Program Best Practices > Global Security Operations Centers (GSOC) >

# Emerging Threats: How High-Performing GSOCs Are Adapting

By the Security Executive Council

On March 9, the SEC partnered with Topo.ai and LifeRaft to host Emerging Threats: How High-Performing GSOCs Are Adapting, an interactive panel discussion with Rob Gummer, the NFL's Director of Intelligence Operations; Nathan Mills, Zoom's Senior Manager of Physical Security; and Ed Shubert, McKesson's Senior Director of Global Security and Safety.

The hybrid event, hosted both virtually and in person by the NFL, explored the role of the GSOC in identifying and managing emergent threats, the power of executive influence, and more.

The meeting began with an overview of preliminary data from a GSOC-centered pre-event survey provided to participants, as well as preliminary results of topo.ai research dealing with executive influence and metrics tracking.

Preliminary pre-event survey results showed that participants expected the top threat to their brand in 2022 and beyond to be insiders (78% of respondents)

**What do you forecast will be the top three to five emerging operational risks or threats to your brand in 2022 and beyond?**
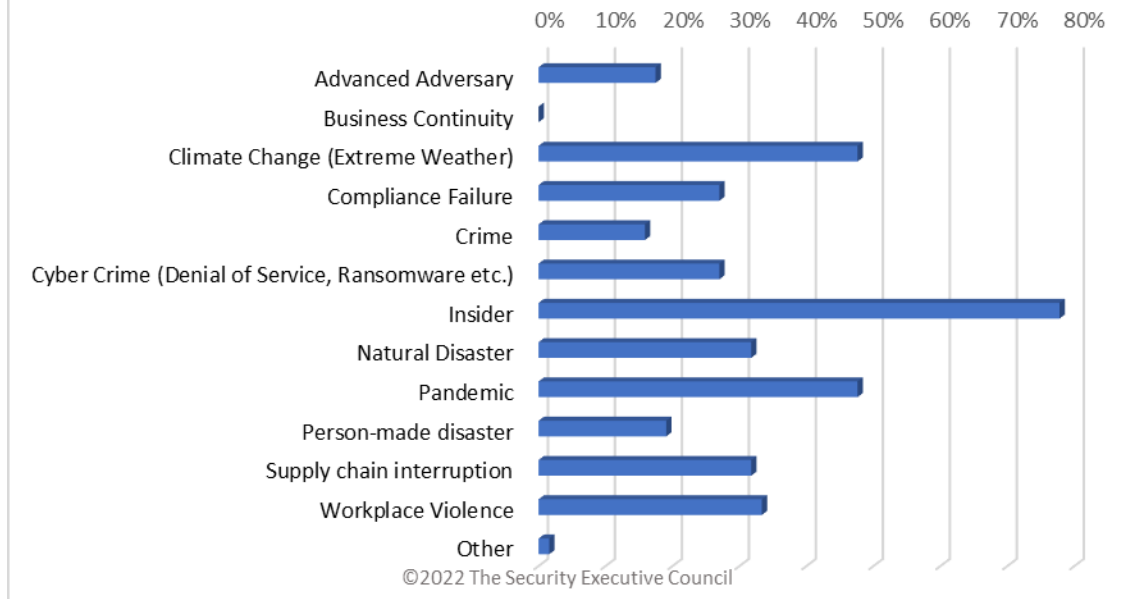
When asked what their company's primary working model would be moving forward, 92% said a hybrid of work-from-home and in-office.

The SEC also requested participation in two open research opportunities.

- The SEC's Security Leadership Research Institute (SLRI) is partnering with Resolver to investigate the organizational cost of loss due to theft, fraud, and abuse in hopes of finding an average cost of loss that would allow practitioners to compare their own numbers against it. Click here to participate.
- The SLRI and Kennesaw State University Institute for Cybersecurity Workforce Development are jointly investigating the current state of security convergence in order to build an improved model of how corporate and cyber security can or should work together for optimized risk mitigation. Click here to participate.

Here are some highlights from the conversation.

