

Was ist überhaupt ein SOC

SOC ist die Abkürzung für Security Operation Center. Dies ist eine Zusammenfassung die aus mehreren Komponenten besteht:

- Mitarbeiter die Umgang mit IT Sicherheit geübt oder besser noch geschult sind
- Produkte für die IT Sicherheit
- Einen Raum (mindestns) der für diesen Zweck vorgesehen ist und entsprechend eingerichtet ist (z.B. mit mehreren Monitoren zur Überwachung)

Die üblichen Aufgaben der Mitarbeiter umfassen:

- Überwachen der Infrastruktur
- Betreuen der Infrastruktur
- Updates der Infrastruktur
- Schulen der Kolleginnen und Kollegen
- Überwachen und Betreuen der Clouddienste
- Überwachen und Betreuen der Internetanbindung

Revision #1

Created 2022-12-17 12:39:23 UTC by Peter Leibling

Updated 2022-12-17 13:29:26 UTC by Peter Leibling