How to build a SOC

Rafael Cloosters | Security Solutions Architect

Was ist überhaupt ein SOC?

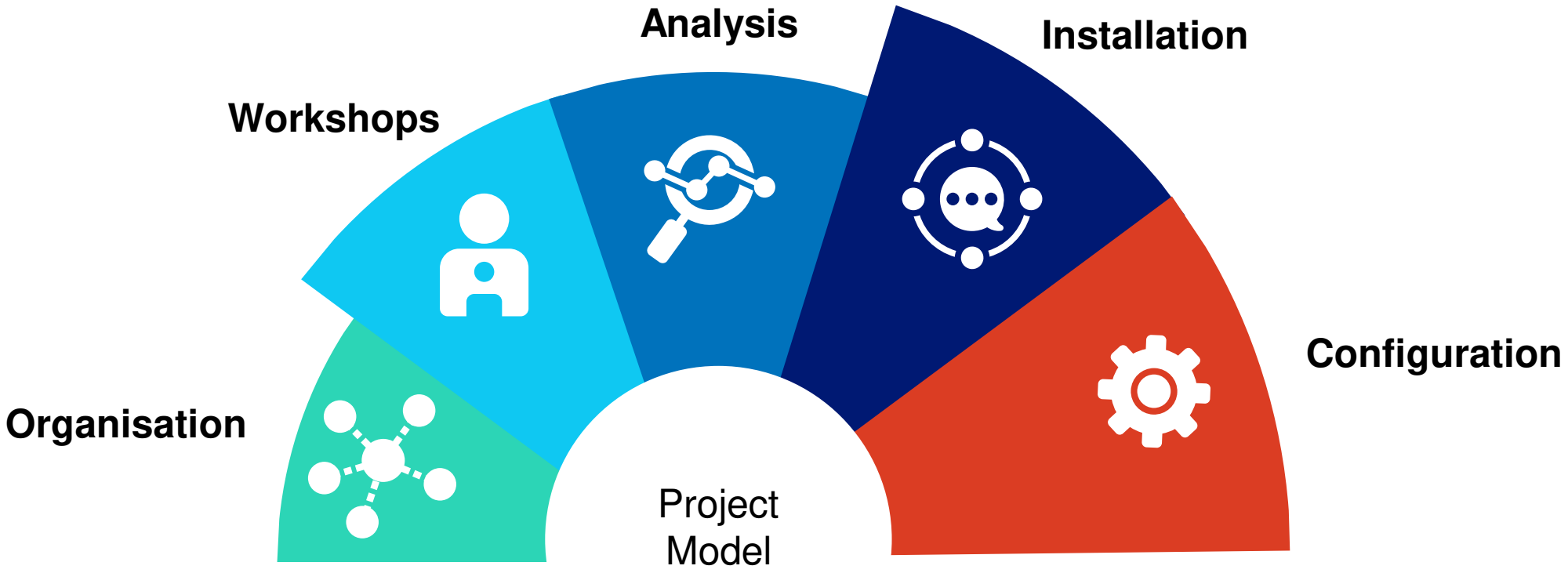
- Security Monitoring + Incident Communication
- Kein Aktives eingreifen
- Kein Patching

