Interested in learning more about security?

SANS Institute InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

A Model for Handling Security Issues within a Network Operations Center

The Network Operations Center uses numerous tools ranging from Intrusion Detection (Snort) and Intrusion Protection (Tipping Point) to simple SNMP monitors (Netsight Element Manager). I will discuss how they use these tools to maintain a secure IT environment and assist Network Administrators as well as protect the campus community. The Network Operations Center also provides a level of physical security for critical University systems, both campus-wide as well as internal to the Network Operations Center. This paper w...

Copyright SANS Institute

Author Retains Full Rights

AD

Take control of vulnerability threats Now! Request a Free Trial Secunia Stay Secure

Date: July 1, 2004

Name: Tonya Heath

Certification: GIAC Security Essentials (GSEC)
Version 1.4b Option 1

Eye of the Hurricane: A Model for Handling Security Issues within a Network Operations Center

Abstract

This paper will provide a model for how to handle IT Security related issues within a Network Operations Center or NOC. It will use a Network Operations Center in a University environment as an example. Because this paper contains specific tool and architectural information, the name of the institution has been withheld to protect the integrity and sensitivity of its operations. I intend to explain: a) the functions of the Network Operations Center, b) the IT Security services it provides, such as monitoring the Intrusion Detection and Intrusion Protection logs, monitoring incoming and outgoing internet traffic for spikes in bandwidth, and using packet sniffers and analyzers to examine possible bad traffic and c) possible areas for improvement and growth.

The Network Operations Center provides a broad range of services, and I will cover the applicable functions that pertain specifically to IT Security. There are several tools that the Network Operations Center employs that assist with handling the various security issues, such alerting and coordinating efforts in containing virus outbreaks and disabling or re-enabling network access for various other types of infections.

The Network Operations Center uses numerous tools ranging from Intrusion Detection (Snort) and Intrusion Protection (Tipping Point) to simple SNMP monitors (Netsight Element Manager). I will discuss how they use these tools to maintain a secure IT environment and assist Network Administrators as well as protect the campus community. The Network Operations Center also provides a level of physical security for critical University systems, both campus-wide as well as internal to the Network Operations Center. This paper will explain how all of the different departments utilize the Network Operations Center and how the Network Operations Center provides assistance to these areas while using Standard Operating Procedures and how this applies to IT Security.

Finally, I will elaborate on two possible ways for improving the Network Operations Center: improving documentation methods and creating a stand alone Security monitoring area.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

I. Network Operations Center, Where it all Goes Down - Literally: Explanation of the Network Operations Center and its functions

This Network Operations Center has been in place, in its current state, for approximately six years. The "NOC", the preferred local nomenclature, is constantly evolving. What began as a place for operators to utilize simple tools has become an extremely technical, secure location where highly skilled NOC Administrators are responsible for monitoring and analyzing specialized tools used for detecting various IT related outages, outbreaks and / or "meltdowns".

The NOC is staffed with a rotating staff of Administrators that ensure around the clock coverage, 24 x 7 x 365. There are other members of the NOC that handle various other duties, including an in-house software developer, a network and security specialist, Remedy developers, an electrical engineer, and, of course, a manager.

Day to day, Administrators in the NOC are responsible for many tasks. However, one may not realize it if you happened upon an Administrator during his or her shift. The job is quite sedentary and if all is quiet on campus, then all is quiet in the NOC. On the other hand, if there is any type of outage they are likely to see it first. For example, when a power line is cut by one of the construction crews working outside of a building within the campus LAN, the NOC will be the first to know because the network switches in that building are being monitored. Admins are then responsible for notifying campus electrical distribution, Networking and the Help Desk. They help in coordinating efforts with Networking Analysts, Electrical Distribution and the Networking technicians dispatched to handle any switch reboots that may need to take place. Assisting Networking in making sure that the network is available throughout campus is a critical function of the NOC. This is an example of how the Availability portion of the C-I-A concept is utilized within the NOC. Traditionally, information security has been aligned towards the accomplishment of three objectives: Confidentiality, Integrity and Availability, referred to as "C-I-A".[2] Other instances of C-I-A will be addressed later in the paper.

