

SOC-as-a-Service or DIY SOC?

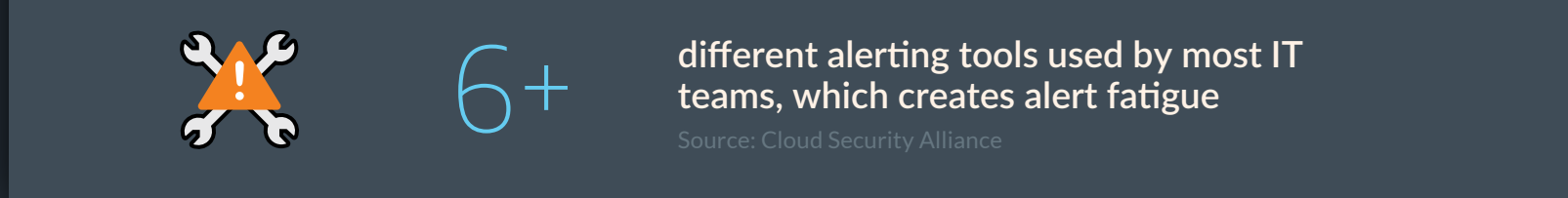
What should companies pay for the comprehensive security of a security operations center (SOC)?

Leading consultancy Frost & Sullivan conducts a total-cost-of-ownership (TCO) analysis

Security Operations Centers Have Become a Mainstay of Comprehensive Cybersecurity Defenses

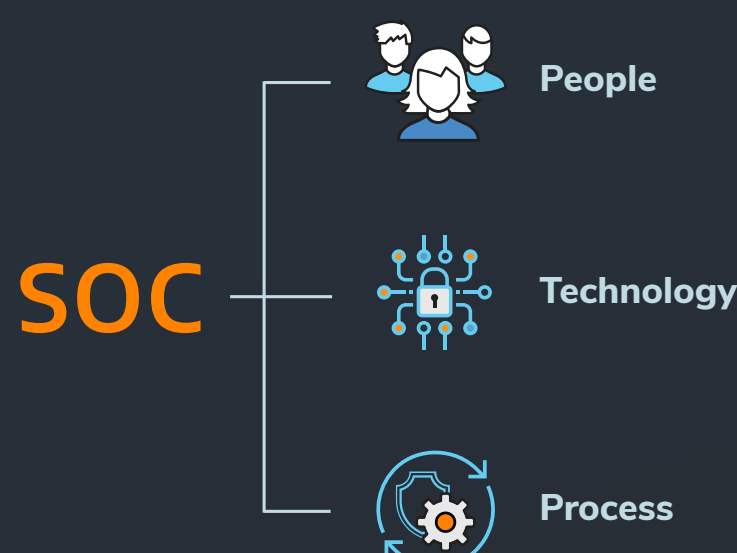
Companies of every size are starting to realize how essential a security operations center (SOC) is to establish the type of cybersecurity posture they need. A SOC provides all the people, processes, and technology that companies require to detect, analyze, and respond to threats.

Here are today's leading drivers of SOC adoption:



The SOC: A Triad of Security Operations

A SOC is built upon three components. It leverages not only advanced technology like security information and event management (SIEM) tools, but also security experts with the skills to manage it. In addition, it requires proven, repeatable processes for incident response.



Source: SANS Institute—Building a World Class Security Operations Center: A Roadmap

SOC ≠ SIEM

Technology alone is not enough. You need trained security analysts and repeatable triage and investigation processes.

A SOC is a combination of threat detection and response technology, people with cybersecurity skills to manage it, and incident response processes.

