HiveWatch

Selecting an In-house GSOC vs. a GSOC-as-a-Service for Your Organization

How to ask the right questions, determine the best fit, and choose technology that empowers teams

A common decision organizations face is if, when, and how to create a physical global security operations center (GSOC) to manage day-to-day operations. In the past, the only option was to build something internally from the ground up, but now security teams are empowered with the choice of keeping things in-house, or outsourcing the operation (commonly known as GSOC as-a-service, or GSOCaaS).

Both are viable options and there's a time and place for each.

This eBook aims to educate security leaders and practitioners about the role the GSOC plays in the overall security posture of an organization and proposes questions around whether the organization should stand up its own GSOC, or look toward an external provider. Here's what you can read more about:

- The roles and functions of a GSOC
- The differences between an in-house and outsourced GSOC (and what a hybrid model looks like)
- How to approach the decision to build a GSOC or outsource one
- Questions to ask GSOCaaS vendors
- Sourcing components of an internal GSOC
- Technology considerations to make during development

See what these end users from JetZero and ServiceNow had to say about standing up an external GSOC in this on-demand webinar.

WHAT IS A GSOC?

Definitions are everything, so how we define what constitutes a GSOC is crucial before we start telling you whether you need one in-house (or outsourced).

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. However, there are other names that exist:

- Command Center
- Physical Security Operations Center
- Fusion Center
- Regional Security Operations Center
- Operation Center
- Central Intel Center

No matter what your organization calls it, when we talk about the GSOC, we mean a facility that is tasked with monitoring and responding to security events on a global scale.

> **Global Security Operations Center (GSOC):** n. A facility that is tasked with monitoring and responding to security events on a global scale.

WHAT IS THE FUNCTION OF A GSOC?

The GSOC serves as a central hub for collecting, analyzing, and responding to incoming security data. The GSOC integrates intelligence from different sources to improve response during security incidents or emergencies and prevent them from even happening in the first place. They are essential for reducing risk to an organization, safeguarding assets and individuals, and staying informed about the security challenges across multiple locations.

GSOCs play a multitude of roles, such as:

- Monitoring the performance of cameras and access control point solutions to ensure continuous data flow and availability
- Communicating with internal and external security personnel (guarding resources, resource officers, 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 operators and analysts who are tasked with managing incoming alerts, from identification to elevation to response.

WHAT KIND OF DATA IS FUNNELED INTO THE GSOC?

Internally, GSOCs may receive data from human resources, access control systems, video surveillance data, security officers and their patrol information, supply chain oversight, and more. For instance, the GSOC may have access to executive travel plans to alert relevant parties to potential threats and monitor for safe arrival and departure.

External data might include local law enforcement scanner information, traditional news sources, weather data, social media feeds, government-related alerts and PSAs, and even dark web monitoring.

All of the data from these sources is typically centralized in a GSOC for comprehensive situational awareness and quick response to incidents, as well as proactive planning and response. The data helps operators make more informed decisions and coordinate security teams and their response more effectively.

Examples of data that can be ingested into a GSOC:


Human Resources Data


Access Control Systems


Alarm Systems and Sensors


Video Surveillance


Incident Reporting Systems


Threat Intelligence


Law Enforcement and Government Feeds


Building Management Systems


Supply Chain Oversight


Security Officer Reports


Communications and Collaboration tools


Vehicle and Traffic Monitoring


Weather Data


Social Media and News Feeds

DEFINING IN-HOUSE AND GSOC-AS-A-SERVICE

Understanding what role a GSOC plays in the overall goals of a security program is the first step in identifying the role that it will play in yours. The next step involves learning the differences between keeping the function in-house, or outsourcing to a third party – or GSOCaaS.

What is an in-house GSOC?

An in-house GSOC refers to a security operations center that is managed and operated internally by a company's own staff in their own physical location, rather than outsourced to a third-party service provider. It serves as the hub for overseeing and managing physical security operations, handling real-time monitoring, threat detection, incident response, and crisis management for an organization.

It is used to monitor multiple locations (such as across a geographic region) or a single campus, depending on the size and scope of the location.