➔ *„Security Monitoring Center“*

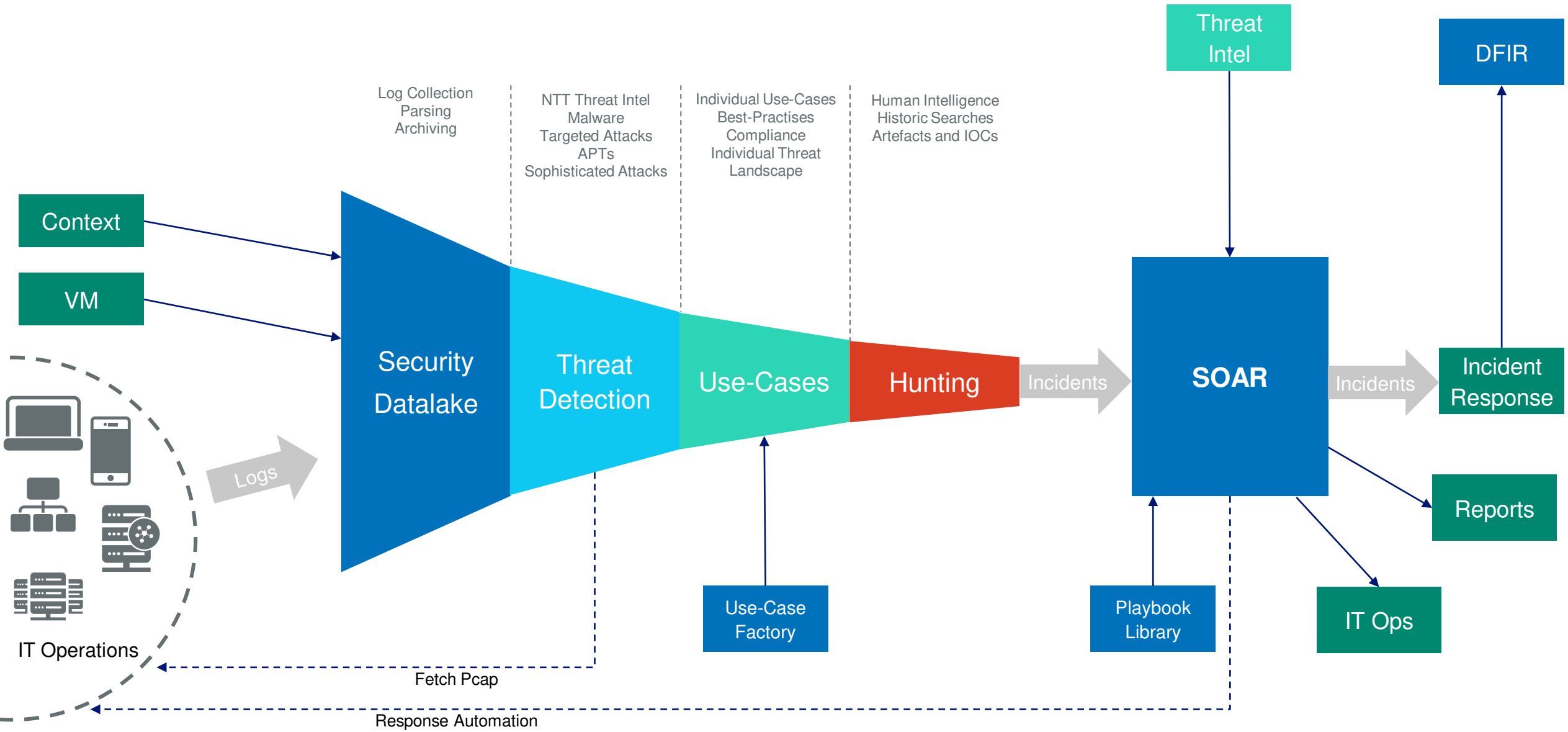
Let‘s build a SOC

Technically
Organizationally

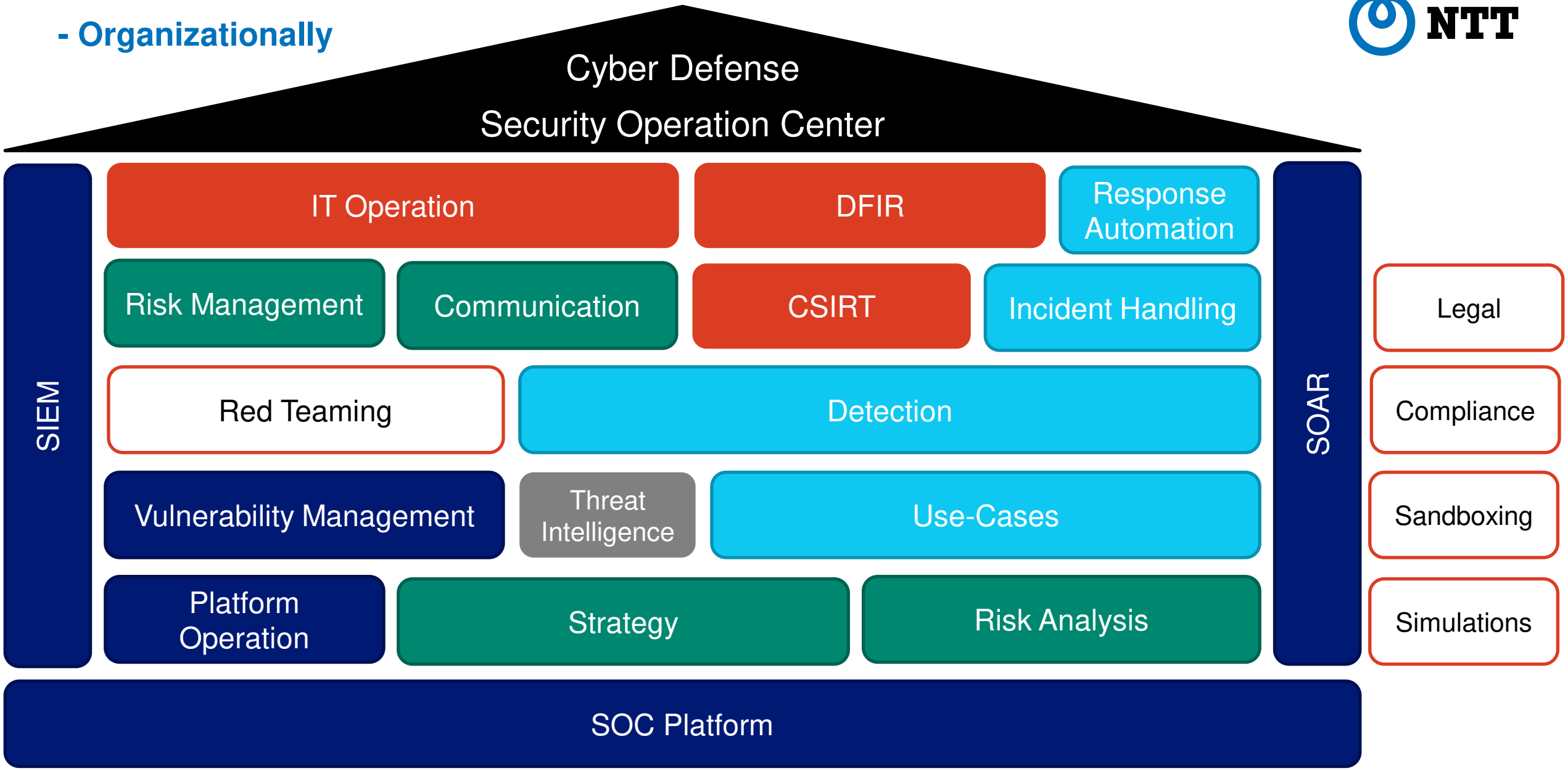
SOC Project



Detection Architecture - Technically



Detection Architecture
- Organizationally



