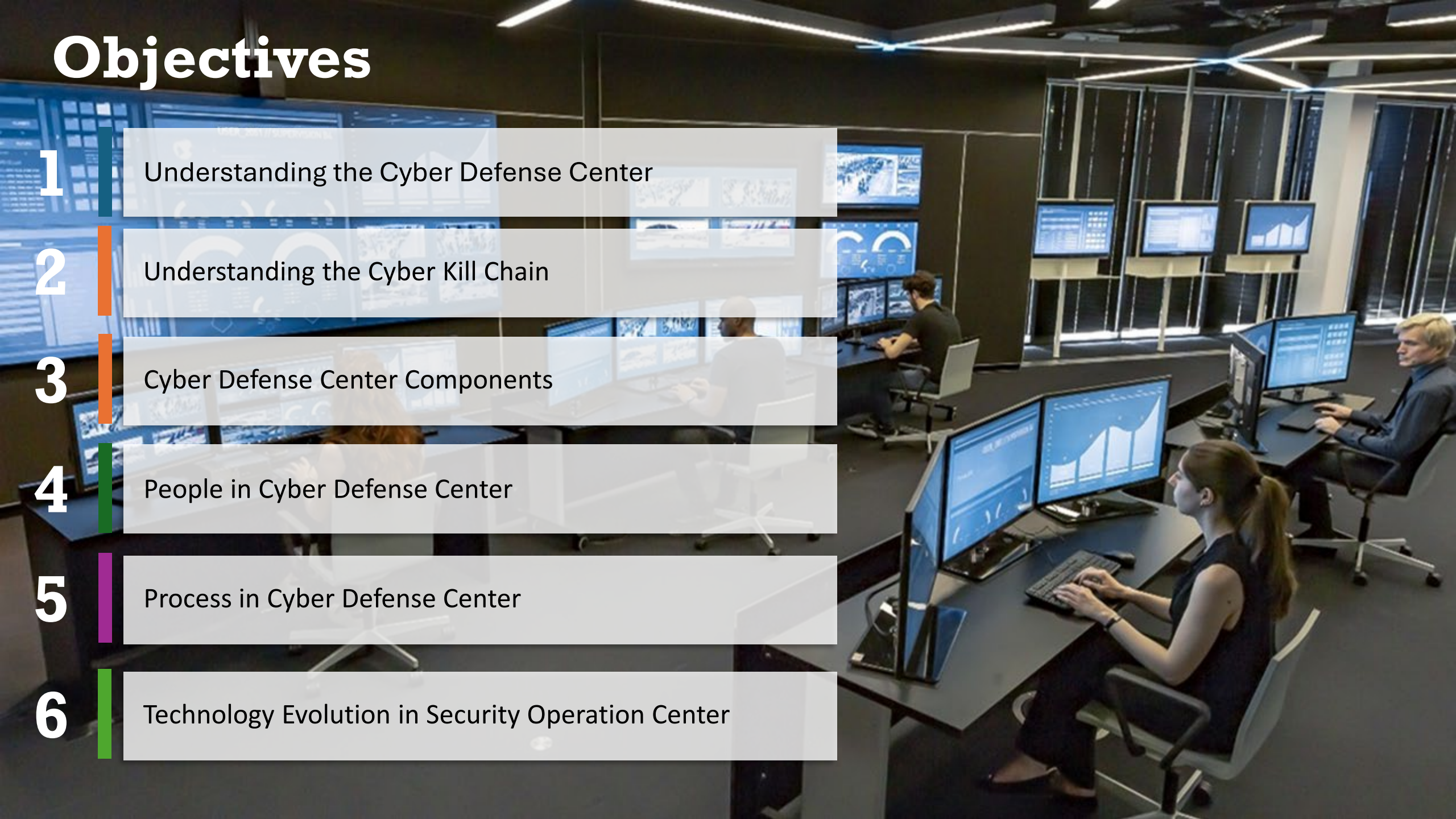
Cyber Defense Center

Objectives



1. Understanding the Cyber Defense Center
2. Understanding the Cyber Kill Chain
3. Cyber Defense Center Components
4. People in Cyber Defense Center
5. Process in Cyber Defense Center
6. Technology Evolution in Security Operation Center