Benefits of an in-house GSOC

- Provides ownership and control over the GSOC infrastructure, staff, processes, and data, as well as security policies and procedures.
- Staffing is done by internal employees who work directly for the organization, including security analysts, operators, incident managers, or other security personnel. This allows for better control over cultural fit, as the staff members interact more regularly with other employees.
- Aligned with the company's security requirements, risks, and objectives.
- Monitoring and response protocols are customized to the organization's specific security concerns (examples: protection of critical infrastructure, retail locations, high-value assets, or confidential information).
- Integration with the organization's broader risk management, crisis response, and business continuity strategies. During a critical event, the presence of a security manager can help streamline decision-making.
- Since it's on-site, there's a familiarity with facilities, layouts, and key players outside of the security organization.

Drawbacks to an in-house GSOC

- High initial cost to set up, including an extensive capital investment in infrastructure, technology, software, and security systems, such as video surveillance, access control, and alarm systems (and much more).
- Ongoing operating costs, including hiring and training skilled staff and analysts, maintenance of systems and solutions, ongoing updates to systems and software, and more.
- Continuous investments are needed for training and additional expertise as threats evolve.
- The need for more technical support of systems and solutions – both software and hardware.
- Lack of scalability as the needs of the organization change and growth occurs.
- Geographic limitations depending on the needs of the organization.
- Business continuity risks and the potential for a single point of failure within the GSOC; for example, a natural disaster or flood, power outage, or cyberattack.
- Longer time to plan, train, and implement an in-house GSOC can mean a delay in return on investment (ROI).
- Compliance, data security, and business continuity risks that must be managed internally.

WHAT IS A GSOC-AS-A-SERVICE?

GSOC-as-a-Service consists of outsourced, external resources available to oversee and respond to physical security events in real time from a centralized location. Typically, this is a customized solution built around the individual needs of how the company operates, but managed by external experts. These service-based 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 opt for GSOCaaS as they build their infrastructure in an effort to transition their existing security programs to an in-house model. Outsourcing GSOC services helps organizations save money by reducing the need for internal resources and the training required to establish such an operation.

Benefits of GSOC-as-a-Service

- Cost-effective access to advanced technologies and skilled personnel with an upside to having an operational expenditure model (OPEX) that's billed as a monthly or annual fee, which might be more budget-friendly.
- Access to expertise that is hard to secure and retain. GSOCaaS providers maintain the responsibility of ensuring that everyone who works in the GSOC is up-to-date in certifications and training.
- Advanced technology and state-of-the-art tools that are needed to monitor ongoing situations.
- 24/7 monitoring and faster response times during an incident or emergency.
- Scalability to meet growing or changing security needs, such as adding more locations or supporting organic growth.
- Access to global threat intelligence and analytics, which helps keep organizations ahead of evolving risks and threats.
- Reduced complexity in managing security operations, saving time, money, and resources that can be allocated elsewhere in the company.
- Faster deployment and continuous support for business continuity and redundancy.

Drawbacks of GSOC-as-a-Service

- Perceived loss of control, as you can't physically direct day-to-day operations in the GSOC.
- Data security and privacy concerns.
- Potential communication and coordination challenges, which might include response time delays.
- Dependency on third-party providers for their capabilities, infrastructure, and reliability.
- Concerns with quality of service and the ability to easily switch if this becomes an ongoing issue.

WHAT IS A HYBRID MODEL?

Some organizations have the option to operate with a hybrid model, which involves a combination of in-house GSOCs (regionally, for example) with an outsourced GSOCaaS model. This might make sense if you have an in-house GSOC that covers incidents that occur within working hours or operational hours (like 9 a.m. to 5 p.m.) and would like to have 24/7 coverage. In this scenario, an external third-party provider would take over monitoring and incident response once the in-house GSOC was shut down for the day.

