Chapter 3

Strategy 1: Consolidate CND Under One Organization

The first strategy is the most obvious but the least often followed: consolidate functions of CND under one organization whose sole mission is executing the CND mission. As discussed in Section 2.8, SOCs must be able to respond in a time scale relevant to the actions of the adversary. As a result, elements of CND must be tightly coupled. Bringing the CND mission into a single organization makes possible the following goals:

- Operations are synchronized among the elements of CND.
- Detection and response are executed efficiently, without sacrificing accuracy, effectiveness, or relevancy.
- Resources spent on CND can be maximized.
- Cyber SA and incident data is fed back into CND operations and tools in a closed loop.
- Consolidated, deconflicted SA is provided to the director of incident response and his/her management chain.

As a result, we recognize five indivisible, atomic elements of CND that should be under one command structure:

1. Real-time monitoring and triage (Tier 1)
2. Incident analysis, coordination, and response (Tier 2 and above)
3. Cyber intel collection and analysis
4. Sensor tuning and management and SOC infrastructure O&M
5. SOC tool engineering and deployment.

As we describe in Section 4.2, there are many different ways to bring these under one roof; that said, here is one typical organizational structure with functional responsibilities:

Unfortunately, contact with several dozen government and commercial SOCs reveals

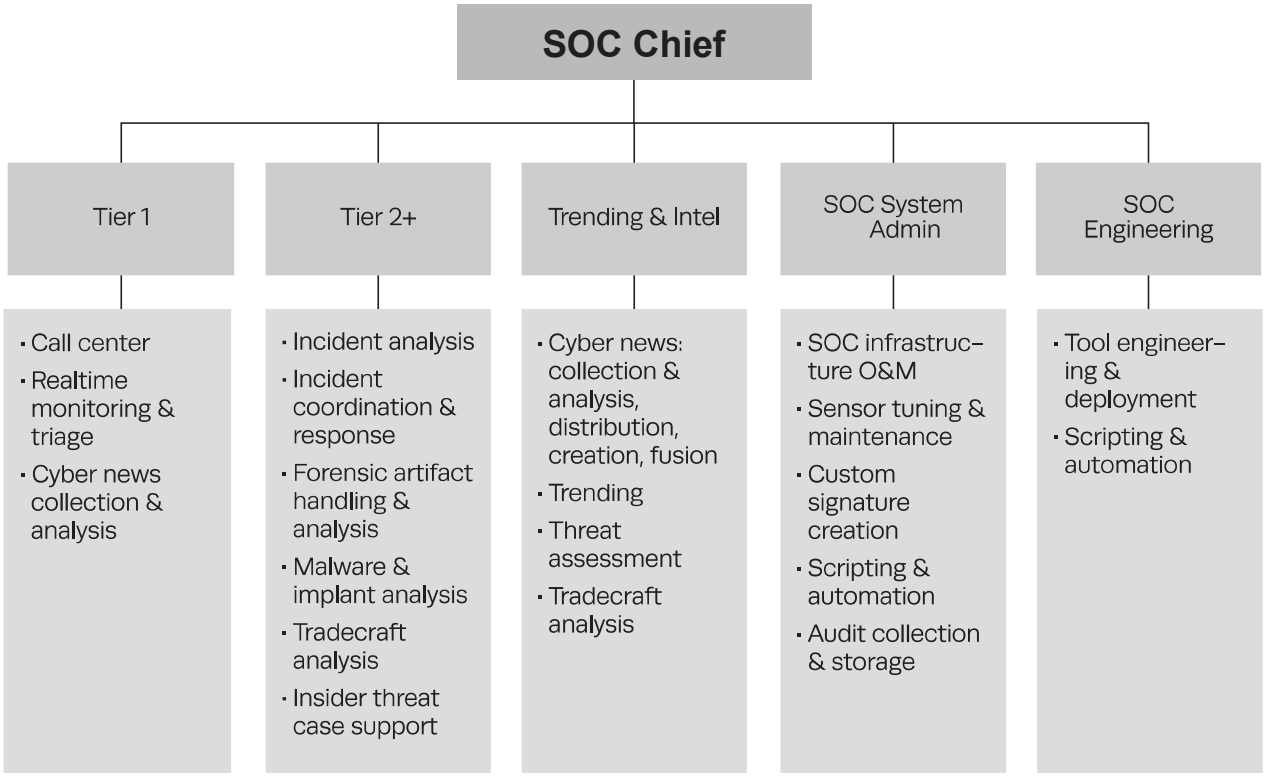

Figure 10. All Functions of CND in the SOC

that CND is frequently broken into multiple independent organizations. For instance, we might see Tier 1 IDS monitoring in a NOC, but Tier 2 incident response located in the office of the CIO.

When we divide up these core functions, we typically see one or more of the following: (1) depressed ops tempo, (2) broken or ineffective internal processes, (3) ineffective communication, (4) slow improvement in mission capability, and (5) animosity/distrust among different parties supporting CND. The result, of course, is a subtle yet profoundly negative impact on the defensive posture of the constituency. Consider the consequences of removing each of the core functions of the SOC:

- Real-time monitoring and triage or incident analysis, coordination, and response:
  - The incident escalation and follow-up process is disjointed and fragmented.
  - Incidents are slow to be followed up, and Tier 1 receives little feedback.

  - Quality control of what comes off the ops floor is hard to correct.
  - Career progression, and thus retention, of analysts is stunted.
  - In some scenarios, CND monitoring architecture and tool set are badly fractured, usually due to subtle differences in user requirements and decentralized resourcing.
- Cyber intel collection and analysts:
  - Nothing drives focus or improvement to SOC monitoring.
  - The SOC does not keep pace with the current threat environment.
  - The SOC is not viewed as resource for cyber SA by constituents.
  - Monitoring tools poorly leverage TTPs and indicators from available cyber intel sources and, thus, do not maintain parity with current threats and vulnerabilities.
- Sensor tuning and management:
  - SOC systems fall into disrepair.
  - Downtime of SOC systems is prolonged because responsible personnel are not accountable to SOC management.
  - Sensors lack current signatures.
  - Monitoring and incident results do not drive improvements or customizations to signature packages or SIEM content.
  - The SOC cannot maintain effective separation and protection from the rest of the constituency because its sysadmins and/or tools are thrown into the general pool of IT support.
  - Systems go down, and SOC personnel's hands are tied when applying tactical corrective actions or resolving larger system design issues.
- SOC tool engineering and deployment:
  - Intense distrust develops between SOC and engineering because of overlapping technical knowledge, but divided priorities and vision.
  - Engineering does not match operational priorities of SOC, both in terms of timely delivery of new capabilities and the needs of the operator.
  - The artificial division between ops and engineering causes confusion over responsibilities; the separate process restricts the SOC from leveraging tactical solutions.
  - Because the engineers are not embedded in ops, they do not fully understand the operators' needs, regardless of how robust and detailed the requirements specification.
  - Many SOC capabilities are best developed in a spiral fashion, providing immediate benefit to ops, and can change as the mission demands it; engineering life cycles where projects are "thrown over the fence" do not support this.

- Ambiguity over funding sources for SOC capabilities can make coordinating program funding, capital expenditures, and maintenance budgeting problematic.
- Fractured CND program budgeting can introduce an imbalance in money for tools, staff, and training.

Based on our discussion from Section 2.8, one can see how splitting up these functions of the SOC can have overwhelmingly negative consequences. SOCs that are fractured in this manner *might* achieve some success if three compensating measures are enacted:

1. The removed capability resides in a single organization; that is, if SOC infrastructure O&M is pulled out, it is assigned to another group whose sole responsibility is that job.
2. The managers of respective organizations (such as SOC ops and engineering) have an excellent working relationship, mutual respect, and constant communication with one another.
3. The organization that operates the capability pulled away from the SOC is still accountable to it through policy, procedures, and, perhaps, a contractual relationship.

