Hierarchical Task Analysis of Intrusion Detection Systems

By
Shibu Bashir

A Research Paper submitted to the Faculty of Computer Science
In partial fulfillment of the requirements for the degree of
Masters of Electronic Commerce

Supervisor
Dr. James Blustein

Dalhousie University
Halifax, Nova Scotia 2004

Table of Contents

* Diagrams are also attached (as TIFF files) to the PDF file.

1. INTRODUCTION

It is apparent that information technology is the backbone of many organizations, small or big. Since they depend on information technology to drive their business forward, issues regarding network security have become a high priority. Companies use technologies such as e-mail, web services, databases, applications, etc. – accessed via a network - on a day to day basis to perform various organizational functions and duties.

The task of protecting a company's network falls on a single or group of persons called Network Security Administrators. They use a wide variety of tools and procedures to keep the company network secure. One major classification of tools used are Intrusion Detection Systems or IDS. IDSs are capable of monitoring network traffic and system usage for anomalies (activities that are not part of the norm).

The aim of our study is to perform a hierarchical task analysis of functions carried out by a typical Network Security Administrator in a small to medium sized company. Hierarchical task analysis is the detailed description of a job or function from top to bottom. By performing this study, we are able to design better user interfaces for applications used for intrusion detection. Current practices involve using a variety of text based tools and utilities, monitoring log files, etc., all of which may be time consuming, monotonous, and error prone. A better user interface for the IDS would allow the Administrators to be more efficient and productive in their job and reduce the probability of error.

2. INTRUDER DETECTION SYSTEMS

Intruder Detection is the process of detecting inappropriate or harmful activities in a network infrastructure. Intruders to a network can be external, or from within the organization. Recent studies conducted by the FBI and Computer Security Institute have found that more than 81% of intrusions have been committed from within the organization [1]. While organizations are more guarded against attacks from outside, they often neglect the danger within; damage done by inside intruders has the potential to be more severe. Therefore, while protection from outside intruders using securities like firewalls would be strong, inside network may be left vulnerable to attacks from an insider. The use of an Intrusion Detection System can help track down internal hackers, monitor them, and catch them in the act.

2.1 Types of Intruder Detection Systems

There are three major types of Intruder Detection Systems. They are:

- Host based Intrusion Detection System.
- Network based Intrusion Detection System.
- Hybrid based Intrusion Detection System.

2.1.1 Host based intruder detection systems

This IDS entails monitoring servers, application software, database servers, and so on. Monitoring is usually done by examining log files for unusual activities, and analyzing system processes, hard disk usage and critical system files such as password, network and server configuration files.

Host based IDS can be signature based or anomaly-based.

Signature based tools monitor well known signature and patterns of worms and scripts. *Signatures* are well known sequence of string or combinations of packet headers that match a known network attack. Such tools have to be kept periodically updated to new and evolving patterns.

Anomaly based ID systems, such as *tripwire*, use well known facts about the system such as timestamp, size of key system files, etc. This system will notice when an important file has changed and will alert the administrator if the change was unauthorized.

2.1.2 Network based Intrusion Detection systems

A network based Intruder Detection system monitors the network traffic for well known patterns generated by intruders. This is done by placing a network sensor to capture all traffic that flows through the network segment. A sensor can be a network device that does not alter network traffic, thus remaining invisible to the network, but at the same time reading all the traffic and analyzing packets for interesting patterns that match known signatures [2]. Network based IDS can also monitor ports for suspicious connections and watch for well known port attacks.

For example, a Unix command string such as *"rm -rf /"* can potentially delete a complete Unix file system or *echo "++" >$HOME /.rhosts* can allow any user from any host to log into the system without requiring a password. When a network based IDS senses such a sequence of string, it can take defensive action. For instance, the IDS can block out the intruder, or alert a security administrator. Some examples of network based Intrusion Detection systems are *AXENT (www.axent.com), ISS (www.iss.net) and CyberSpace*. A popular open source network based ID system is *snort (www.snort.org)*. *Snort* works both on Windows and Unix platforms. It comes with a set of rules that can trigger actions, and also allow customized rules.

2.1.3 Hybrid based Intrusion Detection Systems

Both Network and Host based IDS have their own unique advantages and disadvantages. Network based IDS are easier to deploy and are less expensive to purchase and maintain. However, their performance depends on known security exploits and signatures. If a new exploit is used that the IDS is unaware of, the system could easily fail to detect the attack. A host based IDS is only as good as the security administrator who maintains and monitors it. Becoming skilled at, maintaining and monitoring this software can be a daunting task. Therefore, the best approach is to use a combination of the best features of Network based and Host based IDS to improve resistance to attacks and to provide greater flexibility. This approach is commonly referred to as Hybrid IDS.

2.2 Types of network attacks

Some well known types of network attacks are listed below.

i. *Denial of Service or DOS attacks* attempts to deny an authorized user from using the system for productive use [3]. For example, sending a TCP SYNN packet which is constructed with the same source and destination IP addresses. This can potentially lock up the system and will have to be rebooted. Another common DOS attack, called the *Ping O' Death* attack, sends a ping request with an abnormally longer payload (over 64K bytes). This can cause a buffer overflow in older operating systems and can possibly lockup or reboot the machine [3].

ii. *IP address spoofing* is a method of constructing or spoofing IP packets so they appear to be from a trusted or known host. An intruder could gain access to internal servers by pretending to the server that the network traffic from the intruder is from a trusted system [10].

iii. *Sniffer attack* is carried out by using special applications that can read network traffic and extract interesting information such as passwords, credit card numbers or other sensitive data. Encrypting network data using digital signatures can prevent sniffer attack [10].

For an intrusion detection system to be effective, it should meet several basic characteristics. Some of the basic characteristics of a good Intrusion Detection System include the following.

- It must be able to protect itself from intrusion by monitoring itself. An intrusion detection system is of no use, if it can be compromised by an intruder.
- It should not make a big impact on the performance of the network or the hosts it is monitoring.
- It should be able to monitor the network for deviations from normal behavior or normal usage of a computing resource.
- It should be customizable for different types of organizations. For example, a university will need a different network security level than a bank. A bank requires a network policy that would make the network very secure to minimize threats to its application and minimize uptime. Universities will have a huge number of workstations in their network and students would require a more open network system, but at the same time protect important applications and databases.
- It should be rule based so an administrator can add or change rules which will allow enhancing the system to counter new security threats.
- If it's a network based IDS, it should be able to keep itself updated with the latest patterns of attack. This can be done by downloading and applying new rules automatically from trusted sources.

3. HIERARCHICAL TASK ANALYSIS

Hierarchical task analysis is the detailed description of a job or function from top to bottom. This is done by decomposing each step required to complete the job into greater detail. It shows the hierarchical relationships between the tasks and provides an in-depth understanding on how a job or function is carried out.

Our aim in this study is to perform a hierarchical task analysis on the use of various intrusion detection software used by a network security administrator. By studying the various tasks associated to the function of a network security administrator, we will be able to design an effective user interface for intrusion detection systems. A well designed user interface would allow administrators to meet their goals faster and more effectively.

The hierarchical task analysis were developed using the following steps:

- Observing the use of intrusion detection systems in a medium sized organization.
- Studying commonly used intrusion detection techniques in the industry.
- Interviewing network security specialists.

Seven major tasks were identified in securing the network in an organization. These tasks are explained in detail in their respective task descriptions. The seven major tasks are [4]:

1 Developing Security Policy
2 Selecting an Intrusion Detection System
3 Hardening and Secure Network and Servers
4 Preparing for Intrusion Detection
5 Detecting Intrusion
6 Responding to Intrusion
7 Improvement

3.1 Network Security Administrator

The *Network Security Administrator* is an individual or a group of people within an organization who are responsible for securing the network, servers, workstations, data and other IT related assets in the organization. An intrusion detection system can only be useful when proper precautions are taken to lock down the network, and by having network administrators who are vigilant, alert, and knowledgeable about the system and about users of the system. This can be compared to having a security system in your home but forgetting to lock the windows and doors at night and when away from home or having alarm signals that are not acted upon. It is also important for the organization to have a detailed security policy.

3.2 Functions of Network Security Administrator:

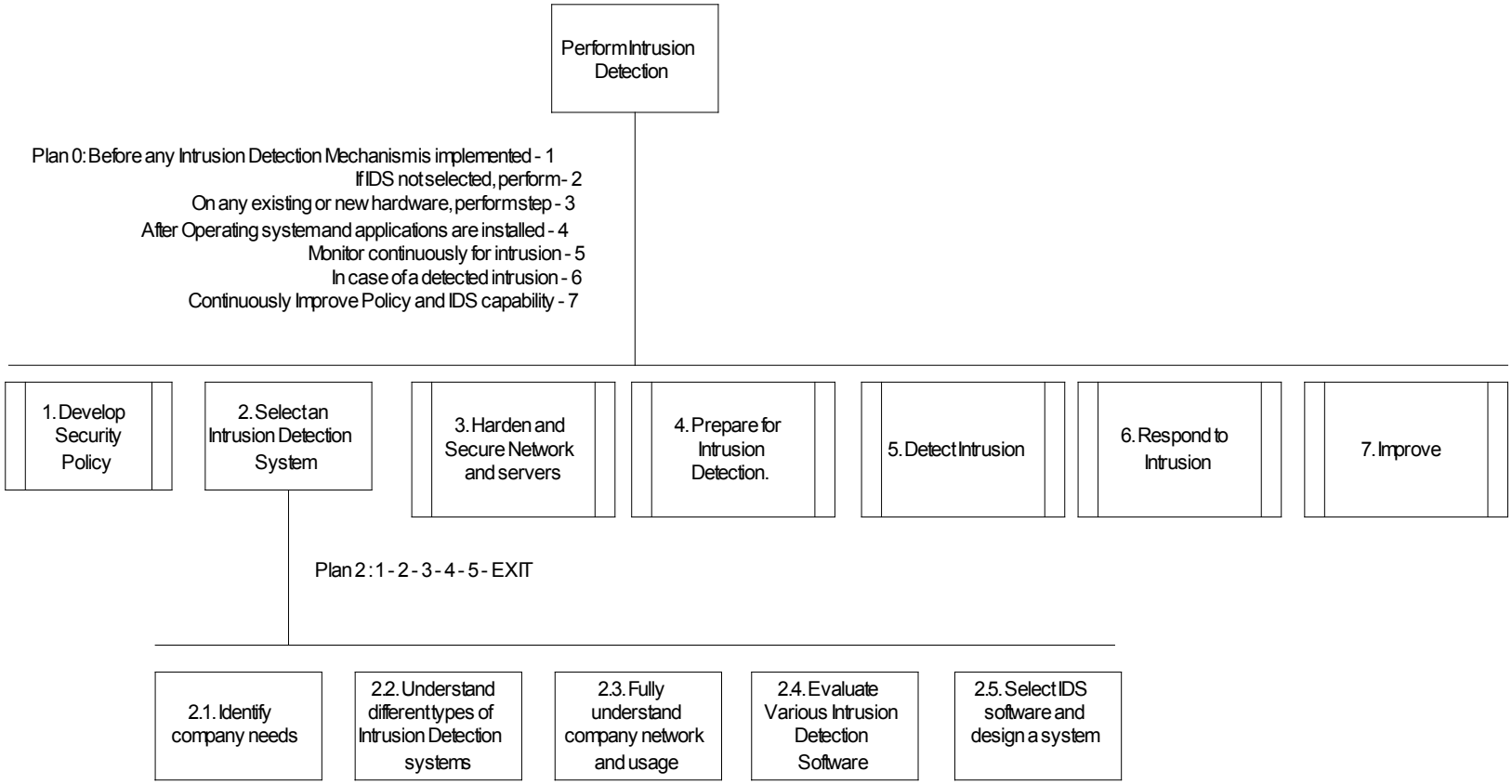
Some functions of a network security administrator or group of administrators are listed below.

