Knitting SOCs

A Security Operations Center (SOC) is designed to centrally control information security operations, providing situational awareness and monitoring of all enterprise information assets. When building an SOC, many organizations struggle with defining or selecting employee roles within the SOC to adequately cover the detection, prevention, and response of security incidents. This paper describes factors to be considered in the design of SOC team roles, and suggests commonly used roles, job descriptions, and development a...

Knitting SOCs

Designing and Developing the Staff of a Security Operations Center

GIAC Certified Incident Handler (GCIH) Gold Certification

Author: Courtney Imbert, cimbert@giac.org

SANS Technology Institute MSISE Candidate

Advisor: Rick Wanner:

Accepted: May 24, 2015

Abstract

A Security Operations Center (SOC) is designed to centrally control information security operations, providing situational awareness and monitoring of all enterprise information assets. When building an SOC, many organizations struggle with defining or selecting employee roles within the SOC to adequately cover the detection, prevention, and response of security incidents. This paper describes factors to be considered in the design of SOC team roles, and suggests commonly used roles, job descriptions, and development activities based on a job task analysis of SOC team members and managers, as well as research into best practices in information security.

1. Introduction

Over time, the list of "must-have" security appliances and services has become ever larger. Security departments may find themselves managing firewalls, anti-malware scanners, IDS/IPS systems, vulnerability and patch management, DLP, and other services. These services may each reside at multiple points on the organization's infrastructure, from hosts to the perimeter. Modern attacks, especially targeted ones, take advantage of multiple points of weakness. The best way to identify and defend against multi-faceted attacks is to correlate events from disparate sources. Security Operations Centers (SOCs) provide a way to correlate, aggregate, and normalize the growing number of security events and sources of data (HP Enterprise Security, 2011). Once the territory of governments and large corporations, SOCs are now in place for a broader range of organizations, either as an internal or outsourced center for preventing, detecting, managing, and responding to incidents.

Central Control Rooms or Operations Control Centers are not new concepts; they have a long-standing place in the military, for flight controllers, and utility providers. Many IT departments are already familiar with Network Operations Centers (NOCs). In NOCs, employees are focused on the uptime and operation of enterprise systems and services. It makes sense for employees with unique, but related, skills to serve on the same team to collaborate and share information. Similarly, Security Operations Centers (SOCs) are teams of employees that work on continuous monitoring and rapid response to anomalies, but with a focus on information security. Having organized roles and procedures to manage information security is critical to reducing both the frequency and impact of security incidents (Nathans, 2015).

This paper is not an attempt to standardize the staff of a SOC, but to provide a snapshot of common roles for SOCs based on a sample of organization job postings and a survey of SOC subject matter experts. Our intent is to provide a starting point for organizations at the beginning of their journey toward establishing a SOC. The job descriptions included in this paper can be integrated into an overall plan to develop a SOC. They should be customized to an organization's security mission, risk tolerance, and particular business needs.

2. Methodology

The methodology used to develop the staffing models involved data gathering, a targeted survey, and job task analysis. To gather initial data and form the basis for our survey, approximately 200 recent job postings were collected, each containing terms identifying them as part of a SOC. The job postings were divided into rough categories, using the job titles and content as a guide.

A survey was issued asking about the current configuration and staff of SOCs, using SurveyMonkey.com for the design and administration of the survey. The survey was used to refine the results gathered from parsing job postings, and also to identify participants for follow up questions. It was distributed to several information security email lists, and publicized on professional social media networks. There were 56 respondents to the survey.

The roles found to be common in SOCs, according to the job posting data collection and within the survey, were more deeply explored using Job Task Analysis (JTA) techniques. This study was performed by reviewing job descriptions to identify similar jobs across different organizations. Conversations were then held with individuals familiar with SOC environments to confirm the results. The final results of the data collection, survey, and conversations with SOC employees were incorporated into the list of roles included in this paper.

3. The Role of SOCs in Organizations

Many organizations become interested in developing a SOC when one or more incidents uncover gaps in their incident response processes. Given the urgency and complexity of an incident, it can be difficult to "tie it all together". A lack of cohesiveness is indicated by problems like a slow response to threats, lack of coordination between teams, lack of procedures for threats and incidents, or inaccurate or incomplete communication about incidents (Wang, 2010). A well-designed SOC brings both human and network resources together to consolidate the functions of incident response, and execute more effectively.

Building a SOC from scratch can be a daunting challenge. Few organizations agree on best practices, or even common nomenclature. The functional team referred to here as a "SOC" may be called other names by other organizations, including a Computer Security Incident

Response Team (CSIRT), Computer Incident Response Center (CIRC), Computer Emergency Response Team (CERT), or many other variations involving the words "network", "computer", "cyber", "incident", "operations", "defense", or "enterprise" (Zimmerman, 2014). Incident Response Teams can also be a separate entity from SOCs, or they can be embedded in each other! Because there are so many variations associated with SOC-related terminology, this paper uses the most common definitions found in the field at the time of writing. For the purposes of this paper, a SOC includes the operational monitoring of a network, and the prevention, detection, and initial response to information security incidents.

SOCs have a primary goal of collecting, monitoring, and responding to information security data, using a central team of employees. However, these teams may pull in additional resources to respond to incidents. This may occur by way of a pop-up team, like an emergency operations center (EOC), by hiring external consultants, or by pulling in specialized employees as needed (Nathans, 2015). The SOC has a symbiotic relationship with the organization it protects; it must both support and be supported by an organization's business and IT units.