Many SOC implementations separate tool engineering and some aspects of system administration from the SOC. This is especially problematic for reasons not recognized by many outside the CND practice. As we will discuss in Section 7.1, two prerequisites for being an effective analyst are a strong background in programming and in network/system administration. As a result, a SOC will naturally have the expertise necessary for SOC tool engineering and deployment in house. If they are not allowed to perform this function for process reasons, it breeds intense frustration and animosity between engineering and ops.

The CND ops tempo demands solution delivery in days or weeks, not months or years. One reason often cited for pulling engineering out of the SOC is to enforce CM. This is a fallacious argument, considering that robust CM processes can (and should) be implemented entirely within the SOC, along with code review and system hardening. Another argument made is that ops and engineering fall under separate lines of business. Because CND demands a unique mind-set and skill set, there is an argument to be made for excepting the SOC from this organizational construct. Also foreshadowing Section 7.1, CND personnel are not interchangeable with staff from other areas of IT, further bolstering this argument.

> **Do not break apart the five atomic SOC functions into disparate organizations; this will almost always work to the detriment of the CND mission.**

In fact, bringing these functions into one organization (the SOC) usually isn't enough—they also should be physically collocated. For instance, if engineering is located in Omaha and ops is located in Atlanta, collaboration and mutual support will likely suffer. Personnel supporting these capabilities should collaborate on a daily or weekly basis, a topic we return to in Section 4.2.

Chapter 4

Strategy 2: Achieve Balance Between Size and Agility

SOCs serve constituencies of almost every size, business function, and geographic distribution. The SOC's structure must correspond to that of its constituency, balancing three needs:

1. The need to have a cohesive team of CND specialists
2. The need to maintain logical, physical, or organizational proximity to the assets being monitored
3. The budgetary and authority limitations inherent in the constituency served.

In our second strategy, we seek to strike a balance among these competing needs. As a result we have three closely linked choices to make:

1. What SOC organizational model is the right fit
2. How to place SOC functions into sections with line managers and command structure
3. Where to physically locate members of the SOC, and how to coordinate their activities.

In order to realize this second SOC strategy, we will cover each of these choices in turn. In this section, we also lay out a number of concepts that we build upon in later sections.

4.1 Picking an Organizational Model

4.1.1 Drivers

Key drivers for determining which organizational model is best for the enterprise include:

- Size of constituency, in terms of users, IP addresses, and/or devices
- Frequency of incidents
- Constituency concerns for timeliness and accuracy of incident response.

Size of constituency is both a driver and a challenge. We need to build up a group of well-resourced CND professionals, but they need to maintain visibility out to the edge, operate within the decision cycle of the adversary, and maintain resourcing levels proportional to the constituency's IT budget. For instance, in larger constituencies, the desire to build a team that covers the whole enterprise may be overshadowed by the team's resulting inability to maintain mission relevancy and agility.

> **The further an analyst is separated from monitored assets—logically or physically—the less he/she is able to maintain context and sense of what is normal and abnormal behavior on those hosts and networks, and able, therefore, to respond in a relevant or timely manner.**

This fact is absolutely key to understanding how best to structure security operations in large enterprises. Without strong SA and operational agility, even world-class analysts and tools will be of little value. Luckily, we can use the organizational models discussed in Section 2.3.2 to help us resolve these competing needs.

A team of analysts can maintain familiarity with only so many assets and enclaves. Our goal here is to structure our analysis resources in a way that they can do that while still operating as one team, working toward a common set of objectives with a synchronized ops tempo. Most CND practitioners are used to working in a paradigm where they have direct access to raw data and can directly impact the assets they are monitoring. The critical issue is: how do we do this with larger and larger constituencies in a relevant, meaningful,

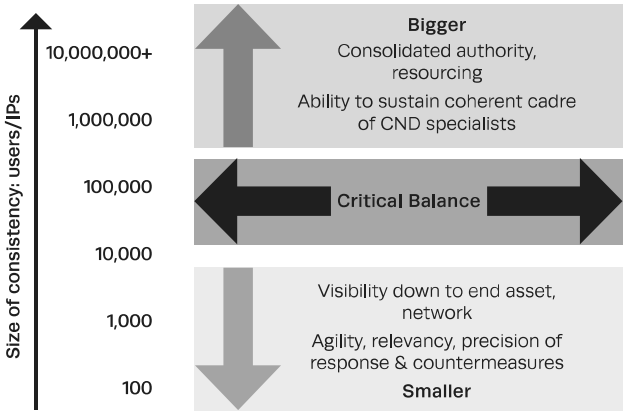

Figure 11. Rightsizing the Constituency

and productive fashion? As of the writing of this book, the answer to this question is not widely agreed upon.

4.1.2 Typical Scenarios

Using what we have discussed so far, we will create five SOC "templates" that we will use throughout the rest of the book, for illustrative and demonstrative purposes. They are shown in Table 4.

Table 4. SOC Templates

1. Virtual SOC	
Organizational Model	Internal Distributed SOC.
Constituency Size	1,000 users/IPs.
Visibility	None/poor. Limited, ad hoc postmortem log review.
Authority	No reactive, no proactive: authorities to prevent or respond to incidents are often vested in the SOC's parent organization.
Examples	SOCs serving small to medium-sized businesses, colleges, and local governments.
Remarks	Comprised of a decentralized pool of resources, this SOC most likely operates out of the office of the CIO, office of the CISO, or in the NOC (if one exists). Incidents do not occur often enough to necessitate constant monitoring.
2. Small SOC	
Organizational Model	Internal Centralized SOC.
Constituency Size	10,000 users/IPs.
Visibility	Limited to good. Instrumentation across major perimeter points, some hosts, and enclaves.
Authority	Shared reactive, shared proactive: the SOC is a voting member in decisions that drive preventative or responsive actions.
Examples	SOCs serving medium-sized businesses, educational institutions (such as a university), or government agencies.
Remarks	Resources for security operations are consolidated under one roof. However, the size of the SOC's budget is limited due to the size of the constituency. If part of a larger organization such as a commercial conglomerate or a large government department, the Small SOC may report to a Tiered or National SOC.

Table 4. SOC Templates

3. Large SOC	
Organizational Model	Internal Centralized SOC, with elements of Distributed SOC.
Constituency Size	50,000 users/IPs.
Visibility	Comprehensive. Instrumentation across most hosts and enclaves.
Authority	Full reactive, shared proactive: the SOC can enact tactical responsive actions on its own, and carries weight in recommending preventative measures.
Examples	SOCs serving Fortune 500 [58] and Global 2000 [59] companies and large government agencies.
Remarks	This SOC is large enough to support advanced services performed from a central location, but it is small enough to perform direct monitoring and response. In more heterogeneous or geographically dispersed constituencies, the Large Centralized SOC may leverage a "hybrid" arrangement with some staff at remote sites for some monitoring and response functions.
4. Tiered SOC	
Organizational Model	Internal Combined Distributed and Centralized, blended with Coordinating SOC.
Constituency Size	500,000 users/IPs.
Visibility	Varies. Some direct data feeds from end assets and enclaves; most data goes to subordinate SOCs.
Authority	Full reactive, shared proactive: the SOC can enact tactical responsive actions on its own, including those that may impact subordinate SOCs, and carries weight in recommending preventative measures.
Examples	SOCs serving multinational conglomerates and large, multidisciplined government departments.
Remarks	Due to the size of the constituency, this SOC has multiple distinct SOCs. There is a central coordinating SOC with its own directly monitored assets and enclaves, most likely located at or near the constituency headquarters and the constituency Internet gateway. There are also multiple subordinate SOCs that reside within given business units or geographic regions, whose operations are synchronized by the central SOC.

