



How to build a SOC

Rafael Cloosters | Security Solutions Architect

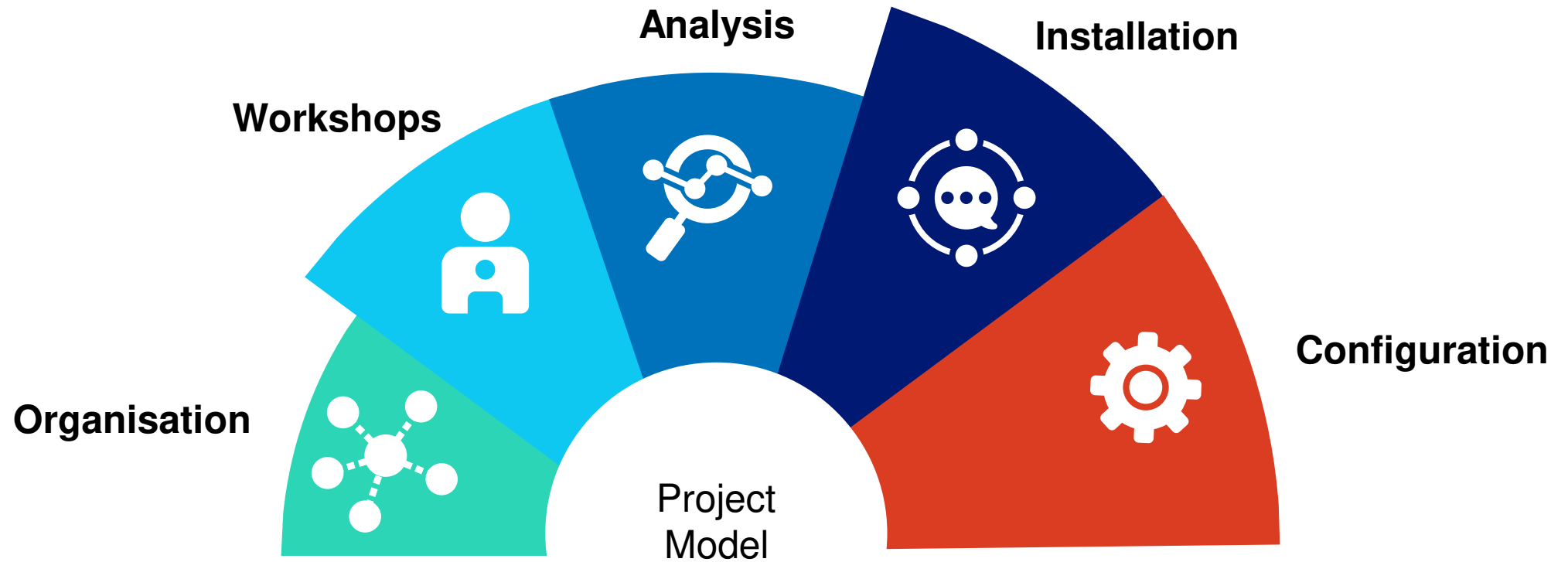
Was ist überhaupt ein SOC?

- Security Monitoring + Incident Communication
 - Kein Aktives eingreifen
 - Kein Patching
- ➔ „*Security Monitoring Center*“

