Gartner
Peer Community

Modern Security Operations Center (SOC) Strategies

Modern security operations centers (SOCs) have the potential to protect organizations against an ever-evolving threat landscape through monitoring, detection and response capabilities, but organizational needs and limitations vary. How are leaders currently deploying and maturing modern SOCs?

One-Minute Insights:

- A hybrid approach is the most common SOC target operating model (SOCTOM)
- Respondents are most commonly satisfied with their SOC's infrastructure, policies and team skills
- Over half assess their SOC's operating model at least quarterly if not more often
- The majority of organizations use penetration testing and red team exercises to evaluate SOC capabilities
- Most leaders see opportunities for improvement in their SOC's aggregation and correlation capabilities

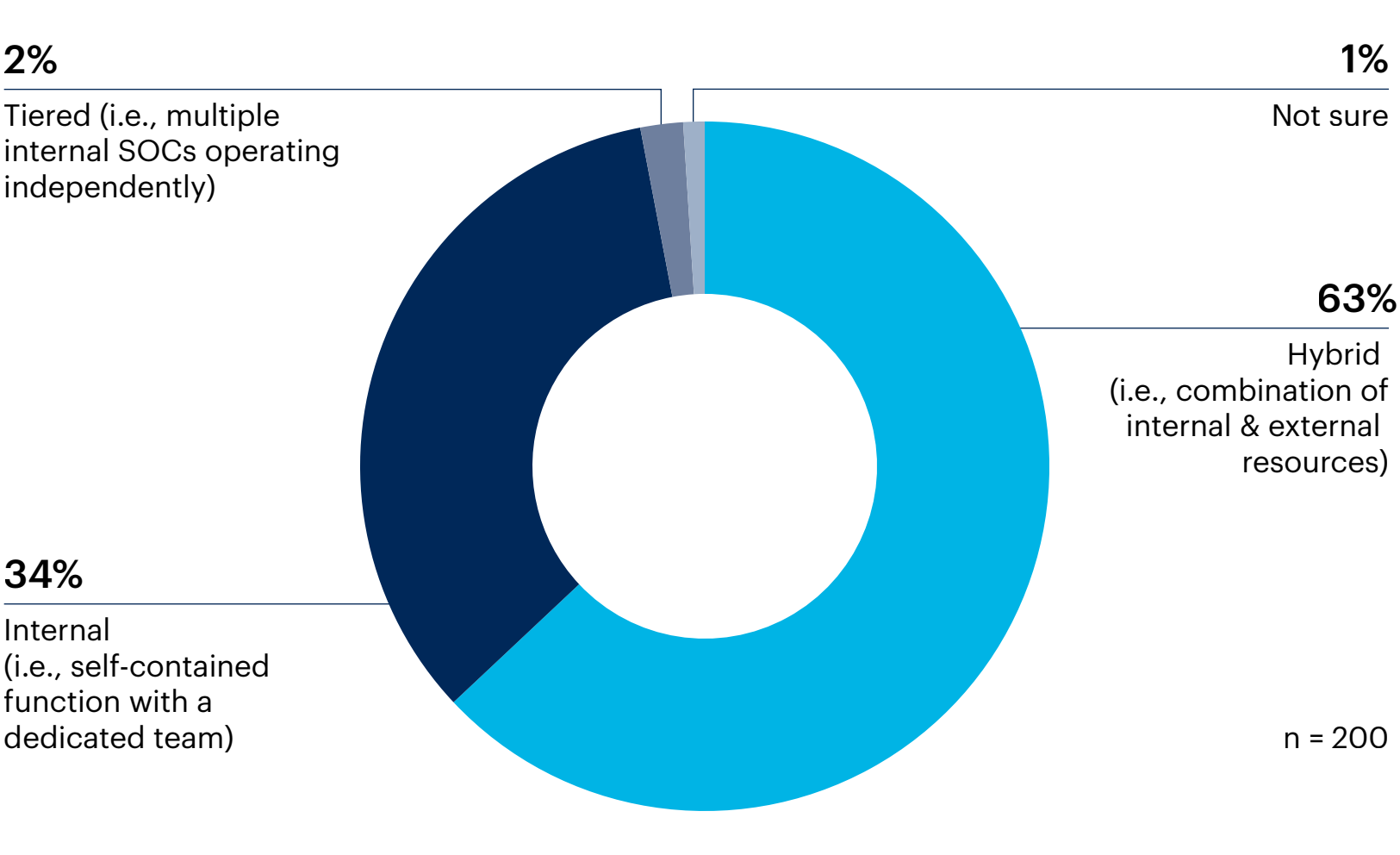
Data collection: Nov 28, 2022 - Mar 2, 2023