Table 4. SOC Templates

5. National SOC	
Organizational Model	Coordinating SOC.
Constituency Size	50,000,000 users/IPs, represented by constituent SOCs.
Visibility	Limited but widespread. No or limited access to raw data *by design*; depends entirely on incident reporting from constituent SOCs; does not directly monitor constituency.
Authority	No reactive, no proactive: despite its powerful name, it is atypical that a national-level SOC can exert substantial authority over its constituents; usually it acts in an advisory role.
Examples	SOCs serving entire national governments or nations.
Remarks	This is a classic national-level SOC that supports dozens to thousands of SOCs within its borders, across governmental, corporate, and educational institutions. Either it does not perform direct monitoring, or, if it does, it provides tippers to its constituent SOCs for follow-up. We will sometimes refer to these organizations as "mega-SOCs." Constituent SOCs operating within the mega-SOC's constituency operate mostly autonomously, which sets this model apart from the Tiered model.

With the first three templates, the SOC is able to maintain direct contact with the constituency, due to its modest size. The last two templates must use sophisticated approaches to support SA to the edge while coordinating CND operations in constituencies of progressively larger sizes. In Section 4.3, we will examine strategies for achieving these goals.

4.2 Structuring the SOC

In this section, we take two of the SOC templates from Section 4.1 with potential capabilities from Section 2.4 to construct a few typical SOC organizational charts. This should give the readers some ideas on how to structure their own SOC to better support smooth operations, without getting into every permutation of what a SOC might look like.

Some strategies we use in structuring the SOC are as follows:

- Put analysts in roles where they function best, but have room to grow both their own capabilities and the SOC mission.
- Maintain separation of duties and eliminate single points of failure to the maximum extent possible.
- Synchronize elements of CND operations so all elements are working in concert toward the same goal, especially during a critical incident.

- Balance energy spent on "managing" with resources devoting to "doing."
- Support the SOC's intended range of capabilities.

4.2.1 Small SOC

Smaller SOCs, in the range of five to 20 people, often find a relatively simple approach to arranging their staff. This is because with few people, there is comparatively less diversification of roles and there are few positions that don't involve full-time analyst work. A classic Small SOC will include two or three sections:

1. Tier 1. Includes analysts who perform routine duties such as watching IDS or SIEM consoles, collecting cyber news, and fielding phone calls from constituents
2. Tier 2. Performs all in-depth analysis on incidents passed to it by Tier 1 such as log and PCAP analysis, and coordinates response to incidents with constituents
3. System administration. Maintains SOC systems and sensors, which may include engineering and deployment of new capabilities.

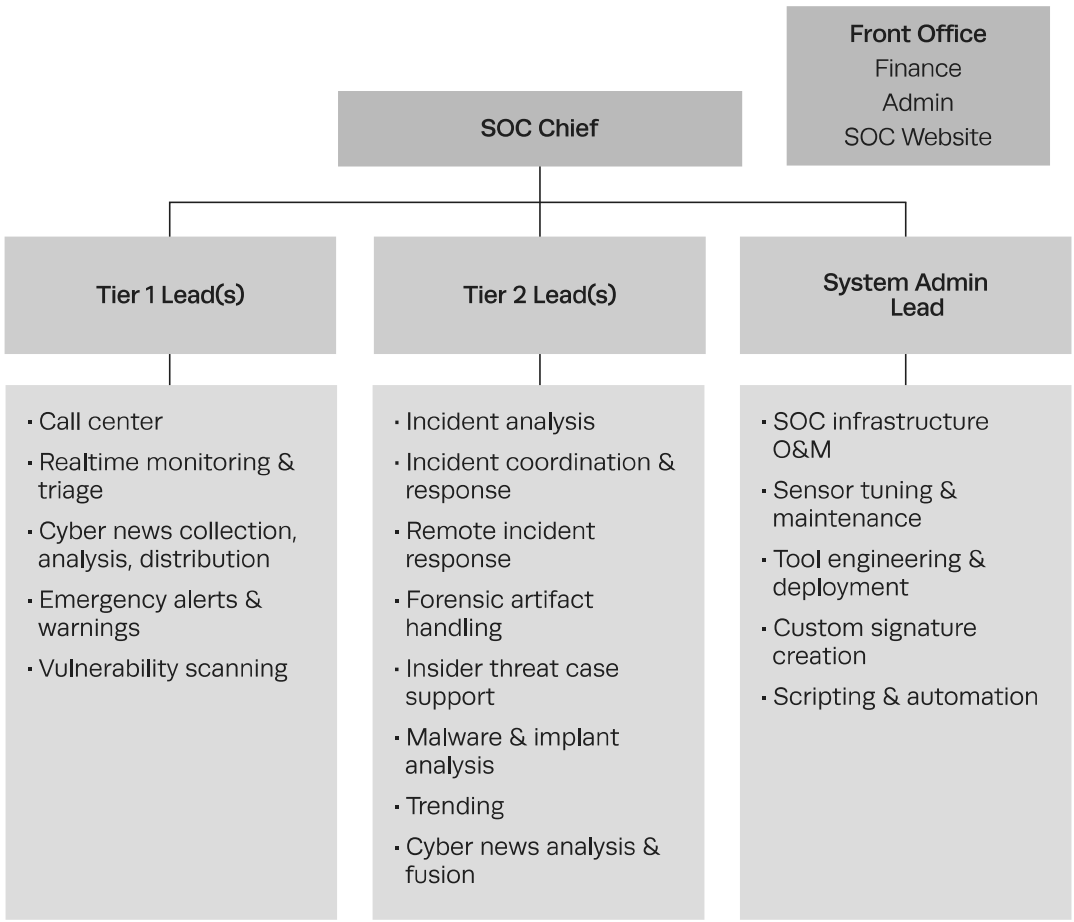

Figure 12. Small SOC

A SOC with this structure can serve a modestly sized constituency while separating "frontline" analysis from in-depth analysis and response. It is shown in Figure 12.

Some SOCs that enforce a tiered analysis structure do not necessarily split the tiers into separate sections. As a variation on the structure shown in Figure 12, we could combine all Tier 1 and Tier 2 duties into one large section with a single operations lead. In this arrangement, we would have two teams—operations and system administration. The other benefit of this setup is that the operations lead can also function as a deputy SOC lead.

