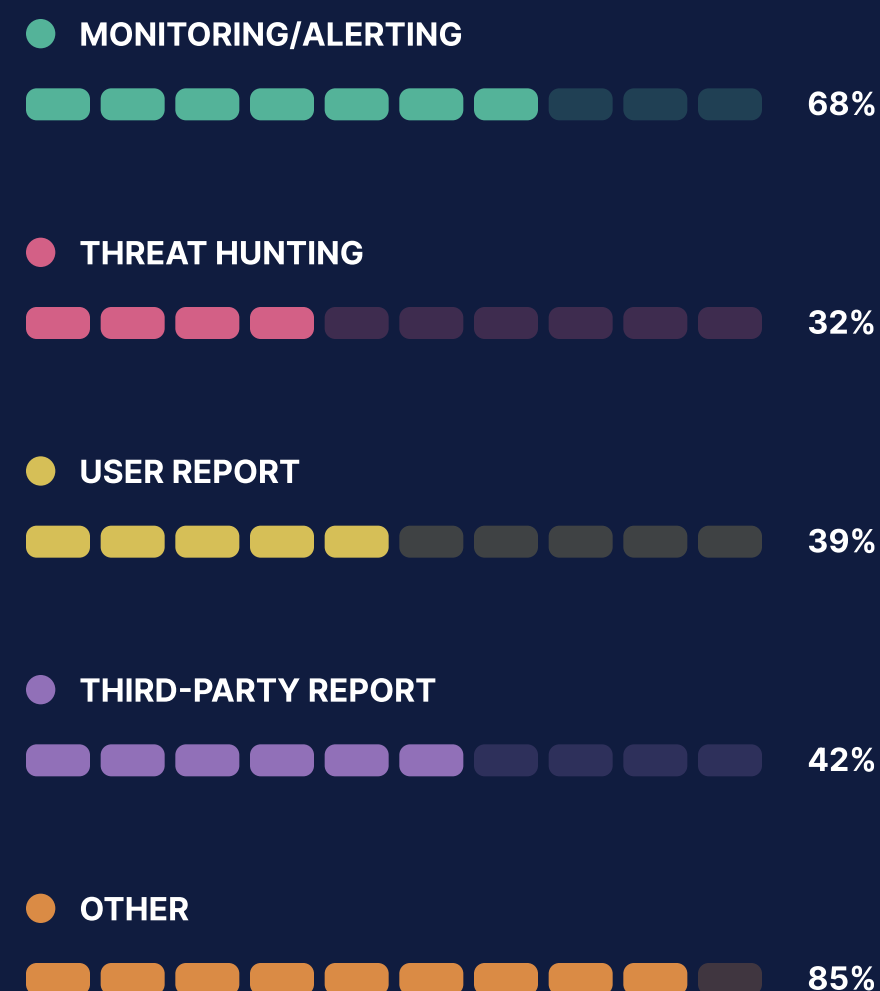# What's happening in your SOC?

As leaders, are we listening to our teams?

How do teams discover incidents?

Though monitoring and threat hunting uncover many incidents, it is alarmingly common to be tipped off by users and third-parties.

● **MONITORING/ALERTING**
68%

● **THREAT HUNTING**
32%

● **USER REPORT**
39%

● **THIRD-PARTY REPORT**
42%

● **OTHER**
85%

Nearly **1/3** of security practitioners feel that management disregards their recommendations.

Why aren't we listening?