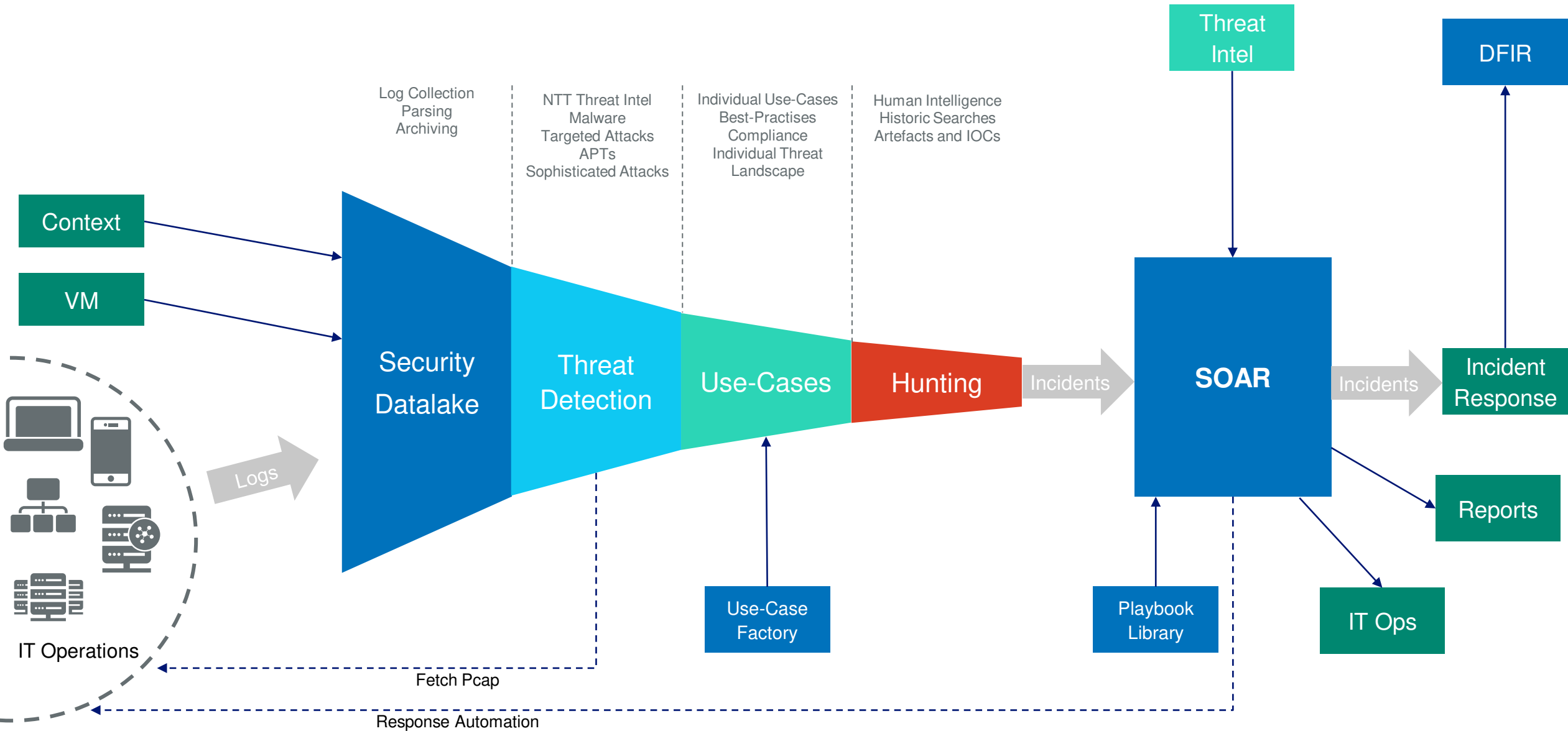
Let's build a SOC

Technically
Organizationally

SOC Project



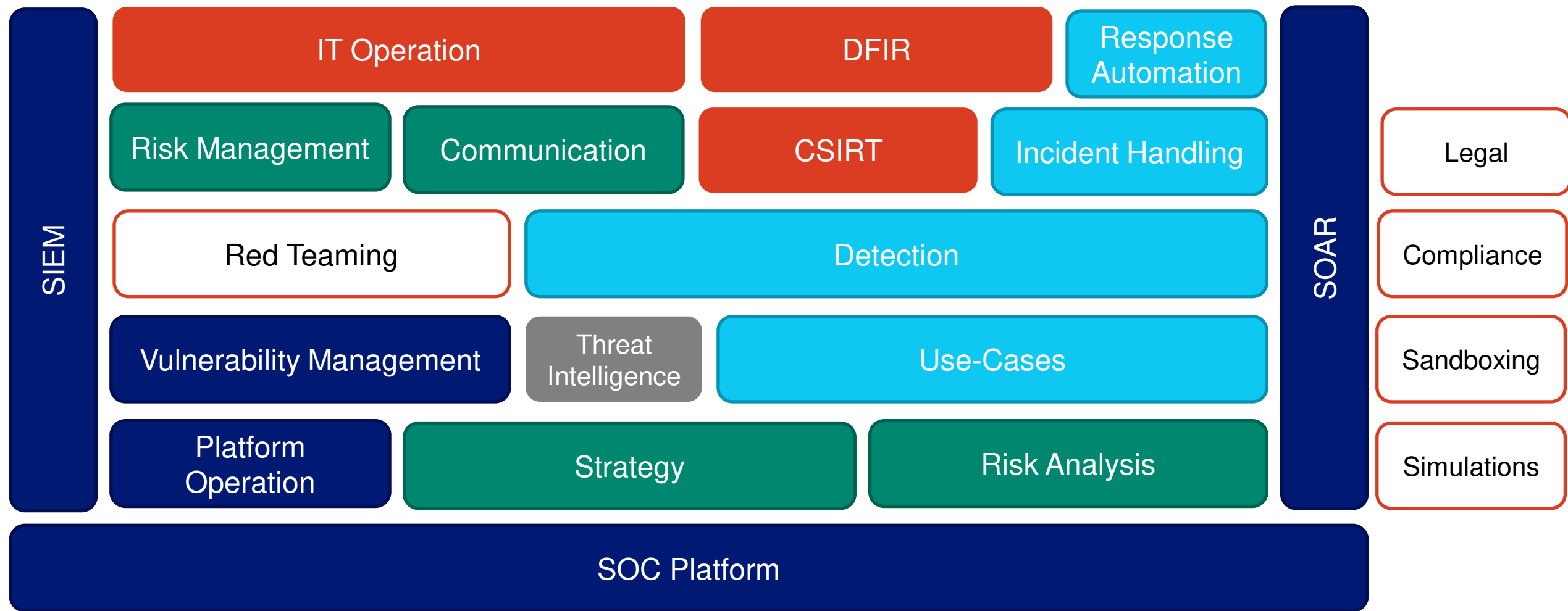
Detection Architecture - Technically



Detection Architecture - Organizationally



Cyber Defense Security Operation Center



Ist das für kleinere Organisationen zu schaffen?

