CHAPTER

Infrastructure 3

CHAPTER CONTENTS

When building a SOC, you not only need to think about all the security tools, systems, and infrastructure needed to protect your organization but you also need to think about all that is needed to support the center as well as the infrastructure the team is going to use to do its job. There are three specific and distinct areas of infrastructure that you must look at when planning your SOC.

- Support infrastructure

This infrastructure is really your SOC's eyes, ears, nose, and throat. These are all the things a SOC needs in order to be able to maintain access to and interact with all the other infrastructure devices, assets, and tools. If required, this will also contain the needed systems to maintain visual representation of real-time statistics such as video walls and projectors so that the SOC can react and be sensitive to potentially negative statistic fluctuations. These are the items along with other physical equipment that you would mostly find inside the SOC being used by the staff.

- Organizational security infrastructure

This infrastructure consists of the technology that is needed to protect your organization. This includes all the items out in the wilds of your network that need tender loving care and need to be reviewed by experts to ensure nothing bad is going on. This is the nuts and bolts of your security footprint and can consist of many, many different types of technologies applied in many different ways all in the effort to protect your organizations confidentiality, availability, and integrity, the triad of security goals. Your SOC may own and manage all or some of these devices or may just be the recipient of the systems technical output or logs.

- Operation center infrastructure

This is where we are going to spend most of our time in this chapter. Infrastructure needed to support your SOC is vital to your organizations security success. There are a lot of things to consider, a lot of important tools to review, and there are many different philosophies on how to approach these different topics. Typically these are the things that the SOC needs to operate but may be installed at remote locations, inside a data center or somewhere outside the physical SOC location.

The first area that we need to address is obviously your organization's overall security infrastructure; this includes any IDS, firewalls, web proxy systems, antivirus, data loss prevention systems, and so on that the SOC might be using or are even responsible for maintaining, see Appendix B. Second you need to look at any special requirements for servers the SOC will need such as the ticketing systems, a security event management system or any other specialized tools needing separate servers. You also need to consider if the SOC will operate its own private protected network and what impact that will have. Lastly you need to think about all the equipment your analysts and engineers will need. This includes not only the Macs or PCs at their desktops but also any video projectors, special monitors, or even separate Internet connections. All three of these technical areas, organizational security infrastructure, SOC infrastructure, and SOC support infrastructure must be addressed when building your SOC.

ORGANIZATIONAL INFRASTRUCTURE > OPERATIONS INFRASTRUCTURE > SUPPORT INFRASTRUCTURE

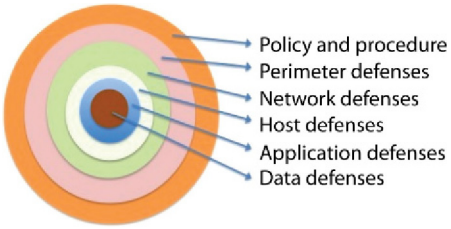
If you ever thought you could just sit back and wait for the screen to tell you something bad happened on your network or with a host system and have lights and sirens go off when someone accesses something they should not, then you are about to have a rude awakening. In most cases, there is no silver bullet to security that will show you an attack has taken place. Most times to catch the bad guy an analyst will need to be patient and also be very determined not to give up looking for that "needle in a hay stack" that will lead them to find security issues needing to be addressed. When it comes to building a SOC, it can be as simple as one person looking at an IDS all day long or it can be as complex as a disperse team of 2500 people all managing and maintaining hundreds of different types of devices around the world. In either case, large or small, you have to take into consideration the same three areas of infrastructure when you are building your SOC.

ORGANIZATIONAL SECURITY INFRASTRUCTURE

As defined above, the organizational infrastructure deployed at the enterprise level is the actual infrastructure you are going to use to protect all the required areas of your organization. These are the devices and technology that will be deployed across the entire enterprise in key locations that will perform the actual job of protecting, detecting, or stopping malicious behavior or attacks. This can be the firewall used at the perimeter or in your network or even at third-party companies and cloud service providers all the way to the antivirus software on a user's endpoint computer. When you look at a defense-in-depth approach to security, you will find many different systems that all need to be managed and monitored by trained security professionals to ensure they all work and are configured properly, they are being looked at and important alerts are being addressed. This section is not here to help you design or build the security of your network. Instead it is here for you to get a feeling, appreciate, or to help others understand the daunting task your SOC may face in managing and monitoring your organizations security. Some people believe that it is not a big deal to run a SOC, you just sit in front of the computer and read whatever the screen tells you and then call someone. I wish it was that easy because then we would not see so many data breaches in the news. When we look at a typical organizational security infrastructure, some people like to talk in terms of a defense-in-depth strategy because it is easy to break down the things needed for security into areas that will be deployed on the network infrastructure.

Let us take a quick look at some of the organizational security infrastructure that would be needed at various levels of that defense-in-depth strategy. This is not a complete or exhaustive list but rather just a sampling to help your thought process around what is really going to be needed by your SOC if you have to manage, maintain, or monitor all this stuff. Keep in mind that I am not going to explain the function of

these devices but rather how these technologies are viewed from a SOC perspective or how they would integrate, be managed by, or be utilized within your SOC.



PERIMETER DEFENSES

At your perimeter, there are a few different types of technologies that you may want to use. But first understand that the perimeter is where your organizations control and management stop and some other service provider, business partner, or untrusted connection begins. The security model here is to prevent as much getting into your network as possible and detect all that you can if you cannot specifically stop it.

The first type of device in this area that you may think of is a firewall. Firewalls are vital to a SOC, they can tell you a lot about what is going on and what is coming into your network. The logs from a firewall need to be collected and analyzed, they are where you are going to find performance issues related to denial of service attacks, attempts by systems to violate access rules or devices being denied access due to many other reasons. But it is not always what is being denied on your firewall that is important. You almost always need firewall logs to help you determine the real IP address of an external system that is accessing your network if you are using Network Address Translation. When you translate real routable internet addresses to internal non-Internet routable addresses, you have to have a way to lookup the relationship to determine who is doing what. Without your firewall logs, the SOCs task of translating back and forth is going to be nearly impossible.

Next, we can think about a VPN or remote access system, this is where members of the organization will connect from outside the network to access internal resources. It is vital to maintain this system to ensure appropriate access is granted to users and that when people leave or no longer need the access it is revoked or taken away. So, monitoring users that access this resource is very important but also looking at where someone is accessing the system from may be even more important. If you see someone logging into the VPN from half-way around the world but they are currently in the office and you just saw them getting a cup of coffee then you may have a problem. Your SOC should be able to utilize these basic systems to gain valuable visibility into what security issues may be impacting your organizations network perimeter and who may be getting unauthorized access. Of course there are many more devices like proxy servers you may find in the perimeter of your network but let us move on.

NETWORK DEFENSE

The next ring or layer deep in your defense strategy is the internal network. This is the internal portion of your organization that communicates together in potentially one or more different segments or areas. Security-relevant items you will typically find here are things like intrusion detection or prevention systems, network access control (NAC) systems, along with data loss prevention systems and behavioral or anomaly detection systems. IDSs should be set up wherever there is a network segment that can communicate with another network segment and data traffic passes between those two different networks or areas. This will act like a choke point and allow you to see all the network traffic that are successfully passed and evaluated by signatures internal to the IDS and determined if anything was bad or not. This could be traffic such as hackers trying to exploit vulnerabilities. The output of the IDS is vital for the SOC to review and evaluate but to also manage and to keep the system updated with the latest signatures to detect bad network traffic. NAC systems are also great at helping to prevent systems that are not owned by the organization to connect to an internal network. The SOC should keep a close eye on the changes to a network and what devices are connected or not connected. An attacker does not need to be outside the network in some far off place, they could be inside an organization's own four walls trying to get access to data and resources or they could be from an unattended conference room. Logs and alerts from these types of systems are important information that should be collected and analyzed by the SOC, this could also include systems that attempt to connect to any wireless networks or try to impersonate the real wireless network the organization is running.

HOST DEFENSES

Quickly thinking about host defenses you would want your SOC to manage and monitor would include systems like antivirus, device controls for USBs or host-based data loss prevention systems. When antivirus software detects the presence of a virus there are a number of things that happen, one of which is hopefully cleaning the virus. But often times there are viruses that get detected that cannot be cleaned. There are many reasons for this but more importantly there has to be some notification of this type of condition that gets back to the SOC so that manual intervention can take place and the impacts of the virus will not cause any real issues. Often viruses are designed to steal data or open up doors to allow attackers easier access into protected networks. When data are going to leave your network, you should evaluate them to ensure they are supposed to leave and that they are being sent by the right person who has permission to send it and that its going to a known or reliable destination. Data loss prevention systems can operate at the network level and the host level, these systems are configured with rules to detect important data that an organization owns and ensure it is being moved across a network properly. The rules that these systems operate with have to be maintained and alerts for violations of those rules need to be reviewed and acted upon by the SOC.