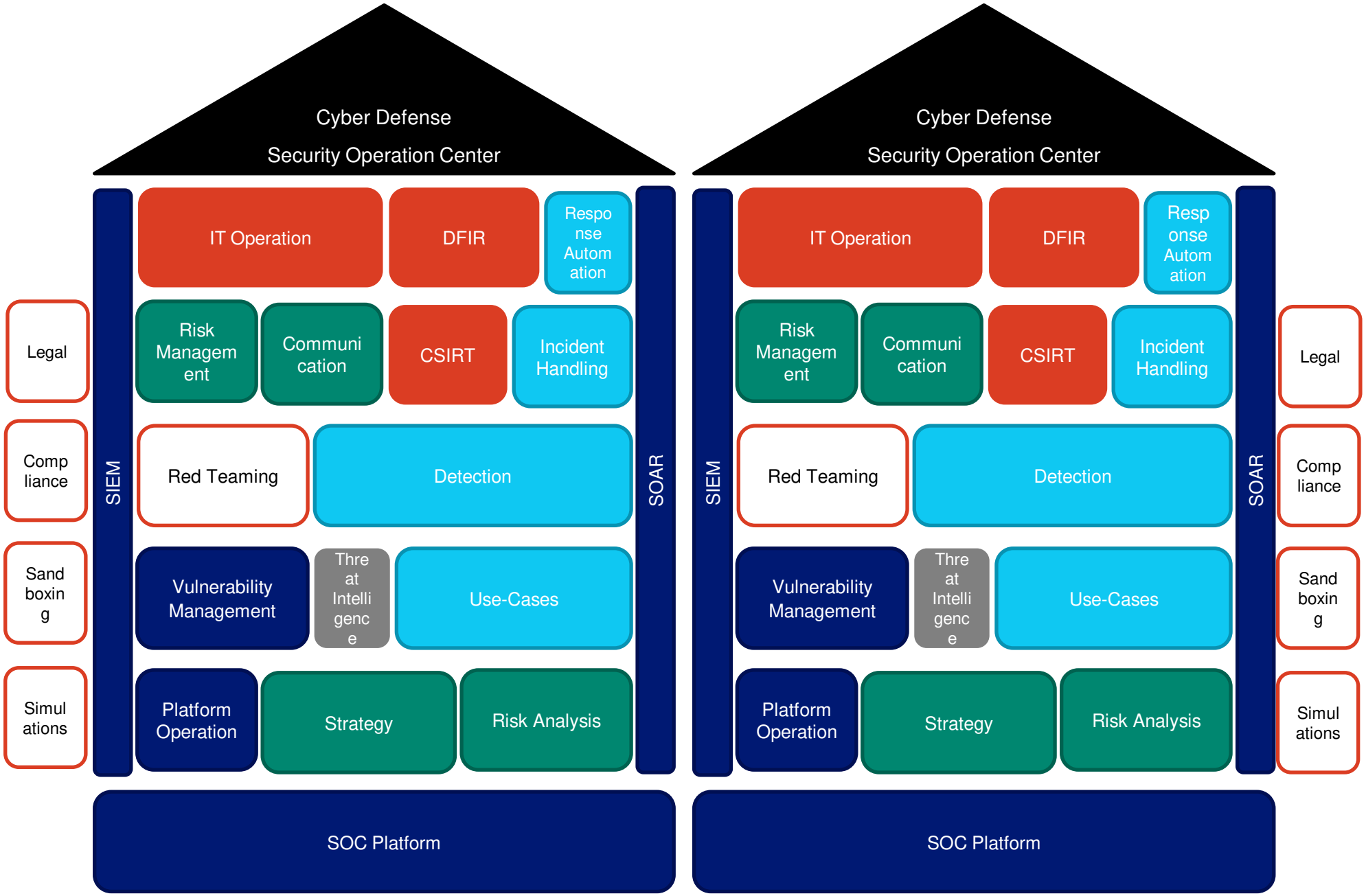
Ist das für kleinere Organisationen zu schaffen?

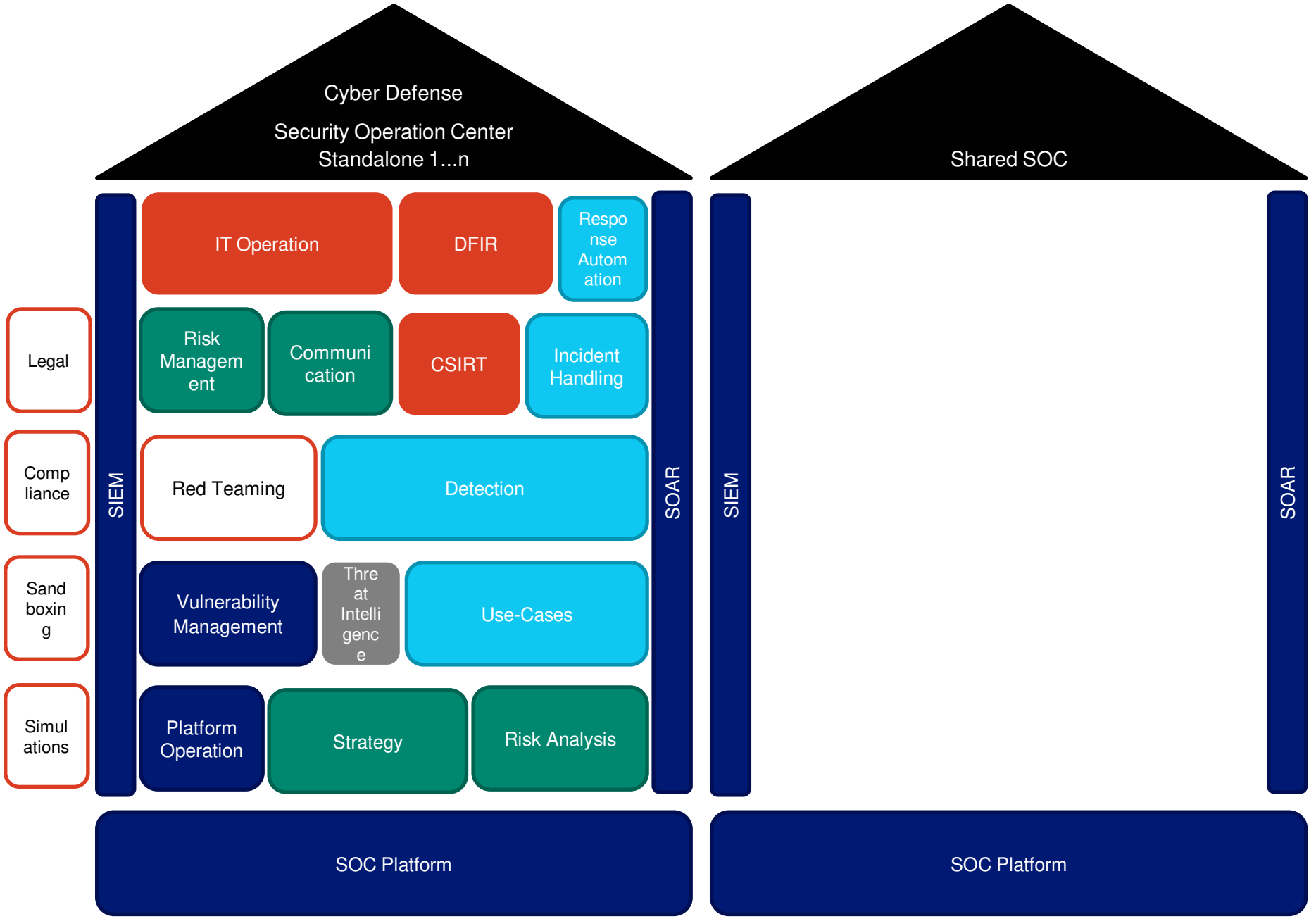
- Große & Komplexe Tools
- Großer Wartungsaufwand
- 24/7 Betrieb
- 24/7 Rufbereitschaften
- Personalmangel:
  - Betriebsteams
  - Expertenteams

