A Guide to Understanding Global Security Operations Centers

By: Greg Newman, VP of Operations, HiveWatch

Many large organizations with an expanded footprint in regional or global marketplaces require the ability to oversee the physical security of their assets, people, and customers from a centralized location. That's where a Global Security Operations Center (GSOC) comes in. And regardless of if you work for an integrator, manufacturer, end user, or something inbetween, you will likely run across a GSOC while working in this industry. So, let's learn more about what this key piece of security infrastructure is all about.

What is a GSOC?

First and foremost, what is a GSOC?. We often refer to it as a GSOC when the organization has a large global footprint and manages multiple sites around the world from a single location. Similarly, you might also hear of it referred to as a Security Operations Center (SOC), which can imply more of a regional focus.

Either way, a GSOC is a facility that is tasked with monitoring and responding to security events on a global scale.

What is the function of a GSOC?

The role that a GSOC plays for an organization is that of a centralized place where incoming security data is collected, analyzed, and acted on. More specifically, a GSOC integrates intelligence from various sources to better facilitate a response in the event of a security incident or emergency. GSOCs act as a core function for mitigating risk to an organization, protecting assets and people from harm, and maintaining awareness of multiple locations and the risks they face.

GSOCs play a multitude of roles, including:

- Monitoring the performance of cameras and access control point solutions to ensure availability and the continuous flow of data
- Communicating with internal teams and external security personnel (guarding resources, security or business operations teams, local law enforcement) in the event of an emergency or incident
- Facilitating emergency response protocols

- Ensuring the safety and security of people, brand, and assets
- Providing valuable insights about the performance of an organization's security program using actionable intelligence
- Gathering data from multiple sources to better inform response through intelligence-driven decision-making

Who works in a GSOC?

GSOCs are primarily staffed by security operators and intelligence analysts who are tasked with managing incoming alerts, from identification to elevation to response.

What is a virtual GSOC?

For some organizations, building a GSOC can be cost-prohibitive or might not make sense to the business in the short-term. In these instances, businesses may benefit from an outsourced, virtual GSOC (vGSOC or GSOC-as-a-Service), which consists of external resources available to oversee and respond to physical security events in real-time from a centralized location. Typically, this consists of a customized solution built around the individual needs of how the company operates but managed by external experts. These vGSOC components utilize technology that the customer has implemented with standard operating procedures (SOPs) that are specific to the customer's needs.

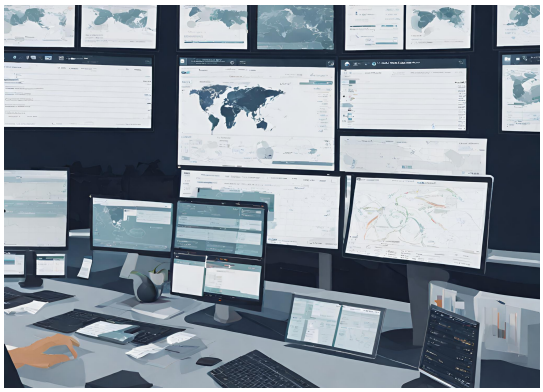
In some cases, companies may engage with a vGSOC as they build their own infrastructure in an effort to make changes/transition their existing security program to an in-house model. Using a vGSOC saves an organization money by cutting down on internal resources and the training needed to stand up such an operation.

What kinds of technology are found in a GSOC?

While incoming data from the more traditional end point solutions, such as access control and video surveillance cameras, can be funneled to the GSOC for analysis by operators, there are other tools that may be used, including:

A video wall/workstations: It might not look exactly like a scene from Minority Report, but a GSOC typically does have large screens displaying any number of information feeds, such as live news broadcasts, social media feeds, video feeds, and more.

Operational dashboards: It's not uncommon for GSOC operators to have to navigate between multiple screens and solutions to get the information they need about a specific incident. However, the modern GSOC should be well equipped with operational dashboards and a fusion platform designed to bring in data from multiple sources and aggregate the information for operators. The result is a more streamlined response that can save money and time.



Artificial intelligence (AI): It may seem like a buzzword, but there's a lot of ways AI is being used in a modern GSOC through threat detection, anomaly detection, and streamlining processes for operators and guarding resources.

Threat intelligence solutions: Software that can ingest the data incoming to the GSOC from various sources, determine levels of risk, and make recommendations based on the findings are changing the way GSOCs are viewed to the organization. Reducing risk is the main goal of the use of this kind of technology.

What are some of the challenges that a modern GSOC faces?

While there are resource-related challenges that GSOCs face – such as a lack of guarding resources, high turnover, and high rates of burnout – there's also the overwhelming amount of incoming data that makes it difficult to drill down into what's important. For many GSOCs, data hasn't been a problem to generate; it's the ability to analyze the incoming data and turn it into usable information for relevant stakeholders that's been a real issue. Particularly, it's a challenge to use that data to show return-on-investment (ROI) on the capital spent on security, and showing a business' security program as being beneficial, not just a cost center.

As operators are able to leverage more intelligent platforms for aggregating the streams of data coming into the GSOC, the result will be a better understanding of pain points within a security program, better response times, and the reduction of noise and false alarms, which can ultimately address some of the causes of burnout.