Table of Contents

What Is a SOC? ................................................................................................................................. 3
Typical SOC Functions .................................................................................................................... 3
Growing a SOC ................................................................................................................................ 5
Common SOC Approaches in Higher Education ........................................................................ 7
  Outsourcing the SOC................................................................................................................... 7
  Hybrid........................................................................................................................................ 8
  Sharing a SOC ............................................................................................................................ 9
  Building an In-House SOC .................................................................................................... 10
  Limited-Budget Approaches .................................................................................................... 10
    Using Student Staff .................................................................................................................. 10
    Limiting Service Hours of the SOC ...................................................................................... 11
  Mix and Match............................................................................................................................ 12
Process Improvement ..................................................................................................................... 12
Summary .......................................................................................................................................... 14
Acknowledgments .......................................................................................................................... 14
Additional Resources...................................................................................................................... 15
Higher education institutions are beginning to organize operational security into security operations centers to monitor and respond to security incidents as a means to improve efficiency. If you are considering establishing your own or outsourcing some or all of these functions, this paper highlights important steps and deliberations. This paper was prepared by members of the Higher Education Information Security Council (HEISC). Learn more about HEISC and the EDUCAUSE Cybersecurity Program.

What Is a SOC?

A security operations center (SOC) is a dedicated monitoring, assessment, and defense facility that responds to real-time information security anomalies and events. A SOC is typically staffed with security analysts, security engineers, subject-matter experts (SMEs) such as threat hunters and forensic analysts, and other support personnel as needed. The success of a SOC depends on trained personnel, security monitoring tools, and clear response processes. Higher education institutions are increasingly deploying SOCs as part of their overall information security program.

Which specific components and capabilities are populated in a SOC depends on the institutional and operational requirements identified by the sponsoring organization, usually the institution’s information security department. Different institutions have different business requirements, risk profiles, and budgets, all of which are important considerations when implementing a SOC.

Typical SOC Functions

Before we get into a description of the different SOC components, it is worth noting that your information security program might already utilize many of the tools listed below or your teams might already perform many of these functions. This is good because you will have less heavy lifting to do if that is the case. It is important to approach looking at a SOC as a means of organizing your security operations for maximum efficiency.

A key component and basic building block of a SOC is network security monitoring (NSM.) This is a focused collection of tools and processes that keep a
watchful eye on the security infrastructure and alerts when potential security threats are detected. In some cases, especially in shared or outsourced SOC situations, these types of monitoring tools may constitute the entirety of an institution’s security operations stance. SOC specialists watch the NSM software for abnormalities that could indicate the presence of an intruder, malware infections, or other security threats. Other commonly used tools include intrusion detection and prevention systems; antivirus (AV) management systems; firewall, server, and router logs; and network flow streams. NSM tools rely on security information event and management (SIEM) software to aggregate security notifications into a format suitable for human interpretation and reporting.

Once an event is determined to be a potential security issue, a computer security incident response team (CSIRT) springs into action. The goals of the CSIRT are to

- minimize or halt any ongoing damage caused by the incident,
- determine the extent of the damage through analysis, and
- lead the organizational response to the incident.

In addition to providing a real-time response to security incidents, the CSIRT is also responsible for conducting a post-incident review to improve future responses to similar incidents, as well as to inform and expand on any identified weaknesses in existing defensive capabilities. An incident response team (IRT) could include network SMEs, application and server SMEs, and digital forensics specialists.

Many established SOCs are now adding a proactive security assessment capability to their existing portfolio of information security detection and countermeasures. Security assessment teams specialize in vulnerability assessment, penetration testing, white-hat hacking (ethical hacking to identify potential security issues and correct, not exploit, them), and measuring the effectiveness of configuration management within IT. Assessments also include red (attacker)/blue (defender) team exercises to measure the effectiveness of the SOC and related IT teams within the organization.