4. Factors that affect the design or selection of roles

Though an organization can use a template or best practices to begin designing a SOC, it is best to customize the roles to the needs of the organization. When an organization sets out to design a SOC, several questions must be answered: which roles must be included in the SOC, how many employees should be assigned to each role, and what are the skill sets required? There are several factors that affect those decisions.

4.1 The Mission of the SOC

When creating a SOC, an organization must define the basic mission for the SOC. The mission should address why the organization needs a SOC, which issues it will solve, and the short- and long-term vision for the SOC (Ernst & Young, 2013). The objective of the organization's security program should drive the mission and subsequent design of the SOC. Clearly defining the SOC's mission increases the chances of long-term success, and avoids conflict with other IT functions.

Once the mission and scope of the SOC are determined, the processes needed to support that mission can be defined and included in the job tasks of roles within the SOC. McAfee includes the following as basic procedures required for maintaining a SOC (McAfee "Foundstone" Professional Services, 2013):

- Monitoring procedure.
- Notification procedure (email, mobile, home, chat, etc.).
- Notification and escalation processes.
- Transition of daily SOC services.
- Shift logging procedures.
- Incident logging procedures.
- Compliance monitoring procedure.
- Report development procedure.
- Dashboard creation procedure.
- Incident investigation procedures (malware, etc.).

Roles can be further defined by creating use cases for the SOC. Examples of use cases include unauthorized devices on the network, or a malicious website being accessed from multiple internal sources. Although not all use cases can be defined, stepping through a use case can be a useful way to find gaps in the design of a team or a particular role.

Though some people may envision a Security Operations Center as a standalone facility with sophisticated technology, multiple monitors and dedicated analysts, an effective SOC can be as simple as a pair of neighboring cubicles in an IT department. As long as it aligns with the security mission, an SOC can be simple or complex, with few or many employees. The mission drives the shift design and physical configuration of work throughout the SOC, and dictates how much coverage is “enough”. Not every SOC operates 24 hours per day, 7 days per week; it is possible to have an 8 x 5 SOC, with analysts on-call for operational emergencies (Anderson, 2013).

Geographically, teams can be centralized in a single room, or they may be distributed across multiple locations. Larger organizations with a large footprint and a need for 24/7 monitoring may find it appropriate to create a global SOC, with employees distributed across time zones and countries. However the SOC is designed, there should be a clear “hand-off” procedure between team members as monitoring is transferred between shifts and locations (HP Enterprise Security, 2011).

4.2 Business & Technical Environment

The size, type, and scope of the organization all factor into the staffing level and role design for a SOC. Larger organizations tend to have more data sources to protect and monitor, and more resources for hiring staff or providing tools to the SOC.

Managers should be sure to document the technical environment before designing SOC roles. This prevents gaps in coverage. Key network and application architecture diagrams should be available while developing SOC team roles, and these should be continually updated and accounted for as they change over time.

For internal SOCs that cover a small environment scope, it is likely that a SOC is designed with fewer team members performing multiple roles. In small organizations, it's common to see a "Jack of all Trades": a single person performing multiple roles to support information security. Having cross-functional employees that manage a small environment means SOC team members will be highly familiar with the environment, and it will reduce the overhead of transitioning work. However, it is critical to manage a small staff carefully to prevent burnout and information hoarding. This can be done in a few ways, including offering support and redundant coverage for SOC team members, cross training, and providing paths to promotion and lateral movement (Appelbaum & Santiago, 1997).

4.3 The Customer (Internal vs. External SOC)

The customer often defines which services are provided by a SOC, and consequently, which roles are needed to staff it. SOCs may be developed from the corporate side as an internal entity, or a SOC may be a service provider, hired to provide SOC services to one or more external organizations. Examples of businesses that provide SOCs as an outsourced service include Symantec, SecureWorks (Dell), and McAfee (Rothke, 2012).

Organizations that opt to create internal teams typically face more up-front cost when developing and recruiting for the staff of a SOC (Rothke, 2012). While small organizations may create a team custom-built to their environment, they may not have the scale to support a full-time specialized employee. For example, a service provider may have the ability to dedicate the training and resources to a full-time incident forensics specialist who works on incidents across multiple organizations as needed. Internally-staffed SOCs are in the unique position of having an IT department that serves as both a customer and a working partner (Nathans, 2015). SOCs do not necessarily need to be 100% internal or external; over 20% of the organizations surveyed identified their SOCs as staffed by a blend of external and internal resources.

Though the job design in a SOC may differ between internally-staffed organizations and externally-staffed organizations, in both cases it is critical to maintain close communication with the customer. The business needs of the customer must be documented, worked into the overall SOC strategy, and addressed by each role in the SOC.

4.4 Compliance Factors

Some organizations may have legal or business-related compliance requirements that contribute to decisions about staffing. In addition to HIPAA, SOX, GLBA, and other compliance-related laws, organizations may need to comply with industry-imposed frameworks such as the PCI Data Security Standard (Swift, 2010). Organizations may also have self-imposed or internal requirements that guide the design of services, like ITIL. Though successful compliance is not the end goal of an effective security program, demonstrating compliance can become a major concern for IT and SOC managers.

Compliance or regulation requirements can affect the staffing of a SOC in multiple ways. The requirements may drive the type of security devices monitored by the SOC. Network monitoring can act as a control (particularly if it is protective rather than just detective), or it can provide reporting to demonstrate compliance (Daudelin, 2014).

Due to the additional technical controls or tasks related to compliance, additional training may need to be built into the design of SOC roles. If the compliance or regulation requirements are particularly complex, it may be necessary to add one or more roles specializing in compliance. Among other tasks, these team members can perform internal audits, provide consultation or expertise, run required reporting, and ensure that changes do not bring the organization out of compliance.