Respondents: 200 IT and information security leaders

Most organizations have SOCs that use a hybrid operating model and leaders are typically satisfied with their SOC infrastructure

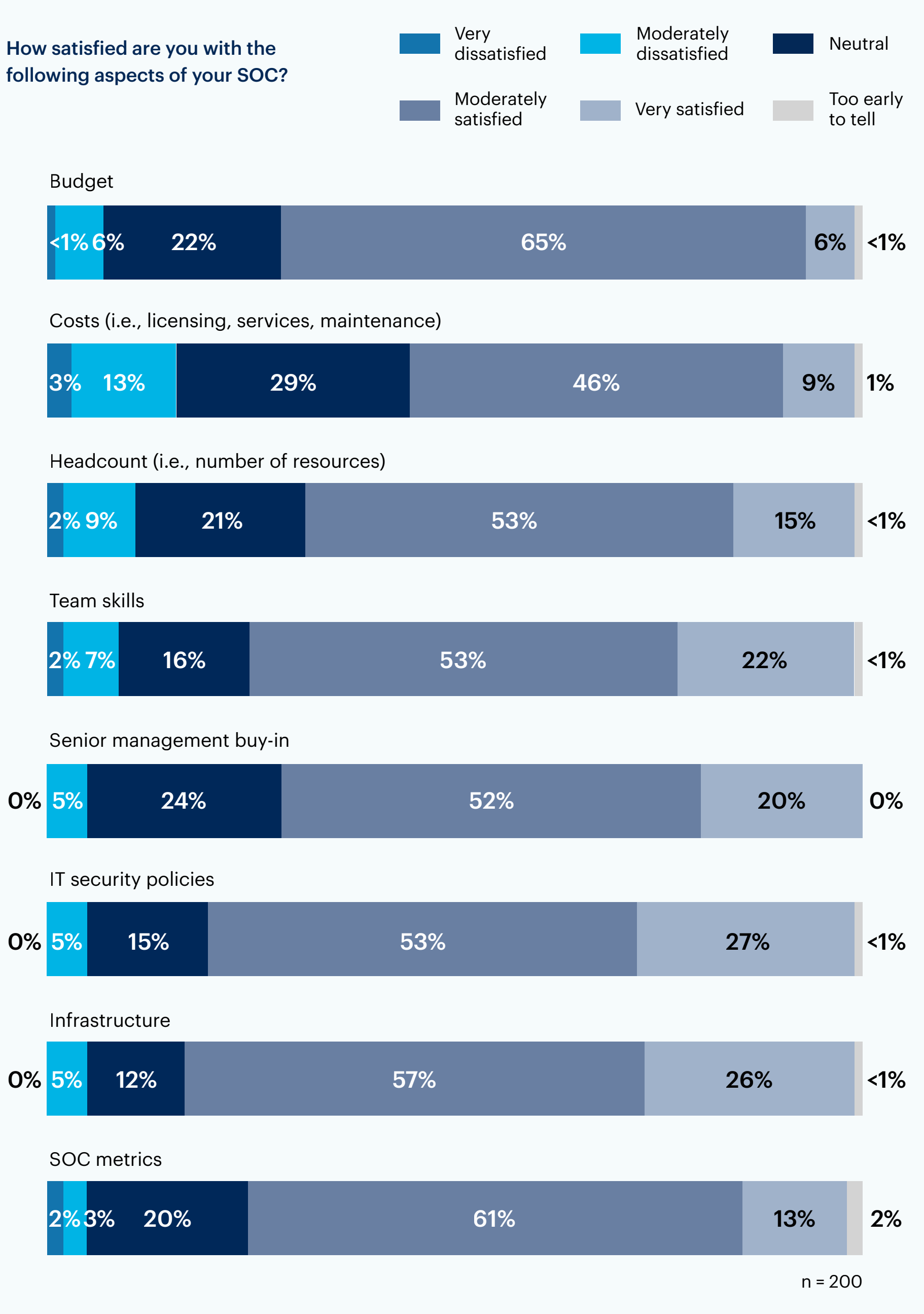
The **most common SOC operating model** is a **hybrid approach** combining internal and external resources **(63%)** but just over a third have an internal SOC **(34%)**.

Which of the following best describes your SOC target operating model (SOCTOM)?



The **majority** of leaders feel **satisfied with their SOC's infrastructure (83%)**, IT security policies **(80%)** and team skills **(75%)**, but costs show room for improvement as just over half **(55%)** feel satisfied with this aspect.

How satisfied are you with the following aspects of your SOC?