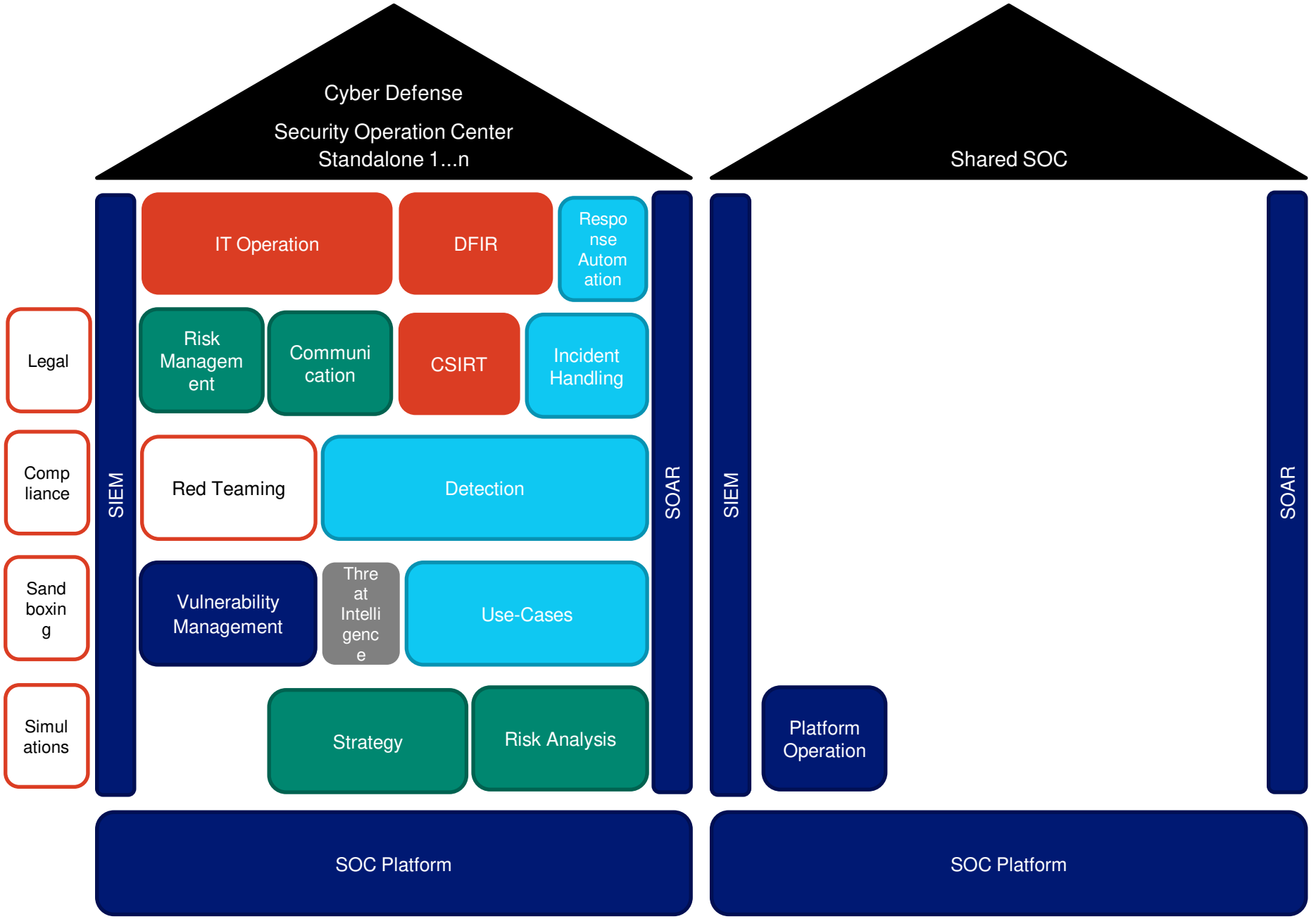
20-25 FTE

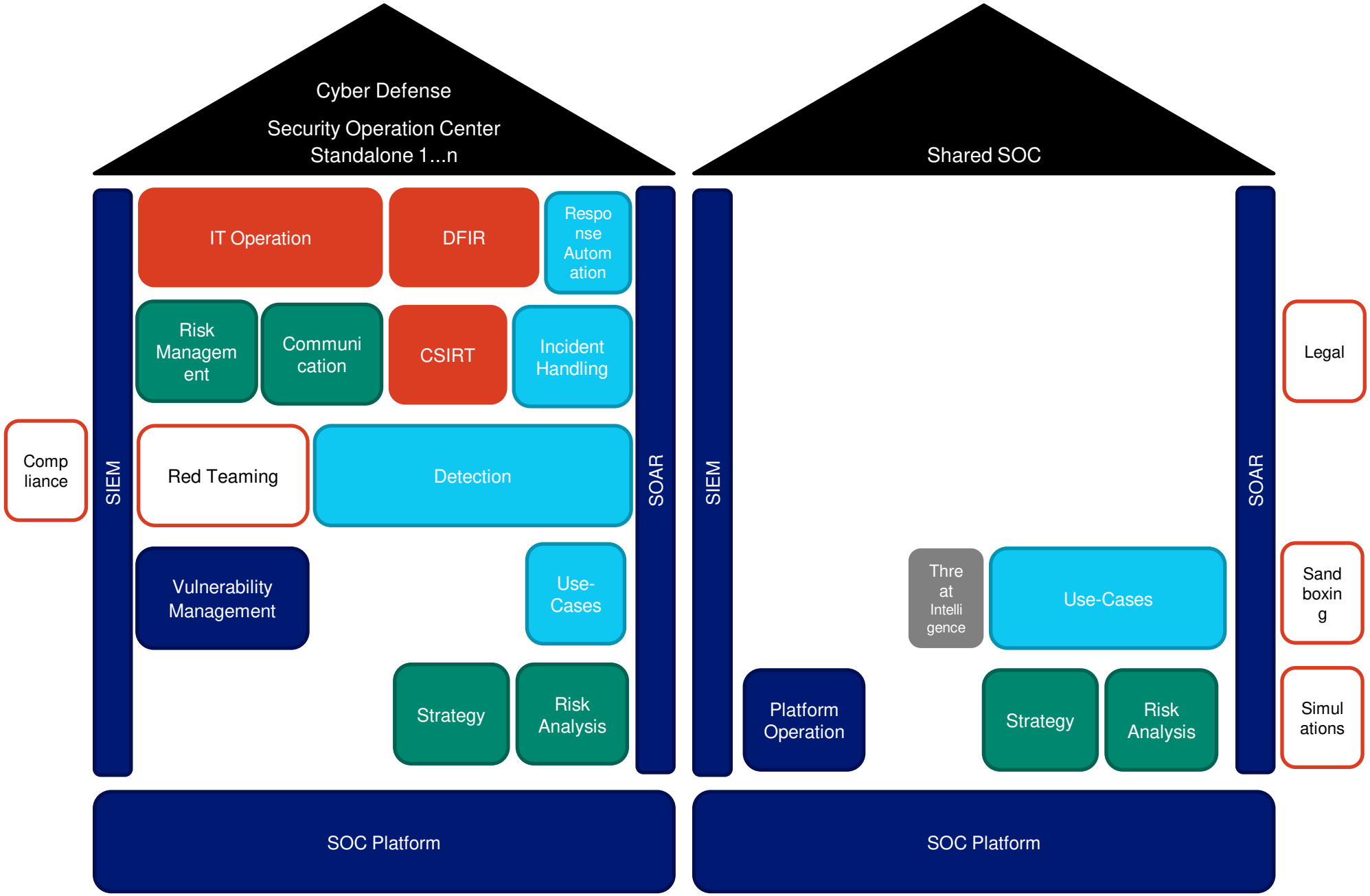