5. Job Descriptions

During the research process, collecting data for SOC-related job roles, even with identical titles, produced a wide range of results. While one job posting might request minimal experience for a Security Analyst, another job post might request ten or more years! This could be explained by the varying level of expertise needed to perform more complex or critical analysis, despite the similar descriptions of tasks. According to the survey, this difference is often represented by tiers; a "Security Analyst Level 1" may operate within the realm of basic triage, identifying incidents and disseminating them to the appropriate teams, while a "Security Analyst Level 3" may perform an in-depth, expert-level analysis into network traffic or malware. Over 70% of respondents reported their organizations divided their SOC into escalation tiers.

"Soft skills" or "core skills" were often included in the job descriptions for SOC roles. These included traits like:

- The ability to work reliably under pressure
- Excellent written and verbal communication skills
- The ability to present technical ideas effectively to an audience
- The ability to work with a team of employees
- Strong organizational and time management skills

Without question, these traits are important for the success of any employee in a SOC. However, this study and the resulting surveys focused on role-specific technical and information security-related tasks and skills. Evaluating and developing general organizational, psychological, personality, and work initiative traits are outside the scope of this paper. Therefore, these traits were omitted from the collection of qualifications unless they were uniquely characteristic of the role. However, core skills should certainly be included when advertising for positions and evaluating candidates.

The following are common job descriptions, tasks, and requirements most commonly found in SOCs. The data was gathered according to our survey, compilation of data from job postings, and conversations with current and former SOC team members. These can be used as basic templates for security roles, but should be customized to an organization's needs, and supplemented with additional roles or competencies as needed.

5.1 Security Analyst

Security Analyst was the most-commonly staffed position in the survey. Security Analysts provide a line of defense against security threats in the SOC. They perform real-time analysis of the inputs into the data center, and respond according to pre-defined, documented procedures developed for the SOC's use. Security Analysts commonly participate throughout the entire life cycle of an incident, from prevention through post-mortem.

Alternate titles:

Alternate titles to "Security Analyst" include Cybersecurity Operations Analyst, Information Security Analyst, Security Operations Center Analyst, and more. Several job postings with the title "Information Security Operator" appeared to include tasks associated with a Security Analyst, but within a narrower scope or at a lower level of triage, and with a lower level of training, education, and experience.

During the task analysis, questions were raised about the difference between a Security Analyst and a Security Engineer. It became clear that many organizations blend the Security Engineer and Security Analyst role. As defined here, a Security Analyst primarily performs monitoring, triage, response, and investigation into incidents; a Security Engineer is responsible for the management of the SOC's security controls. In any organization, the two roles must work closely together, but in resource-constrained SOCs, both roles may are likely to be blended together into a single job.

Tasks:

- Respond to security incidents identified by SOC appliances
- Monitor, manage, and analyze logs generated by SOC appliances and sources
- Monitor the Network Security Dashboard for possible incidents
- Follow SOC policies, procedures, and documentation regarding events
- Review public threat bulletins, warnings, and advisories
- Escalate events to the appropriate group

Knowledge / Skills / Abilities:

- Familiarity with Windows and Linux operating systems
- Familiarity with Security Incident & Event Management Systems (SIEM)
- Familiarity with network perimeter technologies, like firewalls and proxies
- Familiarity with the operation of Intrusion Detection or Prevention Systems (IDS/IPS)
- The ability to analyze network traffic packets and protocols
- An understanding of networking concepts (TCP/IP, network architecture and topology)

Education and Experience:

The majority of job postings preferred or required at least a Bachelor's degree to apply. A small number of postings accepted a lower level of education (Associate's or High School diploma) with additional experience.

Organizations had a wide range of desired experience for this position, from no experience required to 5-10 years. The average organization requested applicants have between three and four years of experience in IT security or with SOC-related technology.

Certifications:

The most common certification requested for this security analysts was (ISC)2's CISSP, followed by GIAC's GCIH (GIAC Certified Incident Handler) or GCIA (GIAC Certified Intrusion Analyst), and EC-Council's CEH (Certified Ethical Hacker). Most organizations indicated the certifications were "preferred" and not pre-requisites, or that the training and certification would be required upon hire.

5.2 Manager

Competent management is key to making decisions and coordinating the efforts of SOCs. SOC managers serve as the liaison between an organization's business objectives and the technical controls provided by the SOC. Managers provide much of the strategic planning that brings a SOC into alignment with an organization's overall risk posture. They must understand the technical needs and status of the SOC, and communicate those elements to non-technical audiences when needed. Though managers may not perform technical tasks themselves, they should have a solid understanding of information security concepts and a high level of technical literacy.

Executive support is key to the success of a SOC. 65% of information security respondents in a 2013 survey cited budget constraints as their number one obstacle to delivering value to their business (Ernst & Young, 2013). Managers must advocate for and allocate resources throughout the SOC to best provide value to the organization. They must situate people and tools to the proper places to respond to incidents effectively. Typically, they also measure the success of the SOC by developing meaningful metrics, and presenting those to upper-level management.

