Daily operations

learning.oreilly.com/library/view/designing-and-building/9780128008997/B9780128008997000069/B9780128008997000069.xhtml

A SOC is not your normal business office atmosphere where people show up to their offices or cubicles everyday on mostly their own schedule or within an acceptable time range. In most office environments, people can customize or personalize their offices or cubes to give them a sense of comfort or a feeling of home. In a typical SOC that operates 24×7 that is not possible, shifts will share desks and computers where personalization is difficult or impossible. The life of someone who works in a SOC is different, make no mistake about it, no matter how it looks or what the space is that you use, if you have a SOC, it is going to be different. Your SOC is on the front line protecting your company by paying close attention to details while rushing to address all priority events stacking up in the ticket queue. It needs to be different, the environment needs to be open, people need to work together, work with each other and count on each other for knowledge, direction, and information. Your SOC needs to be a supportive environment where people are challenged so they can grow and so they come in every day ready to find that needle in a haystack.

It is an interesting ecosystem that needs to be protected and understood to ensure that your staff continue to perform at their best. Your daily operations are critical to the flow of this ecosystem. You have to be mindful of the work tempo, the workload, and individual relationships between people on-shift, between shifts, and with management. Set up your operational schedule up front but do not be afraid to experiment and try new things, as no two SOCs are ever alike.

The SOC is charged with the responsibility of being the first responders to information security incidents and events, they are also protectors of the organizations infrastructure, data and, in some cases, the personal electronic protection of the organizations employees and members. Analysts and engineers need to be held to high standards of conduct, integrity, and job knowledge. As such there are specific expectations and routine daily tasks that need to be performed to ensure that operations happen smooth and efficiently. To ensure continuity and job process integrity are maintained by everyone in the SOC and across all SOC shifts or all geographically separated SOCs. Specific policy and procedures need to be developed in the SOC and documented for everyone to follow. One of the most important of these policies and processes is the SOC daily standard operations procedure (SOP) that provides guidelines for everyone to follow. This chapter represents some of the items you will want to consider implementing in your SOC as part of the daily SOP. It is not meant to be all inclusive as your organization will have other considerations or items that are specific that will need to be included here.

Problem and change event communications

Master station logs

Sometimes referred to as an analyst log, a Master Station Log (MSL) is a great way to capture events that happen outside of a ticketing system or does not have a place to be ticketed such as something that occurs around the SOC but has no place for a true record to be stored. Additionally, the MSL is a great place to highlight items of importance that need to be communicated across multiple teams, shifts, or SOCs. The MSL can be a simple text document that is shared, a workgroup based website like SharePoint or a formal software application that is installed on a server. Either way, the MSL is the official narrative record maintained to document and communicate significant events. As a minimum, like a mini ticketing system, all the entries should contain, the time of the entry, the name of individual making the entry, and the specific details relative to the entry. These entries are necessary for internal communication between shifts and the security groups to affectively monitor ongoing organizational issues that could affect security visibility or the operations in general. It is also a good tool in helping to bridge the gap between shifts or SOCs when issues span multiple time zones or have a lasting impact from one shift to the next.

The events below are an example of what should be reported at a minimum within the MSL.

• Network outage—Any disruption in services that affects the organizations users the ability to perform their job function such as the loss of LAN, WAN, or VPN connection.

• Security outage—Any disruption in security equipment or networks that reduce the visibility of the SOC and limits the ability to perform security services.

• Patching/update notifications from IT or security engineering—Any patching/update notifications to include but not limited to IDS updates, SIEM rule updates, security system reboots, or major maintenance and upgrades. This should include expected service and server down times and what loss of functionality should be expected.

• Hardware failure—server, router, or switch that is has been determined as down or offline and could be degrading performance or causing latency in event detection.

• Special visitors to the SOC such as management, contractors, or auditors.

• Environmental issues such as construction, heating and cooling issues.

• Special announcements made by management

A team leader at the end of every shift should email the MSL or a copy out to the entire SOC organization. This will help ensure that everyone is on the same page and that items that need to be closely watched are documented and communicated effectively. It should be everyone in the SOCs responsibility to review the MSL upon start of their shift to ensure they are familiar with anything that may affect their ability to perform their job function or for anything that they may need to be addressed while on shift. It should also be very easy for SOC leadership to read three reports from the previous three shifts and be completely up to date on what is going on and any issues the SOC is currently facing.

Shift turn overs

Shift turnover is an extremely important part of the shift in a SOC. This is the chaotic time where one shift of people is ending their day and the next shift of people has arrived to start their day. Procedures for performing a shift change should be agreed upon by all the team leads and then posted, trained, and adopted by all members of the SOC. Everyone should know the process to start a new shift and exit the old shift to ensure that there is a clean handoff and that all the required important information is passed along.

To help facilitate the handoff process, each shift should be scheduled with an approximately 15–30 min overlap. This allows for a bit of flexibility in case there are ongoing issues that people need to finish up or if there are unforeseen issues with people showing up on time. The process should start off with all SOC employees spending the first 10 min of his or her shift communicating with the analyst or engineer they are replacing regarding special concerns or critical information. While this conversation is happening, the outgoing analyst or engineer should be finishing up any tickets or calls they may be engaged in and then focus on cleaning their work area for the next person.

The senior shift lead would be responsible for putting together a turn over report that would be emailed to everyone along with the MSL. The shift lead should gather everyone from the shift prior to them leaving for the day and interview each person in a quick stand-up round robin fashion. If any analyst or engineer has a specific issue or items of importance then they communicate it in this rapid-fire forum. The team lead should make notes, ask questions and ensure that they have all the information they need to pass along and ensure that items are addressed properly. Depending on your SOC you may want to formalize roles for this end of shift stand-up report. You could include specific metrics like the number of open events that are being left for the next shift to address, or any specific outages or viruses that are causing problems. Set a specific starting time for the shift change meeting for each shift and enforce it consistently. Make sure you emphasize how important it is for everyone to attend and to not hold up the group, everyone wants to leave work at the end of their shift so being held up by one person is not fair. Because one shift is ending and another shift is starting, the meeting must be completed in a timely manner as to not interrupt the work of the incoming shift and you do not want this to go very long, just long enough to transfer the important details.

The senior lead gathers all the information deemed important to the oncoming shift from the analysts, engineers, and intelligence teams and generates an end of shift email report. The turn over email report will need to be emailed to all SOC analysts, SOC management, or anyone else that would benefit from the information daily at the end of each shift. It should at the minimum captured any critical events that happened on shift that the oncoming shift needs to make a priority, a brief rundown of shift happenings such as system changes, signature updates, rule modifications to SIEM tools, a list of tickets that was worked and that need continued investigation, any other information that the current shift might think will be helpful to the oncoming shift and last but not least it should include relevant cyber intelligence or attack trends that may impact ticket-able events that the shift will likely see.

Between the SOC shift report and the MSL, it all seems like a lot of information and can even be information overload. If you have never been a part of the process before or you are new to the SOC it will be overload but you will quickly get the hang of it and will be able to quickly pick out the important bits that relate to you fairly easy. These reports will change over time and I encourage everyone to try and make these processes better and find better ways to pass on information. More is better when you are doing your shift change, just try and work on how to present the information as best and clear as possible to ensure that everyone has a good grasp on what is going on and what is required for them on their shift.

Each shift coming into the SOC needs to perform some procedures to ensure that everything is setup and working properly. As we discussed, there will already be a hand off process so the incoming shift should be fully updated in the previous shifts activities. The next set of tasks they need to perform is to ensure that all required tools and systems are properly functioning. They should reset the video wall and any projectors to make sure that nothing is hung or stuck, the shift team should check the phones, network connections or any other important technology. If you not running a 24×7 SOC then you need to make sure that phone lines ring into the SOC instead of going to voicemail or an on-call pager. A written process should be created that each shift follows and any issues or discrepancies should be noted or escalated to the proper people to be resolved. Another important consideration is if your handoffs are problematic and items are being dropped or lost, consider staggering your team leads. Have the team leads shifts start and end a few hours overlapped into each shift. That way you have a single team lead spanning two partial shifts as continuity. Also as we will discuss later, having different people in different roles work different length shifts may also help with continuity between shifts. For example if you have the majority of your shift working 8 h but two people work 12's then they can help with the change overs.

Daily operations calls

Depending on the activity level in your SOC or current threat level of your organization you may want to institute a daily operations call. This call would be for your SOC management, team leads or engineering leads that need to perform a verbal review of the day's activities or expectations for incoming shifts. It could be a stopgap measure for management to get better control and visibility into daily operations or it could be a permanent tool that is used to keep everyone in the loop as to what is going on for hot items in the SOC. This is very different from a shift change process, as it will include people who are either not in the SOC or not even be in operations, it could include leads from sales, customer service or IT, depending on your organization. The daily operations call is a management review where SOC leadership gets to report on highlights of the day to management. This could include internal or external customer issues, missed SLAs, ongoing incidents or upcoming events that are significant to the operations team such as network maintenance or outages that may impact operations. The SOC leadership can bring people into the call that they think will add value, this could even be an analyst that is working on a particularly sensitive issue that would be able to answer questions or add valuable details. The meeting should last no longer than one hour and in most cases should be less. During times of critical issues the meeting could include individuals internal to the organization that want to keep close tabs on issues but this is not the time to perform incident response (IR), it is a management review and update call.

The format for this call should be very simple, it should be the senior team lead or manager reporting on activity that they deem to be important or what they think will impact performance moving forward, such as an outage. Then SOC management or security management such as a CISO would have an opportunity to comment or weigh in on each of the topics and provide guidance or take action items to resolve problems. This is a great way to ensure that there is good communication throughout the entire SOC organization and that management is properly engaged. Not only is it good to ensure management is engaged but it also gives them a good opportunity to ask questions, make course corrections or provide them with valuable inputs that they need in order to address issues externally. There are two possible times that this call should happen. The first logical time would be after the first shift change, at the start of second shift. This would typically be at the end of the normal workday about 5:00 p.m. Depending on your SOC and if you run a 7×24 or have many SOCs around the world you may also want to consider a morning call as the primary call. By doing this call in the morning at about 8:00 a.m., you can get information at the end of third shift and help set the stage for first shift, but it may also be the start of second or third shifts elsewhere in the world. If the management calls seems to work then do not shy away from using it, there is no reason to not have two calls, one could be in the morning and the other can be in the evening, either way you will be able to capture inputs from all shifts and have good high level discussion, if you place the calls carefully in-between shifts and logically to how you split your shifts then you should be able to keep up to date on all important activity.

Critical bridges

Because the SOC deals with critical issues that affect the confidentiality, availability, and integrity (CIA) of an organizations data and systems, it is important that when there is an incident that impacts the CIA for an organization that communication be handled quickly, efficiently, and properly. Sometimes depending on how the incident effects an organization or who it affects you will need to swarm the issue. An emergency hotline or critical bridge may be a way to break outside of the normal processes and get the right people to the table to address and resolve issues quickly.

In many cases, escalation to authorities, engineers with different skill sets or to people with different access privileges may be necessary. The SOC is sometimes not in a position to take action all on its own. In some cases, the SOC is only responsible for monitoring a system but cannot make any decisions about it. The analyst needs to know who to call to get approval to remediate a threat or to get someone who can make a needed change that would prevent or fix an issue. The SOC procedures must be documented and have some rules on escalations or when to establish a critical bridge. It should be noted that an analyst should have the power to establish a critical bridge at any time if they deem it necessary, nobody should get in trouble for starting up a critical bridge if it was determined that it was not necessary. You need to make sure that your analysts feel comfortable engaging and asking for help.

Depending on your organization, the critical bridge escalation procedures could be based on the type of system, the type of attack or the business/organizational unit affected. The choice very much depends on how your organization operates, where the risks are, and what works most efficiently for your organization.

Ever wish you had a big red phone that you could just pick up and the right person or people will already be at the other end of the line waiting to help you? Well this is how you can accomplish pretty much the same thing at the time of crisis.

Swarming is not a new concept but using it in a critical operational environment with potential remote or geographically separate resources can be a simple thing to overcome. By swarming an issue, you quickly bring a diverse group of experts together in order to assess and solve complex problems as a team. When you swarm a technical issue like this it could be a quick 5-min call where someone jumps in after hearing the initial problem and then clicks a few buttons and all is good or it could be several hours where multiple people are diligently working to resolve a large problem.

A phone bridge or standard conference call number can be established and all the key people you want to be a part of the critical call or emergency hotline can be given that information to be programed into their phones. Then a webpage can be established that includes the ability to send out a group text/SMS message that notifies everyone that his or her presence is required on the conference call for a critical issue. The text message can either go out to a primary person or if you are able to add logic to your system a secondary or backup person. You also want to ensure you have a paper version that documents this process that details everyone who would need to be on the emergency hotline, their phone numbers and who their backups are in case they are unreachable or on vacation.

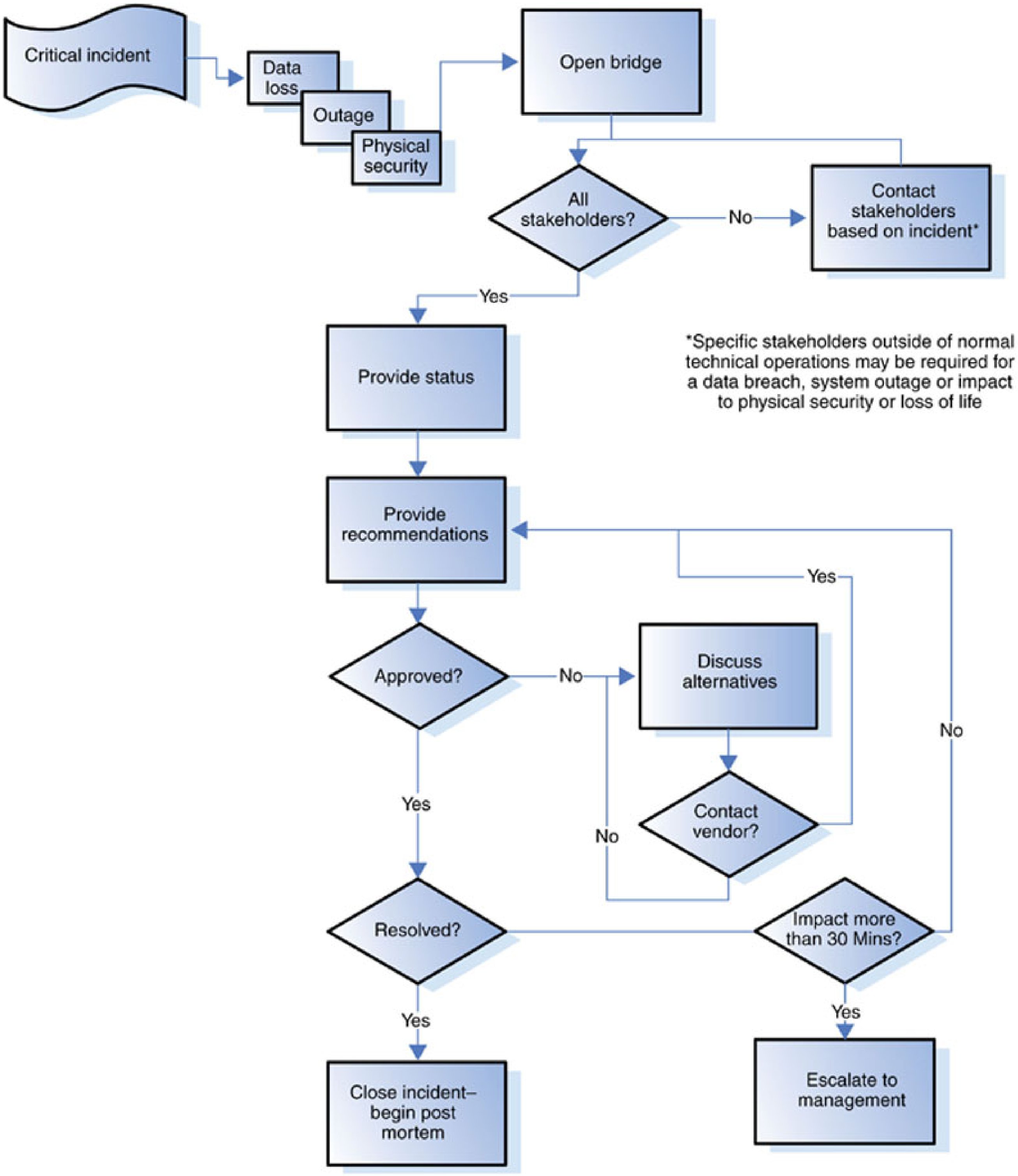
In case of a critical or major incident defined by your organization, which could include a system being attacked, a potential compromise, a denial of service attack or even an unplanned outage, an analyst can, as part of or in addition to IR processes initiate a critical bridge. This can happen any time day or night, it does not matter what time it is as long as the bridge is established in a reasonable time after a critical incident is detected and not too long where participants cannot be effective in making positive remediation's or key decisions. If it takes too long to establish the bridge and get all the right people engaged then there may be too much damage for anyone to do any good, so the calls need to be made quickly after incident discovery and classification. Because these calls can happen at any time you may want to develop a process that has different people on an easy to understand call rotation so that the same people are not being woken up every night.

Once the bridge has been opened and all required personnel are present the SOC will brief everyone of the status of the incident. This brief will consist of where the incident is occurring, who is causing it (if known), what the incident consists of, how long the incident has been going on, and what the potential root cause of the incident is. After the briefing, the SOC will give its recommendations for remediation of the incident, and then open the floor for discussion. During this time, the remainder of the SOC team who are involved will continue their investigation of the incident and provide updates to the bridge as necessary. Once an approved remediation step has been decided upon, the SOC or engineering will implement the solution and provide an ongoing status to the bridge. If it is considered necessary by the bridge team to contact the vendor of the system, the owner of the system or anyone else that can provide value to the team, the SOC will initiate the contact with them. The addition of any further resources can be done on an as-needed basis and would depend on the issue. If the initial remediation action fails or is not complete, the SOC may deem it necessary to escalate to a management in order to inform them of any potential impacts or customer issues that may result from the event. This gives management an opportunity to get ahead of the problem and make any arrangement for initiating proper customer communications or may even allow them the chance to authorize a partial disaster recovery plan to get business flowing again if it is impacted. Management may also be needed to approve the removal of systems from service or to rapidly rebuild systems, regardless of action, management should know if there is any impact to business services or any impact to customers.

Additionally if the critical incident is deemed to have a data loss that would be consider a breach or loss of credit and payment card information or a loss of personal health information then other specific groups must be involved as part of the bridge escalation process. The groups that you may want to include are legal or a privacy department but maybe if you are a large retailer you may have a banking department or credit department that has ultimate responsibility for breach notification to the acquiring banks or credit card companies as required by contract. There may be very specific state, federal, or international laws that you will need to follow after detecting a data loss. By including other groups in the call once you have positively determined a data loss then you are going to give those groups the best opportunity to make key decisions and to make notification to the proper authorities in a reasonable amount of time. It is important for effective daily operations that the SOC work with the organization to understand who would need to be contacted and when for various types of incidents and who would need to be engaged on a critical bridge at the time of significant incidents. Depending on the type of incident, its criticality and who needs to be engaged, it would not be uncommon to have two critical bridges going at once. The first bridge can be for technical experts working together to resolve the issues and the second bridge can be for management and other business resources. This way the conversations can be kept separate and will not get people confused or taken off track of their primary focus. The SOC would act at the liaison between the two calls and would provide updates to both bridges on regular intervals or when important information needs to be relayed.