As a matter of Defense In Depth, the NOC addresses this concept in several different manners. Intermapper and Cricket offer a broad view of the network traffic including incoming and outgoing network bandwidth. Cujo, Spectrum Alarm Manager and Netsight Element Manager offer a machine level view. This concept can also be applied to how physical security is handled within the NOC. Each person is authenticated via the Intellikey system, which will be explained later, and the video surveillance offers a broad view of any activity in the entire area.

[2] SANS Security Essentials with CISSP CBK The SANS Institute (April, 2003): pg. 259

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Administrators must know how to analyze and compare the various monitors in the NOC in order to interpret what kind of "events" may be occurring. There are several monitoring tools that are used that furnish different types of data. The Availability portion of the C-I-A concept applies here. These are the tools that were developed in house:

- Cujo: Performs ping, SMTP, and FTP tests to servers, workstations, and Network switches.
- ISP Latency: Provides graphical information that illustrates traffic levels and latency from various ISPs, i.e., Level3, Qwest, BellSouth and RoadRunner. This monitor is useful when users report problems with connectivity off campus. It could also be an indication of a Denial of Service Attack.
- Pause Monitors: Supplies tabular and graphical illustrations of network related "pauses" on various network equipment. It is also a means for monitoring latency and availability of a network device or system.
- Service Monitor: Gives a top level view of various critical campus services, such as email, DHCP, DNS, Remedy (the trouble tracking system that is used by most IT groups within this organization), University Web, etc. It has a "drill down" capability that gives statistical information about each service as well as dynamic contact information that may be needed in the event of an outage or problem.
- Message Center: A web site that provides postings of scheduled or unscheduled campus events that relate to Information Technology. For example, if a new Gaobot variant has hit campus, Administrators will post a message here warning the Campus community. The message will contain any relevant information for fixes, (i.e. links to websites or numbers to call for help).
- Blox: Also a website that lists machines that have been removed from the campus network for various reasons and placed into the "Penalty Box", DHCP disabled or Port disabled. It also provides a search capability, via MAC or IP address that enables Departmental Administrators, the Help Desk and / or users to determine if they have been removed from the network.

And others not developed in house:

- Cricket: A high performance, extremely flexible system for monitoring trends in time-series data. Cricket was expressly developed to help network managers visualize and understand the traffic on their networks, but it can be used in all kinds of other jobs, as well.[4]

[4]" Cricket Home" (April, 2003): pg.1<http://cricket.sourceforge.net/>

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

- Spectrum Alarm Manager: Spectrum is network management software to monitor the status of devices on the network.[5]
- Netsight Element Manager: Monitors switches, routers and ISDNs. It uses the Simple Network Management Protocol (SNMP) to gather information on the various devices and presents them in a graphical format.
- Tipping Point SMS Client: Provides a graphical illustration, via the "Dashboard" that shows various incoming and outgoing attacks on different network segments. This is an Intrusion Protection System that has broad coverage across numerous network segments.
- Intellikey: Monitor that helps ensure physical security of the NOC. Staff members are given Intellikeys that identify them to the Intellikey system when they use the key to enter any of the four doors that lead into the facility.
- Snort: Snort is an open source network intrusion detection system, capable of performing real-time traffic analysis and packet logging on IP networks.[6]
- Intermapper: InterMapper's active maps give a visual, real-time view of traffic flows through and between critical network devices and links.[7]
- Network Associates Sniffer: Shows the "Top Talkers" on the campus network and allows Administrators to perform real time packet captures. "Top Talkers" is a graphical illustration of users on the network that are using the most bandwidth. The NOC is usually interested in the top 10. A user who is taking up a lot of bandwidth may be an indication that something suspicious is taking place.

It is the responsibility of the Administrator to familiarize themselves with technicalities and the Standard Operating Procedures of each monitor in order to evaluate and glean information from each tool. This needs to be done so that an effective diagnosis can be given as to what may be occurring within the IT campus environment. In addition to utilizing these tools, the Administrator has to be able to communicate with the relevant parties, i.e. Networking, Systems, or Security the problems that may have been found.

