SEC
SECURITY EXECUTIVE COUNCIL
A research and advisory firm

Program Best Practices > GSOC >

Defining Best Practices in Global Security Operations Centers

Initial Output from the SEC GSOC Best Practices Working Group

Created by George Campbell, Security Executive Council Emeritus Faculty and Co-Lead GSOC Best Practices Working Group

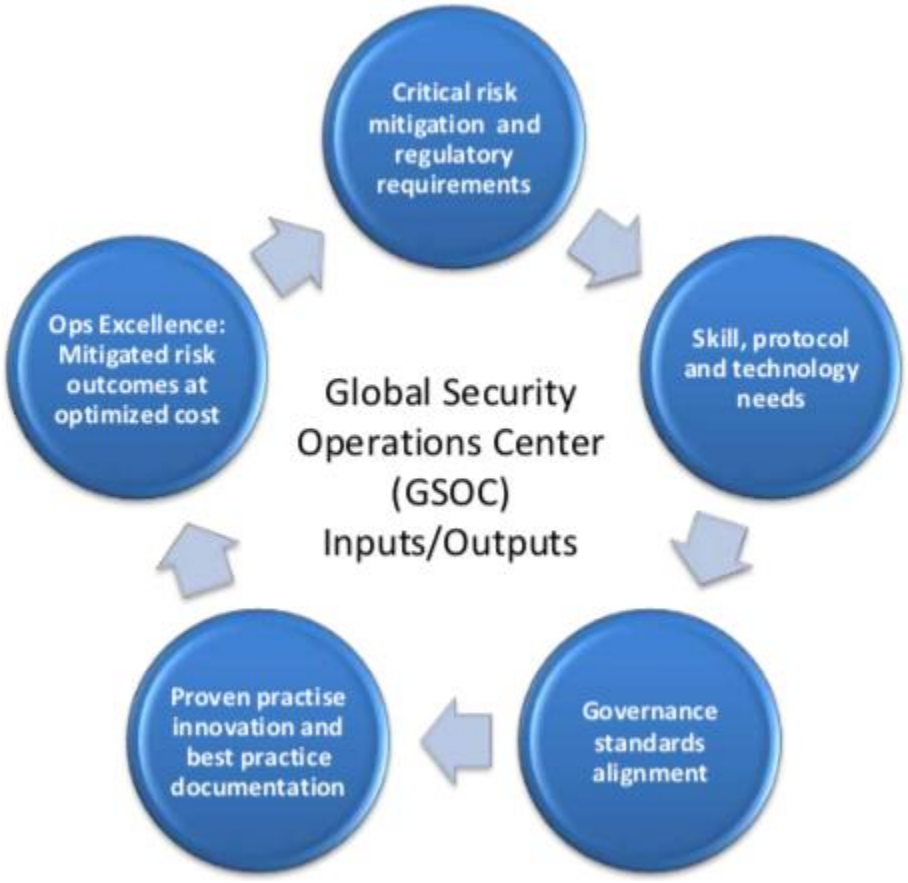
Introduction. Forty plus multinational brands answered a call-to-action in 2014 for informing good and best practices for global all-hazards risk mitigation. The majority of benchmark respondents indicated that their people, process and technology security operations methodologies would continue to evolve. Most expressed interest in forming an ongoing best practice effort to document proven protocols for people, asset and brand protection.

Objective. The Security Executive Council (SEC) GSOC Best Practices Working Group has come together to identify a body of best practices for security operations centers (SOC/GSOC) and to delineate their value proposition. Placing this endeavor within the analytical framework of operational excellence provides an industry-accepted approach and validity to the potential results. If members of this group can establish they have achieved a defined, peer-based level of performance in this suite of security services, it will enable them to demonstrate measurable value to their companies.

A Unique Perspective – When built on a foundation of enterprise risk assessment, a global security operations center can have the single most comprehensive and time-sensitive view of risk in the corporate governance infrastructure.

Process. This SEC program incorporates extensive benchmarking of corporate security organizations to gather baseline data on participating company and security department demographics. These results also provide an extensive profile of GSOC customers, technical infrastructure, service offerings and approaches to mission delivery. Companion polling seeks to do a deeper dive into participant's experience with technology applications, applicable performance measures and sharable best practices. A combination of virtual and on-site meetings engages members in more focused probing of GSOC needs and opportunities.