Once remediation is successful, the incident is considered closed. The bridge will be closed and the SOC will begin building a post-mortem briefing that will be delivered to all involved parties and should include any compliance teams in the organization as well, if available. The briefing will include details around the original event, a complete timeline, who participated on the bridge and what remediation actions were taken. It should also include a root cause analysis and a list of action items that would be needed to prevent future occurrences. It is important that when performing root cause analysis and post-mortem briefings that the documents are kept factual and that the process is not used as a weapon against other teams or evidence as to how someone is not doing their job. For example, if the IT department is responsible for security patching on servers and an attacker is able to take advantage of a vulnerability that was not patched, this is not the time to beat up the IT department. Instead, make sure that you detail the vulnerability, the time frame in which the patch for the vulnerability was available and then you can make comments on the need for increased efficiencies in patch management. The post mortem process can quickly turn to finger pointing and will often put people on the defensive, this takes away from the core focus of helping an organization becoming more secure. The SOC should always ensure they take a factual and passive approach to documenting deficiencies and let management and business leaders work through the challenges that may be present in an organization. Do not let passion to be secure or passion to provide the best service possible get in the way of achieving the goals of the SOC.

The following is a flow of how the critical bridge process can work, it is very similar to the overall incident flow but has the deviation of opening the critical bridge and managing the bridge process.


Critical incident
Data loss
Outage
Physical security
Open bridge
All stakeholders?
No
Contact stakeholders based on incident*
Yes
Provide status
*Specific stakeholders outside of normal technical operations may be required for a data breach, system outage or impact to physical security or loss of life
Provide recommendations
Yes
Approved?
No
Discuss alternatives
No
Contact vendor?
No
Yes
Resolved?
Impact more than 30 Mins?
Yes
Yes
Close incident–begin post mortem
Escalate to management

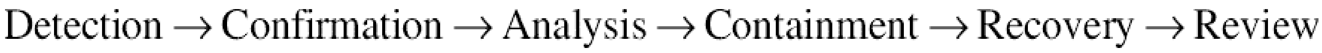
IR

Auditing to regulations whether it be Sarbanes Oxley (SOX), Payment Card Industry, Health Insurance Portability and Accountability Act (HIPAA), or whatever your industry requires is a necessity. It is a good tool and sometimes is required to get Information Assurance goals moved forward. A security department and especially a SOC need to embrace auditing and work with auditors as best as possible and make things as easy as possible. But it seems that without fail, whenever I have built an enterprise SOC in a regulated environment I seem to always get an auditor from an external company that comes around to ask when the last time the SOC tested and practiced an IR.

Key point: You can interview your auditors, even ones provided by large external auditing companies to ensure you are getting the best value for your money.

Joking aside, the SOC performs real IR every single day and with every event that has a ticket created for it. The processes that the SOC has are exercised and used for the most part every single day. The SOC lives and breathes IR and as such are experts in this area. Everyone has different ideas about what should be or not be included in an IR process and many aspects of that process are specific to the organization that the SOC is working for. To that point, I do not want to spend a ton of time going over IR other than to lightly cover key elements in the SOC's view into those components.

Incidents can occur in many different ways, so it is not realistic to provide detailed instructions for every imaginable combination of attack or type of incident. Organizations should strive to prepare processes for incidents that use common attack vectors or cases that are commonly seen in the environment. Different types of incidents merit different response tactics. There are many different types of attack vectors and specific handling measures that should be followed so all IR will follow a normal process that is repeatable, efficient, and logical.


Detection → Confirmation → Analysis → Containment → Recovery → Review

Detection

IR starts off with someone or something detecting and reporting of an event that needs a closer look. This could be a security system or IT infrastructure that sends a log into the SIEM environment and then gets ticketed into the SOC because it met specific thresholds or triggered specific rules. It can also be a user, system administrator or external entity that calls or emails in to report something. No matter how it happens, someone or something detects and reports an event.

Confirmation

Once the SOC has a ticket with all the relevant information, the analysis can begin. The analyst will triage an event, work to categorize the event and try to find what the root cause of the event was. It is vitally important at this step that the analyst do their best to answer the basic question of how an event occurred. It is the real root cause answer to how it occurred or what impact it caused that sets off other wheels in motion. If an analyst confirms an event that has been ticketed is true and that it is either a threat from a malicious threat source or needs further action, then more processes will take place. If on the other hand if an analyst sees the event as a non-issue and can confidently close the ticket with a reasonable explanation as to why, then the ticket is closed and no further action would be required.

Analysis

An in-depth investigation must occur by the SOC to know the full scope of what happened. Analysis or IR teams must establish how successful the attack was, all the systems that were compromised and all data that was access or removed from the devices if applicable. The full extent of the incident needs to be well understood and a complete timeline needs to be documented to ensure that all questions about the incident are answered. For example, analysts should not have any network traffic that is unaccounted for or that cannot be explained. Was there privileged access, were all logs collected, how long did the incident takes place, and what was the ultimate method of compromise. If any data was accessed an in-depth review needs to be performed to understand the nature of the data and if it was intellectual property or regulatory protected data. During this analysis phase is when a determination should be made on how to escalate and communicate the incident. As we will discuss later, the communication plan will be a key document to use once analysis has been performed.

Containment

If an event indicates that there is something bad happening or about to happen, then the event can instantly become an incident and the SOC needs to direct activity in order to have the event contained. The primary purpose of containment is to ensure that further negative impact does not occur. This could be the removal or isolation of a system from the rest of the network, enhanced monitoring, rerouting of network traffic or even the blocking or removing of an email now known to contain malicious attachments. There are many different ways to contain an incident and each will depend on the type of threat, devices, or data that is being threatened as what techniques you will use. Also, during the containment phase the SOC should be rapidly collecting information to understand the full scope of the incident. This information should include a list of any compromised systems or accessed systems, data accessed and a timeline should be generated. Additionally, network flows, IDS events, or any other data related to the attackers activities or the particular incident should be captured and stored in the ticketing system.

Just a word of caution, before you perform containment actions ensure you are working with the system owners in your organization or you are very aware of the outcome of any containment actions you take. If you are not careful the actions you perform could cause a worse consequence than the security issue you are trying to protect against.

Recovery

The recovery phase can be as simple as reinstalling a server or workstation from backup or performing a fresh install all the way to a planned remediation event that includes a complete network shutdown and rebuild. A complete recovery event could include changing everyone's passwords, making significant active directory policy changes to harden the environment, and applying security patches to everything. Depending on the type of event and what you need to do, your actions should not only recover your computing environment back to normal but also keep that type of event happening again. The analysis performed in the previous phase should be detailed enough and clear enough to know exactly what the vector of the incident was and how you would need to prevent it from happening again. The changes needed to be performed could be specific application changes, business processes, or network policy rule changes.

Review

All incidents should have some form of a review whether it be a quality review, a root cause analysis review or an administrative review by legal, compliance, management or other interested parties depending on the scope and degree of the incident and outcome. The final review and reports that the SOC generates for critical or high priority incidents must be completed in a reasonable amount of time to allow for external notifications within any legally mandated time period, if appropriate.

The review document, or root cause analysis document should answer all the questions anyone would ask. It should at a minimum answer who, what, where, when, how, and the impact of the incident. All of that information must be in the report so that there can be a better understanding of root cause or what deficiencies were present in the network or the individually affected systems to allow the incident. It is also important to understand trends or motives of around the incident. A SOC needs to mature and these types of review documents will help make that happen faster and faster. By doing the reviews of individual tickets or incidents for quality control and getting feedback and questions about the incident and the analysis from different viewpoints is extremely valuable, but also doing larger more visible root cause analysis reports gives a SOC a detailed understanding of how they did and what they could have done better. It is a good learning tool and will help the SOC move from a reactive to proactive mentality and will ultimately lead them to be more predictive.

We spoke about the maturity of the SOC before but this kind of review is a key ingredient to help make that maturity happen. You will know if your SOC is reactive in securing the organization because they will be focused on post incident detection, confirmation, analysis, containment, and recovery as we have just discussed. The SOC should always perform their tasks in the above way but if the focus is on the process and executing the process then they are reactive. Once the SOC starts to grow and mature they will start to be more proactive. This happens when the SOC has the ability to avoid threats against computers and networks through the understanding of the environment, working with different groups or departments in the organization and IT and be able to analyze potential future impacts along with the ability to implement defensive measures. Lastly, the analysis done on incident reviews and understanding trends and motive will allow the SOC to become more predictive. They will be able to anticipate future threats and vulnerabilities based on that strategic analysis along with threat intelligence, and the understanding of how the correlation of the two will impact the organization. The goal of maturing the SOC should not be to move the entire operations into a predictive mode. Instead you need to stay focused in each area while you move toward a predictive security posture. For example, performing forensics and malware analysis is an advanced skill set that you can either have in your SOC or use the services of an external third party or MSSP. The forensics and malware analysis function is reactive in nature but advanced as far as skill sets. The SOC should have advanced skill sets across each of the evolutionary areas in order to provide the best operations to secure an organization.

Communication plan

The SOC should have a standard communication plan above and beyond what we have already talked about in daily operational management calls or critical bridges. This communication plan should detail all the different scenarios where distinctive people should be contacted and what their contact information is when specific events or incidents occur. Organizations should work hard to establish the best IR communication plan as possible and it should be reviewed on a regular basis to ensure that lessons learned and organizational changes are accurately reflected.

The communications plan should include an easy to read table of contents that list specific types of incidents and page numbers or tab number. Each incident listed should have a short description of the event along with conditions in which an analyst would execute the communications procedure.

The procedure should be a list of functions or roles of people in the organization or outside the organization that would need to be contacted. Some of the communications would be through email where as more critical notifications would be direct phone call. Each incident would have its own listing of who gets emails versus who would get the phone call. The variation of who gets what would be listed on a case by cases basis based on the incident as different incidents would have different importance’s to different departments or groups. The plan may just list the departments or individual roles that an analyst is to call, such as V.P. of IT Infrastructure or Security liaison to Legal, external marketing or communications. The plan should not list individual’s names in the description or procedure portion, instead the specific names and contact information should be included as an easy reference in the back of the plan. This way the plan does not need to be updated every time someone changes phone numbers or positions.

Each person assuming a role in the organization that would have incident or breach notifications should have a simple record of contact information in the back of the procedure book. The information to include is basic:

- Name
- Title
- Phone #
- Alternate phone #
- Email address

The number of people that can be included in the communications plan can be extensive, it may be more manageable to split the contacts up into different groups. For example, the first group could just be general SOC and IT management along with other closely interested people. For example, if you had an internal incident that was a violation of policy you may want to include SOC and IT management and also HR, but it may not necessarily be appropriate to contact legal right away. Instead you may want to save notification to legal as a secondary escalation. Then if legal believes that the person should be arrested or if there is going to be an external agency brought in then you may want to include public affairs as a third level of escalation notifications.

Additionally your notifications may not necessarily be just to individuals that are assuming roles in your plan. You may also want to reach out to vendors or third parties that may need to get involved to help or provide services. This could be an IR team as part of your managed security services, or just your Internet provider that can help you block specific types of unwanted traffic. If your SOC has a relationship with local law enforcement you may want to include them as well.

Here are some of the people you may want to consider being part of your communications plan:

- SOC manager
- Incident handler
- Legal affairs
- MSSP
- Privacy officer
- CIO or CISO

- Public affairs
- Internet service provider
- Internal audit local law enforcement
- Local FBI
- Bank
- Human resources

Regular workshops

Once you have established your incident processes and communication plans you need to get on a program of continually improving upon the program and making sure everyone is up to date. You cannot just sit back and feel good that it is done because sometimes as soon as it is done you will find its time to update it.

Annual or quarterly workshops are a great way to not only make sure that all the information is correct in the communications plans but that everyone still agrees with the processes. Brining organizational leaders together and the people who are part of the communications plan to discuss the detail of the plan will help to keep everyone knowledgeable and up to date. The workshops can consist of an update of everyone's personal contact information. It should also then talk about any metrics or challenges the SOC has had regarding the execution of the communications plan. Lastly there should be a table top discussion and sample scenarios that are discussed to see how people would respond, who would want to be notified and what details would trigger additional actions. These regular workshops are a great tool to help validate that the SOC processes are not only the right processes but that they are appropriately up to date.

The workshop is also a great training opportunity not only on the process itself but not everyone lives with security everyday like a SOC, so it is a good opportunity to discuss security, its importance, and the value the SOC brings to an organization. Do not miss a great opportunity to market the SOC and help bring the mission of security to the front of people's minds.

Checklists

It is important to have some basic checklists that the SOC will use in the daily environment. These checklists can be built into the ticket system that is used in the SOC, be a webpage, word document, or can just be paper copies. Either way, it is important for processes to be consistent and to ensure that analysts and engineers capture the right and complete information that is needed, make sure you have checklists that mimic your important processes.

The example below is an incident report form, this form could be used to document a specific incident and that would be used to distribute information to interested people or management. It should be factual and accurate and should include all the relevant information someone would need to make basic conclusions about the incident. The form should relate to a specific ticket and the ticket would have more detailed information and back-up data to support the completion of this form. A status should be stated on a form like this, an open status would indicate that the form is being worked on and could be waiting for more input. Whereas an in-progress status may indicate that the form is complete but that action items or activities are still pending. Lastly, a closed status would mean that all actions have been take and the issue is now fully resolved.

The type of issue could be related to the category of the threat such as a virus, insider threat or denial of service and the result of the activity would also be detailed to include an indication if there was any outage as a result. To answer the question of who did it, you should try and determine the origin of the attacker. Sometimes it is easy because it could be an insider or unknowing accidental system administrator or it could be an external hacker and even a former employee.

The rest of the form is fairly straightforward and should be self-explanatory. Once complete a copy of the form should be associated or uploaded to the original ticket that was used for the investigation and then it can be emailed or stored in a central location for others to review and comment on. The form can also be established inside of your ticketing system or in an IR portal. Completed form submissions can be automatically emailed out and also have the answers stored in a database. Depending on the criteria you use to complete these types of forms and how frequently you use them, it may not be a bad idea to perform a weekly or monthly review of all incident reports. You could have management representation as well as technical experts review the forms to make sure that needed action items are being taken care of and that if specific trends are emerging then those issues can be bubbled up to a more strategic level to be dealt with. If you have enough of these forms being filled out, you may even want to perform regular metrics and trend analysis on various elements in these forms as well, it may help you get a better idea on some of the organizations weak spots or at least be able to quantify the costs associated with your efforts in dealing with issues that are not getting resolved.

SOC Incident report form			
Ticket#:	Status:	Date:	Reporter:
Type of issue:		Results:	

SOC Incident report form	
Has the problem been experienced before? Yes / No	Caused outage? Yes/No
How was this detected?	Attacker?

Target system(s)			
IP/MAC:	Mission critical?	System type	Additional info:
	Yes/No		
	Yes/No		
	Yes/No		
	Yes/No		

Current security measure(s) in place			
□ Firewall	□ HIPS/NIPS	□ Strong passwords	□ Whitelisting
□ Antivirus	□ Encryption	□ Physical security	□ Log monitoring
□ Anti-spyware	□ ACL	□ Warning banners	
□ Secure remote	□ File integrity	□ Digital signatures	

Recommended action			
□ Disconnect	□ Validate binary’s	□ Inform legal	□ Restore
□ Validate Permissions	□ Physically secure	□ Reinstall	□ Virus scan
□ BLOCK	□ Collect logs	□ Vulnerability scan	□ Forensics
□ Other:			
Relevant packet or log data			
Comments			
Timeline			
After action notes			

Other types of forms can be useful but as you develop them but do not make them too ridged, allow for modification and alteration. All too often when you put a new form into operation you may quickly discover deficiencies or issues. Allow your forms and checklists to change as you grow, mature, and learn the needs of the organization you are protecting. Sometimes forms and checklists can come from necessity, if there are operational issues where people are not following direction or mistakes are occurring too frequently, enforcing that a checklist be completed can help not only be informative to ensure everyone knows the process and the required steps but will also help resolve any issues with people cutting corners or just not following process.

Other types of forms and checklists you may want to consider using are specific incident forms such as a checklist regarding what to do in the case of a credit card breach or loss of Patient Health Information. If your organization has lots of direct connections to other organizations through VPNs or direct links then you may want to checklist for how to handle incidents regarding third parties. The checklists do not have to be based on incident workflow, it could be for any process, but the primary checklist you will likely have will be based on either incidents or troubleshooting of tools in the SOC.

Shift schedules

Planning security operation shift schedules can be an art but the goal is very simple right? Just make sure you have the proper coverage during the hours you need it most.

One of the main questions I get asked about running a SOC is what the best schedule is to maintain and how to maintain schedules with SOCs that may be spread out all over the world. SOCs that want to run 24×7 will have its own unique staffing problems and many of these will concern what the right recipe is for staffing levels and who they have to fill needed shifts. The fact that an organization offers security services or wants to monitor its network around the clock does not always mean that the staffing requirement will remain constant. You will need to make sure that the ebb and flow of staffing changes and fluctuations are properly reflected in your scheduling. You will most likely have your workday divided into something that resembles a shift, even if there is only one shift, which is a normal workday or weekend. Each shift will have different requirements in regards to staffing levels, skill mix and the type of role you need to be present in the SOC. For example, the workload in the SOC may require two people during the week but only one during the weekends. You will need to make sure that whoever is responsible for managing the staff schedule is fully aware of what will be needed for each shift and that they have the right reports and metrics to back up the schedule. For large operations, this is not just a case of devising one schedule and using it continuously without regard for changing conditions, you have to be able to adapt. The demands in regard to work will always be changing in most organizations and staffing levels will need to reflect this, especially around the holidays and for international organizations you will need to consider staffing in all your SOC locations based on international holidays, not just the more popular or local holidays. The person looking after scheduling should be able to anticipate what is going to be needed for each shift and should be able to plan accordingly far in advance. Determining and maintaining optimal staffing levels is critical to efficiency of your operation. Overstaffing is costly and you may not have the required resources such as computers and desks to allow everyone to work, this may result in you sending people home so it is not just a cost to payroll, it is also a moral issue. If overstaffing happens to the same person over and over it could cause that person to lose interest in the organization and result in them having poor performance on the job, as they will feel underutilized and not needed. On the flip side, understaffing creates can create stress and pressure on your SOC staff and also can cause excessive overtime. It can also become a safety risks from fatigue, absenteeism, and even cause burnout.

In SOCs that needs to operate 24-h a day will require several shifts filled with different people performing in different roles and who have distinctive skills sets to ensure that all the hours are covered and the right resources are available to deal with any incident or event that occurs during that shift. The first shift or day shift usually would start around 8 a.m. and go until 4:30 p.m. The day shift is a nice shift to have in a SOC because it is the most normal working hours. It would mimic what the rest of the organization and the world work for the most part. Second shift, evening shift or what is also commonly called the swing shift is a shift that starts in the late afternoon at about 4 p.m. and runs into the late evening typically until about 12:30 a.m. Working on the swing shift can be demanding, especially for parents, as it requires unusual sleep schedules and does not work well with school hours for kids who may need daycare. Nevertheless, there are some advantages with being on the second shift for students as it may allow them to take courses in the morning and early afternoon, and then go to work in the evenings.

