Göteborgs Stad

Risk management in ICS

Rikard Bodforss, CIO Gothenburg Sustainable waste and water

Info class: Public

Who am I?

Göteborgs Stad

- 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

Göteborgs Stad

Who are you?

Göteborgs Stad

A quick baseline

To make sure we’re on the same page

IT v/s OT?

Göteborgs Stad

Why is security in OT crappy?

Göteborgs Stad

Threats risks and risk management

Know your enemy, know yourself….

Göteborgs Stad

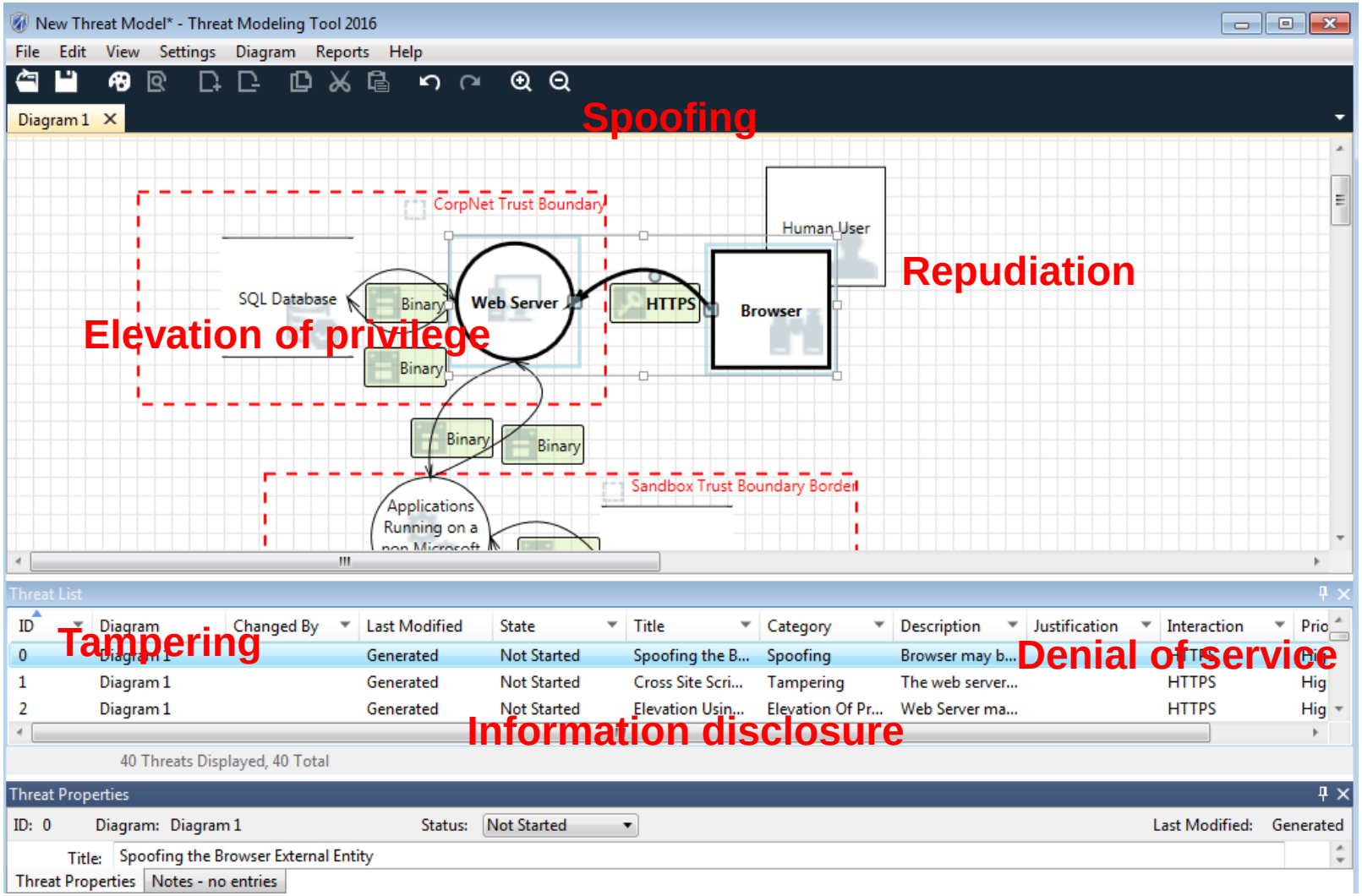
Who am I up against?

Göteborgs Stad

I can protect against anything, right?

Know your system!

Identify attack vectors



Göteborgs Stad

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?