Tasks:

- Manage cross-functional SOC teams, which may include analysts, engineers, and supervisors, as well as outsourced specialists
- Ensure operational excellence, coordination, and quality throughout the SOC
- Serve as the formal business owner of information security processes and policies
- Serve as a leader in teams across functions, clients, and employees during SOC-related projects or incidents
- Manage coordination and escalation for critical incidents
- Develop, maintain, and present security analysis metrics for the SOC

Knowledge / Skills / Abilities:

- The ability to manage and lead people
- Familiarity with operating enterprise security and threat management technology
- Familiarity with information security frameworks and general best practices
- An understanding of contractual, legal, or regulatory requirements like PCI, SOX, and HIPAA (depending on the environment)
- Experience developing detailed metrics, reporting, and presentations for audiences

Alternate titles:

The management staff for a SOC is often determined by the size of the SOC. In small SOCs with a flat management structure, a single manager with control over multiple functions of the SOC may have the title of "director". Frequently, "Supervisor" and "Manager" roles shared similar characteristics, and some organizations may blend these roles into a single job.

Education and Experience:

Employers expect SOC managers to be seasoned professionals. On average, job postings required 7-8 years of management experience in an IT or information systems environment, with a related bachelor's degree or (for higher tiers of management) a Master's degree. The most frequently requested bachelor's degrees included Information Technology or Information Systems.

Certifications:

In most cases, experience was emphasized above information security certifications for management roles. However, some certifications were seen as helpful for SOC managers: (ISC)2's CISSP, ISACA's Certified Information Security Manager (CISM), GIAC's Certified Incident Handler (GCIH), and EC-Council's Certified Ethical Hacker (CEH).

5.3 Security Engineer

Security Engineers were present in the SOCs of over half the respondents. Security Engineers manage and monitor performance of the security appliances, devices, and software, and provide support and configuration for those products. Engineers may have specialized areas of knowledge, like SIEM or IDS, or they may be responsible for multiple security technologies throughout the SOC. They may also provide ad-hoc support to Security Analysts or Operators during the incident response process.

Tasks

- Design and implement security-related network infrastructure based on business requirements
- Select, design configure, test, and provide daily support for security-related technologies like SIEM, IDS/IPS, firewalls, encryption, and malware detection for optimal performance
- Perform or support vulnerability assessment across the organization, and perform remediation for devices that do not meet security standards
- Follow, evaluate, recommend, and adjust SOC policies according to organizational needs

- Provide incident response support, investigating and responding to security threats within the scope of the Security Engineer role
- Seek opportunities for automation, and implement them
- Provide data for operational metrics and progress reports

Knowledge / Skills / Abilities

- Familiarity with the operation and administration of operating systems like Windows, Linux / Unix, including server systems
- An understanding of information security and operations logging and monitoring tools
- Understanding of network technologies (LAN/WAN, TCP/IP, and network protocols)
- In-depth understanding of security technologies and concepts like SIEM, IDS/IPS, patching, application whitelisting, hardening, scanning, and monitoring
- Experience with or understanding of relevant compliance standards
- Experience analyzing business requirements and making security recommendations based on those requirements

Alternate Titles and Similar Roles:

In some cases, a "Security Architect" provided similar services at a higher level with a focus on vendor selection, security service placement, and the rollout of new products. "Operations Engineer" or "Information Engineer" were job titles found to contain similar tasks and requirements. "Network Security Engineer" was cited as a role in the SOCs of over 30% of respondents, though this role is more likely to specialize in the management of network or perimeter security devices, like IDS/IPS.

As mentioned in the "Security Analyst" section, many organizations blend the Security Engineer and Security Analyst roles together into a single job.

Education and Experience:

The Security Engineer role was generally the most technical role profiled. In the vast majority of cases, a Bachelor's degree in a technical field like Computer Science, Computer Engineering, or Information Systems was required to apply for the job. Master's degrees were sometimes listed as "nice-to-have", but were not identified as a requirement during the job analysis. In a small number of cases, the employer was willing to accept a high school-level diploma with extensive experience.

The number of years of experience requested by employers ranged from two to ten years. On average, organizations requested five to six years of experience with security-related technologies.

Certifications:

The Security Engineer role was the most likely to require certifications before starting the job. The certifications were sometimes vendor-specific, like the Cisco Certified Network Associate (CCNA), Check Point Certified Security Administrator (CCSA), or Microsoft Certified Solutions Expert (MCSE). Other requested certifications included Network+, Security+, CISSP, ISACA certifications, and GIAC certifications.

5.4 Specialist

Specialists include technicians that support the SOC with their deep understanding of subject matter, and can be called upon to provide input during development projects or incidents. Approximately one-third of survey respondents identified a specialist as a key role in their SOC. Specialist may include technicians with knowledge of a particular product, or a technical area of information security expertise, like reverse engineering, database administration, or vulnerability management.

Not surprisingly, job descriptions for SOC specialists varied widely! It was difficult to identify specific tasks for Specialists, since these varied with the needs of each organization. A Specialist role may fall closer to the definition for Security Analyst, reviewing specialized data sources for operational purposes, or it may be more aligned with a Security Engineer, configuring and administrating security appliances. For the sake of performing task analysis, we assumed the Specialist acts in both capacities, managing systems related to their specialization, while providing monitoring and response support in an expert capacity.

Tasks:

- Analyze threat intelligence and risk reports related to the area of expertise
- Review log files and data correlation to identify events of interest
- Assist in network investigations, providing insight and context into specialized areas
- Act as administrator or security support on specialized tools or devices
- Provide support during incident response, within the scope of their area of expertise
- Research, develop, recommend, and implement current testing tools, techniques, and process improvements for their area of expertise
- Provide training to SOC team members as needed

Knowledge / Skills / Abilities:

- General proficiency working with internet, web, application and network security technologies
- Extensive experience working with the technology required for the specialist role

Alternate Titles and Related Roles:

Specialist roles sometimes include the area of specialization in their title, like "Vulnerability Management Specialist". Specialist roles can easily blend together with higher-tier Security Engineer or Security Analyst roles, since both require an in-depth technical understanding of SOC-related technology.

