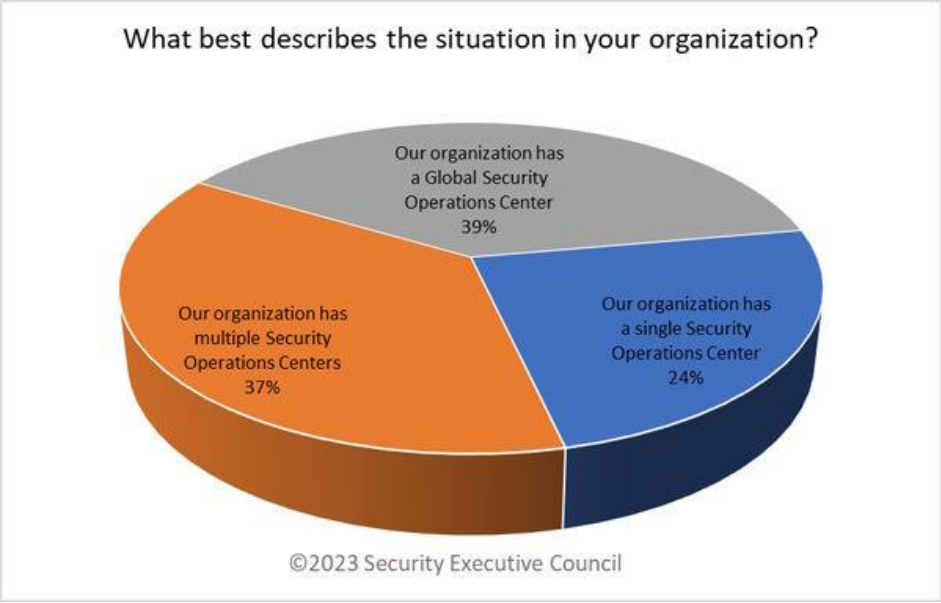
SEC
SECURITY EXECUTIVE COUNCIL
A research and advisory firm

Program Best Practices > GSOC >

Security Barometer: How Many Sources of Information Are Coming into Your SOC?

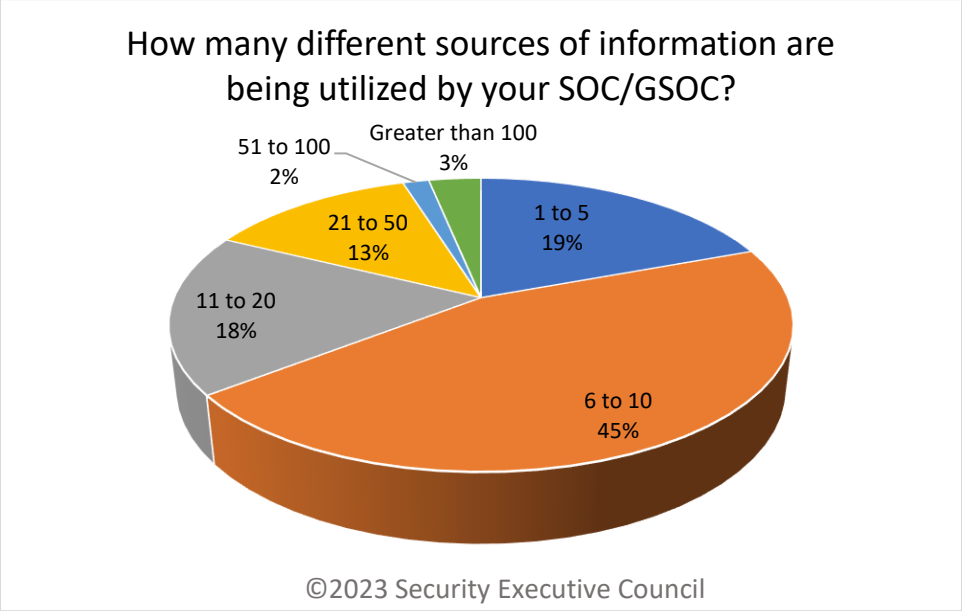
One of the purposes of a security operations center is to streamline monitoring, detection, and response by consolidating risk information. With the glut of data sources available, how many information streams are SOCs and GSOCs commonly using? And what are security leaders doing to ensure that the information they're analyzing is being disseminated and used by the functions that can benefit from it?

Our May 2023 Security Barometer examined these questions.