The third shift is also known as the night shift or graveyard shift. This shift will typically start at 12 a.m. and go to 8:30 a.m. The night shift can be very difficult to adjust to even if it is your permanent shift. A nice benefit to the night shift is that it does give you the day off to do errands, attend to kids or anything else you want because most places will be open for business once you get off work. People who work the night shift will typically stay awake for the day and sleep during swing shift so that their daily routine is the same as most people where they wake up, get dressed, and go to work albeit midnight. There are many different variations of shifts and schedules, and organizations will have to figure out what works best for their organizational goals, the SOC and their people. Typically, the more senior someone is in a SOC, the more he or she will be able to control their own work schedule or choose the shift that works best for them, while less senior people will usually find themselves on graveyard and swing shifts, rather than the usually coveted first shift.

Types of shift schedules

8 × 5

	Weekly SOC schedule						
	SUN	MON	TUES	WED	THURS	FRI	SAT
First shift 9 a.m. to 5 p.m.		X	X	X	X	X	

In smaller organizations, doing a standard workweek where people come in and work in the SOC an average of 8 h a day Monday to Friday may be sufficient. This does not mean that people will only work standard hours. Instead they can be on-call or configure their SIEM to alert them via SMS or email when something passes a threshold and triggers an alert that needs to be addressed. This is a great option for smaller organizations that cannot afford to hire lots of people for round the clock shifts. With a simple schedule like this you could run your SOC with only one or more people. Also, in smaller organizations it is typical to see network traffic be dramatically reduced after the normal workday is over. This is because there are less people on the network generating events, and triggering rules. This means that the rate of incidents will go down that require investigation and the SOC can let the system run on autopilot and just get alerts remotely when something is going bad. If this is a problem and people are not able to sleep at night because they feel nobody is watching the security of the organization then instead of hiring more people you can consider outsourcing to a MSSP. During the day, the internal SOC will handle all the regular Tier-1 events all the way up to the engineering issues but at quitting time the SOC can just turn over the initial triage and Tier-1 analysis to the MSSP. With an MSSP doing the overnight monitoring you can rely on them to analyze events and only call you when needed. Instead of handing off the analysis to an MSSP, you do not have to be an on or off type of relationship, you can keep the MSSP monitoring 24×7 and your internal SOC can just handle escalations by the MSSP around the clock and perform IR as needed. If you only have one person running all of your security then you may also want to look to see if you have anyone in your IT organization that could be a suitable backup resource in case of that one person going on vacation or taking sick time.

8 × 7

	Weekly SOC schedule						
	SUN	MON	TUES	WED	THURS	FRI	SAT
First shift 8 a.m. to 4:30 p.m.	X	X	X	X	X		
First shift 8 a.m. to 4:30 p.m.			X	X	X	X	X
First shift 8 a.m. to 4:30 p.m. (*Optional)		X	X	X	X	X	

If the SOC needs to cover weekends because the organization is active or there are specific risks that need to be monitored for, then an 8×7 schedule can be used. In this schedule, you can do multiple things and start to get creative but as before the SOC is only staffed during normal business hours. You need at least two people to accomplish this schedule and have your weekends covered. With this schedule you have each person work one weekend day and only four work week days. This way each person still gets two standard days off but each has to work only 1 weekend day. This is also a nice option because they will still be able to work together, train together and advance security together during the 3 days that they are overlapped. Sometimes this schedule can get in the way of peoples personal time or family vacation plans when it is every single week that they need to cover a weekend day. The two people may be able to cover a shift for each other from time to time or a week, and then have it made up to them in a later week. Another option is to bring in a third person assuming the workload warrants it. This third person could work a normal Monday through Friday shift and cover on the weekends when needed. Also, keep in mind that having three people at the same time in the middle of the week may be too much, but it gives you the option of spreading things out and creating an optional rotation.

15×7

The next logical step once you need to grow the number of hours people are in the SOC is to move to a 15×7 schedule. This is a great option for an organization that may need to cover hours of operation in multiple time zones. If the SOC is located in the eastern part of the US and business hours need to be maintained in the SOC for the west coast then there are additional hours that need to be covered. Adding a second shift would easily cover the 3-h time zone difference. You can also easily move the two SOC shift hours to start earlier to cover GMT, Eastern, and Pacific Time zones.

	Weekly SOC schedule						
	SUN	MON	TUES	WED	THURS	FRI	SAT
First shift 8 a.m. to 4:30 p.m.	X	X	X	X	X		
First shift 8 a.m. to 4:30 p.m.			X	X	X	X	X
First shift 8 a.m. to 4:30 p.m. (*Optional)		X	X	X	X	X	
Second shift 4:30 p.m. to 12:30 a.m.	X	X	X	X	X		
Second shift 4:30 p.m. to 12:30 a.m.			X	X	X	X	X

	Weekly SOC schedule						
	SUN	MON	TUES	WED	THURS	FRI	SAT
Second shift 4:30 p.m. to 12:30 a.m. (*Optional)		X	X	X	X	X	

24×7

	Weekly SOC schedule						
	SUN	MON	TUES	WED	THURS	FRI	SAT
First shift 8 a.m. to 4:30 p.m.	X	X	X	X	X		
First shift 8 a.m. to 4:30 p.m.			X	X	X	X	X
First shift 8 a.m. to 4:30 p.m. (*Optional)		X	X	X	X	X	
Second shift 4:30 p.m. to 1:30 a.m.	X	X	X	X	X		
Second shift 4:30 p.m. to 1:30 a.m.			X	X	X	X	X
Second shift 4:30 p.m. to 1:30 a.m. (*Optional)		X	X	X	X	X	
Third shift 1:00 a.m. to 1:00 a.m.	X	X	X	X	X		
Third shift 4:30 p.m. to 1:00 a.m.			X	X	X	X	X
Third shift 4:30 p.m. to 1:00 a.m. (*Optional)		X	X	X	X	X	

When you move to a 24×7 schedule you need at least six people but with only six you leave no room for sick time or vacation time. It would be best to have at a minimum nine people working in your SOC for complete 24×7 coverage. This will allow several overlap opportunities and shift rotations to cover for any absenteeism. Adding in the third shift is an interesting dynamic and you need to pay close attention to how you operate this. The third shift can easily start to feel left out, as there may be less management members on a night shift, fewer opportunities for special projects and less options for training. If most training opportunities happen during the day then your third shift will be left out. Make sure you give them the option to stay late for early morning training or allow them to temporarily switch their shift for the duration of a training program.

As you grow larger you may have several combinations of each of the previous schedules all going on at the same time. You may find that what works best is that the analysts will cover 24×7 monitoring but engineers will only work 8×5. To compensate for not having engineers physically available for every shift, the engineers can work out an on-call rotation. This way the SOC analysts can reach out to an available engineer at any time to assist with issues or problems. These on-call engineers would also be the ones to participate in management calls and critical bridges if needed. Additionally, SOC management may only work normal business hours but can also be on call for any critical problems that arise.

Different roles and responsibilities may be needed in the SOC at different times of the day or night or even weekends. The size of your SOC and the volume of work that your SOC performs will also be a driving factor in how you manage your shift schedule.

Other shift options

12’s

One popular SOC shift schedule is to run is to have a few people on 12-h shifts. This is a great idea if most of the SOC members are on 8-hour shifts and a few are on 12’s. This allows for greater consistency between shifts as you have individuals who overlap and are able to blend information for those two shifts. An individual who is going to work 12 h shifts will typically do 3 days of 12 h shifts in a week with 4 days off and then do 3 days of 12-h shifts with 1 shift of 4 h in a 2 week period. This way the SOC member gets a full 80 h across 2-week schedule. It is not advisable to try and run two 12-h shifts as your only shifts to cover the complete 24-h day. The 12-h shift can be popular with some people but not everyone as it could lead to a drop in productivity and fatigue. But some people will enjoy the extra days off that a 12-h shift will bring them.

4 Tens

Sometimes there are SOCs that will run 4 tens as an optional rotation. This is where people will work four 10-h shifts in a row with a 3-day weekend. You would run this the same as the 8×7 schedule where you will have overlapping days. The one advantage of doing this is you can get greater overlap in the shifts across 24 h and you will also have greater flexibility when looking to provide training to everyone in the SOC. Not everyone is cut out for this type of schedule and this will typically have the highest burnout rate. On the other hand people will enjoy having 3 day weekends every week and that may be a great moral booster.

Follow the sun

I often hear about operations groups doing a follow the sun rotation to manage needed coverage for their SOC. The follow the sun shift rotation is where a SOC located in the Americas, Europe, India, and maybe the Far East have been established. Each SOC will work during normal daytime business hours and hand over tickets and issues to the SOC in the next time zone as the day goes on. This seems to be a popular option and a logical one but I have seen more problems with this model then any problems it was designed to solve. This can be very expensive as you have a duplication of offices and facilities that go unused for 16 h out of 24 when you are only running an 8-h shift. You also loose efficiency and accuracy in shift hand-off because it is not happening face to face unless you use video conferencing. You also have to deal with inconsistency in training, customer service and skill sets. A better practice for the follow the sun shift rotation is to have one primary SOC run 24×7 and have other SOCs around the world take on work as needed. This helps establish a base with core skill sets that will control the flow of work and will stay on top of escalations. The SOCs located in different countries can be established to help with international privacy laws regarding the moving of protected data outside of the country. Having international SOCs around the world can also help with local language support if you have customers or business units in foreign speaking locations. If you do have international or geographically separated SOCs make sure you work to blend them as best as possible. All the SOCs will need to share processes, knowledge and work load. If travel budgets are available, move people around from SOC to SOC, this will give them exposure to coworkers and allow them to build good working relationships with each other. It may also be a nice benefit to allow someone to do international travel for a few weeks, it gets them away from the daily grind and helps expand their experience while building new bridges with coworkers.

Shift rotation

Shift rotation is a practice followed by many organizations that work 24×7. Analysts and engineers working in the SOC will do a rotation of nights to days to swing shift and back again on a regular basis. Some people may feel that this is a fairer way of assigning shifts especially when people do not really like working nights. Keep in mind that people will encounter problems with this rotation system as it can be difficult for people to adjust to the time changes. Try to make sure that people have a few days gap to adjust otherwise people can start to have some health problems. Alternatively, it is preferable to have a permanent night shift where people are hired specifically to perform during those times. Keep in mind that for people who work the third or overnight shift you want to work out a way for them to get any training the rest of the SOC may get such as switching their schedules temporarily or trading them temporarily with someone who is on first shift that may already have the training. This training can also be given early in the morning as they are finishing their shift or later in the evening and they can come in earlier to start their shift.

The way you run a shift rotation is based on a 28-day revolution. A slow, forward rotation from day shift to swing shift to night shift will happen across the 28 days. It will take your four teams of people (which could only be 1 person per shift) to accomplish a complete 24×7 rotation and the average hours worked will be about 42. Because this is a shift rotation you provide at least 2 days off after any 7 working days and 3 days off after seven consecutive night shifts. This allows for recovery time and lets people adjust to their next 8-h shift schedule. The down side to doing this is that an individual will only get a free weekend once every 7 weeks and they will have to work one 7 consecutive days stretch and one 7 consecutive night stretch during that 28 day cycle. The good news is that everyone is only working 8-h shifts and the average overtime would only be about 2-h per employee per week unless you can cut people early off of a shift. Here is how it would look:

	Days 1–7	Days 8–14	Days 15–21	Days 22–28
Team 1	DDDDDDD	OOSSSSS	SSOONNN	NNNNOOO
Team 2	OOSSSSS	SSOONNN	NNNNOOO	DDDDDDD
Team 3	SSOONNN	NNNNOOO	DDDDDDD	OOSSSSS
Team 4	NNNNOOO	DDDDDDD	OOSSSSS	SSOONNN

D, day shift; S, swing shift; N, night shift; O, day off.

Deciding on the best shift rotation or schedule for your SOC can be a tough choice but do not do it alone, it is often a good idea to allow the people in the SOC to have some say in what way they would like to approach it or what schedules they would prefer to work. This way the people in the SOC will have more say in their schedule rather than having a certain shift rotation just thrown at them. It will never be possible to please everyone with any type of shift rotation or schedule but a general consensus should be able to be reached. Some SOCs will have less flexibility when it comes to deciding on the form of rotation and schedule because of the organization they work for and the hours that need to be covered, so it may be necessary to assign people purely on the basis of skill mix and availability to a specific shift.

Dealing with absenteeism

Nobody likes to have to deal with a member of the team that just cannot make it to work. That being said, it is going to happen and you will have to deal with it. The first thing you need to consider is a policy on not coming into work. In a SOC, it is different that working a regular job especially in a SOC that operates 24×7. Typically an individual coming to start a shift in a SOC is going to relieve someone else so they can go home, but if they do not show up and your short-handed what are you going to do. From a policy perspective if a member of the SOC wants to call in sick they should do it at a minimum of 8 h prior to their shift. This gives team leads or management time to find someone who can cover that shift. If the person calling out does so any less than 8 h it should count against them during review time and should affect any raises or promotion opportunities and if continued issues occur they should be terminated. It is just not fair for everyone else when there is a lack of respect by someone who cannot plan far enough in advance as to not negatively impact other people, it does not make a good teammate and will lower moral in the SOC. How should sick calls handled? The shift lead or senior team lead needs to begin calling people who are not schedule to work to see of anyone can cover the shift. Optimum coverage would be the preplaned number of people who were designated to cover the shift but the team lead or shift supervisor may feel that one person will not make a difference and could decide to go without that one person for a day. Typically it would be best to find someone to cover the whole shift but you could also offer over-time to people to work a half shift by asking them to stay late or even ask someone on a later shift to come in early, as this may be a bigger attraction to an individual and it may help you get over a potential busy rush. Another option may be to offer call-back pay and round trip mileage for anyone willing to pick up an extra shift as well to entice people to help cover required shift gaps. This all seems logical when you are paying people hourly but it is also possible to give people additional pay and bonuses when they are salary so get creative, it will work.

There are a ton of sites on the web that can give you different ideas about how to best work your shifts, how to split the shifts and make things as efficient as possible. This brief overview of the different kinds of shifts and patterns that you can use in your SOC should help get you going in the right direction. Knowing where and what time you need the bulk of your SOC to operate is half the battle. Keep a good eye on your staffing levels for each of the different roles and skill sets you need in the SOC. Then make sure you monitor how effective events and incidents are being worked. Based off of those metrics you can add date and time stamps to see when things are falling through the cracks or when you have everything covered, then adjust your staffing levels accordingly.

Intelligence

learning.oreilly.com/library/view/designing-and-building/9780128008997/B9780128008997000094/B9780128008997000094.xhtml

Chapter 9

Abstract

Applying security intelligence into the tools protecting the organization is what is required for a SOC to move from a reactive to proactive. Getting the right type of intelligence and being able to effectively apply it to the SOC ecosystem is a critical component in the overall protection of the organization.

Keywords

intelligence

OSINT

information

automation

IP

domain

blacklists

attributes

lists

Chapter contents

“If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not your enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.”

Sun Tzu

Security intelligence is critical for a SOC to have in place. It is the single greatest tool that is used to help protect an organization’s network. What is security intelligence as it relates to the protection of information technology and why do you need it?

Intelligence information can come from many different sources and is the process of gathering information, evaluating it, correlating and interpreting, and then disseminating it to decision makers or, in the case of the SOC, applying it to rules and tools that make it valuable.

There are arguably more than two types of intelligence, but I want here to break intelligence down into two simple types based on ultimate source.

First, you have reactive information gathered internally by fully evaluating system compromises, forensic examinations, malware analysis, and also by asking key questions and building metrics to explain an increase in successful security incidents or if there is some kind of trend underway. This information is typically more in line with traditional security and is a trailing or lagging indicator of something gone wrong. An absolute critical component to your intelligence program is that once you know something bad about one system, you can then go look for that same bad thing on all your other systems to see if there is more out there. You can “wash, rinse, repeat” this information over and over again and every time you find something new on your network you can go over it again and again.

Next you have proactive threat information or leading indicators. These typically are gained from external sources. This is information that is open source (OSINT), purchased information, or information gained by being a part of an organization that shares threat data. This is information that is gained from other organizations that may have already seen this activity but is advanced knowledge to you because you may not have known about it previously. These proactive methods employ the use of information from partners, suppliers, reputation, and trust databases. The intelligence information can be extracted from web pages, blogs, wikis, IRC chat sessions, search engines, phishing emails, open FTP sites and file sharing networks, P2P networks, newsgroups, online auctions, and many others. It is a move from a more tactical approach to a more strategic focus.

This is an approach that integrates intelligence analysis methods, tools, and processes proactively to address security risk in today's highly threatened environment. This is an equal part practical application of traditional Internet and network monitoring with applied intelligence analysis. Your SOC will need to perform advanced search strategies and pattern recognition techniques to identify, detect, and analyze actual and potential threats to your organization. The use of intelligence is uniquely able to protect an organization or enterprise as well as individuals and their identities. By identifying threats generated by criminals, predators, extremists, activists, insiders, and other blackhats, information can be collected and analyzed and actions can be taken toward the prevention and mitigation of security risks.

By using these two types of intelligence, you can create a new form of warning system or warning intelligence. This is collective information that can alert you to emerging threats and can be inputs to your risk management system. For example, if you know of a piece of malware that is taking advantage of an exploitable bug in software you run on a critical system, but were not able to patch previously, you may be able to do something about it now knowing your risk may be increased. Some of the warning intelligence is a bit of a no brainer. For example, if you are seeing nine out of 10 of the latest malware variants taking advantage of holes in Adobe Flash, then perhaps you should make sure that all Adobe Flash players on your network are up to date to mitigate that threat. Other times it may not be so obvious, but knowing how a specific malware family works may help you dial-in to effective mitigations. A good example is how the Blackhole exploit kit works. I don't want to get into too many technical details here, but it's worth a quick look.

A user who visits a web page hosting the Blackhole exploit kit becomes compromised. How this works is simply that JavaScript quickly determines via a vulnerability scan what applications and versions of those applications, such as Adobe Flash or Acrobat, Microsoft Office, or Internet Explorer are on the user's computers and loads exploits to which it thinks the computer is vulnerable to and tries to exploit those applications. Once the computer is compromised, it will download further malware. Your intelligence research may yield you two things: first is a list of known domains and links that are hosting the exploit kit. If you are able to load up those domains into a SIEM or other log management system or build rules around the domains in other tools, then anyone on your monitored network going to those domains will be spotted and you can react appropriately. Second, you may discover that there is a loose pattern around how the domain names are built or what the links are and you can build a regular expression rule to catch anyone going to a URL matching that pattern. In this case, you may have a high degree of false positives; but, if you correlate that information with antivirus logs, you may be able to detect the exploit activity to some degree of success. Short of having a rock solid intrusion detection rule built and deployed on your network, this is a great example of how multiple pieces of intelligence can be used to build an effective warning system. Getting this information, digesting it, and being able to use it in an innovative way to protect your organization is just another way your SOC will provide continuing value and remain relevant.