Education:

Perhaps because specialized knowledge is often gained outside the classroom, a college-level education is not necessarily demanded by employers for specialist roles. Only 25% of the specialist roles studied required a Bachelor's degree, while it was listed as "preferred" or not requested at all for the remainder. On average, employers requested between 3 and 4 years of on-the-job experience with technologies related to the specialization needed, sometimes specifying experience with specific products.

Certifications:

As with other SOC roles, general security-related certifications like the CISSP, GIAC certifications, and EC-Council's Certified Ethical Hacker (CEH) were desired. Depending on the specialization, certification requirements could be specific to areas of knowledge, like forensics, or product-specific.

5.5 Supervisor

Competent supervisors are critical to making the SOC team run smoothly. They are operationally responsible for the day-to-day performance of SOC teams or shifts. The supervisor must be capable of performing the jobs they are responsible for, and directly mentoring the team members in those jobs. Supervisors should have an up-close view into daily operations to guide technical people to success, whether that means recommending a development plan or rewarding outstanding performance. They must also align managing people with quality control, monitoring the service levels of the SOC and making adjustments where necessary.

Supervisors can be assigned cross-functional teams according to geography or shift, or they can be asked to oversee unique functional areas like incident management or security engineering (Nathans, 2015).

Tasks:

- Oversee a functional, shift-based, or geographical team in a SOC environment
- Prioritize, direct, and monitor workflow
- Coordinate and schedule coverage for the SOC, and assign resources to critical incidents or projects
- Monitor and meet triage, quality metrics, and service level agreements
- Provide coaching, feedback, training, and mentoring to SOC team members
- Manage the escalation of incidents, ensuring they're addressed by appropriate team members
- Help develop, implement, and maintain SOC policies, procedures, and processes

Knowledge / Skills / Abilities:

- Competencies similar to those of the members of the team being supervised, if not better
- General technical knowledge and experience with security technologies and concepts
- Interpersonal skills for team building and coordination with other groups

- Project prioritization, management, decision-making and organizational skills
- Skilled at explaining complex technical issues to non-technical business employees

Alternate Titles and Similar Roles:

Supervisors may also be referred to as "team leads" or "operations leads". In smaller SOCs, the role of "Manager" and "Supervisor" may be blended together into a single job.

Education and Experience:

The supervisor role may be an ideal promotional path for a team member in an existing Security Analyst or Security Engineer role, since it requires both technical aptitude and organizational familiarity.

When recruiting from the outside, a Bachelor's degree with a technical focus like Computer Science, Computer Engineering, or Information Systems was the most common request.

The range of experience desired ranged widely, with some job postings requiring ten or more years of experience for supervisors of high-profile teams. At least 3 years of experience in security operations were requested by all job postings, with many requesting two or more years of experience specifically managing teams.

Certifications:

Typical security certifications were requested for this role, including CISSP, CISA, or GIAC certifications. Supervisor job descriptions had some specialization in requested certifications, which may reflect the function of the team being managed; for example, forensics certifications like GIAC Forensic Analyst (GCFA) or Encase Certified Examiner (EnCE) certifications were requested in a minority of job postings.

5.6 Other Roles

Other roles were identified during the research phase. Though they were not common enough to SOCs to be included in the task analysis, the titles may give fledgling SOCs ideas for possible roles to include in a SOC staffing plan. These include:

- Technical Writer
- Security Administrator
- Threat Intelligence Analyst or Manager
- Project Manager
- Data or Metrics Analyst
- Security Architect
- Forensics Analyst
- Database Administrator
- Security Software Developer

6. Skill Development

An employee's level of competence within a role is determined by the level of practical and thinking skills, experience, and knowledge he exhibits within his job. Most organizations will not have employees ready to "hit the ground running" within a newly formed SOC. In a competitive job market, it can also be difficult to recruit employees with the needed skill sets. In most cases, some form of training will need to take place to bring a team member into alignment with the needs of a job.

Training needs are unique to each role in a SOC, and should be mapped to the tasks and competencies demanded by the role. Additionally, training needs differ by individual; organizations should do a competency assessment to find knowledge gaps before creating a training plan (Stanton, Salmon, Jenkins, & Walker, 2010). The individual's learning style and personality type may also feed into the selection of a training format.

Different forms of training provide different benefits. Ideally, multiple forms of training are integrated together to increase a SOC team member's level of competence. Having a SOC team member without formal external training might mean he knows only how to do the procedures assigned to him, without an understanding of the foundational concepts of information security. Conversely, sending a SOC team member through formal training and immediately starting work before training him internally might mean he makes critical mistakes as he becomes familiar with the organization's security environment.

6.1 Formal External Training

Formal external training can come from a variety of sources, including university or college programs. Examples of security training providers include the SANS Institute, EC-Council, and SkillSoft. Training can be performed in-person, but it is becoming ever more flexible, with options like online or pre-recorded classes. External training can provide a "big picture" for the new employee, but it must be supplemented with internal training to create an effective SOC team member.

6.2 Formal Internal Training & Mentorship

Well-documented procedures, processes, and policies are critical to the successful operation of a SOC (Stanton, Salmon, Jenkins, & Walker, 2010). When recruited from outside the organization, even the best team member will need to be familiarized with the organization's procedures and communication processes. By training staff internally, the SOC can customize learning to fit the individual being trained (Dillon, n.d.). Conversely to formal external training, internal training can be expensive to develop, but it is typically customized to the environment in which the team member will work.