**On choosing technology and vendors:**

- In the past, technology choice was driven by availability. Users had to see what solutions there were on the market, then adapt their culture and requirements to fit the available solutions. Now, users can and should start with their requirements and be very specific about what they need, how they need it, and then find or request the solutions that will meet their requirements. It's important to set aside the time to plan for this.
- Technology is there to augment staff. Ask - how are your tools and technologies making your talent better? Is it too complicated to use? Does its complexity add value or does it mean that you can't build processes that are quick and responsive?

**On integration and open architecture:**

- Tools that talk together through open architectures amplify the value of all the technology you have, and if you can start with open protocols from the ground up, it will be much easier to expand capabilities as risks and needs change.
- When contracting with vendors, make sure to discuss an open API up front, and try to get it without any charge.

**On staffing models and retention:**

- Panelists ran their GSOCs on all-outsourced and hybrid (contract +FTE) models.
- The all-outsourced model allows the GSOC to add qualified staff more easily and quickly because the staff is sourced through the vendor. It also allows for an embedded analyst that can focus on deep-dive, subject-specific analysis and can draw from the hundreds of other analysts at the vendor company for support. This model tends to be expensive.
- The hybrid model requires that the company look at both the contract employees and the staff as GSOC team members, with the same expertise and access. It's important to establish a team culture and to award both staff and contract employees to show they're valued.
- GSOC operations is a highly demanding job. To keep these staff, it's important to get them the right training, to ensure they're getting their needs met, to ensure they can access professional growth, and to give them opportunities to do things beyond gates, guards, guns, and monitoring. Give them opportunities to innovate.

**On adding and demonstrating value:**

- One panelist remarked that his team keeps metrics on everything his operators touch. It's important to look at your processes, clearly understand where their value can be shown, and identify the opportunities to capture that value in metrics.
- One panelist collects and sends metrics reports through the CSO to the C-suite monthly, meaning they are constantly seeing this information. That makes it much easier to make

a business case for resources or expenditures. Another sits on weekly committee meetings to report on incident forecasts. Being proactive in getting the value numbers in front of the right audience is critical.

- In some cases, value is found when the GSOC takes over processes previously being done through contractors. In this case, value can be easily calculated.
- In others, GSOC technologies can be used for product quality assurance, prevention of spoilage or environmental damage of products. The amount of loss had the products been rendered unusable can be captured as a cost avoidance metric.
- It's greatly helpful to be able to show the budgetary committee a visualization of all the issues the GSOC has addressed at the site level, so it is easy to see how these capabilities could expand for greater value. Outcome-driven metrics tend to resonate with the C-suite.

**On branding and awareness of the GSOC:**

- Use good stories to your advantage. If there's a story of a heart attack victim getting care in time because of a GSOC-assisted evacuation, package that story and share it through the organization. This builds familiarity and confidence in the function.
- The terminology you use is important. One panelist switched from using the words "monitoring shipments" to "protecting shipments," and the message made a much greater impact on buy-in after the change.

**On prioritizing activities:**

- Staff and time are finite, but it's hard in a GSOC to drop any element of operations because so many operations at the GSOC are mission critical.
- One panelist deals with the challenge of prioritizing GSOC activities by clearly outlining each activity's objectives and key results, and if those don't align to the organization's objectives and key results, then the activity is dropped. If the team thinks the activity is too important to drop, they push it up to the COO to ask if it could become a strategic objective.

One common theme throughout the panel was the importance of sharing insights and ideas with other GSOC teams. The SEC's Next Generation GSOC Group serves exactly this purpose. It is a community of security leaders who are planning to consolidate, expand, or enhance their GSOCs. The group offers opportunities for benchmarking, information sharing, and continuing education, as well as access to resources and discounts. Click here for more information.

**Visit the Security Executive Council web site to view more resources in the [Program Best Practices: Global Security Operations Centers (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](mailto:contact@secleader.com)
Website: [https://www.securityexecutivecouncil.com/](https://www.securityexecutivecouncil.com/)