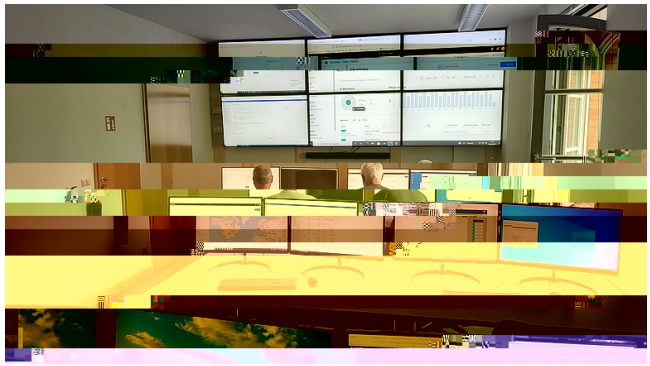
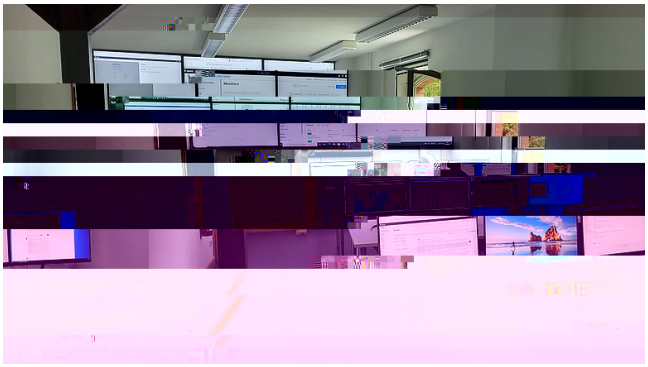
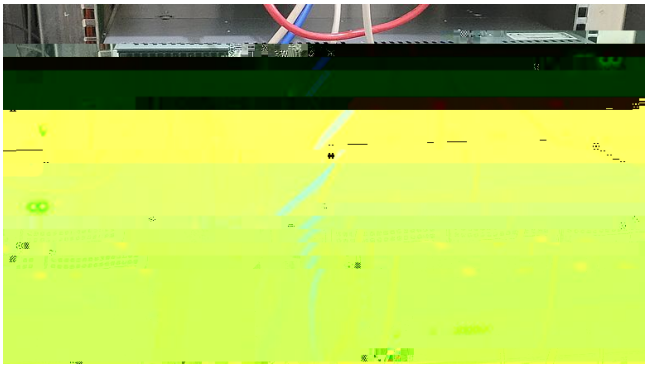
Demo-SOC

In Zeiten von RansomWare (Verschlüsselungstrojaner) und Advanced Persistant Threats (hochwertige, gezielte Angriffe) wird die frühzeitige Erkennung von Cyberangriffen und anderen sicherheitsrelevanten Ereignissen in Organisationen (Detektion) immer wichtiger. Wenngleich ein hundertprozentiger Schutz vor Schadsoftware in einer digitalisierten Gesellschaft faktisch nicht erreichbar ist, kann durch frühzeitige Gegenmaßnahmen (Reaktion) oftmals größerer Schaden abgewendet werden. Die Sicherheitsexperten für diese Detektion und Reaktion werden oftmals in sogenannten "Security Operations Centern" organisiert. Das DemoSOC-Labor bereitet auf einen solchen Einsatz vor: ein vollständiger, moderner Software-Stack insb. für die zentrale SOC-Technologie "Security Incident und Event Management" (auf Basis ElastikStack) lässt die Erkennung von Angriffen komplett nachstellen - realitätsnah mitsamt wandfüllender Monitorwand, wie es aus den Medien inzwischen bekannt ist. Die Projekte im DemoSOC-Labor fokussieren auf die Detektion beim Betrieb Kritischer Infrastrukturen - hier kommen einerseits oftmals sehr interessante und forschungsrelevante IT-Komponenten (beispielsweise Medizintechnik oder Steuerungsanlagen aus der Wasserversorgung) zum Einsatz; andererseits ist der Schutz besonders wichtig, weil die betroffenen Dienstleistungen besonders relevant für die Gesellschaft sind.

Gebäude	Bibliothek
Raum	B.1.11
Wissenschaftl. Leitung	Prof. Dr. Michael Pilgermann
Wissenschaftsgebiete	Netzwerksicherheit; Detektion: Protokollierung, Monitoring und Security Information and Event Management; Sicherheitsüberwachung und Security Operation; Schutz Kritischer Infrastrukturen
Branchenkompetenzfelder	Medien / Information und Kommunikation (IKT)

- 

- 

- 

Ausstattung

- 6 PC-Arbeitsplätze (Windows)
- 1 Visualisierungs-Arbeitsplatz (Windows)
- 6 Mobile Arbeitsplätze (Windows)
- Netzwerkkomponenten (Netgate Firewall, D-Link Switch)
- 2 Server und 1 NAS
- Videoleinwand mit 6 Samsung-Fernsehern und HDMI-Switch

Forschungs-/Ausbildungsschwerpunkte

- Netzwerksicherheit
- Detektion: Protokollierung, Monitoring und Security Information and Event Management
- Sicherheitsüberwachung und Security Operations
- Schutz Kritischer Infrastrukturen