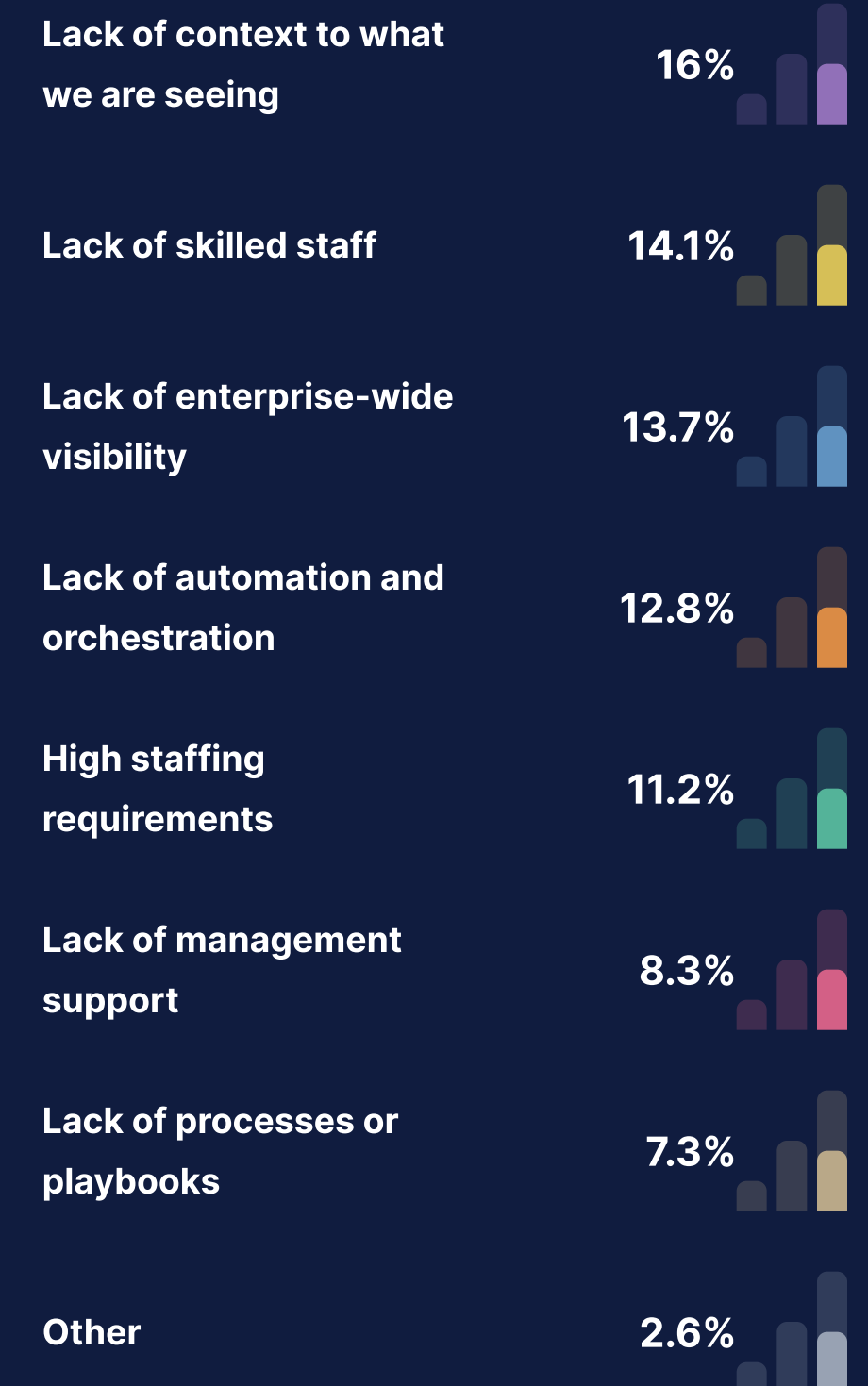Management must consider an array of additional factors, such as:

LEGACY TECHNOLOGY CONTRACTS

SERVICE PARTNER REQUIREMENTS

TEAM EXPERTISE

What hinders team success?

The greatest barriers to full utilization of SOC capabilities by the entire organization:

Lack of context to what we are seeing — 16%

Lack of skilled staff — 14.1%

Lack of enterprise-wide visibility — 13.7%

Lack of automation and orchestration — 12.8%

High staffing requirements — 11.2%

Lack of management support — 8.3%

Lack of processes or playbooks — 7.3%

Other — 2.6%

elastic

Review the **2023 SANS Institute SOC Survey** to better understand your SOC.

See how **modernized security operations** can help your teams accelerate incident response, contextualize security data, and optimize resources.