***Developing a Customized Security Operations Center (SOC) Framework***

### **1. Security Needs Assessment for Dedeman**

#### **Dedeman's Security Needs:**

* **Cybersecurity:** Protecting customer data and IT systems from cyber threats such as hacking, phishing, malware attacks, DDoS, etc.
* **Physical Security:** Ensuring the physical protection of locations and equipment, including preventing theft and vandalism.
* **Compliance:** Adhering to security regulations and standards applicable to the retail and construction industries.
* **Business Continuity:** Ensuring the continuity of operations in the event of security incidents, such as cyberattacks and natural disasters.

#### **Key Objectives of the Security Operations Center (SOC):**

* **Incident Detection and Response:** Quickly identifying security incidents and responding appropriately to minimize their impact.
* **Continuous Monitoring:** Constantly supervising networks and systems to detect suspicious activity.
* **Vulnerability Management:** Identifying and resolving vulnerabilities in the IT infrastructure.
* **Reporting and Compliance:** Ensuring adherence to regulations and reporting security incidents to relevant authorities.

### **2. General Action Plan for the Security Operations Center (SOC)**

#### **SOC Functions and Responsibilities:**

* **Monitoring and Analysis:** Continuous surveillance of networks and systems to detect suspicious activity.
* **Incident Response:** Investigating and managing security incidents to minimize their impact.
* **Vulnerability Management:** Identifying and remediating weaknesses in the IT infrastructure.
* **Reporting and Compliance:** Ensuring regulatory compliance and reporting security incidents.

### **Description of SOC Roles:**

1. **Security Analyst**
   * **Functions:** Monitors networks and systems to detect suspicious activity.
   * **Responsibilities:** Analyzes security alerts and investigates incidents.
2. **Security Engineer**
   * **Functions:** Develops and implements security solutions.
   * **Responsibilities:** Manages and remediates vulnerabilities in the IT infrastructure.
3. **SOC Manager**
   * **Functions:** Coordinates SOC team activities.
   * **Responsibilities:** Ensures compliance with regulations and manages incident reporting.
4. **Incident Response Specialist**
   * **Functions:** Investigates and manages security incidents.
   * **Responsibilities:**Leads incident response efforts and minimizes their impact.