Global Information Assurance Certification Paper

Functioning of Managed Security Services

Written by : Mohamed Sabah Mohamed
Program : GIAC - GSEC
Email : Mohamed.Sabah@DataFort.net
Date : 30-7-2002

Table of Contents

I Introduction

One of the hottest topics in the Information security industry now is the Managed Security Services. Everyday, we keep hearing about different organizations proposin g for managed security services, presenter's preparing hundreds of slides on describing the functions, importance and benefits of managed security services. This report is an attempt to highlight the operational workings of a Managed Security Services Providers and thereby help the readers in understanding what is involved in op erating and functioning in Managed Security Centers.

The report includes an introduction on why Managed Security Services, and how to function in Managed Security Services centers, a nd what is the operations and actions which are being currently practiced and implemented in a MSS center in brief.

The report will also demonstrate briefly the operational procedures which are running in an MSS center, like Incident handling, security h /w and s/w fault maintenance, monitoring of security assets, managing the security assets, and reporting. The report will also demonstrate the working of a Managed Security Services Center, explai ning and evaluating MSS processes and procedures in brief.

An introduction on the correlation model and how to integrate all of the security systems in one reporting model and an example of a correlated event will be included also. A basic investigation for the current practices in Incident Handling will also be discussed.

Because running Managed Security Services is a trade secret to many MSS providers, and because it's a new field, it is hard to find more detailed information on running MSS centers and the best practices in functioning the MSS center from the Internet or Books,. It's obvious that this type of information is confidential to many MSS providers and they will never publish their trade secret and their operational procedures and processes for the public. Although to find a full overview on what is a n MSS is very easy process and the resources are many in the Internet

That's why, most of th is report information is based on the experience which I have from my company, and I will be so careful in writing it in order to not expose the full practices whi ch we have in our company's MSS center because of the confidentiality of it and I only will try to have an introductory demonstration to the general and the com mon practices in any MSS center.

II What & why Managed Security Services

Let's have a brief introduction on the meaning of MSS. It is well known that most of the organizations around the world have an IT infrastructure. And most of those organizations have confidential data which is needed to be protected. Some of the organizations deployed some security consulting and having some security solutions like Firewalls, Intrusion detection systems, Antivirus and Virtual Private Networks. Most of these organizations deployed these security solutions and forgot about them. Most of them never monitor the logs or the performance in order to detect any hacking attempt, if it's still happening or happen in the network or to the data and it been never discovered or reported.

Technology alone will not protect organizations from the new threats and vulnerabilities. Firewalls, Intrusion detection systems and other security devices generates huge amount of data which is very hard to analyze and collect. Even the most experienced security engineers struggle to separate critical events from large amount of log data and because of the lack of available resources.

The main role of Managed Security Services is to manage the security devices or software's and monitor them in order to report and detect in a fast time minor any kind of incidents or threats which may appear at any time. The risk is there in from the Internet or from inside the organization, but does anybody go and check for these threats and attempts? The answer is no, why? Because to have dedicated staff where they need to monitor these security devices 24 * 7 is a very expensive solution and needs a lot of operational procedures, resources and budget.

That's why the idea of Managed security services has been represented, it is in order to have a very fast response and detect to any kind of attempt to damage or misuse the data from an internal or external threat . Most of the managed security services centers have a high expensive hardware and software and qualified men power.

Let's list the role and elements of Managed security services centers:

- Fault and Performance Management.

In order to instantly detect any failure, the need to have a 24/7 monitoring with proper alarm notifications like pagers, SMS and SNMP is very critical in a Managed Security services centers to prevent from downtimes and unavailability of services. The fast response and fast fix is very crucial.

- Configuration Management.

In Managed Security services centers, the engineers have the full knowledge in installing or configuring and managing the security assets like IDS's, Firewalls or Access controls. The proper configuration management will

enhance the security architecture and will prevent from unexpected errors or failures.

- Security Reporting Management.

All the operational and security assets logs and alarms will be corr elated in order to detect false positives or attack attempts 24/7. Then a deep analysis for all the logs from the security assets like Firewalls or IDS's will be examined to decide the further action. A detailed report will be prepared to demonstrate the complete activities on the security assets with a full analysis for all the security alerts, incidents, false positives, devices health and even failed services.

- Vulnerability Assessments.

Most of the operating systems, software's and Security assets ha ve vulnerabilities and every day new ones are discovered also. So it is one of the Managed Security Services Centers jobs to detect and analyze all the systems for any kind of vulnerabilities and report and patch or fix them. The vulnerability assessment a re conducted on a schedule basis wither monthly or weekly depend on the customer requirement.

- Anti Virus Management.