APPLICATION DEFENSES

Applications that perform critical functions or store important data for your organization need to be protected as well. These applications can live almost anywhere in your network at your organization from individual hosts to primary servers or mainframe computers. This is a fairly large and broad area for security as there are many different considerations in how to protect different applications but also for how a SOC would interface with those protection systems. It is important that applications are patched, a SOC that runs regular vulnerability scans should be able to detect when an application is out of date with its patches and escalate that information as a notification to the application owner in order to get it updated. Viruses, shellcode, and other malicious logic can take advantage of your applications and make them do things that they were not supposed to. Being able to detect when application files are inappropriately being modified or when a user keeps trying their password over and over again 1000 time per second are all things that the SOC needs to be on the look out for.

DATA DEFENSE

You have all these layers of defense but it all comes down to the data and the resources storing that data. What kind of protections will you put in place to protect your data? Will you use file and volume encryption on your endpoint devices, secure vaulting on your servers, special group access, or even physical protections? Regardless of how you decide to protect your data, someone has to watch and react to alerts or modify the systems rules as needed.

POLICIES AND PROCEDURES

Although not as technical as a ring like we have just been reviewing, policies and procedures will have large impacts to not only how your SOC operates but also what they are able to do and how they will do it. When you have a web proxy in place to protect your users from going to malicious sites, your SOC needs to review those events to ensure there are no infected systems with malicious software causing systems to access bad websites but your organization may also have policies on what can be download or what an employee is allowed to view on their computer. If you have a policy that says nobody is allowed to research guns and weapons while at work on a work computer then it may be the responsibility of your SOC to catch that and to properly report it to the HR department. There are many other policies and procedures that will impact the operation of your SOC, carefully review what your organization has and see what can be included into the SOC as part of their business objectives and help business controls. The policies and procedures will touch every aspect of not only how the SOC operates but how devices are configured, tuned, and deployed to protect against.

SECURITY ARCHITECTURE

Now that we have talked about some of the enterprise level devices and organizational infrastructure out there that your SOC may be responsible for or get information from we need to talk about how this all comes together. If you were starting off from scratch or if you really need to take a good look at what you have and want to make sure you have the right equipment to protect your network, you would need the help of a security architect. This is someone who understands the needs and goals of the organization and who has a good understanding of where potential weaknesses could be. They will then work to recommend technology or configurations of existing systems to improve the overall security posture of a network. They will work with the larger IT organization to purchase, configure, and install security products that will monitor and protect the infrastructure. The architect should design countermeasures for different types of attacks such as unauthorized user access, data loss, hacking, malware, and many others. It is worth mentioning this role here because it is vital to the organization but will not always be a part of the typical SOC unless you are an MSSP. In many MSSPs, you will indeed find or should find security architects in the SOC. This does not mean that architects cannot be a part of the SOC but they are typically part of a larger security organization and will work along with the SOC to identify areas of weakness or areas that need improvement. These architects need to be responsible for understanding industry standards and best practices and be able to convert those to realistic technical controls. They have to keep up with not only networking trends but also emerging security technology as it relates to your core organizational security needs. They should be able to work effectively to help an organization design, size, and scale security solutions specific to organizational needs on a project by project basis or as part of an overall security strategy. Your architect will know what tools are out there to achieve security goals.

There is too much security technology that can be implemented at an organization to be covered in this one small chapter. Whether it is the access management system, network-based intrusion system, or core information technology infrastructure, you have to understand the size of the overall infrastructure you are protecting in order to make the right decisions on sizing your security solutions to be implemented. Basic example of this is if you plan to implement an access management system, you need to know how many users you have so that you can install the software on the right sized hardware meaning, memory, hard disk drive, as well as processing power, then you need to buy enough licenses to cover all of your users who will be accessing the system.

In keeping with the same example when we start to look at the structure required to run your SOC, we also need to know what the expectations are for the SOC in utilizing the implemented organizational security infrastructure. The requirements for your SOC will be very different if your access management system is fully automated opposed to a system where the SOC will be managing access grants and revocations from the system. You also have to consider if the access management system will talk to other systems such as sending logs to an SIEM infrastructure. So, for each

IT system implemented in your organization, you need to have an honest and open discussion about what needs to be protected how it is to be protected and what the expectations are for the SOC in protecting those systems. For some companies, this is a standard risk assessment. In many cases, there may be systems where the SOC may not be directly responsible for managing such as a web server, but there may be very real and specific requirements for the SOC to protect that web server from intrusions. Different organizations will employ different technologies for this purpose, all depending on the risk assessment of that device and the organizations desire to protect it. This could mean the implementation of application layer firewalls all the way to just collecting logs in a centralized log management system. But you do not need to boil the ocean when looking at your organizational infrastructure and how it is secured before you set up your SOC. You do, however, need to create a positive forum in your environment in which information technology, security, and business representatives can openly discuss what needs to be protected and what the risks are to an organization compared with the level of security currently being provided for a specific asset. Once you get a good idea about the entire organizational security infrastructure that needs to be either managed, control or utilized by your SOC can you then start to think about what is needed for your SOC in order to perform the job. Even if you think you have everything covered and you were correctly sized in your environment you still need to make sure that you allow enough capacity to grow. You want to make sure that as you develop your security infrastructure you are flexible enough to scale up or even down depending on your company or organizational needs and financial condition.

SIEM/LOG MANAGEMENT

There are a ton of papers and books[1] written on the topic of SIEM or just security event management, whichever you choose to call it. There are also a ton of papers and books written about log management. Since both are very heavily covered topics there is no real reason to cover them in-depth in this book except for the fact that they are critical and extremely functional components to a SOC and deserve a review.

Years ago when the function of security was really just starting out people who were trying to protect a network from hackers would build a basic IDS or a file integrity checker. They would build this system, get it up and running, connect it to the right part of the network, and watch it like a hawk. Their eyes would be glued to the screen waiting for something to happen and then pounce on every alert like a cat chasing a mouse. After a while, it tends to get boring or you have to install several systems on different parts of your network and the review of the information gets very tedious. I am talking about a time when we did not have fancy graphical interfaces and webpages to look at. Everything was command line and stored in

[1]NIST SP 800-92, Guide to Computer Security Log Management, which is available at http://csrc.nist.gov/publications/PubsSPs.html.

files. When you have several different systems, going back and forth to each system looking for events and chasing down potential issues becomes difficult and very time consuming. To help resolve these issues programs were created to generate emails when changes were detected. Similar to the way email groups worked these messages could be sent for every alert or digest versions could be sent once a day. This helped make things a bit more manageable but there was just too much information to consume. Now, fast forward time to today where we have more advanced systems each with their own graphical interface, dashboards, and charts along with raw data visualizers, all viewed as a web page or inside a custom application, it does not make things any easier. Although these systems have come a long way to provide better value in managing their data and events, a typical security infrastructure can employ hundreds of different types of security systems, and thousands of rules that all generate an amazing number of events 24 h a day. To really manage these events properly you need to be able to prioritize and address as many of the most critical ones as close to near real time as possible. SIEM tools have really helped in this area. By creating a system that can consume events from hundreds of different types of devices and systems and then build rules around those events, the SIEM has become what is known as a force multiplier, meaning it can make a few people do the job of many. By collecting all these events and building rules around them, you can really ensure that your SOC works what you want as a priority and stays on top of events. The SIEM can handle reporting to your ticket system and even perform any additional communication or notifications you need. Today, a SOC that operates without some kind of a SIEM tool is seriously handicapped. A SIEM tool is one of the best ways to utilize security intelligence data to proactively monitor for suspicious indications of threats. Additionally a SIEM tool is going to be able to provide you a significant ability in metrics reporting and security analytics that may be required to not only spot problem areas but to also provide reports to management. I am not saying that every organization needs to go out and buy their SOC the best tool money can afford, and there are even some low cost if not free ones out there, you can definitely find champagne on a beer budget, but to not aggregate and collect events from your security tools into a central repository that has been built with your organizations workflow, priorities, and objectives in mind will significantly reduce the efficiency of your SOC and reduce the effectiveness of your overall security strategy.

Log management is a bit of a different story and I want to separate it out from SIEM because they are really two entirely different things. Some people believe or understand log management and SIEM to be relatively the same but they are really not and should not be considered the same in any way. I would like to place a clear definition on each for the purpose of how a SOC and your organization should view these systems.

SIEM should be considered as a system that is capable of the short-term collection and storage of security-relevant data and information that has functions and controls to aggregate like events, correlate multiple events in a series or chain in order to build new security-relevant events to be investigated by trained security personnel. High speed and performance are going to be your two primary concerns for the hardware running your SIEM solution.

Log management should be considered as a system that is capable of the long-term protected collection and storage of complete raw event data that has advanced search and reporting capabilities for auditors to ensure compliance with organizational controls and for security personnel to perform forensic and historical research. Large storage and backup capabilities are going to be your areas of focus for your log management solution.

All too often I see organizations trying to use a log management system to perform the tasks that a SIEM was created to do and vice versa. This does not mean that the two types of systems do not have similar capabilities but they will usually approach the problems from different perspectives. A system that is designed to evaluate events against hundreds of rules at high speeds will be a very expensive system to use as a log aggregation repository. A log management solution should be able to store logs at a much cheaper cost.

