When to Set Up a Security Operations Center

What's a SOC?

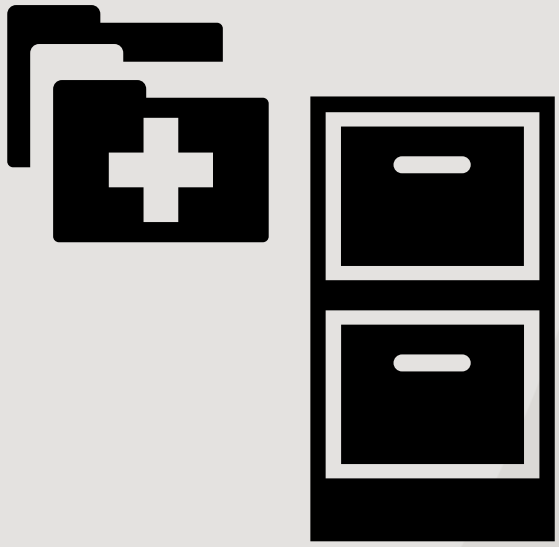
A SOC, or a Security Operations Center, is a central location where security personnel monitor, assess, and defend a company’s digital assets, such as websites, apps, databases, servers, and endpoints.

Why are SOC's created?

- To centralize visibility
- To optimize operations
- To respond to incidents faster and with better accuracy

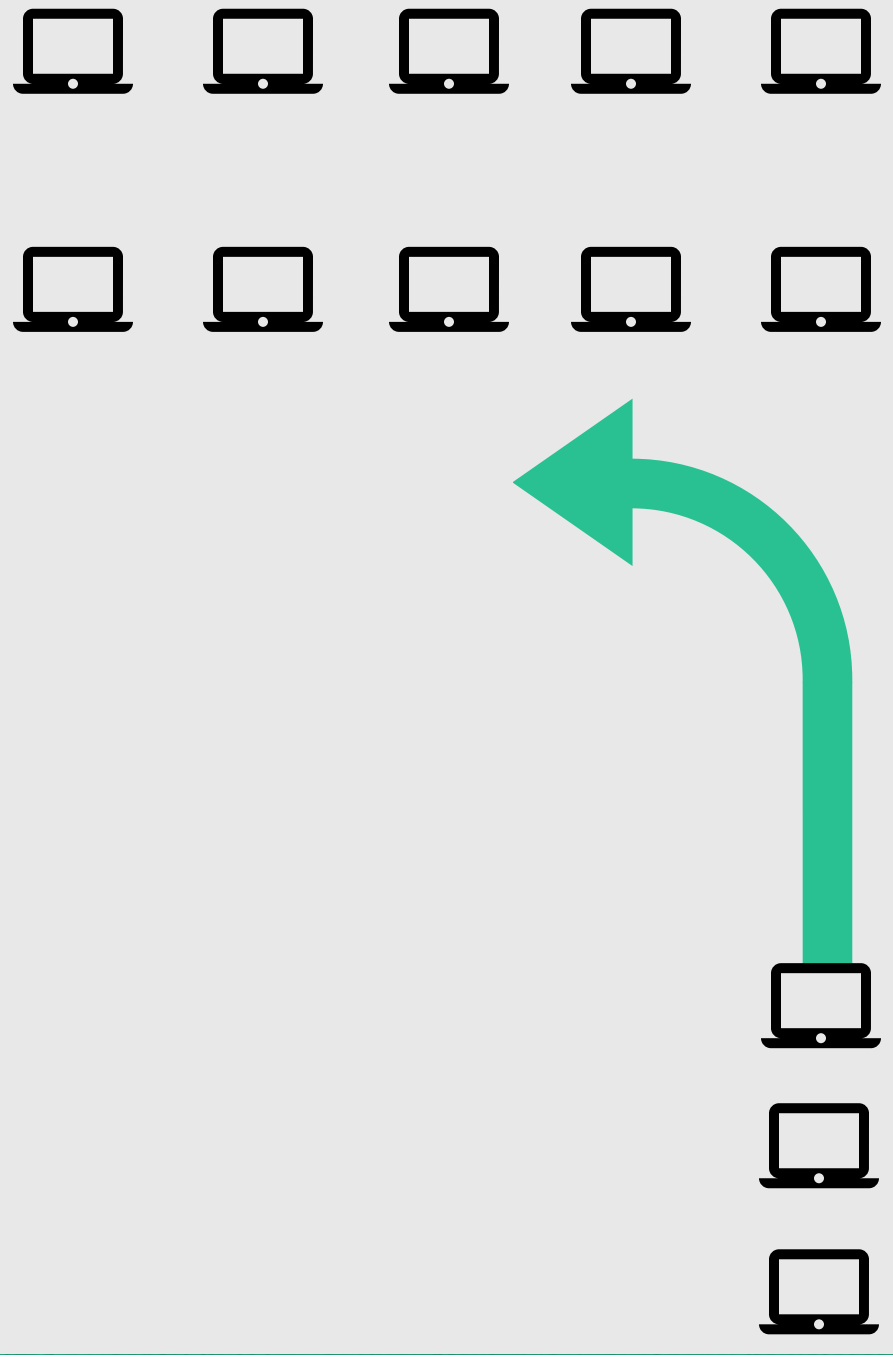
When should you set up a SOC?