The previous example seems fairly straightforward. You can argue the effectiveness or the accuracy and by the time this book is printed, the exploit example may be old news, but the point remains the same. Your effective use of intelligence information will go a long way to protect your organization. In that pursuit, you also always need to keep in mind the quality of the intelligence you receive from outside sources and ensure that the information is accurate and as complete as possible. You also should make sure that the information you are getting is timely and that it's real. Timely may not be that big of a deal if it's ongoing and valid data, but depending on what you are dealing with you need to make sure your information is as accurate as possible. A good example of this is in one SOC where I worked. The thinking at the time was that creating a massive MD5 database of all known good and bad files would help to make things much more secure. You can block the known bad or only let the known good execute or both. There are plenty of tools and hash databases out there to help you with this as well. The National Software Reference Library is a good example of where you can get this type of data (http://www.nsrl.nist.gov/). I am not going to tell you that MD5 hashing is good or bad, but as an example of inaccurate intelligence, this MD5 system will choke you. You see, the SOC was putting so much time and effort into creating MD5 hash databases that a good hash got into the bad hash system. There obviously was a process step missing to validate information and the quality of the intelligence that was being fed into the database. Unfortunately, the bad hash database was preventing any files from executing on participating systems that matched the bad hash list, essentially creating an execution black list. The hash that was incorrectly inserted into the database was a key file needed to run the endpoint antivirus software, which essentially caused a shutdown of antivirus on all the workstations and laptop systems on the network. HaHaHa, very funny, well let your imagination run wild a bit and see how badly this error could have impacted an organization's operation such as a hospital or power plant. Again, I am not saying that MD5 hashing is a bad idea, but this example shows you how bad intelligence fed into the wrong system can have very negative impacts. Make sure you have high quality of data and that you have the right processes and procedures to validate and test that data.

You need to know the quality of the intelligence you are receiving and also need to do some evaluation of that information as you apply it to your tools. Change management in this case becomes a very important function that your SOC needs to engage not only internally but also with the remainder of the IT organization on an ongoing and regular basis.

When one of your SOC analysts or engineers generates intelligence information internally, using your tools, that information should be considered both highly reliable and trusted, especially if they are following internal SOC processes to develop that information. If you get some intelligence from a magazine, newspaper, TV, or some random blog site, then its source and reliability may not be of such high quality. Information Security Intelligence is very fast moving, and can change in seconds. You are not always able to get verification of information from multiple sources, thus you have to trust the original source as much as possible and do the right thing with the information. Good intelligence information can include IP addresses, domain names, strings found inside an executable, and file hashes but these elements can be highly volatile or they may stick around for a while. Whether you generate your own intelligence information, purchase it, or get it for free, keep in mind that the more generic your information, the more false positives you likely will have; but, at the same time, intelligence that is too specific will not be agile enough to spot minor variations in your applied data.

Security intelligence is a constantly growing collection of information from outside sources (know thy enemy) and from within your own organization (know thyself).

Know thyself

Adversaries are constantly changing their tactics, techniques and procedures (TTP). SOCs need information related to these new TTPs to ensure their tools are configured properly to see and/or stop the attacks the adversaries are making or be able to detect malware coming into the environment. By collecting all usable information from every incident, performing forensics, network analysis, malware analysis, and discovering new ways to better detect those events is intelligence you build yourself. They all are part of the "know yourself" side of the equation. But that is only part of the battle, you need to know how your network is configured, how your desktops and servers are hardened and protected, what active directory group policies are applied, and how your networking infrastructure—such as routers and switches—are managed. As stated before, if your organization has a mature IT department, your SOC also need to be a part of change management and have access to asset management tools. SOCs need to know what systems are doing on the network, what is their purpose, who put them there, and who must be contacted if there are questions or issues. This may appear like a lot, but it is basic information that helps the SOC determine if there are issues or if they are just chasing ghosts. It also helps the remainder of the IT organization because the SOC is not typically involved in building infrastructure. Thus, when there is an issue, the SOC will need to call people from IT to get answers instead of being able to help themselves. For example, just knowing that a specific server is a database server such as MySQL may be very helpful to a SOC instead … of guessing it is a web server that an attacker just compromised.

Having access to an asset management system goes a long way for an organization like a SOC in the "know thyself" part of the equation.

There are several places from which an organization can obtain intelligence. The type of information you can use depends on the level of sophistication in your SOC and the tools you have deployed. Information such as honey-pot-captured payloads may be used to create your own IDS or you can even find already-built signatures to try. Sometimes you can find IDS or scan logs of large sensor networks that can indicate trends you may want to search for on your network. Intelligence related to denial of service attacks (DoS) statistics may prove helpful if you can translate the information into something with which you can tune your devices to protect against or detect. Of course, there is also a wealth of information out there regarding general security news and vulnerability reports. These are helpful for noting how your organization is effected or protected and can even help prioritize needed upgrades or remediation issues. Captured malware samples are good to see trends and test your anti-virus tools to ensure you are properly protected. Phishing infrastructure and sample data is good to use to help tune your spam filters and prevent these types of email messages from getting to you users. Also botnet command and control data are fantastic intelligence data that you can use to check if systems on your network are talking to known bad servers.

Let us get into a bit more detail and describe what you can do with this information, how you can benefit, and perhaps even spark some ideas for you. Getting information and finding good sources of information are the first steps. But, be sure you evaluate the information you find and ensure you can build a valuable use case for that information. Being an intelligence hoarder does not sound like a bad idea, but collecting information for the sake of having it will only overwhelm you and your tools. You need to make sure you have the right information to achieve your goals.

The information you collect should all be actionable; then your actionable threat intelligence must be optimized for collection, analysis, and delivery.

When building an intelligence component of your SOC, you must gather, correlate, and aggregate events from across many different threat vectors and then apply them appropriately to the tools you have. Then you need to focus on how to present the information in a way that provides context and relevance. The intelligence information will then provide you situational awareness and actionable data and give you the visibility you need to protect your organization or begin your incident response and notification processes. In order to make this work in your SOC environment, you need to ensure your events are properly correlated and aggregated into incidents that matter to your organization and to organize the threat landscape to provide situational awareness. Then, as discussed in other chapters, your incidents will then be prioritized by relevance and severity for incident response actions and remediation efforts.

Key point: Sometimes intelligence information can come in the form of a single string or thousands of IP addresses. Your SOC should work to automate as much as possible: automate the collecting of the information and the application of the data. Scripts can update different tools or software and in some cases can be created by the SOC team.

The following are examples of current intelligence feeds that your SOC can use in its tools arsenal to help combat such things as advance persistence threat and common botnets, but also the more common financial cybercrime and identity theft.

Known IP space, know thy enemy

A quick search on the Internet can get you lists of IP addresses by country. This information may not appear like very useful cyber intelligence, but blocking as much IP space as possible is always a good way to start protecting your network. The SOC should always be aware of what IP space an organization does not need to allow access. If there are specific countries with which you do not work, then shut out their IPs from connecting to your network. There may be IP addresses from countries or locations you are unsure of and can't block, by identifying these IPs you can put them on watch lists and see what they do. There are also lists of other classifications of IP addresses you may be interested in watching. Known proxy IPs, VPN networks, and transient DHCP networks may also be of interest to you. By classifying these external IP addresses, you can categorize the connection information and begin to build some intelligence from them.

There are also many other types of bad-IP lists that your SOC can use to give you greater fidelity into what may be going on with your network or hosts in your organization. Known spamming IPs … botnet network IPs … there are also many different block lists of IP addresses that have done various bad things for which you may want to be on the alert. These lists can get more and more fine-tuned as you get into it and as you find them. There are also various intelligence exchange networks that you can become join. These exchanges can offer you IP reputational databases that are updated in real time and tell you of bad-acting addresses. This can help you find internal IP addresses that may be communicating with known Command and Control (C&C or C2) servers. These C2 servers may be master consoles of botnet or zombie networks and if you discover internal systems communicating with them, you have some incident response and possible forensic work to do. The exchange also may be able to give you information that will help you spot peer to peer (P2P) botnet activity. P2P activity can be very difficult to spot on your network and any information or intelligence about the different botnets out there can only help.

Various companies and the open source community have installed several honey-pot networks. These honey pots collect information about attacks and probes and then publishes that information for you to consume and use to help protect your network. One such honey pot watches and monitors how data is stolen or exfiltrated from a network. This server network allows an attacker to compromise the server systems and then watches what the attackers do to remove data from the network. The attackers are observed using the normal web protocols of HTTP, FTP, SSH, or they even just email the information to themselves. An attacker will use these methods as well as more covert data transfers like DNS or ICMP. This by no means covers all the ways an attacker can steal data, but the important thing is that this information can be observed and valuable intelligence can be gained from watching the actions of the attackers. This information can then be shared in the cyber defense community and be used by your SOC further to advance the capabilities of the tools deployed in your organization's network to detect this type of activity.

Another such intelligence database focuses on malware. I am not talking about an antivirus database or how antivirus software detects malware but something even more. This database catalogs the network exploit packets, which are the actual packets that are seen on the network that indicate a system has been compromised. These packets are sometimes too sophisticated for intrusion detection and need advanced correlation between DNS requests and web proxy URL requests to be seen properly. Additionally, this database can be used to help spot how the C2 connection appears on the network. Sometimes a system will only send one packet or beacon of information to a peer or central server to register itself to the botnet network. This is like looking for a needle in a haystack. If you employ the information from the malware database properly, however, then you ultimately will be more successful and prepared when that one packet of information gets transferred. You may think this information is fairly static, but if you look at the statistics from any of the major antivirus vendors regarding the number of new malware entered into the wild every day, you easily will realize that this is a large set of information with which to deal. Over the last year or so I have seen this information grow and change to the point where there are 400 new communication strings and hosts a day that a SOC needs to be aware of and track.

Blacklists

A few years back, a new tool in the network defense arsenal started popping up. Blacklists containing information about IP addresses that exhibited poor behavior started growing. Each blacklist created focused on a different thing in an effort to differentiate themselves. These lists ranged from spamming IP addresses to websites hosting malware. Many lists were created to track spammers and some lists have not survived over the years, but there are a few out there that are worth a look.

Most commercial vendors, spam filters, and web proxy companies will use these blacklists as well. It is important for a SOC to be aware of them in case they need to further apply specific lists that their tools may not be utilizing or if there are technical reasons why they want to apply the information in a different way or with different tools.

As with what I mentioned before, the biggest lists contain IP addresses of systems that have been seen sending various types of spam. But others also include information on universal resource identifiers (URI) that are typically seen inside of phishing emails that entice a user to click a link. Email can easily be spoofed so the true sender may never be known and mail servers from which the messages are sent can change rapidly, but the link the attacker wants a user to visit will change less frequently. By adding this type of intelligence to your tool set, you will be adding one more piece of information that will help you see when something bad goes wrong on your organizations network.

As mentioned before, knowing what IP addresses are operating as a proxy can be an important piece of intelligence information. There are free and open public block lists that are dedicated to tracking IP addresses that are being used for this purpose. Some lists track

IP addresses that are purposefully operating as a proxy such as IPs that are on the onion routing (TOR) network, but there are also lists that actively go out and scan systems looking for those that are open proxies where the owner may not know they are being used to proxy network traffic. The use of this information can be invaluable, for example, knowing that an IDS attack is coming from a proxy's IP address helps you validate the malicious intent of the traffic.

Phishing has become one of the most effective vectors for attackers these days. The way the attackers can entice a user to click a link to open an email attachment is nothing short of genius. We as security professionals have to hand it to our advisories, they really do their homework and have studied our users, their habits, and what will get unsuspecting users to click on something. I mean, why play the lottery when there is a general in Nigeria hiding from political prosecution that we can help out for a few million bucks, that is worth it, do not you think? Or how about those loveable cats, who can resist a few pictures of a few cute cats, I know I cannot. What about when our bank emails us to tell us there has been fraud on our account, are not we concerned about that? When I get those emails I click the link right away! But I am not looking to get what they want to give me, instead I want their malware, their domains, their IP addresses and everything and anything I can get from their miserable attempt to compromise our organization's users. There are several phishing databases and working groups that can help you spot when a user is in trouble. But first you have to understand the problem we want to solve. Phishing is a simple-to-understand concept, but at the same time takes a complex technical execution to make it work. Phishing attacks use both social engineering and technical knowhow to achieve the attackers goals. Social-engineering schemes use "spoofed" e-mails to lead users to counterfeit websites designed to trick people into giving out information that they should not, such as company financial data, credit card numbers, account usernames, passwords, and social security numbers. You need to keep in mind that phishing is always a multi-stage attack. What I mean is that it does not stop with an email, it only starts with the email and then further advances via malware and then unfortunately attacker activity on the compromised system.

This is not your regular run of the mill spam. Phishing or even spear phishing (the practice of sending malicious emails to senior executives) takes finesse, skill, and a command of the language of the people that may be targeted. I say language because this is not specifically an American or English problem, instead, depending on who you are and where you are this may be a criminal problem, advanced persistent threat, or a money-making venture for the attackers. So whether or not you are in the United States, United Kingdom, Australia, Germany, Japan, Italy, or somewhere else that has money, you are a target. Years ago it was easy to spot spam or emails that contained viruses because the spelling of the worlds in the email was so horribly wrong that you would just delete it without a second thought. These days' emails are "spoofed" to look like they are from people you know, they are written in the same voice or tone that you would expect and contain information in which you may be interested. In some cases, the email accounts of your friends, coworkers, colleagues, or associates are compromised and used further to send out malicious emails to you as well as others. This is not like the viruses of old either where the virus automatically would send or email itself to the first 50 people in your contact list, but instead the attackers would handcraft these emails to users you may typically email but include malicious attachments of documents in which they may also be interested. This all makes spotting the bad messages much harder for the end users. So knowing all, this how would you stop it, slow it down, or detect when it is going on? That is something for your SOC to work on and is an invaluable service that you can offer the organization that you serve.

Because email addresses can be changed and spoofed, the addresses themselves are not reliable … so blocking will not work. Even if you are sure that bad emails are coming from a specific address, that address is easily changed. Not only are these attributes easily changed, but they can be changed as frequently as each email so that you cannot spot a common pattern of these messages so you would be able to add to a rule to block them. But there is still hope, as we have discussed before, there is intelligence to which you can subscribe that may help open up a wealth of information that will help you spot this activity without using email attributes.

Going back to the example we had before, what if we knew the links that were bad and were being included in the emails that were being sent out? We can protect our users in several ways with this information. First we can block those domains and make sure that if a user goes to that URL or domain that it's blocked. Second, when a user does go to that URL it sets off an alarm that the SOC can respond to and ensure that not only the access was blocked but that no harm came to the computer or the network. Then an investigation can take place to see what emails were sent that got the user to click and some internal intelligence can be gained and used to further strengthen the SOC's tool sets.

Several open source intelligence databases are available to aid in this effort and can be used as real-time sources of information to either block users from accessing or to import into other tools such as your log management system to detect when a user clicks a link. But again, when you use this as a detection method it's a lagging indicator, meaning the event already happened by the time the SOC gets to it so you are in reactive mode. You job is then to only ensure that no harm came to the end user and that there are no other emails or events of significance for which you need to search. As stated before, the phishing is only the first part of the attack; if successful, then you may see password dumping, privilege escalation, and eventually data exfiltration. Ultimately, your SOC has many opportunities to detect and prevent this type of activity and protect the network.

As a side note, this may differ from your experiences but as a rule you may want to use the number five as a magic number. What I mean is that when you are investigating attacks such as this, they rarely ever happen as a single instance. When you spot something, use the Rule of Five, which means that when one thing happens look for at least four more. You may find that with specific malicious emails they operate in campaigns of multiple victims of either a specific group of employees, all the people in one specific department, or several people who are part of a project team but otherwise are not associated inside a company. Once you are able to discover who, if any, are the other people in your organization receiving the same malicious email, then you may be able to draw a conclusion as to how the attacker got those email addresses. This information can then lead you to a completely different compromise of another system or data. Further, this also can help you develop some great indicators or internally generated intelligence information. For example, your SOC may be able to create a rule that when the same five people get the same email, send an alert for an analyst to investigate to see if it is indeed legitimate or another attack.

Certainly to fight this battle there is nothing more powerful, more effective and beneficial in the field of information security then user-based security awareness. Security professionals have fought this battle with users time and time, again but organizations struggle to secure their computers and networks while users fall prey to these phishing tactics. So, while technology and intelligence plays an important role in doing so, end user education is vital to securing your organization and you need to make sure your SOC is educating users at every opportunity it can.

I know that this is a chapter on intelligence, but this seems like a good time to mention user intelligence, meaning how do we make the user smarter. We have to face it at some point, because it’s not a matter of if we will be compromised by a phishing email, but rather when. When we talk about educating our users, we should not just focus on one specific area such as phishing, but rather give them a broad range of topics to think about that can help the organization become more secure. Topics that you may want to include are things like password safety and security, how to store passwords, not sharing passwords, and that tech support will never ask you for your password. Remember that social engineering does not always come in the form of email, but may be a phone call. Users are accustomed to multitasking, so you need to hammer in the concept that they are not to give out their password under any circumstance. Additionally, you obviously want to focus on email safety and giving them the tools to be able to detect current trends in phishing, scams, spam, abuse, and harassment types of email messages. You also may want to educate your users consistently on your organization’s acceptable use policy. This will help users to understand better the dos and don’ts of the organization and how to steer clear of trouble.

You can have too many resources in your SOC, but chances are that you will never have enough. In order to increase your effectiveness as a security organization, not only do you need to use effective intelligence as we are describing here, but also you need to employ your users to be an extension of your SOC and educate them on what to look for and how to properly escalate and report malicious behavior so that you can engage effectively and efficiently to prevent any damage to the organization.

Phishing intelligence is very broad and there are many lists to which you can subscribe that will give you very good information. There are even a few lists out there that are actually master lists that they include information from several lists in one easily formatted location. But, again, you have to think about how you are going to use these lists and what they means to you. In some cases, these lists will include the domain or the IP address where the hosted phishing site is located, but your web proxy vendor may already know that information and will very quickly block access to that site before your users go to that link. Is it enough for you silently to block that nugget of information? If it were my organization's network, I would want to know that a user clicked on a bad link so that I can investigate how and why and if there are any other systemic issues I may need to address or remediate. So, your tools may be configured properly to block the link in a phishing email and your alert system may be configured properly to notify you when a link is clicked, but what you do next is really up to you. In the case of an efficient and mature SOC, I usually will want to run this to the ground, meaning that I will investigate it until I find the original email or website that was sent or viewed and all the users to whom the phishing email was sent. I say this is for mature a SOC only because new security organizations typically will not have time to chase down failed or blocked incidents and should focus on more specific threats that require immediate attention. If possible, I will work to get the offending email, extract all the attributes from the email, and create new rules that in the future may help me detect this same activity or block it from happening again.

With a bit of focus back on open source intelligence, there are a few lists that you can find out there that give you a lot of the information in an easily formatted way that includes multiple data sources combined into a single list. What this means is that there may be several lists out there, but some are masters that deduplicate entries, domains, or subnets to give you a clean and efficient list that you can use for your tools.