Let us look at a typical scenario where this difference can be expressed. When a hacker attacks a server, there can be hundreds of unique requests to that server being made and can typically be very noisy as far as the volume of events. In a log management system, this noise can be very difficult to see with thousands of other logs all being collected at the same time. With a SIEM tool, rules can be created to see this type of activity automatically and create a single new alert that notifies your SOC that a potential attack is in progress. A more difficult example of this may be an attacker who tries to disguise a server attack by initiating requests very slowly and waiting long amounts of time between attack requests. In this case, reviewing a single day or week's worth of logs may not show you any recognizable trends, like a needle in the haystack. But with the right rules and properly trained SOC staff, they will be able to recognize these trends when they are analyzed over a week, or month inside a SIEM. The attackers source IP address may even be automatically captured by the SIEM tool immediately upon the first detected event and then as the attacker gets more aggressive or performs other threat-based events the system will automatically raise the criticality of what that IP address is doing on the network to raise the awareness, whereas the log management system will just simply collect all the events.

I do not want to diminish the needs of collecting logs at all, it is a vital part of any complete and robust security operation. You must be able to collect the right data in your logs, monitor for anomalies and store them for a reasonable amount of time. Not only do logs need to be collected they also need to be protected especially if an attacker is able to compromise a server. A log management system serves a great purpose as it gives you the ability to move log files off of a system so that an attacker who wishes to cover their tracks cannot alter those logs. This goes well beyond setting permissions on a system log or encrypting the logs, it takes them well out of reach by ensuring they are safe on a completely separate system. Most all servers and systems today provide some kind of log or Syslog[2] capability and these logs are

[2]Syslog is defined in IETF RFC 3164, The BSD Syslog Protocol, which is available at http://www.ietf.org/rfc/rfc3164.txt

what tell you something has gone wrong. The logs, regardless of how or if you collect them will tell you very important information, if configured correctly. They can tell you when suspicious activities have occurred and that something requires further investigation, they can also tell you what an attacker is doing by recording their commands or actions. Last but not least, your logs can become the subject of legal proceedings and therefore should be captured and stored in a safe and sound place. Most larger organizations will have audit departments that will work with a SOC and will help provide guidance on what reporting they need, how long to store the logs and what kind of storage system is acceptable from a legal perspective.

SIEM and log management can become a very expensive, systems can generate a ton of logs and these logs take up huge amounts of storage. For larger systems, this could be billions of events per day and when designing a system, it is very easy to under estimate the space that would be required to keep these systems running. Typically auditors and regulators like to see storage of specific logs for a year or more, when looking at the storage needs for billions of daily events over the course of a year the storage will get expensive. A log management system will understand the long-term storage needs and will be able to address that with data compression and other interesting and inexpensive ways to achieve your goals. The storage needs can fluctuate depending on what you are doing and what investigations you are performing, for example, you may decide to pump up the log detail on a specific device to get more information temporarily, this can easily become a concern for storage. Administrators of these systems have to closely monitor the size of the storage systems in the log management and SIEM environments to ensure they continue to operate properly. It is also worthwhile to note that as an organization grows systems, servers and networking equipment being used in an organization can grow in numbers or drastically increase in event rates, you need to take that into account and plan for storage growth in these tools and consistently revisit those plans. To help combat increasing log sizes and running out of storage, your SOC should work with your organization and auditors if you have them, to level set what is actually needed, and what can be removed from being captured in the logs. What is relevant and what can be eliminated are important items to review as some types of network devices and servers will allow you to select what types of events get logged and have the capability to turn off what you do not want. By eliminating what you do not need will help you store those important events at a lower cost. Do not just collect everything, make sure that your SOC, engineering, and management work together to ensure you get what you need.

OPERATION CENTER INFRASTRUCTURE

TICKETING SYSTEMS

An issue tracking system or ticket system is a vital part of your operation center. You need to be able to create, update, and resolve reported issues as well as track work progress. Just using a single security tool in your infrastructure may not be

sufficient to properly analyze an event, though using all of the tools you have available combined to effectively monitor the network will empower the analyst to be successful. Each analyst over time will develop his or her own style of monitoring. Using a ticketing system will allow for a central repository of all notes and data used to perform each events analysis. This will not specifically instruct an analyst on how to do a particular job but help contribute to a better understanding of work flow and best practices and will allow others to follow behind them, read their notes, and validate their findings.

A ticket system can often also contain a knowledge base containing information on resolutions to common problems or may even have indicators about what true positive event looks like opposed to a false positive and can include ticket numbers that were previously solved as actual references. Consistent use of a ticket tracking system is considered one of the fundamentals of a good operation team. As such, we are going to spend some good time talking about different systems and what are some needed and optional components to your ticketing system for your SOC. This is such a vital resource to the SOC that you need to spend some good time thinking about what the requirements are before you implement anything. You need to know what the SOC team members will need and what kind of metrics you would like to get out of the system.

One of the primary features of a ticket system that you should look at is its ability to capture analyst's notes. This is critical as you analyze events, you need to make sure that notes are properly captured, time stamped, and easy to follow. The flow of notes can be cumbersome, you need to make sure you know what works for you. One time I worked in a SOC that had a ticket system that took me forever to find notes, they were buried somewhere and you could only see one note at a time. So I had to open the note, see if it was the one I wanted, then close it and open another. Each opened a new screen, it was a huge hassle even after I figured out how it worked. Some systems make you click on every note to see what is written, whereas other system list out all the notes in a very long linier way then there are other systems that have separate notes but as you click on each a text box activates with the information that you can easily see.

If you have a lot of devices in your security infrastructure or are protecting a large device list then it may be important for you to have your ticket system include an asset database to collect information on devices under management or being protected by the SOC. This is optional as this can also be accomplished if your organization already has an asset database so your needs may vary. Having an asset database included in your ticket system may afford you additional automation, workflows or easier access to information customized inside every ticket.

An array of communication methods such as text, email, or SMS text is also a major requirement you should think about with your ticket system so that you can automatically notify people of required actions. Additionally you will want to see what other systems or integrations are possible with your ticket system. For example, maybe your ticket system can automatically communicate with a change database or asset database. This will help you deconflict issues that arise looking like a security

problem but is really an authorized change. There may be many different types of communication integrations possible with your ticket system so spend some time evaluating the possibilities as this will only extend your capabilities and improve the performance of your SOC.

A good basic ticket system will allow team members to create new entries that are individually numbered for easy tracing, and then allow the members of the SOC to make free form text entries regarding a specific case, events, or issue. The ticket system should track who made the entry, what time and date the entry was made and allow for different ticket statuses. Ticket statuses can be as simple and as basic as open or closed but can be also be very complex and detailed such as "waiting for system administrator call back" or "escalated to management".

Event analysis/investigation is a time-sensitive process and crucial information can be flushed or overwritten from security devices or sensors lacking large storage devices. if the processes take too long to retrieve the information you need. No matter what, you are going to work against the clock if you are under attack and you want to reduce the impact of that attack. Quickly reacting to threats and attacks may allow you to get an intrusion prevention block in place or shut down a system to prevent the spread or escalation of an attack. The SOC needs to always perform work quickly, but not hastily. They should not have to think about the current process and what the next steps should be, the ticket systems and workflows should be there to support them. In order to make your ticketing system work best for you, think about your events and what problems or malicious activities might cause a certain set of system alerts to be ticketed, then build your ticketing system to match those events and the workflow you will need to be the best at effective analysis, communication and ultimate conclusion of those events your SOC will address.

When an analyst has used all of the security tools available to them and determined that an incident has occurred or further validation is needed, entering information into a ticket should always be the next feasible step an analyst will need to do. It is crucial that all of the information available is put in the event ticket that was generated or created and the information should be in great detail. Capture all of the logs, screen shots, and network flows as possible during the investigation and include it in the ticket. There should be no issue with information overload inside your ticketing system. The robust information you include in each and every ticket will only help when more than one person in the SOC gets assigned to work a ticket so that everyone can better understand what the original analyst was seeing or what they are basing decisions on. You should also consider that tickets may need to be reviewed hours, days, or even months after an incident and it can be difficult to remember all the gory details, good data in your ticket will help. Multiple people working a ticket is common as this can happen for example, if an event gets created during first shift and another analyst picks up and works the event on second shift. Or if an analyst needs to escalate a ticket to a more senior person such as an engineer, that second person who gets the escalation should not have to redo all the original research as all the required information needs to be in the ticket.

You should also consider using the concept of queues. This will allow you to split up your tickets into different areas for either team focus or organization. For example, you may want a general queue where all tickets get automatically created or created by your tier-1 analysts. Next you may want a separate engineering queue, this is where your analysts can place existing tickets that need the attention of the engineering team. This type of queuing will allow different teams to focus and see only the tickets they are concerned about and remove extra information and noise that they do not.

BUILDING THE TICKET SYSTEM

There are many different ticket systems out there to choose from. There are free and open source ticket systems and also very expensive ones that you can choose. From a technical or implementation perspective, there are many different decisions about features, functionality, licensing, support, and platform that you will need to consider.

