**Cybersecurity roles/task and contribution breakdown**

### **1. Requirements & Data Classification Lead**

1. Gather **functional requirements** from the features of the website/app.
2. Document **security requirements** based on app features.
3. Classify data by **sensitivity levels** (High/Medium/Low).
4. Work with Threat Modeling Lead to identify **what data needs the most protection**.

### **2. Threat Modeling Lead**

1. Identify **possible threats** to each ClockKo feature (data breaches, API abuse, phishing, etc.).
2. Map threats to **risk levels** (High, Medium, Low).
3. Recommend **security controls** for each identified threat.
4. Use tools like **OWASP Threat Dragon** or **Microsoft Threat Modeling Tool**.

### **3. Security Architecture Designer**

1. Create the **security architecture diagram** (network + app layers).
2. Define **data flow** between client app, API gateway, and database.
3. Decide on **network segmentation, encryption, and authentication methods**.
4. Ensure architecture aligns with **SSDLC security requirements**.

### **4. Cybersecurity Frameworks & NDPR Compliance Lead 🆕**

1. Map ClockKo’s security requirements to relevant **cybersecurity frameworks**:  
   1. **NIST Cybersecurity Framework (Identify, Protect, Detect, Respond, Recover)**.
   2. **ISO/IEC 27001** (Information Security Management).
   3. **OWASP ASVS** (Application Security Verification Standard).
2. Ensure compliance with **Nigeria Data Protection Regulation (NDPR)** by:  
   1. Implementing **data minimization** and **purpose limitation** principles.
   2. Documenting **consent management** for user data.
   3. Setting **data retention and deletion policies**.
   4. Ensuring **cross-border data transfer controls** if using foreign servers.
   5. Provide a **compliance checklist** for the project.

### **5. Implementation & Secure Coding Lead**

1. Integrate **security controls** during coding.
2. Recommend **secure coding guidelines** (OWASP Top 10 awareness).
3. Ensure encryption (**TLS 1.3 in transit, AES-256 at rest**) is implemented.
4. Review **dependencies** for known vulnerabilities.

### **6. Testing & Verification Lead**

1. Conduct **Static Application Security Testing (SAST)** on code.
2. Run **Dynamic Application Security Testing (DAST)** on staging environment.
3. Perform **basic penetration testing** on APIs and app.
4. Document vulnerabilities found & work with devs to fix them.

### **7. Monitoring & Incident Response Lead**

1. Set up **log monitoring** (AWS CloudWatch, ELK Stack, or SIEM tools).
2. Define **alerts** for suspicious activity (e.g., multiple failed logins, high API traffic).
3. Write a simple **Incident Response Plan** for ClockKo.
4. Propose **backup & recovery procedures**.

**How It Works Together**:

**#1 & #2** → Handle the **front-end of SSDLC** (requirements & threats).

**#3 & #4** → Turn that into a **secure design aligned with NDPR & frameworks**.

**#5 & #6** → Build & verify the protections.

**#7** → Maintain ongoing security and respond to incidents.