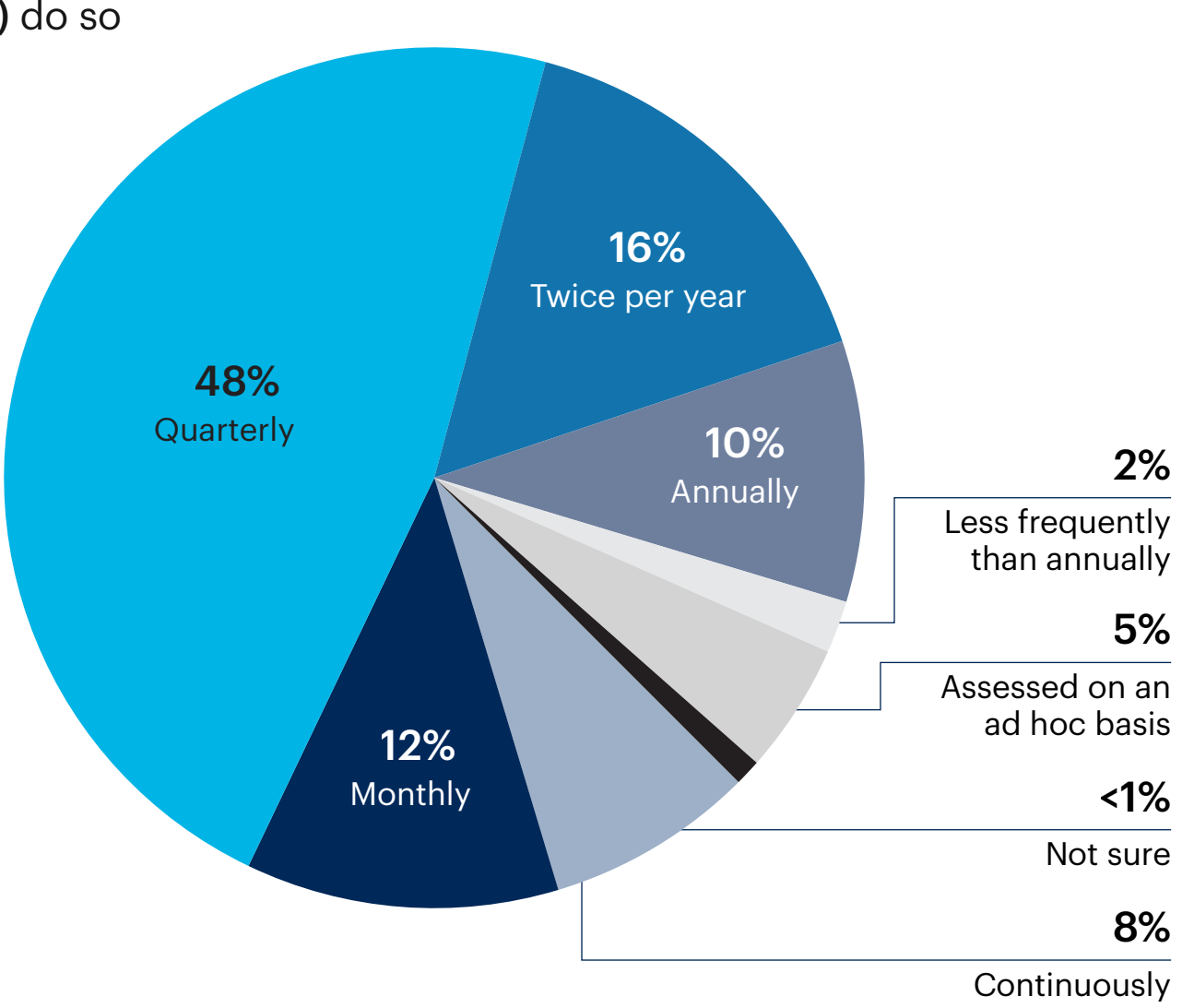
> "Gaining true, 100% visibility into our environment has been the biggest goal for our SOC."
>
> - VP, natural resource extraction industry, 10,000+ employees

> "Resources and skills are the main challenge for us."
>
> - C-suite, finance industry, <1,000 employees

Many leaders asses their SOC models at least quarterly and change them in response to transformation initiatives or evolving threats