As SOCs mature, they may also develop a threat-intelligence capability that tracks specific threats to the organization’s environment, identifies and monitors specific threat actors, and provides operational intelligence to other IT teams to help improve response and shore up protections. One thing that the proliferation of cyberthreats has made clear over the past ten years is that the threats tend to evolve as the detection and protection tools get more effective at detecting and stopping those threats. Cybersecurity is thus an ongoing process, not a goal to be
achieved. The motto of a SOC should be *semper vigilis*, ever vigilant, because security threats never take a day off.

**Growing a SOC**

One of the first considerations in whether and how to implement a SOC is the maturity level of the institution’s information security program as a whole. A security program that struggles to manage day-to-day tasks, for whatever reason, should think very carefully about whether adding the increased workload of rolling out a SOC is a wise move until the underlying organizational issues have been rectified.

There is no single “right” way to build an effective SOC. Depending on staffing resources, budget, available physical space, and the amount of time allotted, an organization can pursue one of several approaches to implement a SOC. Many higher education information security programs still tend to be budget constrained, even though university leadership is beginning to emphasize information security as an institutional priority. Being able to balance the organization’s need for information security monitoring and response with the available resources is the key to a successful SOC implementation.

Here are some best practices you can use when evaluating your readiness for a SOC and the implementation steps that are typically required.

- Assess the current maturity level of your organization’s information security program and determine how a SOC would (and should) change the way you do business.

- Design operational parameters based on need balanced against resource commitments/constraints; a high-throughput organization with bigger compliance needs will generally need all of the SOC functions.

- Don’t try to start everything at once. Start with NSM, then layer the other functions above as you mature. This said, once you do bring up NSM, a strong IRT function will soon need to follow.

- You might also discover you are more mature in one area, such as vulnerability assessment and penetration testing. If so, this seems a natural move to incorporate these functions earlier into the SOC. Know what’s available, and plan accordingly.
Select a staffing model:

- **Full-time professional staffing:** This can be the most expensive option, depending on desired hours of operation as well as current staffing levels and capabilities. But establishing a SOC can be great from an organizational standpoint—a way of focusing your operations into an interconnected whole. This is where some efficiency can be gained.

- **Mixed:** This includes full-time professional staffing and part-time student staffing. For some, the dream of staffing a SOC would be fiscally out of reach but for the force multiplier offered by student populations. Find students who are interested in pursuing cybersecurity as a career, and this can be a great match.

- **Outsourced SOC/managed security services:** While most of the commercial services might be out of reach for many institutions, we’re starting to see multi-institution collaborations spring up, making the dream of having SOC functions available at reduced cost a reality.

- **Hybrid:** This can be a mix of any of the above. For example, an institution could have a SOC 8:00 a.m. to 5:00 p.m., Monday through Friday, that is supplemented by outsourced network security monitoring on evenings and weekends to get the 24/7 coverage desired. Throw in a couple of interns working on special projects over the summer and you’ve managed to capture all three.

Budget-wise, determine what the organization can afford in terms of dedicated daily coverage of SOC duties. Few organizations starting a SOC jump directly to 24/7 operations. A full-time SOC requires assigned shifts and additional staff. Be sure to include staff turnover in your budget and time planning for the new SOC.

A phased approach to implementing a full-time SOC could look like this:

- Begin with weekday business hours.
- Expand to covering 12 hours per weekday by staggering shifts (most active hours).
- Extend by supplementing coverage hours with student employees/interns.
- Expand to three shifts covering 24 hours, Monday through Friday.
- Implement full-time or hybrid staffing, 24/7/365.

Regardless of the staffing structure, common SOC planning activities include the following:

- Define and implement documentation processes and procedures.
- Develop a staffing plan to transfer existing staff resources, hire new SOC analysts, or leverage third-party services to help staff the SOC.
• Create an onboarding process that defines analyst access to tools, escalation trees, etc. The onboarding process should list specific action items for new SOC staff that includes activities for day one, week one, month one, and so forth.

• Include new-hire training on confidentiality and compliance, reporting requirements, traffic-light protocols, emergency communications, and other areas.