- Develop, maintain and implement an IT security policy for the organization. Educate the management and stakeholders about the need to abide by the policies. Train, and get feedback from the users of the infrastructure.
- Implement and maintain a firewall that keeps unwanted traffic out of the network.
- Monitor the network and servers for unusual activity. This is done by auditing important logs in servers, workstations and routers. Special tools can be used to automate monitoring logs. For example, *"Logwatch"* is a popular log utility that produces customized reports of several important log files.
- Monitor critical system files. Tools like *"tripwire"* help system administrators keep check on the integrity of critical system files. Some examples of files that need to be monitored on a regular basis are password files, database and web server configuration files, private keys of servers, binary files of the operating system such as kernel etc. Intruders also try to replace critical binaries and install back door *Trojan horse*. A *Trojan horse* is a program that pretends to be a useful application, but is really is a destructive process that could allow an intruder

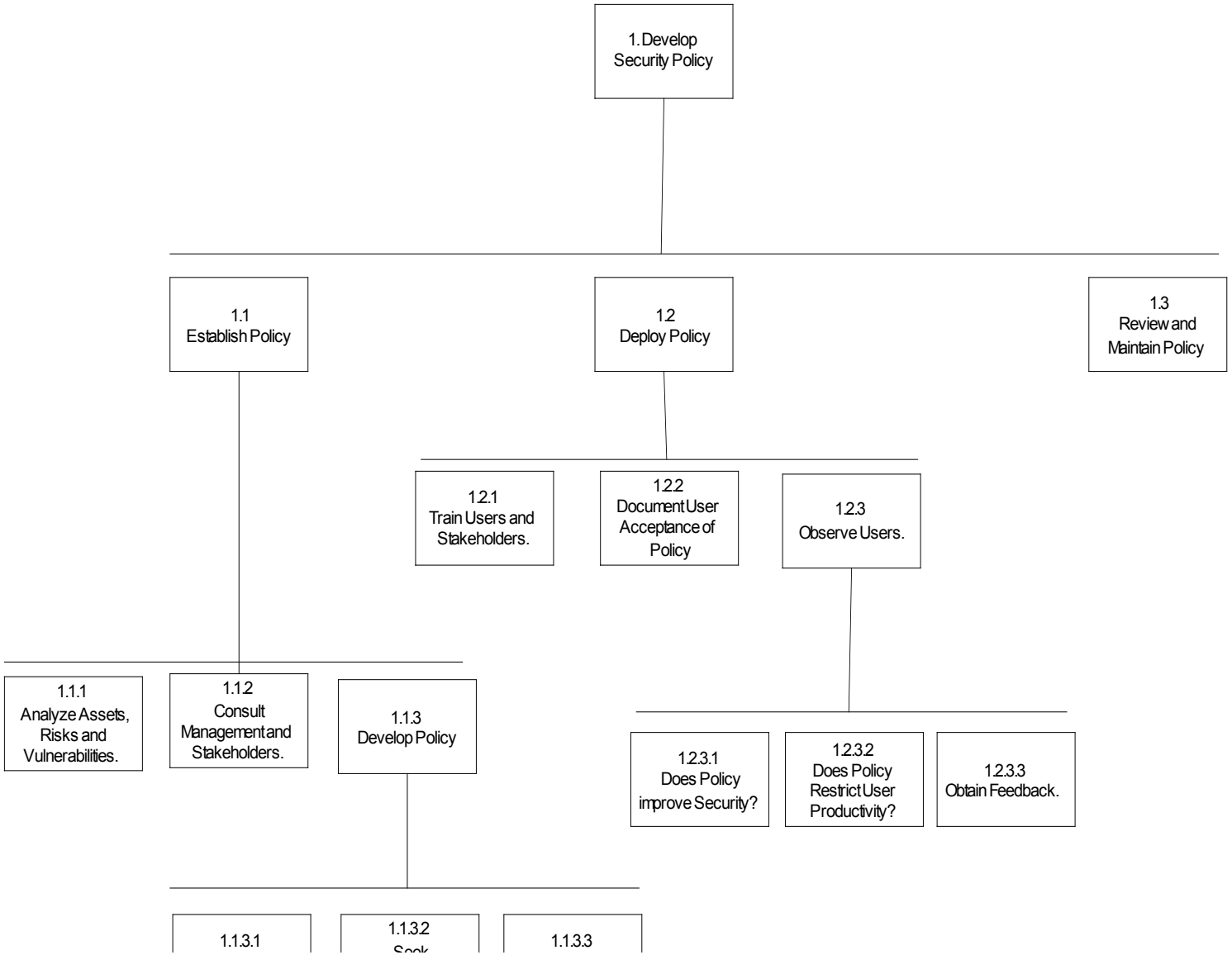
access to the system, or create harm to the system. An example could be a free anti virus software from an unknown web site that could actually be a program tainted with a virus that would cause damage to the system.

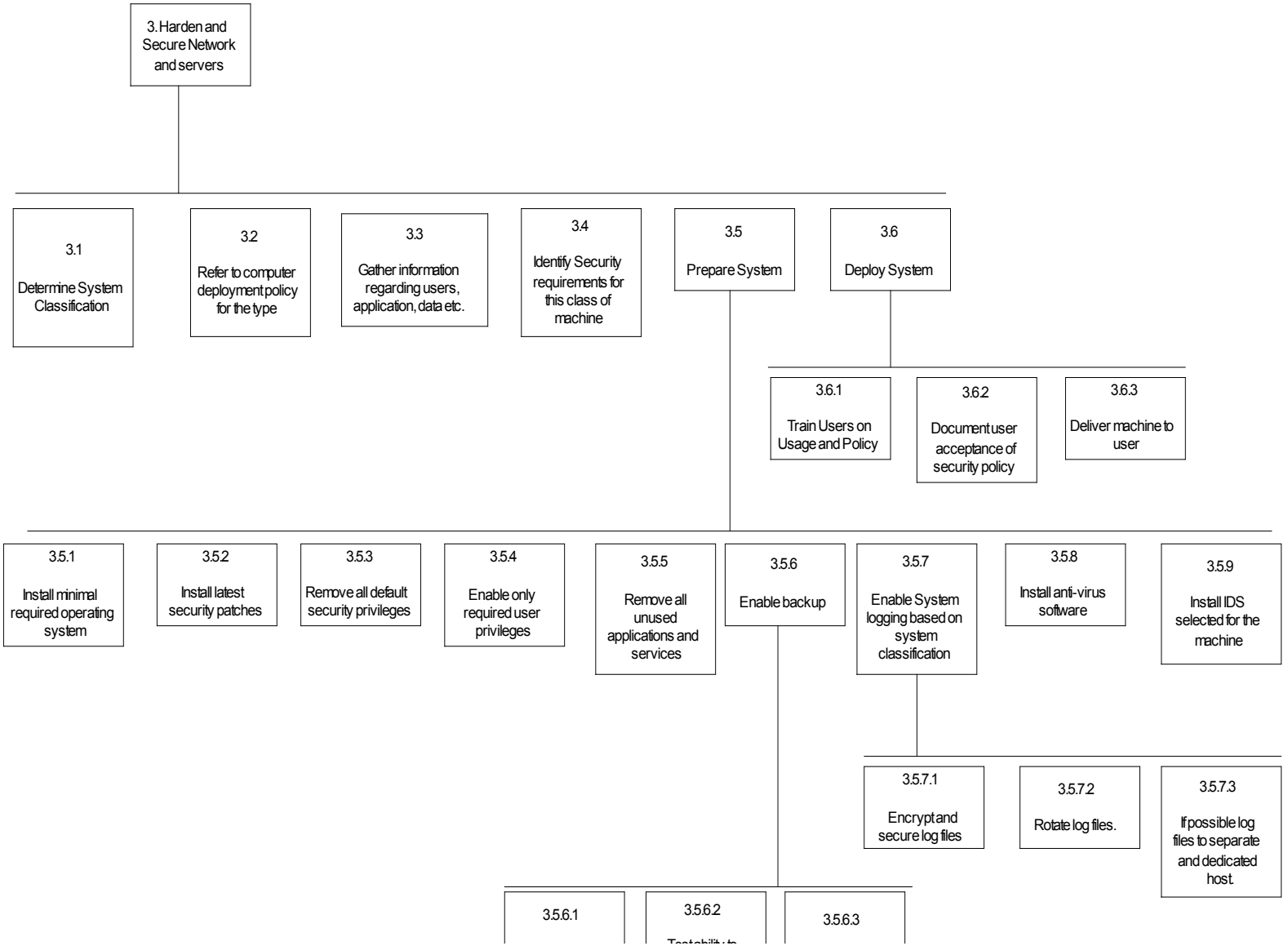
- Backups are an important part of a secure network. In the event that a server was compromised, the administrator should be able to restore the server from secure backups with minimal downtime, and loss of data. Tools like *tripwire* can take a complete snapshot of the system in a secure state. The administrators need to check daily backups, and make sure that the media is stored in a safe place.
- Network forensics will enable the administrator to find out exactly what damages are made to a system in the event of an intrusion. For example, consider that there are many servers running database, web and application servers. If an intruder broke into the one of the systems, the administrator should be able to quickly determine exactly which systems were compromised before more damage is done. In most cases, the whole network cannot be brought down to contain the situation. Forensics can help in isolating the intrusion and help contain such situations. This method will also halt an intruder before they do further damage.
- Secure servers and workstations by removing default operating system privileges, unused open ports, and so on. By limiting functionality to what is really needed by the user, the risk of compromise is reduced.

