



Outro

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

I'm a Virgin

[but this is an old t shirt]



My vision:

Detailed Basics

But also

Overview of current situation / State of the Art
Exploitation

Detailed vs. Completeness

Free Speaking vs. Slides as Documentation

Understanding of Details vs. Understanding of Concepts

Self-Thinking vs. Step-by-Step description

Hands-On practice vs. Theory

Incremental Building Steps vs. Goal-Driven Explanation

Detailed vs. **Completeness**

Free Speaking vs. **Slides as Documentation**

Understanding of Details vs. Understanding of Concepts

Self-Thinking vs. Step-by-Step description

Hands-On practice vs. **Theory**

Incremental Building Steps vs. Goal-Driven Explanation

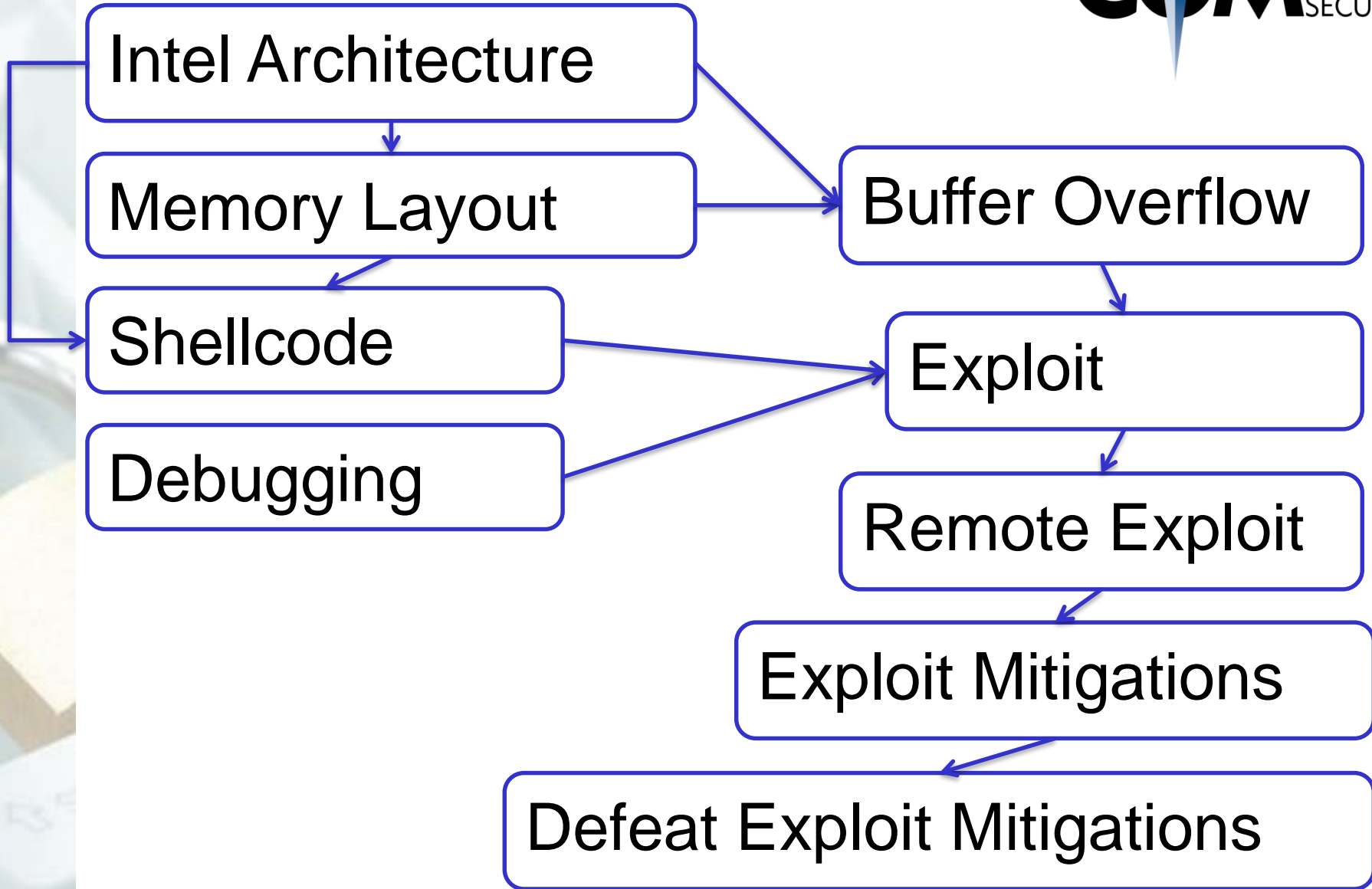
Getting lost in slides... Not enough time