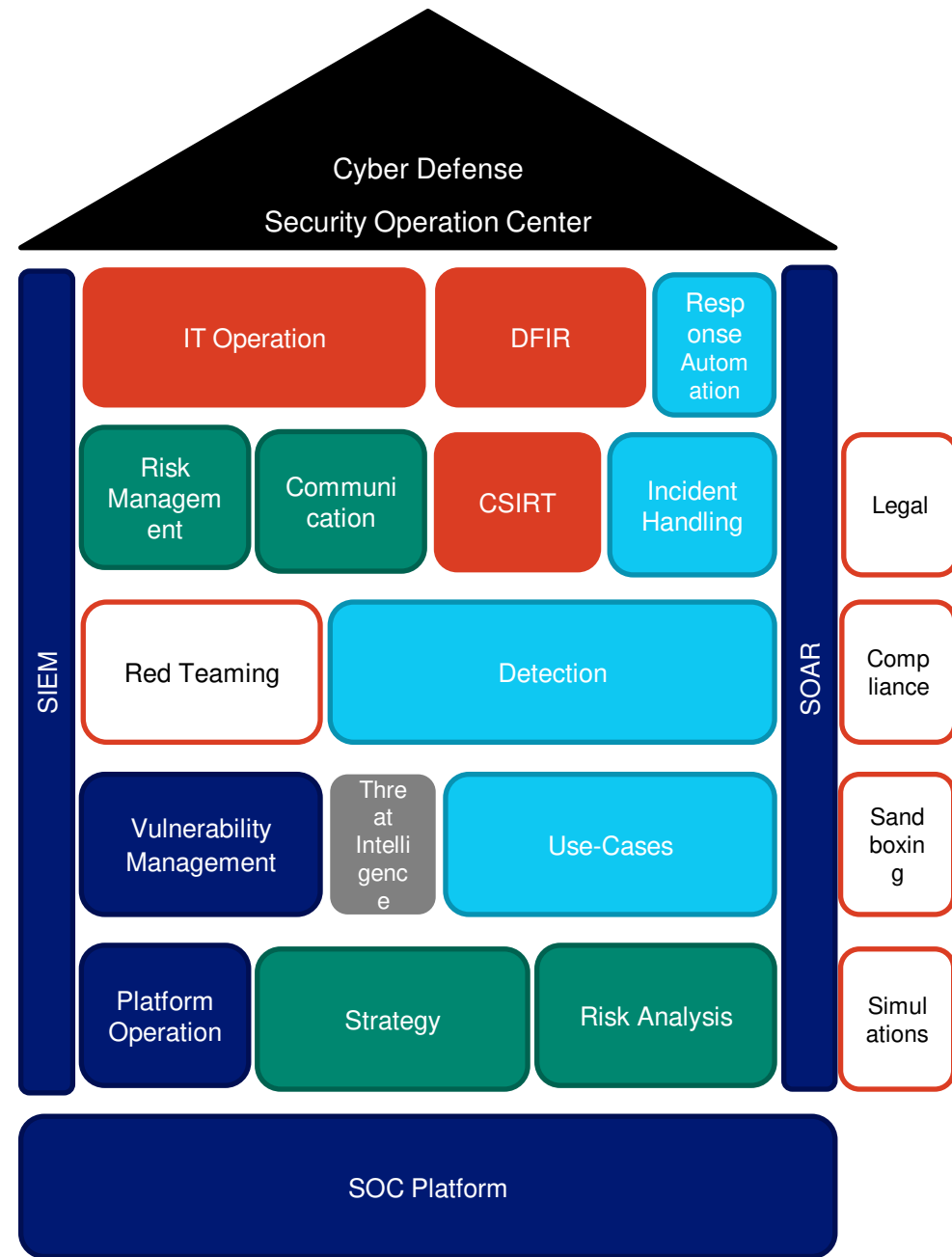
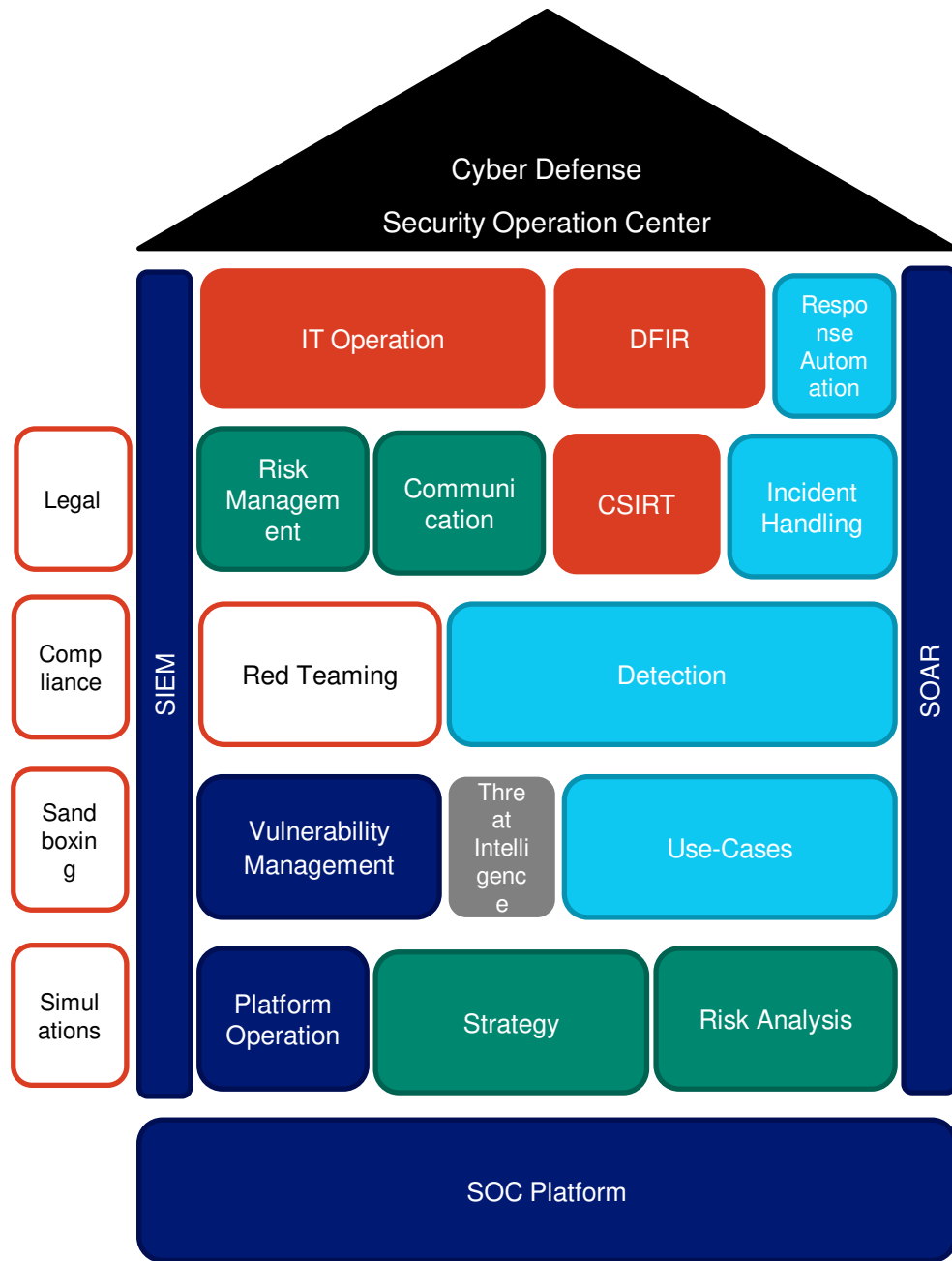