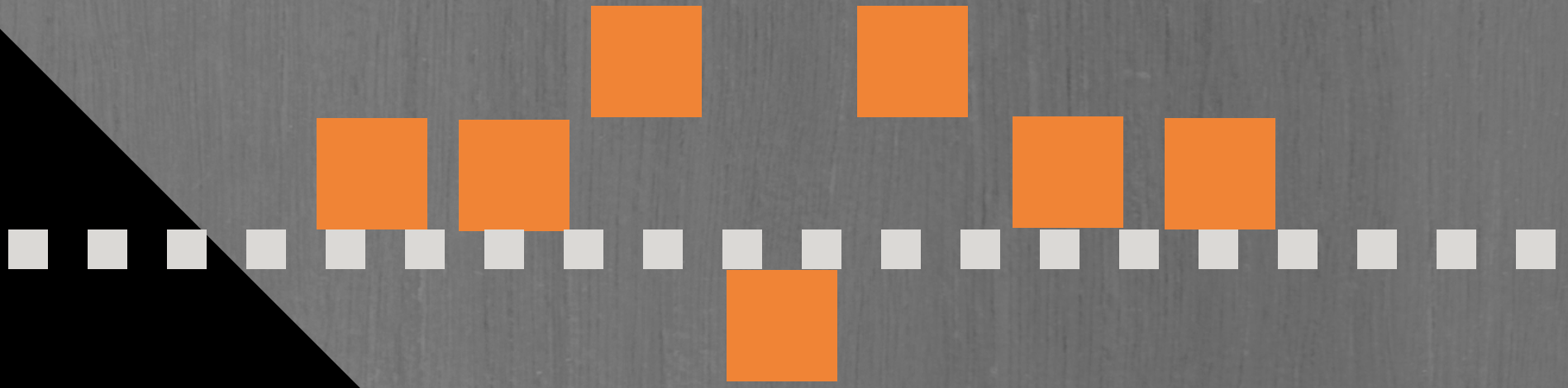
1. When your firm is handling increasing amounts of sensitive data