Any IT person knows how harm is a virus to a system, and the amount of damage to the system and data. In order to detect and have a fast response to viruses or worms, a proper management should be implemented and a fast response by updating the signatures or rectifying and recovering effected systems, which is strongly needed in a very fast time manner, and it should be by 24*7.

III Running Managed Security Services

1- Operational Procedures & MSS Operator Tasks

In a Managed Security Services Centers, a lot of procedures and operations should be implemented and managed. These procedures are the unique thing about any MSS center. Each p rocedure is a number of technologies and knowledge to detect and prevent from failures and attacks or incidents. During these procedures, the MSS engineers and operators have to do a number of security tasks and procedures. Let's list some of the tasks and procedures which are being conducted in most MSS centers:

- Log Analysis.

It is not enough to let the automatic security systems to detect errors or attacks. It is too important for the security engineer to check frequently the log files and data in orde r to see and discover any kind of incidents. This includes checking firewall syslogs, IDS logs, access control system logs and network performance logs. This procedure will prevent or discover any system from

failures, errors or attacks and it is too important also to differentiate between false positive events.

- Preventive Maintenance.

It is too important in any MSS center to have very frequent maintenance procedures to prevent and detect any kind of hardware or software service error or failure. This procedure will be conducted for all the security devices and servers, like firewalls, IDS's, servers, operating systems, internetworking devices, network & electricity cables and even operational software's. Sometimes without proper scheduled maintenance, a heavy error or failure may not be discovered only after a disaster has been appeared.

- Backup.

This the golden word in any incident or attack. By proper backup and secure storing, any unexpected incident or failure or attack will not have that big damage or loss of data, because all the data and information will be stored and easily restored at any time. The backup procedure is being processed in a schedule phases where it depends on the type of information which is being backed up, it could be daily differential backup or weekly incremental and monthly full.

The backup procedure depends on the type of environment and the type of the data which is needed to be backed up. The MSS Engineer should also be responsible in checking the efficiency of the backup and the availability of it. It is too important also to periodically test to restore the data, just to insure that the process will not be failed once an indent occurred and the backup was unready or failed.

- Reports Generation.

MSS reports are the unique element and the final fruit from all the 24*7 operations and analysis's of all the data and information and the complete efforts of the MSS engineers. Reports are the show case and the only touchable thing which the customer or the management will going to receive.

Depend on the type of the report and the type of the system or customer, the MSS engineer process each report based on the requirements, level, timing and importance of the information and data. The MSS engineer should deliver daily, weekly or immediate reports, based on the situation and the type of information of the report, summary or detailed report or graph to be submitted, and weather to send a soft copy or hard copy or even immediate SMS or pager summary reports.

- Vulnerability Assessments.

One of the most important tasks in the Managed Security Services is the Vulnerability Assessment of all security systems, Operating systems, Internetworking devices, Firewalls, IDS's, servers and even access controls. All the security systems should be assets and analyzed with all the new bugs or vulnerabilities which been discovered everyday.

Through using proper tools for vulnerability assessments, a proper test and report will be generated with all type of threats and vulnerabilities will be submitted. The report should include the description of the threat and vulnerability, the solution to fix the problem and providing total detailed solutions in protecting and preventing the system from any threats and harms.

- New Viruses & Vulnerabilities Advisories.

Because of the fast growth and development in the Information Technology industry, IT people can't full concentrate in protecting their systems while working on developing and updating their systems in a fast time manner. Because most of the IT projects need to be finished very fast, a lot of bugs in the program codes or in the installation activities will be discovered. The managed Security Services centers are a very good environment for discussing security threats and new vulnerabilities beca use of the type of environment which the engineers work in.

One of the MSS engineer's big tasks is to search the net for all the security alerts and news, searching in mailing lists and message boards for any new viruses and Trojans, and instantly, alert ing the IT administrators with the new advisories depending on the type and the criticality of the system they have. Even updating the Intrusion Detection Systems and the Anti Virus systems with the new signatures and update it manually or administrate it automatically which is a very important task. The advisory process should be sent through a hard copy or soft copy through E - mails etc.

2- MSS Correlation

Event correlation is one of the most the new challenging aspects of security and network operation s management. Event correlation is the result of relationships between multiple events for some period of time. These events may be from different systems or applications, and may even be about different types of elements (faults, security, performance, et c.), but when viewed as a set of related events, they pinpoint a particular problem.

Events from multiple sources can be correlated to pinpoint problems. Individual events may not be a problem, but when combined with other events, it will help correlate the root cause of network conditions and initiates the appropriate response. Depending on the systems type which triggers the different kind of events, the correlation system must collect all the events from all the security systems and analyze them, then the MSS Engineer job is to investigate wither an specific attack or incident is being on progress or not.