Let‘s build a SOC together

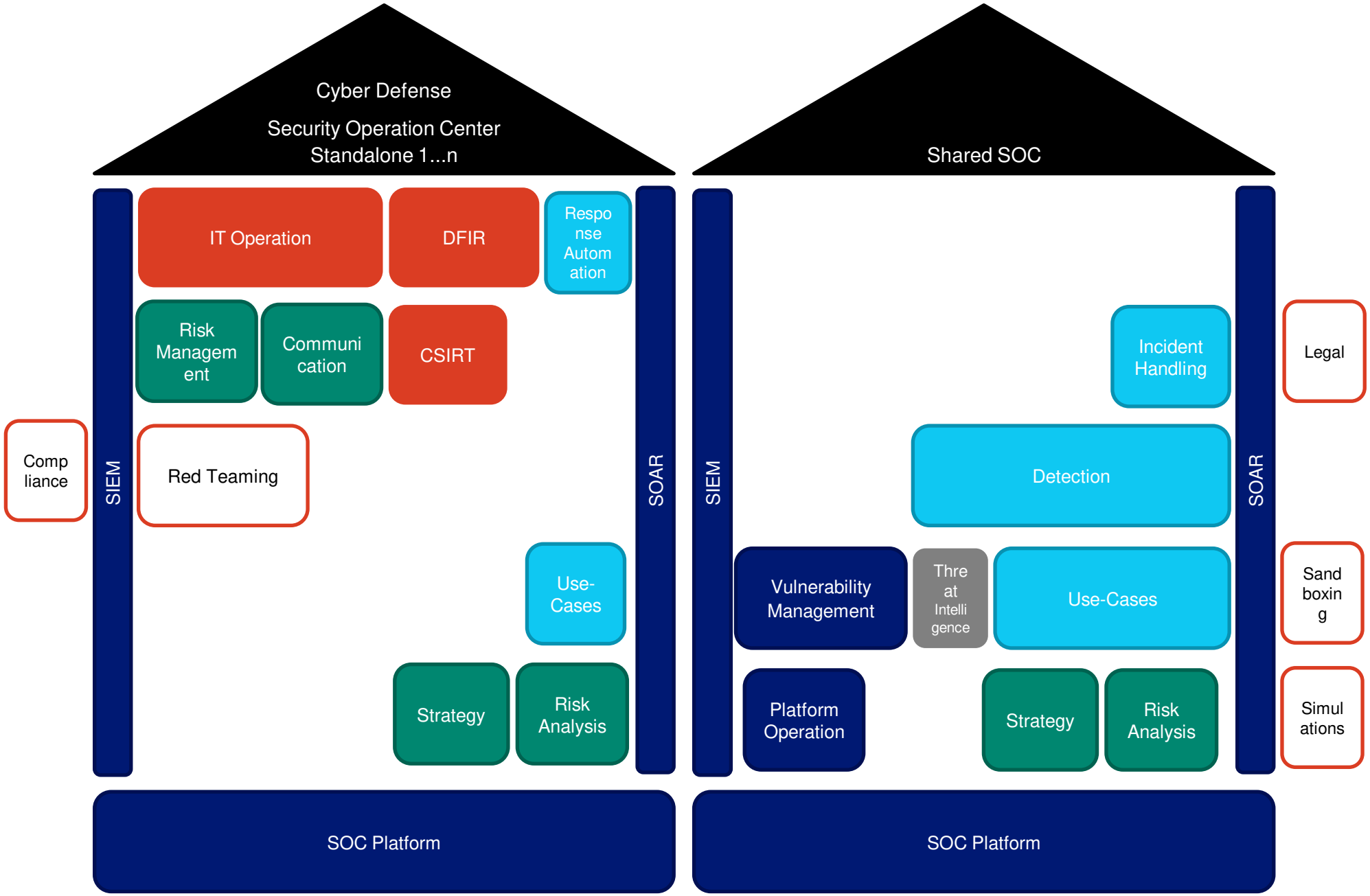
How to handle the Workload in a Partnership