Mentoring is a common and effective method of training and guidance for new employees. Mentoring itself may take on several forms, like one-on-one mentoring by a supervisor, peer mentoring from a co-worker, group or "circle" mentoring by rotating through team members, and virtual mentoring. Though informal mentoring or "shadowing" can be effective in training new employees, many organizations find better success when they provide support by way of training checklists or transition plans. Mentoring can serve different purposes throughout the employee life cycle; including helping new recruits onboard and providing support throughout organizational changes (United States Office of Personnel Management, 2008).

6.3 Self-Driven Training

Self-driven training can include activities like reading books or websites about information security, participating in Capture-the-Flag or competitive challenges, and watching conference talks about information security skills. Some training providers, like the SANS Institute and CompTIA, offer their class materials as a "self-study" option at a lower cost to facilitate self-driven training.

This type of training may be more difficult to locate and assess effectiveness, since it is often done on a small scale or as a single event. However, don't underestimate the effectiveness of self-driven training - many information security professionals find this type of training rewarding and fun!

6.4 Team Training

While individual competence is important, a group of competent employees is not the same thing as a competent team. Once team roles are determined and fulfilled, SOC teams should be trained and assessed as a whole. Because teams are unique for each organization, team-focused training is often provided internally by the organization itself. Typically, this is done with drills or exercises that reflect some SOC use case or procedure. Team training can also be incorporated into the "Lessons Learned" phase of an incident; the review of an incident provides a valuable opportunity for a team to identify and highlight effective behaviors, as well as troubleshoot gaps in communication or procedures.

7. Skill Assessment

Once the tasks, knowledge, skills, and abilities are identified for a SOC role, a plan should be developed to assess the competence of individuals within the role, both when identifying recruits and throughout the team member's life cycle.

Competence assessment doesn't necessarily need to be in the form of a formal exam. It could be as simple as asking an employee to rate his confidence with specific technologies or skills, and can be performed as part of a regular performance evaluation. It's important to continue assessing competency as the team member matures, providing "pulse points" in order to measure the effectiveness of training and development. As team members exceed the requirements of their given roles, it may be a sign that they're ready for promotion or participation in major or more challenging incidents (Stanton, Salmon, Jenkins, & Walker, 2010). Some organizations use formalized Competence Management Systems (CMS) to manage these results and track them with the needs of the team or SOC.

Competence assessment is important after completing training programs. Using a certificate of completion does not prove competence. Training improvement metrics can be achieved with organizational skill tests, college-developed exams, standardized certification exams, or "360" style assessments of skill using the input of the employee and surrounding team members.

8. Conclusion

SOCs provide a variety of services within an organization, including real-time monitoring, reporting, and incident-related analysis (Rothke, 2012). They play an important role in coordinating previously disjointed efforts to prevent, detect, and respond to information security incidents. According to an article in Dark Reading, "Tomorrow's SOC will spend more time on security analytics and less time on perimeter defense." (Wilson, 2010). With the increasing automation of network defense systems, the need for coordinated response and nuanced, contextual analysis is growing. Having a well-qualified staff to analyze, evaluate, and respond to security threats in an ever-changing environment is critical to success. The first step to finding well-qualified staff is to define team roles clearly and cohesively.

As job roles were collected, it became evident the agreement on job titles and the division of SOC-related work is still underway. As one commenter mentioned in the survey, "I've noticed that the computer security field has yet to settle on some vocabulary and team roles. For example, some companies have a SOC in their CIRT, and others have a CIRT in their SOC. And my company has a separate team that does security engineering […] apart from IR."

Despite the range of staff configurations, several sets of tasks emerged as common roles in SOCs, each role present in at least a third of SOCs surveyed: Security Analysts, Security Engineers, Managers, Specialists, and Supervisors. The core tasks associated with those roles enable the smooth operation of a SOC, in turn supporting the security posture of an organization. Fledgling SOCs can use these titles, core tasks, and requirements as an initial guide for the design of roles, adjust them to account for a specific SOC environment and the organizational security objectives, and compare the roles to SOC processes and use cases to ensure adequate coverage.

As roles are designed and fulfilled, it is important to account for continual skills development and assessment to ensure that both individuals and teams can perform at a high level of competence. Successful SOCs include effective policies, technologies, and people. A competent, responsive SOC staff with clearly defined responsibilities is in a better position to prevent, detect, and respond to incidents.

References

Anderson, B. (2013, July 17). *Building, Maturing & Rocking a Security Operations Center*. Retrieved from sans.org: https://digital-forensics.sans.org/summit-archives/DFIR_Summit/Building-Maturing-and-Rocking-a-Security-Operations-Center-Brandie-Anderson.pdf

Appelbaum, S., & Santiago, V. (1997). Career Development in the Plateaued Organization. *Career Development International*.

Daudelin, A. (2014, 01 21). *Dark Reading*. Retrieved from darkreading.com: http://www.darkreading.com/compliance/hipaa-sox-and-pci-the-coming-compliance-crisis-in-it-security/d/d-id/1113516

Dillon, S. (n.d.). *The Purpose of Internal Training for Employees*. Retrieved from Houston Chronicle: http://work.chron.com/purpose-internal-training-employees-3973.html

Ernst & Young. (2013, October). *Security Operations Centers against cybercrime: Top 10 considerations for success*. Retrieved from ey.com: http://www.ey.com/Publication/vwLUAssets/Security_Operations_Centers_against_cybercrime_-_Top_10_considerations_for_success/$FILE/EY_Security_Operations_Centers_against_cybercrime.pdf

HP Enterprise Security. (2011, August). *Building a Successful Security Operations Center*. Retrieved from hp.com: http://h71028.www7.hp.com/enterprise/downloads/software/ESP-BWP014-052809-09.pdf

McAfee "Foundstone" Professional Services. (2013). *Creating and Maintaining a SOC*. Retrieved from mcafee.com: http://www.mcafee.com/us/resources/white-papers/foundstone/wp-creating-maintaining-soc.pdf

Nathans, D. (2015). *Designing and Building a Security Operations Center*. Waltham, MA: Elsevier.