2. When your threat landscape requires dedicated security resources

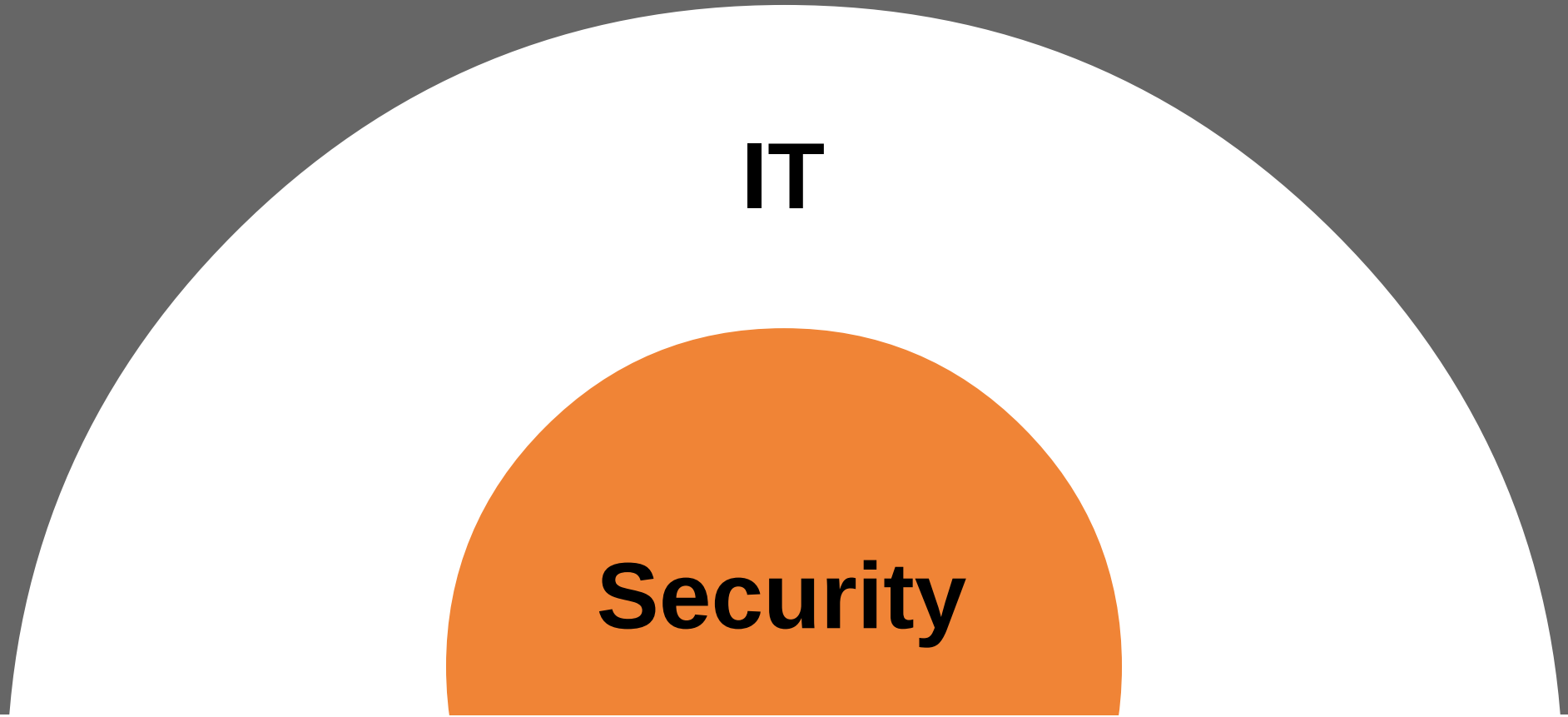
3. When your organization is growing, with more machines and users to protect