Most SOCs of this size have a hard time pulling Tier 2 analysts away from the daily grind of processing incidents. In addition, there are many incidents that stem from activity that does not fall into the structured use cases handed to Tier 1. If this is not corrected, the SOC will likely suffer from stagnation and increased turnover. Foreshadowing Section 11, some SOCs have found it valuable to establish a separate "advanced capabilities" section, shown in Figure 13. This section's roles may vary, but usually incorporate functions such as "Tier 3+" incident analysis, process improvement, and advanced threat detection/

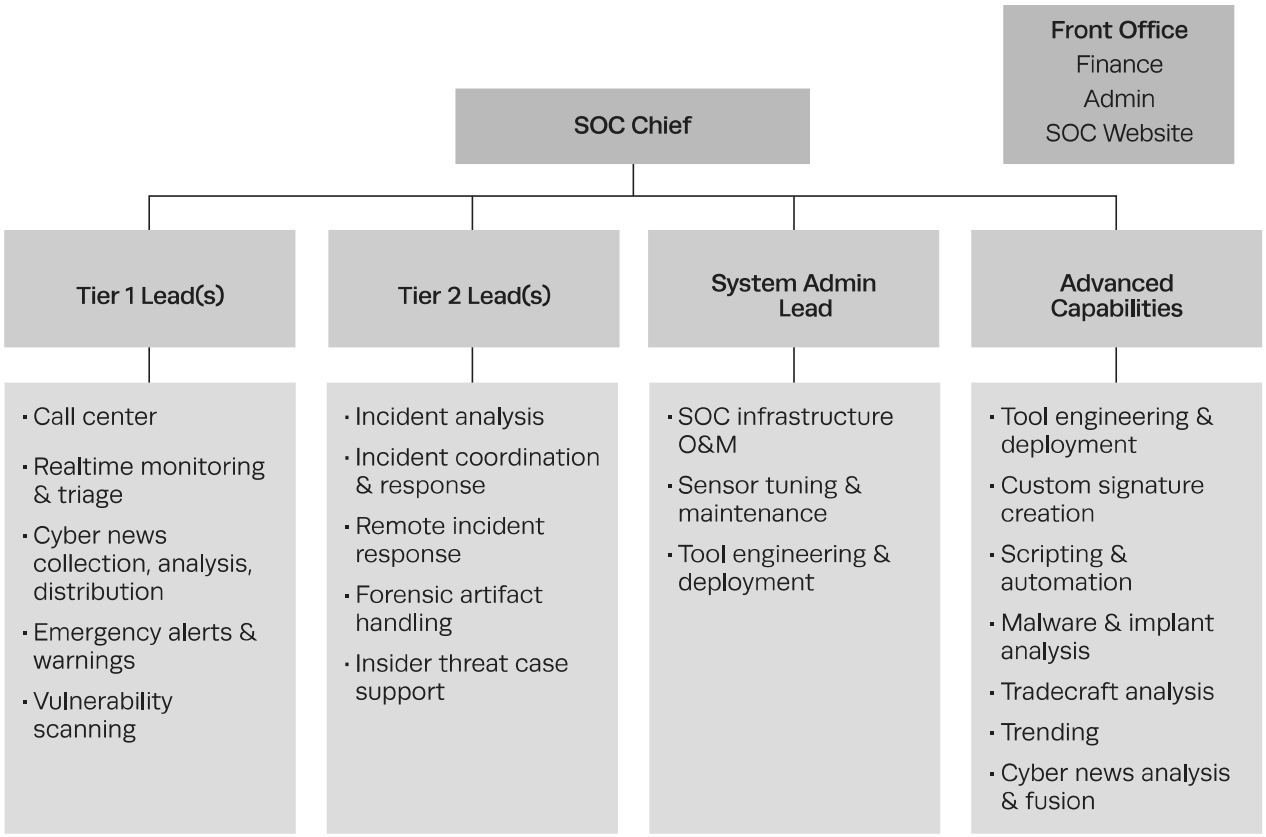

Figure 13. Alternative Arrangement for a Small SOC

response. The advanced capabilities team can be composed of staff (pulled from Tier 2) who demonstrate initiative and out-of-the-box thinking and can be rotated in and out of duties that place them in the "daily grind."

4.2.2 Large SOC

A large constituency can support a SOC with an advanced set of capabilities and full-fledged division of roles and responsibilities. Following our discussion of the Small SOC from the previous section, we have added the following features:

- Tier 1 focuses on fielding phone calls and catching real-time alerts and warnings in the SIEM or other sensor console(s), as a Small SOC does.
- Tier 2 focuses on running incidents to ground, regardless of whether it takes hours or months, as a Small SOC does.
- We have a new section that is responsible for ingesting trending cyber intel and analyzing network activity and adversary TTPs over months and years.
  - This job is often the most ambiguous because analysts are asked to look for open-ended, unstructured threats not currently on the radar.
  - This section is best staffed by self-starters and out-of-the-box thinkers (e.g., the "rock stars" mentioned in Section 7.1.1).
- We have added a host of new capabilities and created a new section that performs both routine network and vulnerability scanning and Blue/Red Teaming for constituency networks and systems.
- O&M and engineering of SOC systems have been divided into distinct groups under one shop, "Systems Life Cycle."
- Within the system administration shop, we will likely have one or two people devoted to each of the most important sensor packages and SIEM.
- The SOC is large enough that it usually has a dedicated deputy position, which may or may not be in addition to the role of ops lead.
- Some SOC chiefs will find it useful to designate middle-level managers in each functional area—analysis and response, scanning/assessment, and system life cycle.
- The "front office" may be added to take away administrative, budgeting, or CM burdens from SOC leads.
- Although not pictured, if the SOC chooses to integrate maintenance of perimeter protection devices such as firewalls, this can be integrated under the systems life cycle lead as a third team.

It may be possible to achieve the same separation of duties for these functional areas in the Small SOC model, but in doing so some staff may be "pigeonholed" into one role,

increasing the adverse impact of staff turnover. On the other hand, in the Large SOC, almost every core function is carried out by two or more people.

A potential organizational model for a Large SOC is depicted in Figure 14.

When a SOC gets this large, it is important to ensure there is effective cross-training and cross-pollination. Engineering must stay cognizant of the ops group's main challenges and "pain points" and how to quickly leverage 90 percent solutions. As a result, we can rotate personnel into engineering and development positions, as we did with the advanced capabilities team in the Small SOC model. Moreover, even though we may have multiple layers of management, operators in one section should not hesitate to work directly with any other part of the SOC.