This initial report leverages this body of member experience and examines the range of elements that may serve to define operational excellence and best practices in these critical security services. We intend to periodically update these benchmark findings for currency and relevance.



What is Operational Excellence? "Operational Excellence is the execution of the business strategy more consistently and reliably than the competition. It is evidenced by results. Given two companies with the same strategy, the Operationally Excellent companies will have lower operational risk, lower operating costs, and increased revenues relative to its competitors, which create value for customers and

shareholders."[1] At its core, it is about achieving stakeholder value by delivering superior performance and results.

Best Practice Defined. "A best practice is a method or technique that has consistently shown results superior to those achieved with other means, and that is used as a benchmark… Best practices are used to maintain quality as an alternative to mandatory legislated standards and can be based on self-assessment or benchmarking. Best practice is a feature of accredited management standards such as ISO 9000 and ISO 14001."[2]

Standards. The work performed by security operations centers is central to the delivery of corporate security services, and a variety of organizations have established performance standards that may be applicable to measuring GSOC excellence and best practices. Having said that, a hunt for SOC standards and best practices primarily finds sources with exclusive focus on IT, cyber defense and commercial and proprietary central stations. Several of these are seen in the table below.

UL Standard 827 & 2050	Factory Mutual 3011	DHS Interagency Security Committee Standards & Best Practices
ISO 22301 Business Continuity Standard and ISO 28000 Supply Chain Security	Central Station Alarm Association (CSAA)	National Fire Protection Association Standard 72 (NFPA)
National Industrial Security Program Operating Manual (NIOSPOM)	ASIS/SHRM Workplace Violence Prevention & Intervention Standard	Selected DHS critical infrastructure Security standards
ANSI / Department of Homeland Security Standardization Initiative	U.S. Fire Administration / FEMA Communication Center Manual	Commission on Accreditation for Law Enforcement Agencies (CALEA)
Association of Public Safety Communication Officials (APCO)	National Emergency Number Association (NENA) and others.	ISO 17799 and 27000 series associated with monitoring and response to cyber risk management.

We are early in the evolution of the broadly mandated and enabled corporate security GSOC, so there are few, if any, established quality standards specific to these services.

Proof of superior results. Where a security practice can be shown to deliver consistently superior results to an alternative process that has been applied and tested by others, it could be advertised as having achieved a level of excellence. The key is in the ability to measure the "superior result," and that requires detailed task and process analyses that are consistent elements in virtually all business excellence disciplines. Demonstrating superior results requires performance metrics to establish reliability and validity.

[1] http://www.wilsonperumal.com/blog/a-better-definition-of-operational-excellence/

[2] https://www.eschaniel.com/bestpractices

A superior result in a security operations center may be demonstrated as:

- Centralization of diverse threat monitoring applications that reduces human overhead and empowers a more aggregated view of risk
- Faster cycle time that measurably benefits the customer or improves the process outcome
- Lower cost of continuing expense in the form of reduced occupancy and insurance cost or elimination of the need for staff-based processes, for instance
- The measurable reduction of previously established levels of targeted threat and risk over an extended period
- Increased output and productivity at same or reduced cost
- Increased awareness across multiple security-related applications

Context. We seek to define a suite of GSOC services that can drive and support exceptional performance across the broadest possible range of risk management and business objectives. We focus on the GSOC because the criticality of its mission defines and underscores the absolute need for operational excellence in service content and delivery. Flawless competence is expected.

The Initial Challenge: Defining Excellence in a Diverse Operational & Resource Environment. A key conclusion from our benchmarking was that each industry sector applies its own unique operational and resource requirements to the overall security mission, and these heavily influence the GSOC suite of services. While there are some common elements, there is no uniform corporate security model to structure the complete fit and function of a GSOC. To our collective benefit, this diversity likely helps us define a broader scope of service requirements and related capabilities.

