Rising from the Ashes:
How to rebuild a security program gone wrong...
With help from Taylor Swift
We are...

Mike Hracs...
• Deloitte “Purple” team
• Security Operations Analyst/Pen Tester/Incident Responder
• GREM and GCFA certified and many more...
• Enjoys sweet talking pcaps by moonlight

Shelly Giesbrecht...
• Incident Responder at Cisco
• SANS Technology Institute MSISE student
• GREM, GCFA, GFCE, GCIA, GCIH and GSEC certified
• Enjoys imaging servers and chianti
Inspiration

*we believe all images used are common use. Thanks Internet!
Agenda

• People
• Process
• Technology
• #Winning
• Questions
People

Bad Blood...

Eyes Open...

We Are Never Ever Getting Back Together...
People

• Don’t be *that* new guy

• Ask questions and listen to the answer

• Learn to say yes... or at least maybe
People

• Transparency

• Involvement

• Accountability
People

• Trust is hard won and easily lost

• Be Rick Astley, not Taylor Swift
Process

Crazier...

Sweeter Than Fiction...

Shake It Off...
Process

• Finding the needle in the needle stack

• Answer the questions before they are asked

• Review, rinse and repeat
Process

• Who does what when and how?

• A crisis is never a good time to “test”

• Make auditors your friends (I know... ewww...)
Process

• Smoother operators

• Responding and reporting made easy

• Roles and responsibilities (did we mention that?)
Technology

Safe And Sound...

Out Of The Woods...
Technology

• Threat, risk and gaps, oh my!

• Horse & carriage vs stealth bomber...

• Big budget + no plan = shelfware
Technology

• People + Process + Technology = Secure?

• But the vendor said.....

• The last piece...
#Winning

• Bad Blood

• We are never ever getting back together

• Eyes Open

• Never gonna give you up (guest artist Rick Astley
#Winning

- Crazier
- Shake it off
- Sweeter than fiction
#Winning

• Safe and Sound

• Out of the Woods
#Winning

Everything has changed...
We are...

Mike Hracs...
• mhracs@deloitte.ca
• bumjubeo@gmail.com
• Twitter: @bumjubeo

Shelly Giesbrecht...
• sgiesbre@cisco.com
• headnerd@nerdiosity.com
• Twitter: @nerdiosity
Questions?