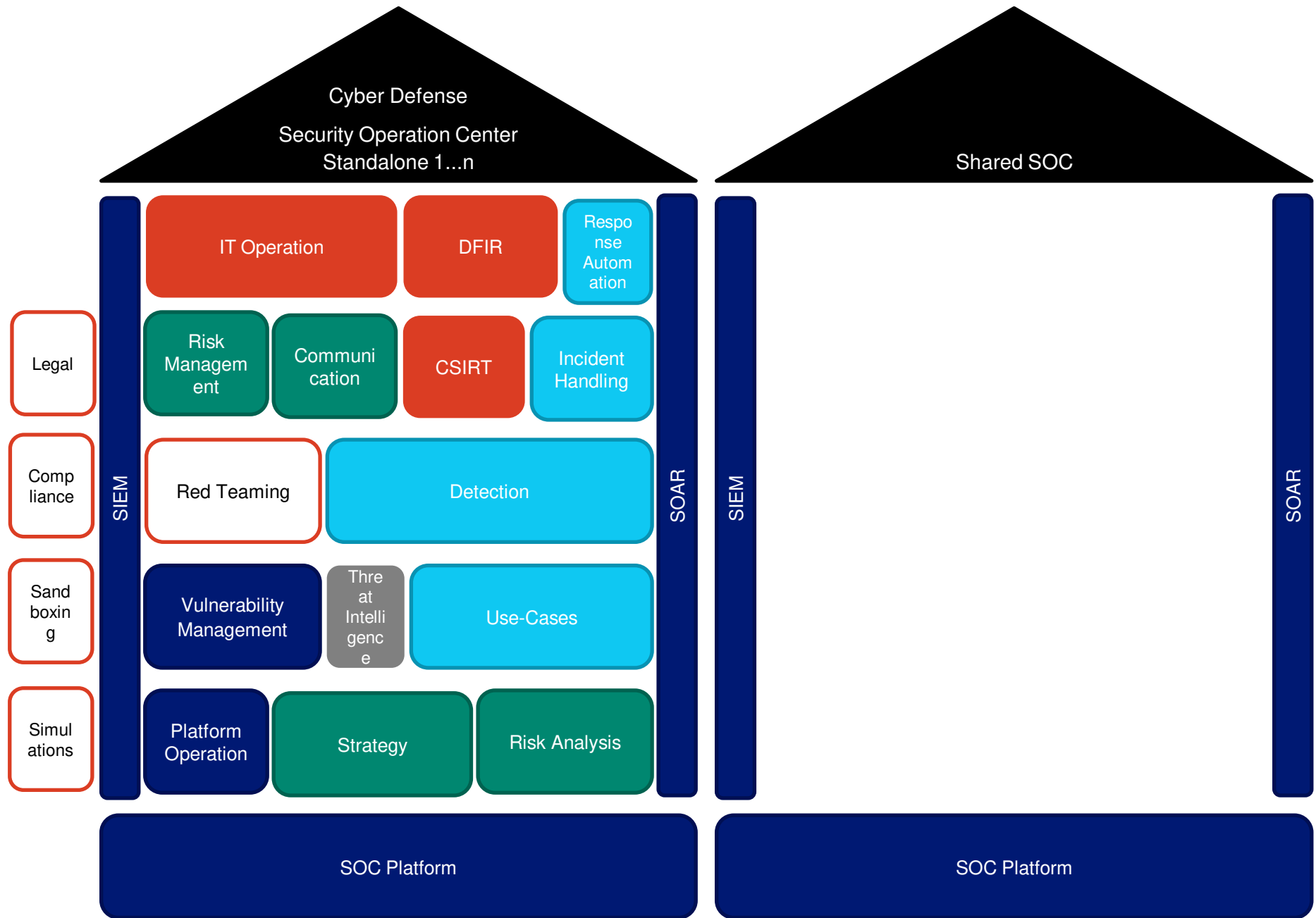
- Große & Komplexe Tools
- Großer Wartungsaufwand
- 24/7 Betrieb
- 24/7 Rufbereitschaften
- Personalmangel:
 - Betriebsteams
 - Expertenteams