Here are some of the areas in which our sampled population showed marked diversity:

1. Diversity of industry risk and business drivers that frame the corporate security program's mission.
2. Variations in the perception of immediacy of risk requiring a broader and deeper scope of security services.
3. Presence of a deeper regulatory environment with related monitoring and dispatch requirements.[3]
4. Diversity of Security's staff sourcing and financial models including proprietary, outsourced or hybrid.
5. Diversity of limited vs. broader notions of GSOC mission and related technology suite.
6. Range of response mission- local, regional, national or global.
7. Dependencies with IT that drive a more integrated relationship with information security requirements.

[3] For example, the DoD NISPOM requirements for classified area alarm response and clearance.

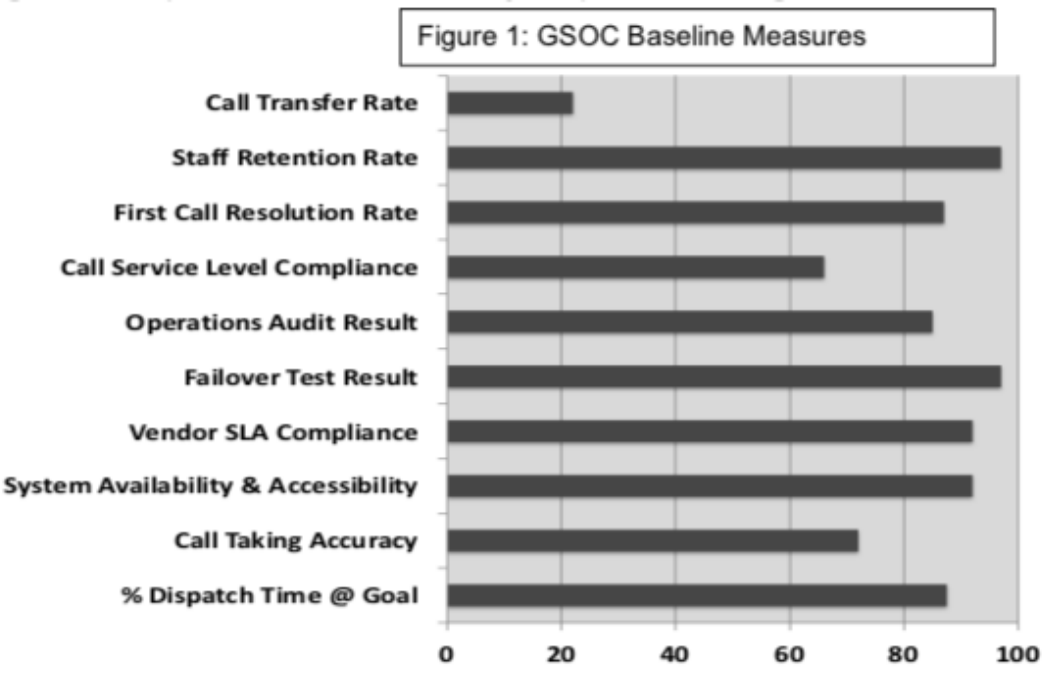
8. Dependencies with critical business processes such as that found in retail and financial services.

To accommodate this diversity, consideration of best practices and notions of service excellence will need to provide a selectable framework so that users can approach an evaluation of options. Fortunately, the options are growing almost exponentially with the speed and global reach of IT networks accompanied by the expanding intelligence and open architecture of security technology.

What Factors Drive Operational Excellence in GSOC Services?

When we step back and focus on what constitutes excellence in the basic processes at work in a GSOC, we have to consider the experience of similar corporate functions, since they establish an accepted baseline. The most prevalent are customer call centers, which have a well-established body of performance measures that may be appropriate for best practice targeting. The following chart displays a variety of factors that are measured along with a few that are more directed to security management.

In this example, multiple proprietary operator/dispatchers are posted on three shifts and receive heavy call volumes from North America and Europe. Call management criteria—timeliness, accuracy and quality—are emphasized.



- Call service level compliance relates to the overall SOC goal for customer responsiveness.