Questions

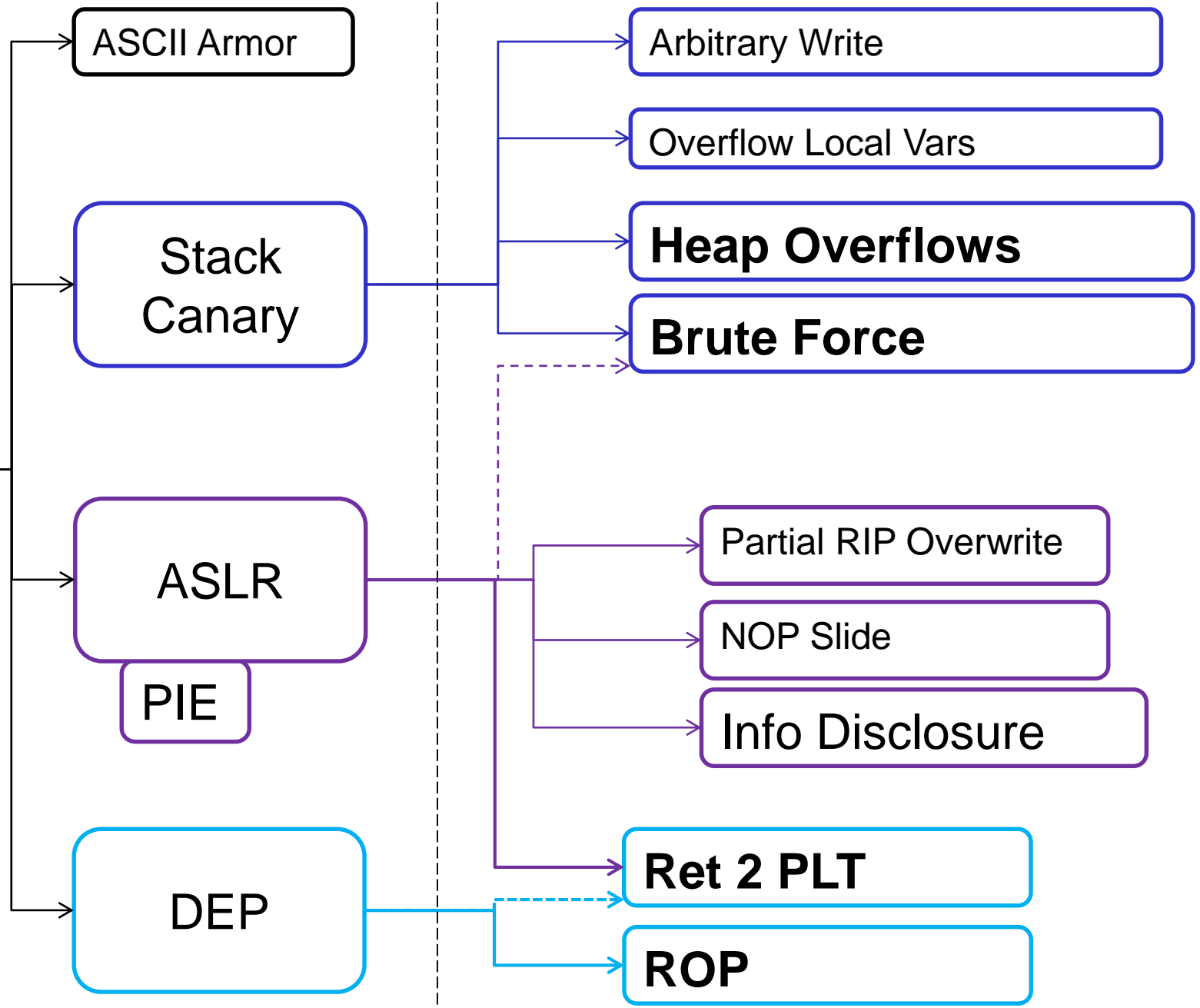
Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch





Exploit Mitigations



Was gibt es für Anti-Exploit Mechanismen?

- ✦ DEP
- ✦ ASLR
- ✦ Stack Canary

Erzähl mir was über Anti-Exploit Mechanism [X]

- ✦ Gegen welchen Teil eines Exploits schützt es?
- ✦ Wie funktioniert er?
- ✦ Ist der Mechanismus effektiv?
 - ✦ Wann nicht?
 - ✦ Warum nicht?
- ✦ Wird der Mechanismus eingesetzt (Default, Linux, Windows)?