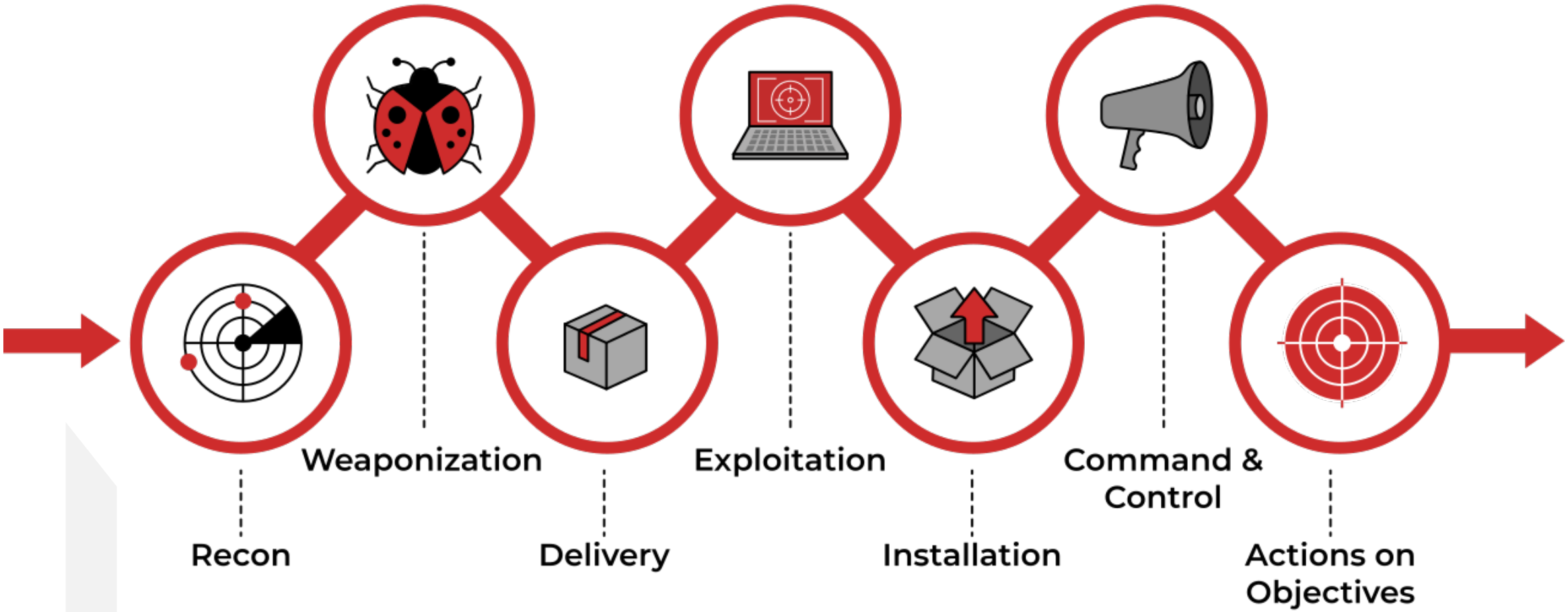
Understanding of Cyber Defense Center

Cyber Defense Center - is a security operations unit that works to minimize organizational risk and reduce the impact of security breaches through effective detection and response processes and procedures

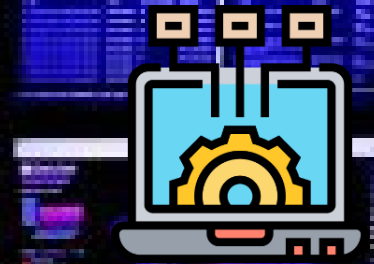
What are **Cyber Defense Center** components ?

What are **Security Operation Center** evolutions ?

Understanding of Cyber Kill Chain



Cyber Defense Center Components



People

- ❑ SOC Manager
- ❑ Threat Intelligent
- ❑ SOC – Tier 1
- ❑ SOC – Tier 2
- ❑ Threat Hunter