Let's investigate the architecture of an MSS correlation. First we have the Security systems, where we gather events, logs and information from diff erent kind of systems like Intrusion Detection Systems logs, Fire walls syslogs, system events, access control events and network management monitoring events like HP Open View for example. Then the second step is to collect all these data and send it in o ne centralized location where a proper data collection and backup will be conducted. This Centralized event database will

contain all the information and data from all security systems and from different kind of customers and parse it for the third analyse s step.

Then once the centralized event collector is ready, a further deep analyses and investigation will be implemented in order to detect and understand all the type of events and have more certain conclusions about what is happening and if there is an incident in progress and it is not been discovered without the combination and correlation of all the events and data. Once the analysis phase is finished, further actions are being conducted, let's investigate them:

- Reporting.

Depends on the organiza tion or customer requirements, further reports is being processed and submitted. The reports will demonstrate all the type of information which is been analyzed and the further results and conclusions which is been discovered. Then different kind of report s is being presented, hard copies, electronic mails or soft copies and they can be submitted daily, weekly or even immediately where it will contain detailed information for the steps and actions to be initiated and the recommendations to protect from futu re incidents and rectify them.

- SMS notifications.

In order to have a fast response to any type of incidents, a further fast SMS messages or Pagering can be triggered and sanded.

- Web.

Even a soft copy if the reports or a more information of an inci dent or an even can be submitted in a secure web page or even through using WAP.

MSS Operational & Correlation software's

Every day a new technology arrives and makes the life easier. Even in managed Security Services Centers. A lot of new technologies h ave been implemented in order to help the engineers developing and submitting efficient and professional reports and investigations. These new technologies automate what the normal MSS engineer used to do manually and they provide fast and very reliable re sults. In most MSS centers, a lot of operational software's is being used, like for example:

-HP Open view ® and Big Brother and Galileo ® for system and network fault & performance monitoring.
-Net Forensics ®, Web Trends ®, Private I Nvision ® or E -Security® for the analysis and correlation of different system and security logs of different security devices, like different kind of firewalls and Intrusion detection Systems.

These tools and operational software's will collect all the logs and security information from different kind of systems and correlate them in order to detect any error or a hacking attempt. Then it will trigger a security incident which will be triggered to the notification systems for further actions.

An Example of a correlated event

Let's go through an incident example which can't be detected without correlating between the multiple security systems events and logs:
On the 5-8-2002 at 4:30 AM, the Host based IDS on the corporate public web server for the corporate domain name whi ch is http://www.SomeWebSite.com alerted us that an IP address of XX.113.12.54 was trying to send some suspicious HTTP traffic to it. So, The MSS engineer s analyzed the traffic and they discovered that the type of the IDS signature which the Host based ID S alerted was HTTP IIS Unicode. The corporate Web server is running MS IIS, so the alert wasn't a false positive.

So in order to have more analysis and information on the situation, an investigation of the Router gateway and the firewall syslogs and the Network based IDS for the web server's network is needed to be conducted. By checking the firewall logs, the MSS engineer discovered that the source IP address of the attacker which is XX.113.12.54 has been logged in the firewall. The same IP address appear ed many times on the firewall and it was only been permitted for the HTTP traffic which is allowed in the firewall to the web server.

But, there were a lot of denies from this IP address traffic to the internal web server behind the firewall , the attacker was trying to connect to multiple ports and services to the web server IP address at the same time and the firewall blocked him because it only allows PORT 80 to the web server IP address. By going to the main Router which routes all the traffic from th e internet to the firewall, and by filtering all the logs for the attacker IP address, the MSS engineer discovered that the attacker IP address was logged many times where he was trying to connect to many IP addresses behind the router.

Finally, through analyzing the web server's HOST IDS events, and the firewall logs which protects the web server and public gateway router, the MSS engineers discovered that the same attacker IP address was trying to connect to many IP addresses behind the firewall and tryi ng to send a lot of suspicious traffic which been also detected on the Network Based IDS on the firewall outside's subnet from the same attacker IP address and at the same time. So the engineers concluded that the attack was planned and the motive was their from the IP address owner to attack the protected corporate systems. And the incident was reported for further actions.