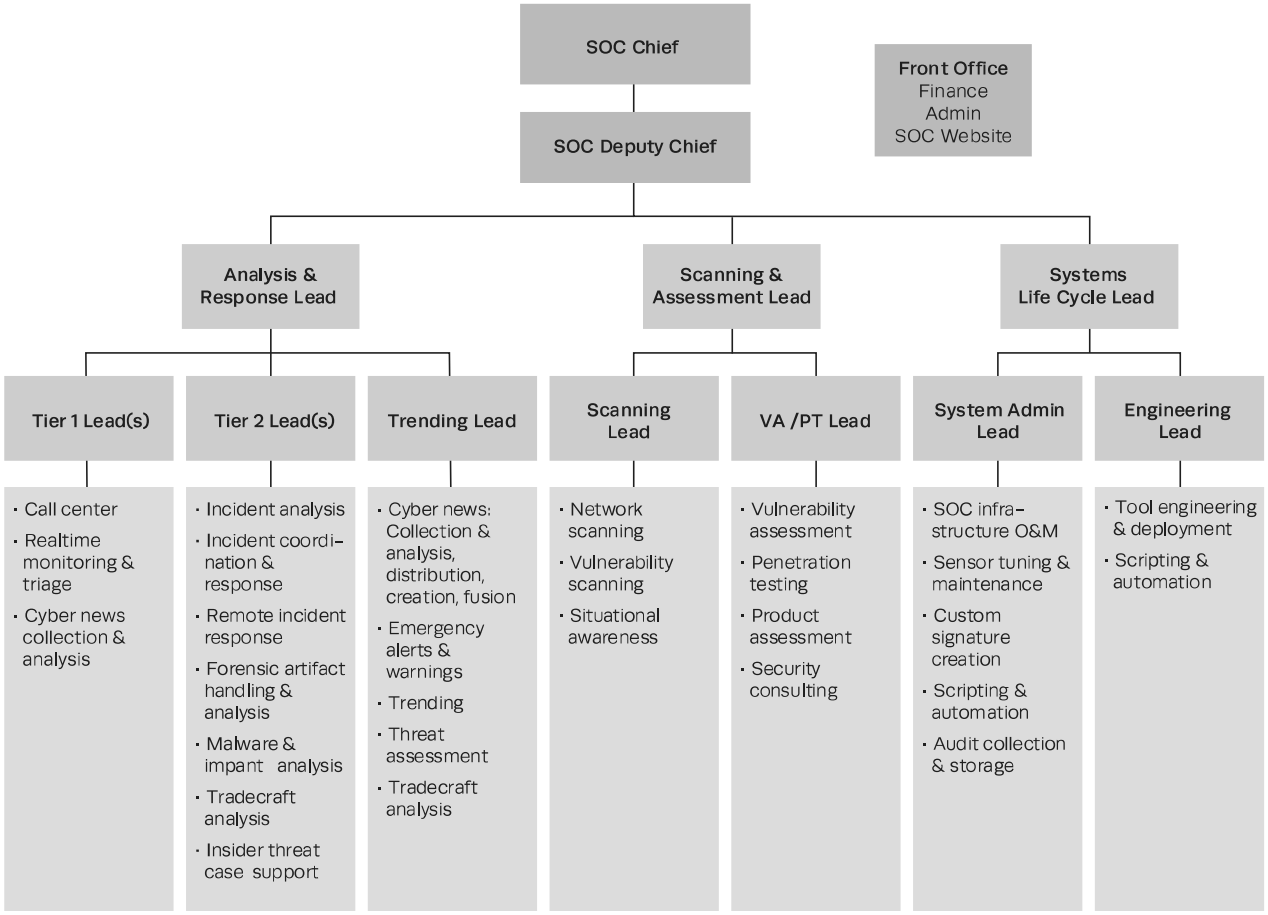

Figure 14. Example: Large SOC

4.3 Synchronizing CND Across Sites and Organizations

The SOC can find its physical location a great help or hindrance, depending on a number of factors. In Section 4.1.1, we talked about the balancing act between SOC size and the need to maintain closeness to the end asset and mission. This may compel us to place SOC personnel at multiple sites, as in distributed or tiered organizational models. In this section, we address the following intertwined issues:

- Where the SOC should be physically placed
- How to arrange SOC resources distributed among several locations
- How to split out duties between a central coordinating SOC and subordinate SOCs, all within one large organization
- Suggested roles and responsibilities for national coordinating SOCs.

In Section 3, we mentioned how the five atomic functions of the SOC should never be broken apart into separate organizations. While we should centralize CND organizationally, we may elect to distribute it physically. So we will offer an important corollary to the previous point:

> **Close physical proximity is instrumental in maintaining a synchronized ops tempo and priorities among parts of the SOC.**

While we have plenty of affordable real-time telecommunications capabilities—Voice Over Internet Protocol (VoIP), video teleconferencing, real-time chat, and desktop webcams—it is rare in an operations shop that we can use them to completely replace physical presence. When different sections of the SOC are moved apart—even to different rooms in the same building—collaboration can suffer. For this reason, we often mix elements of centralized and distributed organizational models, such as leveraging "forward deployed" analysts to reinforce Tiers 1 and 2 at the main SOC ops floor.

4.3.1 Goals and Drivers

Let's highlight some of the needs that we want to meet in making decisions on where to physically place SOC resources. (See Table 5.)

We will use these drivers in the following sections to examine some strategies for the SOC templates from Section 4.1.2.

Table 5. Considerations for SOC Placement

Goal	Discussion
Provide the SOC with a physical space that meets the SOC's mission needs	With the exception of virtual SOC, a physical operations floor will be needed. This usually entails an ops floor, back offices, and server room, all with secure access. This also means having ample bandwidth to constituency wide area networks (WANs), campuses, and data centers. Existing constituency office facilities and data centers may meet these needs better than other options.
Synchronize operations among the sections of the SOC	The atomic functions of CND must be brought into one organization, the SOC. It is also highly useful to bring them under one roof, supporting regular, healthy, and usually informal collaboration.
Maintain clear lines of separation between SOC functions and IT and cybersecurity functions	The SOC sits at the center of a political vortex—plenty of other people in the constituency believe that some element of CND is in their swim lane—fueling conflict with the SOC. Physical presence near these other entities gives the SOC an advantage by supporting close, ongoing contact that can help keep the SOC's interests and impact visible to other stakeholders.
Keep close contact with constituency leadership and other groups from Appendix B	The SOC must leverage support from parent organizations and coordinate with various groups in response to incidents, especially major ones. While this can be done virtually, it's best if they can be brought together physically.
Provide analysts better constituency mission and operations context, speeding analysis and response efforts	Being at a site where IT assets and users reside automatically gives the SOC many advantages—the ability to interact with constituents, perform touch labor on sensors, and execute on-site incident response.
Ensure the SOC's focus on the constituency is not biased to any one organizational or geographic region	Analysts will tend to automatically tune into what is going on at the site where they are located. This is both a blessing and a curse. If analysts are biased toward their site, what are they missing at the others? In more extreme cases such as large, heterogeneous enterprises, remote sites will perform their own security monitoring and incident response functions without coordinating with the SOC—in large part because they feel the SOC is out of touch with their mission.
Better position the SOC for staff hours that mirror when the constituency is open for business	The SOC's business hours should encompass those of the constituency. It helps to place the SOC in the same time zone as a plurality of the constituency. If the constituency's users and IT assets are spread all over the world, the SOC may have more options to maintain 24x7 operations while keeping analysts employed only during the daytime.
Ensure continuity of operations of the CND mission through geographic diversity of SOC assets	The SOC should ideally be considered integral to the constituency's mission. This may compel SOC management and constituency executives to create one or more additional redundant or "load balanced" operations floors, giving the SOC some geographic diversity and resiliency.

4.3.2 Where to Place the Main SOC

In theory, the SOC could operate from any location that has ample rack space, office space, and connectivity to the rest of the constituency. If the constituency has consolidated its IT into one or a few data centers, the SOC could operate there, providing on-site response for a large proportion of incidents. Doing so would also allow the SOC to orient toward mission systems, enabling them to focus more on what's going on with the computing environment and less on routine politics. In practice, this isn't always the best strategy.

Practically speaking, most SOCs are members of their own constituency. Furthermore, they rarely have absolute authority in incident prevention or response. In this regard, their most important contact(s) are those from whom the SOC derives power, such as the CIO. The SOC must maintain continual contact with constituency seniors in order to stay relevant; this is a distinct characteristic in comparison to IT or network operations.

> **The best place for the SOC is at or very near the constituency headquarters.**

SOC representatives will likely need to meet with key constituency technical points of contact (POCs) (CISO, sysadmins, security personnel, etc.) on a regular basis, and also with constituency seniors (chief technology officer [CTO], chief operating officer [COO], CIO, CEO, etc.) from time to time. There are constant changes to policy, monitoring architecture, threat, and incidents, all of which require regular coordination. If there is insufficient power, space, and cooling for SOC servers or no suitable place for a SOC operations floor in the headquarters building, it may be better for the SOC to find a suitable space at a nearby office building, preferably one already owned or leased by the constituency.