Common SOC Approaches in Higher Education

Due to the unique budgeting and financial challenges found in many higher education IT organizations, choosing a SOC implementation approach and strategy can be challenging. Looking at each of the implementation options in more detail helps organizations match the best approach to their specific maturity level, budget, timeline, and staff skill sets.

Outsourcing the SOC

Fully outsourcing SOC operations is by far the quickest way to implement a SOC. It is also likely the most expensive route to getting your SOC up and running in the shortest time. That said, many organizations start with a third-party SOC provider as a way to kickstart their SOC activities. Advantages of this approach include, obviously, the quickest realization of SOC information security protection and benefits; the ability to have the third-party SOC provider provide elasticity of staff as needs or demand changes; and providing the least amount of staffing pain for the sponsoring IT organization. Disadvantages of outsourcing include the following:

• The sponsoring IT organization loses situational awareness, as far as SOC operations are concerned.

• A large portion of the SOC startup tuning process and information security procedures definition will go to training the third-party employees rather than internal staff.

• SLA compliance and incident response times must be closely monitored to ensure the third-party SOC provider is addressing information security alerts and proactive activities in a timely manner.

One university contracted with a major vendor to get from the ground to a functional SOC in a short, compliance-driven time frame. The vendor was originally tasked with monitoring logs and alerting the security team, but in a high-noise environment, the vendor-provided “actions” overwhelmed the onsite
team. Clearly a service mismatch for the scope and complexity of the higher education IT environment, the service was terminated because the vendor did not understand the business model. It may have worked for a “locked down” environment, but did not provide sufficient value to the higher education CISO to warrant continuation. Key lessons learned:

- Ensure internal SOC processes are well documented so that tasking can clearly be matched with a vendor.
- Security teams need to be able to ensure that contracts for security services are clearly written and understood by the vendor and are therefore enforceable.
- Ensure that the cultural aspects of the IT environment at your institution are accounted for in the service agreements, such as whether the vendor will communicate with IT operations or the information security teams only.

The next step for this university is the pursuit a hybrid model SOC service.

**Hybrid**

Georgia Institute of Technology utilizes a hybrid model SOC that is staffed by six student analysts and two full-time employees, one of whom serves as handler-on-duty at any given time. Their coverage hours are 8:00 a.m. to 5:00 p.m., Monday through Friday. Georgia Tech’s SOC focuses on security incident response and vulnerability assessment. Unique to this model, the student analysts handle all communications with university IT staff.

Seton Hall University started the process to implement a SOC using its vendor that implemented an in-house SIEM (Splunk ES). Eventually the university pivoted to a smaller, more agile Splunk vendor for reasons of expertise and cost, and this is a solid example of a hybrid SOC model. In particular, the vendor monitors SIEM alerts off-hours and then escalates to the internal team, which consists of two full-time employees and ten student workers. Seton Hall also offers an undergraduate certificate in cybersecurity, so this ensures a pipeline of students who are taught basic Splunk elements and monitoring for “red” events. Additionally, the university has expanded its monitoring and alerting with an endpoint security vendor, which is using a fully managed suite, intervenes in user-device infections, and even performs some threat hunting.

Over a two-year period, Yale University moved its in-house intrusion detection work to a hybrid SOC model. Tier 1 activities are split between the in-house help desk, DC OPS team, and an outsourced security vendor, while their Tier 2– and Tier 3–level work escalates to in-house Information Security staff. Two years ago,
this staff consisted of five analysts actioning all tickets within a 24/7 model. Recognizing that this was not a sustainable model, the team sought a creative solution. They connected with a smaller “boutique” vendor to augment their efforts overnight (5:00 p.m. to 7:00 a.m.), on weekends, and during school breaks. The vendor initially helped optimize and improve workflows and playbooks for routine actions, identify and streamline redundant work, define new plays, and consolidate existing processes. As processes improved, the vendor started actioning “daytime” Tier 1 work. This permitted Yale to give its operations team more advanced problems to solve, which aligned with the strategic objectives of the program. To manage the process, the institution implemented a regular quality assurance (QA) review of service tickets and security requests, allowing for playbook optimization, vendor training, and continuous improvement of the process. Next steps are to think about how they can automate actions and reduce the number of tickets sent to the hybrid SOC, which will allow for new work to take the place of automated Tier 1 activities. A long-term plan is for the vendor or internal support groups to become a primary point of intake for security-related issues.