Weighing the Decision: Build vs. Buy

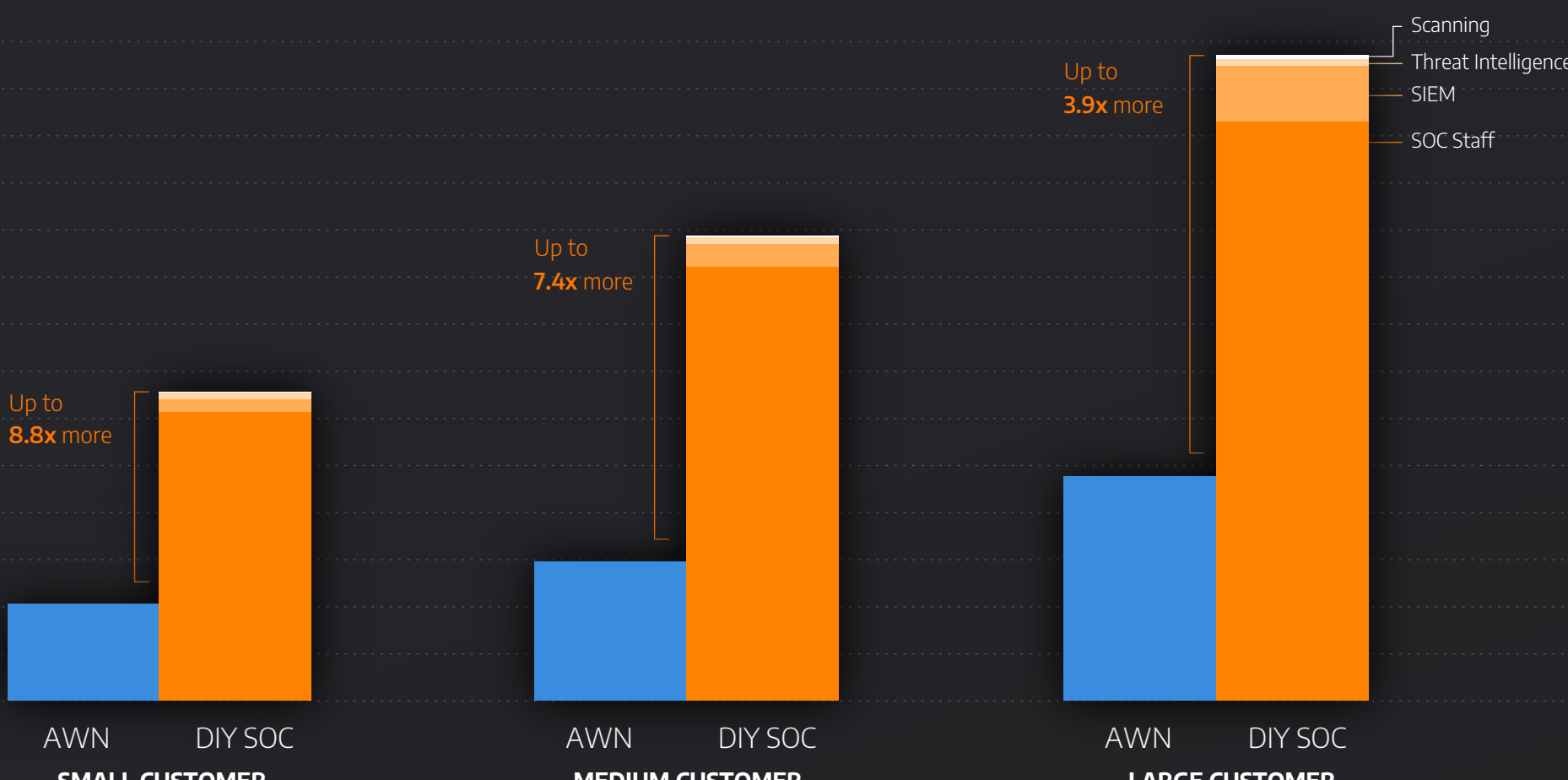
Evaluating the various attributes of an in-house SOC against Arctic Wolf's SOC-as-a-service, the AWN CyberSOC™ service.

Attribute	AWN CyberSOC™ (SOCaaS)	DIY SOC
Cost	Predictable and economical	Unpredictable and cost prohibitive for small to midsize companies with no/limited security staff
Staffing	Fully managed by Arctic Wolf	Entire responsibility for recruitment, training, and retention rests with the organization
Deployment	Turnkey	Months to potentially years for full deployment
Customization	High within the AWN CyberSOC platform's feature set, with customer-customization orchestrated by tenured experts	High within the feature set of SOC technologies purchased, but dependent on SOC staff's time and expertise to customize
Resiliency	Cloud-based design to ensure enterprise-grade service reliability	All factors that could contribute to downtime must be identified and accommodated by the organization
Technology Evolution	Fully managed by Arctic Wolf with new features and upgrades offered to all customers following testing and implementation	Timing and frequency dependent on organization's planning, budgeting, and implementation efficacy

Source: Frost & Sullivan

The Verdict: Comparing Costs Between Arctic Wolf's SOC-as-a-Service and a DIY SOC

Over a three-year span, Arctic Wolf's AWN CyberSOC™ service saves your organization up to 9x compared to building and implementing a SOC on your own—from purchasing a SIEM to hiring security staff to developing all required incident response processes.



“SOC-as-a-Service versus DIY SOC: The Business Case for AWN CyberSOC is Compelling.”

For a complete cost breakdown and further details behind Frost & Sullivan's comprehensive TCO analysis

[Download the Report!](#)