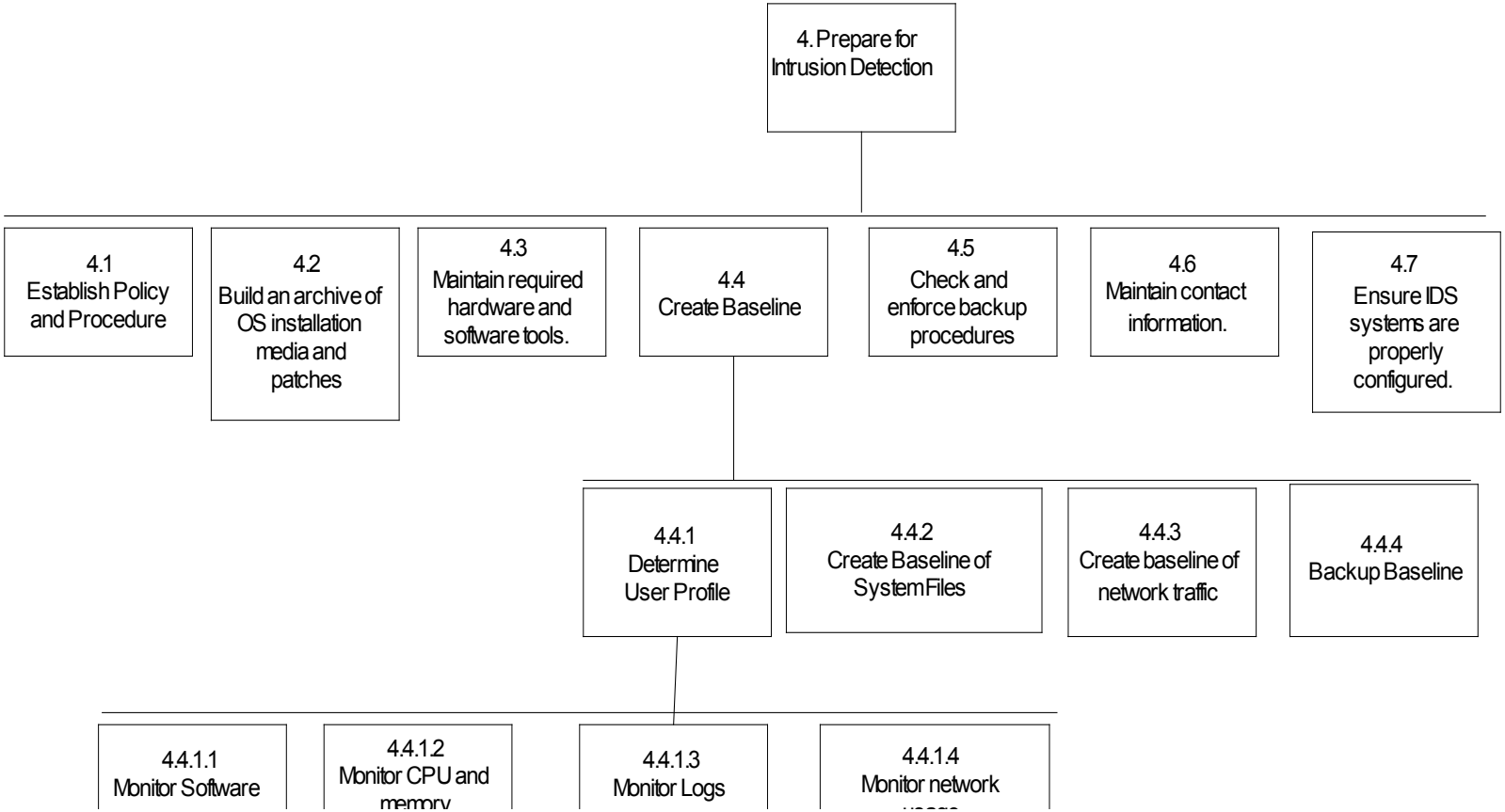
4. DIAGRAMS

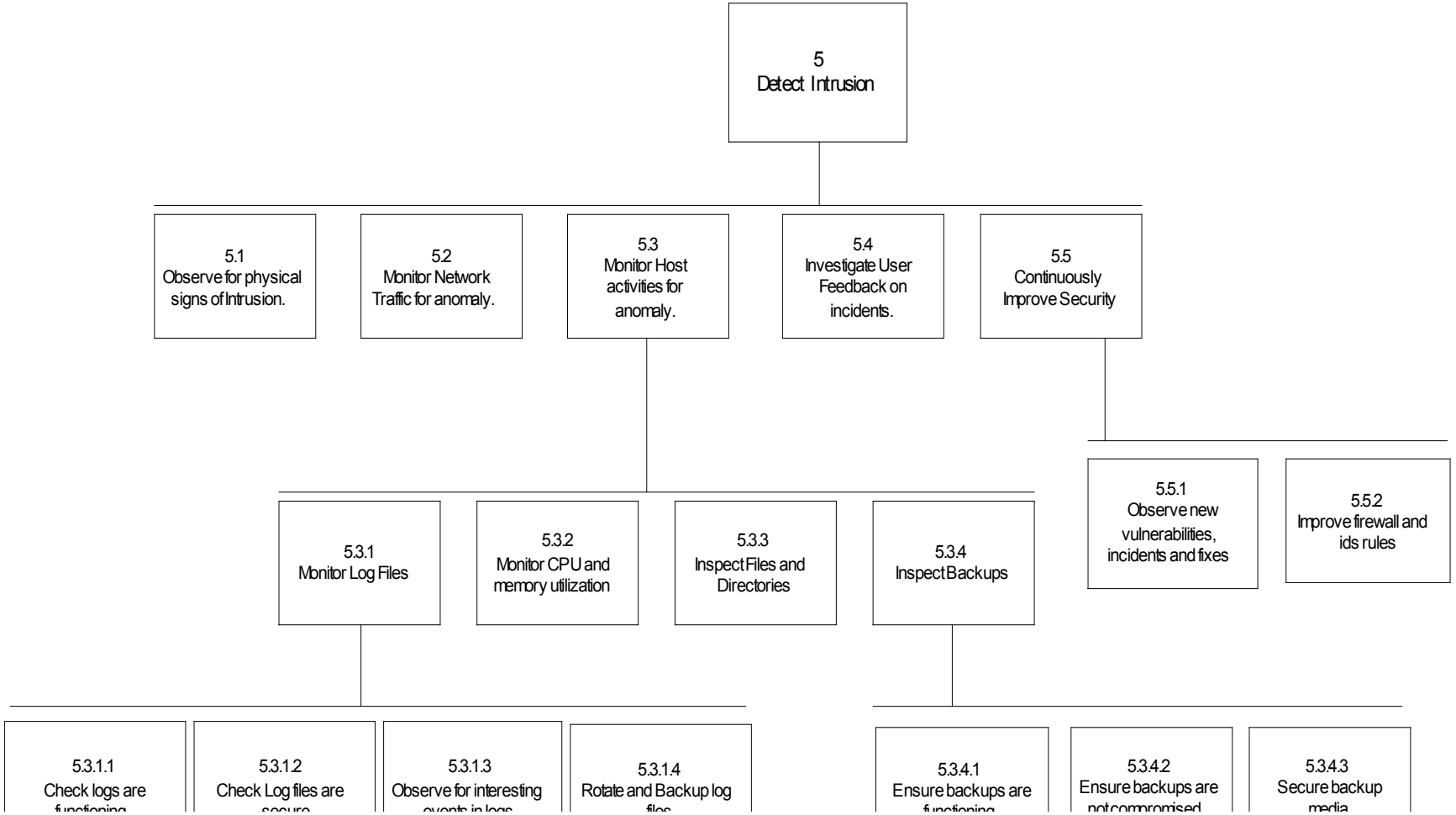

Perform Intrusion Detection
Plan 0: Before any Intrusion Detection Mechanism is implemented - 1
If IDS not selected, perform - 2
On any existing or new hardware, perform step - 3
After Operating system and applications are installed - 4
Monitor continuously for intrusion - 5
In case of a detected intrusion - 6
Continuously Improve Policy and IDS capability - 7
1. Develop Security Policy
2. Select an Intrusion Detection System
3. Harden and Secure Network and servers
4. Prepare for Intrusion Detection.
5. Detect Intrusion
6. Respond to Intrusion
7. Improve
Plan 2 : 1 - 2 - 3 - 4 - 5 - EXIT
2.1. Identify company needs
2.2. Understand different types of Intrusion Detection systems
2.3. Fully understand company network and usage
2.4. Evaluate Various Intrusion Detection Software
2.5. Select IDS software and design a system

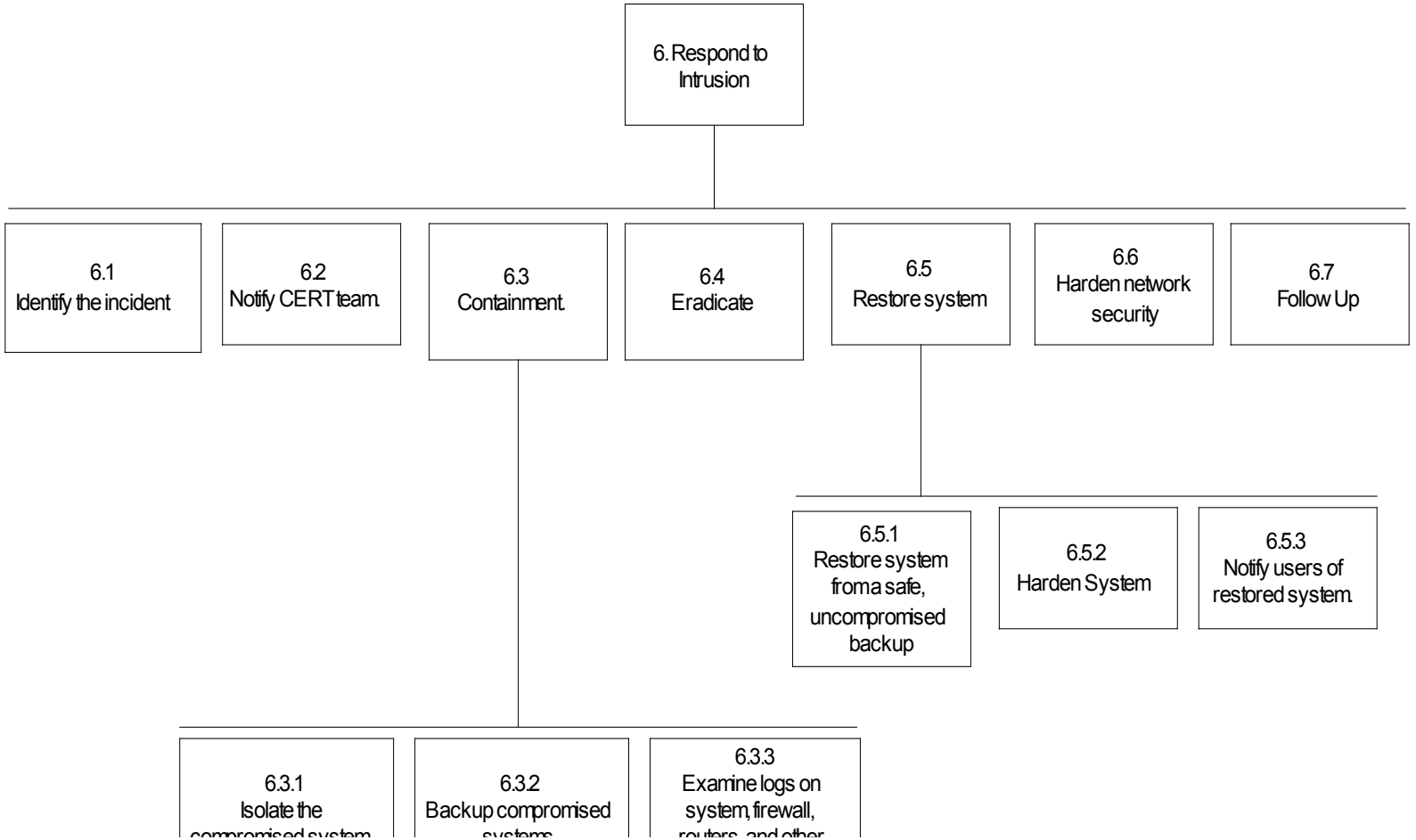
Legend

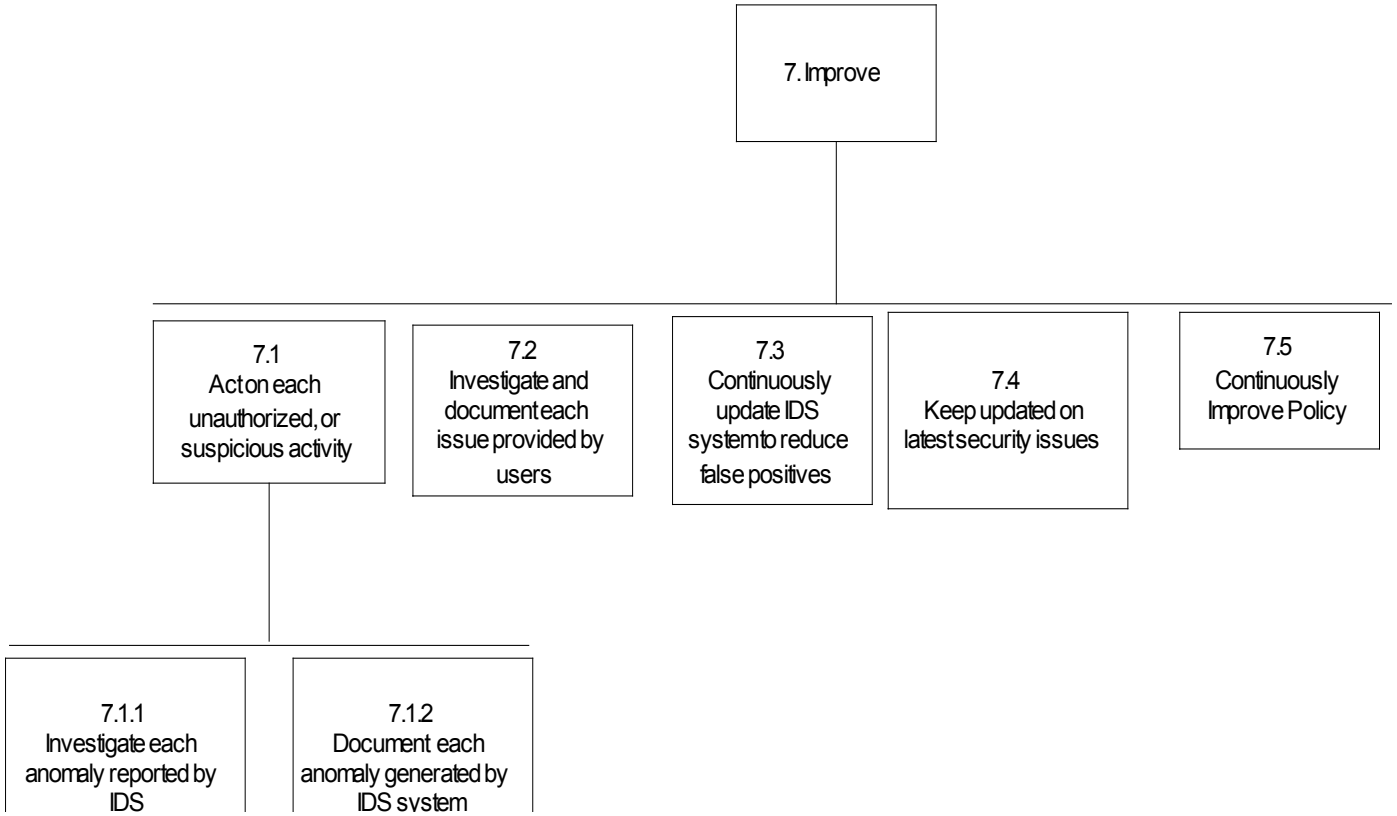

1. Develop Security Policy
1.1 Establish Policy
1.2 Deploy Policy
1.3 Review and Maintain Policy
1.2.1 Train Users and Stakeholders.
1.2.2 Document User Acceptance of Policy
1.2.3 Observe Users.
1.1.1 Analyze Assets, Risks and Vulnerabilities.
1.1.2 Consult Management and Stakeholders.
1.1.3 Develop Policy
1.2.3.1 Does Policy improve Security?
1.2.3.2 Does Policy Restrict User Productivity?
1.2.3.3 Obtain Feedback.
1.1.3.1
1.1.3.2
1.1.3.3