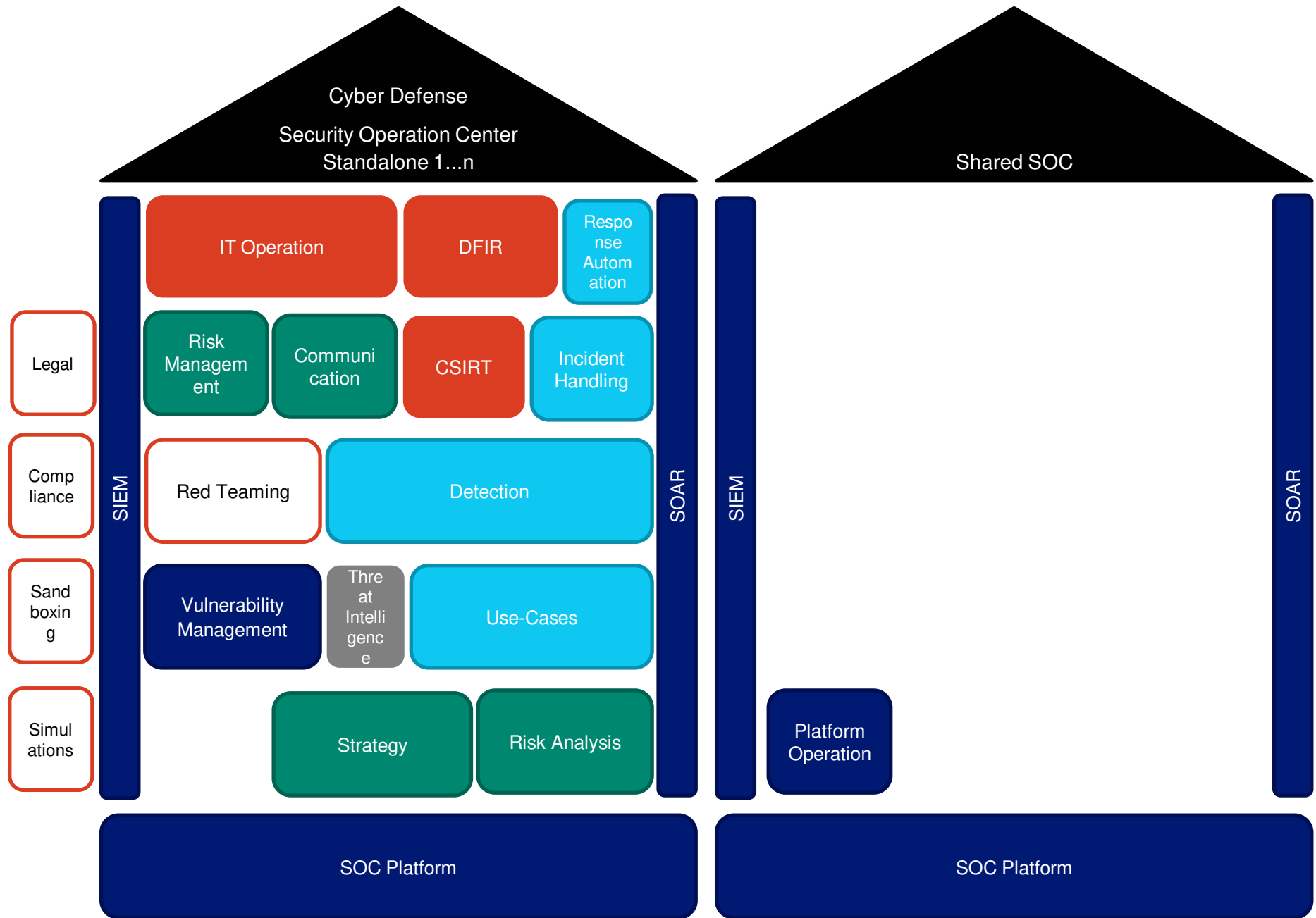
20-25 FTE

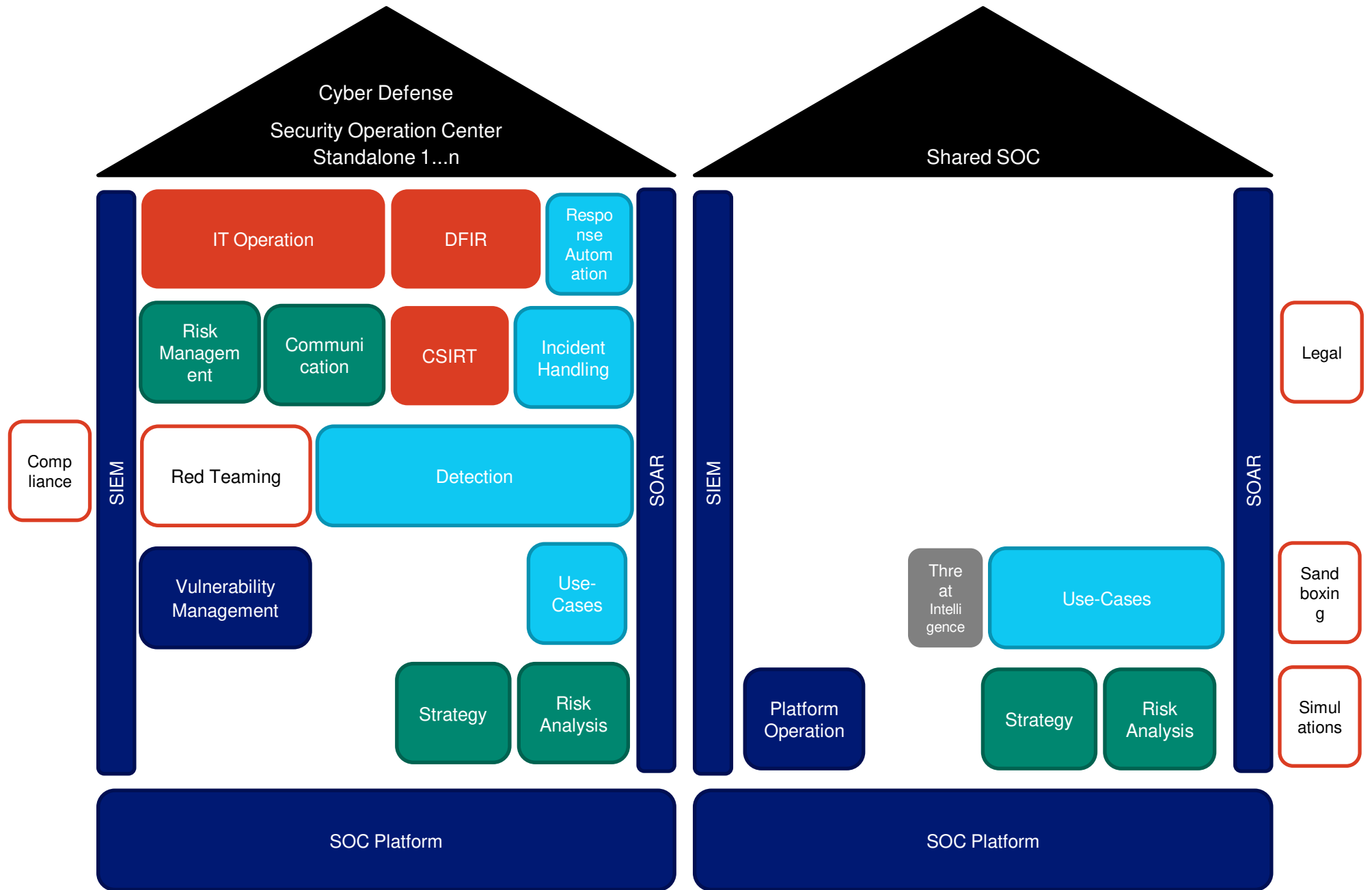