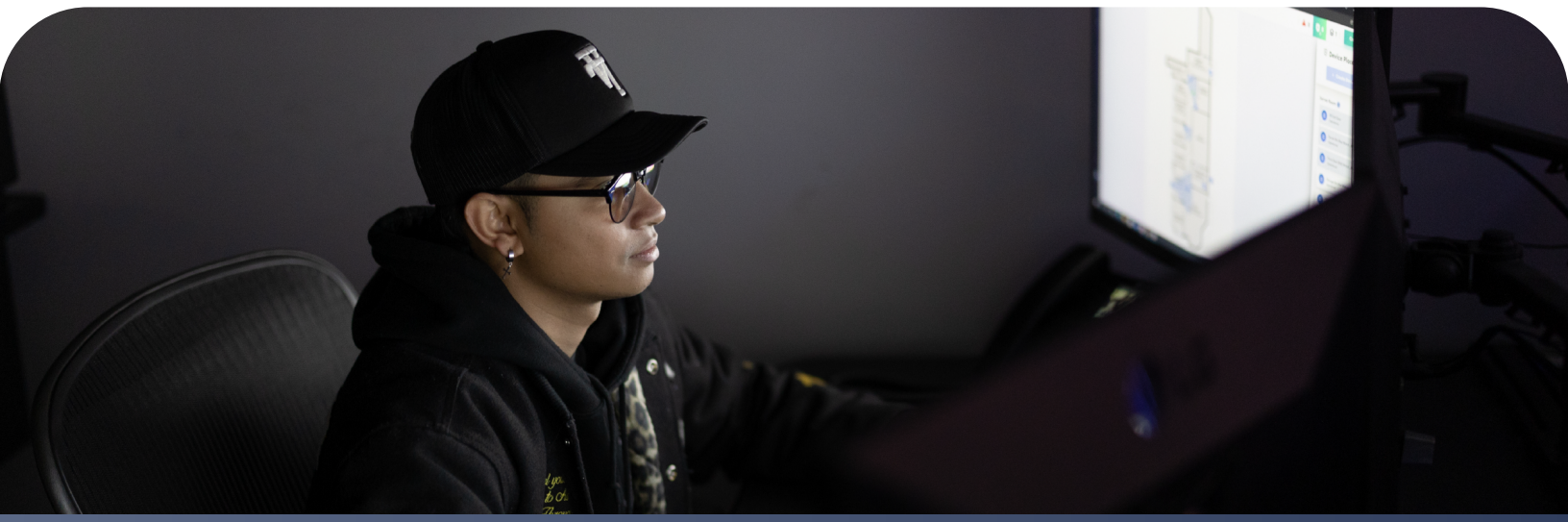
A hybrid GSOC model combines the strengths of both in-house and outsourced security operations, offering a balance of control, scalability, and cost-efficiency. This model is particularly useful for organizations that want to maintain control over critical assets and sensitive data, while also benefiting from the scalability, advanced technology, and 24/7 coverage provided by a third-party GSOCaaS provider. However, clear communication, defined roles, and strong integration are essential to ensuring the hybrid model operates smoothly and without security gaps.

Benefits of a hybrid model

- Cost efficiency can be achieved by outsourcing certain functions of a GSOC in an effort to decrease costs associated with staffing, technology, and more.
- Improved coverage ensures 24/7 incident response and monitoring for the organization.
- Expertise is readily available – whether in-house or external.
- This solution is easily scalable in either direction – when business needs change, reductions in external support can be done, while in growth, additional support might be leveraged.

Drawbacks of a hybrid model

- Added complexity around coordination and communication between the two locations might be a factor.
- Data segmentation might become an issue if the technology isn't seamlessly integrated.
- There might be a gap in coverage when certain duties of each aren't outlined.
- Integration of technology might become an issue if the external third-party uses different technology than the in-house GSOC.



TO BUILD OR NOT TO BUILD? DECIDING WHICH OPTION IS BEST FOR YOUR SECURITY PROGRAM

While both in-house and outsourced GSOCs have their advantages and disadvantages, approaching the decision to choose one over the other comes down to several considerations: time, cost, risk, and scalability.

Time

Ask any security consultant or operations leader and they will tell you that the amount of time it takes to set up a security program, establish a risk assessment and profile for the organization (which expands with each location covered), and hire/train personnel is lengthy. It takes a lot of time to execute a security strategy that involves standing up an in-house GSOC and the time should be factored into any decision being made.

Cost

The initial set-up of an in-house GSOC requires substantial upfront investment in technology, infrastructure, and personnel, not to mention the opportunity costs of security managers' time and focus. Ongoing costs, such as training, upgrades and new technology, new locations, and more can add up as the organization's needs change (and the company grows). And when you're working to answer to a c-suite or board of directors, the cost conversation might be THE most important one.