Rothke, B. (2012). *Building a Security Operations Center (SOC)*. Retrieved from RSA Conference: http://www.rsaconference.com/writable/presentations/file_upload/tech-203.pdf

Stanton, N. A., Salmon, P., Jenkins, D., & Walker, G. (2010). *Human Factors in the Design and Evaluation of Central Control Room Operations*. Boca Raton, FL: Taylor & Francis Group.

Swift, D. (2010, November 24). *SANS Reading Room*. Retrieved from sans.org: http://www.sans.org/reading-room/whitepapers/compliance/compliance-primer-professionals-33538

United States Office of Personnel Management. (2008, September). *Best Practices: Mentoring*. Retrieved from opm.gov: http://www.opm.gov/policy-data-oversight/training-and-development/career-development/bestpractices-mentoring.pdf

Wang, J. (2010). *Anatomy of a Security Operations Center*. Retrieved from nasa.gov: http://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20110011188.pdf

Wilson, T. (2010, November 22). *SOC 2.0: A Crystal-Ball Glimpse of the Next-Generation Security Operations Center*. Retrieved from Dark Reading: http://www.darkreading.com/soc-20-a-crystal-ball-glimpse-of-the-next-generation-security-operations-center-/d/d-id/1134811?

Zimmerman, C. (2014). *Ten Strategies of a World-Class Cybersecurity Operations Center*. Bedford, MA: The MITRE Corporation.

Appendix A. Survey Results

The survey was issued in March of 2015, and concluded with 56 respondents.

Q1. Which of the following categories best describes your employer?

Answer	Responses	%
Academic / Education	7	13.21%
Banking	0	0%
Business Services / Consulting	4	7.55%
Communications / Media	0	0%
Construction / Construction Supply	0	0%
Energy / Non-Petroleum	1	1.89%
Financial Services	4	7.55%
Government (non-military)	2	3.77%
Health Services	1	1.89%
Hospitality / Travel	2	3.77%
Insurance	3	5.66%
Manufacturing	4	7.55%
Non-profit	1	1.89%
Petroleum	2	3.77%
Pharmaceutical / Biotech	0	0%
Real Estate	1	1.89%
Retail	2	3.77%
Software - Info. Sec.	2	3.77%
Software - Non Info. Sec.	1	1.89%
Technology - Info. Sec.	9	16.98%
Technology - Non Info. Sec	2	3.77%
Utility	2	3.77%
Whole / Distribution	0	0%

Q2. Which of the following best describes your organization's SOC?

Answer	Responses	%
Staffed by our organization's employees (in-house)	32	58.18%
Employed by another organization (outsourced)	2	3.64%
A blend of in-house and outsourced staff	12	21.82%
We provide SOC(s) to other organizations as a managed service	9	16.36%

Q3. What is the size of your SOC in terms of staff?

Answer	Responses	%
Fewer than 5 people	12	21.43%
5-10 people	12	21.43%
11-15 people	8	14.29%
16-20 people	6	10.71%
More than 20 people	17	30.36%
Not sure	1	1.79%

Q4. How long has your SOC been in operation?

Answer	Responses	%
Less than one year	11	19.64%
1-5 years	27	48.21%
More than 5 years	17	30.36%
Not sure	1	1.79%

Q5. What is the relative operating budget of your SOC?

Answer	Responses	%
Less than $100,000	9	16.36%
$100,000 - $499,999	7	12.73 %
$500,000 - $999,999	4	7.27%
$1 million - $3 million	8	14.55%
Over $3 million	8	14.55%
Not sure	19	34.55%

Q6. Review the following list of roles. To your knowledge, which of these roles does your SOC employ? The titles might not match perfectly, so select the ones that most closely match the roles in your SOC.

Answer	Responses	%
Security Analyst	43	79.63%
Manager	34	62.96%
Security Engineer	31	57.41%
Specialist	19	35.19%
Supervisor	18	33.33%
Director	17	31.48%
Network Security Engineer	17	31.48%
Operator	15	27.78%
Security Administrator	12	22.22%
Software or Application Engineer	10	18.52%
Metrics or Data Analyst	9	16.67%
Technical Writer	4	7.41%

Q7. Are there any important roles in your SOC that were not included in the list? (text field)

- Threat Intelligence Analyst (4 respondents)
- Security Architect (3 respondents)
- Incident Responder (3 respondents)
- Forensics specialists (2 respondents)
- Team lead (2 respondents)
- Windows and Unix Administrators
- All other roles are outsourced
- Project manager
- Solutions Architect
- Vulnerability Management Analyst
- In the future, we may add a Detection Analyst (someone whose job it is to create more and better detection methods).
- SIEM Engineer

- Software Developer
- IDS Engineer
- Compliance Officer
- Security Researcher
- Penetration Tester

Q4. Are there any roles listed you consider redundant? (text field)

- Manager & Director
- Manager & Supervisor (3 respondents, though one noted this may differ in a union shop)
- Security Engineer & Network Security Engineer (3 respondents)
- Operator, Specialist, and Security Engineer
- Operator & Security Analyst
- Specialist & Security Analyst
- Security Administrator
- "Can never have too many eyes on the bad guy"

Q5. Does your SOC use a multi-tier support / escalation system (eg. SOC Engineer Level 1, 2, or 3)?