- Percentage dispatch time at goal: Risk assessment and analysis has resulted in a 2-minute goal for all critical calls and 3 minutes for non-critical. The performance objective is a running 90% average per reporting period. Using a more established call center performance measure, we would categorize this as average handle time.
- Call taking accuracy is measured by Shift Supervisors using direct observation, log review, and periodic incident post mortem review. Communication skills and operator knowledge for customer responsiveness are key elements in this assessment.
- First call resolution rates are transactions that are successfully completed within the initial call without a transfer to another individual.
- Transfer rates are calls that cannot be effectively handled by the initial call taker and must be transferred or escalated to another individual such as a supervisor or specifically designated desk. The performance issue here may be a training gap in the call-taker, inadequate customer direction for service, and the delay that accrues to the transfer.
- Operations audit is a scheduled or no-notice deep dive by a team into organizational performance. Its focus may be specific or more general.
- Staff retention (or turnover) rates are critical performance indicators in these operations. Where SOCs are outsourced, turnover has imposed degraded operator competence and service level performance.
- Failover testing is the essential resilience assessment and confirmation that is assigned to all critical business processes.
- System availability and accessibility is a measure of critical system and sub-system or process up-time reliability. While specific security head-end equipment is performing at 99.9%, other interdependent components or human factor processes may be less, resulting in service level degradation. This is a key performance contributor to call service level compliance.
- Vendor Service Level Agreement (SLA) compliance relates to quarterly rating of vendors who provide core services to the organization that directly impact SOCC efficiency, quality and service level. Examples are vendor-provided dispatcher/operators and equipment or infrastructure maintenance personnel.

You can't argue the critical importance of the call center experience for companies that rely upon these operations for their primary sales and customer connection. The focus is on time management and customer satisfaction: call hold and handle time, defined wait thresholds, and operator error rates.[4] These centers also emphasize operator

[4] These workload measures are very similar to those found in our benchmarking population. The difference is the often heavy impact on customer satisfaction for call volumes in corporate call centers versus the lower levels found in GSOCs.

staffing to workload ratios, or percentage of logged time in servicing calls versus idle time. This should be a placeholder for our purposes, since 24/7/365 security operations centers will likely have idle time that may be more productively applied.

Best Practice Group Experience with Metrics. The GSOC members' benchmarking feedback indicated relatively low application of performance metrics, with the highest responses being 28% for dispatch time at goal, staff training and turnover at 26%, critical system reliability at 24% and call service level compliance at 20%. Our 2014 follow-up survey of best practices provided some additional data primarily focused on workload measures including call volumes, response times, alarm rates and response to service requests. Supporting staff and security technology application performance review were also common areas of measurement. Given the GSOC's potential range of inputs and outputs that are capable of yielding risk mitigation and security management performance data, it should be clear that much more can be done to obtain value-based metrics from these operations.

A Few Key Business Drivers. While call management is clearly relevant, the corporate security mission frames a more risk-centered set of drivers for our operations centers. These four need to be taken into the consideration of operational excellence in GSOC services:

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 rightly 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. It can be demonstrated that 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. Performance excellence and best practices are absolutely critical here. 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. It is clear that 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. In this case, there are multiple qualitative perceptions:

   - Consider three perspectives on value:
     - We may find value when the cost of a secure business process is less than the consequences of risk;
     - or, the cost is additive but those at risk feel measurably safer and more productive;
     - or, 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.

   - When a security activity is peer-reviewed or benchmarked against available standards or best practices and exceeds qualitative measures of performance, value may be claimed. This is about a proven level of clearly superior service.

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 have the ability to not only improve performance but 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 need to be plotted on the scalable matrix of best practices.

These four business drivers form the quadrants of qualitative measurement that need to be factored into a GSOC performance management scheme. They provide the structure for more specific objectives and consideration of best practices such as those that are summarized below.

GSOC Objectives Directed to Operational Excellence & Application of Best Practices. There are multiple business and risk management objectives that may contribute directly to GSOC operational excellence and best practices. They target threat knowledge, alerts and containment; faster, better decision-making and response. Generally these enable more effective enterprise risk management. Eight examples are

briefly described below and cross-referenced to best practice targets in the accompanying table.

1. **Facilitate Risk Event Identification, Escalation; Response & Recovery.** The GSOC is the receptor, qualifier, communicator and key facilitator in real-time risk mitigation activities. It is uniquely positioned to intervene in the event continuum. Best practices here may be the difference in an employee's life or death and clearly provide for reduced consequences of risk events.