Risk

Security leaders are tasked with assessing the risks to the organization – both internal and external – which can dictate whether an in-house GSOC makes the most sense. Using an external GSOC involves sharing sensitive information with a third party, which might raise concerns about data security and confidentiality. It might also be risky for the organization to give up complete control over how incidents are managed and reported.

Scalability

As an organization grows, so does its footprint, which requires additional security investments and expansion of the program. In-house GSOCs might require additional investments in personnel and technology, while a vGSOC might be better able to absorb the burden of growth as the organization grows.

THE DECISION-MAKING PROCESS: QUESTIONS TO CONSIDER

When considering whether to establish an in-house GSOC or opt for a GSOCaaS, there are several questions that an organization should ask to assess operational needs, costs, technology requirements, and the overall security strategy.

OPERATIONAL AND STRATEGIC NEEDS

What are the primary security goals of our organization?	Define what success looks like for your GSOC, including key functions like threat detection, incident response, and compliance monitoring.
What specific risks or threats do we need to address?	Understand your organization's unique threat landscape–whether it's physical security risks, cybersecurity threats, or both–and determine how these threats should be monitored.
Do we need 24/7 monitoring, or is part-time coverage sufficient?	Assess whether continuous monitoring is critical for your operations or if certain times (e.g., business hours) require more focused security attention.
How critical is direct control over security operations for our organization?	Evaluate whether you want to retain complete control over the security strategy and operations (which favors an in-house GSOC) or if outsourcing certain tasks is acceptable.

COST AND BUDGET CONSIDERATIONS

What are the upfront costs of building and maintaining an in-house GSOC?	Factor in infrastructure, technology, personnel, training, and ongoing maintenance costs for building a full GSOC internally.
How do the long-term costs of an in-house GSOC compare to GSOCaaS?	Compare the capital and operational expenses of an in-house model versus the recurring costs of subscribing to a GSOCaaS provider.
Is our organization ready for the capital expenditure required for an in-house GSOC?	Determine whether your organization has the financial resources and willingness to invest in the infrastructure, technology, and staffing for an in-house GSOC.
Can we scale up an in-house GSOC cost-effectively, or would scaling be more feasible with a GSOCaaS?	Understand how each model will handle growth or expansion in terms of budget, personnel, and equipment.

STAFFING AND EXPERTISE

Do we have the in-house expertise to manage and operate a GSOC effectively?	Consider whether you have or can hire staff with the skills necessary to operate and manage a GSOC, including monitoring, incident response, and technology management.
Can we recruit and retain skilled security personnel for a 24/7 operation?	Assess the availability of qualified personnel for an in-house GSOC and the cost associated with recruiting, training, and retaining them.
What level of training is needed for our in-house team to stay current with evolving threats?	Consider how much training will be required to keep in-house staff updated on the latest security threats and technology.
Can the GSOCaaS provider offer better expertise and technology than we could develop internally?	Evaluate whether external providers offer specialized expertise, certifications, or cutting-edge technology that would be difficult to replicate in-house.

TECHNOLOGY AND INFRASTRUCTURE

What technology (software, hardware, tools) do we need to build and operate an in-house GSOC?	Identify the core technology components required for an in-house GSOC, such as video surveillance systems, alarm systems, incident management platforms, and real-time threat intelligence tools.
How scalable is the infrastructure for an in-house GSOC compared to GSOCaaS?	Evaluate whether your infrastructure can scale easily with new security needs or site locations, and how GSOCaaS providers handle scalability.
Do we want to manage and maintain our security systems, or would it be more efficient to rely on an external provider?	Determine whether you want full control over your systems and technology or if you prefer to offload maintenance and management responsibilities to a third-party provider.
Is our existing security technology compatible with a third-party provider's systems?	Ensure that your current systems (e.g., access control, video surveillance) can integrate with a GSOCaaS provider's technology platforms if you choose to outsource.

DATA PRIVACY AND COMPLIANCE

Do we have regulatory or compliance requirements that necessitate keeping data in-house?	Assess whether laws like GDPR, HIPAA, or PCI-DSS require sensitive data to be managed internally, which could influence your decision toward an in-house GSOC.
What data security measures does a GSOCaaS provider offer, and do they meet our compliance standards?	Review how the third-party provider manages sensitive data, including storage, encryption, and access controls, to ensure compliance with relevant regulations.
What are the potential risks of sharing sensitive data with an external GSOCaaS provider?	Consider the risk of data breaches or unauthorized access when using a third-party service and what safeguards are in place to mitigate those risks.