Sharing a SOC

One example of a shared SOC environment is OmniSOC, a recent collaboration between five institutions: Indiana University, Northwestern University, Purdue University, Rutgers University, and the University of Nebraska. The founding members are looking for cost savings and to share information security intelligence—both the digital and the human varieties—among institutions and staff facing similar information security threats. A collective SOC with expenses distributed among multiple sponsoring institutions and knowledge disseminated among shared SOC staff has a better chance of finding and retaining high-caliber information security professionals to manage the shared SOC. So far, the shared SOC experiment is proceeding well. Participation has been open since early 2019 for other similarly sized (large) institutions, both inside and outside of the Big Ten Academic Alliance. OmniSOC management is actively working on a strategy to accommodate smaller and mid-sized colleges and universities by early- to mid-2020 since the need for such a service is important to institutions of every size. If successful, the OmniSOC will help demonstrate that shared SOCs are a practical, fiscally sound alternative to the cost and complexity of implementing an in-house SOC.

CyberPosse is another example of a shared SOC-as-a-service offering that provides colleges and universities with extended support capabilities, including managed detection and response services. The University of Texas at Austin
Information Security Office has been providing these services to a large customer base since 2009, offering extended coverage and protection to 15 campuses in the University of Texas System; 77 independent school districts, small colleges, municipalities, and hospitals; and dozens of state agencies. CyberPosse is a proven and reliable service for institutions needing to augment, optimize, or accentuate their existing cybersecurity program.

**Building an In-House SOC**

Building a full-time SOC in-house avoids the main disadvantages of the outsourcing model because rather than training external staff on SOC procedures and activities, the institution leverages and develops internal expertise as part of the SOC implementation process. A SOC developed in-house also has much more control of the operational means and methods for providing the required level of information security expertise. Using only in-house staff for a SOC also provides an important career path for internal employees who are interested and are driven to develop their information security skills and knowledge.

One disadvantage of developing a SOC using only in-house staff is the managerial—and financial—overhead of hiring, developing, coaching, and mentoring internal staff as you would any other employee. Another significant disadvantage is that, with cybersecurity skills in such high demand, organizations will struggle to find—and retain—qualified SOC staff. That said, if building a strong knowledge base of SOC capabilities and information security skill sets using in-house talent is an organizational imperative, building that expertise via in-house hires and development may be the best option available.

**Limited-Budget Approaches**

Several additional options are available to the intrepid SOC manager that can be leveraged in specific situations to address and offset the disadvantages of outsourcing or insourcing your SOC staff. None of these is a cure-all for the challenges of building a new SOC, but all deserve consideration as stand-alone or hybrid techniques to reach SOC nirvana.

**Using Student Staff**

Using students to augment existing SOC staff, whether outsourced or insourced, can be a way to cut costs. Students pursuing cyber-related degrees can work in the SOC to build their information security experience and cybersecurity bona fides.
Students might be employed as relatively low-cost hourly workers, or they might be able to participate as interns in a cybersecurity training program that includes operational work in the live SOC environment.

Many teams have successfully integrated students as SOC staff. While great for the students and great for the cybersecurity programs at an institution, this approach does require careful planning. Student interns or employees will, by definition, be pursuing their studies while working in and around the SOC. As such, managers will have to take the extra time required to schedule around other academic pursuits such as exams or class projects. Staff turnover may be higher than with an outsourced or insourced SOC staffing model, given that students will hopefully graduate within a reasonable amount of time. With this turnover comes the need for more formalized training, better documentation, and a clear delineation of access, capabilities, and responsibilities. While student staff may increase the amount of structure and daily guidance required, working to develop the next generation of infosec professionals is frequently a source of work satisfaction for the permanent staff.