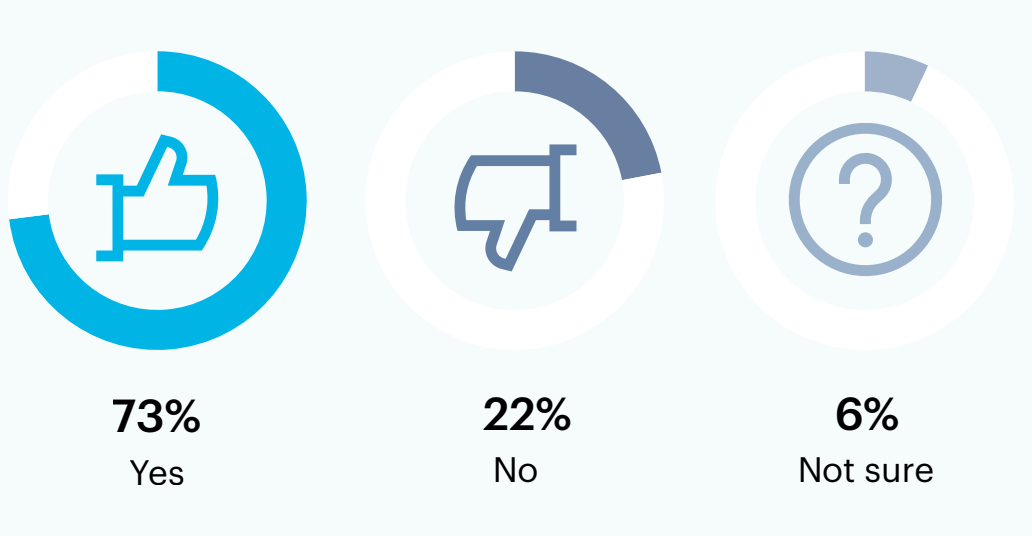
Most organizations **(48%) evaluate their SOC models** on a quarterly cadence but a fifth **(20%)** do so more frequently.

How often is your SOC model assessed?



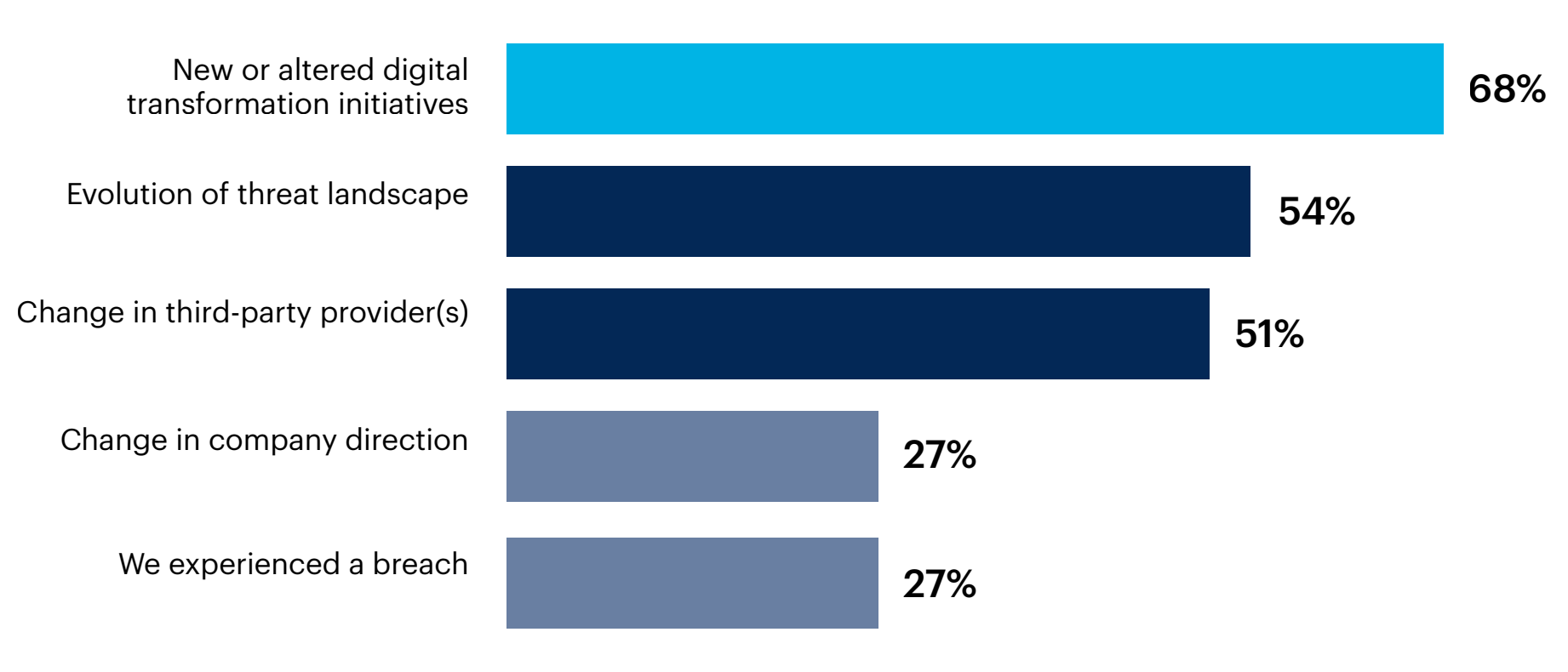
Nearly three-quarters **(73%)** of leaders saw their **SOCTOM change within the last year**.