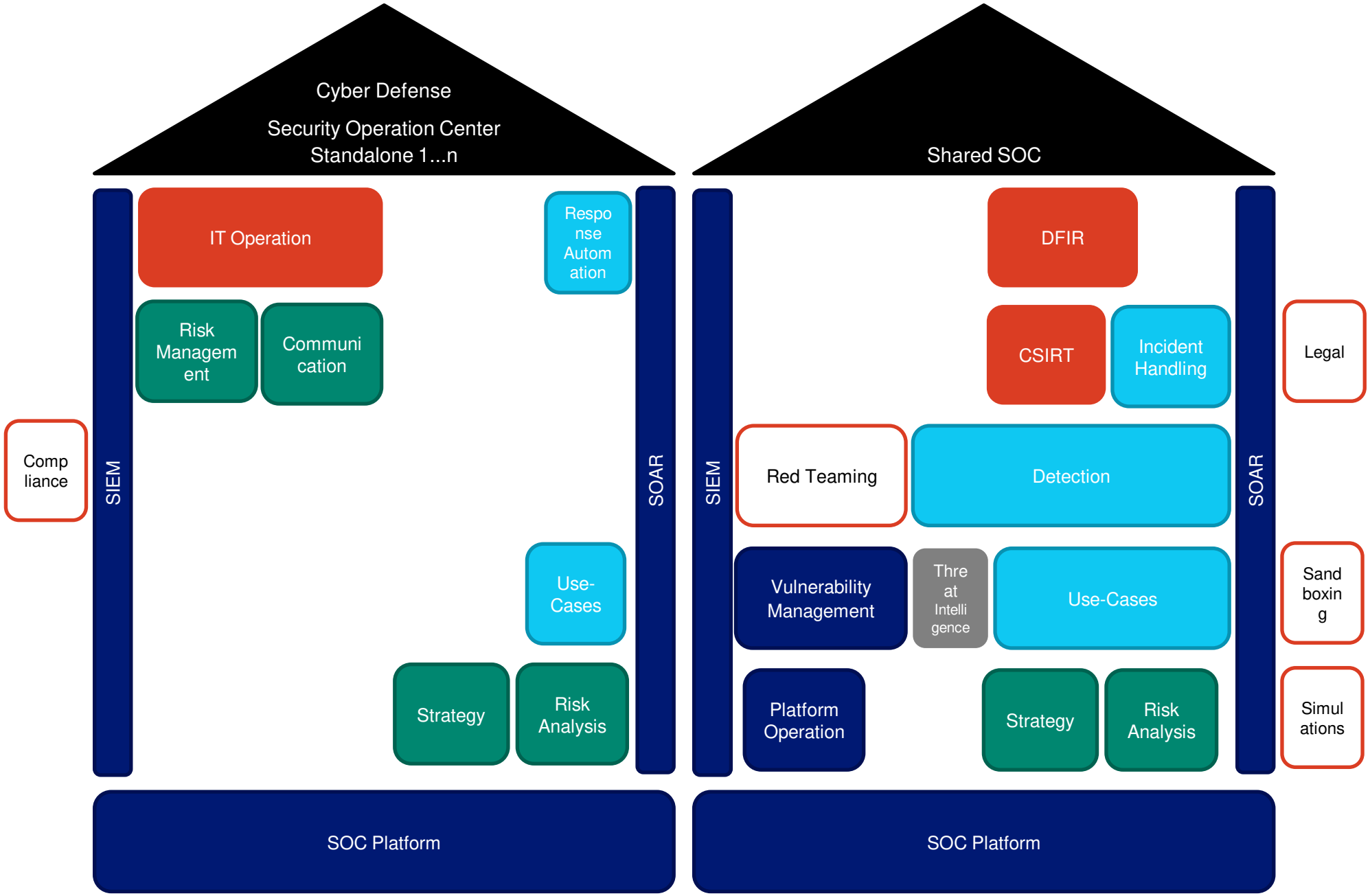


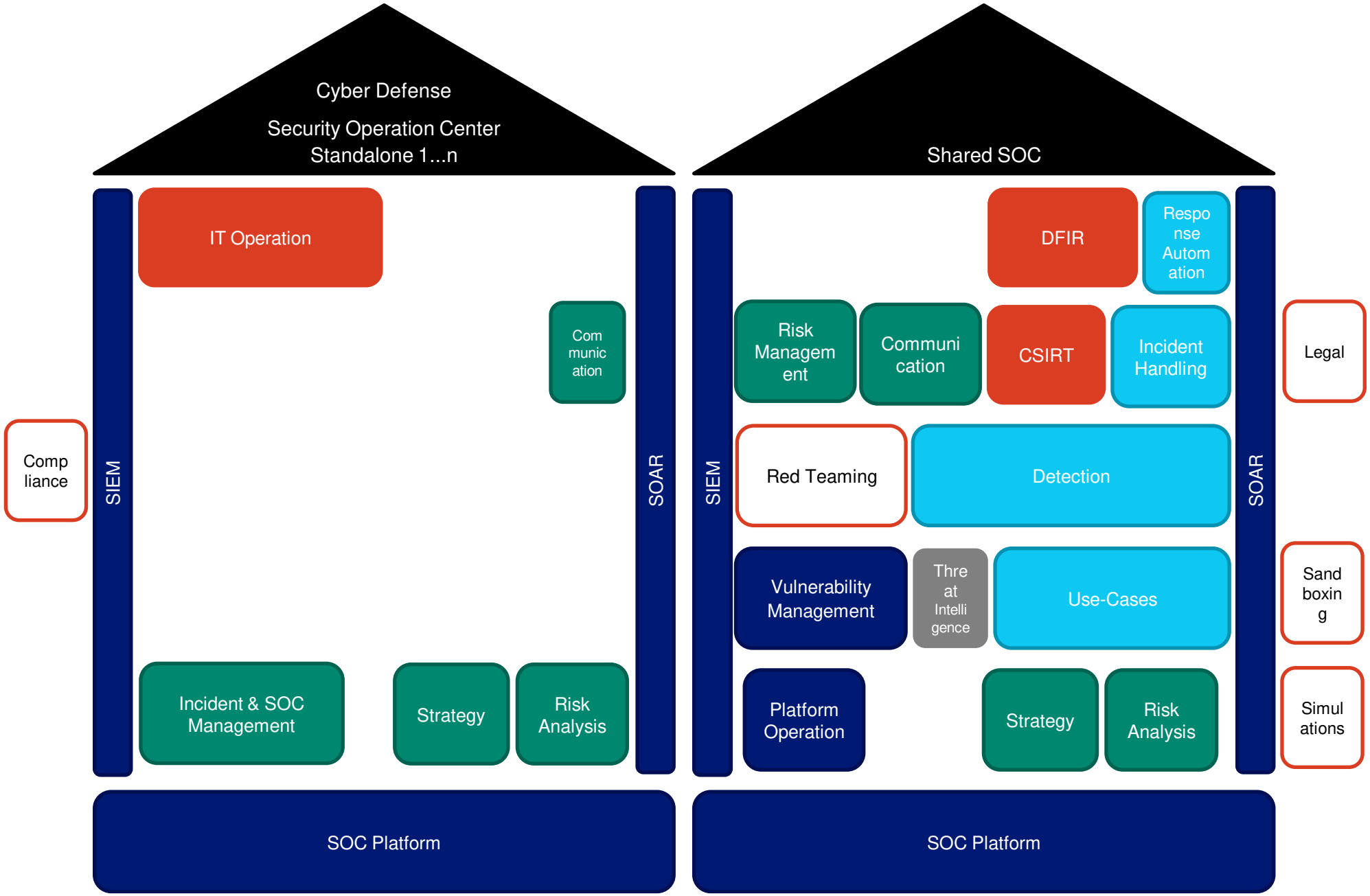


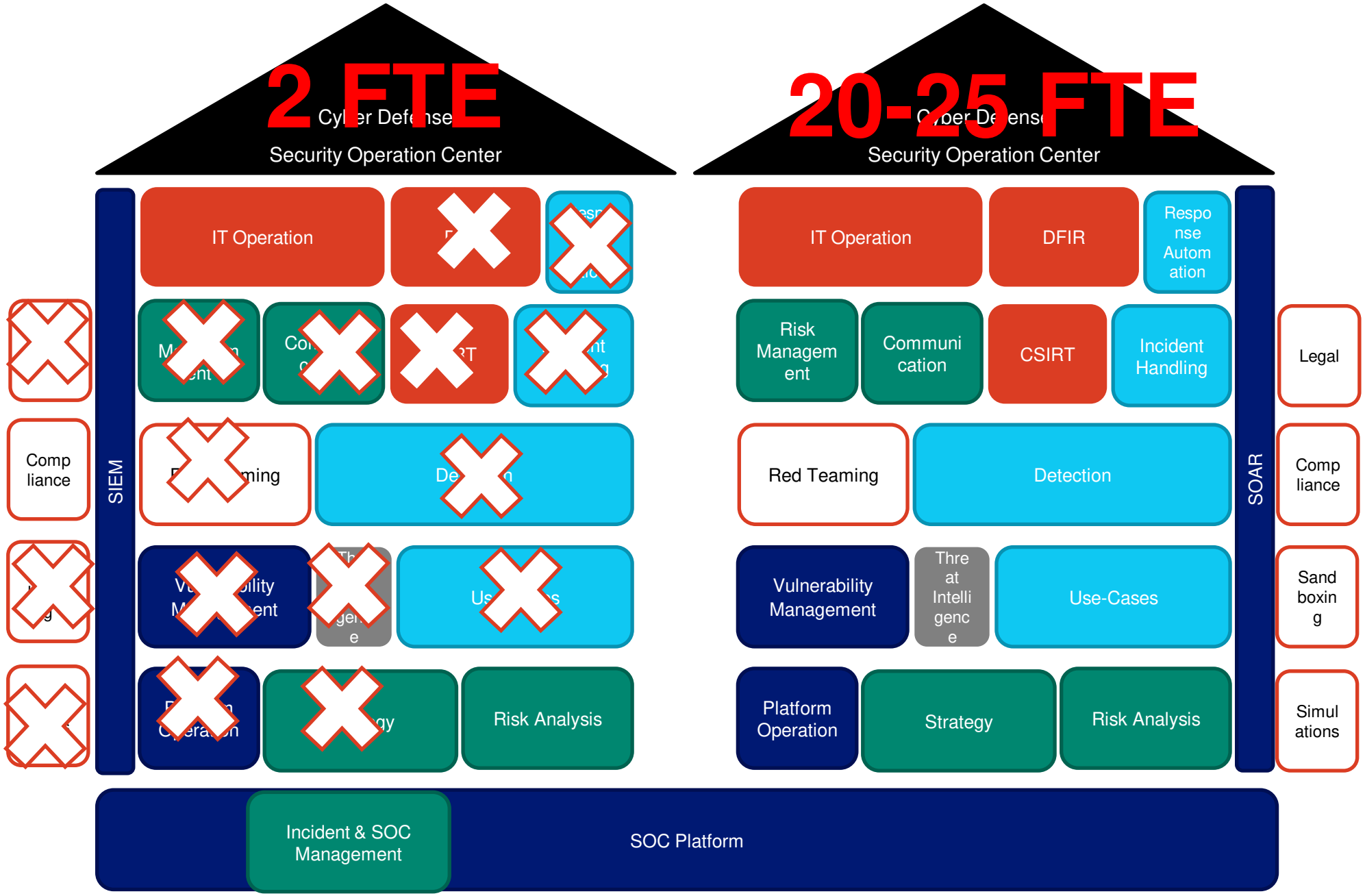


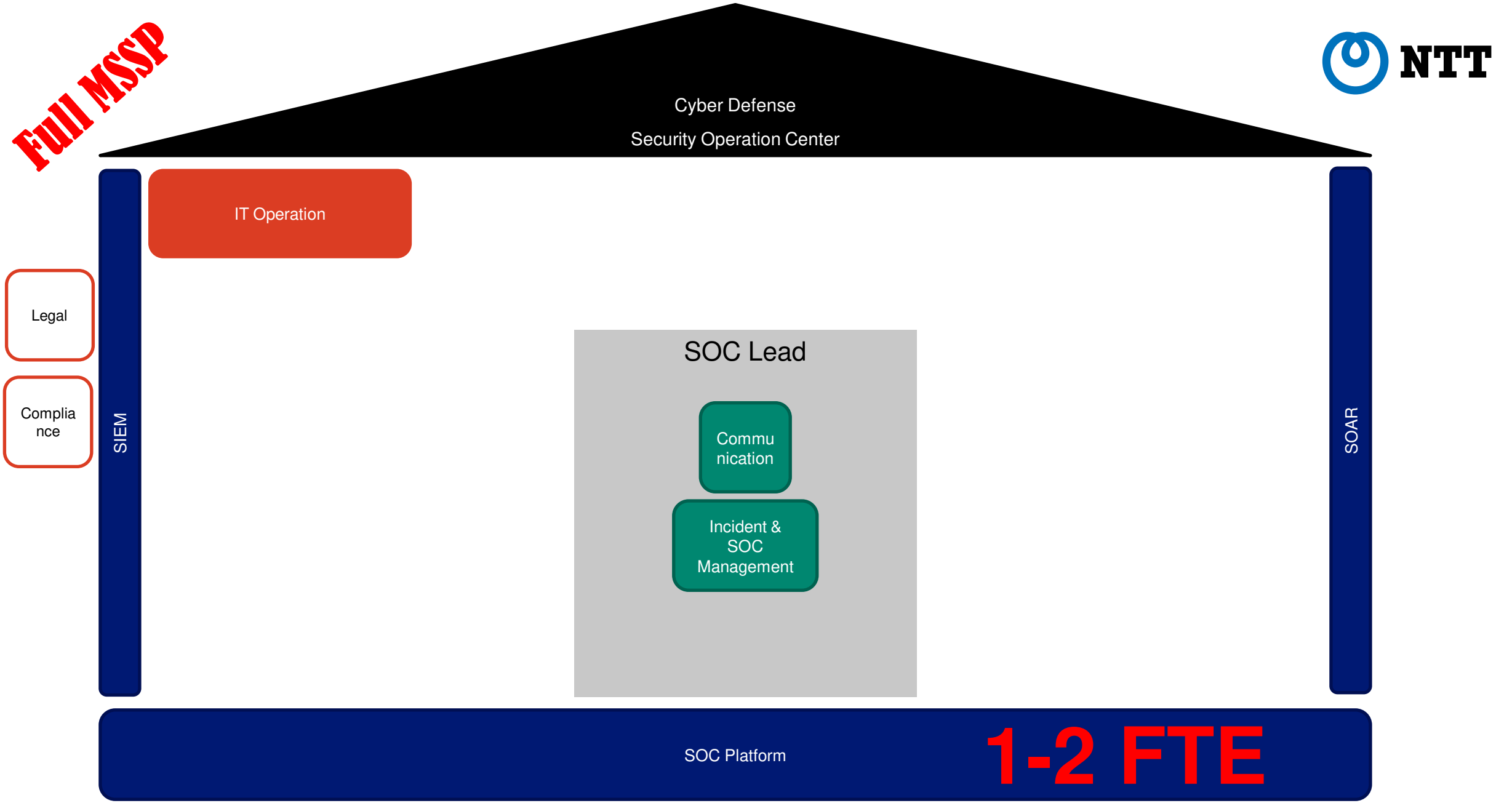












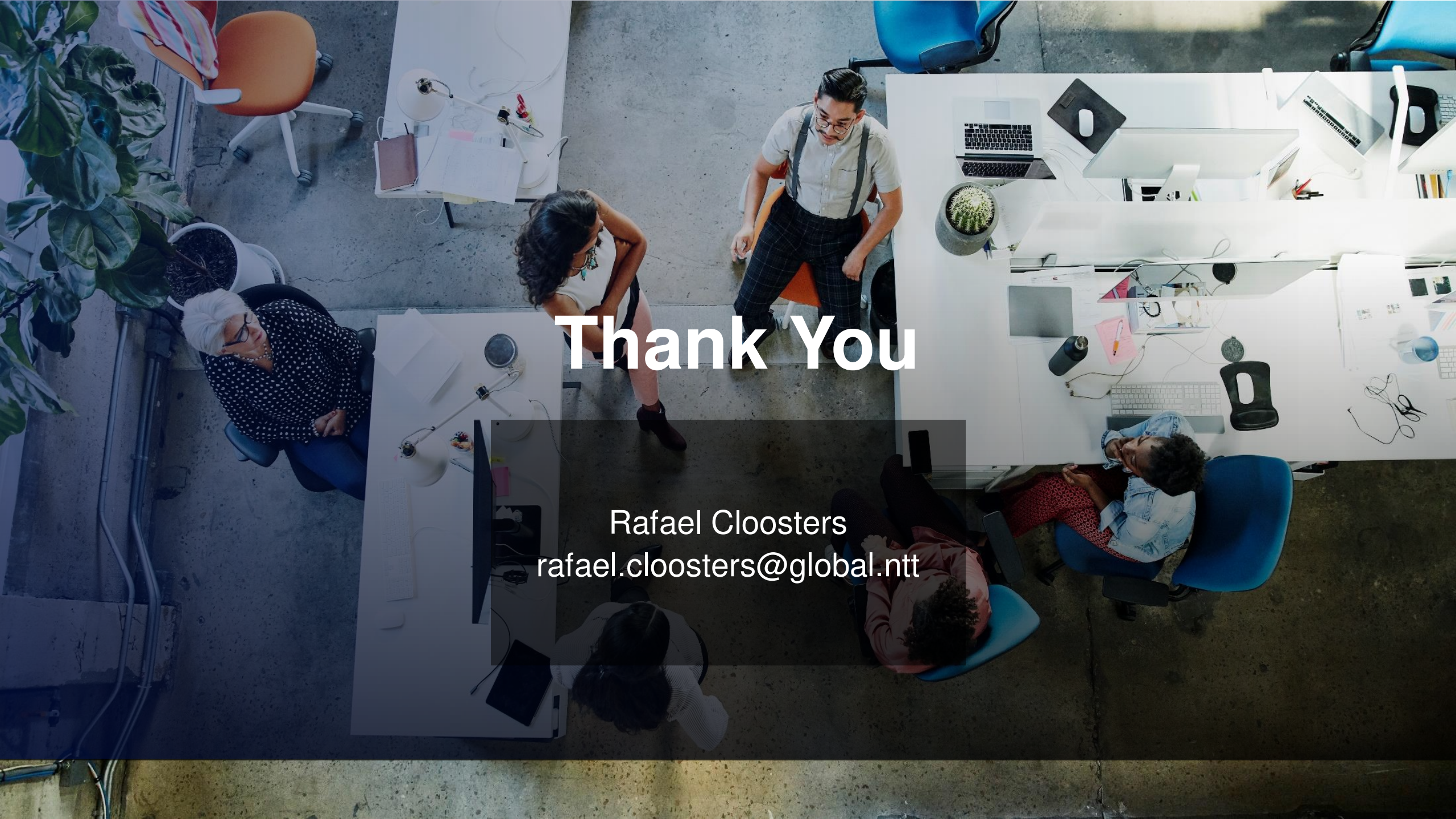
Ist das für kleinere Organisationen zu schaffen?

20-25 FTE

- Technisches Fachwissen
- Expertenteams
- Viel Personal
- 24/7 Betrieb

2 FTE

- Organisatorisches Fachwissen
- Erweiterung der vorhandenen Incident Prozesse
  - Bsp. 24/7 Rufbereitschaft für Security Incidents
- Cyber Security Incidents Response Prozesse etablieren



Thank You

Rafael Cloosters
rafael.cloosters@global.ntt