The communication of reporting problems to departments outside the NOC is governed by the Standard Operating Procedures (SOPs) documented on the internal portion of the NOC website. NOC administrators must authenticate to the NOC website in order to access this information. This is another example of how the C-I-A concept is applied: Confidentiality and Integrity.

---

[5] "Spectrum Basics" (November, 2000): pg.1 <http://www.unc.edu/~hope/help/spectrum/basic.html>
[6]" What is Snort?" (June, 2004) pg.1 <http://www.snort.org/about.html>
[7] "Intermapper Networking Monitoring and Alerting" (June, 2004) pg.1 <http://www.intermapper.com>

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

These SOPs are very detail oriented. Large amounts of time have been taken to meticulously define the processes contained within the SOPs. There is an SOP that exists for *each* monitor. Escalations are built into each SOP so that *someone* is contacted in the event of an outage or problem. The overall NOC documentation has a large influence on their success. Because the documentation grows as the NOC grows, there is a rather large amount of information contained in the SOP portion of the website. The internal website has a search functionality that allows Administrators the ability to access SOPs quickly.

As mentioned earlier the NOC, as well as other IT departments within this organization, uses a problem tracking system called Remedy. Remedy provides a centralized location to enter data that pertains to a specific problem. It also provides escalation mechanisms which are key in a time sensitive environment such as the NOC. Remedy allows the NOC and the NOC manager to document the impact of outages. There is a field with preformatted text in which Admins can enter specific information that allows for tracking. After an event, reports can be generated that can tally the length of downtime as well as how many systems were affected. This information can be used to possibly improve processes for the next attack. As we have learned in the IT community there is always another attack.

In addition to its monitoring and technical duties, the NOC also serves as a central point of contact for most emergency situations that may arise on campus. These situations can range from a weather emergency, such as a hurricane, to a personal security incident that may have occurred in the area. The NOC is responsible gathering relevant information for campus police and University Public Relations and disseminating that information through the proper channels, using the Emergency Notification Procedures posted on the internal NOC website and on a clipboard inside the NOC.

The NOC's ability to access Critical SOPs is imperative. There is a dedicated machine in the NOC that is directly attached to a NOC server that contains the SOPs. The connection between the NOC machine and the server is not dependant on the network. In the event of a network outage, Administrators can still get to information they need. As a back up measure, all Critical documentation is printed out on an as changed basis and posted on a clipboard inside the NOC.

An important note to make: Since communication is one of the vital functions of the NOC, it depends heavily on the use of the radio. There are two radios in the NOC. One is set to Priority Scan, which means it is constantly scanning the different bands on campus for activity. There are several bands on campus that the NOC monitors for security reasons. The volume is kept low except during a campus emergency. During emergency situations the NOC has the capability to communicate with the facilities department and campus police using this radio.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

The radio is critical for communication when the network is down (no access to email, Remedy or other commonly used functions that depend on the network). The second radio is used daily in communicating with the Networking and Security staff during network attacks or other events. On this radio there are different channels that are used by different groups. The NOC has the capability of switching channels in order to communicate with the group necessary.

II. How They Catch the Bad Guys:
Tools for Analyzing Internet and Campus Network Security

Of the aforementioned tools, the NOC specifically uses some of them in evaluating IT Security related events. They are, in order of relevance:

- Tipping Point SMS Client
- Intermapper
- Cricket
- Snort
- Sniffer

The Tipping Point sits inline on the campus network and blocks "bad traffic". However, it can serve as an indication of an event that may already be occurring *on* campus, therefore serving as a warning to Administrators for what may be to come. Also worth mentioning is the ability of the NOC to identify hacked machines via the Tipping Point and have their network access removed.

The Network and Security Specialist within the NOC has created a monitor using Intermapper that observes incoming and outgoing bandwidth from the two campus border routers. Intermapper also graphs the CPU utilization of each router. Should the Administrator on duty notice a spike in traffic, incoming or outgoing OR jumps in CPU utilization they may determine that this is the result of a Denial of Service (DoS) Attack.