Answer	**Responses**	**%**
Yes	38	70.37%
No	15	27.78%
Not sure	1	1.85%

Q6. Which areas do you view as the primary focus of your organization's SOC?

Answer	Responses	%
Monitoring & detection	52	94.55%
Response	38	69.09%
Prevention	18	32.73%

Additional free-form comments: Cyber/threat intelligence, Containment

Q7. Which areas does your organization include within the scope of the SOC?

Answer	Responses	%
Monitoring	47	87.04%
Detection	47	87.04%
Incident Response	40	74.07%
IDS	38	70.37%
Forensics	29	53.70%
IPS	28	51.85%
Penetration Testing and/or Vulnerability Assessment	23	42.59%
Firewalls	21	38.89%
Hardening	14	25.93%

Additional free-form comments: Malware analysis (2), threat intelligence (2), Data Loss Prevention, Secure Email Gateway, Web Proxy, Supporting/Coaching Engineers, Business/paper based security

Q8. Does your organization have plans to increase the size or scope of its SOC, now or in the near future?

Answer	Responses	%
Yes	32	58.18%
No	14	25.45%
Not sure	9	16.36%

Q9. - Q11. Collection of demographics and additional contact information

[Results not shared due to a privacy statement that the survey will not release potentially identifying information of respondents.]

Q12. Do you have any other comments, questions, or concerns? (text field)

- You are smart!
- It would be nice to include SOC hours - 8x5, 24x7, 10 or 12 hour days, etc. Ours is staffed 8x5 currently.
- Good luck!
- I've noticed that the computer security field has yet to settle on some vocabulary and team roles. For example, some companies have a SOC in their CIRT, and others have a CIRT in their SOC. And my company has a separate team that does security engineering (firewall, web filtering, etc.) apart from IR.

Last Updated: April 23rd, 2018

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Riyadh April 2018	Riyadh, SA	Apr 28, 2018 - May 03, 2018	Live Event
SANS SEC460: Enterprise Threat Beta Two	Crystal City, VAUS	Apr 30, 2018 - May 05, 2018	Live Event
Automotive Cybersecurity Summit & Training 2018	Chicago, ILUS	May 01, 2018 - May 08, 2018	Live Event
SANS SEC504 in Thai 2018	Bangkok, TH	May 07, 2018 - May 12, 2018	Live Event
SANS Security West 2018	San Diego, CAUS	May 11, 2018 - May 18, 2018	Live Event
SANS Melbourne 2018	Melbourne, AU	May 14, 2018 - May 26, 2018	Live Event
SANS Northern VA Reston Spring 2018	Reston, VAUS	May 20, 2018 - May 25, 2018	Live Event
SANS Amsterdam May 2018	Amsterdam, NL	May 28, 2018 - Jun 02, 2018	Live Event
SANS Atlanta 2018	Atlanta, GAUS	May 29, 2018 - Jun 03, 2018	Live Event
SANS London June 2018	London, GB	Jun 04, 2018 - Jun 12, 2018	Live Event
SANS Rocky Mountain 2018	Denver, COUS	Jun 04, 2018 - Jun 09, 2018	Live Event
SEC487: Open-Source Intel Beta Two	Denver, COUS	Jun 04, 2018 - Jun 09, 2018	Live Event
DFIR Summit & Training 2018	Austin, TXUS	Jun 07, 2018 - Jun 14, 2018	Live Event
Cloud INsecurity Summit - Washington DC	Crystal City, VAUS	Jun 08, 2018 - Jun 08, 2018	Live Event
SANS Milan June 2018	Milan, IT	Jun 11, 2018 - Jun 16, 2018	Live Event
Cloud INsecurity Summit - Austin	Austin, TXUS	Jun 11, 2018 - Jun 11, 2018	Live Event
SANS Crystal City 2018	Arlington, VAUS	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS Cyber Defence Japan 2018	Tokyo, JP	Jun 18, 2018 - Jun 30, 2018	Live Event
SANS ICS Europe Summit and Training 2018	Munich, DE	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS Philippines 2018	Manila, PH	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS Oslo June 2018	Oslo, NO	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS Cyber Defence Canberra 2018	Canberra, AU	Jun 25, 2018 - Jul 07, 2018	Live Event
SANS Minneapolis 2018	Minneapolis, MNUS	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS Vancouver 2018	Vancouver, BCCA	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS Paris June 2018	Paris, FR	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS London July 2018	London, GB	Jul 02, 2018 - Jul 07, 2018	Live Event
SANS Charlotte 2018	Charlotte, NCUS	Jul 09, 2018 - Jul 14, 2018	Live Event
SANS Cyber Defence Singapore 2018	Singapore, SG	Jul 09, 2018 - Jul 14, 2018	Live Event
SANSFIRE 2018	Washington, DCUS	Jul 14, 2018 - Jul 21, 2018	Live Event
SANS Malaysia 2018	Kuala Lumpur, MY	Jul 16, 2018 - Jul 21, 2018	Live Event
SANS Cyber Defence Bangalore 2018	Bangalore, IN	Jul 16, 2018 - Jul 28, 2018	Live Event
SANS Doha 2018	OnlineQA	Apr 28, 2018 - May 03, 2018	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced