oneconsult
together against cyberattacks

TLP:CLEAR

Mistakes happen, either learn from them or rinse and repeat!

Gregor Wegberg | 35th Annual FIRST Conference, 8 June 2023

Gregor Wegberg

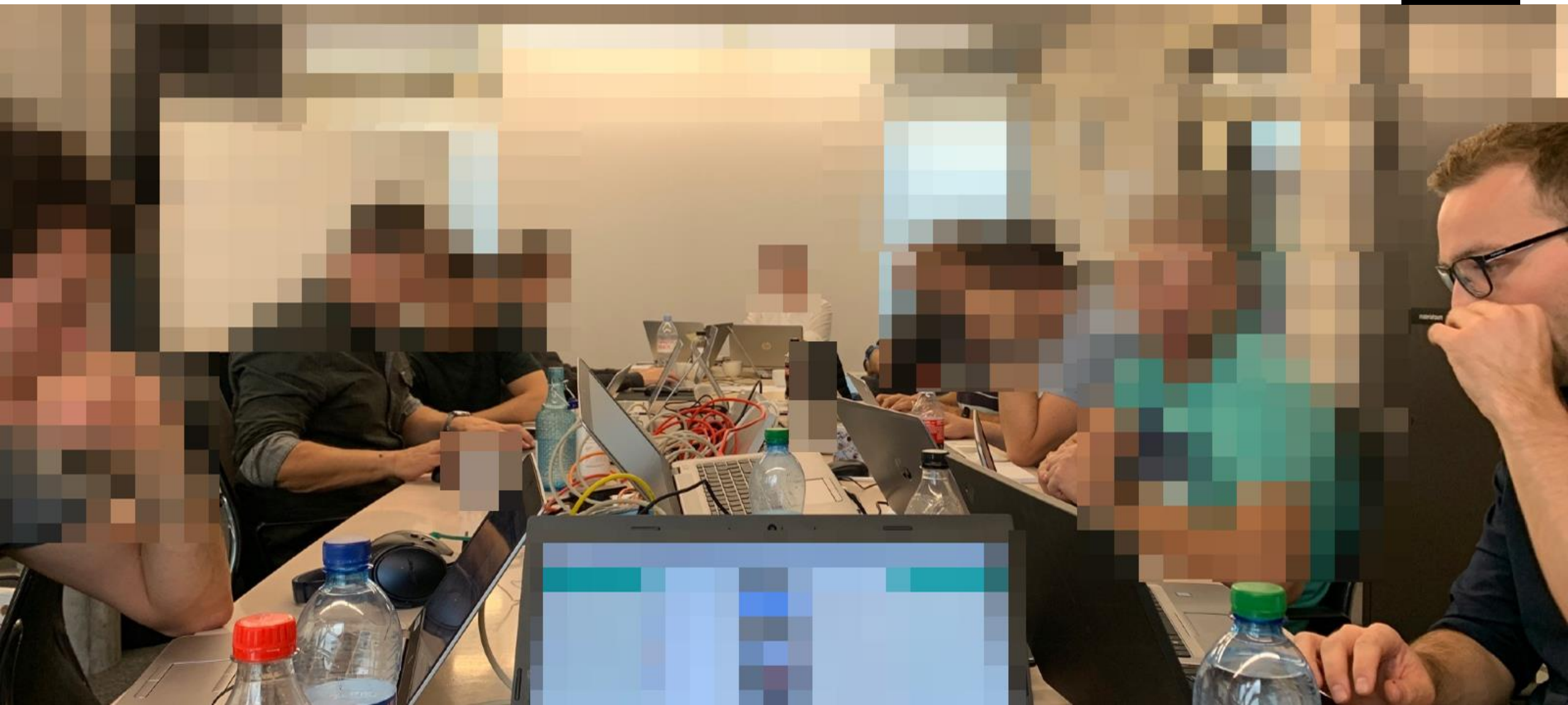
Head of Digital Forensics & Incident Response

Lecturer at Eastern Switzerland University of Applied Sciences

Fun fact: I have three passports / citizenships (I am not a spy)

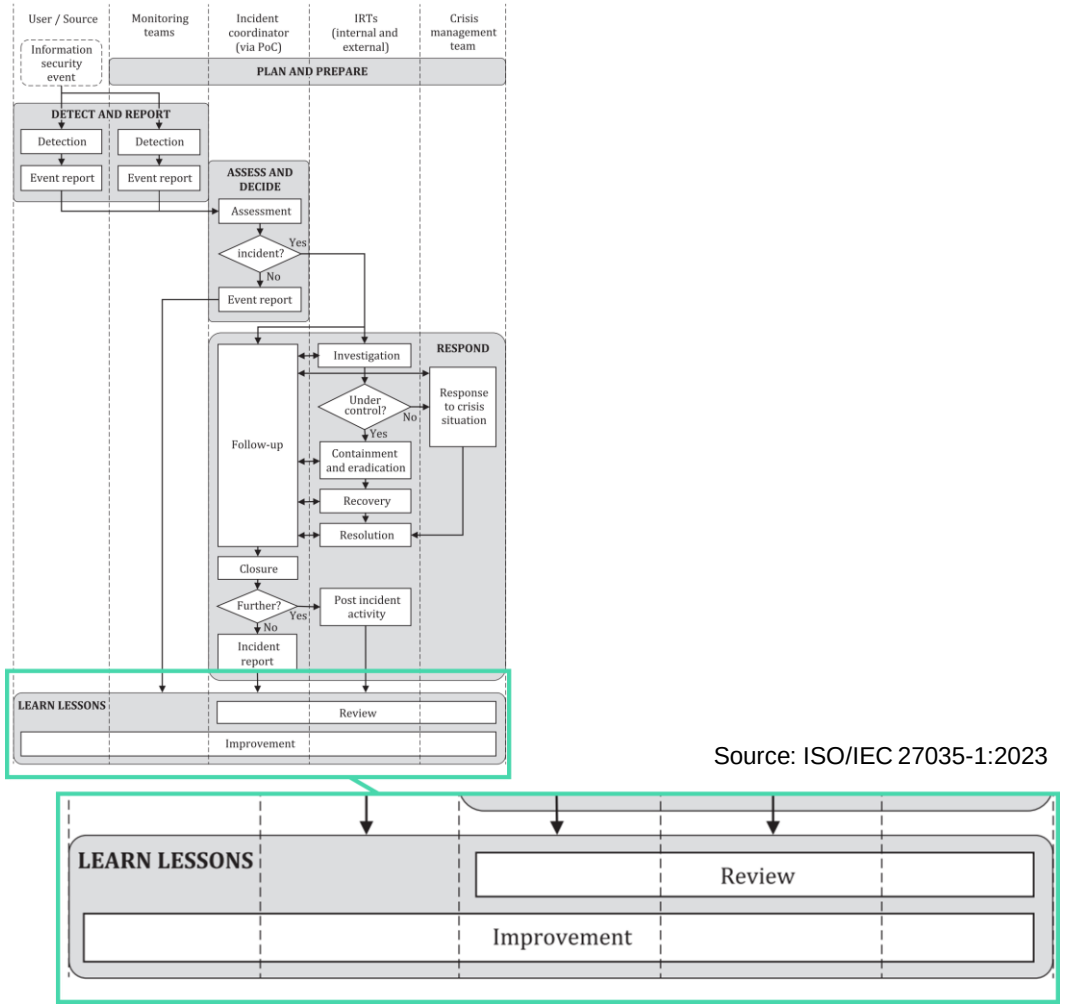
The following lessons are taken from our everyday life (responding to ransomware)

TLP:CLEAR

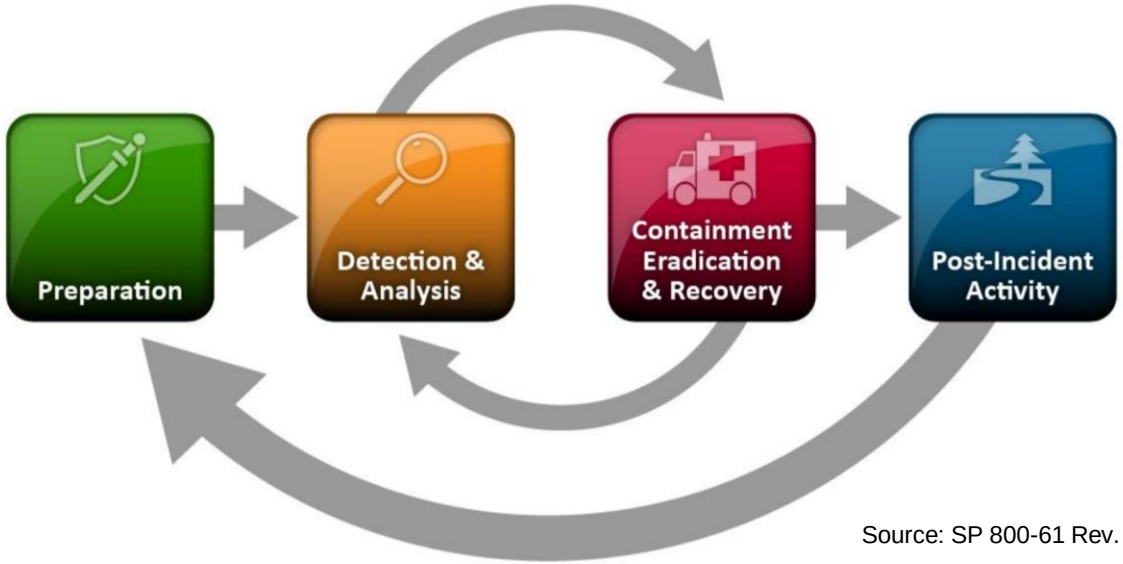


Failure is allowed if we learn from it

TLP:CLEAR



Source: ISO/IEC 27035-1:2023



Source: SP 800-61 Rev. 2

“One of the most important parts of incident response is also the most often omitted: learning and improving.”

Technical lessons learned

TLP:CLEAR

intentionally left blank

How major incidents feel for most people

Photo by nikko macaspac on Unsplash

Your very first immediate measure:
Take a break and drink some coffee/tea and relax

TLP:CLEAR

Photo by Priscilla Du Preez on Unsplash

The right tools are important.
But people are the crucial factor

TLP:CLEAR


Photo by Jude Infantini on Unsplash


Photo by Jessica Delp on Unsplash


Photo by Mae Mu on Unsplash

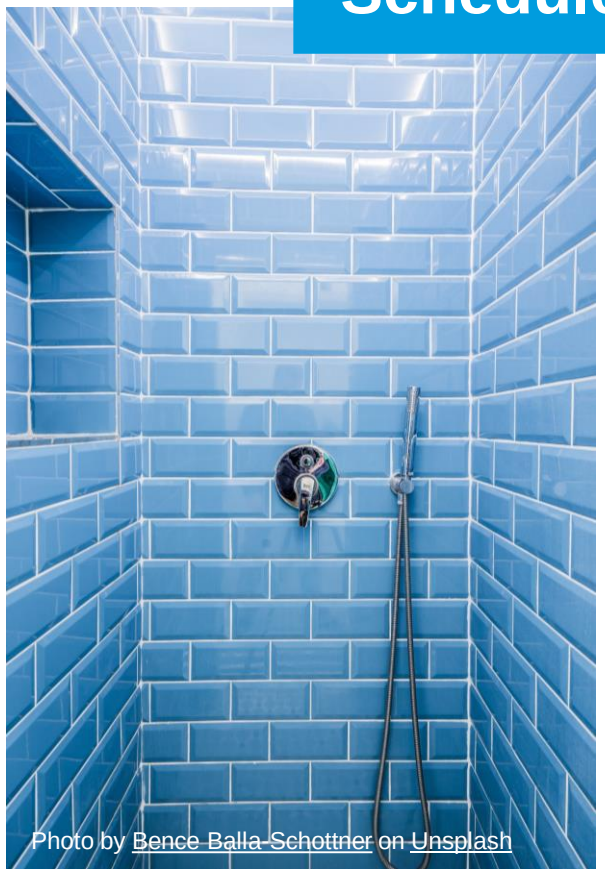
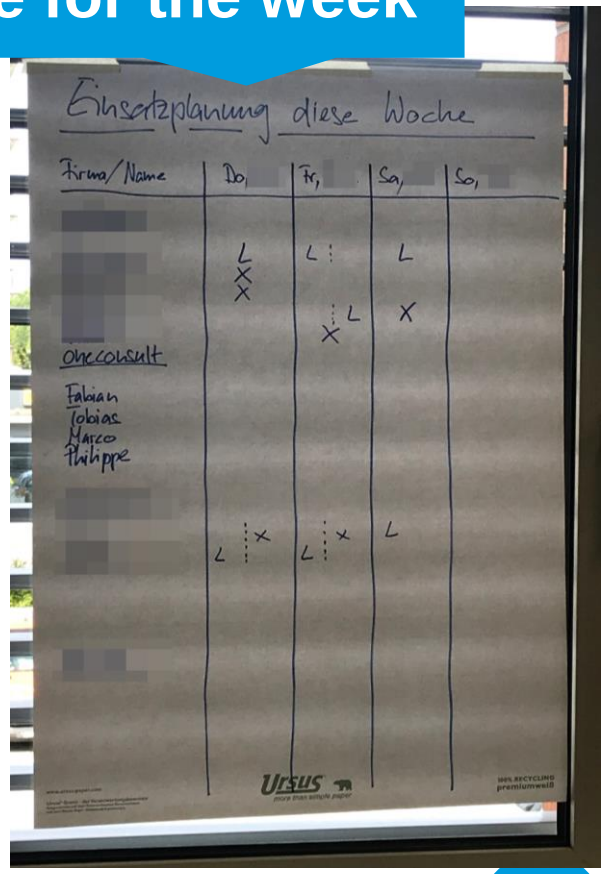


Photo by Bence Balla-Schottner on Unsplash

Schedule for the week



DFIR is difficult
Especially under high pressure

TLP:CLEAR

Obvious, yet crucial to internalize

- We are humans
- Humans make mistakes
- We will make mistakes

Many find it difficult to accept this during their first major incident.