Has your SOCTOM changed in the past year?



Organizations typically **changed their SOCTOM** due to new or updated digital transformation initiatives **(68%)**, developments in the threat landscape **(54%)** or changing third-party providers **(51%)**.

Why did your SOCTOM change over the past year?



Skills availability **24%**, Changing business conditions due to Coronavirus pandemic **23%**, Change in security leadership or strategy **22%**, Budget constraints **15%**, Increased complexity of organizational needs **12%**, Lack of business-specific focus in previous model **5%**, New or updated regulatory/compliance requirements **4%**, None of these **0%**, Other **0%**

n = 145

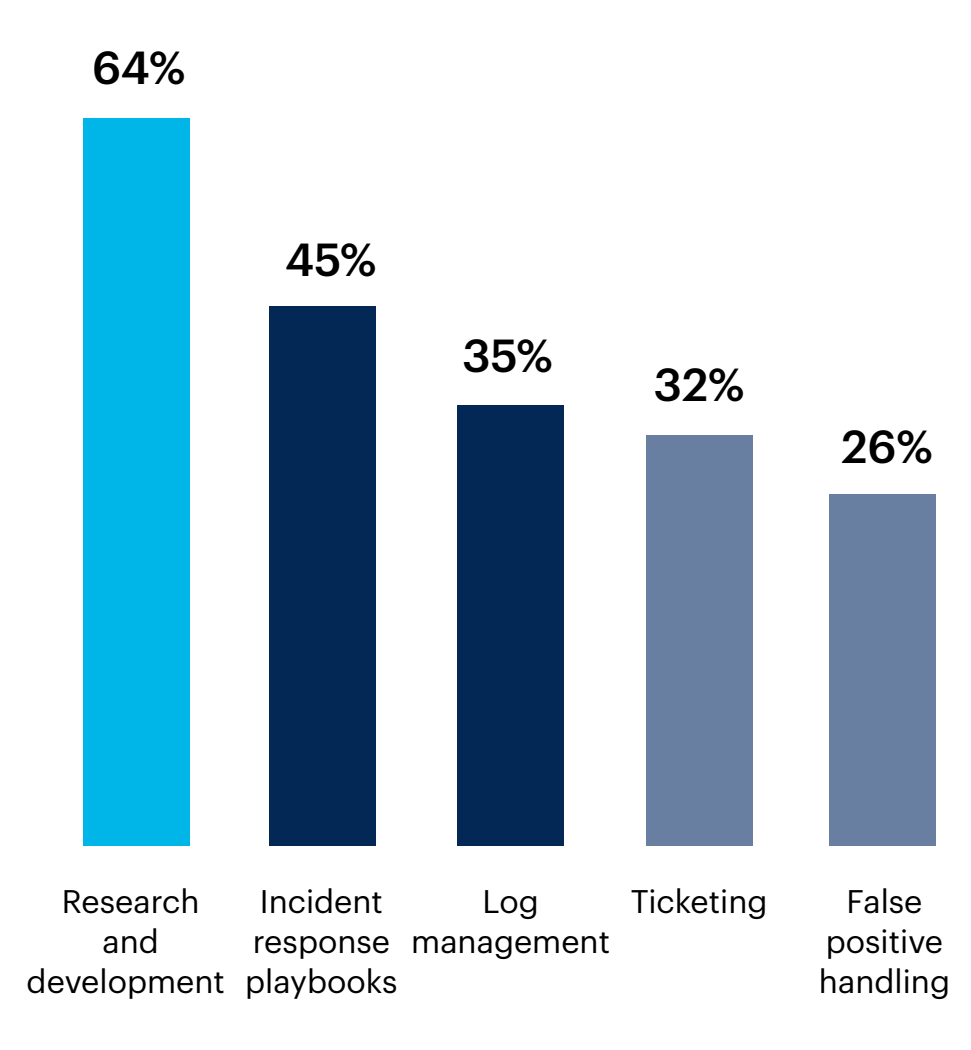
> "Our strategy has evolved with the launch of our own digital services — we now need a responsive, available SOC."
>
> - C-suite, software industry, <1,000 employees

> "Our SOC has been augmented by a third party to keep up with skills and tools required."
>
> - VP, telecommunications industry, 5,000 - 10,000 employees

> "It's a never ending update process."
>
> - Director, software industry, 5,000 - 10,000 employees

SOC research and development processes need to be improved, as do aggregation/correlation capabilities