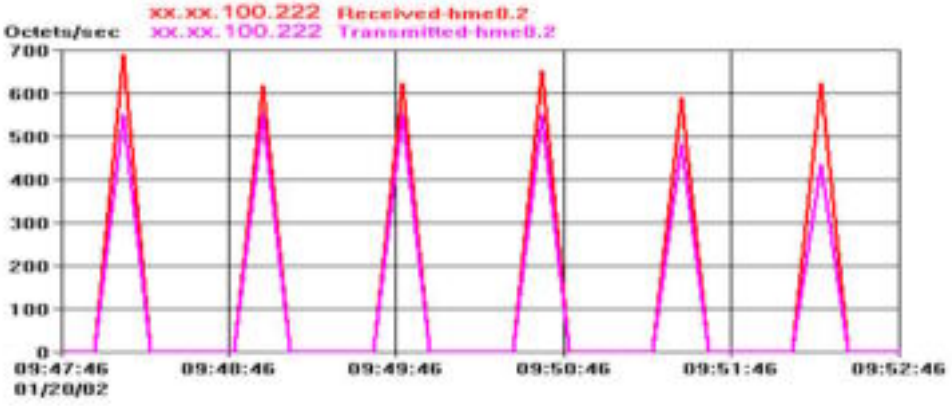
IV MSS processes

1- Fault & performance & security monitoring & management of security assets

We had already talked about the fault & performance & security management in Managed security Services earlier in this report. This section will go through some sample graphs and reports which been prepared personally by me through Private I ® From Open Systems http://www.opensystems.com/ and

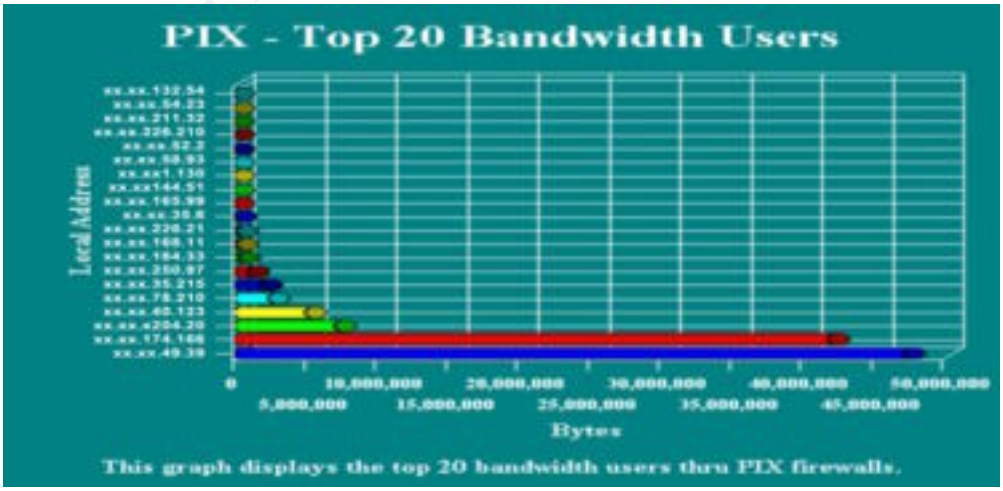
took the Cisco PIX ® firewall as an example and Snort Snarf from http://www.silicondefense.com/software/snortsnarf/ and took the Snort IDS as an example and Galileo ® from NetVion http://www.netvion.com/pages/3rd_level/galileo_main.html and took the PIX firewall as an example. These Graphs describes the performance and the status of the security services with some brief description of each sample with mentioning the MSS engineer security advisory, analyses and recommendations.

- Received and Transmitted packets in a network interface



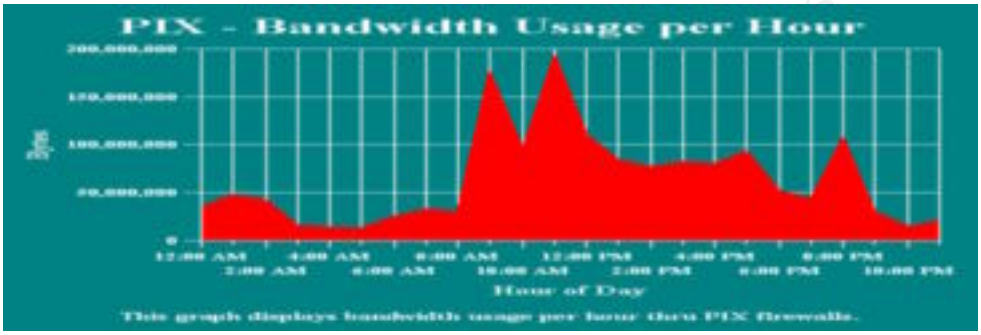
This graph which been prepared by me through Galileo ® from NetVion by collecting the SNMP traps from a Cisco PIX ® firewall through HP Open View ® demonstrates the number of packets being received and transmitted per second via interface 1 of the firewall between 9:47am and 9:52am. By analyzing the graph, we can see that the maximum number of packets received per second is about 700 and number of packets transmitted is about 550. The graph shows us that the load on the interface is very low and there is still plenty of room for growth and everything is normal on the firewall security system.