Charles Leggett leads such a program at Georgia Tech. That institution’s SOC has an extensive knowledge base of procedures, combined with a good deal of over-the-shoulder training and monthly all-hands meetings. But one area typically needs more work, he finds. “When the students first start working here, they are not really confident,” Leggett noted, and in some cases, it can take almost a year to get them there. Overall, he finds that student employees are dependable and that “they are adults and employees” and should be treated as such.

Limiting Service Hours of the SOC

Staffing a SOC only during peak demand hours—typically 8:00 a.m. to 5:00 p.m., Monday through Friday—is another useful technique to reduce the cost of SOC operations. This limitation greatly reduces the staffing requirements and allows all employees to work a day shift. But considering that information security never sleeps, the SOC must still have a method for monitoring cybersecurity alerts and providing a timely response regardless of when an incident occurs. The after-hours time periods can be covered by an on-call staff member who can accept, address, and escalate SOC alerts as needed.

It is amazing how quickly our students transition from “hourly student employee” to “security analyst.” Since we’re partnered with our cybersecurity program, they come in knowing the basics and now get to apply that knowledge to real-world scenarios. If anything, one of our biggest issues is making sure they don’t go over their scheduled hours each week, as they are so engaged and excited about what they’re doing.

—David Nevin, Director, Oregon Research & Teaching Security Operations Center at Oregon State University
The after-hours shifts could also be covered by an outsourced SOC provider. This gives the SOC a reliable method of monitoring security-related events during the times that the internal SOC is not staffed, with the added expense and training requirements necessary with a third-party provider. Many organizations start their SOC by having in-house staff available during peak hours only, then gradually transition the outsourced SOC shifts back to in-house staff as budget and training allow.

**Mix and Match**

As described in the various options and approaches outlined above, there is no right or wrong way to plan, implement, and manage a new SOC. Every organization has different budgets, internal staff capabilities, goals, and priorities, so some combination of the above approaches may be the most appropriate course of action. Also, remember that going down one path to initiate your SOC doesn’t mean that a different approach might not be more suitable at some point in the future. Perhaps you start with in-house and student staff working only during peak hours, with on-call or third-party coverage during off hours. That arrangement could transition gradually or suddenly to more coverage hours by in-house and fewer hours of outsourced SOC staff. Take all of the variables into account as you devise a short-term, medium-term, and long-term SOC strategy that makes the most sense for your particular organization and situation.

**Process Improvement**

When developing metrics for your SOC, it is important to consider the key reasons for implementing a metrics program. Metrics help facilitate process improvement, track progress to goals and objectives, and convey the value of the SOC to outside groups like campus leadership. Consider implementing a daily or weekly SOC update newsletter—or a SOC status and reporting website—that gives all interested stakeholders visibility into the latest activities of the SOC. Visibility and recognition of SOC activities increase staff morale, provide ongoing SOC justification to IT and campus leadership, and help promote information security principles and activities among all stakeholders.

There are a number of resources available to help you understand what information security metrics are and how to create and use them. The following examples provide a starting point as you develop metrics for your SOC:
Limit the number of measures. When determining what metrics to use and how to gather them, resist the temptation to try to measure everything and "boil the ocean" just because you can. The fact that something can be measured does not mean it should be. Instead, tie one outcome measure to each of the SOC’s goals and objectives. Too many metrics will lead to confusion and can result in putting more effort into collection than into the analysis.

Limit the number of changes to what you measure. Once you have identified core metrics and determined how they map to the SOC’s progress toward goals, the next aspect to consider is the stability of what and how you measure. As with other processes, cycles of improvement need to be accommodated, but with metrics the time between these improvement cycles should not be rushed. If how or what you measure is constantly changing, the metric cannot provide accurate trending over longer periods of time, rendering it useless for tracking effectiveness or progress.