Again, you do not want information just for the sake of information. You want to be efficient in the data that you collect and apply to your tools. As you collect more and more intelligence data, you will have to be very mindful not only of the false positive rate but also the sheer volume of information because your tools may not be able to handle the load. Ensuring you are not duplicating information or crating rules that max out your processing power will be a key to your success. As you look at generating lists that include phishing links you want to use, be certain you know what sub-lists they include and how they are gathering the information.

Although phishing may be your number one attack vector, it may not be your number one intelligence source or intelligence-based information to include in your tools. For years, we security practitioners have known some very obvious facts. These are facts that are not able to change in the world of networking or the Internet. There are just some things that will always stay the same and the knowledge of these things can help us apply intelligence to our network defense systems and spot problem areas before they actually become a real problems. Sounds like something will really want to do right? Is it magic or is it reality?

Black listing projects

To further the discussion on open source intelligence, we can review a few more focused projects that collect IP address, domain names, or URLs of known bad actors. Some of these also are lists you may want to generate yourself, as well. What I mean is that if you can see this type of activity on your own organization's network, then you can apply real-time actions in response to the activity and be proactive in your response, but also have it automated.

One such list that you may find out there captures and logs IP addresses that are seen performing brute force attacks. With the correct configuration and collection of logs, this is also a list you may be able to create for yourself. If an IP address somewhere on the Internet is tying administrative SSH logins and you can learn that information before that IP address tries it on your network, then that list may be of value to you. A simple tool that you may use to see if this happens on your devices is Logwatch. This tool reviews all your local logs and generates an email that summarizes activity on the devices. The tool is also able to store that information locally as well, if you want to parse the data further and script it into something that you can use elsewhere, such as block rules for your firewall.

These logs may look something like this:

(As is in common practice the "x" in the IP addresses are to obfuscate the real IPs because this is for example purposes only)

```
SSHD authentication failures:

root (182.62.x.x) 1388 Time(s)

root (80.91.x.x) 965 Time(s)

root (121.8.x.x) 220 Time(s)

root (203.122.x.x) 180 Time(s)
```

If Logwatch is not something you wish to deploy or you would like to have a sampling of IP addresses that are broader than what you are seeing on your network, then you can find SSH blacklists that include this information. You may also find blacklists of IP addresses that are trying administrative windows logins as well. The honeypot network is once such place where you can find this information. An attacking IP gets published on a blacklist, which is updated every few minutes and contains IP addresses of hosts that tried to brute force into any of the honeypots hosts. The honeypot hosts are located all around the world and are setup to report and log those attempts to a central database.

Again, if you are able to automate blocking of these IP addresses on your network, then this may be an extremely valuable exercise to try. In some cases, your organization's SOC may not have permission to implement automated IP blocking or even have access to modify firewalls. In this case, correlating logs from multiple sources may be very important.

If you are have firewall logs and are able to detect these IP addresses making a successful connection to your organizations network and are able to match that attempt up against a device log in your DMZ, then that may be something you want to know if the authentication is successful. A nice metric for later review may be a report showing the number of IP addresses from your list that attempted but failed to login, but also the total number of failed vs. successful (there should be none) login attempts. As mentioned in the metric chapter, this is a really valuable way to show how your SOC is implementing effective monitoring. Once the automation is in place, there should be no real effort to alert on successes and report on success and failure attempts on a regular basis.

By way of comparison to similar things that you may implement, typical installations of this type of list could see up to 7000 new IP addresses per hour become added. Because the number of IP addresses is so high, you may want to implement an expiration period where the IP address would automatically fall off of your list. I do not believe there is any hard and fast rule as to what is typical for how long you would want to keep using this data. Then, again, you will need to determine what the odds are that an IP address once seen performing a brute force attack of an administrative account across the Internet would no longer be a threat.

Other types of lists

If you believed that an IP address had done something bad in the past, maybe even the most recent past such as just a few seconds ago, would not you want to know about it? This is where intelligence can play a key role in your overall security strategy. If you could have a lists of IP addresses that are likely to perform malicious behavior or have recently even been detected attempting SQL-injections attacks, DOS attacks, or any other confirmed type of behavior on someone else's network, what would you do with that information? I know that if I have that information, I can monitor it, respond to it, and most importantly prevent it from causing a problem on my system. The information is out there and available and open to the public, all you have to do is search for it.

Those are just a few examples, and I bet you would love for me to call out a few specific examples and give you a few types of places that you can get a lot of this intelligence information from. I do not like to endorse a product, website, or tool, but also want to be as helpful and complete as possible. Because these sites are providing free open source intelligence information, mentioning them here is a simple way of saying "Thank You." Again, as mentioned many times before, please evaluate this information for you own use. You may find it a great starting point, invaluable data, or not for you. Any or all of the possibilities are fine because this includes free publicly available websites that regularly publish trends and emerging threat information. Organizations freely publish information for several reasons: For one, vendors publish security relevant information from their own products to help protect their customers, but also to help market the power of their products. This information includes announcements of security relevant patches or bugs and how to resolve those issues. Additionally, there are several organizations that like to publish limited general security intelligence to show off how their products work. Even though these are just small samples of intelligence, they can be incredible resources. There are many sites available with free IT security intelligence and here are a few examples to get you started:

- Atlas.arbor.com: Arbor has a product suite that actively monitors a customer's network and can identify many different types of security related traffic. The Atlas site is a public resource that provides intelligence derived from its own sensor network, as well as opt-in customer networks that provide data on host/port scanning activity, zero-day exploits and worm propagation, security events, vulnerability disclosures, and dynamic botnet and phishing infrastructures.
- Senderbase.org: SenderBase is a website with data from Cisco's IronPorts network that collects information on email traffic and gives a view into email-based security threats. Organizations can use this site to research reputation scores on specific domains or IP addresses or even use the top 100 spammers report to block or report on spam email for their own organization.
- securityfocus.com: A community driven website that contains information on vulnerabilities, exploits, and emerging threats. It is also the home for BugTraq, where typically all new vulnerabilities are announced and discussed. There are also several mailing lists that you can join that contain a wide array of security topics to keep your SOC up to date on security issues.
- ThreatExpert.com: This site gives you the ability to post suspicious files and have them analyzed to obtain a report if the files are a computer viruses, worm, trojan, adware, spyware, and other security-related risks in a fully automated way. The site also provides interesting reports on other samples and is a good resource when looking for intelligence to add to your systems.
- Spamhaus.org: Spamhaus is a non-profit organization that has been around for many years and includes several spam lists and blacklists. I highly recommend you visit this site and review the many lists it has to determine how you may benefit from its information. Specifically, its XBL list contains good information on known IP addresses performing exploits in real-time.

Organizations and industry partners

Paid-for and purchased intelligence services can be a bit more focused and tailored to your organization and even provide you relevant information regarding security issues and attacks across your industry. More specifically, these types of services can help you monitor your name and brand on the Internet. If your organization is worried about unauthorized use of your brand in domain names or phishing emails, paid-for intelligence services can help by monitoring for this type of activity and alerting you to any issues. They also can watch for unauthorized disclosures of corporate information in blogs, message boards, social networking, and other online areas and alert you before any damage can occur. Additionally, some of the paid-for intelligence services, like the open source services, can provide advanced information regarding IP addresses of known bad servers, websites, or where malware is being stored on the Internet so that you can configure your tools to keep users away from those places.

Other paid-for services may give you much more details that just IP addresses. Depending on the intelligence you are looking for, these services can provide you in-depth analysis on attacker groups and help you understand who these people are that are attacking your networks and what they seek. By understanding a bit about these groups, you can further asses the risk you have, ensure your security systems are deployed in the right place to protect against the areas they want to attack, and, if their habits change, your paid-for intelligence service may be able to provide you with that information as well.

These services also work very hard to provide real value in the intelligence they are selling. Some companies perform reverse engineering on malware and gain very detailed understandings of what the malware is designed to do, how it's doing it, and in some cases who programed it. This detailed intelligence information is key to finding and remediating threats such as the advanced persistent threat (APT). APT is the name typically given to very skillful, well-funded, and sometimes nation-state supported attackers. The groups that make up APT understand technology very well, they understand their target very well, and they also understand how to circumvent security controls and avoid detection. This is largely due to the fact that APT uses all the same tools your organization uses, except instead of using all those security tools to protect their network, they use them to test out all their attack tools and ensure they can sneak in to your network undetected. Furthermore, they know how to beat most all antivirus tools. Because of this, it is very important that when you find any evidence of APT activity or APT malware that you analyze it as fully as possible. These paid-for intelligence services can do that for you, but can also share information with you regarding other types of APT attacks and malware they have seen. They can provide you information that not only contains MD5 hashes of files, but what windows registry keys typically get changed or added. They may be able to tell you what to look for in running memory of a system that is exhibiting odd behavior. Other valuable information they may be able to provide include services, ports that may be running on a compromised systems, or even what special strings in packets a system may be sending to remote C2 servers. So, for example, an intelligence service may be able to give you all the relevant components of a post-attack analysis and attribution information. This could be explained through a series of indications that match up to a certain group.

So, if a particular registry key is changed while at the same time a new service is running on a precise port number and is sending a string of "A(j@@7" to what would seem like random IP addresses or domains on the Internet, then this is known as an "xyz attack" and is attributable to “xyz gang.” Make sure that if you subscribe to any of these services, your SOC has the right tools in place to use the information and find the bad guys on your organization’s infrastructure.

Industry organizations are arguably one of the best places for security intelligence. It has been shown repeatedly that security attacks across an industry usually have the same or very similar characteristics. By sharing security information with partners and competitors, you can see very quickly who or what is targeting your industry and use that information to see if you have also been targeted and use that information to configure your tools to prevent those attacks from being successful. An organization such as an Information Sharing and Analysis Centers (ISAC) is a great place to participate and share. A review of the National Council of ISAC[1] will help you learn if there is an organization out there for you and should help to put you in touch with the right people to begin. Constant participation by industry organizations allows for the gathering of reliable and timely security intelligence information from industry partners, but also other organizations that may have been invited to join the community such as commercial security firms, government agencies, law enforcement, and other trusted resources. Typically in these types of organizations, information is not just one way; they operate quickly to disseminate threat alerts and other critical information to you as a member. The information often not only includes IP addresses and malware analysis, but can also include recommended solutions and protections from leading security experts in your industry. These organizations are built on trust and are very careful to not expose individual organizations information publicly or attribute information to a single entity in any way. The generic sharing of information is based on trust. Normally, industry members of these information-sharing organizations will sign non-disclosure agreements (NDA) with each other. The NDAs help to enforce rules, such as all sharing by default is non-attribution and cannot be shared outside of the sharing organization without permission from the original data owner. These organizations also will have standardized and reliable procedures for submitting and distributing information and will even regularly exercise critical notification processes to ensure everything is working.

If there are no industry groups that appear to match up with your business, you can also look at participating with a local chapter of ISACA. These are local groups usually sponsored by or run by the local or regional branch of the FBI. Depending on your area, you will see different levels of value in this group, but it can never hurt to partner with a law enforcement agency that thrives on the collection and analysis of intelligence data.

Proactive activity monitoring

Security intelligence information is a critical ingredient to the SOC and invaluable in the efforts to protect your organization’s network. The SOC needs to work hard to know what is “normal,” whether network traffic is normal or not, and what the “normal” processes and files are on an end-user computer. A network, its configuration, traffic patterns, and the hosts that reside on it need to be as quiet and stable as possible. Similar to how ballistic gel works, when something goes wrong, the SOC needs to be able to see clearly into what happened and determine all the attributes necessary to make an assessment on its threat and risk to the organization. Although user monitoring does not appear like intelligence, information it can be the most effective key to alerting your SOC that something just went horribly wrong. Similar to the lists of IP addresses discussed previously, a list of system administrators or privileged accounts on your organization's network is critical. If you are able to use that information against administrative functions being performed on the network, you will be able quickly to see problems. For example, when a user with administrative permissions logs into a system that houses users account information, that occurrence can be matched up with your administrative user account list to ensure that user is on the administrative-permissions list. If they are not on the list, then either an attacker got onto a system and was able to elevate the user permissions or someone else gave an employee administrative permissions when they should not have. Of course, if it is a legitimate employee then it is less of an issue, but can still be a violation of security procedures or policy and in any case would be important to detect.

I bring these examples up now because all along we have been discussing the type of intelligence you can get from outside sources that are in the form of distinct data elements that you can use to find indications of malicious activity. But that does not always need to be the case. In many instances, intelligence can be in the form of logical rules that help detect behavior indicative of malicious behavior. Building intelligent rules may be your best defense; nobody is going to give you a list of 900,000 IP addresses that just participated in the last distributed denial of service attack (DDOS). Instead, an intelligence rule that can detect what a DDOS looks like on the firewall allows you to spot trouble the second it happens and respond to appropriately. In the SOC world, or security world, for that matter, real-time detection and appropriate response are activities we live by. It is impossible to think that the SOC can stop all attacks or even stop all successful attacks. Sometimes the best we can hope for is to see a successful attack and be able to respond to it quickly and avoid any residual negative effect of the attack such as data loss.

If you are at the phase of maturity in building your SOC where you are active in these intelligence organizations and are leveraging the information you are receiving, you should have a realization that you will never build a big enough SOC to combat the enemy. By participating in consistent collection of reliable intelligence from a range of free and paid subscriptions; and government, industry, and internal sources will allow you effectively to create a force multiplier for your organization. It will give you a more complete picture of what your advisories are doing, what their motivations may be and you will be able to categorize their activities. Focusing on these areas will allow you to fuse the information together in order to develop actionable intelligence from all these sources and then feed it back into your tools. This will keep you focused, fresh, and make you as proactive as you can be and allow you to be more precise in your defense in depth strategies against any evolving threats. Lastly, you will see your overall security improve at a more cost-effective rate.

Metrics

learning.oreilly.com/library/view/designing-and-building/9780128008997/B9780128008997000082/B9780128008997000082.xhtml

Chapter 8

Abstract

Data are there to become information and information can be turned into metrics. Metrics need to be generated so that analysis can take place. The analysis of metrics is what you need to take appropriate action. Informed actions are what you need to make proper changes to better help your SOC become more efficient and to better protect your organization.

Keywords

metrics

analysis

information

knowledge

data

statistics

charts

graphs

fields

values

Chapter contents

To know that we know what we know, and to know that we do not know what we do not know, that is true knowledge.

Copernicus

Information is the key to success in anything that you do and knowing that you are on the right track and you are being successful is a great feeling. Without metrics we are just guessing that we are doing the right thing. We need numbers in our jobs to track what we are doing, to show we are being successful, or that we are failing for some defined reason that can be shown through metrics. In security and especially in security operations, we collect a lot of data, a huge amount of data and for some people too much data. But, data are an invaluable raw material that must be harvested. Once you have data, you can turn it into information. The information tells you something, it has structure and tells you a story, and allows you to organize into meaningful metrics. You need to analyze metrics, it causes you to think and evaluate. In order to understand what the metrics tell you, you need to question it. The analysis of those metrics gives you what you need so that you can act. Metrics are a product of that process where you take data, turn it into information, and analyze that information in order to take action.

Data > Information > Metrics > Analysis > Action

Metrics for the sake of metrics does nobody any good. I have spent a great deal of time creating metrics out of ticketing systems, security devices, end point devices and a combination of devices, you name it. I have created some of the most visually appealing, interactive charts, images, and dashboards that you have ever seen and that nobody will absolutely ever use because the data are completely worthless to anyone. You can get lost in metrics for years and make some of the most complicated and complex data sets that even you will not be able to figure out what you did a week later. Once I sat down to make some metrics and focused on nothing else for a week to generate some useful data. At the end of the week I had just over 100 different data sets and metrics. All individual reports, charts, graphs, and spreadsheets that were easy to update and were all interlinked to each other. I presented my weeks' worth of hard work to my leadership team and I got looks like I had three heads. They all had the same question, what do you want us to do with all this?

I realized one critical value that I was missing from all my cool wizardry, the user! I did not think about the practical application of any of the metrics I had created. Instead I just created some very powerful and visually appealing junk. This does not mean that the data were bad but once I put the reports into context of who could use it and why then the reports took on a life of their own and became one of the most powerful tools an operation center could ever utilize.

In the next few sections I am going to discuss metrics as it relates to various people and positions. The idea is not to give you a prescriptive metrics list of who needs what, but instead to help you put valuable data sets in focus of the user who needs it most. It is very important that you have accurate representation of metrics in a SOC. You may not have all of these positions in your SOC or you may call them something different or may even combine some of these into one, it does not matter how you break it up or combine them. Take the concepts and apply it appropriately to your situation as you desire.

What are the types of metrics to use and how you use them are almost as important as the information they represent. Simple visualizations may include a table showing the metric result for the organization whereas graphical visualizations where the metric result is plotted on the graph. Additionally you can use complex visualizations for displaying the metric result for cross-sections by organization or ticket type, incident classification, or incident priority. Additionally your metrics may indicate threats to high valued assets (targets) in your organization. This could include assets that contain valuable data but are vulnerable due to missing patches or updates. Later in the chapter we will talk about using metrics to prioritize assets in order to gain a clear vision of how critical an incident is to your organization, which will ultimately help you communicate the criticality of an event to your senior leadership or it may help you highlight the fact that there are a large number of assets that are largely un-managed or owned in your organization which could quickly become targets for attackers.

Heads up display

If you have ever seen an operation center, the first thing you may notice are the large monitors, projectors, or video walls of what seems like really cool graphics, moving charts, TV channels, and so on. It is the one major impressive thing that an operation center has for eye candy. All too often I have been in an operation center and have seen tons of money spent on these large walls of impressive multimedia but when the work begins nobody really uses it. Nobody looks up at them and the screens just blink away silently. Seems like such a waste of money and energy powering all that eye candy.

It is such a shame when that happens because these massive video walls can be an operation centers must valuable asset. Take a good look at what you display on your wall, if something is not useful in keeping analysts informed or updated about important events then get rid of it. These large video walls are large for a reason, they are needed to help convey important information and there is what seems like never enough real estate to display it all. If you do not believe this is true, turn all your monitors off for a day, does your operation still run? Did things still go as they should? If so, you may need to rethink what you are displaying and evaluate the metrics that you cannot live without.

Supervisor metrics

Let us take a look the purpose of your supervisor or shift lead you may have at your SOC. They may be there to ensure people show up on time, take escalations from more junior analysts or help to resolve unforeseen problems, customer issues, or begin the incident response and communication process. Additionally supervisors may be ultimately responsible to ensure that organizational service level agreements are consistently met. Metrics for this position is your first line of defense to combat any issues and to keep everyone focused. It is important to give them real-time metrics so that they can make on the spot course corrections as needed.

If you have priority ticket types or priority customers how do you know that those tickets are actually being worked in a priority manor or are given the special attention they deserve. One key metric would be a simple visual or heads up display that would alert the supervisor to the presence of a ticket or issues that meets those criteria. Your ticketing system may be able to do this for you or maybe you can develop a way to make this a visual or noticeable item that would attract some attention on a video wall or projector screen. Once a supervisor sees that something like this exists they can then evaluate what work is being performed currently in the SOC and assign the priority event to the next best analyst to work on or even handle it themselves.