Let's build a SOC together

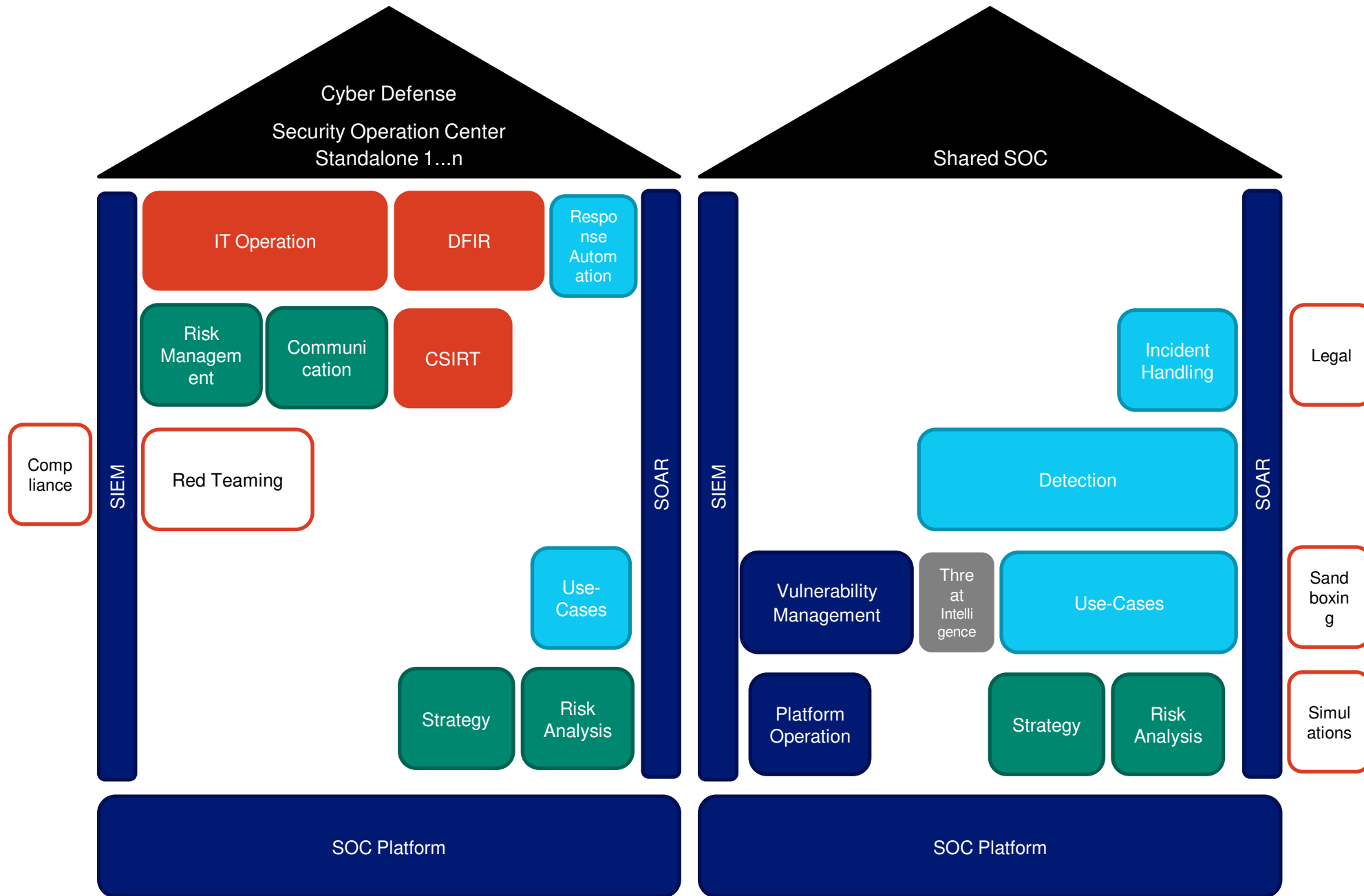
How to handle the Workload in a Partnership