This is where it is important for the Administrator to be able to combine information from multiple monitors and give a valuable analysis of what may be occurring. Spectrum Alarm Manager may begin "losing switches" which can indicate that campus switches are inundated with data and therefore become dysfunctional. During certain security events one tool, such as the Tipping Point, may be the only source that gives any indication of a problem. During other, perhaps more obscure events, a combination of tools could help provide data.

Snort is available to provide real time packet information as well as logs of different events that have occurred. The Network and Security Specialist on staff systematically goes through the logs in order to identify machines with various types of viruses, worms or other infections that may have appeared on the network. He then requests that network access of the offending device is removed until it can be cleaned or disinfected.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

The Sniffer can be of assistance in detecting sources and / or destinations of attacks. During an attack or virus outbreak, the Sniffer can be useful in tracking, and identifying culprits of "bad traffic". This information can be helpful in blocking and / or removing offenders from the network.

III. Model for Identifying and Isolating Compromised Machines

Financial losses due to cybercrime declined steeply last year. The findings, based on responses from 494 computer security practitioners in U.S. corporations, government agencies, financial and medical institutions, and universities, show that financial losses attributed to cybercrime have declined for the third year in a row.[8] This may be due to ever increasing technology and the ability to halt viruses, worms and various other hacks quickly and efficiently. It is one of the primary duties of the NOC to monitor, identify and assist in isolation of hacked machines.

There are four ways of isolating a user from the campus network:

- DHCP disable – Once the current DHCP lease expires, users are not able to renew until Networking, Security or the NOC allows them to do so.
- Port disable – Networking may disable the port of the switch the user in which the user is connected.
- Penalty Box – Networking may place the user's MAC address in the "black hole VLAN"
- Router Filter – The Networking WAN group can place a router filter on one of the campus border routers to stop traffic from an offending device.

Currently the Networking department employs SecureFast along with 802.1Q VLAN technology to manage the campus network. VLANs are used to segment the network and reduce broadcast traffic. A VLAN (Virtual Local Area Network) is defined as a broadcast domain within a switched network.[9] This technology has several benefits, including segmenting the network based on needs of users rather than adhering to geographical limitations. It also allows smaller broadcast domains which increases available bandwidth to users. SecureFast has a Network Management tool called VLAN Manager that enables Networking and Security to remove users from the network by placing their MAC address in a "black hole VLAN". The black hole VLAN is a closed VLAN that does not have a route table, therefore all communication is hopeless. Because it is a closed VLAN users cannot infect others within the black hole VLAN. This organization endearingly refers to this place as the "Penalty Box", hence the "Blox" monitor.

---

[8] Newsfactor.com *"Security Pays Off as Hack Attacks Decline"* (June 2004) < http://www.newsfactor.com/story.xhtml?story_title=Security-Pays-Off-as-Hack-Attacks-Decline&story_id=24839&category=netsecurity>

[9] *"Internetworking Technologies Handbook"*. Cisco Systems, Inc.(February, 2001) pg. 394

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

The Blox Monitor provides a summary of all isolated machines on campus, whether they are port disabled, DHCP disabled, or Penalty Boxed. The Blox Monitor has a search functionality that helps IT personnel determine if a machine has been removed from the network.

Another tool used for isolation is a script that was developed in house, called the SmartBoxIt Script. It enables authorized security or networking personnel to enter an IP address and have a Remedy ticket created based on a DNS lookup performed by the script. The script can create hundreds of tickets and therefore remove network connectivity from hundreds of offending machines in a matter of minutes. There are triggers built in that will alert Managers within the Help Desk when ten or more users have been removed from the network. This helps to serve as a warning to the Help Desk that an outbreak may be on the horizon.