RESPONSE TIMES AND INCIDENT MANAGEMENT

How quickly do we need to detect and respond to incidents?	Determine the required response times for your security operations and whether a third-party provider can meet those expectations.
Will the GSOCaaS provider be able to respond as effectively as an in-house team during critical incidents?	Evaluate the incident response capabilities of a GSOCaaS provider, especially in high-risk or high-stakes scenarios where immediate action is required.
How will incident escalation and communication work between our internal teams?	Clarify the incident escalation protocols between the in-house team and the outsourced provider to ensure smooth communication and hand-offs during emergencies.

CUSTOMIZATION AND CONTROL

How much customization and flexibility do we need in our security operations?	Identify the degree to which you need a tailored security solution. In-house GSOCs offer greater control over customization, while GSOCaaS providers may have more standardized services.
Can an outsourced GSOC provider customize their service offerings to meet our specific needs?	Ask about the flexibility of the GSOCaaS provider to customize monitoring protocols, reporting, and alert thresholds based on your organization's specific requirements.
Do we need the ability to quickly modify security protocols or change monitoring priorities?	Consider how agile you need to be in changing security strategies or protocols, and whether an external provider can adapt as quickly as an in-house GSOC.

SCALABILITY AND FLEXIBILITY

How rapidly can we scale an in-house GSOC as our business grows or our needs change?	Evaluate the time and costs associated with scaling up an in-house GSOC in response to company growth, new threats, or geographic expansion.
Does the GSOCaaS provider offer scalable services, and what are the costs of scaling?	Ask about the provider's ability to scale services, the associated costs, and any limits to how quickly they can scale in response to increased demand.

INTEGRATION WITH EXISTING SYSTEMS

Can an in-house GSOC seamlessly integrate with our existing security technologies?	Determine how well an in-house GSOC would integrate with your current access control, video surveillance, alarm systems, and cybersecurity infrastructure.
How easily can a GSOCaaS provider integrate with our current security systems?	Ask potential GSOCaaS providers about their ability to integrate with your existing systems and whether they support your current technology stack.
Will an outsourced GSOC be able to integrate with our internal communication and escalation channels?	Ensure that an outsourced GSOC can align with your existing communication platforms and protocols for smooth coordination during incidents.

LONG-TERM STRATEGY

What is the long-term security vision for our organization, and how does the GSOC model fit into it?	Consider whether your long-term strategy aligns better with the control and customization of an in-house GSOC or the scalability and expertise of GSOCaaS.
Can we commit to the ongoing investment and evolution of an in-house GSOC?	Assess whether you have the financial and operational bandwidth to continually invest in updating technology, training personnel, and expanding an in-house GSOC.
Does a GSOCaaS provider offer long-term stability, and are we comfortable with the potential for vendor lock-in?	Evaluate the long-term viability of a GSOCaaS provider and whether you could face challenges in switching providers or bringing operations in-house later.

HOW HIVEWATCH HELPS

HiveWatch offers various options to support GSOCs in achieving intelligent, efficient, and scalable security at any stage of their lifecycle.

HiveWatch provides solutions that serve organizations of all different sizes, industries, and stages of their security programs – from newly funded startups without a GSOC, to established Fortune 100 companies who are ready to take their program to the next level.

- The **HiveWatch® GSOC Operating System (OS)** integrates information, resources, access control systems, and camera solutions, enabling more streamlined communications between field resources and operators (through the Mobile App), and making it easier for GSOC operators to respond to and detect threats.
- The **HiveWatch® Command Center** is designed for security teams looking to improve operational management and enhance communication without device connectivity.
- HiveWatch also offers GSOCaaS with its state-of-the-art, **in-house GSOC** that uses the HiveWatch® GSOC OS and a trained team to oversee organizations with limited security resources.

Making the decision to build a GSOC or use an external GSOC provider depends on various factors such as the organization's size, budget, industry, regulatory requirements, and specific security needs. In the typical consultant's answer, what's best for your organization "depends" on taking a holistic approach to building your security program and being able to look ahead to see what it might look like in the future.

Request an initial consultation with one of our security specialists to get started and find out how HiveWatch can help your organization reach its physical security goals.

HiveWatch