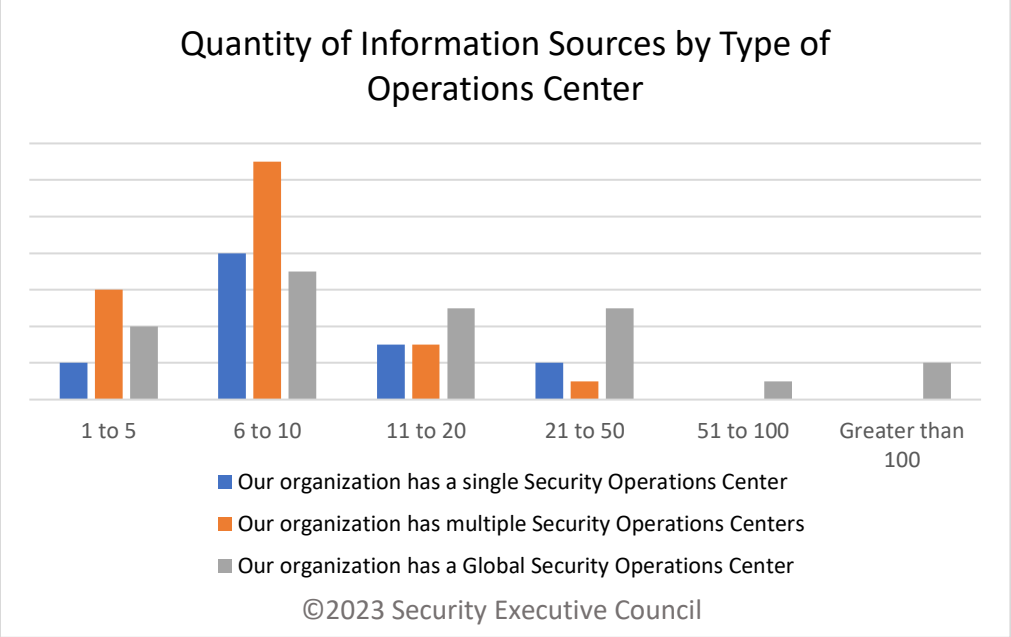


There was an almost even representation of respondents with global security operations centers (39%) and multiple security operations centers (37%). About a quarter of respondents maintained a single SOC (24%).

It's important to note that SOCs can vary widely in their mission and structure. One respondent noted in comments that their organization also maintains a separate cyber SOC, which may or may not interface directly with the GSOC or SOC. One noted that they maintain a single GSOC along with multiple SOCs or command centers, and another said multiple GSOCs manage different components of the business.



Overall, most (45%) respondents reported that their SOCs/GSOCs use 6 to 10 information sources. This was the most-reported response among all types of information center.



Respondents with global security operations centers reported a wider range of information sources than the other two types, with some in every category from 1 to 5 through Greater than 100. No respondents with a single SOC or multiple SOCs reported using more than 50 sources.

Our final question to respondents was this: How do you ensure that functions within the organization are aware of the information available from the SOC/GSOC and that they are making use of it effectively?

Several of the responses focused on the relational, collaborative part of this equation:

- Limit the scope of information collected and that the use case fits our corporate needs. Socialize the type of information we collect or the type of information services we can provide with leaders in other parts of the business.
- This is an ongoing activity to determine information requirements of business partners, establishing collection plans, and then analysis and dissemination workflows.
- Collaborate with other functions or departments to share information about security threats and vulnerabilities. This can help other functions to better understand the potential risks and impacts on their respective areas of responsibility.
- We work closely with our stakeholders to determine what they care about, and disseminate alerts based on agreed-upon, predetermined thresholds. Most importantly, we maintain relationships with these folks outside of incident response, which gives us opportunities to socialize our services and become a familiar partner.
- We have distribution lists both internally to Global Security and externally of our department to our crisis and risk management teams. When major incidents occur, we are sharing the information real time to these groups. This allows them to disseminate further if necessary to other departments who may be impacted. We also handle all employee outreach for global incidents. Our GSOC is impowered to push out intelligence alerts providing guidance and accounting for safety to all employees globally.

Several noted having pre-determined criteria, policy and protocols for information dissemination. One comment specified that dissemination is tied to an incident response plan that clearly outlines the roles and responsibilities of different functions or departments during a security incident.

Many responses focused on the method of dissemination:

- Scheduled intelligence briefings
- Travel briefings and alerts
- Critical event notifications
- Zoom or Teams chat
- Mass notification tools
- Training and awareness education
- ESRM consultations
- Burst messaging
- Weekly email newsletter briefs
- Case management/workflow management tools
- Sharepoint

- Dashboard that both provides insights and tracks usage
- GSOC Web site

Some said organizational awareness of the SOC/GSOC and its capabilities is a struggle, or that there is currently no set process through which to disseminate information.

Next Steps

If you're interested in advancing your SOC/GSOC or benchmarking and networking with other security leaders on GSOC-related topics, consider engaging with our Next Generation GSOC Group.

For information: https://www.securityexecutivecouncil.com/research/knowledge-sharing

Visit the Security Executive Council web site to view more resources in the Program Best Practices : GSOC series.

About the Security Executive Council

The SEC is the leading research and advisory firm focused on corporate security risk mitigation solutions. Having worked with hundreds of companies and organizations we have witnessed the proven practices that produce the most positive transformation. Our subject matter experts have deep expertise in all aspects of security risk mitigation strategy; they collaborate with security leaders to transform security programs into more capable and valued centers of excellence. Watch our 3-minute video to learn more.

Contact us at: contact@secleader.com
Website: https://www.securityexecutivecouncil.com/