Process

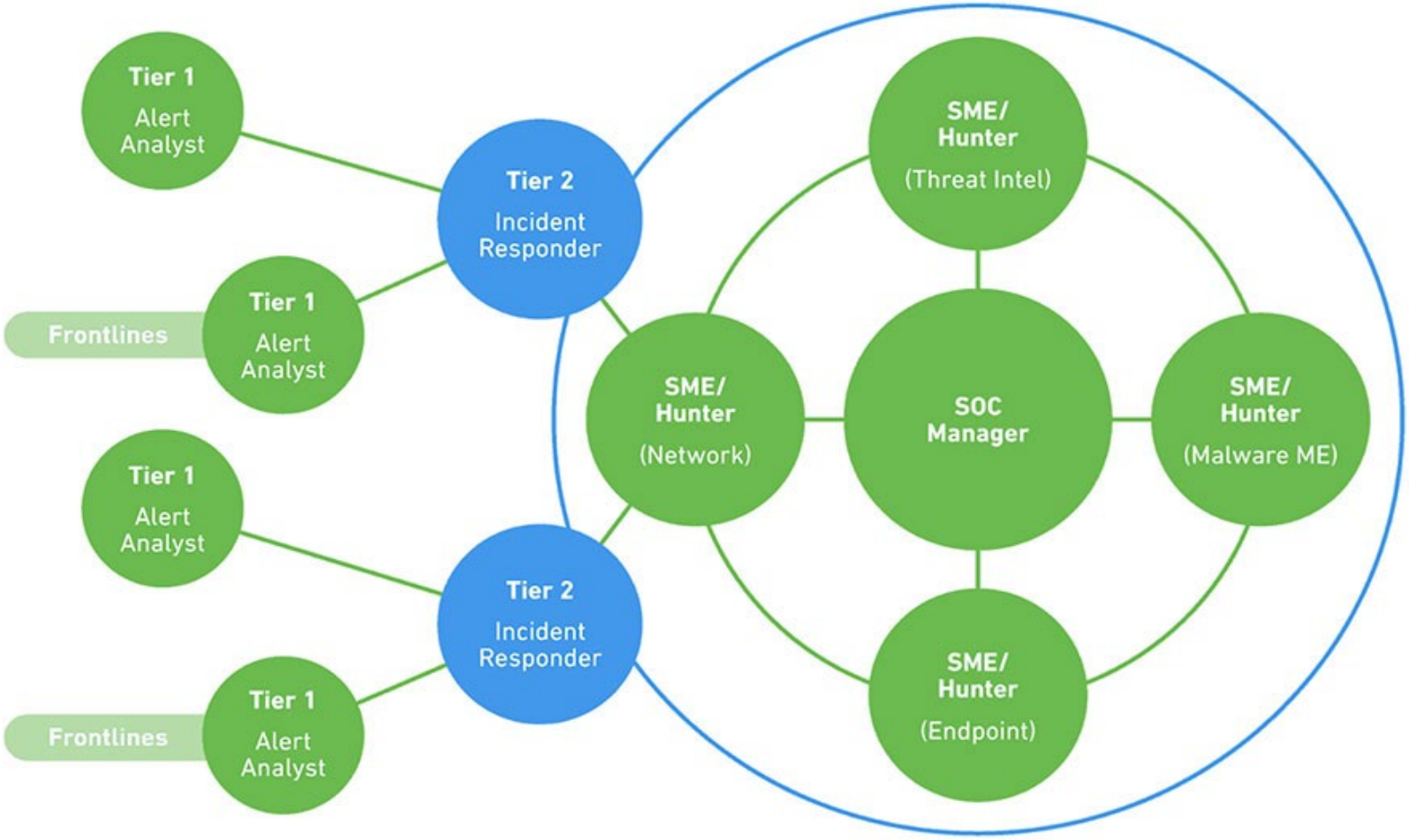
- ❑ IS Incident Management Policy / Procedure.
- ❑ Specific incident management playbooks
- ❑ CSIRT / ISO 27035 etc

Technology

- ❑ SIEM
- ❑ SOAR
- ❑ EDR
- ❑ NDR
- ❑ TIP
- ❑ Sandboxing

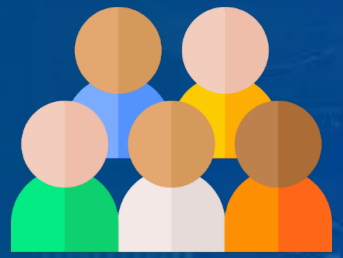
UIH digital infrastructure & solutions

People in Cyber Defense Center



- **Tier 1 SOC**: Perform basic analyst on security events.
- **Tier 2 SOC**: Perform advance/deep analyst for security incidents respond.
- **SME Hunters**: Perform widely threat hunting .
- **SOC Manager**: Overall lead level1 ,2 and Threat Intel and set up proper strategy for protecting org from attack surface.

Process in Cyber Defense Center



Roles and Responsibilities

- ❑ Appoint someone act as **SIM** (Security Incident Manager).
- ❑ Form up resolver groups
- ❑ Service Level Agreement

Policy / Procedure

- ❑ Threat & Vulnerability Management Policy/Procedure
- ❑ Incident Management Policy / Procedure
- ❑ Problem Management

Incidents Playbooks

- ❑ Ransomware
- ❑ Phishing
- ❑ Daniel of Service
- ❑ Lateral Movement
- ❑ Critical Playbooks
- ❑ ETC

Technology - Security Operation Center Evolutions

NSOC / SOC 1.0

- IDS
- Anti Virus
- Firewall

SOC 2.0

- IPS
- Anti Spam
- Statful Inspection
- Vulnerability Management

SOC 3.0

- SIEM
- DLP
- SecOps
- Avance Persistant Threat

Next-Gen SOC

- BYOD
- UEBA
- Sandboxing
- TIP
- CASB

Defense Center

- Next-Gen SIEM
- Sandboxing
- Big Data
- SOAR
- NDR / EDR
- TIP / HoneyPot


Q&A