IV. Steps in Identifying and Isolating a Virus Outbreak or a Denial of Service Attack

As most of us know within the IT community, virus outbreaks can be devastating. Below is a generalized view of how a virus outbreak is handled within the NOC:

<u>Virus Outbreaks</u>

1. Tipping Point – The Administrator may see a spike in blocked traffic on the Tipping Point, usually a jump above 100 attacks. Using the Tipping Point the NOC can determine the vector, type of attack, source and destination addresses, and destination ports.
2. Spectrum Alarm Manager – Depending on the size of the attack, Alarm Manager may begin showing alarms for switches that are not responding. If it is a large scale attack, Alarm Manager may have a large number of switches down. If it's a small scale attack Alarm Manager may not show anything at all.
3. Cujo – Basically the same as above (number 2).
4. Intermapper and Cricket may begin to show signs of high bandwidth incoming or outgoing. If it's a large scale attack, bandwidth may severely drop because switches are unable to pass traffic due to high volume.
5. The NOC is responsible for alerting campus that there is a virus outbreak and to beware. They are to call the Help Desk and convey to the best of their ability what is happening.
6. They are to also send an emergency notice out. This notice is an email that goes out to Departmental System Administrators campus wide. The notice will contain a brief description of what is taking place, the time when the event started, what is being done to handle the event and a number to call with questions, usually the Help Desk. An archive is kept of all notices for tracking and referral purposes.
7. Administrators are also to post any information related to this event on the Message Center.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

8. Depending on the scale of the attack and if there is a significant loss of connectivity, the Major Outage Notification SOP comes into play. This is an SOP that enables the NOC to reach all IT Directors campus wide via voice mail. This voice mail is updated hourly as long as the outage lasts.
9. Once the vector is determined, it becomes a major coordination effort with the NOC to assist with Networking and Security to stop the outbreak. By using a combination of Tipping Point filters, Router Filters and the SmartBoxIt script, the outbreak can be controlled and connectivity restored. All of the Isolations are tracked with Remedy which becomes very important in the Clean up stage.

Cleaning Up:

Once the smoke has cleared lots of users are left without network connectivity due to the fact that their machine was most likely infected with the virus or worm that had dominated network traffic minutes, hours or days before. Remedy and the Blox Monitor are very important in the clean up effort. During this stage there may still be machines on the network that are infected. Networking and Security will *always* handle removing infected machines before releasing clean machines. This is in an effort to make sure the Network is stabilized and that all infections are cleared up before allowing users to regain access.

1. Users will call their departmental support person OR the Help Desk complaining of loss of connectivity.
2. Departmental Admins or Help Desk personnel will then search the Blox monitor to verify whether the person has been pulled from the network.
3. If in fact they have been pulled from the network, the user must clean their machines before network access will be restored. The Help Desk or Departmental Admins can provide support in that area.
4. If a Remedy ticket has not already been created, it will be created at this point and forwarded to Security for clearance.
5. Security will check the worklog in Remedy to see what specific steps were taken to clean the machine. If Security gives the go ahead, the ticket is then forwarded to Networking or the NOC to restore network access. If Security is not satisfied with the work that has been done to clean the machine, they will send the ticket back to the Help Desk for re-checking.

When there is a Denial of Service Attack it often occurs without warning. Administrators must be vigilant in order to catch one as soon as it begins.

<u>Denial of Service Attacks</u>

1. Cricket / Intermapper – The Administrator most often will notice a spike in traffic, incoming and sometimes outgoing.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

2. Network Associates Sniffer – The Administrator then looks at the Top Talkers on the network to determine the source and destination of the DoS Attack.
3. If it is determined that the source of the attack is coming from on campus, a Remedy ticket is created, marked Isolation Requested and forwarded to Networking for Penalty Boxing.
4. If it is determined that the source of the attack is from off campus, a Remedy ticket is created, marked Isolation Requested and forwarded to the Networking WAN group for router filtering.
5. If the campus network suffers an outage due to the DoS Attack, the Help Desk must be notified, an emergency notice must be sent, the Message Center must be updated and the Major Outage Notification SOP must be completed.

Note: When a severe attack occurs the radio may be used for the communication of these requests because time is precious. The Remedy ticket may be created after the fact for tracking purposes. However, all Isolations are tracked with Remedy.

V. Physical Security: Protecting Valuable Resources – People and Equipment

Because the NOC houses millions of dollars worth of critical IT machinery, physical security is of the utmost importance. First of all, and most simply, there is an around the clock presence in the NOC. At no point in time is there a lapse in coverage, nor has there been under current management, which has been almost six years. If an Administrator is late for his or her shift the Administrator currently ON duty must wait until they are relieved.