A supervisor needs to be aware of all the work that is going on during a shift, knowing who is working on what and for how long is critical to keeping things moving. Sometimes analysts can get hung up on a specific problem or issue and dive into it for extensive periods of time. When dealing with technical issues it is hard to ask for help, technical people typically want to be the problem solver, there is an ego and pride to it all. At the same time, there is a business to run or company to protect and other issues to solve. A supervisor needs to know what analysts are working on and how long they have been working it. In a small operation, this is easy because you can verbally check-in with people on a regular basis, there is conversation going on and everyone may be in-tune. In larger organizations, a more technical approach is needed and a metric should be developed to track this.

Time-based service level agreements or objectives are also a metric that is vitally important to a supervisor. Knowing how many tickets are in a queue that are untouched or unresolved or how far an operation is getting behind on issues will allow supervisors to evaluate the work and see where they can apply additional resources or maybe even the supervisor can jump in to help out the queue for a bit to elevate a backlog. Sometimes analysts working tickets will not always take tickets in priority order, instead they may be more selective and only take tickets for issues they feel more confident in handling sometimes called “Cherry Picking”.

This is not necessarily a problem but a supervisor needs to be able spot when this becomes an issue because select tickets may be in the queue for too long, they can then direct people to take specific tickets to keep things moving. A simple metric showing analysts the top 10 oldest tickets in the queue may help motivate them to resolve those issues first, or they may just get sick of seeing them and want to close them out the best they can. No matter how you make these metrics work they are a key component to allowing your supervisors to make course corrections to help the entire operation stay on track and meet obligations. Supervisors also need to know how the people on their shift are doing, what their skill levels are and be able to rate the quality of work people are doing. This is because we want to provide the best possible service to our organization and the supervisor needs to know where problem areas are.

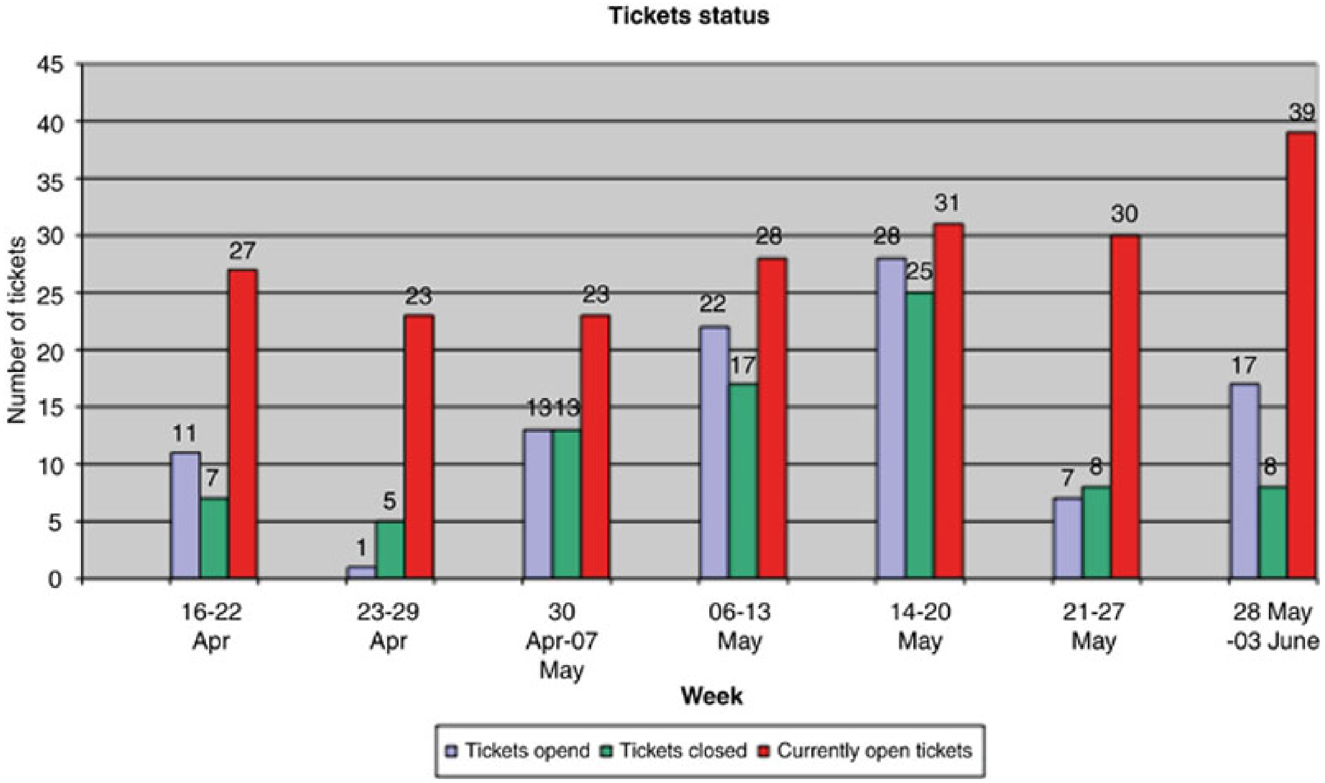
To evaluate analysts, one type of metric that can be useful is a ticket type metric. This is where you look at the types of tickets being worked by each of the analysts on shift. For example, if you notice that a specific analyst is working mostly IDS generated tickets but not working any virus issues then there may be a problem here. This may indicate that the analyst does not feel strongly enough in the skills that it takes to properly analyze and investigate those types of tickets. A supervisor needs to evaluate his staff to ensure everyone has the right training to be able to appropriately respond to potential incidents. A metric like this could be a good indication of a problem where someone needs additional focus, training, or mentorship.

Time based metrics can also be very valuable for a supervisor but are also very hard to create. Your ticketing systems need to have a time tracking function build in and then you can begin to track all kinds of interesting things. For example, imagine a report that tells you the average time a new ticket has to wait before being taken out of the queue and worked on by an analyst.

So for your supervisors as well as the managers it would be important to know the number of tickets per analyst that has been opened as well as closed. This will help you understand the number of tickets that your operation is actually dealing with on a regular basis. By looking at the same information by day as well as by week and month will also help you in understanding what your maximum load may be as well. You should also look at the number of individual closed versus open instead of a total SOC average. I would not use this metric to see how Bob is doing compared with Charlie but instead see who is doing what and like what was discussed previously who may need training.

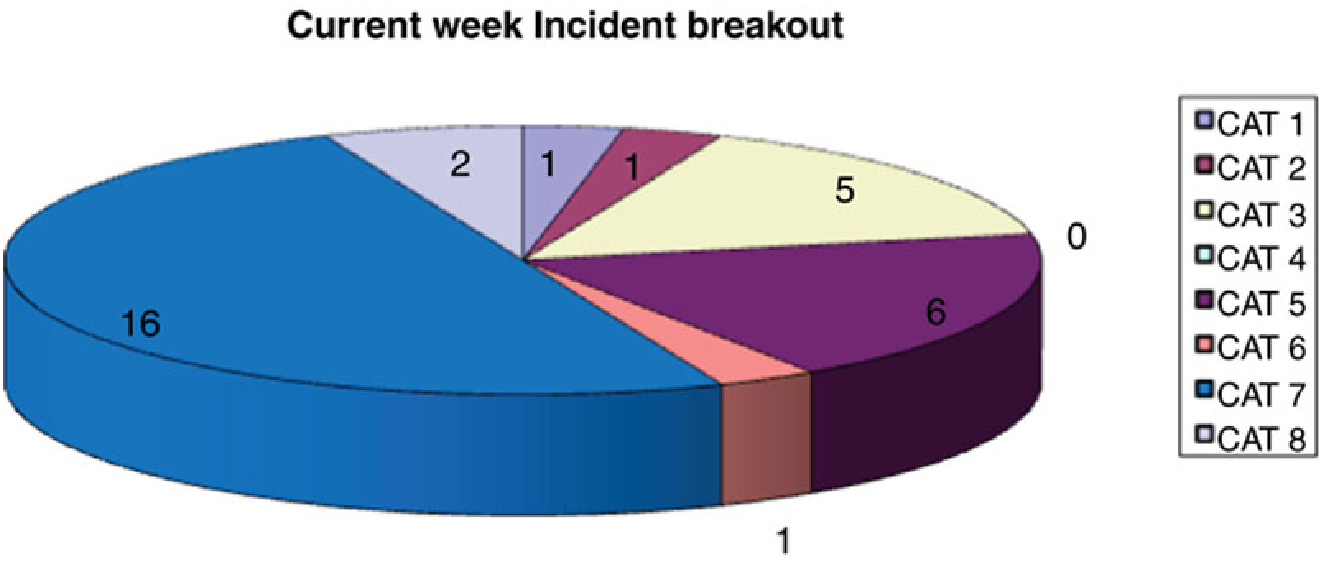
Average time from ticket creation to ticket closure is a another nice ticket based metric, depending on how detailed you can get you will be able to find out not only how long it takes each ticket or ticket type to be worked to completion but you will also be able to spot problem areas that can be addressed to help you close tickets faster. You may even find that you need to work on your communication skills or relationships outside the SOC as the longest time to resolve tickets may be getting action or information from other departments.

Average time worked on the ticket is always good to try and figure out. Unfortunately time is not always an exact value to measure. Depending on how you implement the time tracking your results will vary. If you ask analysts to enter time values for each work log entry into the ticketing system, you may find that they are not very accurate as sometimes when people get heavily involved in technical issues, time escapes them and 3 h may seem like 30 min. When a ticketing system tracks time the system can only do so much. If an analyst opens a work log entry and the system starts to track time based on the fact the log is open you might think that is a nice automation until the analyst goes to lunch and forgets the clock is ticking in the ticket. Another issue regarding this is when an analyst does the majority of the work outside the ticketing system and then just copy and pastes their work into the ticket. Then 45 min of work could look like 4 or 5 s of logged work. Sometimes to most basic of time based measurements are the best like total average time/days open or a weekly metric to show how many tickets are open, closed, or currently open but neither closed or opened that week.

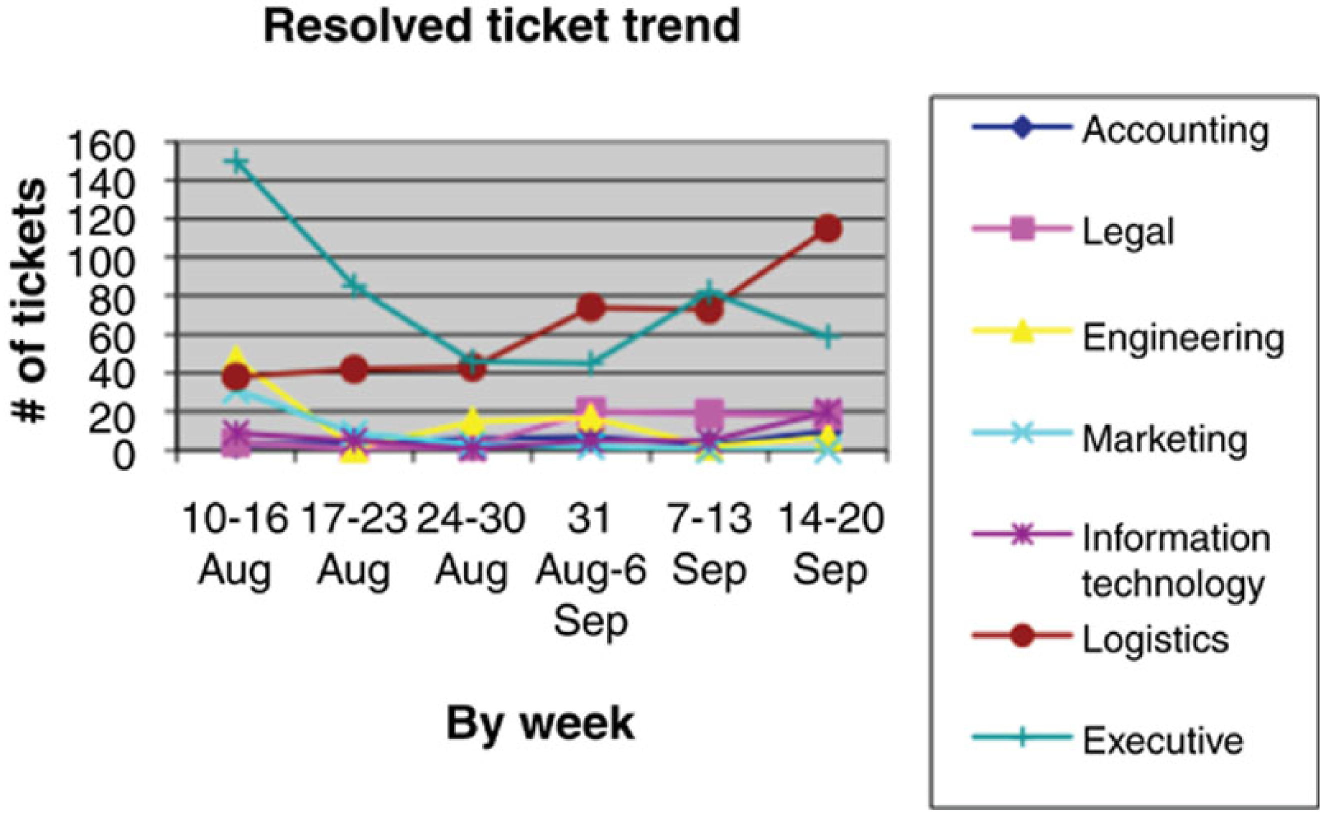


Ticket type is another interesting ticket based metric that can be interesting and fun to look at. I typically design my tickets systems to have tickets be categorized based on the US-CERT incident categories as we detailed in Chapter 3.

Once you have all your ticket categorized properly you can start to track what tickets are being opened for and really get a sense of what your SOC is doing.



Number of tickets by division, location, or industry is also helpful so that you can easily identify where problem areas may be.



For the supervisor here is an idea, how about one of the simplest yet effective metrics you could ever display on a video wall. A single value that shows the number of tickets in a queue. Simple, right? But effective! People want to get the queue cleaned and if supervisors push the priority to get it cleaned out then people will always glance at this number to see how they are doing or where they are or how they are doing.

Got a problem with missing SLAs on tickets? How about a simple metric that shows how many ticket SLAs have been missed. Of course these are all metrics about tickets but there are plenty of other metrics that are important like if your network is up, are your devices up, web sites alive, and so on.

In one SOC, we had a 15-min service level agreement to acknowledge all new tickets. Using the time based functions of the ticketing system we were able to project on our video screen ticket numbers that were in jeopardy of missing the SLA because nobody has touched them. This quickly became known as the jeopardy queue and when things were busy, this is where everyone would go to get their next ticket to work on. You can even take the approach of changing the visualization of a ticket based on time. For example, if your ticketing system displays tickets with a ticket number and short description and date/time created then you should be able to display the oldest ticket first at the top of the list. To go a step further, taking the 15-min example, if all your tickets are displayed in black text maybe you can get your ticketing system to display all new tickets 5 min old as red text to visually separate them from the rest of the tickets, then you may even be able to get tickets 10 min old to not only be red but blink. These are good examples of how to get your SOC to take notice of priority work through visual metrics.

Time based metrics can also help you maximize your staffing efforts and make you more efficient. By looking at how many tickets are in the queue when you most frequently miss your SLAs for new tickets can help you determine the backlog levels. After you obtain your backlog levels, you can then map that against the time of day and the number of analysts you have on shift. Depending on the frequency of missed SLAs and the volume of tickets you may discover that you have too many people on one shift and not enough on another and therefore need to make some shift staffing changes. Depending on your SOC and the volume this metric may just tell you that you are getting overwhelmed. Your next step would be to look at the ticket types and how long it takes each of them to get resolved. If you find that there are always the same ticket types that take the longest maybe you can look into the processes and procedure the analysts are performing to see if there are any efficiencies that can be gained to improve the time it takes to resolve the tickets. In some cases, this time to close metric can mean two different things. First you can look at the overall time it takes from when a ticket is open to when it is completely closed. The other way to look at it is how much time was actually spent working on the issue the ticket was opened for. In other words, a ticket may be open for 5 days but only 10 min of actual work was performed to close it out. The two metrics mean very different things and actions you would take to reduce the time of each are very different. Continuing to make efficiency changes in your processes or apply automation will help you resolve tickets faster but it will also help your increase your ticket to analyst ratio. You need to maximize the number of quality tickets your SOC analysts work on and resolve, that is a lot to say in one simple sentence. What is a quality ticket how do you find out the analyst to ticket ration and how do you know when you are maximized. All good questions can be answered by looking at very simple metrics.

The total number of resolved tickets divided by the total number of analysts obviously would show you the average number of tickets an individual analyst resolves. For many reason this is not a fair average. For example, one analyst may be very fast at investigating and resolving tickets where another is slower but maybe more methodical. Another reason this metric can get thrown off is if there are a few particularly hard tickets to resolve that take long amounts of time and work. In order to help offset these issues are to look at types of tickets resolved divided by the total number of analysts. This way you can dissect the information in a bit more granular way and address specific issues with ticket types. You may find that virus events take longer to resolve but there are more virus tickets the second week of the month compared with any other week, whereas IDS generated tickets occur more frequently on Wednesdays but are relatively quick to resolve. Further investigation of these occurrence may help you realize that Wednesdays are the day the IT department typically patches systems which set off the IDS systems and generate a ton of false positive events. Similarly you may find that the second week of the month is more frequent for antivirus events because that is when patches are typically announced and when zero-day exploits are attempted more frequently.

If your SOC is receiving 5000 or whatever number of tickets per week or per month, take a regular look at those tickets. See what they are and how the staff is handling them, are they resolved, are they remaining open for long periods of time, ask some hard questions about the tickets and the associated events. This may sound silly but ask why the tickets are open in the first place.

Let us say that IDS devices generate a majority of your tickets. Which is not uncommon, many companies like to constantly keep their IDS devices up to date with the latest and greatest signatures treating them like some kind of antivirus update. So they just add signatures as they come from the vendor and take little regard for what the impact or need is to the organization. Take a good look at the top three events that open tickets. There are a lot of questions that need to be asked about these three events. One easy question could be regarding the percentages of false positives each of the three events are generating. If your staff is spending an average of 5 min per event investigating and working an IDS ticket and there are a total of 600 of these three events combined per week then you are spending 50 h of your staff’s time on these, is that worth it?

Efficiencies can be gained by performing regular reviews of work being performed and ask the basic questions such as do we need to be doing this? Is there a better way?

Depending on how your SOC is setup, you may want to set a threshold of a false positive rate on IDS signatures if you can quickly determine that more than 90% of a single signature generating tickets is false positive then take it out of rotation and let someone evaluate it. Can you make the signature better and less false positive? Is it something that the organization can live without? Maybe the signature does not need to be on all devices and only on some that it matters more to. After asking the right questions and reviewing the information take these signatures out of production if you can, let your engineer fine tune them to reduce the false positives or even evaluate whether or not the IDS event is even worthwhile to the organization it is protecting.