-Top Bandwidth users



As we can see here from the graph which been prepared by me through Private I ® from Open Systems , the number of the IP addresses which accessing the department services are fe w, but we notice that there are two IP addresses where they have a very high access in the department comparing to the other IP addresses. The need to investigate these IP addresses, what they are and for what they are using the bandwidth so heavily. These two IP addresses maybe scanning the network or flooding it with packets or trying to do a Denial of service attack.

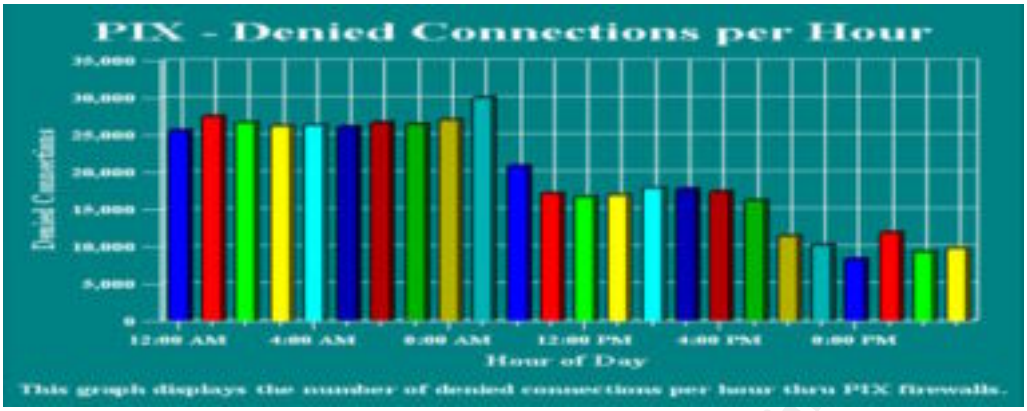
- Bandwidth Usage per hour



This graph been prepared by me through Private I ® from Open Systems from the PIX firewall syslogs. By calculating the number of bytes which had been used by each department, and comparing them between different timing of a day, we will be able to know the peak and non peak times of the network in a day. As we can see, starting from the early morning in the us ual working hours from 8 Am, we can see that the f/W reported that the usage of the network was very high, more than 200 Mb's of bandwidth which is very normal.

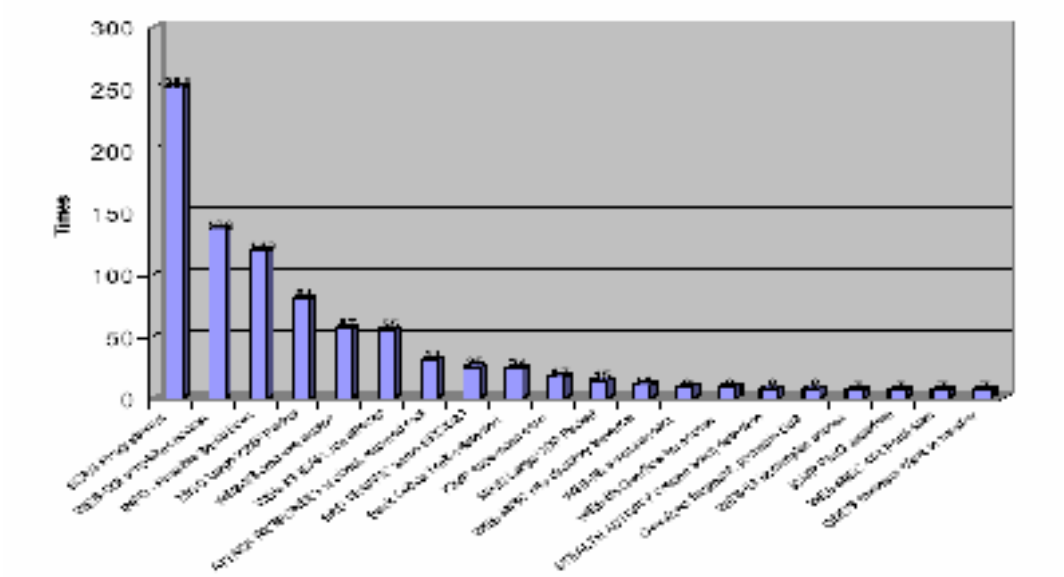
Then it started to decrease after lunch hours from 1 Am down to 4 PM which is very normal als o. The usage of the network bandwidth is limited after working hours and it is stable comparing with the full time working hours. At 8 Pm , after working hours, we discover that somebody was using the network very heavily, which mean that a suspected user is trying to maybe scan the network or flood the network with high traffic, because it is impossible to see people working in these hours of a day.