But, before we dive deep into what your ticket system should look like or do for you, your first step should be to see if there is anything that is already being used in your organization that you could leverage and utilize for your own needs. It may be a very simple process and much cheaper to work with an already established system in your organization. By working inside an established system you can gain significant advantages as there may be existing support structures and knowledgeable people that you can work with on training, design and development in getting new queues and workflows built just for your SOCs use. By utilizing an existing ticket system you will be able to easily move tickets around your organization for when issues need to be addressed by teams outside your SOC or if issues arise that external teams want the SOC to address.

One drawback of using an existing system that you will need to ponder is the security and permissions of how the system is managed. What I mean by this is you need to carefully review who will have access to your tickets and your queues. For the most part having people who are not in the SOC look at tickets will not be a big deal but if your SOC is performing investigations on employees of the company then very tight controls will need to be placed on this data. Investigations in a SOC can and regularly will contain information about users but may not be because of something that a user directly did. For example, assume a user visited a normal and typical news website that happed to display a link or advertisement that was detected by your security infrastructure as malicious. An alert may be generated and a subsequent ticket created. Then inside this ticket, an investigation would be performed that would include the users browser activity, their system logs or antivirus scans plus a bunch of other things depending on your tool sets. All of this investigative activity would be performed to ensure that the computing assets and network components are safe and free of malware but will have little or nothing to do with the actual user. To the casual or mistaken uninformed onlooker, it could be interpreted that the user did

something bad, rumors, and water cooler talk could start and even though the user may never have not known their activity was being investigated people around them could build an unfair negative opinion about them. Without going into another long example, imagine if the SOC was investigating someone for insider threat, stealing data, or unethical behavior. Bottom line is that if you are going to use a ticket system that is already widely used in your organization, make sure that access is well understood, appropriate, logged, and controlled.

When you decide that you want to have your own brand new ticket system either because I scared you off from using the one your organization already has or there is nothing so you need to start from scratch anyway, the first thing you want to think about with a ticket system is its ease of use. An overly complex system or one that does not visually flow properly or make sense will be difficult to use and train people to be successful. The last thing you want is for investigations to get lost, and for your SOC to spend more time using and working the ticket system then analyzing security issues.

Next you will want to think about how you view information and may create different views to support various activities or different uses. For example, your main screen may show you a list of all open tickets but will give your SOC analysts the ability to sort those tickets by date created, criticality or any other criteria you want.

Here is a simple ticket view:

Ticket #	Status	Date	Time	Subject
1875	NEW	6/9/14	12:47	MS-SQL Buffer overflow
1877	OPEN	6/9/14	12:59	Website block
1881	NEW	6/9/14	13:46	Unauthorized FTP transfer
1882	NEW	6/9/14	14:02	Virus found
1888	NEW	6/9/14	14:02	Denied IP by policy

The ability to include tickets or give the SOC users the ability to change the filter of what is being displayed to different statuses may also be something you will want to consider. You might also want to allow for the inclusion of other fields to be viewed. This could be items like the last modified date, the name of the analyst that owns the ticket if it was previously opened and so on. When filtering you may want to only see tickets that are new and nobody has addressed yet, or maybe you want to only see tickets that you own or have been working on. Another option you may also want to think about are using different colors of text to help highlight critical tickets, new tickets, or a tickets that need some kind of special attention.

Here, is the simple example again but with color, the color can be automatic workflow built into your ticket system to help point what the priority events are based on criticality or some automated workflow logic. You will need to make sure you document your workflow so that everyone clearly understands what things mean and how it all happens. In the example below, the different colored text of ticket 1875 may indicate that the ticket has been in a “NEW” status for too long and someone

needs to open it and address it. While ticket 1882, that is all shaded in, may indicate a critical event that needs to be address before all others. Do not be afraid to use different colors to mean different things as long as you do not make it too complex. The idea is to be able to quickly highlight the important tickets when viewing a large list. At one SOC, the fact that tickets were red was not enough, they used the system's ability to blink/flash the ticket text on and off to add an extra sense of urgency on that item. Hopefully your ticket system will be versatile enough for you to be creative on how to color coordinate your ticket views. Remember, make sure that the colors of all the views make sense and are easy to use or are customizable by the user to their preference.

Ticket #	Status	Date	Time	Subject
1875	NEW	6/9/14	12:47	MS-SQL Buffer overflow
1877	OPEN	6/9/14	12:59	Website block
1881	NEW	6/9/14	13:46	Unauthorized FTP transfer
1882	NEW	6/9/14	14:02	Virus found
1888	NEW	6/9/14	14:02	Denied IP by policy

The basic fields that you should have in your ticket system are fairly straightforward. Even though the various fields should be standardized, typically ticket systems are not designed for a SOC but rather a more general purpose like a help desk or call center, so there will be a fair amount of customization you will want to make and will need to think about. In addition to the various important fields of information, you may want to customize workflow to streamline a process or ensure compliance with required steps you want your analysts to take.

Let us take a look at some of the primary fields your SOC will rely on and may or may not be part of a standard ticket system installation.

SUBJECT

This may seem like a no brainer but the actual subject of a ticket is very important. When you are looking at the queue of your ticket systems, you may see rows and rows of tickets and if they all have the same subject then how would you know what ticket you need or would like to work on. The subject of the ticket can be passed to the ticket system by the device that generated the original event. In the case of a SIEM tool, you may even have the ability to customize this field's value. If for example you were sending IDS alerts directly to your ticketing system then the subject field may just be the name of the signature that fired such as "MSSQL Overflow", "New server on network" or "Virus found". If you are able to customize the output of the system that generates an event or if you are going to manually create an event, try and keep the subjects standardized. This way, as you look through tickets or search historical tickets you will find it much easier to get what you want. Some

SOC environments may want to have the source IP address of the device that caused the alarm as part of the subject. That way if you have multiple tickets with the same alert name you can quickly see if it is all coming being caused by the same device or multiple devices.

Example:

Ticket #	Status	Date	Time	Subject
1875	NEW	6/9/14	12:47	MS-SQL Buffer overflow – 192.168.10.51
1876	NEW	6/9/14	12:47	MS-SQL Buffer overflow – 192.168.10.51
1877	NEW	6/9/14	12:47	MS-SQL Buffer overflow – 192.168.10.51
1878	NEW	6/9/14	12:47	MS-SQL Buffer overflow – 192.168.10.51
1879	NEW	6/9/14	12:47	MS-SQL Buffer overflow – 192.168.10.51
1894	NEW	6/9/14	12:48	CMD.EXE execution – 192.168.10.51

Once you are able to find a ticket you need to work on you should be able to select that ticket to begin work and perform your analysis. Once you select a ticket it should open up to the "ticket view". This is a view where you can see all the important elements of your event. It should be arranged in a way that is easy for an analyst to quickly assess the event and make quick decisions on what to do next. It could include asset information, and knowledgebase information all on the same screen as the basic event information.

In most cases, your event information and details should be on the top and the rest of the majority of the screen should be dedicated to allowing the analyst to make notes, upload documents, and perform actions on the ticket such as escalating it, changing its status, or even closing it.

PARSED VALUES FROM EVENTS

Your ticket system may have the ability to parse, chop, or read raw events that gets sent to it. When it reads these events, it can place key information into separate fields of the ticket. This is extremely valuable as it allows you to perform key reporting or search for specific elements of events and build metrics or to even spot trends. Values such as Source IP, Destination IP, Source Port, Destination Port, and of course the time the actual event occurred are all values that you should be able to read from a raw event and place into its proper place. Parsing can be valuable when you want to custom design your ticket view as we discussed above. Parsing events will allow you to put important data elements into the correct locations for easy viewing and searching.

TIME TICKET CREATED

For automatically generated tickets, the time a ticket is created is typically later than the actual time an event was generated. It takes some time for a security device on a remote network to generate a log, have that log get sent either directly to the ticketing system, or be processed in a central log management or correlation engine. Knowing the time difference between when an event was generated and when a ticket was created can be very important especially if the time difference is hours not seconds or minutes. This may indicate problems on your network or some difficulty in processing. This lag is a metric that you should watch very carefully, it may help you to spot busy devices, or configuration errors with your security devices or even network congestion at a customer site. You need to learn what the normal deviation is and monitor or watch for any significant changes.