The NOC uses an Intellikey system to allow authorized personnel to access the facility. There is a process that is required of a person requesting Intellikey access, referred to as Certification of Intellikey Users. Any individual requiring access to the NOC must adhere to the following procedures to obtain an Intellikey as a certified user:

- Fill out and sign the Application for Intellikey Access
- Be sure to designate the area(s) for which access is required
- Have his/her manager approve the request by signing the Application for Access
- Submit the form to the NOC Intellikey Access Manager for approval

All submitted forms will be kept on file by the NOC Intellikey Access Manager.

Only personnel with proper access (Intellikey access) are admitted inside the NOC, all others are prohibited without an escort. There are two different methods used in tracking visitors to the NOC:

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

1. Sign In / Out Sheet
2. Badges

The Sign In / Out sheet is a requirement of all visitors. On the Sign In / Out sheet the visitor is required to provide:

1. Name
2. Time in and time out
3. Purpose of the visit
4. Escort's name
5. Escort's phone number

The Sign In / Out Sheets are kept on file in the NOC for tracking purposes. In the event that there is a question about whom, when and / or why a person was allowed onto the floor, there will be a written record of the occurrence.

A visitor is defined as someone without Intellikey access. Each visitor is a member of one of the following categories:

- Vendor
- Staff
- General

Because of the nature of the NOC equipment breaks, parts need replacing, upgrades are necessary, etc. Outside vendors are often brought in to assist with these tasks. This is where a Vendor Badge would be used. There also is a need for unauthorized staff to be able to access the machine room floor, whether it is for a tour of the facility or for someone to attend a meeting. This is where a Staff Badge would be used. They must have an escort with authorized access. Thirdly, there may be someone who is not a staff member or a vendor, but may have a need to access the floor, such as a staff member's spouse or a visitor from another campus who would like a tour of the facility. This person would also need an authorized escort and would get a General Badge.

Badges are a safety mechanism in place that helps to identify the function that person serves on the machine room floor. For example, if a member of the NOC staff or any other authorized personnel saw someone wearing a General Badge and him or she was tampering with equipment, which would be an immediate red flag that something inappropriate is taking place.

Generally, safety is the top priority when physical security measures are implemented, and most information security practitioners will consider safety the top priority for their enterprise environment.[10] Personnel are often the largest

[10] "*SANS Security Essentials with CISSP CBK The SANS Institute*" (April, 2003): pg. 260

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

asset to any operation. There are several mechanisms in place to protect not only the equipment but the people that are there to manage and protect the equipment.

Placed strategically throughout the NOC, the machine room floor and the hallway outside of the facility are over fifteen video surveillance cameras. From inside the NOC, Administrators have the ability to monitor activity of all video monitored areas via a centralized system. There is 540GBs of available space which enables the NOC to maintain this data for up to one year. Obviously this provides a tremendous security measure for not only the machine room floor and its assets, but also NOC personnel. After business hours the Administrator on duty is often the only person inside the building. He or she has the ability to monitor any activity and therefore possibly prevent any possible personal security problem.

Outside of business hours the doors to the building that houses the NOC are locked. If anyone needs access to the building during that time there is an intercom with camera located at both of the outside entrances. Persons wishing admittance must push the intercom button and wait to be identified by the Administrator on duty before they are allowed inside. The Administrator can unlock the door remotely from inside the NOC. Again, this provides a measure of safety to the NOC as well as for the Administrator on duty.

Another measure of physical security that is worth mentioning is the Master Key Sign In / Out Sheet. The NOC keeps a copy of a Master Key and a Master Intellikey. Often times it is necessary for NOC Administrators to gain access to System Administrator's offices outside of business hours. Also, during business hours, System Administrators sometimes forget their keys or need access to a coworker's office for various reasons. To keep track of who uses the Master Key, the Master Key Sign In / Out Sheet is in place. On the sheet the requestor must supply his or her name, date, the purpose for the key and the time signed out. When the key is returned the Administrator on Duty will fill in the time the key was returned and initial beside the entry. This system not only tracks who used the key and for what purpose but also makes sure that the key has been returned. The keys are attached to a metal 18 inch ruler that is difficult to conceal. The Sign In / Out Sheet is kept on file in the NOC in case they are needed at a later time for reference.