4.3.3 Small and Large Centralized SOCs

If we pursue a centralized SOC model, we must have a way to support a presence at remote sites for purposes of incident response, equipment touch labor, and general visibility. This is crucial when the constituency headquarters is far from major elements of constituency operations. Here are some compensating strategies for a centralized SOC model with a geographically dispersed constituency:

- Have at least two designated POCs or "trusted agents" (TAs) at each major location where the constituency operates. These trusted agents:
  - Are usually sysadmins or security officers (ISSOs)
  - Watch over security-relevant issues at the site, such as new system installs and changes to network architecture

  - Hold the keys to SOC racks or rack cages and are the only people who are allowed to physically touch SOC systems
  - Are the default contacts for on-site incident response
  - Are customers of the SOC's audit collection/distribution capability, if one exists
  - Serve as champions for SOC interests at the site.
- Make contact with site TAs at least quarterly to ensure they're still in the same position and that their contact information is still current. Having multiple TAs at a site will help ensure that if one person leaves, the alternate TA can find a suitable replacement.
- Have SOC representatives participate in IT CM/engineering boards for IT assets that operate at remote sites
- Send SOC representatives to quarterly or annual collaboration forums run by IT people at sites where they discuss major initiatives in site IT
- Keep up-to-date rack diagrams for all SOC equipment, both both local or remote
- Have access to updated network diagrams of site networks and enclaves.

As we can see here, the line between centralized and distributed SOC models may appear to blur when we talk about how to keep tabs on remote sites. The main distinction here is that the site TAs don't work for the SOC as their main job. Therefore, the SOC cannot heavily task them outside the scope of incident response and sensor touch labor. In hybrid and distributed models, this is not the case, as we describe in the next section.

4.3.4 Incorporating Remote Analysts

Taking our model of TAs one step further, we can actually deploy SOC personnel to remote sites, thereby augmenting resources at the central SOC operations floor. While these individuals report to the SOC, the SOC's main analysis systems are still near the operations floor, and most incident calls are routed to the ops floor. However, we now have people who perform all the roles of the TA, above, make CND part of their day job, and are accountable to SOC leadership.

Keeping members of the SOC working in concert while spread across multiple sites will certainly be a challenge. Here are some tips on how to keep the whole SOC in sync:

- Ensure that analysts at remote sites go through the same personnel vetting and indoctrination process as all other SOC analysts.
- The SOC CONOPS and escalation SOPs need to support site escalation and response coordination with SOC operations leads. We don't want anyone at the site taking response actions without the knowledge of SOC leadership.
- Consider hiring analysts at remote sites who previously held IT security–related jobs at that site, thereby leveraging their familiarity with local operations and IT "culture."

- Folks at remote sites may get bored and feel disconnected from the main SOC. Some ways to mitigate this are:
  - Bring them back to the SOC for one to three weeks every year, as budget allows, for team cross-pollination and refresher training.
  - Consider having a "virtual ops floor" where all floor analysts and site analysts join an open chat room, video session, or VoIP session while on duty.
  - Call extra attention to successes by site analysts to the rest of the SOC team.
  - Schedule regular visits and telecons by SOC leadership to analysts at remote sites, giving them "face time" and keeping leadership abreast of site activity.
- For sites that host more than a few analysts, consider a "mini ops floor"—perhaps a small set of cubes where site SOC personnel can interact.
- Consider keeping site analysts on the job during their site's business hours.
- Ensure all SOC data feeds and sensors are integrated into one unified architecture. While the site should have its own specific source of log data and monitoring systems, this should be part of one unified, coherent architecture, with analytics tailored to that site or region.
- Some site analysts may demonstrate skills worthy of promotion to Tier 2, trending, or signature management. Give them appropriate room to further tailor data feeds, dashboards, and SIEM content to use cases specific to the site.
- Consider approaches for extending the SOC enclave (described in Section 10) to the remote site for use by the analysts there, perhaps leveraging one of the following approaches:
  - Connect SOC workstations back to the SOC through a strongly authenticated virtual private network (VPN), and ensure that sensitive SOC material is under close physical control.
  - Use a remote thin-client capability with strong authentication if remote site SOC materials cannot be cordoned off from other users.

4.3.5 Centralized SOC with Continuity of Operations

So far, we've discussed scenarios where the SOC has one main ops floor and one place where its management systems and data resides. If the ops floor is taken offline, the CND mission is offline.

Senior constituency leaders and SOC management may decide that some level of physical redundancy is necessary. The purpose, of course, is to ensure continuity of operation (COOP) of CND capabilities in the event of an outage such as the classic "smoking crater" events (thermonuclear war, fire, etc.), weather events (hurricanes, tornados, severe snow, etc.) or power/network outage.

When building a COOP capability for the SOC, there is often an impetus to implement a full-blown "hot/hot" capability whereby a complete duplicate of the SOC's systems (including a second ops floor) is stood up at a location distant from the primary SOC ops floor. This can be very expensive and is not always necessary. Before rushing into a decision for creating a COOP site, the SOC should carefully examine the following decision points:

- What contingencies is the COOP plan designed to address? How realistic are they, and how often are they likely to occur?
- If the main site constituency systems or SOC enclave were "hacked," are the COOP SOC systems designed to be insulated from compromise?
- In the contingencies described, if the SOC was taken out along with the rest of the site where it is located, what constituency systems are left to defend?
- If activation of the SOC's COOP capability were called for and there were any impediments in the process of executing the COOP, would the CND mission actually be a priority in the eyes of constituency seniors?
- Is a full, second instantiation of the SOC warranted?
  - Will a partial duplicate suffice?
  - Does the creation of a secondary COOP site, even if only partial, outweigh other competing resource needs such as more sensors or more personnel?
  - Does the secondary COOP site need to be regularly staffed? If so, should it be for the same hours as the main SOC (such as 24x7) or will regular business hours suffice (8x5 or 12x5)?
- In a COOP scenario, how long can the SOC be down? How quickly must the secondary capability be brought fully online?
- For the COOP site(s) under consideration, does their functionality (such as WAN and Internet connectivity) depend on infrastructure at the SOC's main site? If so, it may be a poor choice.

Many COOP SOC capabilities are built for the classic "smoking crater" scenario, which is very unlikely to occur. COOP is exercised far more often for non-extreme reasons such as network outages, power outages, or major weather events. The other major reason for a SOC to create a second site is essentially to create a second ops floor that can focus on assets at another major site or region of the constituency. In this scenario, we have analysts manning consoles at both locations on a sustained basis, with the analysis workload load-balanced between the two ops floors—perhaps by network/enclave, geographic region, or line of business. This approach is especially handy for constituencies located primarily at two major sites.

Even for SOCs that have a hot/hot COOP capability with servers and analysts at both sites, it is rare that every section of the SOC resides at both locations. More often, we have

redundant systems such as the SIEM and IDS management servers, local IDS sensors, Tier 1 analysts, and, perhaps, a couple of sysadmins at the COOP site. In this scenario, it's much easier to coordinate operations between sites than if we also spread Tier 2, trending, intel fusion, sensor management, engineering, and all SOC capabilities between two places.

Regardless of what functions reside at the secondary site, the SOC CONOPS should carefully integrate compensating controls to keep both sites in sync. It also helps to have a lead for the secondary site to coordinate operations with the main site leads and to provide care and feeding for the local analysts. One strategy that may work for SOCs with a hot COOP site in a different time zone is to either match or stagger shifts. By staggering shift changes for the two sites, there is always someone watching the console. For instance, if the main site is an 8x5 operation, the working hours for the secondary site two time zones away could be shifted by an additional two hours, giving four hours of overlap. By doing this, each site is up for eight hours, but together they provide 12x5 coverage.