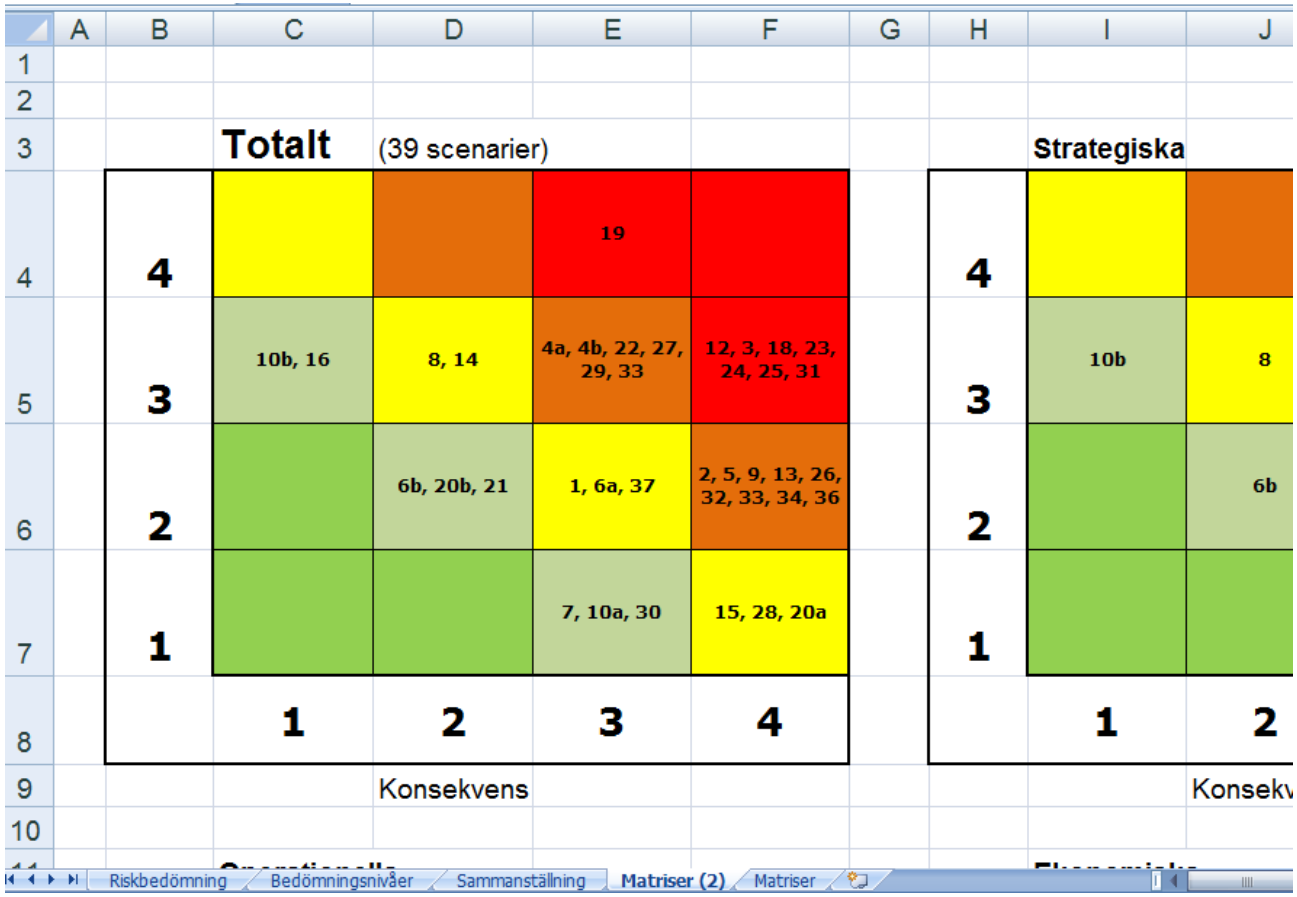
Analyze the threat landscape

Göteborgs Stad

MSB Myndigheten för samhällsskydd och beredskap

Säkerhetspolisen

Risk analysis



Totalt (39 scenarier)

4			19	
3	10b, 16	8, 14	4a, 4b, 22, 27, 29, 33	12, 3, 18, 23, 24, 25, 31
2		6b, 20b, 21	1, 6a, 37	2, 5, 9, 13, 26, 32, 33, 34, 36
1			7, 10a, 30	15, 28, 20a
	1	2	3	4