Assume 50% of staff operates at 50% of normal capacity.

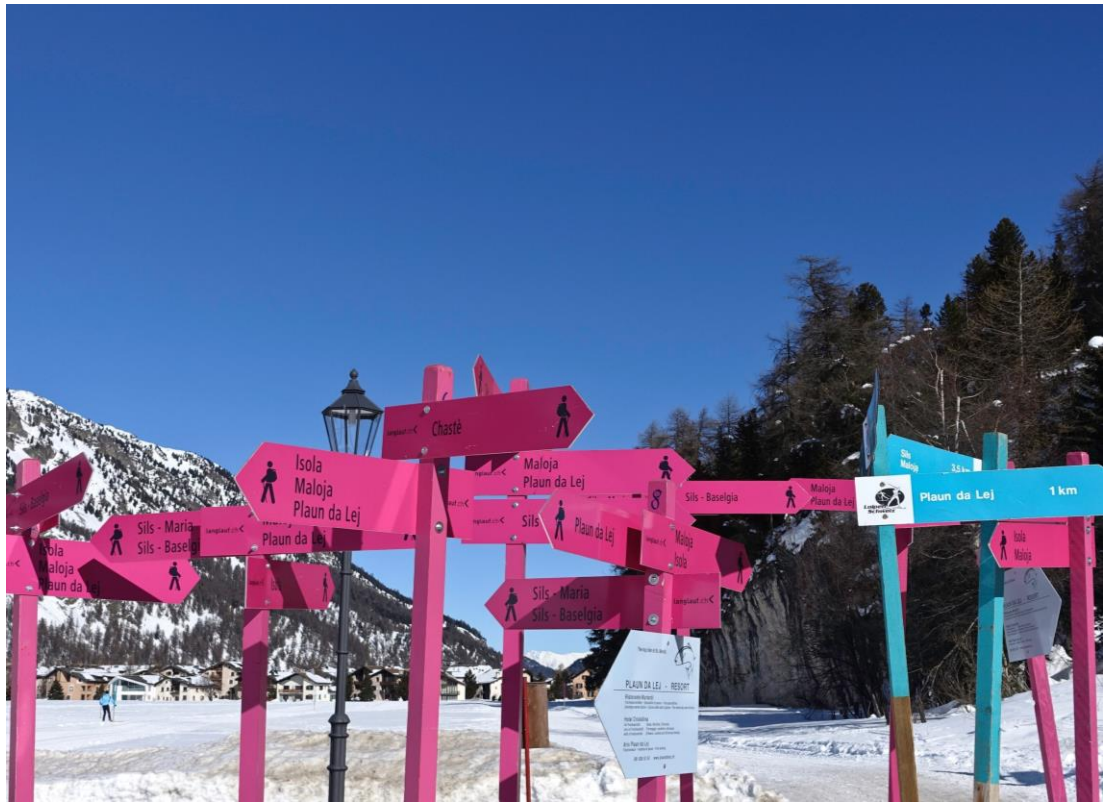


Photo by Daniele Levis Pelusi on Unsplash

It’s difficult for everyone
What kind of incident is it? Ask questions! Be nice.

TLP:CLEAR

Photo by Dario on Unsplash

Why are you even trying?

TLP:CLEAR

Photo by Kelan Chad on Unsplash

TLP:CLEAR

Be wary of digital tools.
Pen & paper works amazingly well

… to bring order to an incident

TLP:CLEAR

Think in smaller, more modular playbooks

TLP:CLEAR

Don't overwhelm yourself with all-encompassing playbooks, e.g., *THE RANSOMWARE PLAYBOOK*.

Many forms of cyber incidents require the same response activities. You can prepare for this!

- Immediate measures when our gut tells us panic
- Reset passwords and other secrets

Photo by Volodymyr Hryshchenko on Unsplash

Serious incidents take their time

TLP:CLEAR

Gregor Wegberg

Mastodon: @groggi@infosec.exchange

LinkedIn: /in/gregorwegberg

E-Mail: gregor.wegberg@oneconsult.com

Twitter: @gwegberg

Photo by Chris Wormhoudt on Unsplash