SOC Architectures and Frameworks

Akash Madhukar
Cyber Security Intern
CyberSapiens United LLP

Table of Contents

1. Introduction

Cyber threats are growing more advanced every day. To protect their systems, organizations need Security Operations Centers (SOCs) to monitor, detect, and respond to threats. Choosing the right SOC setup and framework is key to staying secure and meeting compliance requirements. This guide compares different SOC models and frameworks to help you decide what's best for your organization.

2. Types of SOC Architectures

Centralized SOC

What It Is:

- A single location where all security operations are managed.

Pros:

- Easy to coordinate and communicate.
- Standardized tools and processes.
- Quick response times.

Cons:

- If it fails, everything goes down.
- Hard to scale.
- Expensive to set up.

Best For:

- Large companies operating from one location.

Decentralized SOC

What It Is:

- Several SOCs spread across different locations, each handling local security.

Pros:

- No single point of failure.
- Local experts can respond quickly.
- Scales well for large organizations.

Cons:

- Processes may differ between locations.
- Harder to manage.
- Requires more staff and resources.

Best For:

- Global organizations with multiple offices.

Virtual SOC (vSOC)

What It Is:

- A cloud-based SOC run by a third-party security provider.

Pros:

- Affordable and flexible.
- 24/7 expert monitoring.
- Quick to set up.

Cons:

- Less control over operations.
- Data privacy concerns.
- Dependence on external providers.

Best For:

- Small to medium businesses (SMBs) with limited resources.

Hybrid SOC

What It Is:

- A mix of centralized, decentralized, and virtual SOCs.

Pros:

- Flexible and adaptable.
- Combines the best features of all models.
- Built-in redundancy.

Cons:

- Complicated to manage.
- Requires significant resources.

Best For:

- Companies with complex and evolving security needs.

3. Popular SOC Frameworks

NIST Cybersecurity Framework (CSF)

What It Does:

- Provides guidelines to identify, protect, detect, respond, and recover from security threats.

Pros:

- Flexible and customizable.
- Focuses on risk management.

Cons:

- Broad guidance may need further detail.

Best For:

- Organizations that need a risk-based approach.

MITRE ATT&CK Framework

What It Does:

- Details the methods attackers use to breach systems.

Pros:

- Helps improve threat detection and response.
- Identifies security gaps.

Cons:

- Requires skilled staff to use effectively.

Best For:

- Companies focused on threat hunting.

ISO 27001/27002

What It Does:

- Offers standards for building a security management system.

Pros:

- Recognized worldwide.
- Covers security governance thoroughly.

Cons:

- Focuses on compliance, which can be rigid.

Best For:

- Organizations needing formal security certification.

CIS Controls

What It Does:

- Lists key security controls to protect against common threats.

Pros:

- Simple and easy to apply.
- Prioritized by effectiveness.

Cons:

- Doesn't cover advanced attacks.

Best For:

- SMBs or teams with limited security resources.

4. Comparison of SOC Models

Strengths and Weaknesses

Feature	Centralized SOC	Decentralized SOC	Virtual SOC	Hybrid SOC
Cost	High	High	Low to Moderate	High
Scalability	Limited	High	High	High
Control	High	Medium	Low	Medium
Flexibility	Low	Medium	High	High
Response Time	Fast	Medium	Fast	Fast
Expertise Needed	High	High	Low to Moderate	High

Best Use Cases

- Centralized SOC: Best for single-location enterprises or banks.
- Decentralized SOC: Best for multinational corporations.
- Virtual SOC: Best for SMBs or companies needing affordable 24/7 monitoring.
- Hybrid SOC: Best for organizations needing a mix of control and flexibility.

5. Key Considerations for Building a SOC

1. Budget: What can you afford?
2. Company Size: How big is your organization?
3. Risk Level: How much risk do you face?
4. Compliance Needs: What regulations apply to you?
5. Tech Infrastructure: Do you have the right tools in place?
6. Expertise: Do you have the right people, or do you need outside help?

6. Conclusion and Recommendations

Choosing the right SOC model and framework helps protect your organization from cyber threats. Each option has its pros and cons, so match your choice to your needs and resources.

Recommendations

1. For SMBs: A Virtual SOC with CIS Controls is cost-effective and quick to set up.
2. For Large Enterprises: A Centralized or Hybrid SOC with NIST CSF and MITRE ATT&CK frameworks is a strong choice.
3. For Multinationals: A Decentralized SOC with ISO 27001/27002 can manage security across regions.

References:

https://www.slideshare.net/slideshow/soc-architecture-and-design/48351394

https://link.springer.com/chapter/10.1007/978-3-031-36242-2_3

https://www.splunk.com/en_us/blog/learn/soc-security-operation-center.html

https://www.geeksforgeeks.org/architecture-of-soc/