2. **Enable Enhanced First Responder & Investigative Operations.** A best practice that enables more timely and effective response to threats and risk-laden events provides a measurable return on investment. Redirecting idle time of GSOC personnel to analytical and forensic activities can deliver high value contributions for investigative case closure and reduced cycle times. GSOC connectivity to PDAs can expedite response and improve responder safety.

3. **Enhance Ability to Identify & Track Situations of Risk to Employees & Business Operations.** Remotely overseeing a variety of sources to build a correlated picture of emerging influences on safe and secure business operations enables qualitative anticipation and preparedness. Pre-selected inputs may be monitored for change in risk conditions or operational parameters. Predictive analytics and an increasing inventory of applications for actionable situational awareness provides significant opportunity for high return customer engagement and threat management.

4. **Provide Timely & Relevant Information for Enhanced Decision Making.** The GSOC presents a selectable collection of aural, visual and data inputs available to those engaged in the intervention of unfolding risk events. Qualitative response is best served by the right information, for the right people delivered early in the event.

5. **Monitor Critical Processes or Components for Defects & Anomalies.** The interruption of highly complex and critical business processes can easily cost millions of dollars and impact brand reputation. Critical process parameters can be measured and monitored for defects and anomalies so that timely intervention can restore process integrity. Reliability and benefits of deployed security technology may be more effectively monitored and utilized. Security element performance such as component off-line/down, IP Video and critical alarm point nuisance and false alarm rates must be monitored if the technology infrastructure is to be more effectively leveraged for cost benefit.

6. **Provide Enhanced 24/7 Support to Employees in Need.** The global network provides Security with a one-stop source of information delivery and a 24/7/365 point of contact for the company's personnel wherever they may be. Global situational analysis tools enable GSOC staff to "operate the radar" and anticipate

escalating risk conditions so that resident and transient employees may be alerted, re-directed or protected in place.

7. **Leverage Technology to Facilitate More Cost-Effective Security & Business Operations.** Companies sink significant investment into their network and security infrastructures with global connectivity and increasingly intelligent point of protection devices. Leveraging this backbone and deployed array of technology at a centralized point of collated intelligence presents multiple opportunities to deliver low-cost, high-value input to business units owning risky processes. Best practices may be found in security operations repurposing deployed technologies as more active parts of the protection strategy, by eliminating manned positions in favor of GSOC management of remote activities, by assessing key control points for regulatory compliance, leveraging video capabilities[5] and by active tracking of selected assets.

8. **Maximize GSOC Personnel Capabilities.** A 24/7 SOC with minimal staffing requires about 5 FTEs, and most of the operations in our benchmark group have 2-3 per shift for what may be up to 6000 hours or more of staff time per year. When you plot time applied to call management, dispatch and other essential tasks, there is some measure of idle time (particularly in non-core business hours) that may be explored for application to more productive and challenging activities that can expand the scope of services.

Benchmarking Results on GSOC Best Practices

Our benchmarking of 46 companies asked if members had "identified any best practices associated with their GSOC operations." The results were reported as follows:

Alarm management and efficiency improvement - 45%
Client risk mitigation confidence improvement - 40%
Dispatch optimization - 38%
Risk reporting and mitigation efficiencies - 36%
Return-on-investment business case - 30%
Core business partner P&L improvement - 26%
Quality assurance improvement - 17%
Casualty, injury and loss improvements - 6%

These results are really about capitalizing upon significant improvements in corporate infrastructure and security technology to leverage GSOC modernization. The GSOC's

[5] For example, video tours, facial recognition for threat assessment, remote access management, hazard communications, etc. The backbone is there and the on-board technology is available.

reach can more effectively touch employees and business process and thereby demonstrate to internal clients how these services visibly deliver value.

Exploring Some Best Practice Targets of Opportunity

The eight objectives briefly described above are incorporated in the following table and cross- referenced to fifteen activities that may provide results worthy of best practice characterization. These have been suggested by members or appear to lend themselves to further examination. There are many more that should be explored by this Group that fall within the following buckets of desired outcomes:

1. Services directly enable excellence in supported security operations (measurable contribution to standard of care). GSOC capabilities/processes enable customers to engage in activities that would otherwise be too risky.

2. The cost to customers and infrastructure footprint is measurably minimized and cycle times are managed to more aggressive timelines (response to events is faster and impact cost is minimized).