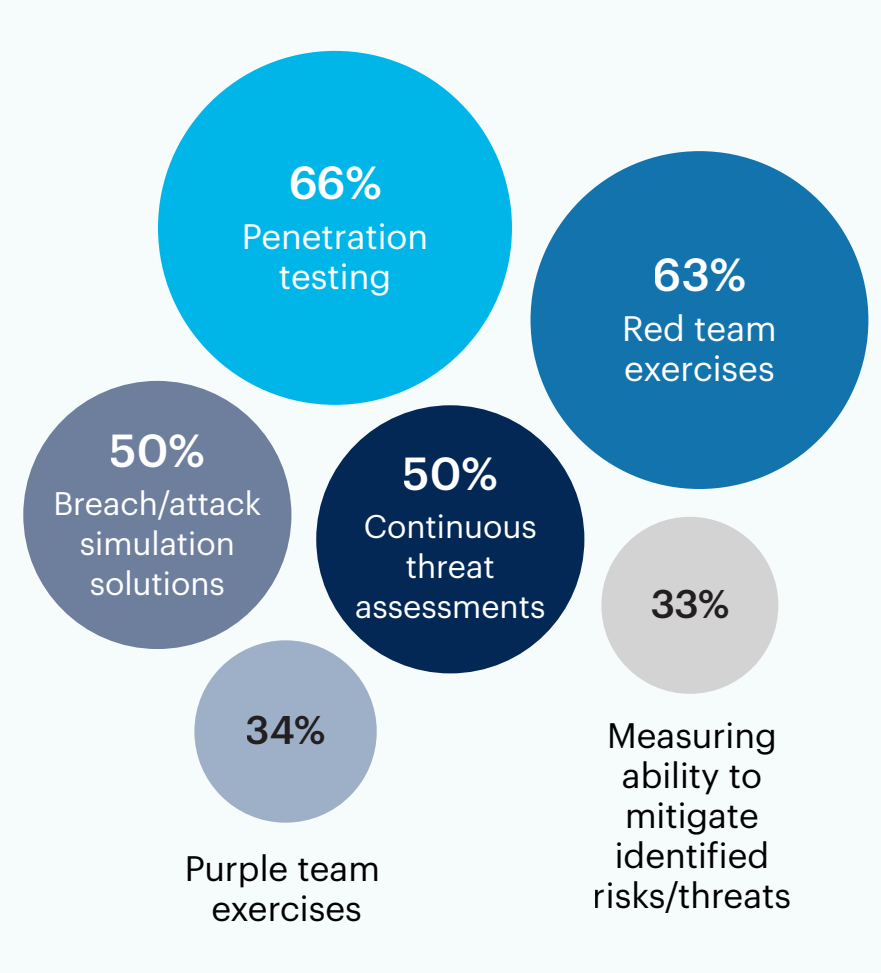
64% of respondents say their **research and development processes** are among those that **require the most improvement**. Many also see optimization opportunities in their incident response playbooks **(45%)**, as well as log management **(35%)** and ticketing **(32%)** processes.



Which of your SOC processes are most in need of improvement?

Infrastructure playbooks **25%**, Breach notification **18%**, Threat intelligence handling **17%**, Forensic handling **16%**, SOAR playbooks **13%**, Offense handling **9%**, Post-incident reviews (PIRs) **8%**, Threat hunting hypothesis creation **7%**, None of these **1%**, Other **0%**