-Denied Connection per hour



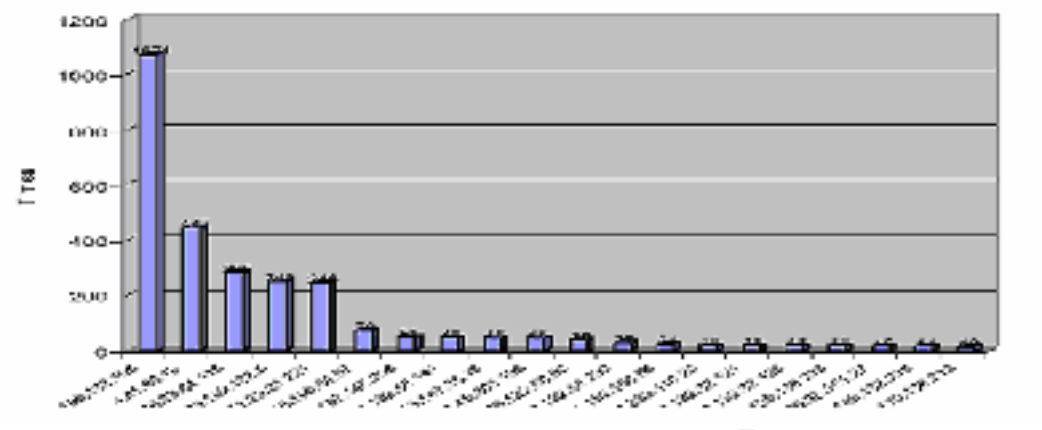
From this graph which been prepared by me through Private I ® from Open Systems, we notice that the number of denied connections is variable and it's somehow not stable. An attack started in the off time working hours, which starts from 12 AM, then reduced from 8 AM. The need to investigate the IP addresses and the denied connectio ns are very important in order to check wither it is a false positive or a miss configuration in a specific system in the network which sends a huge packets and it being denied by the f/w.

- Top alerts of the week



The graph which been prepared by me thr ough Snort Snarf tool and prepared by MS Excel ®, it shows the top 20 attacks of the week from an Intrusion detection System. Some of these attacks could be false positives and some are not. Due to the high number of new worms and viruses which is spread now days, a high number of Web attacks were being reported. This could be due to some well known vulnerabilities in widely used web servers and easily available tools to exploit them. The security system admin could use this graph as a reference to check wh ich attacks are more common and take appropriate action.

- Top 20 attackers.



The graph which been prepared by me through Snort Snarf tool and prepared by MS Excel®, shows the top 20 attackers of the week from the Intrusion Detection System. This graph identifies to us the top attackers IP addresses. It is also no surprise that some of the insiders have been identified in the top 20 attackers. It is recommended that these insiders are also closely monitored and all their activities are logged. Specially the IP address with the high number of attack times, it needs a special monitoring, and to check what exactly this IP address is doing and wither it is a false positive or not.

2- Incident handling

Incident handling is one of the unique procedures in M anaged Security Services centers. Since the MSS center is running 24*7, the MSS Engineers should be well know ledged and they must have good knowledge on incident handling and should follow a proper methodology to do so. With proper incident handling, most of the dangerous incidents can be controlled and recovered. Depends on the MSS center and the type of security systems and environments, the Incident handling procedures will differ, but usually the difference is not that big.

Because most of the MSS organizations have their own developed Incident handling procedures from the standard incident handling procedures, they will keep what they developed as a confidential standard, and they will not present it for the public. That's why in this report we will demonstrate the SANS Incident Handling consensus guide [1] as an example of the most common procedures in the incident handling world. So, we will go through the SANS incident handling steps and actions which should be taken during or when an incident hap pens.

- Remaining Calm.

Remaining calm and controlling one self and thinking very wisely and deeply without rushed judgments or fast decisions and conclusions will give a very big amount of confidence and understanding of a situation or incident. It is very important to handle hard situations and incidents with patience and

without panicking or confusing. Proper judgment and proper analysis should be conducted with clearly and unrushed thinking to prevent any mistakes or unwanted accidents to occur.

- Taking Good Notes.

Through proper management and control of any incident by writing all the notes and all the detailed and discovered elements, proper conclusions will be clear to be executed. The Managed Security Services engineers should have a special Incident forms in order to report any incident in a proper way and to document it for future needs and analysis.

-Notifying the right people.