Passwords are of premium importance and security in the NOC. There is one password that is used for all workstations that the Administrators use for monitoring. This password is changed every 90 days and is only known to NOC personnel. There are other passwords that are necessary for the Administrators day to day functions. These passwords are kept in a secure location that is only known to those working in the NOC.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Again, the C-I-A concept becomes useful. The Availability portion of this theory is thoroughly covered within the NOC by controlling access with: round the clock personnel on staff, Sign In / Out Sheets, and a Badge System. Integrity and Confidentiality are managed by using one secure password and keeping that information and all other passwords secure.

V. Summary

The NOC's functions are constantly evolving. Over the past three years IT Security has become more of an issue within the NOC. With the addition of new and more advanced tools the NOC's capability in identifying, isolating, and filtering bad traffic has become more efficient and effective. Each new outbreak or event teaches the NOC personnel how something could have been handled better.

C-I-A and Safety have always been major concerns within the NOC. The Intellikey system, Badges, Sign In Sheets and video surveillance provide the safest environment possible in that location.

The first area I would like to suggest for improvement would be to perhaps create a primary security monitoring location. Because IT Security is becoming a greater issue within the IT Industry more focus may be necessary in that area. NOC Administrators seem to be able to handle the current workload however, during a massive outbreak or event, it is always necessary to call in outside help.

It is also very important to continue to maintain the Standard Operating Procedures. The NOC must continue to define and refine the searching capabilities of the internal NOC website. The documentation is currently kept in both static and dynamic documents. The dynamic documents are pulled from Oracle databases as they are needed for relevant documentation. Having all documentation in a dynamic format will make it easier for Administrators to find needed information during virus outbreaks, DoS Attacks or other stressful, high impact events.

As with any organization, there is always room for improvement. Management within this organization has always been open to new ideas and ways for improving how the NOC does business. Open minds and flexible management are perhaps the foundation to an effective and thorough NOC.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

List of References:

1. Cole, Eric, Fossen, Jason, Norcutt, Stephen, and Hal Pomeranz SANS Security Essentials with CISSP CBK The SANS Institute April, 2003, p. 259

2. Bless, Terje Cricket Home. 21 Apr. 2003. Sourgeforce. 12 Jun. 2004. <http://cricket.sourceforge.net/>

3. Keller, Joni Spectrum Basics. 28 Nov. 2000. 14 Jun. 2004. <http://www.unc.edu/~hope/help/spectrum/basic.html>

4. Caswell, Brian What is Snort? 16 Jun. 2004 Snort: The Open Source Network Intrusion Detection System 13 Jun. 2004. <http://www.snort.org/about.html>

5. Intermapper Networking Monitoring and Alerting. 1 Jun. 2004. Dartware, LLC. <http://www.intermapper.com>

6. Shaw, Jake Security Pays Off as Hack Attacks Decline. 11 Jun. 2004. Newsfactor.com. 13 Jun. 2004 < http://www.newsfactor.com/story.xhtml?story_title=Security-Pays-Off-as-Hack-Attacks-Decline&story_id=24839&category=netsecurity>

7. Cisco Systems Internetworking Technologies Handbook, Third Edition Cisco Press February, 2001 pg. 394

8. Cole, Eric, Fossen, Jason, Norcutt, Stephen, and Hal Pomeranz SANS Security Essentials with CISSP CBK The SANS Institute April, 2003, p. 260

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Last Updated: May 22nd, 2013

Upcoming SANS Training

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

SANS Malaysia @ MCMC 2013	**Cyberjaya, MY**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
SANS Pen Test Berlin 2013	**Berlin, DE**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
Industial Control Systems Security Training - Houston	**Houston, TXUS**	**Jun 10, 2013 - Jun 15, 2013**	**Live Event**
Security Impact of IPv6 Summit 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 16, 2013**	**Live Event**
SANSFIRE 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 22, 2013**	**Live Event**
SANS Canberra 2013	**Canberra, AU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
Mobile Device Security Summit 2013	**OnlineCAUS**	**May 30, 2013 - Jun 06, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**