

SOC TYPES

1. Private SOC (In-house SOC)

- The company builds and runs its own SOC.
- All security experts, tools, and systems belong to the company itself.
- Example: A bank hires its own security team and sets up a SOC inside its office.

👉 **Good for:** Big companies with money and sensitive data.

2. Completely Outsourced SOC

- The company gives **all security monitoring work** to an outside vendor.
- The vendor runs the SOC for them.
- Example: A small business hires a cybersecurity company to fully manage its security.

👉 **Good for:** Small/medium companies without security staff.

3. Hybrid SOC

- A **mix of in-house + outsourced**.
- The company keeps some security team in-house, but also takes help from an external SOC provider.
- Example: Company monitors office network themselves but outsources cloud monitoring to a vendor.

👉 **Good for:** Medium to large companies needing flexibility.

4. Command SOC

- Works like a **central hub (head office)** that controls and coordinates multiple SOC's.
- Example: A global company has SOC's in India, USA, and Europe → a command SOC oversees them all.

👉 **Good for:** Large multinational companies.

5. MSP Outsourced SOC (Managed Service Provider SOC)

- Security is handled by an **MSP (Managed Service Provider)**.
- The MSP provides tools, people, and monitoring as a **monthly service**.
- Example: A company pays an MSP for security just like it pays for internet service.

👉 **Good for:** Companies wanting **cost-effective 24/7 monitoring**.

6. Virtual SOC (vSOC)

- No physical SOC room. Everything is **cloud-based**.
- Security analysts work remotely and monitor using online tools.
- Example: A cybersecurity team logs in from anywhere and protects a company's systems via cloud dashboards.

👉 **Good for:** Startups or modern companies with remote-first setups.

✅ **Summary in one line each:**

Private SOC → Company's own SOC.

Outsourced SOC → Fully given to vendor.

Hybrid SOC → Mix of in-house + vendor.

Command SOC → Central SOC that controls others.

MSP SOC → Managed security as a monthly service.

Virtual SOC → Cloud-based, remote SOC.

What are the Different Types of SOC Models

