

10 WAYS TO ROCK YOUR SOC

Shelly Giesbrecht

~~**EVIL GENIUS**~~

Senior Security Operations Analyst

Nexen Energy ULC.

AGENDA

- Some stuff about me and how I roll
- Generalities about security operations
- 10 seriously awesome things we do
- Bring it home
- Ask away or tell me I'm wrong



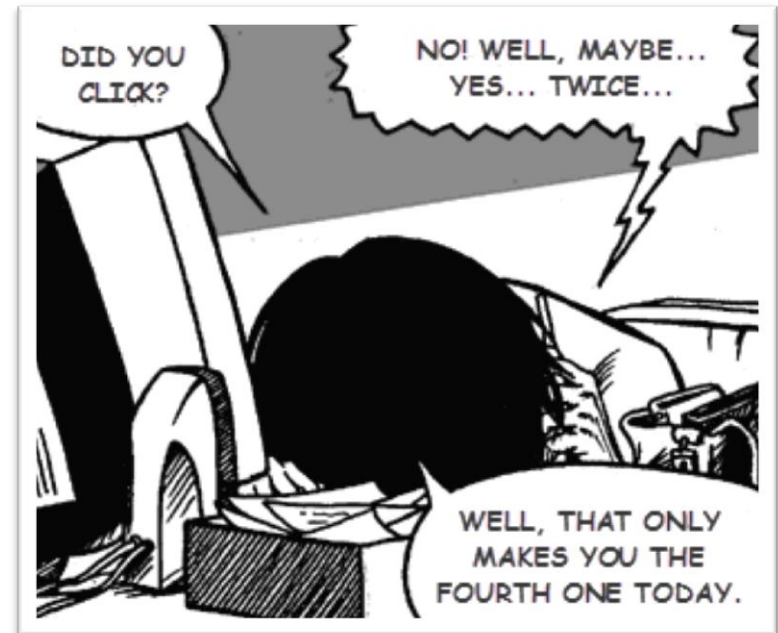
ROCKING THE BOWTIE

- Canadian
- IT for 14 years, Security for 8 years
- Work in oil & gas, previously at an airline
- I'm the G.I.R.L.
- Fan of the bowtie
- STI MSISE student
- Storyteller and fan of own voice



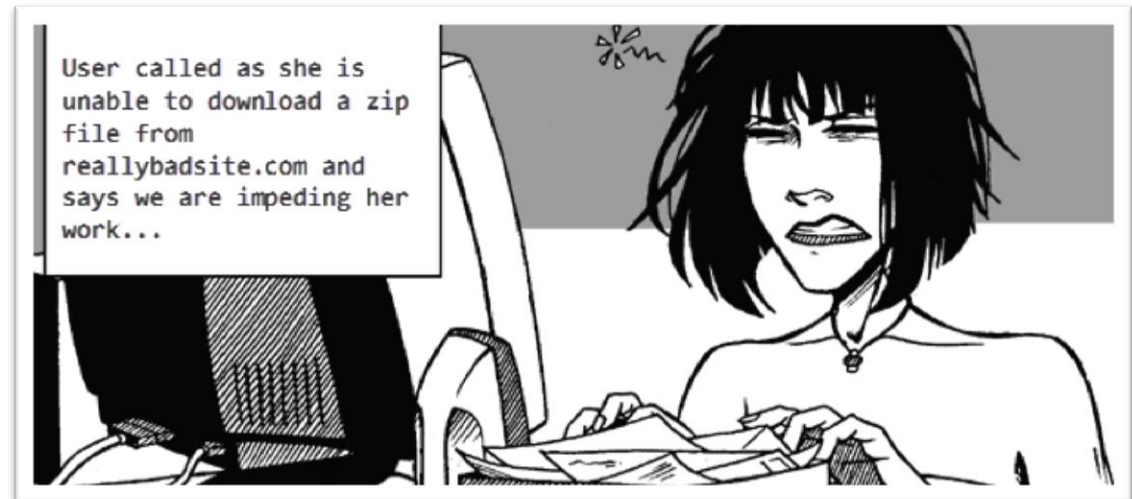
WHY SEC OPS IS HARD

- Jack of all of trades, master of... some?
- Very broad focus
- Different interpretations of sec ops
- Do more with (a lot) less
- “Shh... it’s the security team!”



GET THE INFORMATION YOU NEED

- Helpdesk is also a very tough job
- Bad information can slow down your response
- Help them help you
- Handy in a crisis



MAKE IT ACCESSIBLE

- Who are those dudes with the policies?
- Get off my security lawn!
- Teach a tech to fish (not phish)
 - Accessible
 - Applicable
 - Ownership
- Smarter techs, faster response



FEED YOUR RESOURCES

- Seriously, feed them
- Greasing the wheels
- Rewarding your heroes
- A full audience is a captive audience
- Happy people are helpful people



- I could get that done but I have no budget
- Money doesn't (always) buy success
- Rolling your own
- Know how things actually work
- Better response times

[illegible]

MAKE IT ROUTINE

- Make a list
- Check it twice
- Test it
- Review it
- Easier to spot evil



SHARE THE PAIN

- Make a schedule
- Everyone should participate
- Larger teams can assign by level
- Lather, rinse, and repeat
- Getting vacation approval is easier



MAKE SENSE OF CHAOS

- Who does what and reports to who?
- Document, document, document
- Practice, practice, practice
- Know where the docs are
- Respond more accurately



FIND YOUR SUPERSTARS

- The voluntold or the volunteer?
- Find people who CAN help
- Find folks who actually WANT to help
- Get buy-in for their time
- Willing participants make for better IR



FIND A WAY TO YES

- Walk the talk
- Where are your policies?
- Help your business understand their risk
- Build trust
- Don't say no

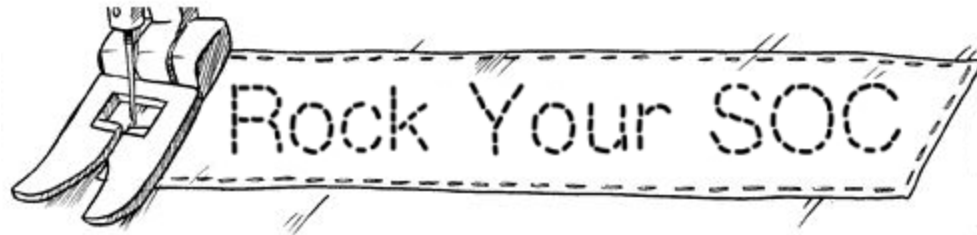


PICK YOUR BATTLES

- Go along to get along
- Being right isn't (always) necessary
- But sometimes it is
- Get an opinion
- Catch flies with honey



WHY THIS ALL MATTERS



- Get the information you need
 - Better info makes better response
- Make it accessible
 - Security isn't just for security
- Feed your resources
 - Happy people make willing helpers
- Script your world
 - Craft your own success
- Make it routine
 - Know what's normal
- Share the pain
 - Everyone knows the drill & big picture
- Make sense of chaos
 - Everyone knows their role
- Find your superstars
 - Help is better when the help is willing
- Find a way to yes...with security
 - Get them to come to you
- Pick your battles
 - Being right isn't the only thing

WHERE TO FIND ME



SHELLY GIESBRECHT

Email: headnerd@nerdiosity.com

Twitter: [@nerdiosity](https://twitter.com/nerdiosity)

Google+: [+Shelly Giesbrecht](https://plus.google.com/+ShellyGiesbrecht)

THANK YOU VERY MUCH!