Some incidents are so complicated where the need for specialist's analysis to a particular incident is heavily requir ed. The expert can very easily differ between incidents and false positives. That's why when an MSS engineer faces new or a big incident, it is very important that he involves his team and the experts into it to have their opinions and recommendations. It is also so important to notify the administrator of the system which has the incident. The incident should also be escalated to the high management if it didn't been resolved or took long time.

-Enforce a Need-to-know Policy

Depending on the type of the i ncident, there are some very confidential incidents and the number of people which required to know about it should be minimum. Some incidents are so confidential were if it's been leaked out, it may effect badly on the reputation of the company. That's wh y confidentiality is a very important manner during incidents.

-Use Out-of-Band Communications

There are some complicated incidents where the confidentiality and the integrity of it are very critical. For example, some attackers when they hack into the systems, and while the system administrators are working in solving the problems and communicating with each other through emails, the hacker can see and watch what they are doing, therefore he will plan some other actions in protecting his identity or stayi ng on attacking the systems without the knowledge of the administrators.

In the occurrence of incidents or attacks, it is very important to keep the incident very low profile and not leaking out any information or the situation's information to any body, just for the proper people. Even the communication should be through Fax's or SMS's or telephones only with carefulness.

-Containing the problem.

Surrounding the problem and controlling it from spreading out is very important. Once an incident has been discovered in one of the systems, this system should be excluded from the entire systems. For example, if we have a PC which has been infected with a dangerous virus, this system has to be excluded from the network in order to protect other systems from th e virus

and from spreading on to other critical servers and PCs, so we will contain the problem in a fewer number of PCs in order have an easy recovery procedures.

-Making Backups.

As discussed earlier in this report, backup is very important and crucial in incidents situations. Without a proper ready backup after the incident, the value and the loss of data or information will be very high and may harm the organization very badly. Once an incident or attack has been discovered in one of the security systems, it is very important to exclude the system from the network and get new media and back it up immediately and store the backup in a secure place for further analysis and computer forensics or for data recovery.

-Getting rid of the problem.

In order to achieve this, the identification, investigation and full analysis of the problem should be established. These processes well prevent and protect the system from any future attempts, and will explain how and when exactly the incident or attack happen and how to recover the problem or destroy it.