In the case of tickets that get manually generated, the ticket created time is also important because that will be the start of any event. This is where the timeline begins and without this it will be very difficult to figure out the chain of events when you start putting all your notes into the logs of the tickets. Sometimes analysts will do some research or complete an investigation prior to creating a ticket. Do not let this happen, anyone performing an investigation needs to have an open ticket first. This not only helps you track time people are spending on tickets doing analysis but it also allows your SOC supervisors the ability to watch the ticket queue to see who is working on what. Not only does it help them see what everyone is working on but if there is a ticket that stays open for a while it will allow the supervisor to check in with the analyst working on it to see what is going on and make sure they have all the resources they need and to make sure they are not dealing with a issues that will require additional attention from other SOC resources or engineers. Additionally if an analyst works an issue outside of the ticket system, you will lose track of what they are doing and will not know how to properly apply your resources. When an analyst is done with his research they may open a ticket and then just dump all their notes into that ticket and then close it. The results of that will make it look like they only had the ticket open for a minute but in reality they worked the issue reported inside that ticket for 2 h. It is very hard to capture the actual time worked on an individual ticket but as your build your system it is something you may want to keep in mind, or the system you select may have enhanced capabilities that allow you better visibility and reporting into how much time is actually spent on any given ticket. Time tracking systems built into your ticketing software can pay big dividends for you when creating metrics and evaluating your SOC. This is critical for resource planning and evaluating where bottlenecks may be in your processes. For more information on these types of metrics, refer to the chapter metrics. In the end, you really want to ensure your analysts are working inside the ticket system because things happen, documents get closed and information gets lost, or people get pulled in multiple directions and then it is difficult to go back to what you were doing if you did not keep accurate records.

USER\GROUP\QUEUE

Tickets can be broken down and organized in many different ways. You need to make sure your organization of open tickets make sense and that they are easy to find, track, and address. All tickets except new tickets should be assigned to either a user or a queue. So when a new ticket is created, if it was created by a user, than that ticket should be assigned to that user automatically or if it was automatically generated then the ticket owner should be blank and it should be in a primary queue waiting for an analyst to open it and address it. If a ticket gets transferred to another group or queue then the ownership should be that queue until another user opens it. The history of actions, notes and ownership should all be logged and tracked inside the ticket for easy viewing. You may have different groups in your SOC such as your tier-1 or tier-2 analysts, engineering, or management and each of these groups should be a different ticket group in your ticket system.

Key point: The more granular the queue you can create the better metrics you can generate to see what is going on. But the more granular the queues, the harder it is for people to notice tickets that may be waiting for their attention. Make sure the division of groups and queues make sense for your workflow and reporting purposes.

Under each group there may be different queues for that group to organize tickets. Depending on your workflow you may only have one global queue for everyone to work out of but if you do have different requirements here is a quick example of what a group and queue structure may look like.

- Tier-1
  - General queue (all new tickets)
  - Health queue (security device or internal system issues)
  - Waiting for callback (tickets that have been addressed but waiting on an external resource to call/email back)
- Tier-2
  - Main escalation queue (location of general tickets that are being escalated to the tier-2 team)
  - Health queue (security device or system issues)
  - Waiting for callback (tickets that have been addressed but waiting on an external resource to call/email back)
- Engineering
  - Main escalation queue (location of general tickets that are being escalated to the engineering team)
  - Device based queues (individual queues based off of device type)
  - Provision/decommission (location of tickets for the installation of new devices or the removal of old ones)
  - Global issues (Tickets that effect overall service or delivery of service)
- Management/team leads
  - Main escalation queue (location of general tickets that are being escalated to management)

- Customer complaints (tickets that need loving care)
- Unresolvable issues (tickets that cannot be resolved due to technical issues, limited information or outages)

SOURCE (SIEM, EMAIL, PHONE)

Ticket generation should come from many different sources. The ability to generate tickets from email messages is almost a no brainier. Emails can be automated from your security devices or they can come from users or customers. Tracking emails by converting them into tickets is a great way to ensure that all communications coming into your SOC are addressed and resolved professionally. Security systems like SIEM system or log management systems will have their own ability to create rules that trigger some action. That action could be a direct connection to your ticket system and have a new ticket opened that needs to be evaluated. The tight integration of your SIEM system and your ticket system is invaluable. Some SIEM systems include their own light weight incident management tracking system but you really need a way to handle tickets and incidents competently, so make sure you are able to effectively get important data from your SIEM to your ticket system. There are also automated ways to integrate your phone system with your ticket system. These integration systems are really nice for organizations that have a heavy call volume or in a MSSP operation, especially when an analyst is able to answer the phone and have a new ticket automatically open with the customer details already populated. This is a great way to make the SOC more efficient and provide great customer service. It also helps the SOC management ensure that all phone calls are tracked and logged appropriately in the ticket system for later review and to ensure that all work being performed in the SOC is being tracked. The sources of your tickets are an important value to keep track of and should have a field in your ticket system. You need to know where your tickets are being generated from for several reasons. First, if you are getting a ton of junk or false positive tickets being generated you should know where they are coming from. If you have many different systems all automatically reporting and sending in information to generate tickets and you do not have the source information then it will be extremely difficult to know what system needs to be adjusted to resolve or tune the problem. You also need to know how your SOC is being informed of issues that need to be addressed. If you are properly engaged with your organization and have effectively communicated what you do, what your specialties and responsibilities are then your tickets should not all come from your automated tools. You should expect a percentage of your tickets to be coming in from phone calls, emails, your portal system, and possibly ticket escalations from outside the SOC. It is very important to track these sources so that you can run effective metrics to determine and evaluate where your most critical or even reliable source of events are coming from. Additionally you should be able to run reports on the kinds of issues you are getting from each source so that you can better understand the value you are getting from that device or team.

CATEGORY

An incident should be categorized as one of the categories as listed in the below table based on the type of incident. These categories are fairly standard in the industry and are regularly used by computer emergency response teams everywhere. the table provides a listing of the different categories and a definition/description of each category.

Category	Name	Description
CAT 1	Root-level compromise	This category is used when an individual gains unauthorized root-level access (logical or physical) to the organization's network, any of the systems, applications, data, or other resources.
CAT 2	User-level access	This category is used when an individual gains unauthorized user-level access (logical or physical) to the organizations network, any of the systems, applications, data, or other resources.
CAT 3	Attempted access	This category is used when an unauthorized user attempts to gain unauthorized access to the organization's assets (local or remote)
CAT 4	Denial of service (DoS)	An attack that *successfully* prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources. This activity includes being the victim or participating in the DoS.
CAT 5	Poor security practice	This category is used when misuse or unauthorized use of an organization's information technology assets is discovered. Also, covers violation of the organizations computer security policies such as weak password, or misconfigured system.
CAT 6	Scanning/ probing	This category includes any activity that seeks to access or identify a company or organizations computer, open ports, protocols, services, or any combination for exploit. This activity does not directly result in a compromise or DOS.
CAT 7	Malicious code	*Successful* installation of malicious software (e.g., virus, worm, Trojan horse, or other malware) that infects an operating system or application.
CAT 8	Unknown	This category can be used for a ticket that does not currently have a determination of what is happening. A ticket with this category selection cannot be closed until a specific category has been determined
CAT 9	Exercise	Since categories will be used for metrics, any tickets generated while exercising or testing should be closed with this category in order to keep these types of events separate from all the real events.
CAT 0	Discard	This category should be used for falsely generated tickets, bad tickets, or any tickets that should just be discarded and not counted.

STATUS

The individual status of ticket is important, it tells you very quickly what is going on with that issue and when combined with other key values it can really help you to manage your flow and rate of ticket closures. You will have to think about what values will make sense to you as your SOC gets going but there are a few basic ones you can start with.

- New—The value of any ticket that was just created and has had no work done or nobody has touched it yet.
- Assigned—Someone is currently assigned to the ticket work may or may not have begun on it.
- In progress—Tickets that are being worked on but that may be scheduled for resolution during a change window or at some agreed upon time.
- On hold—Tickets that cannot be completed right now, something is needed or other actions need to happen before these tickets can move forward.
- Reopened—This is a ticket that was previously resolved and closed but had to be reopened for some reason.
- Resolved—Tickets that are presumed to be closed and have a clear resolution.

It may be a good idea to set time limits on tickets or even force workflow for tickets in different states so that nothing gets lost or forgotten. For tickets put into an "On hold" status maybe you can force a user selectable timeout. So when a user puts a ticket on hold they have to select a specific date and time the status will automatically change from "on hold" to "In progress" or "New". Then you can put specific time limits on tickets that are "in progress" and change their color to signify that they have not been addressed or looked at in too long of a time period. Your imagination can run wild with possibilities, make sure your ticket system is capable of meeting your imaginative needs in this area.

REASON CODES

Not every system uses reason codes but it is a great way to help build metrics or gain better visibility into why a ticket is in a particular state. For example, if you have a ticket that was resolved, why or how was it actually resolved is a bit of a mystery unless you open the ticket and look for a "reason" as to how it was deemed to be resolved. By using reason codes it will help you understand specific states of your tickets and also give you nice clues for tickets that may be in the wrong state or need additional work. A good example of a ticket that is properly resolved would have a reason code of "Infection Cleaned". An example of a ticket in the wrong state would be a ticket that is marked resolved but has a reason code of "waiting for call back". Running reports that show different statuses and their associated reason codes will help you see what is going on very quickly. We talk more about metrics in a different chapter but it should be easy to see how valuable combining fields help build a

very clear picture of what is going on. The reason codes should make sense to your workflow and mean something if you want to pull reports and build metrics. As a quick example, searching for every ticket in a given month that has a reason code of "Infection Cleaned" could be used very effectively. Those may not only be tickets you want to report on but also review to find out what is causing all the infections or what is missing to allow viruses to get in.