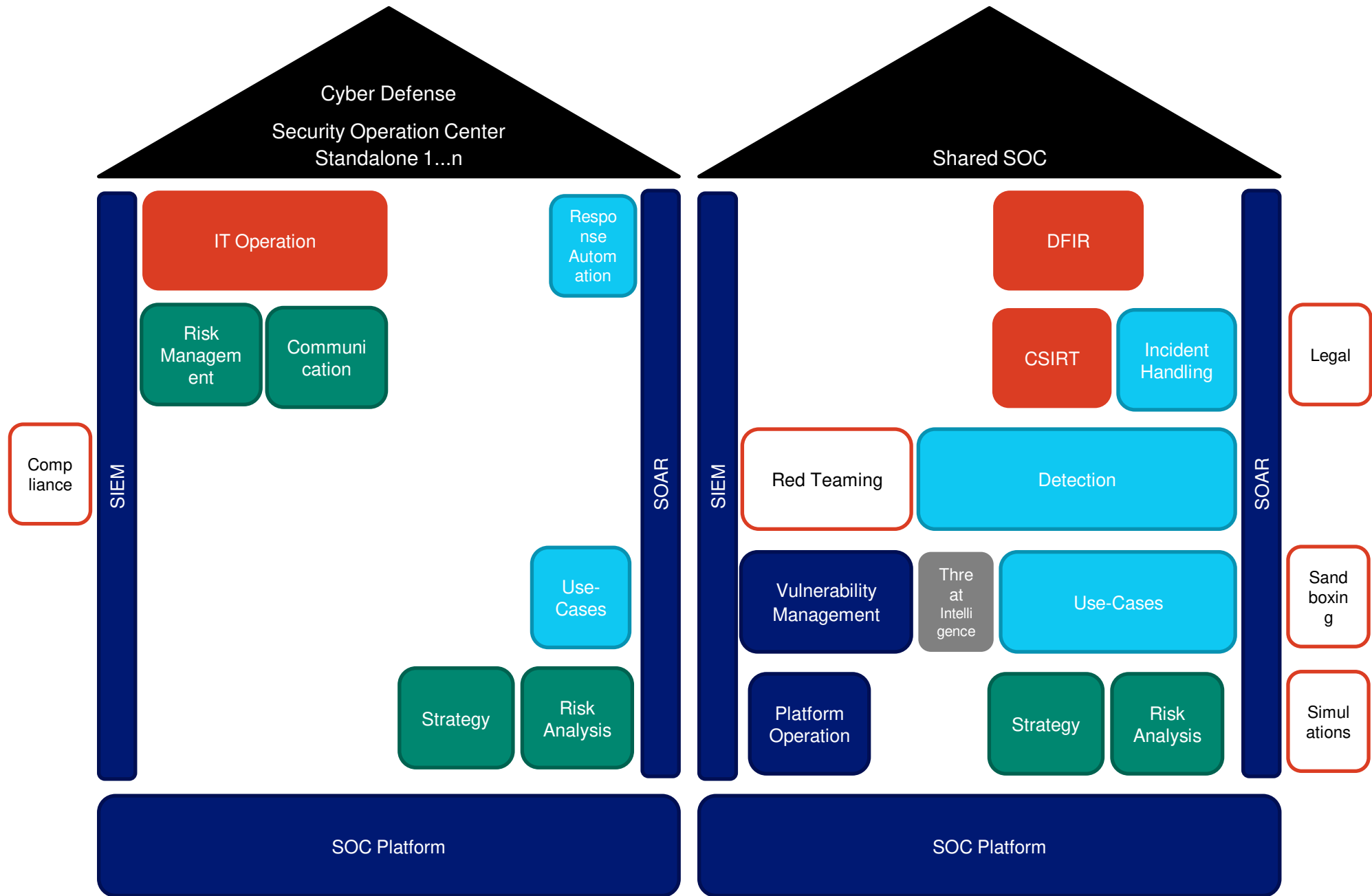


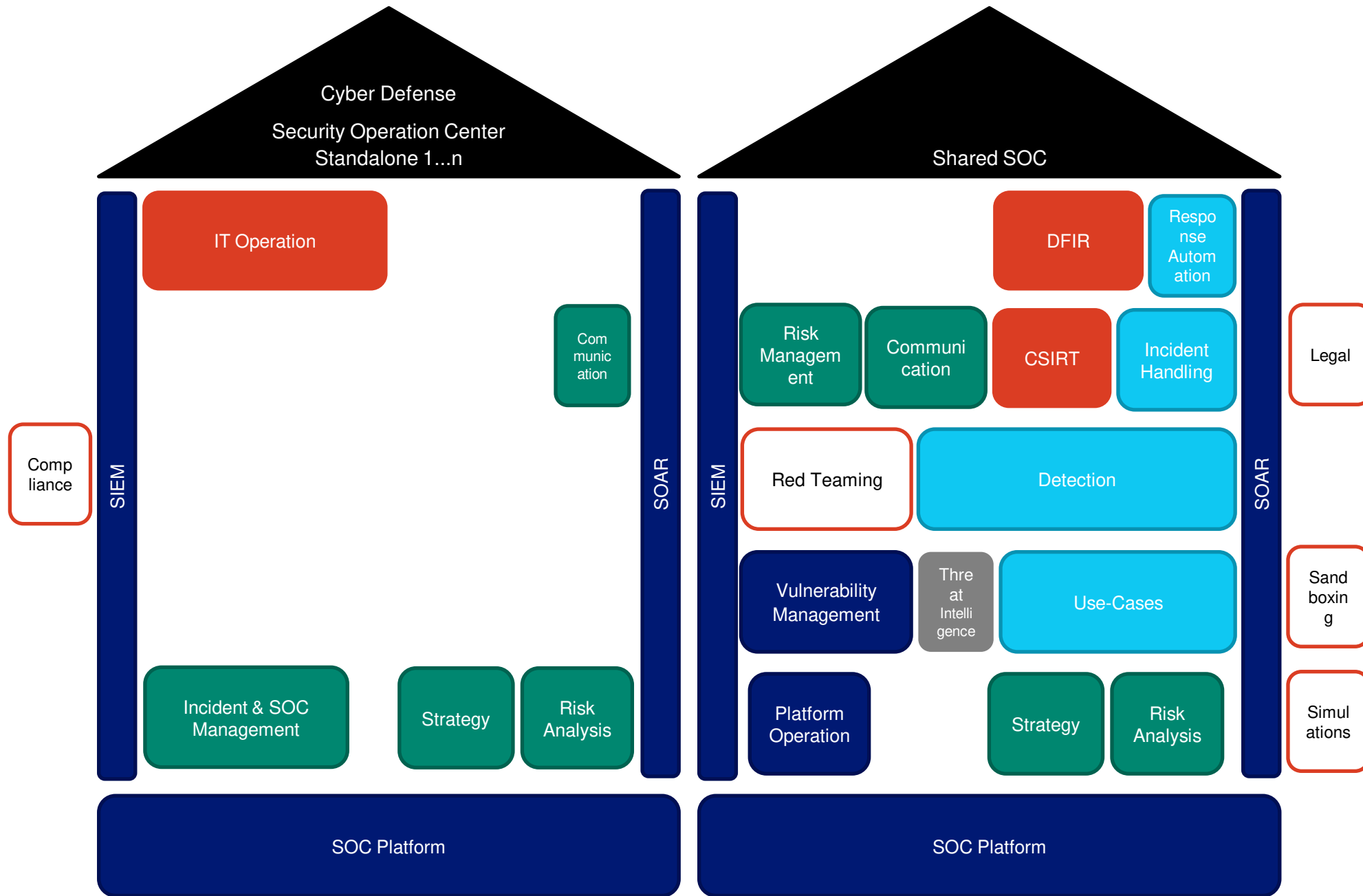










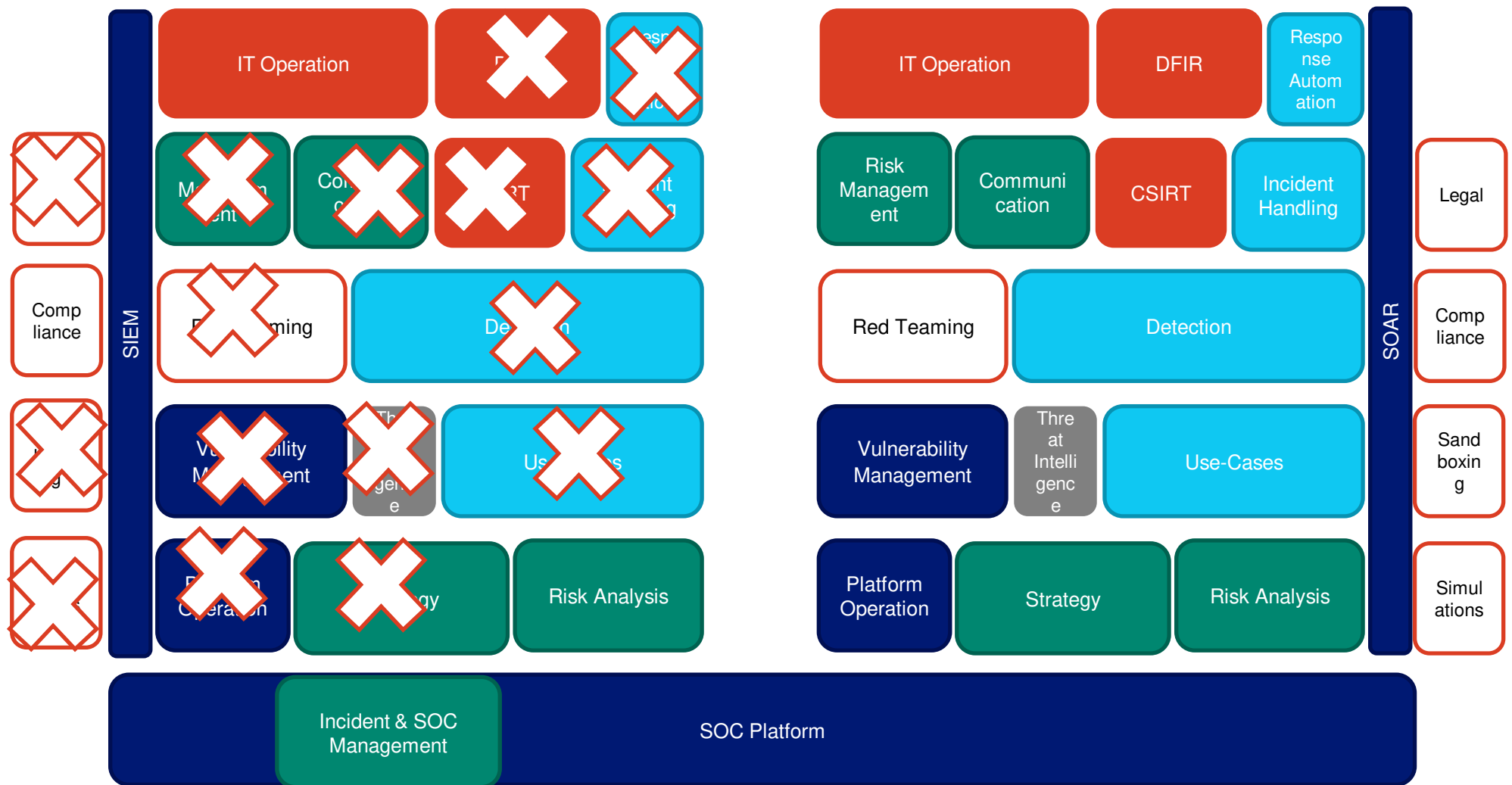


2 FTE

Cyber Defense
Security Operation Center

20-25 FTE

Cyber Defense
Security Operation Center



Full MSSP



Cyber Defense
Security Operation Center

IT Operation

Legal

Compliance

SIEM

SOAR

SOC Lead

Communication

Incident &
SOC
Management

SOC Platform

1-2 FTE

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

An overhead, top-down view of a modern office space. The office is divided into several workstations with white desks. On the left, a woman with white hair and glasses sits at a desk. In the center, a man in a light shirt and suspenders stands talking to a woman. On the right, a woman in a denim shirt sits at a desk. At the bottom, a woman in a pink shirt sits at a desk. The desks are equipped with computers, monitors, keyboards, and various office supplies. A large potted plant is visible on the far left. The floor is a light-colored concrete.

Thank You

Rafael Cloosters
rafael.cloosters@global.ntt