NOT ALL SOCS ARE CREATED EQUAL

7 KEY CONSIDERATIONS

Your selection of SOC provider is no small undertaking. Cyber threats are real and potentially brand destroying.

infotrust

SECURING YOUR FUTURE.

1 SOC protection is only as good as the people who staff it.

- Its vital to determine what type of team has been assembled to manage a SOC's operations.
- It should be confirmed firstly, that the team exists.
- You might also ask how the engineering team interacts with the analysts and other members of the SOC team.
- If so, the workforce should be arranged in a tiered structure staffed by analysts, engineers, and specialists.

2 Your SOC provider should have a client list that includes prominent players within your sector.

- Ask your potential SOC provider who they currently protect.
- A competent SOC operation should have well known clients, including players within your industry.
- The cyber security industry runs on trust, which can only be built over time. Trusted providers should be comfortable demonstrating examples of their work across an impressive list of clients.
- Enterprises in industries such as healthcare, financial services and critical infrastructure should be covered.

3 SOC protection can only be provided by a genuine 24/7 operation.

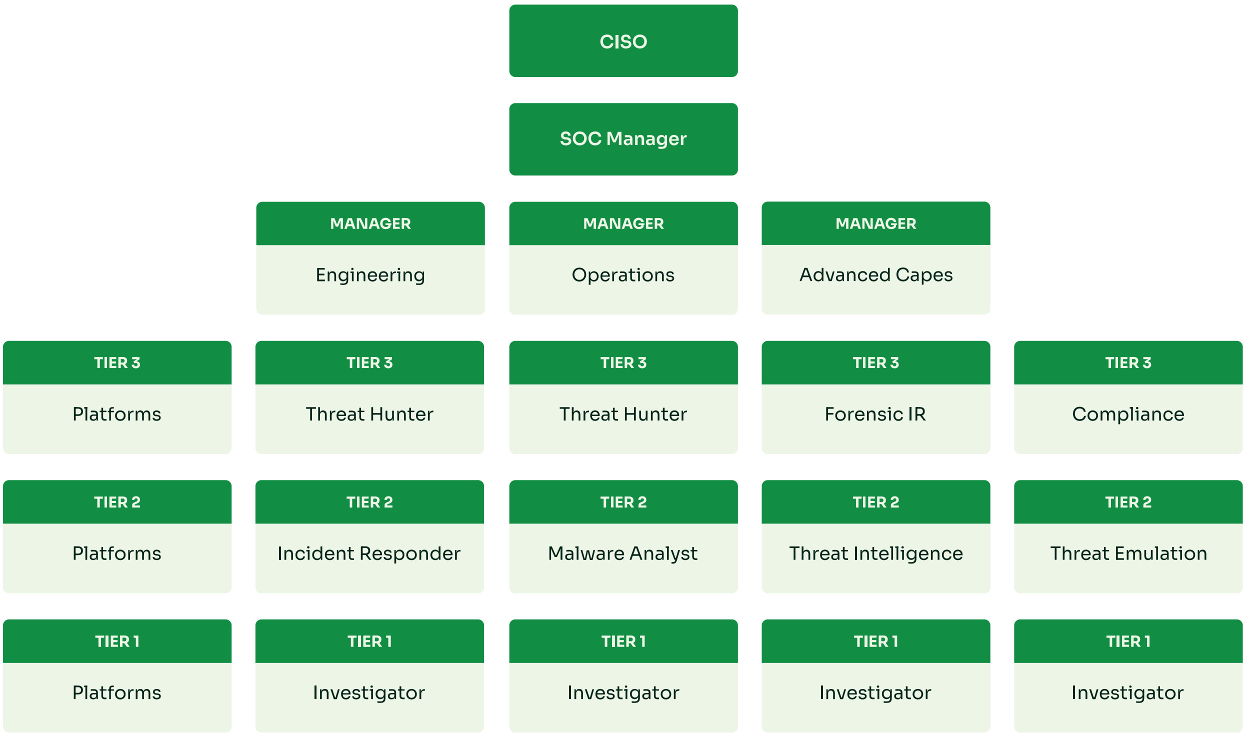
- Unless a SOC is staffed by competent people 24/7, its value is very limited and not worth your investment.
- There must be well-trained eyeballs staring at screens around the clock, as opposed to someone sleeping waiting on a pager.
- Understaffed SOC teams do not have the resources to act in real time and the resultant delays can be the difference between success and failure.
- An adequate SOC should have no less than 10 dedicated staff to cover all outputs.
- There must be well-trained eyeballs staring at screens around the clock, as opposed to someone sleeping waiting on a pager.
- If the SOC provider has more than 25 customers, their staffing should reflect this. i.e ask the provider how many analysts are providing coverage on each shift

4 Your SOC provider should have leaders at all levels with years of SOC experience.

- Your SOC provider should have highly qualified senior management within its ranks.
- This can be demonstrated by years of experience in the cyber security business.
- Without evidence of experience, a SOC provider should be approached with caution.

Teaming

Your SOC relies on specialist skills and depth within teams. Despite what you'll be told, one person cannot do it all.



CISO

SOC Manager

MANAGER	MANAGER	MANAGER
Engineering	Operations	Advanced Capes

TIER 3 Platforms	TIER 3 Threat Hunter	TIER 3 Threat Hunter	TIER 3 Forensic IR	TIER 3 Compliance
TIER 2 Platforms	TIER 2 Incident Responder	TIER 2 Malware Analyst	TIER 2 Threat Intelligence	TIER 2 Threat Emulation
TIER 1 Platforms	TIER 1 Investigator	TIER 1 Investigator	TIER 1 Investigator	TIER 1 Investigator

5 Beware the free lunch.

- If your potential SOC provider is offering an unreasonably low quote, alarm bells should be ringing.
- Running a SOC is a complicated 24/7 operation and there is no room for cutting corners or lapses in protection.
- Constant vigilance by trained professionals should therefore be reflected in the price.
- If you were skydiving, would you buy the cheapest parachute? We hope not.

6 Is your SOC provider capable of providing more than one service?

- It should be expected that a qualified SOC provider can offer a range of cyber security services.
- Explore the list of services to ensure that a team of engineers, analysts, and experts has been assembled across a range of security disciplines.
- A qualified SOC provider will be able to deliver a comprehensive package of services.

7 SOC Service Enhancements

Additional services to compliment your existing SOC operations

Cyber Threat Intelligence

Intelligence Services

- Threat Intelligence Platform integration with SIEM
- Threat reporting powered by curators
- Dark/Deep Web detection and response

Vulnerability Management

VMaaS

- Risk-based patch management
- Asset ID, Scan, Report
- Prioritisation and Testing

Security Operations

Cloud Security

- Cloud access security broker tuning and management
- Secure Services Edge (SSE)

Proactive Security

- Threat Hunting
- Testing & Red Teaming
- Phishing awareness

Email Gateway

- Suspicious email investigations
- Email filter tuning

Data Security

- Data and file security monitoring and tuning
- Insider threat mitigation

Endpoint

- Endpoint Detection and Response (EDR) tuning, policy enforcements and maintenance