Imagine the engineer who on a Friday evening and has been working on a new IDS signature all day. In his rush to get out the door, he installs the signature on 30 production devices and leaves for the weekend. The signature is not too bad but maybe not fully tested and it starts to fire once every other hour, so each hour 15 tickets are generated from the 30 devices. In a small SOC with only one or 2 weekend analysts, this may be obvious but in a larger organization with 10+ analysts it may not be noticed because everyone is grabbing tickets and doing their work. At the end of the weekend, 24 h later using the same 5 min per ticket average you would have wasted 30 h of your analysts time working a bad signature.
15 × 24 = 360 tickets at 5 min each

There are many built in tools from the vendor to help with this problem but it is not always possible to get it right. A good solid process to evaluate, test and install new things that trigger tickets for analysts to work on will pay huge dividends in the long run. One way that I like to measure my engineering staff is by false positive rate. Since the engineering staff can have a dramatic positive or negative effect on SOC analysts performance I will typically make a line item in every engineer's yearly review regarding false positive rates. Installing a bad IDS signature can open thousands of tickets in an automated system and waste a huge amount of time cleaning up unless you have an automated way to do the clean up. There should be a fair amount of testing before putting anything new into the SOC for analysts to react to. A simple metric to use would be percentage of overall tickets closed by the SOC analysts as false positive. This also has another advantage, in several organizations I have been at there is a divide between the annalists and the engineers, this metric gives the SOC back some power and creates a feedback look to measure how well the engineers are doing their job. Do not wait until the end of the year to pull this metric, evaluate every week and see where the problems are, make quick course corrections, and that ensure your annalists are able to focus on the tickets that matter the most.

Getting into more specific security metrics you may want to calculate the number of detected security events the SOC has experienced during a specific time period such as a shift, a day, a week, a quarter, and so on. This metric can further be split by business division or customer type or even by region. You can also define the metric by event type such as policy violation opposed to attempted exploit. In combination with other metrics, this can indicate the level of threats, the effectiveness of a specific security controls, or your incident detection capabilities. Additionally this could also help you see if changes to the environment are positively or negatively affecting your security posture. It will help you to strike the right balance, to find what is too many incidents and what is not enough, this is a good way to see some of that.

Vulnerabilities

Vulnerability management is a vital part of keeping an organization's assets safe; identifying and mitigating weaknesses found on systems especially priority or critical systems and applications reduces the risk of negatively impacting the business should these vulnerabilities be exploited. It is worth mentioning that it is impossible to predict or anticipate what vulnerability is going to be exploited. Because of this it is imperative that IT organizations and individual system, administrators work hard to get as close to 100% vulnerability free as possible. The SOC plays a key role in this area on several levels and can become a great partner in this effort. The primary question this activity is concerned with is: "Are my systems safe?" In vulnerability management terms, this question can be decomposed to: "Are there vulnerable systems? Have systems been checked, and if so, what was found?" and additionally how soon after a vulnerability was found did it get fixed. Finally, the last question is how well are system administrators managing and maintaining systems in the environment? Vulnerability assessment is the process of scanning networked devices and discovering vulnerabilities before hackers can exploit them, which is a perfect task for a SOC. Whereas vulnerability management is the process of evaluating vulnerabilities, communicating required patches, escalating missing patches and vulnerabilities to the right teams as well as approving exceptions and then overall reporting of open vulnerabilities in the environment.

An organizations network relies on accurate and timely exchange of information. Due to the increase of threats and well-known vulnerabilities, an organization must have a vulnerability Management system or process that provides the latest vulnerability fixes and security updates to the organizational network. The SOC can provide analysis on the latest vulnerability information, fixes, and security updates to all divisions responsible for maintaining network and computing assets. The purpose of the SOC engaging in this effort is to monitor and identify new threats and new vulnerabilities (hardware and software) that might affect the confidentiality, integrity or availability of the organizational IT assets. Also, these SOC services should be designed to aid system administrators in identifying existing and known vulnerabilities as they emerge and to look for the successful application of security updates and configuration as recommended by the vendor. Additionally the SOC should be the point of contact to support IT system administrators in the correct application or support of applying patches.

The SOC can also be a focal point for collecting and approving exceptions to patching and vulnerabilities. If a vulnerable system cannot be patched due to operational constraints, the patch breaks core functionality or a system administrator is just too scared to apply a patch, the SOC can help. I say this last sentence partially joking, sometimes system administrators maintain legacy systems that are so old and have been so problematic that they are afraid to touch it because something always goes wrong. The bottom line is that you are only as strong as your weakest link and the process of approving exceptions in a vulnerability management process is one that should not be taken lightly. System/network administrators in cooperation with the SOC should put a mitigation plan in place of each vulnerability that cannot be properly patched in a production environment. Mitigation plans could consist of IDS block rules for the specific attempted exploit for the vulnerability, Removal of the system from a production VLAN, significantly limiting or blocking of the effected ports on the firewall to the vulnerable system or even removing the system from the network till a fix, security update or some kind of mitigation can be applied. I am sure there are many other mitigations you can apply and your organization may even have some unique mitigations. As always it is up to your organizations practice on how you want to apply mitigations as part of the exception process but it should be a joint process between the SOC, your system administration team and your risk or compliance departments if you have them.

Typically the SOC team is responsible for keeping up to date with the latest threats and vulnerabilities and recommending mitigating strategies, solutions or fixes to System Administrators to be pushed to systems connected to the organizations network. The SOC can receive notifications/security alerts of new vulnerabilities and exploits related to security bugs or issues that may affect the network from places such as, US-CERT; full-disclosure; and Bugtraq. Any vendor's technology that you have widely deployed in your environment will likely have a mailing list, twitter account or some kind of news announcement related to vulnerabilities that your SOC can subscribe to and upon receiving an alert of a new vulnerability, the SOC perform vulnerability management processes to determine the vulnerability criticality as it relates to your organization. For example, if your SOC receives a notification that there is a critical vulnerability effecting Firefox on Linux but your organization does not use Linux then the SOC can downgrade the alert from its original critical to something that does not affect the organization and therefore would ignore. Conversely if that same alert effected Firefox in Windows and your organization heavily uses Firefox then the SOC could make the vulnerability widely known throughout the organization that it needs to be patched. There is also a large amount of data that can be obtained from intelligence sources and industry organizations sharing intelligence information but more of that is covered separately in chapter 9.
As part of the vulnerability assessment process I like as a best practice to ensure that every IP address in an organization is tested for vulnerabilities every 30 days. If you want to go back and read the last sentence that is ok because I did say "Every IP!". I typically do not believe in scanning known assets because a network can be a living-breathing thing and as the network gets larger the movement and changes of the network happen faster so you are more likely to miss assets. By scanning IP address ranges you are scanning all possible locations for a device to exist regardless of where it is, how it got there or where it came from. Even in a very strict IT change management program things can take a long time to get updated or can be temporarily missed. By scanning all available IP addresses you can feel confident that you are going to get a large percentage of devices on the network at the time of the scan. The SOC can have another critical role in this area by reviewing scanning results and performing a comparison to an asset management tool to obtain a total percentage of devices scanned. In

almost every environment there is a likelihood of having devices off, not connected to the network during the scan or that are transient such as laptops that do not get scanned on regular schedule because they are not always on the network. Keep in mind that various mandatory regulations may have an opinion in this area, which is something the SOC can help ensure compliance with. For example, the Payment Card Industry—Data Security Standard (PCI-DSS) states "all devices that store, processed, or transmit Primary Account Numbers" are in scope for PCI audits and as such must be scanned quarterly for vulnerabilities and have 4 quarterly clean reports. Something like the PCI-DSS limits your tolerance for devices not being scanned on a regular basis especially if it is in scope for the audit. Ultimately, you will have to figure out what is acceptable percentage for your organization. As I stated before, I like as a best practice in your vulnerability management program to scan IP on a 30 day rotation, this is typically due to the fact that new vulnerabilities are released every month and systems should be patched within 30 days of a patch being announced and available from a vendor. Again, for organizations complying with PCI, the PCI-DSS states that you have to have document quarterly clean scans, but if you only scan once a quarter it is not likely you are going to be successful in producing clean reports. By scanning every 30 days you give system administrators or your patch team three shots at getting a clean scan. This cycle is long enough to not to cause undue network bandwidth or impact performance of servers and desktops but quick enough to be able to see improvement metrics. The SOC has another important role here as vulnerabilities and patches are announced. The SOC should have the ability to pull in patch compliance of something that is deemed highly critical to an organization. This would require all system administrators (assuming system patching is not a responsibility of the SOC) to patch in some time frame less than 30 days. In my experience, there seems to be one or two times a year where a SOC I was building would require quick compliance for patching in 7 days. This is because the vulnerability the patch protected against was severe and that the risk of exploitation was so great that waiting 30 days would be too risky for the organization. Typically in those situations I recommend the SOC hold a conference call or meeting and invite all of IT or all interested parties to join together where the technical implications of the vulnerability and impact to the organization can be discussed. This will allow for clear communication regarding the time compliance expectations and what the requirements are to resolve the issue. It also affords the IT organization to ask questions, raise concerns or offer up ideas on how to move the process faster.

So what is a vulnerability and why does all this stuff matter?

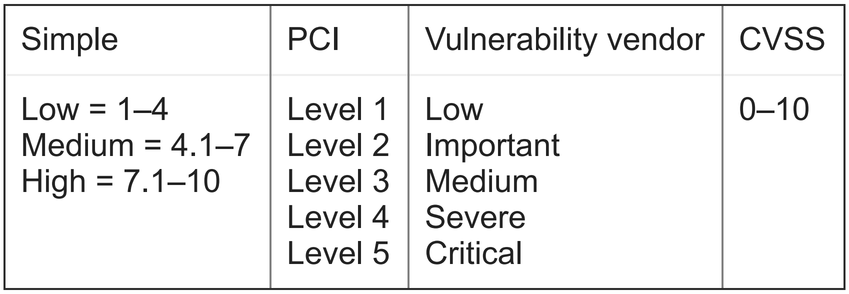
Vulnerabilities are security holes and bugs that are typically defects, or errors in software such as operating systems, drivers, and software applications. Unauthorized users and/or malware can use vulnerabilities to access desktops, laptops, servers or computer networks to steal data, degrade performance or disrupt services, and so on. As these vulnerabilities become known, software publishers develop patches, fixes, or updates that can be downloaded to fix the problem.

A good resource for vulnerability information can be found here → http://nvd.nist.gov/.

Vulnerability prioritizing

There are many different ways to score vulnerabilities but the principles are the same, the highest score equals the most critical vulnerability. An organization needs to have a fair and easily understandable way to score vulnerabilities and different methods mean different things for different people. What is right for your organization is up to you and there are many tools for you to use to help you in this area.

For example here are some ways to score vulnerabilities:



Simple	PCI	Vulnerability vendor	CVSS

Low = 1–4
Medium = 4.1–7
High = 7.1–10
	Level 1
	Level 2
	Level 3
	Level 4
	Level 5
		Low
		Important
		Medium
		Severe
		Critical
			0–10

CVSS2

CVSS2 provides a universal open and standardized method for rating IT vulnerabilities and scores range from 0 to 10.0. The scoring system is fully documented and available for use by the public.

Base CVSS2 threshold

The base equation evaluates the access vector, the complexity involved to exploit a vulnerability and the level of authentication required to perform the exploit as well as the impact of a successful exploit on the confidentiality, integrity, and availability of data. So an exploit of a vulnerability that can be performed over a network connection is easy to perform and requires little or no authentication receives a high score for exploitability. An exploit that reveals confidential information, damages or modifies the information in some way, or makes information unavailable to those who need it receives a high score for impact. The calculated values for exploitability and Impact are used in the base formula to determine the CVSS2 score. The base score is a value ranging from 0 to 10.

More information about CVSS2 Base scoring is available here → http://www.first.org/cvss/cvss-guide.html.
Calculations to establish base score can be found → http://www.first.org/cvss/cvss-guide.html#i3.2.1.

Temporal CVSS2 threshold

The temporal equation produces a score based on the base score as well as the current exploitation, remediation, and validity ratings of the reported vulnerability. A confirmed vulnerability for which a highly effective exploit is available, and for which no fix is available, will have a high temporal score. Temporal scores range from 0 to 10 can be no higher than the base score and no more than 33% lower than the base score.

More information about CVSS2 Temporal scoring is available here → http://www.first.org/cvss/cvss-guide.html.
Calculations to establish base score can be found → http://www.first.org/cvss/cvss-guide.html#i3.2.2.
If you are required to comply with PCI then you have to use an authorized scanning vendor/product to perform your scans and as a scoring system PCI uses the CVSS2 system but puts things into their own categories for compliance purposes. For example, scores range from 0 to 10.0, with 4.0 or higher will indicate a failure to comply with PCI standards and must be patched or an exception must filed and approved. There is also the legacy PCI scoring system that can still be used, as sanctioned by the PCI DSS. This system ranks vulnerabilities on a severity scale from 1 to 5. Any vulnerability ranking above 2 indicates failure to comply with PCI standards.

Level 5 vulnerabilities permit attacks with remote root or remote administrator capabilities that can compromise an entire host.

Level 4 vulnerabilities permit attacks with remote user capabilities and partial file system access.

Level 3 vulnerabilities permit access to specific stored information, such as security settings.

Level 2 vulnerabilities expose some sensitive host information, such as precise versions of services.

Level 1 vulnerabilities expose information such as open ports.

Also with PCI, any vulnerability leading to a cross-site scripting (XSS) or SQL injection will indicate failure, regardless of CVSS score.

Asset prioritizing as a part of metrics

Now that we have reviewed how to categorized vulnerabilities, we need to do the same with assets. Just as a reminder from above, the idea with vulnerabilities is to shut the door on hackers and malware as quick as possible. You want to be 100% patched across your entire organization but need to make sure you compliant as efficiently and as effectively as possible. Prioritizing assets are a great way to measure your overall risk exposure and give the senior leadership a level of comfort that risk is always being reduced in priority order. If you have a system that uniformly applies patches across your organization regardless of criticality I would still perform this exercise. Focused metrics and performance statistics on key or critical assets are extremely valuable and if you are always patched then that is a great metric to produce. This also allows you to measure the effectiveness of risk mitigation by setting goals of reduced vulnerability exposure and speedier mitigation. As you look at these valuable assets in your organization you can use them to audit the performance of security and IT teams performance, and implement process improvements to build a culture of refining your security operations.

Defining the relative criticality of assets is an essential step in your disaster recovery and business continuity planning process; as such this is a great opportunity for you SOC to get involved in detester recovery (DR)/business continuity (BC). In addition, the contingency plan standard in the HIPAA security regulation calls for organizations to “Assess the relative criticality of specific applications and data….”. If you do this right it will save you a significant amount of time because the information is reusable in many different areas. Here are some things to consider before embarking on your asset prioritizing effort.

Keep in mind that the criticality of your information assets is nothing more than a business decision about what systems or applications are more important than others. You should work to get a varying degree of opinions on each system or application. The more views the better. Chances are that an engineering team will have a very different viewpoint than a finance department. The relative criticality analysis is a team effort.

In managing critical assets, many organizations fail to fully understand the meaning behind a criticality ranking of systems. A “critical” asset may have the greatest impact on the organizations function, be it production rate, quality of product produced, cost per product produced, core network functionality or key financial system. Through proper construction of criteria and analysis of systems against that criteria will result in an analysis model that an organization can live by to determine what their critical assets are.

Here are some of the things you may want to consider:

- Business or customer impact

- Financial impact due to downtime

- High availability/uptime requirement (e.g., 7 × 24 availability)

- Safety or environmental impact

- Preventive maintenance history

- Mean time between failures (MTBF) or “reliability”

- Probability of failure

• Replacement or parts lead time

• Asset replacement value

• Planned utilization rate

• Number of users (i.e., large number of users)

• Stores critical information (e.g., grades, social security number)

• Impacts to reputation of the organization due to downtime

Also keep in mind that systems may be a critical part of your organization according to legislation, regulation, policy, contractual, or other predetermined means. There are many books and documents out there to help you in this process, I am merely using these points to show how a SOC can provide value in this area as part of the overall vulnerability management program.

The most common examples of critical servers are departmental file servers, web servers, mail servers, and database servers. A "critical" server can be classified as such by being important to accomplishing organizational missions or one that stores legally protected or other important non-public data. Here are some examples of what you may find as critical servers in your organization:

• Enterprise level services that is used by all employees or significant to one or more lines of business.

• Servers storing significant amount of legally protected data

• Availability is critical or important

• Servers hosting key financial applications

• Servers running or hosting applications for industrial control systems

• Credit card processing servers

• Servers on disaster recovery plans

• Core routers

Now that we have an idea about vulnerabilities, ways to prioritize them as well as assets, we need to put it all together to demonstrate some useful metrics. These metrics are key to how your SOC is viewed outside of its area. It can very quickly become a critical product that becomes one of the key faces of the SOC.

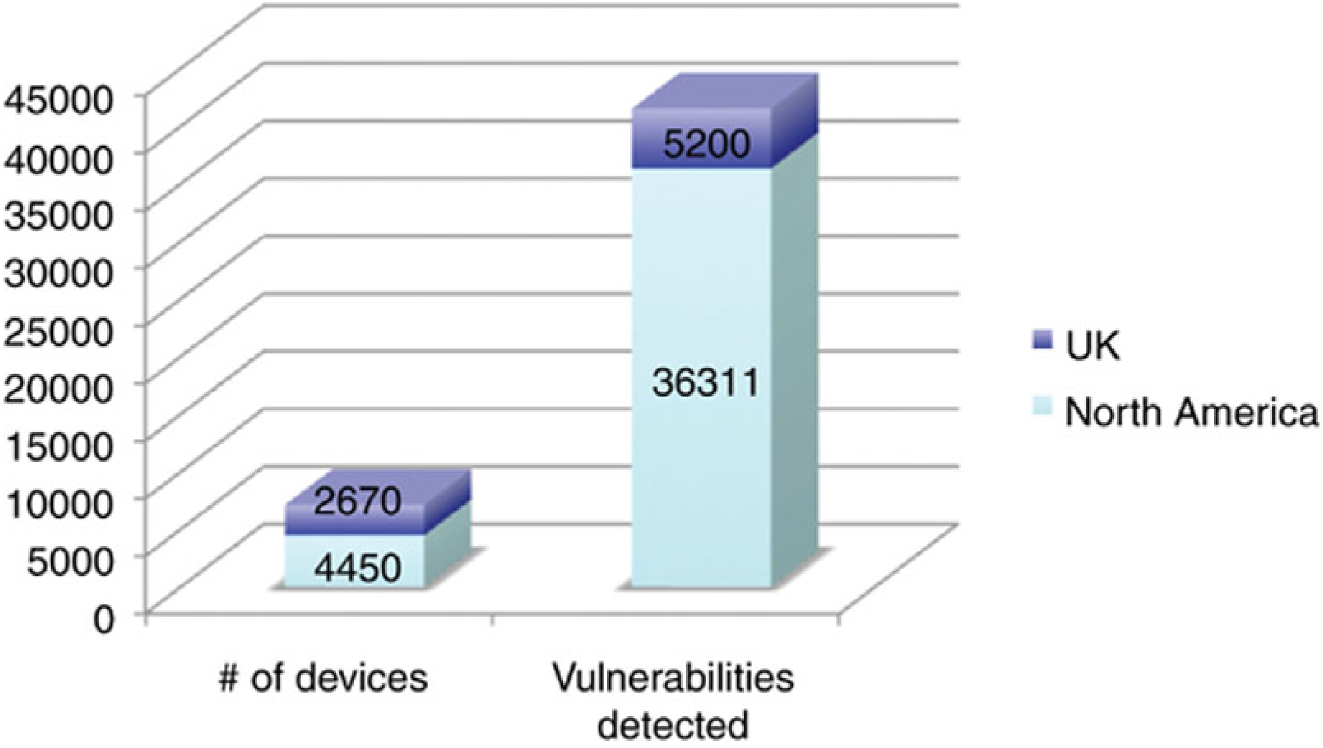
Scanning metrics can be tricky and time consuming to produce, you have to be careful that you represent what is truly happening in an environment. Good vulnerability metrics can be vital to an organization and a key product of your SOC. Vulnerabilities are very dynamic in any environment and it is not always easy to get a handle on it in a consistent way. Creating metrics in this area is highly valuable in order to continually improve your security risk posture, you must measure it using common metrics and compare it to past measurements in some meaningful way.

