against anything, right?**



# Know your system!



# Identify attack vectors



The screenshot shows the Threat Modeling Tool 2016 interface. The main diagram area displays a threat model with the following components and annotations:

- CorpNet Trust Boundary:** A dashed red box enclosing the SQL Database, Web Server, and Browser.
- Sandbox Trust Boundary:** A dashed red box enclosing the Applications Running on a non-Microsoft OS.
- Assets:** SQL Database, Web Server, Browser, Human User, and Applications Running on a non-Microsoft OS.
- Interactions:** Binary files connect the SQL Database and Web Server. The Web Server connects to the Browser via HTTPS. The Browser connects to the Human User.
- Attack Vectors (Red Text):**
  - Spoofering:** Located above the diagram.
  - Repudiation:** Located to the right of the Browser.
  - Elevation of privilege:** Located to the left of the Web Server.
  - Tampering:** Located over the Threat List table.
  - Denial of service:** Located over the Threat List table.
  - Information disclosure:** Located below the Threat List table.

The Threat List table contains the following data:

ID	Diagram	Changed By	Last Modified	State	Title	Category	Description	Justification	Interaction	Prio
0	Diagram 1	Generated	Generated	Not Started	Spoofering the B...	Spoofering	Browser may b...	Denial of service	HTTPS	Hig
1	Diagram 1	Generated	Generated	Not Started	Cross Site Scri...	Tampering	The web server...	Information disclosure	HTTPS	Hig
2	Diagram 1	Generated	Generated	Not Started	Elevation Usin...	Elevation Of Pr...	Web Server ma...	Information disclosure	HTTPS	Hig

Threat Properties for ID: 0:

- Diagram: Diagram 1
- Status: Not Started
- Title: Spoofering the Browser External Entity

**If you change the way you look at things,  
the things you look at change.**

**- Dr. Wayne Dyer**



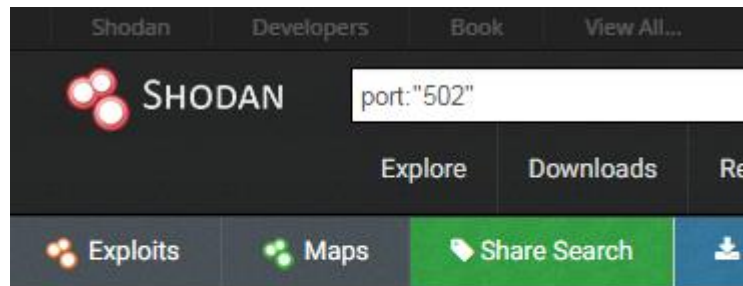


# The level of abstraction

# What is this?



# Analyze the threat landscape



## TOP COUNTRIES



United States	2,563
France	834
Spain	621
Sweden	575
Poland	570


Total results: 11,210

**128.125.31.1**

fit-ph-508.usc.edu

University of Southern

Added on 2016-05-18:

 United States, Li

[Details](#)

Unit ID: 0

-- Slave ID D

b2c343232342d

Unit ID: 255

-- Slave ID D

b2c3432...



Myndigheten för  
samhällsskydd  
och beredskap

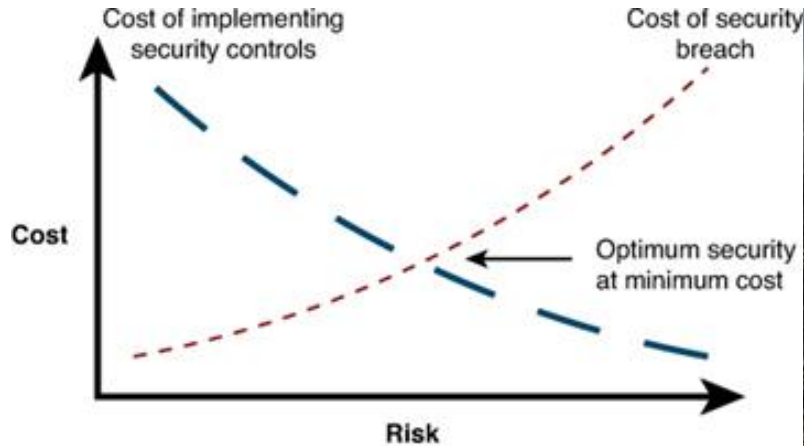


Säkerhetspolisen

# Risk analysis

	A	B	C	D	E	F	G	H	I	J
1										
2										
3			<b>Totalt</b> (39 scenarier)						<b>Strategiska</b>	
4		<b>4</b>			19			<b>4</b>		
5		<b>3</b>	10b, 16	8, 14	4a, 4b, 22, 27, 29, 33	12, 3, 18, 23, 24, 25, 31		<b>3</b>	10b	8
6		<b>2</b>		6b, 20b, 21	1, 6a, 37	2, 5, 9, 13, 26, 32, 33, 34, 36		<b>2</b>		6b
7		<b>1</b>			7, 10a, 30	15, 28, 20a		<b>1</b>		
8			<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>			<b>1</b>	<b>2</b>
9				Konsekvens					Konsekv	
10										
11										

