SEC
SECURITY EXECUTIVE COUNCIL
A research and advisory firm

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

GSOC: Business Drivers and Service Scope

By the Security Executive Council

During the COVID-19 pandemic, companies with existing Security Operations Centers and Global Security Operations Centers have been able to leverage their 24x7 SOC/GSOC capabilities to enable a more prepared and more resilient enterprise, and to add value like never before, as employee information call centers, contact tracing and tracking centers, global infection intelligence hubs, and more.

According to SEC subject matter expert George Campbell, "In the GSOC space, we have seen many examples of CSOs pushing the envelope on analytical tools for active global monitoring of health and safety risk and expanded outreach for security needs of exponentially larger numbers of remote workers. Artificial intelligence and digital transformation are on the cusp of providing a variety of analytical tools to empower our GSOCs to support a more holistic, smart, and business-centered service suite."

The heightened profile of SOCs/GSOCs is likely to continue to pique executive interest in these services well beyond the pandemic. If you don't already operate a SOC, now may be a good time to learn more and to consider whether one could add value in your organization.

The SEC has long researched successful GSOCs, developing benchmarks and best practices, and its Next Generation GSOC Group provides opportunities for leaders planning GSOC expansion and enhancement to receive collaborative feedback from peers.

George Campbell has helped to lead these efforts. Below he lays out some findings on scope and key business drivers that could be helpful as you study the potential for a SOC/GSOC or enhancing the services your existing operations center already provides.

A Few Key Business Drivers

1. **Process Criticality.** Achieving performance excellence in SOC/GSOC services clearly supports a primary mission of the security organization: assurance of safe and secure

workplaces. Security services are measured by timely and qualitative response to emergency and crisis events. The SOC is typically the qualifier and initiator of First Response and provides direction for initial and continuing reaction. Measurable capabilities in safe & secure workplace protection result in increased productivity, lower insurance cost, increased worker morale, and reduced incidence of injury and fatality.

2. **Proactive Risk Management**. Reactive risk management is assumed, and excellence is expected. But we know that events in this space may comprise a small part of the 24/7/365 available time of these operations. It is in the considerable balance of routine operational time where the hunt for increased scope and value may be directed. Current technology-based GSOC capabilities can, on their own, reliably identify, assess and facilitate response to security and business process risk. The deployment of off-the-shelf technology, residing on globally networked platforms with applied intelligence at this point of collection and analysis, can mitigate detected anomalies.

   Global competition and leading-edge practices can breed risky business processes. GSOC operations can directly tie into key points of process oversight (like links in the supply chain) and thereby provide situational awareness. So, we may claim that when a GSOC (or any security service) enables the business to do what would otherwise be too risky or non-competitive, it has delivered measurable value.

   Proactive risk management seeks to capitalize on learning, anticipate, and reach with purpose into risky places and processes.

3. **Business Value Proposition**. Value is in the eye of the beholder. We may find value when:
   - the cost of a secure business process is less than the consequences of risk;
   - the cost is additive but those at risk feel measurably safer and more productive;
   - an incremental increase in asset protection is achieved at reduced cost to the customer;
   - a customer's expectation or service level agreement (SLA) is consistently exceeded in evaluative factors related to value received;
   - a security activity is peer-reviewed or benchmarked against available standards or best practices and exceeds qualitative measures of performance.

4. **Highly Responsive Customer Service**. The GSOC may be the only direct contact the customer has with the security organization. When we can define a level of performance results that deliver a measurable benefit (like less risk or faster, better response), we can both improve performance and positively influence the perception of value by key constituencies or stakeholders. To that end, there are multiple points of potential convergence between a GSOC and the corporate security service population.

These four business drivers form the quadrants of qualitative measurement that need to be factored into a GSOC performance management scheme.

Levels of Service Scope, Capability & Competence

The GSOC can offer a broad array of escalating services. The following approach to leveling is merely to suggest an incremental approach to an eventual GSOC architecture.

Level I - Routine GSOC Operations. This is basic mission management and service delivery. Best practices here will likely focus on two areas:

1. Deliver increased value and cost-efficiency/effectiveness in operations management by implementing initiatives and practices that
    a. measurably drive down bottom line cost of security to the business, and
    b. identify and deliver an expanded scope of services that measurably reduce risk or aid in task performance by employees and in business processes.

2. Leverage the capabilities of the network and technology suite for timely and effective response to emergency and routine calls for service.

Level II - Anomaly Monitoring & Event Escalation

1. Threat assessment targeting known or suspected sources of risk to personnel, secure operations, and business resilience. Exploit monitoring capabilities to pre-select and identify individuals or conditions known to present or characterize threats. Maintain sensory oversight of spaces for changes contributing to increased risk to people or process.

2. Predictive analytics and data mining to prospectively target, identify and exploit patterns that may represent leading indicators of risk and provide early alerts for decision making.

3. Collate, aggregate and provide feeds of data from available sources for crisis monitoring and status reporting.

4. Support ongoing incident investigation and after-action-review (AAR) processes.

Level III - Threat Analysis and Event Management

1. Provide dedicated online and off-line support to threat event escalation and related response activities.

2. Provide ongoing support to dedicated command, control and communications in incident management.

At what level of service and scope would a GSOC provide the best answer to business drivers in your organization? Do you have a roadmap laid out to define the way forward?

For more information on assessing or developing value through a GSOC, visit our GSOC Best Practices page.

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
Website: https://www.securityexecutivecouncil.com/

