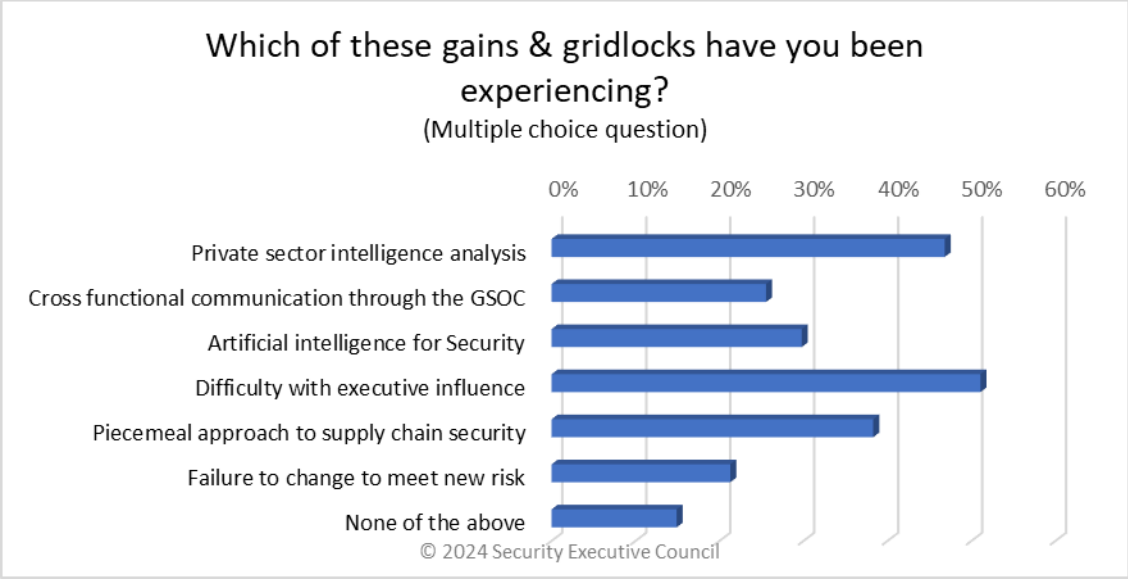
SEC
SECURITY EXECUTIVE COUNCIL
A research and advisory firm

Security Program Strategy & Operations > Emerging Issues >

Security Barometer: Security's Notable Gains & Gridlocks in 2023

2023 has certainly been an interesting year for Security. In discussions this past year with our clients we identified three areas where the industry is advancing in unique and innovative ways and three challenges that are holding back the programs.

In this Security Barometer quick poll, we wanted to see if the challenges and opportunities we have been witnessing our clients face this past year are widespread in the Security community as a whole.



While the results show that executive influence continues to be one of the most common challenges Security leaders face, it is interesting to note that private sector intelligence analysis is considered one of the key areas of emphasis for the Security function.

In addition, the fragmentary approach toward supply chain security continues to be a thorn in the side of organizations concerned with resiliency, quality control and efficient operations.

The survey respondents were provided the opportunity to share their opinions regarding challenges and opportunities their Security organizations are facing. Here are some selected comments provided by respondents:

- While private intel analysis function is being fleshed out quickly (main gain), it seems that other teams are way behind the curve in utilizing intel effectively (main challenge). The challenge usually lies in their turnaround expectations, lack of cleaned internal data for intel's use, lack of organized asks/needs, and discounting security's collective input based on intel products. For instance, executives are getting into the swing of collaborating with intel to enable real time travel monitoring in the GSOC, but they struggle to make clear their expectations around risk assessments (e.g., would they like one made in full for all trips of a certain type? will they actually consider recommended controls for high risks?). This illustrates the old-fashioned mindset of security as an insurance: a must-do reactive fallback, to set up something just in case. Preferably, once they get into a proactive mindset about security instead, executive influence and cross functional support with teams like supply chain will become much easier. Ideally, executives and other stakeholders adopt more of a "security first" attitude as well; this would cut down on decisions made without security input and that cause security to scramble in their aftermath (i.e., Real Estate team gave notice of an in-person site closure announcement merely hours before).
- Company's administrative model creates a unique challenge to implementing the known "corporate security" elements.
- Executive buy-in has definitely been an enduring challenge. We've made some inroads, but still much more to achieve here. We would love to explore more in the AI realm, yet have had to de-prioritize in favor of programmatic maturation.
- Private sector intelligence analysis as it relates to operational security are hard to find.
- 1. Continued experiencing only limited interest from the business in business risk intelligence. Areas of buy-in have focused on support to travel security given concerns over eastern Europe and Israel.
  2. GSOC cross-functional communication improved when our team co-located with IT's cyber security team.
- Many Security Executives will continually face the problem of having to deliver from a reactive vs proactive position. The challenge in mitigating risk is that sometimes you may have to spend funds to maintain a positive security posture. However, if the c-suite does not see an immediate value or benefit that they can quantify then it becomes a challenge to protect assets and mitigate risks.
- We are filling an analyst role this year to assist us in improving in the area of intelligence

analysis. I do feel we are behind in this area. Also, I feel we need to do more with AI. What, I cannot specify, I feel like the saying, you don't know what you don't know. We are looking at [a proprietary AI based video analysis provider] for our video management system, but otherwise I feel there is probably a lot out there with AI that we are yet to act on.

- We have not stood up our EOC (GSOC) as of yet. This should occur in the next couple of months. I do anticipate the following gridlocks: executive influence concerns and struggling to find an identity within our organization.
- The biggest challenge is transitioning the GSOC to a more proactive posture in terms of Global Intelligence.
- Communication within the GOSC and how to grow the team and not be a checklist-oriented team.

See this page for more in-depth information on Security's Gains and Gridlocks.

Visit the Security Executive Council web site to view more resources in the Security Program Strategy & Operations : Emerging Issues 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/