3. Proactive threat identification is enabled. Risk is proactively identified and mitigated (avoided & prevented). Incident investigations are more successfully closed due to enhanced tools & root cause identification (reduced cost and mitigated vulnerability).

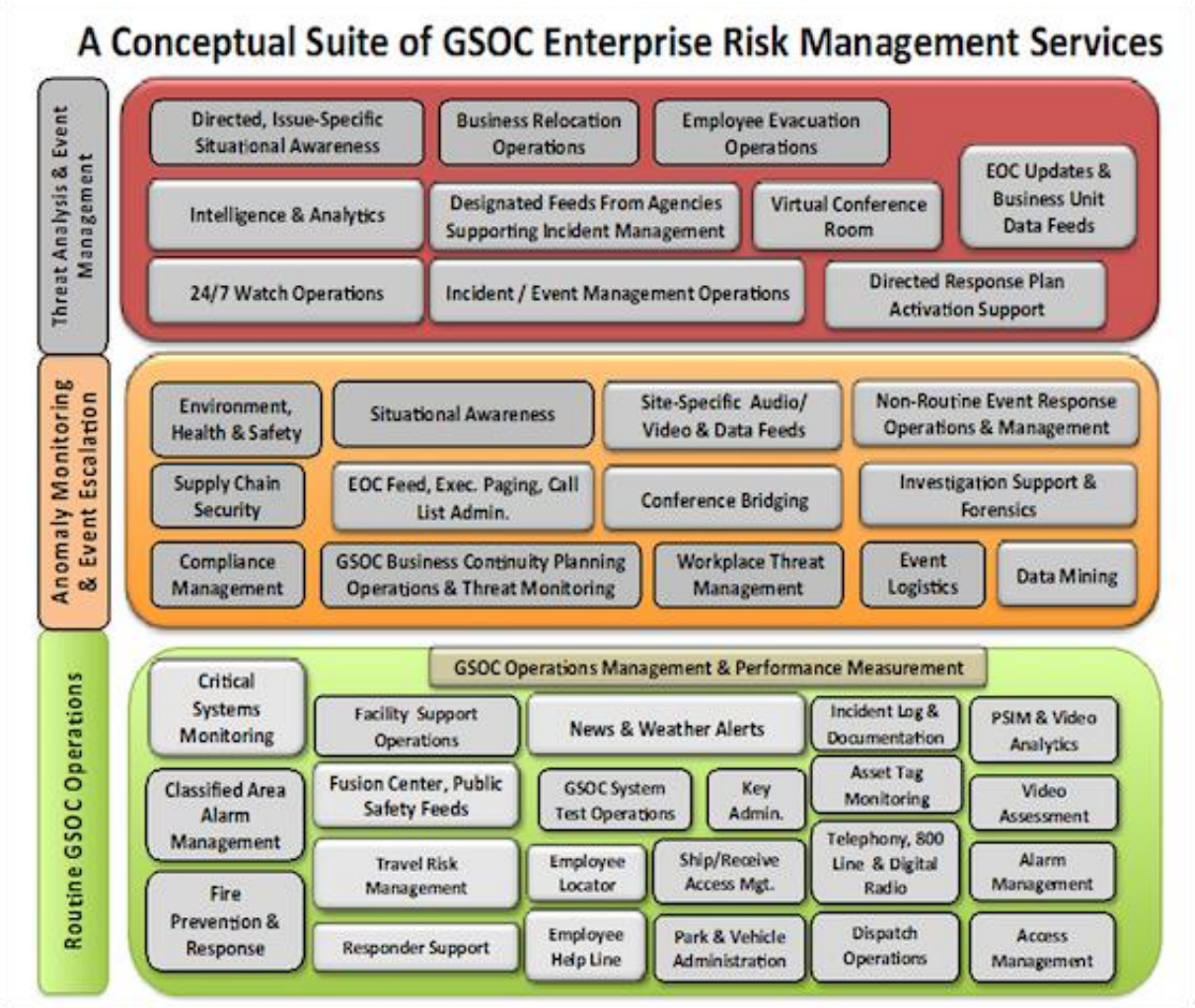
4. Measurable contribution to reduced risk to assets (confirmed by AAR) and measurable contribution to regulatory compliance (confirmed by test).