# Evaluate risk mitigation



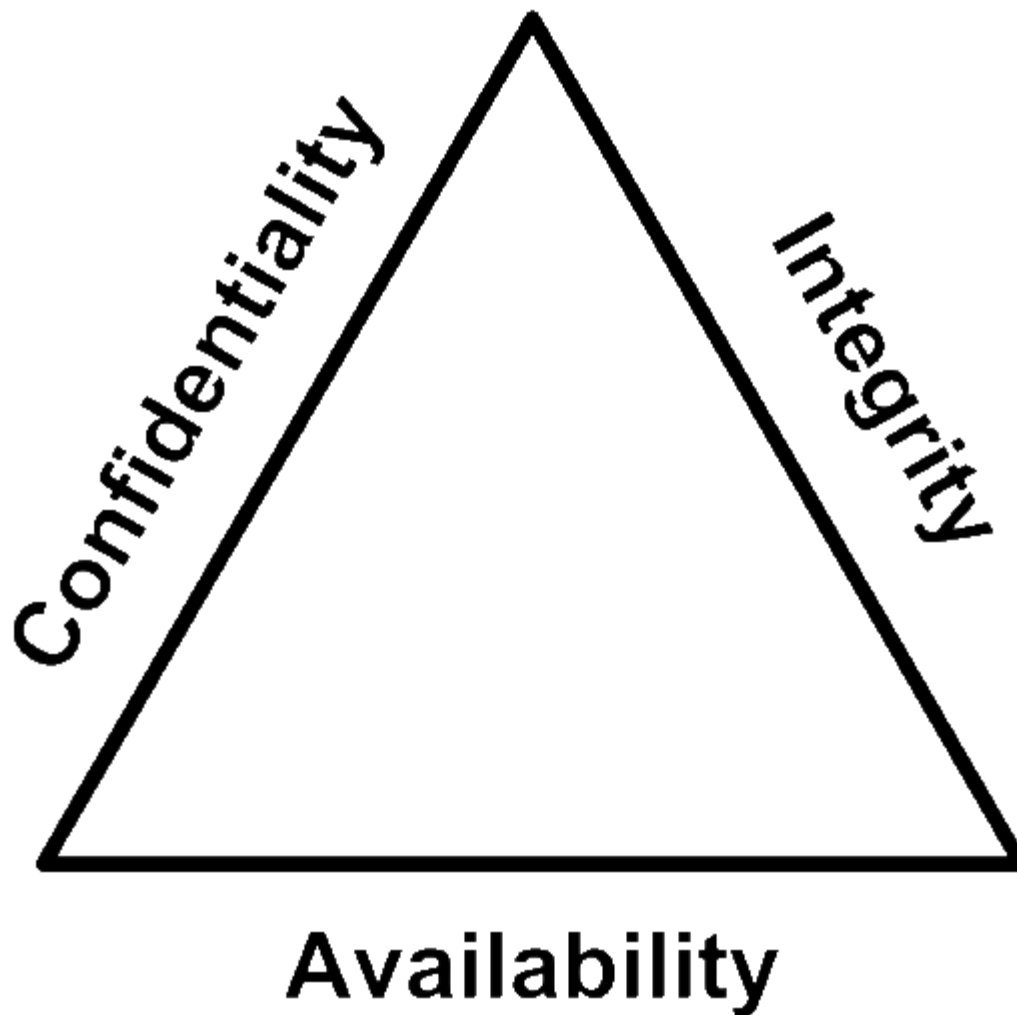
Analysis of cost vs. risk  
Cost of implementing security vs. cost of security breach



Evaluate using the same criteria and scale as other operational risks



# Balance



**Just because you can, doesn't make it a good idea...**





Göteborgs  
Stad

# Auditing sensitive systems

How to avoid turning off the lights when  
pentesting critical infrastructure

# What not to do...



# Working method 1: Passive identification of vulnerabilities





# Passive methods

- Log analysis
- Wireshark, Sniffer, etc.
- Monitor ports
- Passive wireless tools
- Configuration files
- System maps
- Process inventory
- Protokoll analyzers for I2C, RS232, RS485, etc.
- Etc....

## Working method 2: Active identification of vulnerabilities



# Active methods

- Test system (PHYSICALLY separated)
- Virtualization in a lab (PHYSICALLY separated)
- FAT tests at the suppliers site
- SAT tests on new systems not yet in production
- Shodan.io on your own network
- Hack someone else... (NB!!! JOKE! Please don't.)

# Summary

- Identify possible attack vectors
- Analyze the threat landscape
- Prioritize your risks
- Evaluate mitigation
- Reiterate
- never sleep...



Göteborgs  
Stad

# More good stuff

A few places to look for more information

# More reading

- <https://www.msb.se/scada>
- <http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf>
- <https://ics-cert.us-cert.gov/Standards-and-References>
- <https://scadahacker.com/library/>
- [http://www.hazar.org/analizdetail/analiz/cyberattack\\_in\\_ukraine\\_%E2%80%93\\_23\\_december\\_2015\\_a\\_reading\\_list\\_1583.aspx](http://www.hazar.org/analizdetail/analiz/cyberattack_in_ukraine_%E2%80%93_23_december_2015_a_reading_list_1583.aspx)
- <https://www.microsoft.com/en-us/sdl/>





Göteborgs  
Stad

**CONTACT:**

IT Enheten

Kretslopp och vatten, Göteborgs Stad

Rikard Bodforss, IT-chef

[Rikard.Bodforss@kretsloppochvatten.goteborg.se](mailto:Rikard.Bodforss@kretsloppochvatten.goteborg.se)

Twitter: @rbodforss