Creating a second ops floor is very expensive and can be seen as a major drain on resources, especially if regularly staffed. If a SOC wishes to have a secondary COOP "lukewarm" site that it doesn't staff every week, it may consider the following strategy:

1. Choose an existing constituency office building or data center with at least a few spare racks and cubicles.
2. Deploy a redundant instance of key SOC systems such as SIEM, PCAP stores, and IDS management systems, thereby providing failover capability.
3. Find a good spot to place some SOC workstations, perhaps near the TA's office or cubicle.
4. Ensure all security data feeds are directed to both sites or mirrored from the primary to the secondary, at all times.
    a. If the primary site goes offline, having the log data immediately available at the secondary location could be invaluable.
    b. When performing COOP, the amount of time to bring the secondary site online should be minimized. If monitoring systems there are online but not being used, transition is that much quicker.
5. Regularly check (perhaps on a monthly basis) to ensure COOP servers and systems are functional and up-to-date with patches and configuration changes.
6. Schedule semiannual practices of the SOC COOP.

Having redundant core SOC systems will often come in handy. By placing them at a secondary site, the SOC's mission gains an added measure of redundancy. The biggest downside of this strategy is that any touch labor to site systems will come at the expense of the TA's time or sysadmins' travel dollars.

In summary, there are two key elements to an effective SOC COOP capability: (1) create and maintain it against a concrete set of business requirements, and (2) carefully manage the expectations of constituency leadership in the level of continuity the SOC is able to provide.

4.3.6 Centralized SOC with Follow the Sun

In the "follow the sun" model we have three ops floors, each separated by roughly eight time zones. Each ops floor is on the watch during local business hours (e.g., 9 a.m. to 5 p.m.). At 5 p.m. local time, one ops floor rolls to the next ops floor, where it is 9 a.m. This pattern continues every eight hours, giving 24x7 coverage but without making people come to work in the middle of the night.

This approach is very common for IT help desks that serve wide geographic regions (e.g., with major IT vendors and very large corporations). Another advantage is that the operators on shift are more likely to speak the language of those calling during their shift. In terms of pure labor costs, it also may be more affordable than a single ops floor staffed 24x7 because paying people during normal business hours is usually less expensive than paying them to come in at night. However, follow the sun is far less common in security operations because a couple of key assumptions do not carry over.

First, help desks spend a lot of their time talking to users. SOCs certainly interact with users, but they spend most of their time collaborating internally. Therefore, it's important to have all sections of the SOC not only in the same place but at work at the same time. In addition, language barriers and cultural differences among ops floors may be a challenge if each ops floor is staffed by personnel of different nationalities.

Second, although help desks are certainly dynamic environments, SOCs are subject to much more continual change in TTPs. Over the course of a few years, the SOC may completely evolve the way it does business, in response to growing mission demands or new threats. Moving three separate ops floors in the same direction at the same speed is an added challenge.

Third, each SOC Tier 2 and trending analyst will work a number of threads for several hours or days. Handing off an incident from one analyst to the next every eight hours isn't feasible. Either this limits the follow the sun scenario to just Tier 1, or we have three independent Tier 2s, each pursing its respective set of incidents.

If SOC managers wish to pursue a follow the sun approach, it is best to weigh the financial and procedural burdens against the virtues of this model. Of particular importance is the need to synchronize operations and promote cradle-to-grave ownership of incidents.

4.3.7 Tiered SOC

We have introduced the concept of a tiered CND architecture where multiple SOCs operate in a federated manner within a large organization. There are many examples where such an arrangement might be appropriate: within each branch of the DoD, Department of Treasury, Department of Justice (DoJ), Department of Homeland Security (DHS), and so forth. Although each of these entities has one SOC with purview over the entire department, there exist several subordinate SOCs beneath each that perform the majority of CND "heavy lifting" for the organization. These include regional NOSCs under the U.S. Army, Financial Management Service under Treasury, Drug Enforcement Administration under DoJ, and Immigration and Customs Enforcement under DHS. In all of these cases, we have a department- or branch-level SOC, as well as multiple SOCs beneath each.

Both the central and subordinate SOCs have a meaningful role to play, even though those roles can be quite different. Going back to a previous point, we must balance the need to maintain strategic SA with the need to be close to mission assets. Most people familiar with CND are used to operating down in the weeds. This can become a source of conflict in a tiered SOC scenario.

> **In a tiered scenario, the job of the central SOC is to enable security operations across the constituency and maintain a strategic perspective.**

How do we differentiate these roles? Once again, leveraging our capability templates from Section 4.1.2, let's focus on how these two SOCs interact and share the CND mission. (See Table 6.)

It's also important to recognize that not all coordinating and subordinate SOCs fall cleanly into these roles. Some SOCs that sit within a large constituency can support better resourcing, more advanced capabilities, and more strategic reach. Larger organizations can afford more capabilities and, thus, have the potential for greater independence, even though they fall underneath a coordinating SOC. The constructs presented here are only a starting point for establishing roles among tiered SOCs.

Having sorted out the roles and responsibilities of the central and subordinate SOCs, let's look at likely data flows between them. (See Figure 15.)

There are a couple of themes that should emerge here. First, the coordinating SOC handles tasks that scale well across the constituency and can be done in one place. For instance, their expertise in advanced tools and adversary TTPs makes them a good place to formulate training programs for the subordinate SOCs. It's also a great place to perform adversary tradecraft and TTP analysis, because they should have the analysts, the tools,

Table 6. Differences in Roles for Tiered Approach

Responsibility	Central SOC Role	Subordinate SOC Role
Location	Located at or near constituency headquarters	Located at office or headquarters of subordinate constituency
Monitoring, Incident Detection	Across constituency assets not covered by subordinates, such as Internet gateways	Within assigned constituency
Cyber Situational Awareness	Strategic across entire enterprise	Tactical within own constituency
Threat Analysis and Cyber Intel	Strategic across enterprise, reporting to subordinates, detailed analysis of adversary TTPs	Tactical within constituency, consumer of central threat analysis, focused on individual incidents
Incident Response	Cross-constituency coordination, operational direction	Intra-constituency response
Security-Relevant Data Management	Receives summary information and incident reports from subordinates; analysis and retention of data from assets not covered by subordinates, such as Internet gateways	Analysis and retention of own data, augmented with data from other organizations
Training	Coherent program for all analysts in constituency	Execution of general and specialized training for own SOC
Reports to	Constituency executives, external organizations	Own constituency executives, central SOC
Monitoring Capabilities and Tools	Enterprise licensing, lead on tool deployment and refresh	Chooses monitoring placement, specialized gear when needed

the time, and just enough knowledge of constituency networks to make sense of the artifacts handed to them by subordinate SOCs.

Second, it's the job of the subordinate SOCs to perform most of the tactical hands-on monitoring, analysis, and response to incidents. The coordinating SOC is there to make sure its entire constituency is working toward a common goal, and that they have shared SA. While the subordinate SOCs may provide a limited event stream to the coordinating SOC, it's unlikely the coordinating SOC analysts have the context to make sense of that data. Incident reporting and trending from the subordinate SOCs support coherent SA formulated by the coordinating SOC.