3. Harden and Secure Network and servers
3.1 Determine System Classification
3.2 Refer to computer deployment policy for the type
3.3 Gather information regarding users, application, data etc.
3.4 Identify Security requirements for this class of machine
3.5 Prepare System
3.6 Deploy System
3.6.1 Train Users on Usage and Policy
3.6.2 Document user acceptance of security policy
3.6.3 Deliver machine to user
3.5.1 Install minimal required operating system
3.5.2 Install latest security patches
3.5.3 Remove all default security privileges
3.5.4 Enable only required user privileges
3.5.5 Remove all unused applications and services
3.5.6 Enable backup
3.5.7 Enable System logging based on system classification
3.5.8 Install anti-virus software
3.5.9 Install IDS selected for the machine
3.5.7.1 Encrypt and secure log files
3.5.7.2 Rotate log files.
3.5.7.3 If possible log files to separate and dedicated host.
3.5.6.1
3.5.6.2
3.5.6.3


4. Prepare for Intrusion Detection
4.1 Establish Policy and Procedure
4.2 Build an archive of OS installation media and patches
4.3 Maintain required hardware and software tools.
4.4 Create Baseline
4.5 Check and enforce backup procedures
4.6 Maintain contact information.
4.7 Ensure IDS systems are properly configured.
4.4.1 Determine User Profile
4.4.2 Create Baseline of System Files
4.4.3 Create baseline of network traffic
4.4.4 Backup Baseline
4.4.1.1 Monitor Software
4.4.1.2 Monitor CPU and
4.4.1.3 Monitor Logs
4.4.1.4 Monitor network


5
Detect Intrusion
5.1
Observe for physical signs of Intrusion.
5.2
Monitor Network Traffic for anomaly.
5.3
Monitor Host activities for anomaly.
5.4
Investigate User Feedback on incidents.
5.5
Continuously Improve Security
5.3.1
Monitor Log Files
5.3.2
Monitor CPU and memory utilization
5.3.3
Inspect Files and Directories
5.3.4
Inspect Backups
5.5.1
Observe new vulnerabilities, incidents and fixes
5.5.2
Improve firewall and ids rules
5.3.1.1
Check logs are
5.3.1.2
Check Log files are
5.3.1.3
Observe for interesting
5.3.1.4
Rotate and Backup log
5.3.4.1
Ensure backups are
5.3.4.2
Ensure backups are not compromised
5.3.4.3
Secure backup media


6. Respond to Intrusion
6.1 Identify the incident
6.2 Notify CERT team.
6.3 Containment.
6.4 Eradicate
6.5 Restore system
6.6 Harden network security
6.7 Follow Up
6.5.1 Restore system from a safe, uncompromised backup
6.5.2 Harden System
6.5.3 Notify users of restored system.
6.3.1 Isolate the
6.3.2 Backup compromised
6.3.3 Examine logs on system, firewall,


7. Improve
7.1
Act on each unauthorized, or suspicious activity
7.2
Investigate and document each issue provided by users
7.3
Continuously update IDS system to reduce false positives
7.4
Keep updated on latest security issues
7.5
Continuously Improve Policy
7.1.1
Investigate each anomaly reported by IDS
7.1.2
Document each anomaly generated by IDS system

Perform Intrusion Detection

Plan 0: Before any Intrusion Detection Mechanism is implemented - 1
If IDS not selected, perform - 2
On any existing or new hardware, perform step - 3
After Operating system and applications are installed - 4
Monitor continuously for intrusion - 5
In case of a detected intrusion - 6
Continuously Improve Policy and IDS capability - 7

1. Develop Security Policy

2. Select a Intrusion Detection System

3. Harden and Secure Network and servers

4. Prepare for Intrusion Detection.

5. Detect Intrusion

6. Respond to Intrusion

7. Improve

Plan 2 : 1 - 2 - 3 - 4 - 5 - EXIT

2.1. Identify company needs

2.2. Understand different types of Intrusion Detection systems

2.3. Fully understand company network and usage

2.4. Evaluate Various Intrusion Detection Software

2.5. Select IDS software and design a system

Legend

Subtasks Defined in Subsequent Page

1. Develop Security Policy

1.1 Establish Policy

1.1.1 Analyze Assets, Risks and Vulnerabilities.

1.1.2 Consult Management and Stakeholders.

1.1.3 Develop Policy

1.1.3.1 Recommend Policies

1.1.3.2 Seek Management Feedback

1.1.3.3 Seek Legal Feedback

1.2 Deploy Policy

1.2.1 Train Users and Stakeholders.

1.2.2 Document User Acceptance of Policy

1.2.3 Observe Users.

1.2.3.1 Does Policy improve Security?

1.2.3.2 Does Policy Restrict User Productivity?

1.2.3.4 Obtain Feedback.

1.3 Review and Maintain Policy

3. Harden and Secure Network and servers

3.1 Determine System Classification

3.2 Refer to computer deployment policy for the type

3.3 Gather information regarding users, application, data etc.

3.4 Identify Security requirements for this class of machine

3.5 Prepare System

3.6 Deploy System

3.6.1 Train Users on Usage and Policy

3.6.2 Document user acceptance of security policy

3.6.3 Deliver machine to user

3.5.1 Install minimal required operating system

3.5.2 Install latest security patches

3.5.3 Remove all default security privileges

3.5.4 Enable only required user privileges

3.5.5 Remove all unused applications and services

3.5.6 Enable backup

3.5.7 Enable System logging based on system classification

3.5.8 Install anti-virus software

3.5.9 Install IDS selected for the machine

3.5.7.1 Encrypt and secure log files

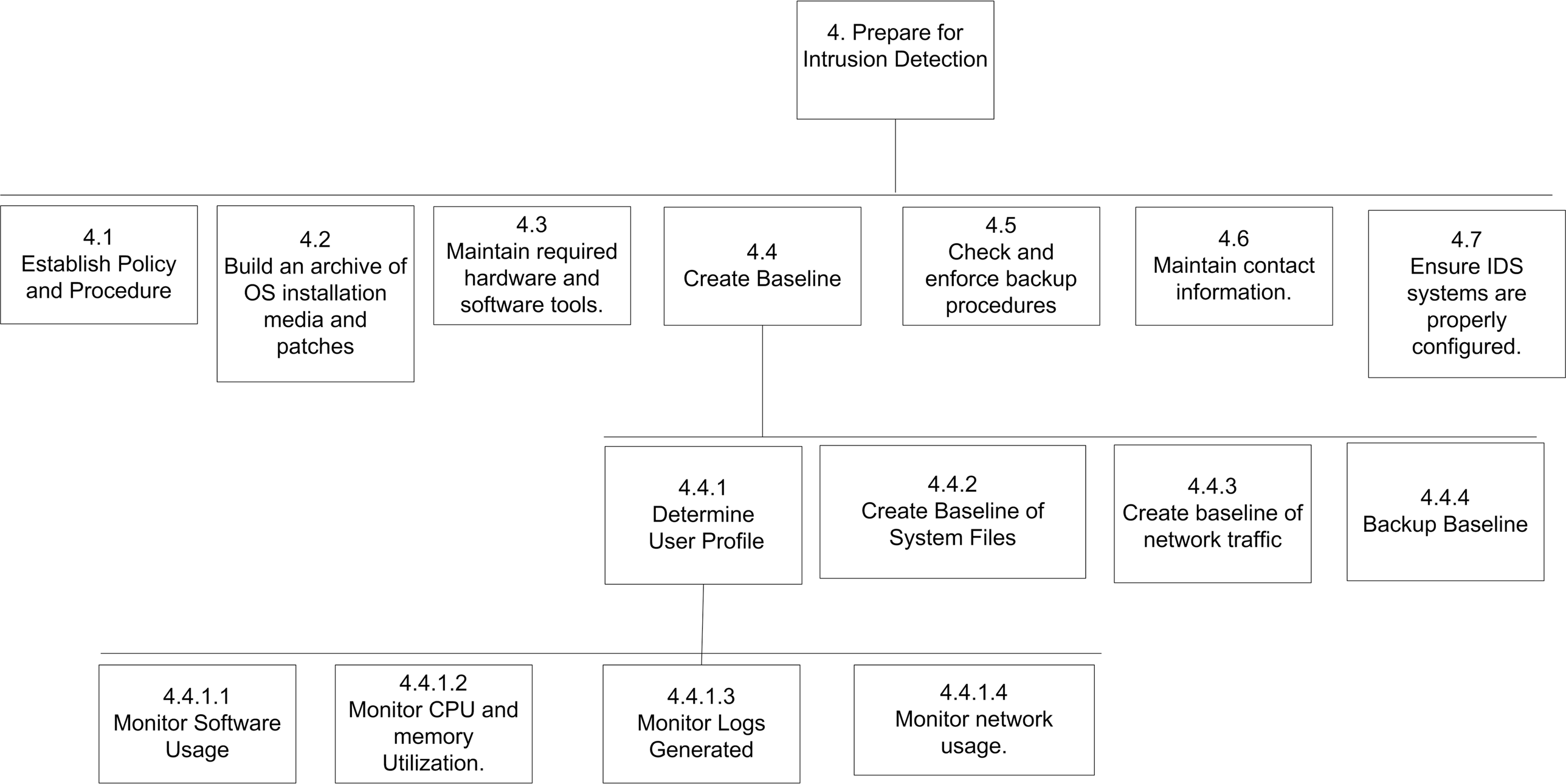
3.5.7.2 Rotate log files.

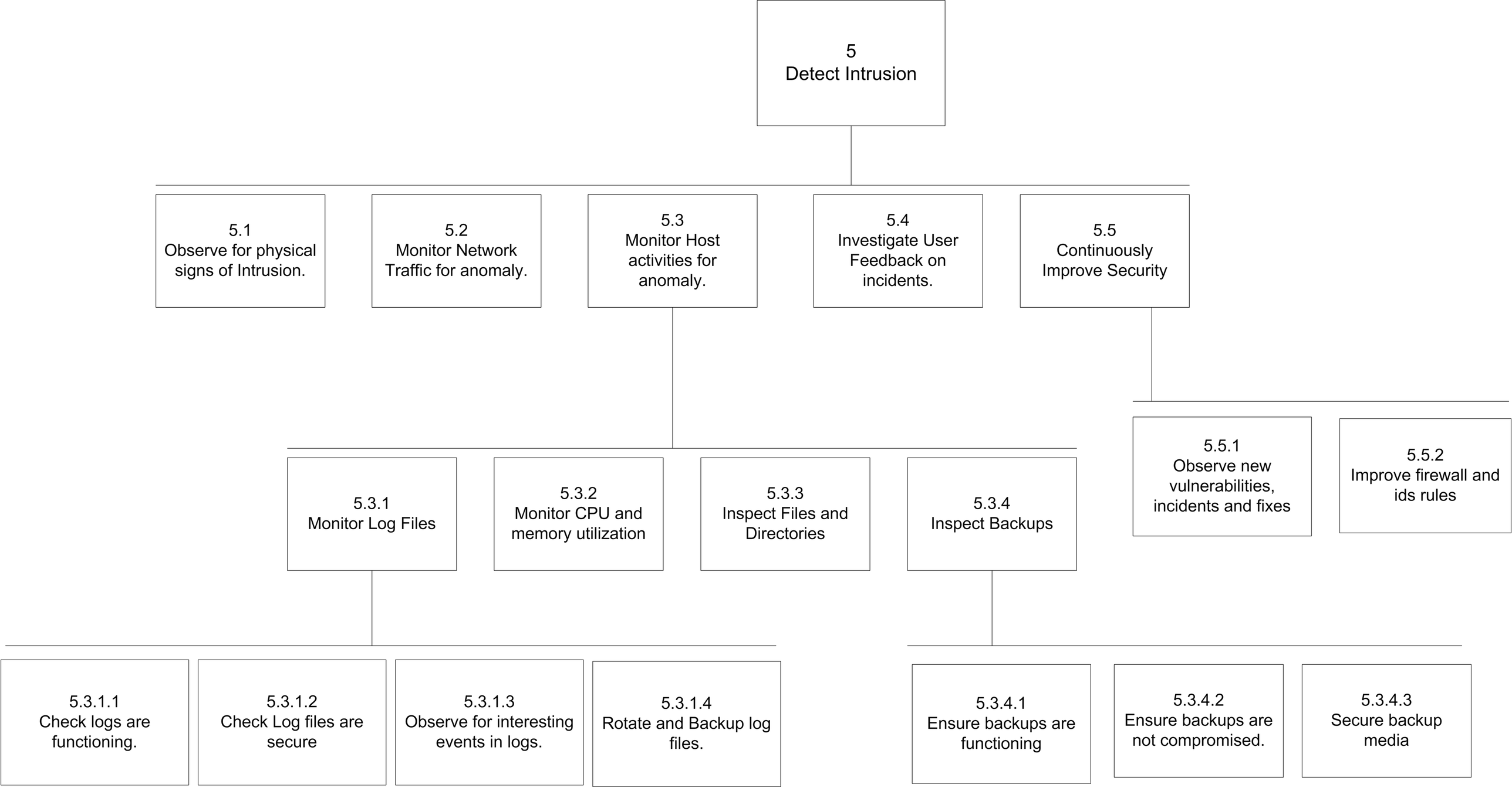
3.5.7.3 If possible log files to separate and dedicated host.