Here are a few reason codes that will help you get started

- Waiting for external ticket update
  - This is good if you are using a different ticket system than the rest of your organization and you want to keep checking the other system or you are waiting for an email to be generated to let you know when your ticket in the other system has been updated. It would be a good idea to also document what the external ticket number is so that you have an easy cross-reference.
- Waiting for a child ticket to close
  - This can indicate that another subordinate ticket is linked to the parent ticket and a child ticket issue will need to be resolved before the parent ticket can be closed. This is good if you have an incident that spans multiple devices, a primary ticket can be created for the main event while individual tickets are created for the review of each potentially effected system.
- Waiting for call back
  - A call from the user or another support group is expected to update or confirm that the issue has been resolved.
- System not vulnerable
  - After your investigation into an event, you determine that the system has been fully checked and is not vulnerable to whatever attack or events alert triggered.
- No infection found
  - For virus alerts, the system has been checked and no infection has been found.
- Infection cleaned
  - For virus alerts, the system has been checked and the infection was cleaned.
- System remediated
  - The system has been checked and a patch, software upgrade, or configuration change has been applied to correct the vulnerability or issue.
- False positive
  - A triggered alert without the presence of proper evidence to support the alert.
- Confirmed security incident
  - Evidence has been collected to support that a security incident has occurred. Tickets with this reason code should have a complete root cause analysis.
- In progress
  - Evidence to support the alert is actively being gathered.

- Review ticket/needs follow-up
  - More evidence is needed within the ticket to support the alert or an assigned group needs to review the information.
- Signature tuned
  - The generating source system signature or rule has been tuned and will not generate another alert like this one.

ACKNOWLEDGMENT/TICKET FEEDBACK

There are two external communication mechanisms that I grouped together but are actually completely separate functions you may want for your ticket system. For acknowledgement, you may want a customer, device owner, or even an internal SOC analyst to acknowledge the creation of a new ticket that was generated in your system. This can be a great customer notification mechanism that alerts them to a potential issue that your SOC is working on and gives them an opportunity to weigh in on the issue right from the beginning. When a customer gets a notification they may look at it and immediately know why the ticket was generated and can help you close it quickly. In the acknowledgement function, you can track to see how long it takes someone to respond and you will have good metrics on response times to your issues. Also, if you require him or her to click on something to record the acknowledgement, it is a good way to make sure you confirm they know about the issue. The acknowledgement could just be a simple reply to an email, click to a website or logging into a portal to view the issue that generated the ticket. Since your SOC will be either working with external customers to your organization or internal customers inside you may want the ability to customize acknowledgements based off of customer or department preferences. May be it is critical that for every ticket generated in the SOC for your organization's web servers, the web team needs to actually acknowledge the ticket whereas another external customer may just want to be notified with no acknowledgement. Customization of how your ticket system interacts with people is vital to the level of customer service you want to provide.

Acknowledgement is typically at the beginning of the process of working an issue but ticket feedback is at the end. It is always a good idea to try and find out how you are doing and by giving people a quick short survey whenever you close a ticket can be extremely helpful. You will want to make sure that you can customize this feature as well or it can become a burden quicker than it can be helpful. Make sure that you are asking the right questions for the survey and change the questions often so that you are getting a good review of different parts of the service you are offering. Also, be mindful of peoples email inbox, do not flood them with a ton of surveys, try to get some built in capabilities to limit how many surveys you send someone out of your ticket system in a span of time. Otherwise people will just ignore these requests as an annoyance.

WORKFLOW AND AUTOMATION

In order to make your ticket system more capable and really aid your analysts, you will need to add some workflow and automation. Workflow can consist of predefined tasks that need to be completed for the type of ticket an analyst is working on. The tasks will need to be performed in order, will dictate the specific details of what needs to be done, and will require input for the task to be completed. This can help if you need to collect specific information for tickets and want to ensure that each analyst collects all the required information and in the correct order prior to closing a ticket. It will also make sure that information is collected and posted to a ticket in an organized and expected way.

Automation is a great way to aid in the regular analysis of information. For example if you could automate the login process to a specific system or external device from the ticket system, it would save you a ton of time having to look up login details. I am not condoning hardcoded password here, I am assuming there is some secure functions happening in the background. For example, if your ticket system had an asset database and when a ticket was generated for a specific device in that database, you automatically had a remote desktop button that you could press. Another good automation idea maybe that when a ticket is generated for an IDS event, the ticket system will automatically pull health information from the device that was the suspected target of the attack and post those details into the ticket notes. It could tell your health information of the device like if the device is still up and online, CPU statistics, network statistics, and so on. This may give your analyst a quick bit of information to tell them if there was any impact associated with the event. The ticket system you evaluate may have many different automation and external system integration capabilities, spend time evaluating these features, and see what you may be able to take advantage of. Having this type of automation will reduce the analyst's manual involvement in gathering data and information by having the system execute rules that automatically perform an action on a ticket when certain conditions are met. There is nothing quite like opening up a ticket to see all the research you need right in front of you, there ready to be evaluated without lifting a finger.

Key point: Count your mouse clicks, if it takes to many clicks to get information or you cannot quickly find information to analyze a ticket then you are wasting time. Figure out how to automate tasks, reduce the number of mouse clicks it takes to perform tasks, and make your SOC faster through automation.

PORTAL INTERFACE

You may think that discussing a portal interface is kind of odd in this section but it is very worthy topic right here. Most ticket systems these days will have some kind of web interface. Even if the ticket system you select does not operate completely through the web, there will typically be some kind of interface that you can leverage.

This is a great feature to offer your internal or external customers. If you are able to give customers an account so that they can see all their tickets, interact with your SOC by placing notes in tickets or be able to even pull custom reports you will be giving them a great self-service capability and making your SOC more efficient at the same time. The portal does not have to be just for tickets, you can use it for posting special information, posting client specific reports or generic reports for all customers to review. You can use the portal to sell additional services or make sure all customers have key contact information to work with in the SOC. Your portal can be anything you want, but having your ticket system be integrated with that portal can really add to the professionalism of your SOC and provide customers with great value.

MOBILE DEVICES

Being able to respond to tickets or just having the ability to quickly look at new tickets once it is generated can mean the difference between saving your organization from a significant breach or being able to finish your lunch. There are many technologies out today that allow you to securely connect to your ticket system and see basic information that allow you to make split second decisions on whether or not something needs to be addressed right away or if it can sit for the time being. As was mentioned previously, your ticket system should have the ability to set a criticality levels to the ticket. The ticket system can email specific types of events to you based on rules you create or for more serious events or special events you should be able to create text alerts as well. These types of remote alerts should be configurable not just to one person but an entire group of people or specifically assigned people based on rules. You should also be able to acknowledge or respond to tickets just by replying to emails and of course all of this interaction should be automatically recorded in the logs of the ticket.

Additionally you may want a mobile application for customers so they can monitor their security posture. This could be done with a small dashboard that details how many open tickets they have, the criticality of those tickets and even the event generation rates over the course of a day, week, or month.

SUPPORT INFRASTRUCTURE

It all starts off with the SOC computer, many times I have been asked, “What’s better for a security analyst to use, Mac or a PC?” What makes this question so difficult is that many organizations have a standard, and because the standard exists, all departments inside of an organization should comply with organizational standards. For many years, now most enterprises have been using Microsoft Windows devices as the common go to platform for most employees. These organizations have spent a lot of time and money building corporate infrastructure to support and manage a PC

environment. So because these corporate infrastructures already exist to support the PC environment, the security analyst wishing to utilize a different platform such as a Mac or even a Linux platform could prove to be challenging. I really do not care to be in the middle of this debate other than to say that some of the best analysts I have worked with will of course have their favorites, but will confidently be able to operate inside any platform or all platforms. In many cases, they will utilize a Mac or PC and Linux operating system in one way or another each and every day in order perform their core job functions. I am sure nobody reading this book will thank me for this section because I know that I am not providing any real definitive answer, nor am I loading up any arguments for one operating system opposed to another. The reality is that I do not see any SOC truly being successful without having access to multiple if not many versions and distributions of different operating systems if not for testing purposes than for special analysis functions. For example, there are many tools written for the Linux platform that make forensic analysis easier when dealing with certain types of cases. The Windows operating systems maybe better when trying to perform malware analysis. Finally the Mac OS X operating system may be easier to work with as it combines many features of the other operating systems but is also extremely capable of running several virtual machines with different operating systems all at the same time.

PHYSICAL

There is a lot to think about when you are designing the physical layout of your SOC. As with any build out of any space there are a ton of considerations that have to be made, many more than this book could detail. Instead of diving too deep into physical space considerations I am only going to touch lightly on some options and important considerations that you should think about, but again this is no way a comprehensive list by any means. Keep in mind that if you are providing a SOC as a service to external customers or you may want to showcase your SOC to internal or external customers then the aesthetics become very important. Your SOC should reflect the work you do and the quality of the services you provide. Be proud of what you do!