5. Deployment of proven technology can reduce costly reliance on personnel and minimize responder headcount while maximizing operator/dispatcher & supervisory knowledge of information essential to incident response & customer service.

Best Practice Targets of Opportunity	Security Process Objective Supportive of Excellence & Best Practices							
	Enable Enhanced First Responder & Investigative Operations	Provide Enhanced Ability to Identify & Track Situations of Risk to Employees & Business Operations	Provide Timely & Relevant Information for Enhanced Decision-Making	Facilitate Risk Event Identification, Escalation, Response & Recovery	Monitor Critical Process or Component for Defects & Anomalies	Provide Enhanced 24/7 Support to Employees in Need	Maximize GSOC Personnel Capabilities	Leverage Technology to Facilitate More Cost-Effective Security & Business Operations
Identify & eliminate root causes of nuisance & false alarms	✠	✠			✠		✠	✠
Monitor key control points for process or component defect identification		✠	✠	✠	✠	✠	✠	✠
Monitor key control points for validation of regulatory compliance	✠	✠	✠	✠	✠		✠	✠
Monitor pre-selected inputs for change in risk conditions or operational parameters	✠	✠	✠	✠	✠	✠	✠	✠
Provide for positive identification & tracking of individuals within designated areas	✠	✠	✠	✠	✠	✠	✠	✠
Monitor & track critical assets		✠	✠	✠	✠		✠	✠
Remotely activate selectable safeguards				✠	✠		✠	✠
Re-direct/automate responses to calls for service that do not require security response or intervention	✠	✠				✠	✠	✠
Enable GSOC to leverage security infrastructure for elimination of fixed & tour-based security officer posts	✠				✠		✠	✠
Monitor & communicate critical incident status for responsive risk intervention	✠	✠	✠		✠		✠	
Provide tools to Security Officers for safer and faster First Response	✠		✠				✠	✠
Provide tools to enable broader & more timely response to employee needs				✠		✠	✠	✠
Provide tools for enhanced forensic and Investigative support	✠		✠	✠			✠	
Engage After Action Review (AAR) processes for enhanced learning			✠				✠	
Eliminate tasks and reduce key cycle times	✠			✠	✠		✠	✠

Levels of Service Scope, Capability & Competence. The collective GSOC capability is graphically evident in the following figure that captures the broad array of services that might be structured in a full-service GSOC. Note the escalation scheme that represents increasing scope of service engagement as threat, situational assessment or event management demands unfold.

Conceptual Suite of GSOC Enterprise Risk Management Services



This representation is intended to convey an array of capabilities that are 1) in practice and proven, 2) off the shelf and available and 3) offer the potential to be brought together within a GSOC to provide a more robust and integrated suite of risk management and business enablement services. They may not be under the same roof but can be networked and inter-connected. The purpose of the display is to capture and encompass a view of possibilities. The following approach to leveling is merely to suggest an incremental or menu-driven 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-- Implementation of initiatives and practices that a) measurably drive down bottom line cost of security to the business, 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 on 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

Summary and Conclusion

When you honestly step back and document the services currently being delivered by corporate security operations centers, you come away with an impression that so much more can be done, especially when one considers the expanding capabilities of the technology applications that may be deployed as inputs and outputs. We no longer are limited by security applications that cannot talk to one another and consume far too

much bandwidth. The post-911 scope of security department reach into enterprise risk management has expanded, as have the implications of regulatory compliance. The scope of risk that may be monitored and alerted is more often global than a corporate campus of a few hundred acres. “Business resilience” and “situational awareness” have far more immediacy and likelihood of threat than in times past. These and other, more business-centered issues drive the potential for a broader and deeper inventory of services for GSOCs.

This is a work in progress. It is hoped that this brief discussion of operational excellence and best practices will contribute to the idea bank of those seeking to push the envelope on the potential benefits and measurable value of their Global Security Operations Centers.

To inquire about becoming a GSOC Working Group member please contact George Campbell at contact@secleader.com. Potential members are asked to take a survey around their GSOC operations as part of qualification. All members are required to sign a non-disclosure agreement. Members meet quarterly in person/online to share best practices and discuss issues.

Visit the Security Executive Council website for other 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 here: https://www.securityexecutivecouncil.com/