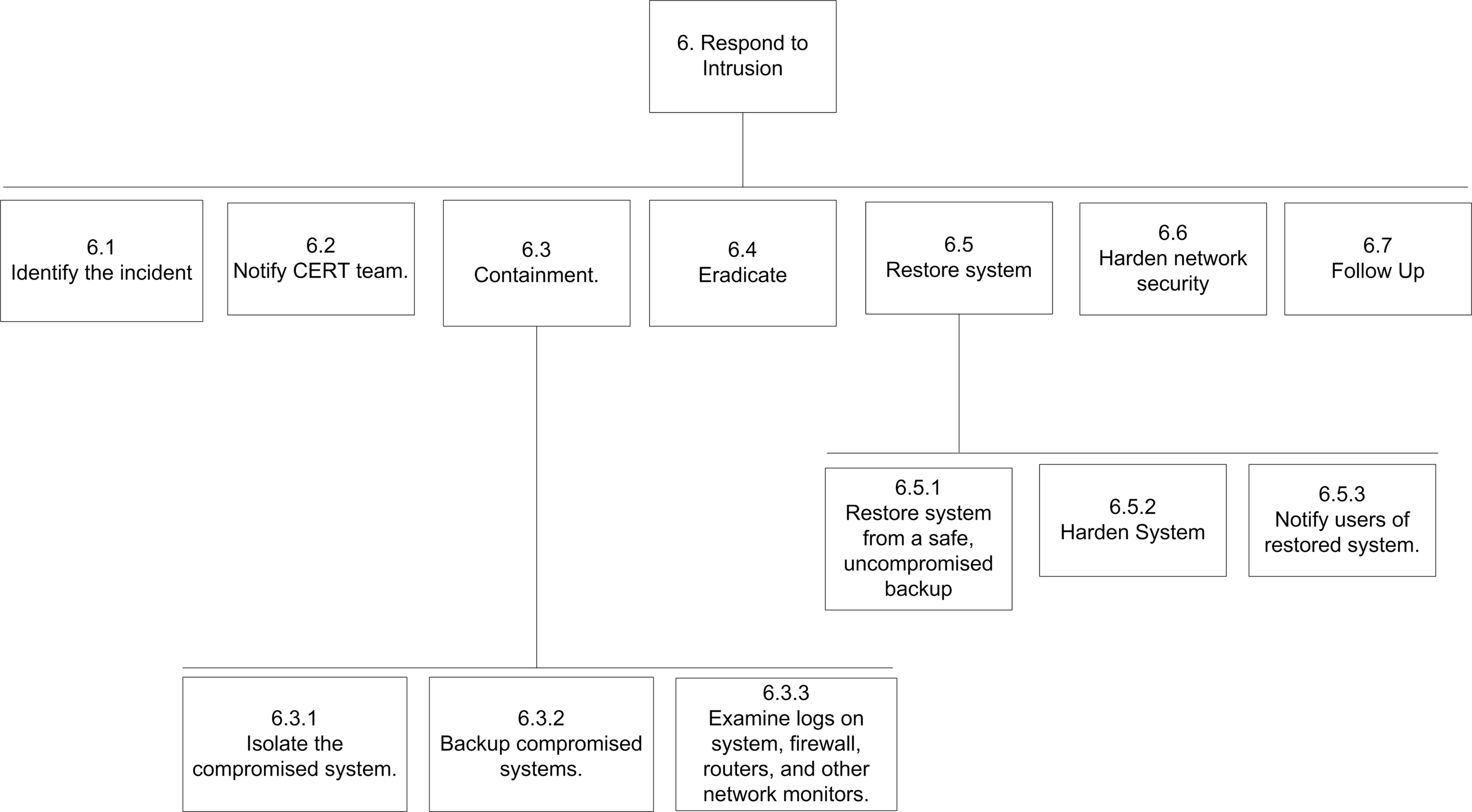
3.5.6.1 Install backup software

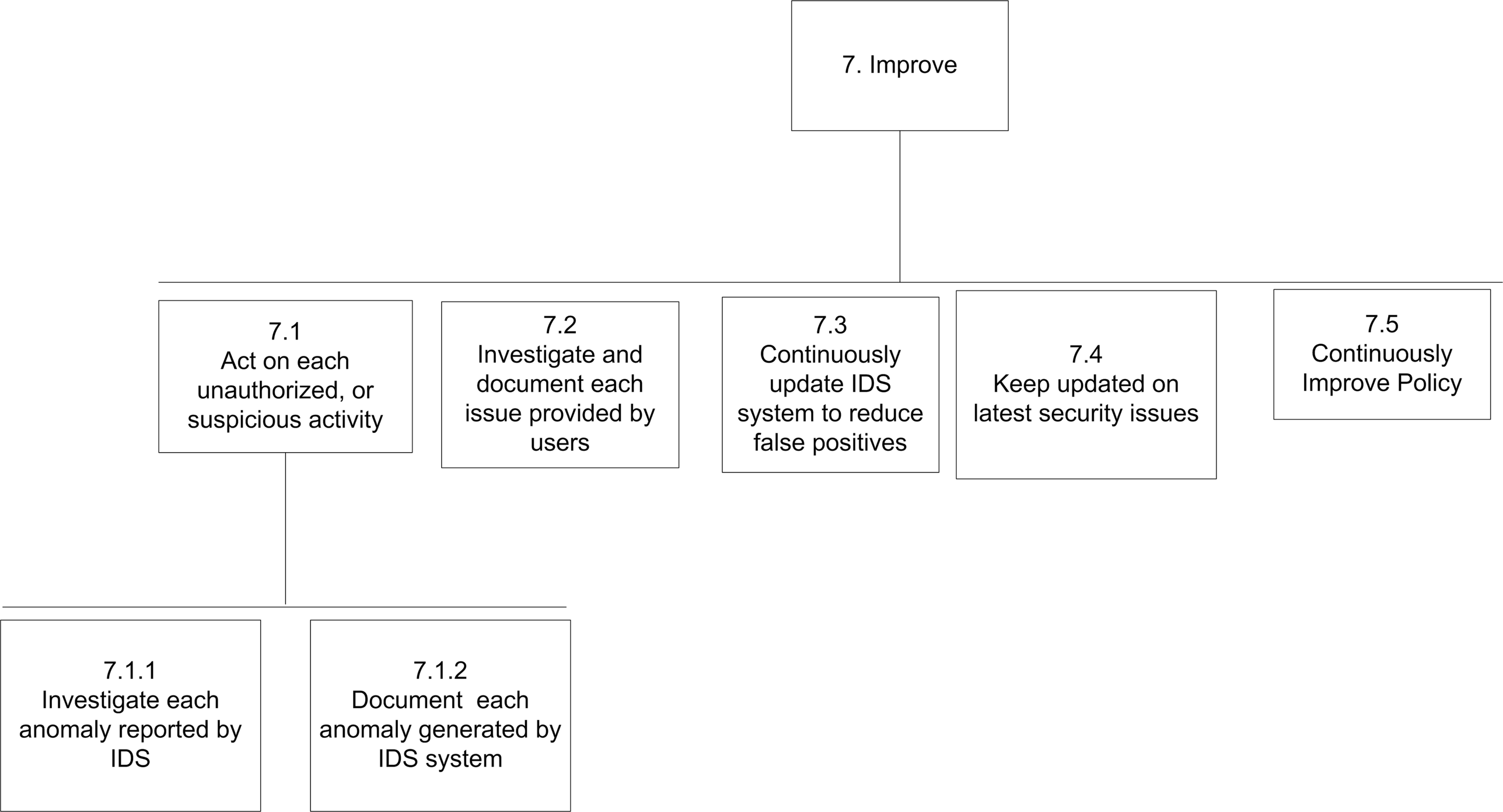
3.5.6.2 Test ability to restore from backup

3.5.6.3 Schedule periodic backups


4. Prepare for Intrusion Detection
4.1 Establish Policy and Procedure
4.2 Build an archive of OS installation media and patches
4.3 Maintain required hardware and software tools.
4.4 Create Baseline
4.5 Check and enforce backup procedures
4.6 Maintain contact information.
4.7 Ensure IDS systems are properly configured.
4.4.1 Determine User Profile
4.4.2 Create Baseline of System Files
4.4.3 Create baseline of network traffic
4.4.4 Backup Baseline
4.4.1.1 Monitor Software Usage
4.4.1.2 Monitor CPU and memory Utilization.
4.4.1.3 Monitor Logs Generated
4.4.1.4 Monitor network usage.


5
Detect Intrusion
5.1
Observe for physical signs of Intrusion.
5.2
Monitor Network Traffic for anomaly.
5.3
Monitor Host activities for anomaly.
5.4
Investigate User Feedback on incidents.
5.5
Continuously Improve Security
5.5.1
Observe new vulnerabilities, incidents and fixes
5.5.2
Improve firewall and ids rules
5.3.1
Monitor Log Files
5.3.2
Monitor CPU and memory utilization
5.3.3
Inspect Files and Directories
5.3.4
Inspect Backups
5.3.1.1
Check logs are functioning.
5.3.1.2
Check Log files are secure
5.3.1.3
Observe for interesting events in logs.
5.3.1.4
Rotate and Backup log files.
5.3.4.1
Ensure backups are functioning
5.3.4.2
Ensure backups are not compromised.
5.3.4.3
Secure backup media


6. Respond to Intrusion
6.1 Identify the incident
6.2 Notify CERT team.
6.3 Containment.
6.4 Eradicate
6.5 Restore system
6.6 Harden network security
6.7 Follow Up
6.5.1 Restore system from a safe, uncompromised backup
6.5.2 Harden System
6.5.3 Notify users of restored system.
6.3.1 Isolate the compromised system.
6.3.2 Backup compromised systems.
6.3.3 Examine logs on system, firewall, routers, and other network monitors.


7. Improve
7.1
Act on each unauthorized, or suspicious activity
7.2
Investigate and document each issue provided by users
7.3
Continuously update IDS system to reduce false positives
7.4
Keep updated on latest security issues
7.5
Continuously Improve Policy
7.1.1
Investigate each anomaly reported by IDS
7.1.2
Document each anomaly generated by IDS system

5. TASK DESCRIPTIONS

1. Task Name: Develop Security Policy

The Goal of this task: Develop, deploy and review a clear security policy for the company.

This task is a subtask of: Perform Intrusion Detection

The subtasks that define this task are:

1.1. Establish Policy
1.2. Deploy Policy
1.3. Review and Maintain Policy

The inputs or actions required by the user are: Stakeholders should have established a company security policy which all employees and contractors should adhere to.

The results or outputs are: A company security policy exists which employees can refer to and abide by.

Special characteristics of the task: Developing the security policy is an ongoing operation. It needs to be continually improved to reduce any forms of possible risks or liability caused to its IT infrastructure.

1.1. Task Name: Establish Policy

The Goal of this task: Develop a clear IT security policy to meet the needs of the company and its stakeholders.

This task is a subtask of: Develop Security Policy (level 1)

The subtasks that define this task are:

1.1.1. Analyze Assets, Risks and Vulnerabilities.
1.1.2. Consult Management and stakeholders
1.1.3. Develop the Policy

The inputs or actions required by the user are: Decide all the risks, vulnerabilities and issues that needs to be addressed by the policy.

The results or outputs are: A clear and well defined policy that is ready to be deployed.

Special characteristics of the task: The policy should relate to the company's IT infrastructure.

1.1.1. Task Name: Analyze Assets, Risks and Vulnerabilities.

The Goal of this task: Understand what the company assets (intellectual property, data, software, hardware etc) are and the risks and vulnerabilities it may be under.

This task is a subtask of: 1.1. Establish Policy

The subtasks that define this task are: None.

The inputs or actions required by the user are: Collect information about company assets, risks to them, and their vulnerabilities. Perform Business Impact Assessment using the following formula to identify risk.

$$R = V * T$$

where R is Risk, V is vulnerability and T is Threat.

Assets are important data or information such as databases, patented design documents, and other sensitive information that is critical for the survival of the company.

The results or outputs are: Useful data that can be used to further develop the security policy.

Special characteristics of the task: This task should relate to the company's IT infrastructure.

1.1.2. Task Name: Consult Management and stakeholders.

The Goal of this task: Consult management and stakeholders regarding development of company security policy.

This task is a subtask of: 1.1. Establish Policy

The subtasks that define this task are: None.