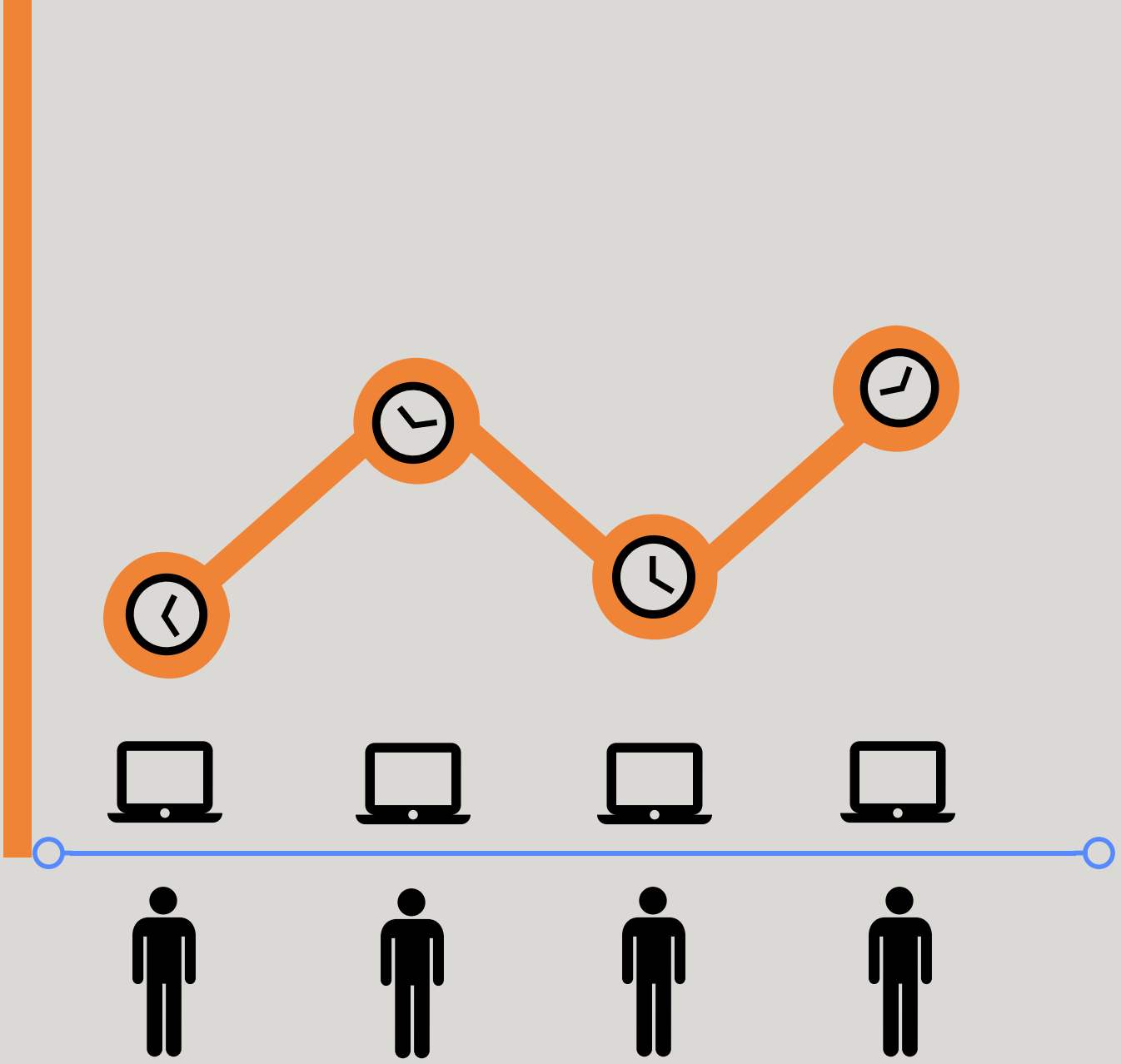


4. When your monitoring and workflows are ineffective

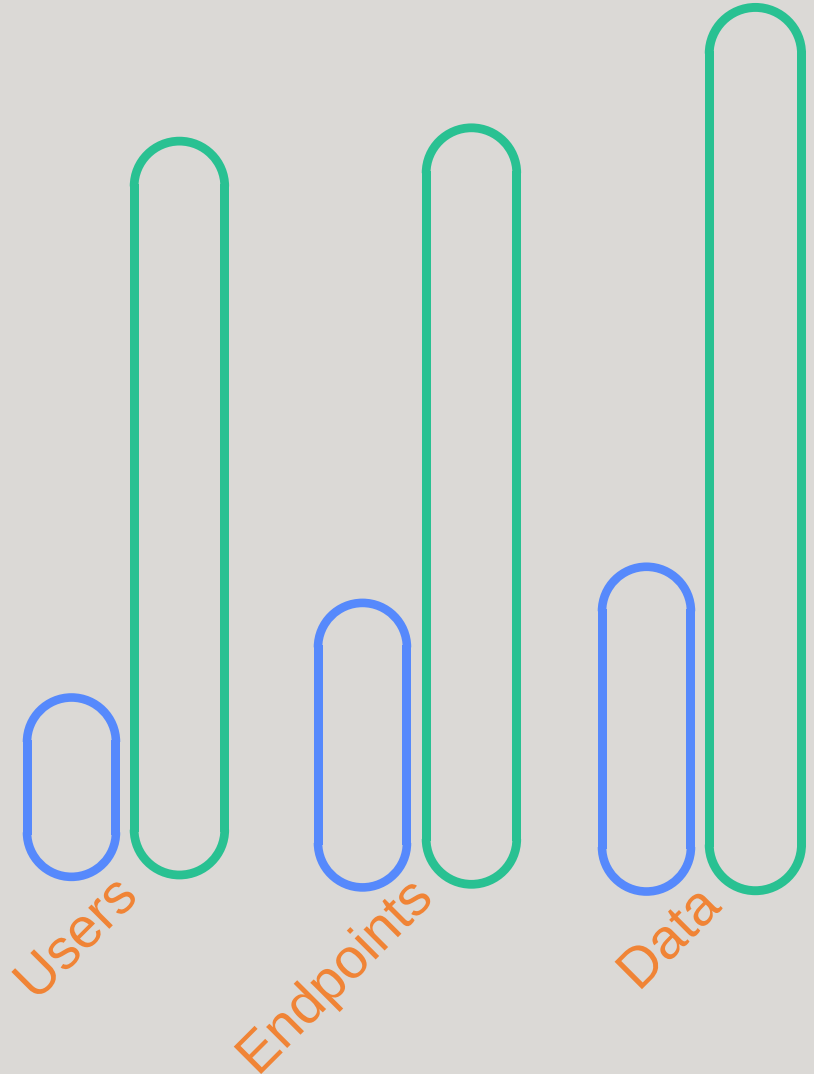
5. When security is part of another function, and difficult to measure ROI



6. When you want to improve monitoring and response capabilities



7. When you've outgrown your MSSP



HOW TO STRUCTURE A SECURITY OPERATIONS CENTER

The Three Key Functions of a SOC:

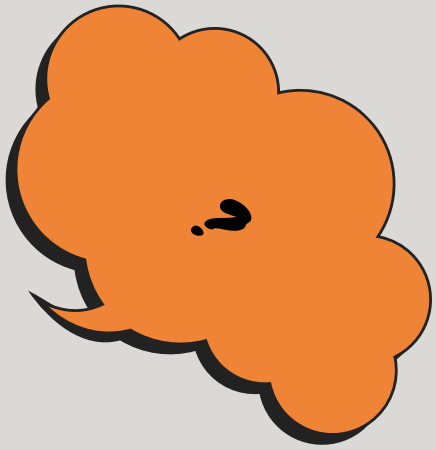
People

Process

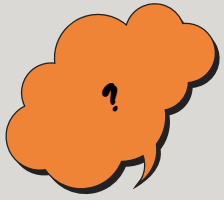
Technology

PEOPLE

People



When building a powerhouse SOC, it's important to inventory your staff and ask some important questions. Questions like...



People

Is anyone currently in a security-only role

Is anyone from IT ready to make the move as a security-only player?