Some of the challenges come from how often new vulnerabilities are announce or the frequency of when patches become available. Additionally, vulnerability-scanning vendors regularly update how they detect vulnerabilities by changing specific methods to verify or discover that a system is indeed vulnerable to an issue they were checking for. For example, this means that in some cases if you have a system where 10 vulnerabilities are detected today and report it as such and then next week you detect that there are 12, did you increase by 2? In fact, all 10 of the previously detected vulnerabilities may have been resolved but 12 new ones were detected. In this case if you reported the metric of 12 you are going to upset the system administrator or the person in charge of patching systems unless you can accurately reflect the previously accomplished work.

For another example to help understand the complexities, let us say that you decide to only report on newly detected vulnerabilities 30 days or older. As scanning vendors update their detection engine you may find that a system was vulnerable to something several months old but not detected until now due to the updated detection method. This is because the scanning vendor constantly tries to improve its product and customers constantly provide feedback and various false negatives get fixed. This does not mean that the system was not vulnerable until it was just detected but it could be that nobody knew about it until it showed up in the scan results. So let us say that this occurs and the newly detected vulnerability was actually announced by the vendor a year ago. This vulnerability has affected the system for a year but it was just detected, so do you beat up the system administrator for having an un-patched vulnerability on their system for a year or do you expect them to patch during their normal cycle now that they know about it and you can hold them accountable to the results? Some would say that administrators should patch their systems regularly and should be fully aware of any vulnerability that affects the systems that they manage regardless of scanning and reporting. Unfortunately this is not always reasonable in large organizations so be aware of this pit fall and make sure when you report your metrics that you are not alienating your IT staff, you need their help.

Now that we have discussed some pitfalls of vulnerability metrics, let us look at some other more specific metrics you may want to consider. This is where a SOC can provide some great benefit. As security professionals the SOC should be able to look at the results of a scan and be able to quickly determine the validity of the results, rule out any obvious false positive items and craft meaningful reports for the various levels of people in the company who need them.

A simple metric is the number of current vulnerabilities detected in an organization. This metric can be shown against the total number of devices in the organization by region if you want.



Sources of vulnerabilities could include new un-patched systems or applications introduced to the organization’s environment or the discovery of new vulnerabilities on existing systems and applications. Unfortunately this can be a fairly large number and a bit scary if you are just starting out. As we previously discussed, one of the very first things you can do is work to classify vulnerabilities and your assets into priorities to help make the process more efficient. If you have a high priority system with a high priority vulnerability then it is obvious you need to fix this first. Then a simple report can be generated to show the top 10 vulnerabilities that exist on the top 10 critical assets. Seems like an ideal punch list for someone to focus on if you ask me!

Let us break this down further and see if there are other interesting metrics that can be produced.

The vulnerabilities can be breakdown by operating system, application, or organization division. The intent is for the metric to show the number of high, medium, and low vulnerabilities that exist in a specific area in the company. Again, as discussed before, you may use a different breakdown of vulnerabilities other than high, medium, or low. This metric provides a high level measurement of how the organization is doing, cut across several dimensions. You can break it up as much as you need to in order to fit your organizational requirements.

A nice example of this metric may be the following:

# Critical vulnerabilities detected	# Devices	Operating system	Department
3474	247	Windows 7	Finance

Another important metric is the most vulnerable applications, with a breakdown into vulnerability score by application version—this metric helps highlight old, vulnerable versions of software that should be upgraded or eliminated. This also demonstrates the risk to an organization associated by a specific piece of software that is not being managed or updated properly. There are many ways to show this and depending on your organizations patch management practices this could be very useful to highlight areas that need more focus.

How about unowned devices and unapproved applications? Vulnerability scanning systems typically do a good job at enumerating device names and if you are performing authenticated scans then the system should be able to provide you a list of installed applications by devices and as an entire list. Assuming your organization uses a standard naming convention for devices, when you look through a sorted list of device names you should be able to easily spot devices that do not belong. If you are able to filter out devices that were detected on guest networks then you should have a fairly good listing of devices that are either misconfigured or just do not belong on your production network. Having your SOC track down these devices and determine why they are connected and who connected them may be a smart thing to do. This metric is very useful to track "unowned" devices that may be rogue devices or simply contractor/consultant systems, as well as the trend of applications that are not specifically allowed on the network.

Historical monitoring of patches

If your SOC announces patches to the organization and tracks those announcements then you can chart metrics based on those previously announced patches between specific dates. Take a look at the announced patches against the number of assets detected to be missing those patches. This will help you determine the number of patches still not installed. This could indicate entire software updates that have not begun to be installed by system administrators or by patch management tools. As a result this can easily tell you the number of open vulnerabilities due to the missing patches that currently exist on your network. Although this is a risk metric it is also a good metric to give your system administrators as they can use it as a priority list of patches to be installed if you assume the highest number should be patched first.

After the fact metrics are also vitally important, you need to know how long patches are an open issue. This will tell you how long your systems are vulnerable for but will also tell you what the average time to remediate systems needed patches take. Like some of the other metrics you can slice and dice this up by device group, by category or by patch type. From a compliance perspective, this metric also tells you how many patches are behind per your organization policy that has a dictated deadline. Additionally this metric can be further expanded and compared with other metrics such as what vulnerabilities are currently being exploited in the wild, are currently not patched in your organization but are also being taken advantage of by malware that AV may not be catching.

Finally your SOC can track how many systems are being compromised due the malware and exploits taking advantage of known missing patches on systems that have been reported to be out of compliance. Depending on how bad this situation is in your organization it would also be important to create a metric show how much time it takes for the SOC to go through this entire process of announcing patches, scanning for vulnerabilities, remediating systems, and providing metrics.

Putting this all together, you can create what I consider a metric of the window of opportunity. This is the time from when patch is available until there is 100% application of that patch is the "window of opportunity" to have that vulnerability exploited and leaves the enterprise at risk. Although you may think there are other items that can be in this list, the basic concept is the same no matter how you want to slice it up. The order usually looks like this.

1. Vulnerability discovery

a. This is a "negative day" event; this is where an attacker discovers a vulnerability and creates to software needed to take advantage of the hole. The attacker will then devise a mechanism to deliver and properly exploit that vulnerability. This could typically happen several days or months before the next step of zero day.

2. Zero day

a. Typically zero day refers to an attack that exploits a previously publically unknown vulnerability in a computer application. This also means that there is no patch to address the vulnerability and close the security hole.

3. Public exploit code available

a. In this stage, the code needed to exploit a vulnerability is no longer in the hands of the select few. It is either published by the original creators or someone else and is now freely available to the general public who are interested in using it.

4. Mitigations deployed

a. Depending on how much you know about a particular vulnerability you may be able to perform several actions to reduce your risk and exposure without actually patching. This could be closing off or restricting firewall rules, deploying intrusion detection signatures for the type of activity that might occur, and so on.

5. Patches available

a. This is the day the vendor publishes the required software patch and procedure to fix the hole.

6. Patches deployed

a. This is the day your organization deploys the required patch.

There are many metrics you can make if you track any of the above information for an individual vulnerability and its specific patch. Select metrics could consist of the mean time to risk reduced. This is great to show how proactive your SOC is and the steps you take to protect the company. A residual risk metric could be a tail value, which would be calculated after your set policy deadline for patching, the number of devices where the vulnerability still exists and the criticality of the vulnerability associated with the effectiveness of the mitigations you deployed. It will also help to demonstrate the current state of risk your organization is in when the vulnerability begins to be exploited and malware begins to arrive targeting the issue.

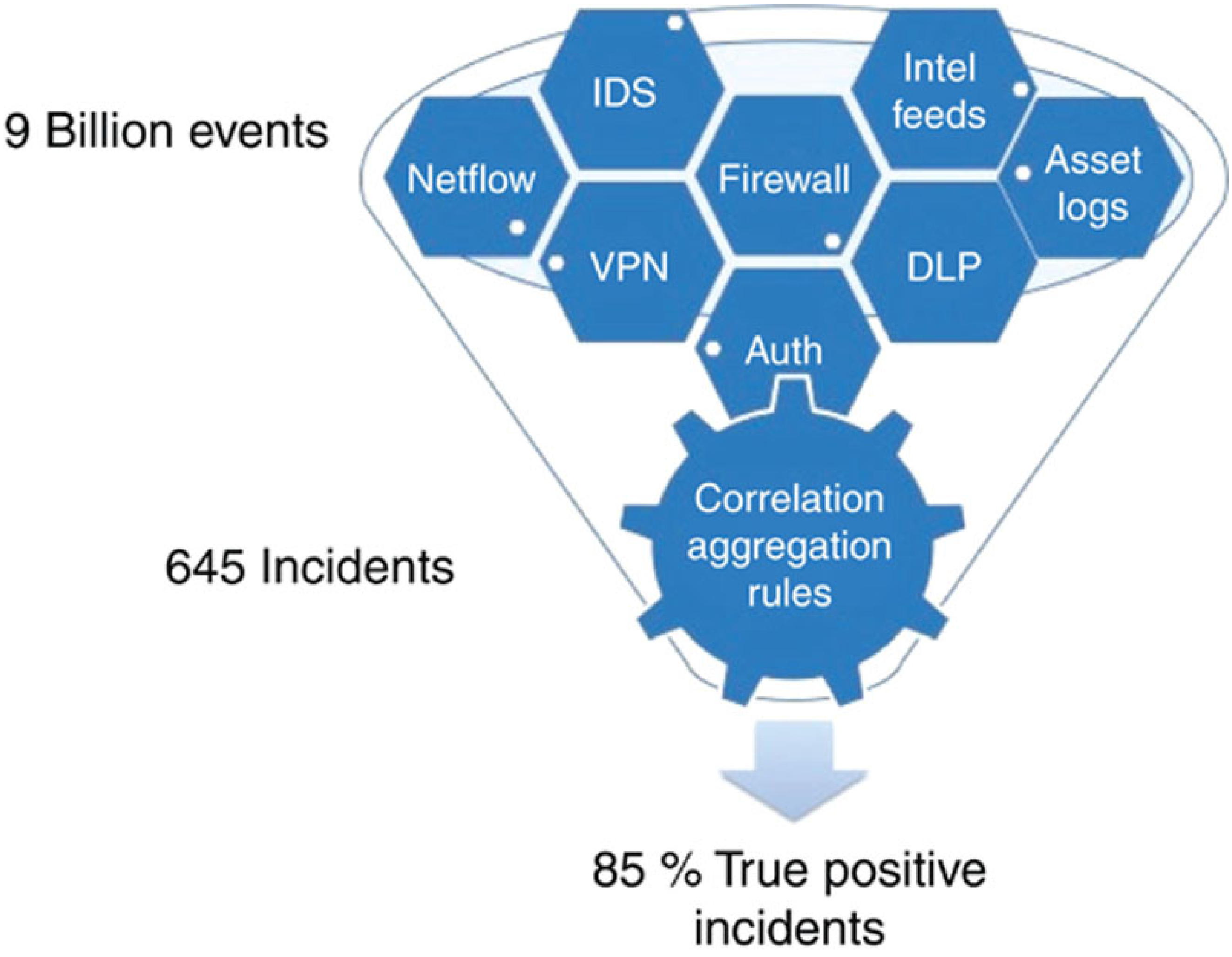
The numbers should help drive the point home that patching in the first place is cheaper, more efficient and just better for everyone involved. Otherwise you are demonstrating through metrics all the hard work of your SOC, which is not a bad thing at all.

Keeping on the trend of incident based metrics, and using them for security analysis, threat based metrics can have some very interesting results and can also help tell you and your organization how well you are doing in specific areas.

Have you ever wondered how many viruses were blocked by the antivirus system? As a security practitioner this is not a value that is very important to you but if your antivirus (AV) systems are doing a good job then people may forget how important the tool is in protecting the computers they are installed on. Your management and leadership may not realize that the care and feeding your SOC puts into making sure systems are kept up to date with AV and how that pays off. Of course the number of viruses AV let through and how many systems get infected on a regular basis is also an important metric and one that should be tracked on a much closer basis.

Sticking with the malware theme, understanding the types of malware encountered (i.e., virus, worm, Trojan) and how this compares to other similar organizations or the universe as reported by an authoritative source is very important. There are a few magazines and websites that publish weekly or monthly virus metrics, you can use these sources to compare what you are seeing on your network. You want to make sure you are seeing and catching the right things or you may find that you are missing something. If possible you also want to find out how the threat penetrated the organization in the first place (i.e., email attachment, website visits, hacking). This information is vital when you look to see how you can improve the overall security of an organization. It will also help you evaluate the need for additional purchases of threat mitigation solutions. It should also help you understand how you should prioritize different threats and which ones you may need to monitor more closely or even which assets you should monitor closer.

Overall metrics are also important to calculate and use especially if the metrics show the effectiveness and efficiency of the SOC. The SOC needs positive press to ensure that people can appreciate the hard work they do. A great way to present the efforts of a SOC into an easy to understand metric is a funnel chart. The funnel chart can show all the data feeds the SOC is currently collecting, such as Firewall data, VPN, IDS, and so on. There is a raw number of events that are generated by all these devices and fed into a log collector or SIEM tool. Based on rules, correlation, and aggregation of these events only a few incidents are generated into tickets that the SOC actually has to analyze. Then there is a false positive rate that can also be calculated based off of ticket information. To build this chart you need to look at every aspect of the SOC.



We start off looking at every single individual event that was either collected or generated into the SOC tools inside of a single month. In the case above, we are looking at 9 Billion events total for the month, this can be broken out by device type or what device generated the event if you want that level of detail. Next, all the events go through a SIEM tool or some kind of collection point that is able to look at the events and determine their validity for a SOC review and analyze. There are many ways that events can be condensed down. First you can have an aggregation process, this is where you take multiple events that are the same, count them up and produce only a single incident representative of all the others. So for example, does a SOC need to see 10,000 deny logs from a firewall or just a single event that states there were 10,000. Aggregation saves a ton of time and dramatically reduces the number of investigations a SOC needs to perform. Multiple events that are generated by the same session or packet, same host or destination or that has similar attack attributes can all be condensed into smaller or single events opposed to sending the raw information to an analyst.

Rules and correlation are a way to take events that mean almost nothing and join them together to mean something that is worth an investigation. For example, one user visiting a website is not necessarily bad unless there is a rule that states the website is bad and an incident gets created for the SOC to investigate.

The reduction of raw events by aggregation and the creating of new events with rules and correlation in the above chart shows that 645 incidents were generated in total for the month out of the 9 Billion presented. This is a good metric to look at and can help you understand many different aspects of your SOC. For example, if the total time it takes to address an incident ticket, analyze, and escalate if needed is appropriately 15 min, then this translates to approximately 161 h of work for the month by an analyst. That is enough work for a single analyst working a 40-h workweek and they will have no time to do anything else.

The next value we see is the 85% true positive rate, this is a very important metric because it shows the overall effectiveness of the system. Out of the 645 tickets generated less than 100 were created falsely. If you have an engineering team responsible for tuning all the devices, creating rules and making everything work then this is a great tribute to their efforts or whoever is responsible for all that hard work. It also gives the team a nice metric to look at when compared to the total number of events, the number of rules and the total effort going into managing the entire system. The focus should be on working hard to get the true positive percentage higher so that nobody is working tickets that do not matter and everyone can work on tickets that do. These types of metrics should also be reviewed along with how many new rules were created in a month, alongside new rules created in security devices such as IDS signatures or data loss rules and how those new additions effected the overall total incidents generated into the SOC and if the overall true positive rate rose or fell for the month. Additionally, these metrics can help you understand the overall level of work being performed in the SOC and what the total capacity is for the SOC to perform its function. If you use the graphed example above in your SOC and you had two analysts then you can deduce that if all the tickets were evenly worked than each analyst worked 20 h a week on incident tickets. Knowing that the average ticket takes 15 min then each analyst has the capacity to work an approximate additional 80 tickets per week, assuming that analysts do nothing else but work tickets. This is important as you look to put more security tools in place and increase the workload in the SOC. This metric allows you to see how efficient the SOC is running and what your overall capacity may be to perform incidents. Obviously there are many other factors that need to be reviewed and a single significant incident that takes all day to resolve or many days or weeks to resolve may cause these numbers to change dramatically.

Lastly you can break down what type of incidents occurred in what parts of the organization against what assets or types of assets. This will help you evaluate repeat issues or targets that may be too soft and needs some hardening or even users that may needs some extra security awareness training. Additionally, by looking at these types of metrics you may even be able to understand better who are our attackers and specifically what are they targeting or possibly trying to steal from you.

As you progress in building your operations, the metrics will help you evaluate your response to security threats. You can ask important questions like how many incidents are you tracking and how long did it take to investigate and remediate incidents or even how effective the security systems are that you have in place. Are your resources allocated appropriately? Do you have the right number of people reacting to issues? Only your metrics can tell you. Your operations center will have largely different metrics than others, that mean something to you and that help identify how well or how bad your tools are behaving for you. Different security suites of tools will lend its self to different metrics that you will want to track. Do not worry about having too much, or metrics that are not good enough, metrics that work and that tell the right story will be asked for by others. Try making metrics, use spreadsheets or pull them from your tools directly, not matter how you get them just get them and try to use them, try to make sense out of them and try to see if others would benefit from them as well.

Every SOC should see themselves as a service organization. Even if you are an internal operations center or especially if you are an outsourced security provider you need to define and identify who your customers are and make sure you are continually providing value to them. Keep your customers engaged, show off your value, produce quality metrics that mean something to them and that is as actionable as possible. Engage with them and ask if there are more metrics you can provide or work with them to define better metrics. The SOC is on the front like every day battling the cyber war, unfortunately there are no physical wounds or physical costs associated with this as it is all virtual. You need to demonstrate your strength, efforts and communicate your weaknesses effectively so that others easily see your value and understand your struggles.

Provide daily metrics to your SOC to keep them on task but do not overload them with meaningless information. Keep it simple, useful and easy to understand. Provide supervisors with a nice mix of daily, weekly and monthly information to help them ensure they are steering the ship in the right direction and have enough real-time data to make immediate course corrections. Provide management with weekly, monthly and yearly metrics to help educate them on trends and ensure they are kept up to date on trends, issues and of course successes. If at all possible, ensure that senior leadership also gets metrics specifically designed to keep them updated on what is going on and things that may be important to them. The SOC may never get a seat at the table with senior leadership but that does not mean you should not provide regular information and updates to the best of your ability. It will go a long way when problems do arise and you can be assured that they will. Do not forget that data become information that can be turned into metrics. It is those metrics that you must analyze in order to take the right actions.