Typically organizations will give all employees a desk, computer, desk phone, and any other desk accessories someone may need to perform the basics of the job they were hired to do. In a SOC that may not be the case and you need to think carefully about the environment that you create to ensure it is comfortable and healthy. Some of you that have never worked in an operation center before many think I am a bit weird about now to bring up comfort and health but it is a real concern that you have to consider. For other more experienced people who have worked a few years in an operations center you know exactly what I am talking about. Working in an operation center is not for everyone and the decisions you make here could be some of the biggest differences in being able to retain good talented people or even keep your SOC up and running.

Take for example a SOC that is chartered to run 24×7 on three shifts 365 days a year or two shifts for 16 h 7 days a week. You would not necessarily give everyone that works in your SOC their own desk, phone, and stapler. Instead you would create shared workspace so that you could reduce costs and reduce the size requirements of your space. Regardless of the physical layout of the SOC it makes perfect sense to utilize shared space if you are running multiple shifts. One of the very first lessons I learned managing a shared space work environment is to always be mindful of health concerns. One person coming into the SOC with a common cold could wipe out all your staff for a few weeks. You may think this is normal for any work environment but in a shared space, operational environment it is intensified. Multiple people are using the same handset on phones, a quick call is one thing but if your SOC analysts are spending a good amount of time on escalation calls or support calls then for the next shift to come in and pick up the same phone is kind of unpleasant. People are sitting at a computer for an 8 h shift using a mouse that someone else was just using for 8 h. Does it make you feel a bit sick thinking about using a mouse that someone else's sweaty hands were just using for the last 8 h? There are other considerations but these two alone are a huge way to pass on germs, virus, and sicknesses to each other. To combat these issues, there are a few easy things that you may want to do. First, consider allowing SOC staff to either bring in their own compatible headsets and mice at their cost to use for work or provide them a standard model of each. During each shift change, each analyst would change over to his or her personal headsets and mice. This could also be a design consideration for the desks and consoles that you would purchase for the SOC. You needed to make sure that the USB ports and phone ports are accessible enough to allow for easy changes or purchase quick connect cables to perform the same function. Moving slightly away from the phones and mice, the desk surfaces were also a major concern. People regularly will eat at their desk during work, whether it be a quick snack or a major meal. Typically not a big deal but now your SOC desks are cafeteria tables and need to be taken care of as well so that people do not get sick. Think about it, do you really want to come to work and sit at a nasty desk that someone was just using who may not have the best personal grooming habits and use their phone and mouse and eat your lunch right where they ate there is a few hours ago? I know that I do not what to go anywhere near that place. Anyway, I think I have grossed everyone out by now just by thinking about this but this is a serious issue and if one person gets sick in an environment like this then you are going to quickly find yourself with an extremely light staffing level as everyone is going to be calling in sick. Depending on the size of your SOC, sometimes it may seem that as soon everyone gets over one round of colds it starts back up again. Allowing people to use personal headsets and mice is one way to combat a part of this issue but you also need to make sure you keep your SOC clean. You may think that regular cleaning would resolve this issue but in a 24×7 SOC there is almost no down time.

Do not let people leave food around. I have a few good stories about this one, as I am sure many other people do as well, people that have worked with me in the past may be chuckling, as I know there are a few pictures out there that bring this point

home very graphically. So make sure that you have adequate garbage facilities or plenty of caution tape. You may also want to think about not allowing food or drinks into the SOC but this could prove to be challenging as well.

Ensure that your organization's facility services has access to your SOC and is able to get in to clean and vacuum on a regular basis just like they normally would any other part of the organization. This all sounds logical but in some of the secure and cleared facilities I have been in I have found it to not be so easy. Plus, you have to remember that depending on your SOC schedule there could be people working around the clock so what is the best time to make noise vacuuming and cleaning. If you are in a secure space the cleaning crew may be required to be escorted at all times but any classified or sensitive processing has to stop and be covered up while they are in the room. Finally, and this is no joke, at one SOC I managed I actually had a budget line item for disinfectant wipes and sprays. I had a regular shipment of wipes brought into the SOC and spread around the various workstations so that during each shift change over people could wipe down and disinfect their areas.

Ventilation is also a key aspect to your SOC space. Most SOC's are behind closed doors or in secure areas and as such needs extra ventilation. There will always be tons of computers in your SOC unless you are using remote technology so you need good airflow for the systems but your people need air as well. By having good airflow and ventilation, you will keep your systems cool and your SOC healthy.

Comfort is another area of concern that you need to spend some time and focus on. The job of working in a SOC primarily consists of sitting in a seat and staring at a monitor for 8 h. There are some very serious ergonomic considerations that need to be addressed. I have found that comfort is an individual taste and that tastes can rapidly change. I am in no way an ergonomist but I do know that issues such as Carpal tunnel syndrome, Tendonitis, and Tension in the neck and shoulders are very real and serious issues that need to be taken into consideration. The quality and efficiency of the work being done may improve in a carefully planned ergonomic and comfortable work environment. Additionally, health care costs may be reduced, and worker morale may be greatly improved by taking your time in this area when designing your SOC. When looking at chairs, I have spent tons of money on high quality top of the line ergonomic chairs for the SOC just to have people swap them out with crappy old chairs from other parts of the organization. Some people like cloth, others like leather and some like mesh, some like adjustable arm rests while others like adjustable reclining. I have personally tried several so-called "8-h" chairs and I could not sit in them for 8 min. Honestly I am convinced that you will never get this right and it is better to have a sampling of chairs so that people can have the option to switch off from time to time which is probably your safest bet. There is no denying, you have to watch the chair issue, sometimes people can get very possessive about chairs and there always seems to be a time in the SOC where there is a single coveted chair. I have actually seen people arrive to work early for their shift just to claim a favorite chair before anyone else does. I have also seen people get upset because someone changed the settings on "their" chair because they had it perfect last time they were on shift. As if you did not already have enough to worry about in a SOC but I would be surprised if at some point down the road, you do not have a "chair issue". In the next chapter, we discuss some fun ways to combat this issue.

Monitors are also another concern that you have to address in the SOC. It has been widely argued that staring at a computer screen for eight hours or more a day, every day will not harm your eyes from a medical standpoint; but, ultimately it could contribute to eyestrain or "tired" eyes. We have all had those days where it feels like our eyes are going pop out of our head if we stare at the screen for one more second, but we push through it and move on, because there is so much to do. To help combat these issues, make sure your SOC staff is taking breaks every hour if for nothing else then rest their eyes by briefly focusing on other things, this should go a long way in to reducing eye fatigue but also keep them relaxed and focused while working. This could even be considered exercise for the eyes. By adjust the lighting in the SOC to keep it at a comfortable level, too much light causes strain to your eyes when you look at the screen. Too little light will make it difficult to read papers and books on your desk. Most SOC's I have built or been in keep it pretty dark where most of the lighting comes from everyone's computer screens or the large video walls and/or projected wall images. In some cases, SOC employees will bring in small desk lamps to augment their light if they feel they need it. It is also important to keep your monitor clean and free of dust as these tiny particles can contribute to eyestrain when trying to focus on the screen. Finally, consider the mounting of the screens. Fixed mounting

can be very hard to deal with as people shift positions all day long, monitors would be best mounted on free swinging arms if possible to give people the greatest range of motion and ability to adjust to their position, height and distance they want to be from the actual screen. Also, considering that your staff are highly trained security wizards you should safely assume that the bigger the monitor the better and nobody should have less than 2 per machine. Video real-estate (size of actual viewing space) is something that most everyone in security takes full advantage of.

Some people may find it hard to work in this type of environment due to the lack of personal space. When people float from desk to desk or share a desk area with other people an individual does not really have a place to hang his or her hat. This problem can be hard to deal with especially if SOC employees are regularly meeting with or visiting other employees in other parts of the company who may have personalized cubes or offices with windows. It can be fairly undignified for an individual to not have an identity or a place to call his or her own at work. Unfortunately in a shared workspace environment this is something hard to combat. You may have some creative ideas of your own but I equate this to grade school or high school where you switch from class to class and do not really have a desk of your own to keep your favorite pen and notebook. One idea you can try is to have desk draws at each workstation or console and make sure you assign a draw to each individual so they can keep their stuff in a central location. Another idea is to have personal lockers for people to store stuff. Having personal storage is important, you want people to have books, reference materials, notebooks or other items that may help them with their job. But sometimes it is not necessary to carry these things home every day, instead people need a place to store stuff that they can feel confident will not be disturbed by others. SOC people are a special breed, give them some space and let them have some ability to customize their environment, it will be best for everyone involved.

Do not lock down SOC computers to much, these are trusted security professionals and you should therefore trust that they can have some flexibility in their computer environment without damaging anything. I am not saying that everyone should be a domain admin, but some custom applications shared across the SOC and some ability to customize the environment should be allowed. Roaming profiles in a SOC is a great thing if you can support it. By allowing your SOC employees to customize their profiles you are in effect allowing them to personalize their living space and that space will follow them around no matter what workstation or console they need to log into, this also works great in remote desktop or terminal service environments. Because as security professionals we all live on the computer, and we like the programs that we like and the SOC should be allowed to use just about any software they need to get the job done, within reason.