The inputs or actions required by the user are: Management and stakeholders should meet to seek feedback on security policy. Using information gathered in task 1.1.1, the management will be able to make informed decisions about the company's implementation of an intrusion detection system.

The results or outputs are: Management and stakeholders of the company would have been consulted on developing policy and procedures for company network security.

Special characteristics of the task: Management will also need to identify the CERT (Company Emergency Response Team). CERT will be a team composed of members from different departments of the company. Each member of the CERT team will have specific roles and responsibilities on handling a crisis related to company network security.

1.1.3. Task Name: Develop Policy

The Goal of this task: To write an IT security policy for the company.

This task is a subtask of: 1.1. Establish Policy

The subtasks that define this task are:

1.1.3.1. Recommend Policies
1.1.3.2. Seek Management Feedback
1.1.3.3. Seek legal feedback.

The inputs or actions required by the user are: Develop an IT security policy using information gained from analysis and consultation.

The results or outputs are: A fully developed policy that is ready for deployment.

Special characteristics of the task: This task should relate to the company's IT infrastructure.

1.1.3.1. Task Name: Recommend Policies

The Goal of this task: To recommend policy for the organization based on information gathered.

This task is a subtask of: 1.1.3. Develop Policy

The subtasks that define this task are: None

The inputs or actions required by the user are: Analyze information gathered, and develop policy and procedure documents that will address all concerns identified in Task 1.1.1.

The results or outputs are: A set of policies that should meet organizational needs.

Special characteristics of the task: This task should relate to the company's IT infrastructure.

1.1.3.2. Task Name: Seek Management Feedback

The Goal of this task: To allow management to review the policy and provide feedback.

This task is a subtask of: 1.1.3. Develop Policy

The subtasks that define this task are: None

The inputs or actions required by the user are: Provide management with a draft of policy and procedure documents. Seek feedback from management.

The results or outputs are: Feedbacks from the management will allow incorporating any issues that may have been missed during initial recommendations.

Special characteristics of the task: It is the responsibility of the management to enforce policy and procedures proposed.

1.1.3.3. Task Name: Seek Legal feedback

The Goal of this task: To get legal feedback on policy.

This task is a subtask of: 1.1.3. Develop Policy

The subtasks that define this task are: None

The inputs or actions required by the user are: Send company lawyers the policy document, and setup meetings to discuss issues. Identify legal implications of performing intrusion detection.

The results or outputs are: Feedback from lawyers allows incorporating any legal issues that may have been missed in initial recommendation.

Special characteristics of the task: Since network IDS captures network traffic that may contain personal data of employees, legal issues specific to privacy should be addressed. If Intrusion detection is to be performed as a covert operation, all legal issues must be addressed.

1.2. Task Name: Deploy Policy

The Goal of this task: Deploy the fully approved policy to employees and other technology users of the company.

This task is a subtask of: Develop Security Policy (Level 1)

The subtasks that define this task are:

1.2.1. Train Users and Stakeholders.
1.2.2. Document User Acceptance of Policy
1.2.3. Observe Users.

The inputs or actions required by the user are: None

The results or outputs are: A fully deployed security policy for the company that is accepted by employees, stakeholders and lawyer.

Special characteristics of the task: A fully developed security policy for the company that is approved by the stakeholders and company lawyer.

1.2.1. Task Name: Train Users and Stakeholders

The Goal of this task: Users and stakeholders need to be educated about the need for a security policy and how it may affect their daily lives. This will help users appreciate the need to follow policies for the sake of security within the company, and what potential damage can be caused if they are not followed.

This task is a subtask of: 1.2. Deploy Policy

The subtasks that define this task are: None

The inputs or actions required by the user are:

- Need to develop detailed documentation for users to study.
- Develop presentation slides.
- Arrange for training schedules for all users in the company.
- Attain feedback from students on how it may affect their work and productivity.
- Attain feedback on how to improve policy.

The results or outputs are: Employees would appreciate the need to understand the policy and abide by it. They will then understand potential risks if policies are broken.

Special characteristics of the task: It is important to train users why a security policy is in place, the reasons to abide by the policy, and how it will help avoid potential risks. Feedback from users during training will help policy developers to understand how policies will affect productivity of users, and how policies can be improved. This can be used to further improve policies.

Some employees may have concerns of how the policy may affect their daily work, and how it may hamper productivity. They may also be concerned about privacy issues. Management should be prepared to address such issues. Most concerns can be addressed by assuring the employee on how information collected from network is used, and the reason and need to enforce such measures.

1.2.2. Task Name: Document User Acceptance of Policy

The Goal of this task: Users need to read the policy and agree to abide by it. It is therefore necessary to get a signed document documenting acceptance of users to abide by policy.

This task is a subtask of: 1.2. Deploy Policy

The subtasks that define this task are:

Develop Policy Acceptance forms for employees
Distribute these forms to employees
Allow sufficient time for employees to sign and return
Collect forms back and file in employee file.

The inputs or actions required by the user are:

The results or outputs are: Company will have formally documented that each employee had read, understood and agreed to abide by the security policy. This can be later used for any disciplinary or legal action if required.

Special characteristics of the task: Some employees may have concerns of how the policy may affect their daily work, and how it may hamper productivity. They may also be concerned about privacy issues. Management should be prepared to address such issues. Most concerns can be addressed by assuring the employee on how information collected from network is used, and the reason and need to enforce such measures.

1.2.3. Task Name: Observe Users.

The Goal of this task: To obtain feedback from users and stakeholders. This will allow us to understand how users work is affected by policies and also if new changes improve security.

This task is a subtask of: 1.2. Deploy Policy

The subtasks that define this task are:

1.2.3.1. Does Policy improve Security?
1.2.3.2. Does Policy Restrict User Productivity?
1.2.3.3. Obtain Feedback.

The inputs or actions required by the user are: Some form of feedback mechanism should be developed so that users can easily communicate to the policy author about any concerns, praise or suggestions.

Also, it is possible to monitor systems if any breach of policy takes place. This will help in finding out why the breach occurred, and if the policy was in place to avoid it. (Refer Task 7 Improve Policy)

The results or outputs are: A security policy that has been tested and accepted by all employees.

Special characteristics of the task: The policy author needs to communicate well with the technology users and provide and frank and open communication channel with the policy developers. Such dialogue will allow the users to be an integral part of the policy development.

1.2.3.1. Task Name: Does policy improve security.

The Goal of this task: To find out if the new policy does indeed improve security.

This task is a subtask of: 1.2.3. Observer Users

The subtasks that define this task are: None

The inputs or actions required by the user are: Monitor network and systems and look out for unusual or undesirable network or system activity.

The results or outputs are: An understanding if the new policy is being adhered to and if it does enhance security in networks and systems.

Special characteristics of the task: Special network tools like network sniffers, port scanners, and intrusion detection systems should be used to collect information.

1.2.3.2. Task Name: Does Policy Restrict User Productivity?

The Goal of this task: To find out if new policies hamper employee productivity.

This task is a subtask of: 1.2.3. Observer Users

The subtasks that define this task are: None

The inputs or actions required by the user are: An open communication channel should be provided to users so they can bring forward concerns on how the new policies may hamper their productivity. The communication channel can be forms that users can fill in and return, online surveys, or even taking time to meet users personally.

The results or outputs are: An understanding on how policies can be improved so it minimizes user frustrations and increases productivity.

Special characteristics of the task: Developing proper communication channels with the users.

1.2.3.3. Task Name: Obtain feedback

The Goal of this task: To collect data from network, servers, and systems along with user feedback. This data will help further improve the policy to reduce risks and enhance user experience.

This task is a subtask of: 1.2.3. Observer Users

The subtasks that define this task are: None

The inputs or actions required by the user are: User had to use his analytical skills to derive intelligence from collected data.

The results or outputs are: Knowledge on deficiencies of current policy, and how to improve it.

Special characteristics of the task: Policy developers' experience in network security, and communication management.

1.3. Task Name: Review and maintain policy

The Goal of this task: It is necessary to continually review and improve security policy to counter newer security threats, to meet new technology requirements and to enhance employee productivity. Policy can be reviewed periodically based on risks posed by new threats.

This task is a subtask of: Develop Security Policy (Level 1)

The subtasks that define this task are: None.

The inputs or actions required by the user are:

Constantly Review latest security news like cert.org etc.
Monitor network and system activity for anomalies.
Communicate with users about problems they may face.

The results or outputs are: A continuously improving security policy for the company.

Special characteristics of the task: This is a repetitive task. Security analysts should possess all required security tools and experience to monitor systems for anomalies.

2. Task Name: Select an Intrusion Detection System

The Goal of this task: To select a combination of intrusion detection software to be used in the network and host computers.

This task is a subtask of: Perform Intrusion Detection.

The subtasks that define this task are:

2.1. Identify company needs
2.2. Understand different types of Intrusion Detection systems
2.3. Fully understand company network and usage
2.4. Evaluate various types of Intrusion Detection Software
2.5. Select IDS software and design a system

The inputs or actions required by the user are: Perform tasks 2.1., 2.2., 2.3., 2.4. and 2.5.

The results or outputs are: Company will have acquired intrusion detection software to help detect intrusion in network and hosts.

Special characteristics of the task: None.

2.1. Task Name: Identify Company Needs

The Goal of this task: To identify the needs of the company in terms of Intrusion Detection.

This task is a subtask of: 2. Select an Intrusion Detection System.

The subtasks that define this task are: None

The inputs or actions required by the user are: Before selecting Intrusion Detection software, a needs analysis has to be performed. The analysis will help understand what risks the company will face if an IDS system is not implemented. It will also help understand what features are necessary in an IDS system to help eliminate those risks.

Performing needs analysis will involve consulting with company stakeholders, management, users and other Information Technology users.

The results or outputs are: A needs analysis Document identifying needs for an Intrusion Detection system.

Special characteristics of the task: Communication and documentation are necessary skills to perform a needs analysis. Information gathered during analysis needs to be clearly documented for future reference.

2.2. Task Name: Understand different types of Intrusion Detection systems

The Goal of this task: To understand the different types of Intrusion Detection Systems available.

This task is a subtask of: 2. Select an Intrusion Detection System.

The subtasks that define this task are: None

The inputs or actions required by the user are: Conduct research about different Intrusion Detection technologies available. The major types of Intrusion detection systems are

1. Host Based IDS
2. Network Based IDS
3. Hybrid IDS, which is a combination of both Host based and Network based IDS.

The results or outputs are: Clear understanding of different types of Intrusion Detection technologies available.

Special characteristics of the task: None.

2.3. Task Name: Fully understand company network and system usage

The Goal of this task: To fully understand company network.

This task is a subtask of: 2. Select an Intrusion Detection System.

The subtasks that define this task are: None

The inputs or actions required by the user are: It is important to understand the company network architecture. Other areas that need to be carefully analyzed are:

1. Bandwidth usage: It is necessary to identify the traffic peaks and lows associated with different times of the day, week, month and year. Example, there may be high network traffic when employees submit time sheets on Monday morning, and low traffic Sunday nights.
2. Network Protocols used (e.g. TCP/IP, IPv6 etc)
3. Server Services provided (HTTP, FTP, SMTP etc.)
4. Firewalls and other network security software.
5. Software installed on systems (Server and Client).

The results or outputs are: Network and system usage are included in the needs analysis document.

Special characteristics of the task: This task will involve monitoring network traffic and documenting the findings.

2.4. Task Name: Evaluate Various Intrusion Detection Software

The Goal of this task: To evaluate various IDS software in the market to determine if they meet the needs of the company.

This task is a subtask of: 2. Select an Intrusion Detection System.

The subtasks that define this task are: None

The inputs or actions required by the user are: Evaluate various IDS software available in the market. Evaluation is performed by:

1. Allowing vendors to demonstrate their products.
2. Downloading, installing and testing evaluation versions of IDS systems
3. Analyzing the benefits of the different systems.
4. Comparing the features and benefits between products offered by different vendors.

The results or outputs are: Understanding the features and benefits of different IDS software in the market.

Special characteristics of the task: None.

2.5. Task Name: Select IDS software and design a system

The Goal of this task: Select and acquire an IDS solution that best fits the needs of the company network security.

This task is a subtask of: 2. Select an Intrusion Detection System.

The subtasks that define this task are: None

The inputs or actions required by the user are: Use knowledge gathered from previous steps to decide which combination software best suits the needs of the company. Acquire the necessary software. It may be decided that the best solution is to build a custom software to meet all the needs identified.

The results or outputs are: Company will have acquired the necessary IDS software that best fits the needs of the company network security.

Special characteristics of the task: None.

3. Task Name: Harden and Secure Network and Servers

The Goal of this task: To harden and secure the network and servers in the network.

This task is a subtask of: Perform Intrusion Detection.