Konsekvens

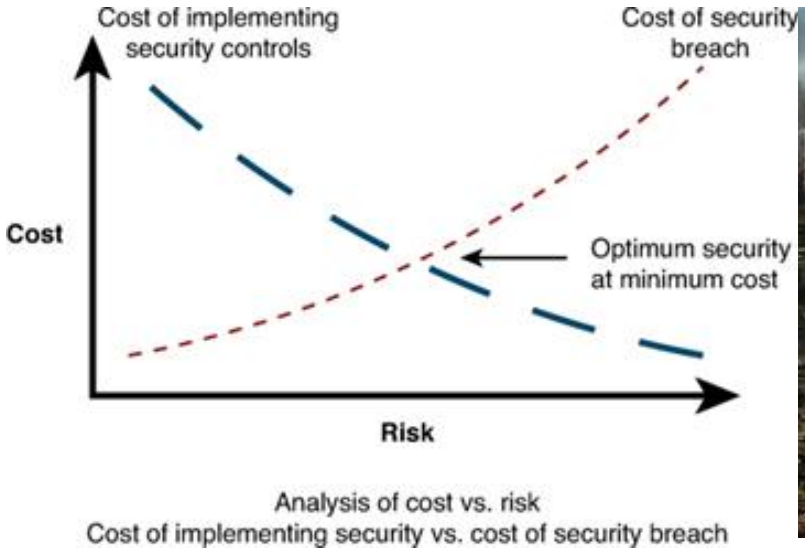
Strategiska

4		
3	10b	8
2		6b
1		
	1	2

Konsekv

Riskbedömning | Bedömningsnivåer | Sammanställning | Matriser (2) | Matriser

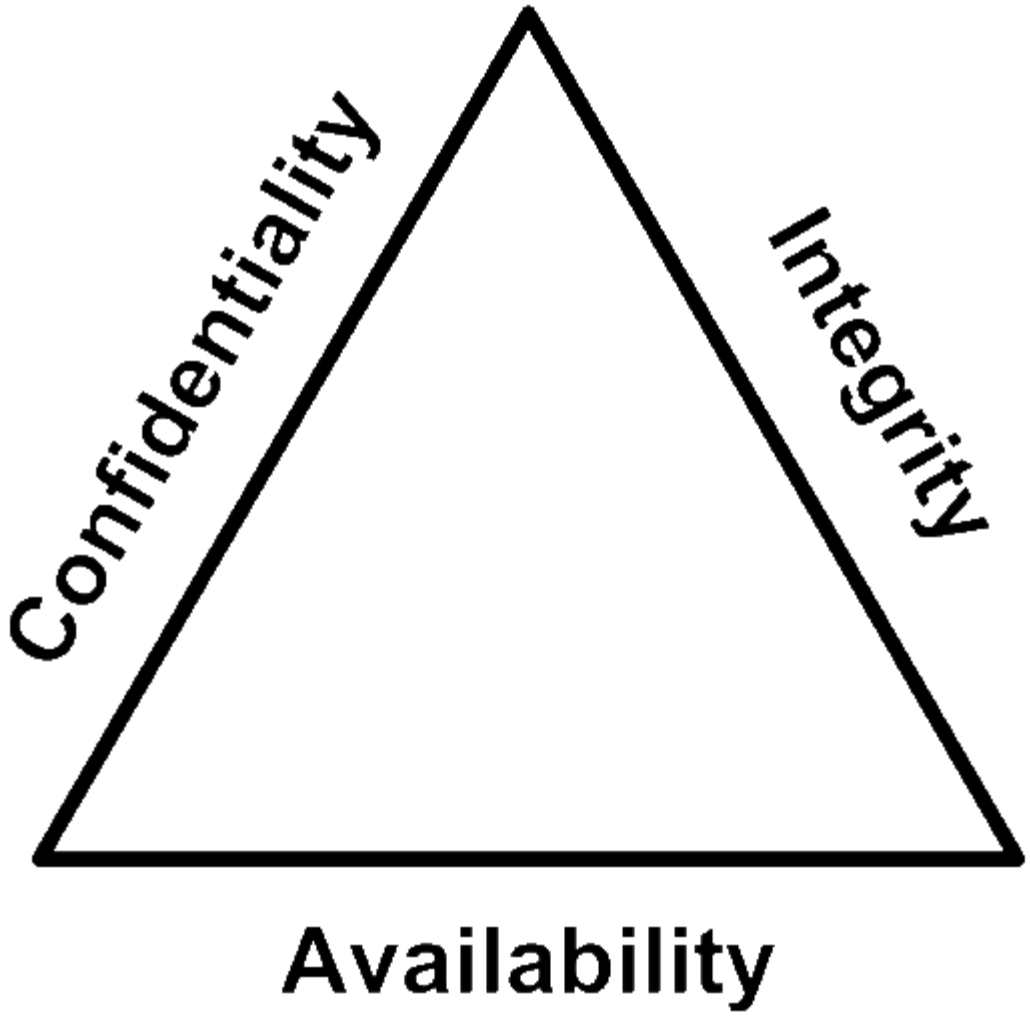
Evaluate risk mitigation



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

Göteborgs Stad

How to avoid turning off the lights when pentesting critical infrastructure

What not to do…

Göteborgs Stad

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….

Göteborgs Stad

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

Göteborgs Stad

- 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

Göteborgs Stad

- 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
- https://www.microsoft.com/en-us/sdl/

CONTACT:
IT Enheten
Kretslopp och vatten, Göteborgs Stad
Rikard Bodforss, IT-chef
Rikard.Bodforss@kretsloppochvatten.goteborg.se
Twitter: @rbodforss