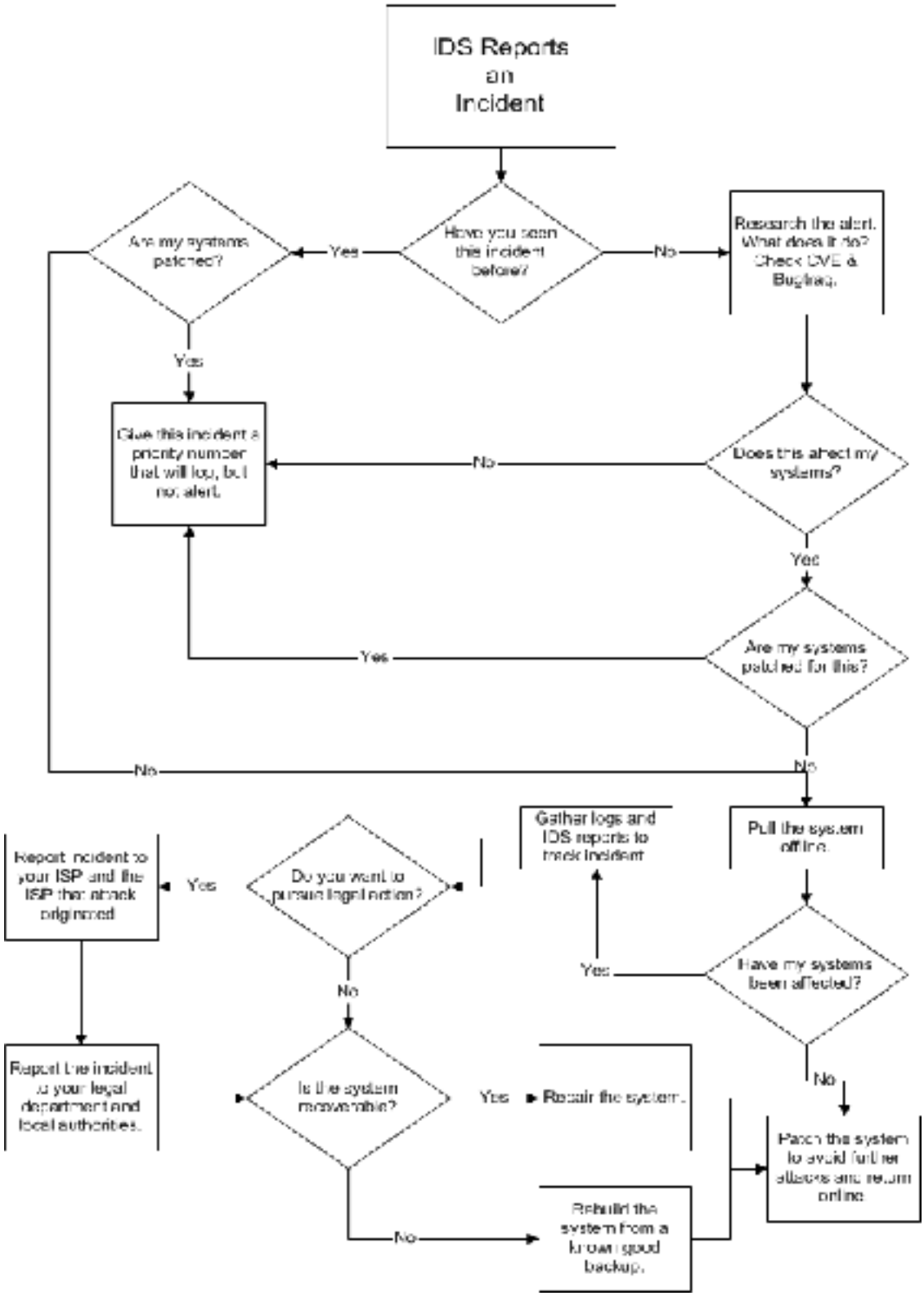
-Getting back in business

Getting back in business involves returning or recovering affected systems from attacks or hacking incidents. Recovering the systems through restoring the backed up data with the assurance of the safety of the restored data from any infected or corrupted data is a very important step. Once the 100% assurance that the new restored data are safe to be restored, and the successful recovering procedure has been conducted, a further deep monitoring should be conducted for the infected system.

Putting an eye on the restored system and monitoring it continuously will prevent the system from further continuously attack and protect it from future incidents also. This procedure is very critical where returning an infected or corrupted system to the same network or environment may affect all the uninfected systems badly if the attack has been triggered again from an external or internal system, or person.

-Here is an example of other useful Incident handling procedures which been prepared by Dante Mercurio <dmercurio@ccgsecurity.com> and been published on the Symantec Security Focus web site on Jun 17 2002 URL: http://online.securityfocus.com/archive/96/277239. This flowchart just demonstrates other methodologies in Incident handling procedures, this flow chart is not an standard in Incident handling, but it is just been added to be as an example although the methodologies and actions are littlie different than the SANS Incident Handling methodology which is been presented in this report:

IDS Incident Flowchart



V Resources & References

1- SANS - Computer Security Incident Handling: Step -by-Step
URL: http://www.sans.org/newlook/publications/incident_handling.htm (4-7-2002)

2- Counter Pane - Managed Security Monitoring: Network Secur ity for the 21st Century
URL: http://www.counterpane.com/msm.html (5-5-2002)

3- Guardent – Managed Security Services Overview
URL: http://www.guardent.com/mss_overview.html (5-5-2002)

4- SANS Information Security Reading Room - Managed Room
URL: http://rr.sans.org/managed/managed_list.php (20-5-2002)

5- Data Fort - Managed Security Services
URL: http://www.datafort.net/mss.php (20-5-2002)

6- 1-Net - Managed Security Services Frequently Asked Questions
URL: http://www.1-net.com.sg/0231securityFAQ.htm (10-5-2002)

7- CERT - Responding to Intrusions
URL: http://www.cert.org/security-improvement/modules/m06.html (12-6-2002)

8- Network Intelligence- Envision – Private I software
URL: http://www.opensystems.com/ENT_products/Software/ (2-7-2002)

9- Net Forensics- Software Solutions to Secure the Enterprise
URL : http://www.netforensics.com/products.html

10- The Secure Solution
URL: http://www.pwcglobal.com/extweb/manissue.nsf/DocID/0B6E4A47A89C257C85256BC0006DBC91 (26-6-2002)

11- RFC 1244 - Incident Handling
URL: http://www.net.ohio-state.edu/rfc1244/incident.html (4-7-2002)

(22-6-2002)

12 - Intelligent Distributed Fault and Performance Management for Communication Networks
URL: http://www.isr.umd.edu/TechReports/CSHCN/2002/CSHCN_PhD_2002_-2/CSHCN_PhD_2002-2.phtml (24-6-2002)

13- IDS Incident Flowchart . By Dante Mercurio <dmercurio@ccgsecurity.com :
URL : http://online.securityfocus.com/archive/96/277239 (20-7-2002)