Fully understand your metrics. Metrics are valuable because they help you better understand your SOC operations and whether your SOC is meeting its goals. But the answers metrics provide are not always clear-cut. You might implement a measure to track certain aspects of your SOC, believing it will drive efficiency in the organization, and yet the end result could turn out to be something you did not anticipate. Oftentimes metrics can illustrate potential pain points in SOC operations. Take the time to review the metrics describing your program, particularly those metrics that may indicate potential areas of concern. Do you understand how those metrics were calculated and any anomalies that might cause that metric to be viewed with suspicion? Can you describe the metrics to various audiences and why they are important? And, are you prepared to act upon any areas of concern that your metrics indicate?

Ensure that metrics are not punitive. As your metrics program is being executed you should ensure the measures will be used for process improvement and not be punitive in nature. When people believe that metrics are being used in a punitive or negative manner (as the basis for a performance review rating, for example), they will tend do what they need to do to ensure that the metric is recorded in the most favorable way possible. Any type of gamesmanship could come at the expense of doing what is right for the institution. Ensuring that SOC metrics are not treated as individual employee goals or measures can help alleviate this problem.
Summary

Information security threats are becoming ever more prevalent and continue to evolve as quickly—or perhaps more quickly—than countermeasures can adapt to them. Institutions can no longer afford to wait or analyze any further; having a proactive plan to protect institutional data and users is now a must. As a result, higher education institutions are increasingly deploying SOCs as part of an overall information security program.

That said, not every institution has the capacity or security program maturity (or can afford) to build its own SOC from scratch. If the institution’s information security program is not mature enough to establish and operate a SOC, then getting to that maturity level should be job one. If the maturity level is sufficiently advanced but there is no budget with which to establish a SOC, then securing funding for the SOC should be a priority. But neither of those activities allows an institution to postpone aggressively addressing information security threats while maturity and finances are addressed. Using students to staff the SOC or outsourcing your SOC to a third party are viable methods to get around both the maturity and fiscal roadblocks. And the promising development of shared SOCs is also a great way to share the financial burden as well as grow institutional knowledge intrinsic in a SOC. Whatever the eventual real-time information security solution ends up being is up to each institution, but not providing SOC-like services on campus is no longer a workable strategy. The stakes are just too high.

Acknowledgments

This paper was prepared as a group effort by a number of higher education professionals passionate about evolving SOC practices. We hope you find this resource useful in establishing and improving your institution’s SOC.

- Tom Davis (Indiana University)
- Scott Fendley (The University of Alabama at Birmingham)
- Earl Follis (Vantage Technology Consulting Group)
- Joanna Lyn Grama (Vantage Technology Consulting Group)
- Brian Kelly (EDUCAUSE)
- Mike Maltbie (Case Western Reserve University)
Security Operations Center Case Study

- Dave Nevin (Oregon State University)
- Tom Siu (Case Western Reserve University)
- Valerie Vogel (EDUCAUSE)
- Paul Walker (The University of Alabama at Birmingham)

Additional Resources

- CyberPosse: A SOC-as-a-Service for Higher Education (hosted by the University of Texas, Austin)
- A Guide to Effective Security Metrics
- Budget-Conscious Information Security Resources

About EDUCAUSE

EDUCAUSE is a higher education technology association and the largest community of IT leaders and professionals committed to advancing higher education. Technology, IT roles and responsibilities, and higher education are dynamically changing. Formed in 1998, EDUCAUSE supports those who lead, manage, and use information technology to anticipate and adapt to these changes, advancing strategic IT decision making at every level within higher education. EDUCAUSE is a global nonprofit organization whose members include U.S. and international higher education institutions, corporations, not-for-profit organizations, and K–12 institutions. With a community of more than 99,000 individuals at member organizations located around the world, EDUCAUSE encourages diversity in perspective, opinion, and representation. For more information please visit educause.edu.

© 2019 EDUCAUSE. Creative Commons BY-NC-ND 4.0.