The subtasks that define this task are:

3.1. Determine System Classification
3.2. Refer to computer deployment policy for the type
3.3. Gather information regarding users, application, data etc.
3.4. Identify Security requirements for this class of machine
3.5. Prepare System
3.6. Deploy System

The inputs or actions required by the user are: Perform tasks 3.1. through 3.6.

The results or outputs are: The security in the network and servers will have been hardened.

Special characteristics of the task: None.

3.1. Task Name: Determine System Classification

The Goal of this task: To determine the type of system that needs to be hardened. The different types could be laptop, desktop, server, router, pocket pc etc.

This task is a subtask of: 3. Harden and Secure Network and servers

The subtasks that define this task are: None

The inputs or actions required by the user are: None.

The results or outputs are: Determine the type of system in order to perform further tasks of hardening.

Special characteristics of the task: Determining the type of system will depend on the knowledge and experience of technicians. There may be newer types evolving in the future for example, Tablet PC.

3.2. Task Name: Refer to computer deployment policy for the type

The Goal of this task: To understand the security policy before configuring the server for delivery to user.

This task is a subtask of: 3. Harden and Secure Network and servers

The subtasks that define this task are: None

The inputs or actions required by the user are: Look up security policy for system type on the company intranet or in policy handbook.

The results or outputs are: Technician will understand what the policy is on configuring this system type.

Special characteristics of the task: Technician should know where to find the security policy easily for quick reference. There are tools available to automate the preparation of different type of systems.

3.3. Task Name: Gather information regarding users, application, data etc.

The Goal of this task: To determine requirements of the user so machine can be prepared.

This task is a subtask of: 3. Harden and Secure Network and servers

The subtasks that define this task are: None

The inputs or actions required by the user are: It is necessary to find out what the user requirement for the system is. This can be done by having the user submit a requisition with the required information. The requisition may need to be approved by the management before any work is started on the system.

The results or outputs are: Understand user requirements before system is configured.

Special characteristics of the task: Company should have a requisition process in place which should capture all user requirements before equipment is purchased. Company security policy should address the equipment requisition process.

3.4. Task Name: Identify Security requirements for this class of machine.

The Goal of this task: Different types of systems may have different security requirements bases on what the system is to be used for. For example, security requirements of a Web server will be different from that of a firewall server.

This task is a subtask of: 3. Harden and Secure Network and servers

The subtasks that define this task are: None

The inputs or actions required by the user are: Find out the function of the system and refer to security policy to determine which configuration is the best.

The results or outputs are: Understand the security requirements for the system.

Special characteristics of the task: Company security policy should address security requirements for systems to be used in different roles.

3.5. Task Name: Prepare System.

The Goal of this task: To prepare the system based on information gathered above. The system will conform to existing security policies and meet user requirements.

This task is a subtask of: 3. Harden and Secure Network and Servers

The subtasks that define this task are:

3.5.1. Install minimal required operating system
3.5.2. Install latest security patches
3.5.3. Remove all default security privileges
3.5.4. Enable only required user privileges
3.5.5. Remove all unused applications and services
3.5.6. Enable backup
3.5.7. Enable System logging based on system classification
3.5.8. Install anti virus software
3.5.9. Install IDS selected for the machine

The inputs or actions required by the user are: None

The results or outputs are: The system ready to be deployed will conform to existing security policies and meet user requirements.

Special characteristics of the task: The technician should collect all necessary software, data and hardware.

3.5.1. Task Name: Install minimal required operating system

The Goal of this task: Install the OS on the system based on system type and user requirements.

This task is a subtask of: 3.5. Prepare System

The subtasks that define this task are: None

The inputs or actions required by the user are: Collect installation disks or prepare to install via network

The results or outputs are: A system with operating system installed.

Special characteristics of the task: Make sure the version of Operating System installed is a current version and follows company policy.

3.5.2. Task Name: Install latest security patches

The Goal of this task: Install latest updates and patches for the operating system from the vendor.

This task is a subtask of: 3.5. Prepare System

The subtasks that define this task are: None

The inputs or actions required by the user are: Make sure update and patch files are available on disks, network or online.

The results or outputs are: A fully patched operating system installed on the system

Special characteristics of the task: It would be helpful if updates and patches are thoroughly tested on a similar system before they are applied, to avoid potential risks.

3.5.3. Task Name: Remove all default security privileges

The Goal of this task: Remove all default users and rights on the operating system. This will close possible access paths to threats.

This task is a subtask of: 3.5. Prepare System

The subtasks that define this task are: None

The inputs or actions required by the user are: Disable all user accounts except for root or Administrator accounts. Change all default passwords.

The results or outputs are: A fully patched operating system with unused user and group accounts disabled.

Special characteristics of the task: Different operating systems will have different user and group settings. Ensure root or Administrator account is secure and open so operating system is accessible.

3.5.4. Task Name: Enable only required user privileges

The Goal of this task: Create or enable user accounts for those users who will use the system.

This task is a subtask of: 3.5. Prepare System

The subtasks that define this task are: None

The inputs or actions required by the user are: Find which users will access the system and create or enable their user accounts. Allow the users to change the password on their first login.

The results or outputs are: A system with only required user accounts enabled.

Special characteristics of the task: None.

3.5.5. Task Name: Remove all unused applications and services

The Goal of this task: Remove applications and services running on the system that are not required by the user. This will reduce the number of open ports that can be compromised. Examples of services that may be enabled by default and could be potential security risks are telnet, FTP, SMTP in a Linux or Unix system. In a Windows system, applications such as windows media player, or instant messengers are potential risks.

This task is a subtask of: 3.5. Prepare System

The subtasks that define this task are: None

The inputs or actions required by the user are: Find what processes and applications are installed. Find what applications and services are required by the user and disable all others that are not required.

The results or outputs are: A system with all unused applications and services removed.

Special characteristics of the task: Application and services vary in different operating systems.

3.5.6. Task Name: Enable backup

The Goal of this task: The goal is to be able to take backups of user data and other important system files periodically.

This task is a subtask of: 3.5 Prepare System

The subtasks that define this task are:

3.5.6.1. Install backup software
3.5.6.2. Test ability to restore from backup
3.5.6.3. Schedule periodic backups

The inputs or actions required by the user are: None

The results or outputs are: System will be able to backup data on a regular basis. Data can be restored at any time if required.

Special characteristics of the task: Backup requirements may differ for different systems. For instance, servers may have more frequent backups than desktops and laptops.

3.5.6.1. Task Name: Install backup software

The Goal of this task: Install necessary backup software in the system to enable backup of data to alternate media such as tapes or optical media.

This task is a subtask of: 3.5.6. Enable Backup

The subtasks that define this task are: None

The inputs or actions required by the user are: Find required backup software for the type of system. Install and configure it on the system.

The results or outputs are: The system would have backup software installed.

Special characteristics of the task: Backup software may vary for different types of systems. Ensure necessary space is available in backup media. Backup media may be tape drives, network drives, or optical drives. It is recommended backups of sensitive data be protected via encryption, password protection and stored in a safe, secure and remote location.

3.5.6.2. Task Name: Test ability to restore from backup

The Goal of this task: To make sure backup and restore operation works.

This task is a subtask of: 3.5.6. Enable Backup

The subtasks that define this task are: None

The inputs or actions required by the user are: To schedule a test backup, and restore data to an alternate location. Check if restored data is same as data backed up.

The results or outputs are: Backup and restore functionality has been tested.

Special characteristics of the task: For servers, backups may be needed to be tested over a period of time to make sure periodic backups succeed.

3.5.6.3. Task Name: Schedule periodic backups

The Goal of this task: Make periodic backups of changes to data everyday. In case older data needs to be restored for some reason, it would be possible.

This task is a subtask of: 3.5.6. Enable Backup

The subtasks that define this task are: None

The inputs or actions required by the user are: Determine the interval and type of backup (Differential, Incremental, Daily) that needs to be setup for the system

The results or outputs are: System is backed up on a scheduled basis.

Special characteristics of the task: Different system types will require different schedules. For example, servers, and databases will need to be backed up more often than a desktop. Backups should be tested over a period of time to know that schedules are working fine. Backup schedules should cause minimum downtime or disruption to users.

3.5.7. Task Name: Enable System logging based on system classification

The Goal of this task: System logging will allow the security analyst or administrator to track error messages or monitor for anomalies in system behavior.

This task is a subtask of: 3.5 Prepare System

The subtasks that define this task are:

3.5.7.1. Encrypt and secure log files
3.5.7.2. Rotate log files.
3.5.7.3. If possible, log files to separate and dedicated host.

The inputs or actions required by the user are: Enable logging of specific events (e.g. unsuccessful login attempts, system reboots etc). Refer to security policy to determine the level of security required for the type of system.

The results or outputs are: System logs will be available for the administrators or security analysts to look at.

Special characteristics of the task: The verbose level should be decided based on policy requirements. E.g. Servers will need a higher verbose logging than a desktop machine. For best results, logs should be sent to a central logging server which will allow central monitoring of all systems.

3.5.7.1. Task Name: Encrypt and secure log files

The Goal of this task: Make sure that logs created by systems are secure. System logs could reveal sensitive information about the system that could compromise its security. Also, if there is a break in, the attacker should not be able to change the log file to hide his activity.

This task is a subtask of: 3.5.7. Enable System Logging

The subtasks that define this task are: None

The inputs or actions required by the user are: Encrypt log files by configuring operating system and server software. It is a good idea to send log files to a single server where it can be encrypted and stored in centralized location.

The results or outputs are: System logging would be secure.

Special characteristics of the task: None.

3.5.7.2. Task Name: Rotate log files.

The Goal of this task: Rotate log files so it would not take up more disk space than allocated for logs.

This task is a subtask of: 3.5.7 Enable System Logging

The subtasks that define this task are: None

The inputs or actions required by the user are: Develop and implement scripts that would rotate (compress, backup, delete) log files on a periodic basis or when certain preset disk quota is reached.

The results or outputs are: Log files are rotated and would never fill up the disk which would otherwise cause downtime.

Special characteristics of the task: None

3.5.7.3. Task Name: If possible log files to separate and dedicated host.

The Goal of this task: Logs should be sent to a central logging system so all logs can be monitored from one place. IDS software can use these logs to detect possible anomalies.

This task is a subtask of: 3.5.7 Enable System Logging

The subtasks that define this task are: None

The inputs or actions required by the user are: Configure the operating system to send logs to a central logging system.

The results or outputs are: Central server has logs for all the systems in the company.

Special characteristics of the task: Log polling servers should be a powerful enough server with ample disk space to handle the load.

3.5.8. Task Name: Install anti virus software

The Goal of this task: Install anti-virus software to prevent the virus from infecting the systems, and allow periodic scanning and cleaning of viruses.

This task is a subtask of: 3.5. Prepare System

The subtasks that define this task are: None

The inputs or actions required by the user are: Install anti-virus software, and update the latest virus signatures from vendor. Enable scanning of incoming and outgoing files. Enable automatic updates of virus signatures from vendor.

The results or outputs are: A system that has anti-virus protection.

Special characteristics of the task: Mostly required for windows based desktops and laptops. Security policy should address security issues such as users downloading software from the internet, and opening email attachments.

3.5.9. Task Name: Install IDS selected for the machine

The Goal of this task: Install Intrusion Detection Software on the system. This will alert the system administrator of any anomalies in the system behavior and possibly prevent intrusion depending on the type of IDS used.

This task is a subtask of: 3.5. Prepare System

The subtasks that define this task are: None

The inputs or actions required by the user are: Install and configure IDS in the system. Read security policy to determine IDS rules for the type of system.

The results or outputs are: The system will be alerted of any attempted intrusions or malfunction.

Special characteristics of the task: Different type of systems will have different requirements for IDS software. For example, IDS software required for a server level system will be different from IDS software required for workstations and laptops.

3.6. Task Name: Deploy.

The Goal of this task: To deploy the prepared system to the user.

This task is a subtask of: 3. Harden and Secure Network and servers

The subtasks that define this task are:

3.6.1. Train Users on Usage and Policy
3.6.2. Document user acceptance of security policy
3.6.3. Deliver machine to user

The inputs or actions required by the user are: None.

The results or outputs are: Users received the system and have accepted security policy.

Special characteristics of the task: The technician may physically need to move the machine to the user location.

3.6.1. Task Name: Train Users on Usage and Policy

The Goal of this task: To educate user on computer usage policy.

This task is a subtask of: 3.6. Deploy

The subtasks that define this task are: None

The inputs or actions required by the user are: Users should be given a brief overview of computer usage policy and a printed copy of the usage policy.

The results or outputs are: User understands what the company policy is on computer usage.

Special characteristics of the task: Prepare key points to talk to user about usage. Make sure copies of required parts of policy manual is available to the users. Users can be members of employees, management, or customers.