Is anyone currently in a security-only role

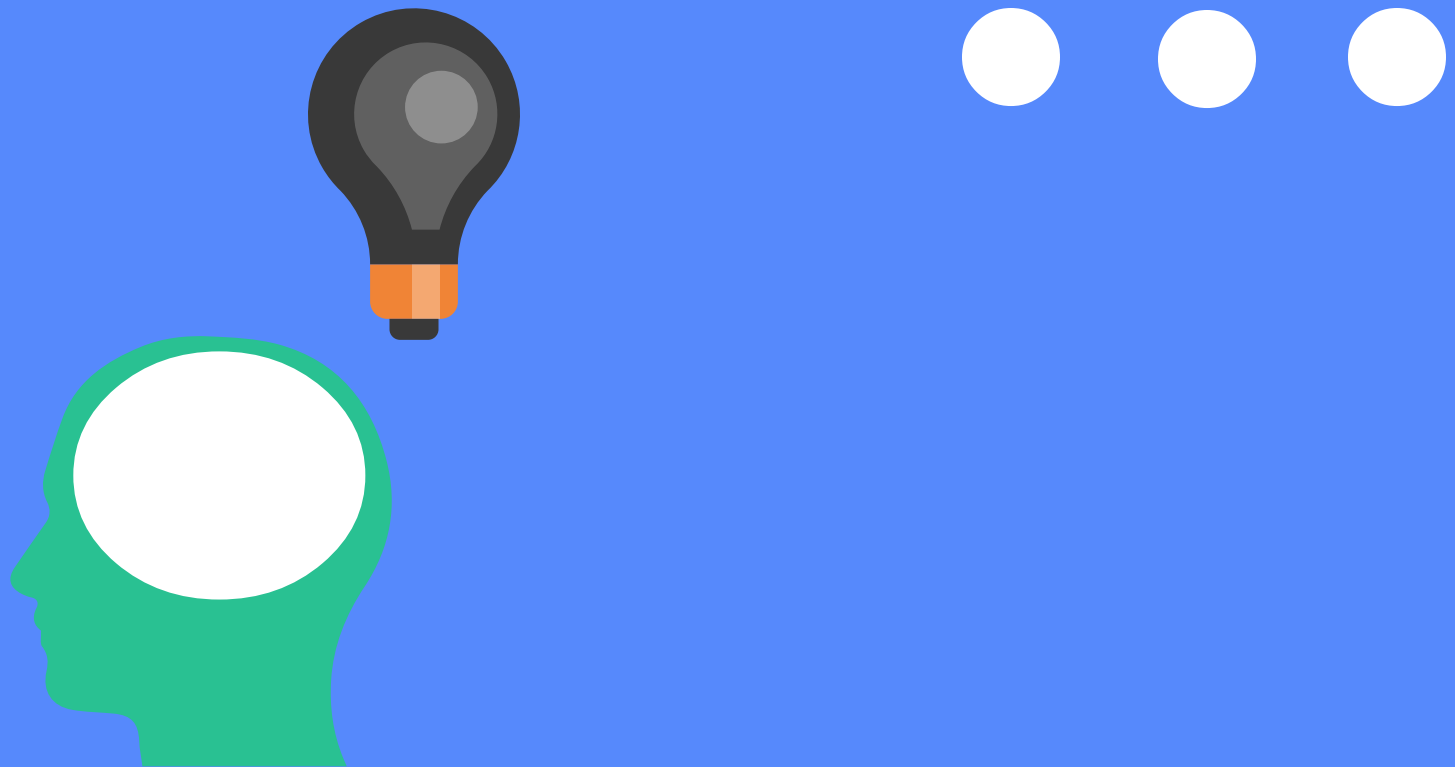
Is anyone currently in a security-only role

People

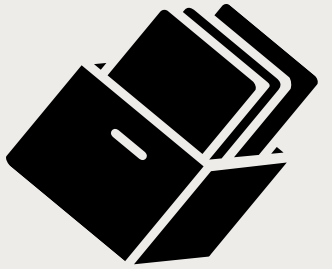
Many organizations choose to build their SOCs with in-house resources, while others opt for hybrid mix of in-house and external resources.

Neither approach is wrong. Your best option depends on internal resources, your budget, and the urgency of the threats you face.

Once you have the answer to these questions, it's time to figure out the makeup of your team. Some more questions to ask during this phase



People

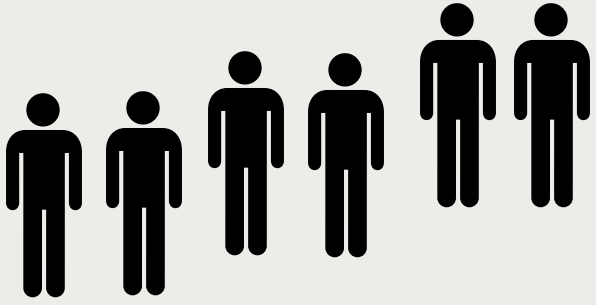


What is the budget for hiring?