Third, it is more likely that the central coordinating SOC will have a sizable budget for big technology purchases and custom tool development. Requiring subordinate SOCs to use

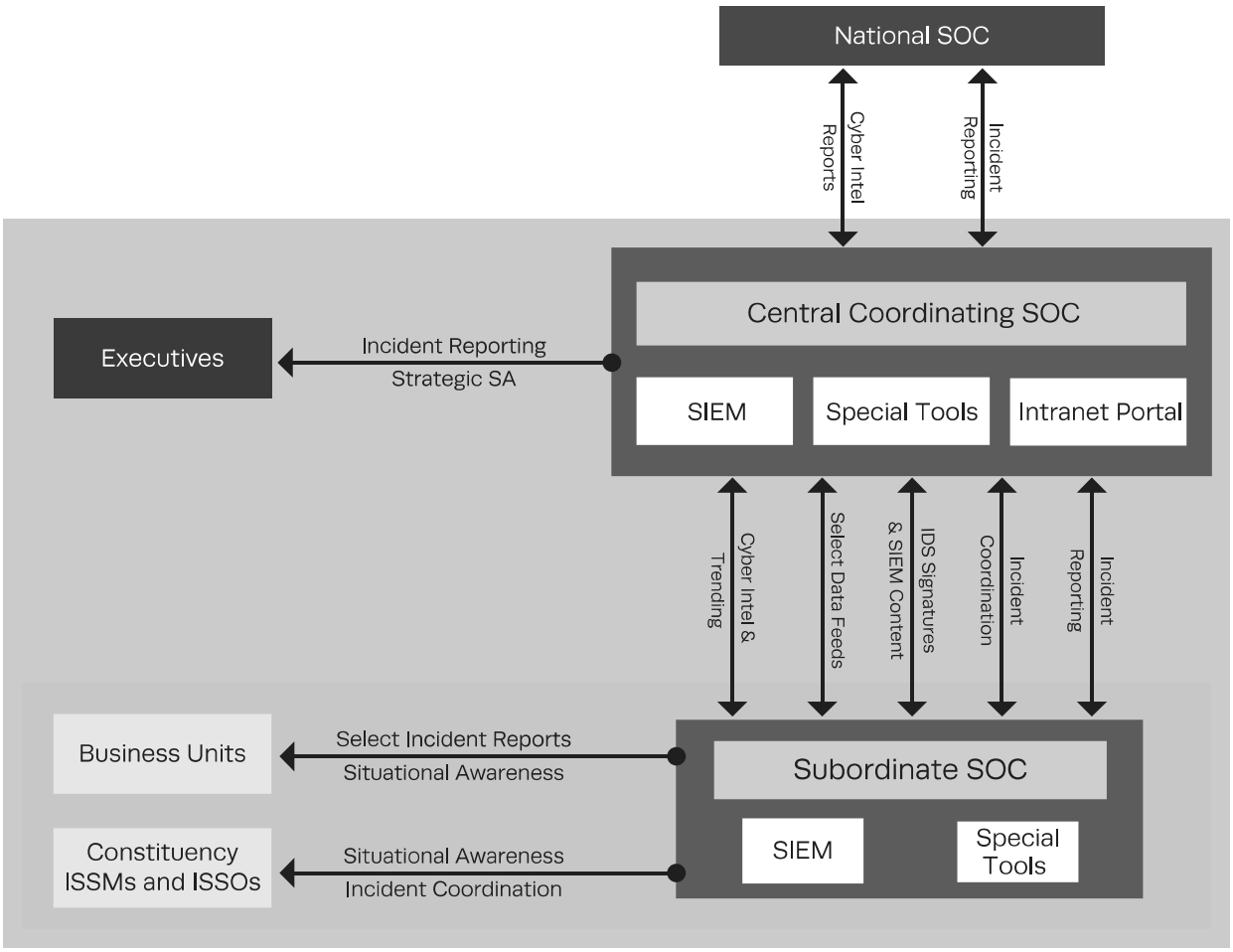

Figure 15. Data Flows Between Central and Subordinate SOCs

a specific product may be too heavy-handed. Instead, what may work is to mandate the use of a type of tool and provide free copies of one specific brand. As a result, the subordinate SOCs can use the enterprise tool if it fits their needs or pay for their own if it doesn't.

Last, and perhaps most important, the coordinating SOC must work very hard to maintain relevance and usefulness in the eyes of the subordinate SOCs. The SOCs at the bottom of the food chain are typically sitting on a pile of raw data. The coordinating SOC has little apart from the incident reporting, cyber intel, and select data feeds from its subordinates. The coordinating SOC must also be careful that downward-directed guidance and tasking are perceived as relevant and useful.

They must work in a symbiotic relationship that stems from perceived value and analyst-to-analyst contact, far more than mandate and policy. The coordinating SOC may offer substantial help in the form of in-depth forensics capabilities, cyber intel, and SA to

its subordinates, in exchange for the subordinates' processed incident reports. The subordinates turn data into information; the coordinating SOC turns information into knowledge. This relationship is self-reinforcing over time and, usually, must begin by the coordinating SOC offering something of value to its subordinates that these subordinates cannot get on their own, such as tools and authority.

4.3.8 Coordinating SOCs

At the most extreme end of constituency size are national coordinating SOCs, which we will colloquially refer to as "mega-SOCs." Today, there is limited agreement on the proper role of these organizations. They are comparatively few in number so their capability portfolio and influence are subject of some debate. National-level coordinating SOCs have a unique mission; their goals include:

- Forming a coherent SA picture for their entire constituency, focusing on constituency vulnerability to threats, and adversary TTPs
- Harmonizing operations among their subordinate SOCs
- Bringing their subordinate SOCs up to a baseline set of capabilities.

By contrast, most CND analysts and leaders are used to operating down in the weeds where they have access to raw data, have some measure of vested authority over their constituency, and are direct participants in incident response. The "mega-SOC" doesn't always have these things, and when it does, they often take on different forms than with the mega-SOC's subordinates.

Instead of focusing on direct reporting of raw event feeds or promulgating detailed operational directives, the coordinating SOC may achieve its goals by providing a unique set of capabilities that its subordinates usually can't. These include:

- Providing secure forums for collaboration between subordinate SOCs (e.g., wikis and secure online forums)
- Performing strategic analysis on adversary TTPs by leveraging a wealth of finished incident reporting. A mega-SOC is uniquely positioned to focus on observing and trending the activity of key actors in the cyber realm.
- Providing a clearinghouse of tippers, IDS signatures, and SIEM content that other SOCs can directly leverage without further legwork. A mega-SOC could harvest indicators from human-readable cyber intelligence and provide it back out in both human- and machine-readable form for ingest by subordinates' analysts and SIEM, respectively. In order for this to work, however, intel should be turned around in a timescale and with detail that is beneficial to its recipients. This will likely mean processing and redistributing cyber intel in timeframes of hours or perhaps a few days, and in so doing preserving as much original detail and attribution as possible.

- Aggregating and sharing CND best practices, process documents, and technical guidance
- Providing malware analysis and forensic services to constituent SOCs that have collected the necessary files or images but don't have the staffing to analyze them
  - Of all the things a mega-SOC can do, this is potentially one of the most impactful, because many SOCs have a hard time maintaining the skill set to perform the malware analysis or forensics that is critical to have during a major incident.
  - This can include an automated Web-based malware detonation "drop box" (See Section 8.2.7.) or in-depth human analysis of media or hard-drive images.
- Providing enterprise licensing on key CND technologies such as network and host monitoring tools, vulnerability scanners, network mapping tools, and SIEM, provided the following two conditions are met: (1) subordinates are not forced to use a specific product, and (2) there is sufficient demand from subordinates to warrant an enterprise license
- Providing CND analyst training services:
  - On popular commercial and open source tools such as IDS and malware analysis
  - On the incident response process
  - On vulnerability assessment and penetration testing
  - Leveraging a virtual "cyber range" where analysts can take turns running offense and defense on an isolated network built for Red Team/Blue Team operations
  - Running SOC analysts through practice intrusion scenarios, using real tools to analyze realistic intrusion data.

In many ways, these services are far less glamorous than flying big sensor fleets or collecting large amounts of raw data, especially to those running the mega-SOC. From the perspective of the constituent SOCs, they are far more valuable, *because they provide something back.* By providing these services, the Mega SOC is likely to achieve its unique goals better than if it tries to provide the same capabilities as its subordinates.

For more details on standing up a national SOC, see [60].