n = 200

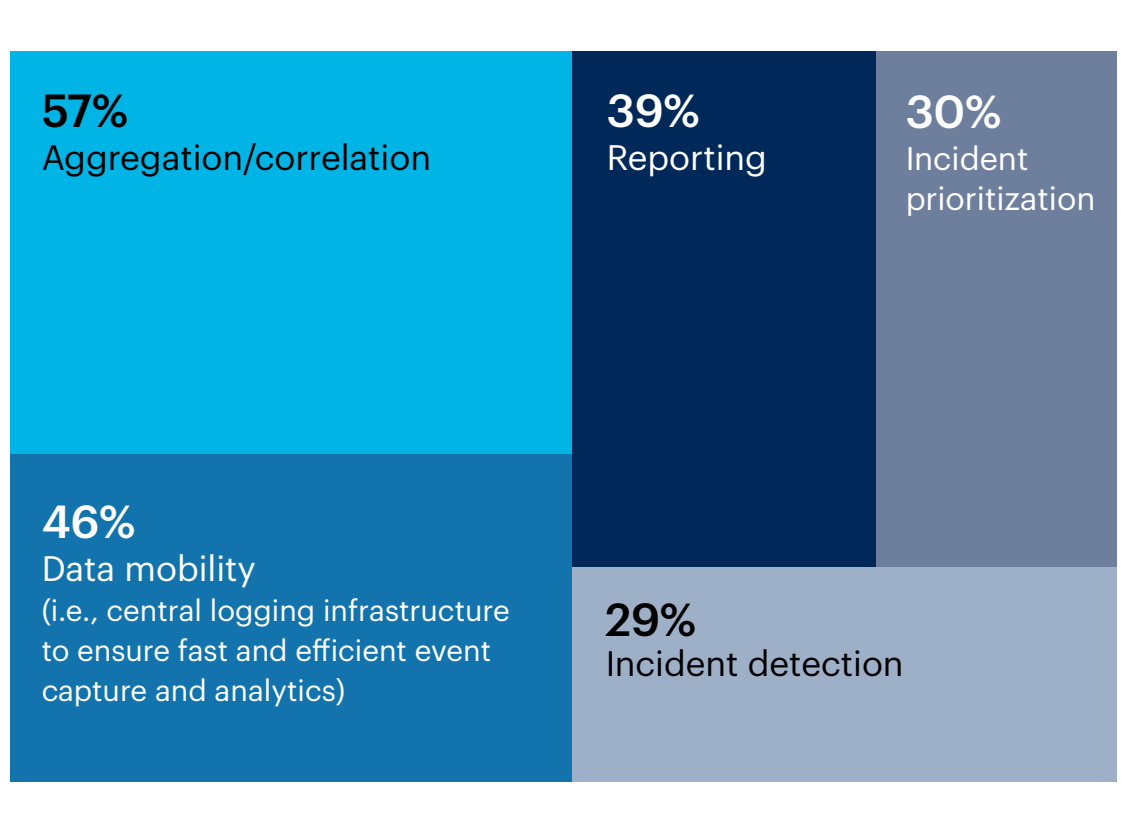


Leaders report their organizations **evaluate SOC capabilities** using penetration testing **(66%)** and red team exercises **(63%)**. Half of respondents **(50%)** employ continuous **threat assessments and breach/attack simulations.**

What methods do you use to assess your SOC capabilities?

None of these **2%**, Other **1%**

n = 200



Lateral movement tracking **28%**, 24/7 SOC monitoring **17%**, User risk detection **14%**, Complex threat detection **12%**, Incident response **10%**, Threat intelligence data management **9%**, Integrations **8%**, Risk visualization **8%**, Alert pipeline management **7%**, None of these **0%**, Other **0%**

Over half **(57%)** find their SOC's aggregation/correlation capabilities lacking. Data mobility **(46%)** and reporting **(39%)** capabilities in the SOC are also common target areas for improvement.

Which of your SOC's capabilities are most in need of improvement?