You can have fun and laugh about some of this but I will honestly tell you that a clean and healthy work environment with some ability to make personal customizations will create a significant and positive impact to your organization.

As for the layout of your SOC, you may decide to keep your SOC open and free flowing. This is ideal to help keep the SOC from becoming stale and looking like a regular office with cubes. In an open environment the idea is to eliminate many of

the barriers that create that office style environment in the first place. Getting rid of cubicles and replacing them with desks or modern work area furniture creates open spaces which is an environment that allows employees to interact with one another, share ideas and interact. Console desks are a great idea and accommodate flat panel monitors and hide all the cables required to run multiple computers. You want to take a look at all the possible furniture options from traditional to specialty console furniture. You want to ensure people have enough storage to eliminate daily build-up of clutter

Space is not usually an abundant commodity, plan carefully when building your SOC and purchasing furniture. There are a lot of space saving options that can maximize the number of people you can accommodate with the least amount of floor space, offering a clean and uncluttered workspace. Another option is to create clusters, at the same time as keeping the physical layout as open as possible, you can also give emphasis to teamwork and cooperation for select groups of people such as tier 1 or 2 analysts and engineers by keeping them localized to specific areas. Clustering desks throughout the office, you can create teams to spur competition as well as cooperation. This also gives teams the ability to discuss issues and work together without interfering or bothering other teams or nearby people who may not be involved in the issues the team is currently working on. Open spaces tend to cause people to swarm and issue, where several people overhear a conversation or issue and the swarm together to contribute or help resolve the issue. This is great teamwork and can sometimes help expedite the resolution of issues as well as provide a training mechanism for less experienced people. But there are diminishing returns when too many people are involved and other issues get dropped. Clustering helps eliminate that problem by keeping swarms localized to specific teams or groups. I am not partial to one or the other, the decision depends on what you have to work with, the size of your teams and your furniture choices.

If you are looking to build a bigger SOC then a more traditional operation center built on a stadium model may be more of what you need. In this layout you would have a large video wall and rows of desks or consoles positioned in the room to give everyone a good view of the wall. In some cases the floor will be sloped so as the front desks are lower than the back to give it a stacked or stadium feel. In the back of the room, you would have management desks or offices for supervisors or watch officers. You may even have small conference rooms in the back as well. In working in a busy SOC with lots of people walking around you need to take great care in not only how you position the furniture but that you have the proper ventilation for all the computer systems and that cables are neatly tucked away.

PRIVATE SOC NETWORK

There is no doubt that your SOC will have special computing needs. The software that will be used to access security devices and resources are going to be very different than what is installed in the rest of an organization. The information and data

the SOC will be looking at is sensitive if not extremely critical to an organization. Knowing all that plus the fact that in some cases your SOC analysts may have administrative credentials to lots of IT systems it is extremely important to ensure that all the security systems, your SOC users and their equipment are very secure and protected. In larger SOC environments and at MSSP organizations it is not uncommon to have resources fully dedicated to the security of the SOC. These resources would work as a regular analyst or engineer but would be solely dedicated to supporting the security of the SOC, this could include the networking of system resources, the management of computers, laptops, and servers, and the safeguarding of data. You could almost picture this as a SOC inside a SOC. When deciding on if a SOC should operate on a completely separate network or just a private virtual network take data flow into consideration. I have seen situations where and IDS event was generated and when that single event was sent to the SOC it passed by another IDS sensor and generated another alert as the second IDS system detected the bad data being transferred as well and had the same rule configured. Having a private network is not a must have item especially for smaller organizations. But just because your SOC is focused on security and you have extremely smart security people working there does not mean they are not susceptible to attacks. Attackers will target users in the SOC just like any other user in your organization but there will be increased focused attacks on your SOC by attackers looking to gain internal network knowledge or credentials to key systems. To better protect your organization and to give your SOC a bit more freedom a separate network infrastructure with proper firewalls and security controls should be used. This also helps separate your SOC and their equipment from directly being exposed to key business resources and systems.

VIDEO WALLS

These are often very impressive in a SOC and can also be very expensive. Although a video wall is another optional component for running a SOC you may have very good reasons to use one. There is a wide range of sizes and resolutions as well as different technologies to build a video wall. Having visualizations of big data sets that engage with your analysts and engineers daily activities can be invaluable especially if it enables them to make real-time decisions. From cubes to long stretches of seamless border LEDs there are almost an endless array of options these days. The video walls can be used to display metrics to indicate performance health of customers systems, changes in network activity or special alarms generated out of the SOC's ticketing system. The screens of the wall could also be configured to display important news channels or the entire screen could be utilized to present training videos to the entire group. The screens should be standardized and organized as we will discuss during the chapter on metrics but keep in mind that there are no set rules as to what you can do and the screens can be changed to suit your needs of the day.

VIDEO PROJECTORS

Projectors are an absolutely viable option as opposed to a complete video wall or in addition to a video wall. There are projectors that are designed for 24/7 continuous use if that is how you are running your SOC. This could be a great cost effective alternative to more expensive video walls. Additionally video projectors can be more versatile in that the size of the screen can be adjusted as your needs change.

LABS

The building of lab can be a vital part of any SOC and a critical tool used every single day if done correctly. A lab environment is typically a self-contained network that includes many different types of devices, virtual machines and may even include a separate Internet connections all built for multiple purposes. The lab can be used to train new analysts on how to manage and maintain equipment that you use on your network. It can contain the equipment necessary for analysts to train towards certifications and you can even use the lab for people to learn new skills that will help advance their careers. It can also be used by engineers to try new mitigation technics or test newly developed IDS signatures before sending them to production equipment. The lab is a great place to try new things that is consequence free if things going bad. These SOC labs can also be used to develop security intelligence by trying new exploits and performing security research and testing.

The value of real hands on experience cannot be matched and with a lab you can give people that experience at any time.

Labs can quickly become very expensive so you will have to build it wisely. To give your SOC the ability to manage and maintain equipment in a lab environment is a huge gift that will pay big dividends. Those dividends will be paid in the form of better-trained staff, better execution of changes and management of your security infrastructure.

The lab environment can also be used to test changes to your critical infrastructure before you do it in your production environment. This will give you a higher degree of confidence that changes are implemented with a lower risk of causing negative impact to your organization.

In your lab you can have virtual systems that contain specialized software and different operating systems for people to try or use. Depending on the size and ability of your lab infrastructure, you can give everyone in your SOC their own server to use and play with. Allow them to develop new tools, test out new skills or install different hacker tools to see what the capabilities are. You can help train your SOC staff to perform different tasks that may be needed from time to time like performing vulnerability scans or even give them the ability to do penetration tests of other systems in the lab. For your analysts you may want to consider training them on passive tools that would aid them in their jobs like being able to port scan systems to see what is responding or banner grabbing of known open ports to help figure out what applica-

tion a server is running. These are all things that can be done in a safe environment in the lab. When your SOC is dealing with more real and live incidents such as malware analysis or performing forensics, a lab is a great tool to be able to contain these types of activities so that it would not affect normal SOC operations if something bad got loose. When looking to purchase new equipment to add to your security infrastructure you can install demo versions of the systems in your lab and perform tests to see how it works and test its reactions to your simulated environment. Additionally you can use the resources of your lab to test your staff with exercises and training materials that will be elaborated on in a later chapter. There is no right recipe for the building of labs, just make sure that if you are going to build one that its proportional to your SOC organization and that you build clear roles and responsibilities and ensure its properly maintained.

There is a lot that goes into what you need to build your SOC. There are 3 distinctly separate areas you need to consider, organizational security infrastructure, operation center infrastructure and support infrastructure. When you evaluate the needs of your organization first it will help dictate what you need in your SOC to support those organizational needs. Then the support infrastructure needed for your SOC will almost design itself but putting good upfront time and creative efforts into that support structure will enable your SOC to perform at the peak of its ability.

The SOC will never run out of things to do as attackers get more sophisticated and running a good SOC will increase your organizations ability to detect and respond to those attacks. With the right tools and right reporting you will quickly gain a positive opinion of the SOC outside your organization regarding what you are doing for them that will result in additional tasks and responsibilities. The infrastructure you design that runs and supports your SOC is just like building a house, you want to ensure you have a good foundation. Do not be afraid to use what you have, no reason to run out a make tons of purchases. Building your SOC can be an iterative and incremental process that grows and builds. It is ok to start small and add people, processes and technology as you mature your organization and develop your goals. It is also ok to look for tools and products that are a champagne taste on a beer budget to get you going, just make sure you are not sacrificing on key features that you will need to be successful. Your organization may just be building its security infrastructure so build your SOC along with it, make sure you are efficient and have all the tools to be successful. I did not even come close to discussing all that is need to support a SOC or an organizations security infrastructure but I hope that I have at least got you going in a good direction, have provided you with some deep thoughts on direction and have given you some insight into some key considerations.

Page left intentionally blank