SECURITY MANAGEMENT, SECURITY OPERATIONS & SOC

Focus: understanding how security is organized inside a company

---

 Big Picture Idea

Think of the company as a **castle**.

- **Security Management** = leaders who create rules and strategy
- **Security Operations** = guards who enforce the rules daily
- **SOC (Security Operations Center)** = command room watching everything 24/7

All three work together.

---

1 Security Management — "The Planners"

Security Management focuses on **planning and decision-making**.

They:

- create security policies
- decide budgets and tools
- manage risk
- ensure compliance & audits
- set responsibilities

Examples:

- password rules
- backup policies
- data protection policies
- incident response plan

📌 Key idea:

Security Management = **long-term strategy + rules.**

---

2 Security Operations — “The Doers”

Security Operations performs **daily security work**.

They:

- monitor systems & logs
- apply patches
- manage firewalls
- fix vulnerabilities
- support incident response

If management says:

“All doors must lock at 9 PM.”

Operations makes sure:

“The doors are actually locked at 9 PM.”

📌 Key idea:

Security Operations = **real-time action.**

---

3 SOC — Security Operations Center

SOC is the **central monitoring team**.

They:

- watch alerts
- analyze suspicious activity
- detect attacks
- escalate incidents

- document everything

Tools used:

- SIEM
- EDR
- SOAR
- ticketing systems

SOC is like a **command room with screens**, tracking the entire organization.

📌 Key idea:

SOC = **detect, investigate, and respond.**

🔗 How They Work Together

Security Management → sets rules & strategy

Security Operations → applies the rules

SOC → monitors & responds to threats

None of them work alone — they depend on each other.

🧠 Why SOC is Needed

- hackers attack at any time
- too much data for humans to manually check
- early detection reduces damage
- older systems remain vulnerable

SOC gives visibility and fast reaction.

🎯 Key Takeaways

- Security is **organized**, not random

- Strategy → Operations → Monitoring
- SOC analysts work inside this structure
- Strong processes matter more than tools