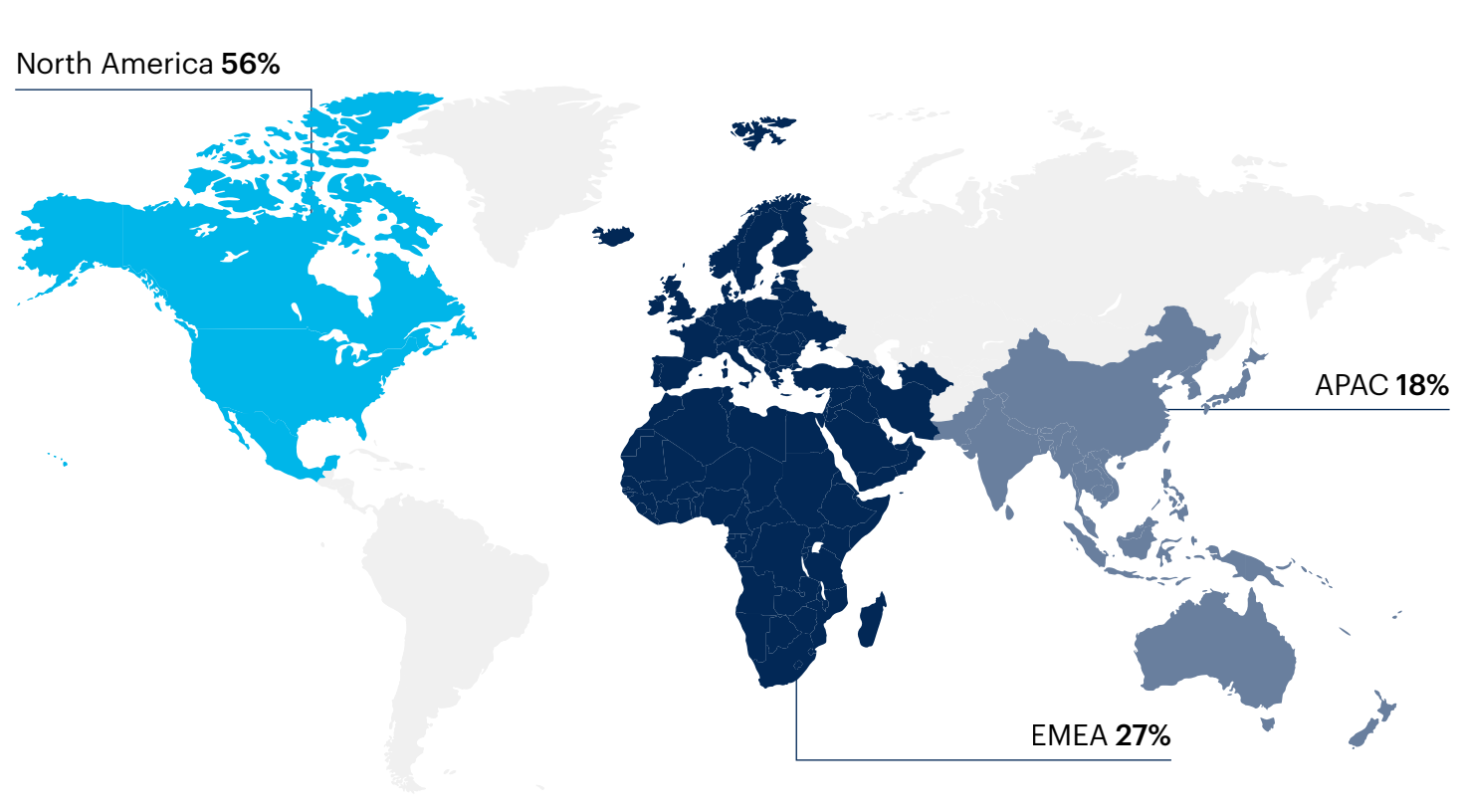
n = 200

> "False positive[s] and alert fatigue continue to be a major challenge for our SOC."
>
> - Director, professional services industry, 10,000+ employees

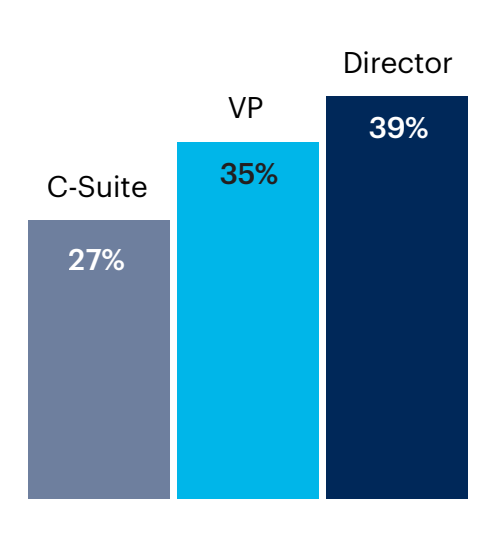
> "Unfortunately, due to the economic crisis, we have to make do with what we have. The team is on continuous high alert and barely have time to breathe due to lack of funding and quiet resignation. It's a really tough period."
>
> - C-suite, educational services industry, <1,000 employees

Respondent Breakdown

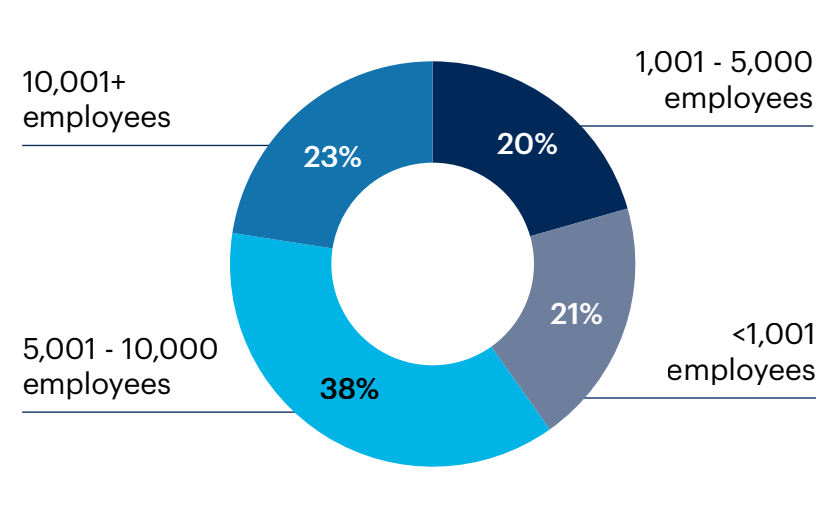
Region



Job Level



Company Size



Gartner

Source: Gartner Peer Community, Modern Security Operations Center (SOC) Strategies survey