How Effective Is Your SOC?

Inside Security Operations Centers

Key Data from the Exabeam 2020 State of the SOC Report

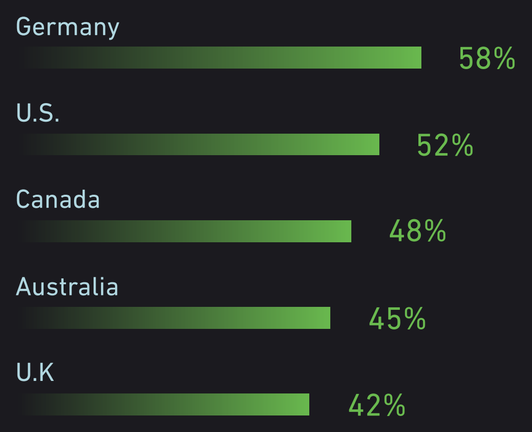
Security operations centers (SOCs) are major investments in the security of an organization's IT assets and intellectual property. They need to function as efficiently as possible in order to help a company thrive and function smoothly—and the future points to the cloud as the answer. Our "Exabeam 2020 State of the SOC Report" uncovered the ways that survey respondents across the world ensure their SOC is as effective as possible.

Process Makes Perfect

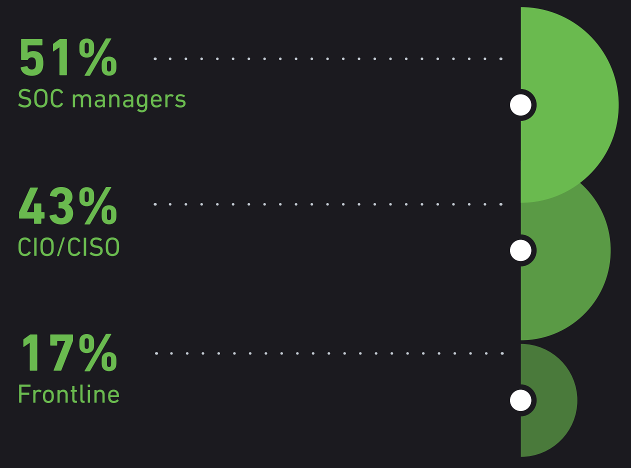
While U.S. and U.K. SOCs reported significant year-over-year declines in their ability to perform threat modeling and budget/resource allocation, concerning overall processes, German and U.S. SOCs view themselves as more effective.

When it comes to effectiveness by role in the company, we discovered that frontline employees are less confident in their abilities—with the greatest difference found in threat modeling.

Overall effectiveness of SOC teams by country:



Ability to conduct threat modeling:



This year's study reveals that 82% of SOCs are confident in the ability to detect cyberthreats, despite just 22% of frontline workers tracking mean time to detection (MTTD), which helps determine hacker dwell time.

Hiring and Staffing is Key

Hard skills will always be important in SOC teams. But this year, 62% of SOCs expressed an increased emphasis on soft skills as a top factor in hiring candidates.

The most important soft skills for a SOC candidate:

- Ability to work in teams
- Communication
- Effective management
- Leadership ability
- Personal/social skills

The biggest hiring challenges SOCs face:

40%
say there are not enough qualified people

34%
struggle to find candidates with the right expertise

▶ SOC staffing remains a critical issue as well, with

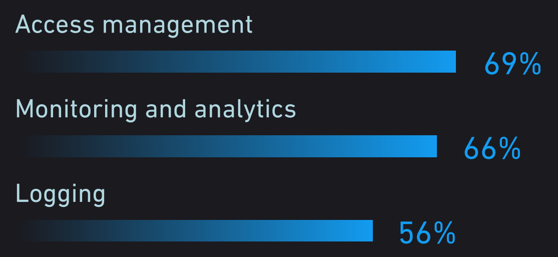
38%
of organizations reporting feeling that their SOC is understaffed. However,

48%
of less effective SOCs reported feeling more overstaffed and lacking necessary investment in technology, training, and staffing.

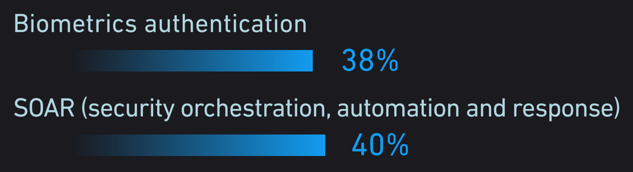
Cloud Takes Center Stage

As organizations move to the cloud, their priorities have started to shift—as well as their expectations about which tools will become crucial in the future, and which pain points are the most difficult to deal with now.

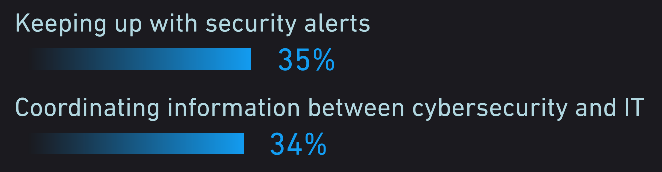
Top priorities for SOC roles:



Which tools will take precedence over other technologies over the next 3-5 years?



Top technology pain points



exabeam

Want to learn more? Read the full 2020 State of the SOC Report here.