How many people will you hire?

What roles will you hire?

How fast can we build the SOC team?



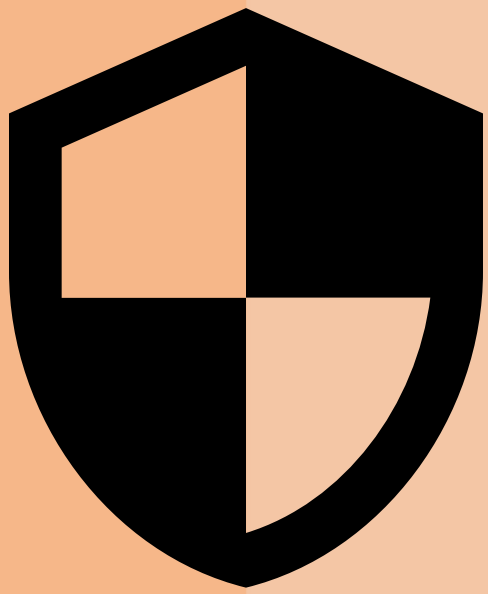
When you have the answers to these questions, it's time to move on to process.

PROCESS

Process

In order to *define ownership* and *streamline procedures*, make a full *evaluation* by asking these questions:

Process



Who monitors for threats?

Who promotes security events to incidents?

Who is accountable for fixing them?

Are the current processes documented?

Process

Then determine where you need process.

Here are a few ideas to get started:

- Monitoring
- Alerting
- Escalation
- Investigation
- Incident logging
- Compliance monitoring
- Reporting

Also consider processes for common attacks, such as:

Brute force attack

Social engineering/cyber fraud

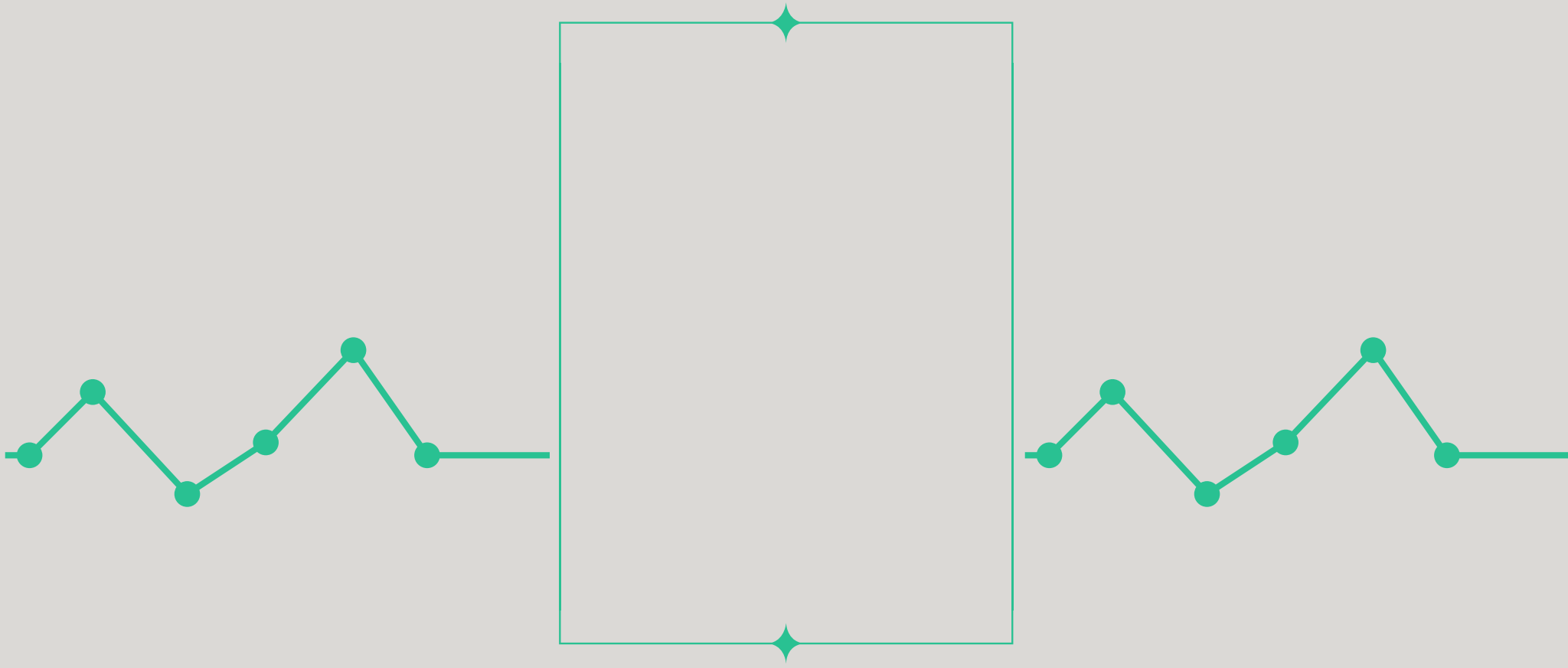
DDOS

Phishing

Malware, spyware, ransomeware

TECHNOLOGY

Technology



Evaluate your current security strategy, determine if technologies are tailored to your needs, and think about where you need coverage.

When choosing a tool, think about:

The environment you operate in (cloud, on-premise, or hybrid)

The type of threats you face (malware, phishing, etc.)

The compliance mandates you're required to uphold (HIPPA, SOC2, etc.)

And then think about the type of coverage you may need. Some examples include:

Security Monitoring

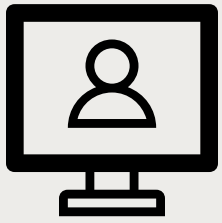
Incident Detection and Response

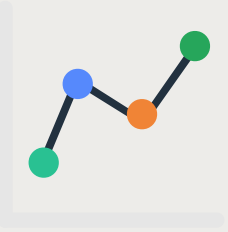
Log Collection and Aggregation

Application Security

Malware Analysis

Threat Intel



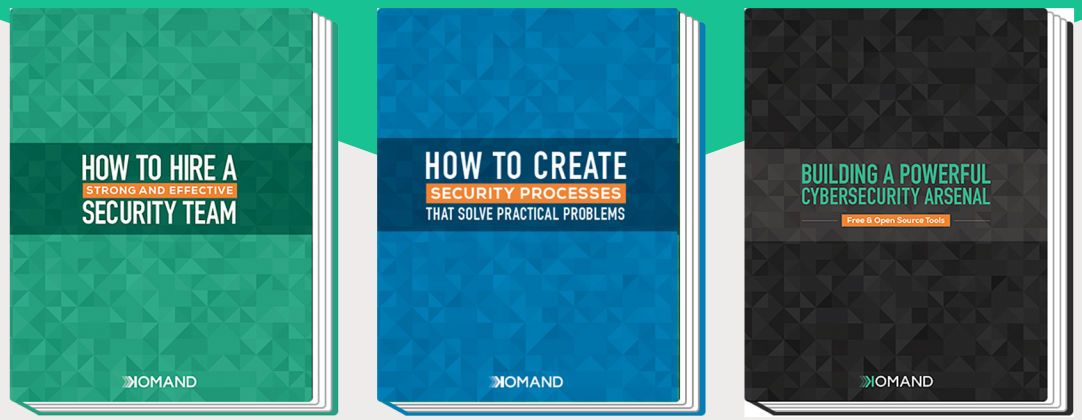


Lastly, it's important to understand how your tools are interconnected. This power of connection between your tools provides more value across your entire security technology suite.

Ready to start building a SOC?

Use our Cybersecurity Starter Bundle

Three free eBooks on People, Process, And Technology to help you build a security operations center now.



Get the Cybersecurity Starter Bundle

HOMAND