3.6.2. Task Name: **Document user acceptance of security policy**

The Goal of this task: To get proof that users have accepted the security policy. This is necessary to take disciplinary or legal action in case of breach of policy.

This task is a subtask of: 3.6. Deploy

The subtasks that define this task are: None

The inputs or actions required by the user are: Allow users to read the usage policy and present them with a policy acceptance form for the user to sign and return. Provide the form to the Human Resources Department to be stored in employee file.

The results or outputs are: Documented proof that users have accepted company computer usage policy.

Special characteristics of the task: Policy acceptance forms need to be provided by the Human Resources Department. A workflow mechanism should be in place to streamline process. This is also repeated in Task 1.

3.6.3. Task Name: **Deliver machine to user**

The Goal of this task: To physically deliver, and install machine at user location.

This task is a subtask of: 3.6. Deploy

The subtasks that define this task are: None

The inputs or actions required by the user are: Move machine using special tools to user location. If required, remove any older equipment. Install the new system and test if it's functioning properly.

The results or outputs are: User has new system delivered and ready to use.

Special characteristics of the task: Installation of servers or routers would require special precautionary measures such as backing up old data, minimizing downtime, etc.

4. Task Name: Prepare for Intrusion Detection

The Goal of this task: Prepare for Intrusion Detection

This task is a subtask of: Perform Intrusion Detection.

The subtasks that define this task are:

4.1. Establish Policy and Procedure
4.2. Build an archive of OS installation media and patches
4.3. Maintain required hardware and software tools.
4.4. Create Baseline
4.5. Check and enforce backup procedures
4.6. Maintain contact information.
4.7. Ensure IDS systems are properly configured.

The inputs or actions required by the user are: Perform Tasks 4.1. through 4.7.

The results or outputs are: The organization, its personnel, and assets will be prepared for Intrusion Detection

Special characteristics of the task: None.

4.1. Task Name: Establish Policy and Procedure

The Goal of this task: The company policy and procedure manual should address the following:

1. Important information assets.
2. Threats faced by important information assets.
3. Procedure to follow to detect, and prevent threats to these assets.
4. Procedure to follow if these assets are compromised due to intrusion.

This task is a subtask of: 4. Prepare for Intrusion Detection

The subtasks that define this task are: None.

The inputs or actions required by the user are:

1. Identify information assets through research and communicating with stakeholders.
2. Document procedures to needed to detect, and prevent threat to these assets, and
3. Document procedures to follow if identified assets are compromised due to intrusion.

The results or outputs are: The policy and procedure manual will address steps on how to detect, prevent and respond to threats to important information assets.

Special characteristics of the task: This task is also linked to Task 1 (Develop Security Policy). The procedure and policy manual has to be continuously improved to address new and evolving threats. Therefore this is an ongoing and repetitive task.

4.2. Task Name: Build an archive of OS installation media and patches

The Goal of this task: To build and archive all used Operating System installation media, their patches, and other important software.

This task is a subtask of: 4. Prepare for Intrusion Detection

The subtasks that define this task are: None.

The inputs or actions required by the user are:

1. Archive installation media of all used Operating System.
2. Archive bootable disks for all Operating Systems.
3. Archive all the latest operating system updates, and security patches saved in CDROM or other trusted media.
4. Archive all other tools required for data recovery such as backup software, imaging software, anti-virus software etc.

The results or outputs are: The software needed to recover any system and its data is readily available.

Special characteristics of the task: It is recommended that the software archive be in a secure location that is accessible only to IT personnel. The archive has to be continuously updated with new patches, and software version releases. Therefore, this is an ongoing and repetitive process.

4.3. Task Name: Maintain required hardware and software tools

The Goal of this task: To keep required hardware and software tools readily available.

This task is a subtask of: 4. Prepare for Intrusion Detection

The subtasks that define this task are: None.

The inputs or actions required by the user are:

1. Keep all the hardware needed to perform repairs on any system.
2. Keep in stock spare hardware such as hard drives, backup tapes, and other computer components. This will help in reducing downtime in case a hard disk needs to be replaced, or backup tapes run out.
3. Keep software tools and utilities necessary to perform recovery and testing readily available.

The results or outputs are: Software and hardware tools needed to perform recovery of a system are readily available anytime.

Special characteristics of the task: This is an ongoing process, as new tools, hardware and software needs to be added as technology evolves.

4.4. Task Name: Create Baseline

The Goal of this task: To identify a baseline of system and network activity. Baseline is a snapshot of network, CPU, system files, and process activity when a system is in a stable and trusted state. Baseline can be used to detect activity that is anomalous to the known state.

A network baseline is a snapshot of network activity and bandwidth usage in a known and trusted state. Network baseline can be different at different times of day, and month based on the organization's activities such as month end account balancing, employee time sheet submission on Mondays etc. Another example is low network traffic on a company holiday.

This task is a subtask of: 4. Prepare for Intrusion Detection

The subtasks that define this task are:

4.4.1. Determine User Profile
4.4.2. Create Baseline of System Files
4.4.3. Create baseline of network traffic
4.4.4. Backup Baseline

The inputs or actions required by the user are: Perform tasks 4.4.1 through 4.4.4.

The results or outputs are: Identified baselines for systems and network.

Special characteristics of the task: Baseline of network traffic and system usage changes over time as new software and services are added to the network. For example, if the organization has implemented new enterprise accounting software that is installed on a server, the normal everyday network traffic will be different prior to when the software was implemented. Therefore, identifying the baseline of network and systems needs to be an ongoing task.

4.4.1 Task Name: Determine User Profile

The Goal of this task: To determine usage of system resources by users.

This task is a subtask of: 4.4. Create Baseline

The subtasks that define this task are:

4.4.1.1. Monitor Software Usage
4.4.1.2. Monitor CPU Utilization.
4.4.1.3. Monitor Logs Generated
4.4.1.4. Monitor network usage.

The inputs or actions required by the user are: Performs tasks 4.4.1.1. through 4.4.1.4.

The results or outputs are: An understanding of the usage of system resources by users.

Special characteristics of the task: This is a repetitive task since system usage will change with time as new technologies are acquired by the company.

4.4.1.1 Task Name: Monitor Software Usage

The Goal of this task: To determine software usage on computers.

This task is a subtask of: 4.4.1 .Determine User Profile

The subtasks that define this task are: None

The inputs or actions required by the user are: Determine software frequently utilized by users in the company. This information can be gathered by using a software and hardware inventory system used to track different software and hardware installed in each computer within the network.

The results or outputs are: Understanding the different software installed and used in each system.

Special characteristics of the task: None.

4.4.1.2. Task Name: Monitor CPU and memory Utilization.

The Goal of this task: To determine usage of system resources by users.

This task is a subtask of: 4.4.1. Determine User Profile

The subtasks that define this task are: None

The inputs or actions required by the user are: Use operating system tools such as the *"top"* command for Unix and task manager or performance monitor for Windows environment to find out CPU and memory utilization on systems at different times of the day.

The results or outputs are: An understanding of normal memory and CPU utilization on systems during different times of the day.

Special characteristics of the task: None

4.4.1.3. Task Name: Monitor Logs Generated

The Goal of this task: Monitor logs generated by systems to detect anomalies.

This task is a subtask of: 4.4.1. Determine User Profile

The subtasks that define this task are: None

The inputs or actions required by the user are: Configure systems to send important log files to a central log server. Install log monitoring software such as *"EventSentry"* or *"EventTracker"* for Windows platform or *"LogWatch"* or *"firelogd" for Unix.* LogWatch and firelogd are tools that email a concise report of interesting events from the log files on a daily basis.

Some of the log files which have interesting information are messages (important system messages), lastlog (logs user logins), and http logs (logs generated by the web server).

The results or outputs are: Log files created in hosts are monitored.

Special characteristics of the task: This is an ongoing task. Reports from log file monitoring tools need to be reviewed everyday.

4.4.1.4. Task Name: Monitor network usage

The Goal of this task: To start monitoring the network usage based on user demographics (different types of users). Information gathered from this exercise can be used to detect anomaly from normal network traffic generated by users. For example, if there is an unusually high bandwidth usage on weekend by a specific user, this may be considered an anomaly and may need to be investigated.

This task is a subtask of: 4.4.1. Determine User Profile

The subtasks that define this task are: None

The inputs or actions required by the user are:

1. Install and configure System and Network monitoring tools.
2. Monitor network traffic usage of different user segments.

The results or outputs are: Users are monitored for their network usage.

Special characteristics of the task: None.

4.4.2. Task Name: Create Baseline of System Files

The Goal of this task: To create a baseline of important system files and directories (for example, kernel, configuration files and directories etc.) This baseline can be used to determine anomalies if any of the files are altered.

This task is a subtask of: 4.4. Create Baseline

The subtasks that define this task are: None

The inputs or actions required by the user are: Use tools such as tripwire for Unix or System File checker for Windows to create a baseline that can be used to monitor changes to important files and directories.

The results or outputs are: Baseline of key system files is available.

Special characteristics of the task: None

4.4.3. Task Name: Create baseline of network traffic

The Goal of this task: To establish a baseline of network activity and bandwidth usage.

This task is a subtask of: 4.4. Create Baseline

The subtasks that define this task are: None

The inputs or actions required by the user are: Observe network traffic and bandwidth usage during various times of the day, week and month. Generally, network traffic is monitored by placing a sensor on a network that needs to be observed. The sensor can determine the types of network traffic, and bandwidth usage.

Network traffic will vary based on times of day, week, month and year. For example, network traffic will be considered light during lunch hour, weekend, and annual holidays. Network traffic will be high when employees enter their timesheets through an online system on Monday and during year end account closing at the end of the financial year.

The results or outputs are: Baseline of network usage at different times of the day, week, month and year is available for reference.

Special characteristics of the task: Use tools such as snort, and other operating system tools to create baseline. This is an ongoing process since network traffic usage will vary as the organization acquires new systems and services and the network grows with the addition of new employees.

4.4.4. Task Name: Backup Baseline

The Goal of this task: To keep backups of baseline of system and network usage. Baselines should be protected because if they are altered by intrusive activity, they will be rendered useless.

This task is a subtask of: 4.4. Create Baseline

The subtasks that define this task are: None

The inputs or actions required by the user are: Backup all baseline related data in a secure media. Also, store the media in a secure location where it is easily accessible by the security personnel.

The results or outputs are: Baseline data is backed up and stored in a secure area.

Special characteristics of the task: This task will be executed when tasks 4.4.2. and 4.4.3. are executed.

4.5. Task Name: Check and enforce backup procedures

The Goal of this task: To make sure backups are functioning properly and proper backup procedures are followed.

This task is a subtask of: 4. Prepare for Intrusion Detection

The subtasks that define this task are: None

The inputs or actions required by the user are: Refer to backup and restoration procedures defined in the company policy and procedures manual. Check if backup agents are installed on all systems and important files, directories and data are set to back up periodically. Check if data can be successfully restored using existing backup procedures.

The results or outputs are: Backup procedures defined in the company policy and procedures manual are enforced.

Special characteristics of the task: None.

4.6. Task Name: Maintain contact information

The Goal of this task: To maintain a database of important contact information.

This task is a subtask of: 4. Prepare for Intrusion Detection

The subtasks that define this task are: None.

The inputs or actions required by the user are: Collect and maintain important contact information about law enforcement officials, company stakeholders, vendors, clients and so on. During an emergency, important contact information should be readily available.

The results or outputs are: Important contact information is readily available.

Special characteristics of the task: None.

4.7. Task Name: Ensure IDS systems are properly configured

The Goal of this task: To make sure Intrusion Detection software is installed and properly configured.

This task is a subtask of: 4. Prepare for Intrusion Detection

The subtasks that define this task are: None

The inputs or actions required by the user are:

1. Ensure Intrusion detection software is installed and functioning as expected.
2. Check rules to reduce false positives.

The results or outputs are: Intrusion Detection software is installed and properly configured.

Special characteristics of the task: This task is repeated in task 3 (Harden and Secure Network and Servers).

5. Task Name: Detect Intrusion

The Goal of this task: To detect any form of threat to the network or the computers.

This task is a subtask of: Perform Intrusion Detection.

The subtasks that define this task are:

5.1. Observe for physical signs of Intrusion.
5.2. Monitor Network Traffic for anomaly.
5.3. Monitor Host activities for anomaly.
5.4. Investigate User Feedback on incidents.
5.5. Continuously Improve Security

The inputs or actions required by the user are: Perform tasks 5.1., 5.2., 5.3., 5.4., and 5.5.

The results or outputs are: Any form of internal or external threat to the network will be prevented.

Special characteristics of the task: None.

5.1. Task Name: Observe for physical signs of Intrusion.

The Goal of this task: To determine if there is any physical evidence of intrusion.

This task is a subtask of: 5. Detect Intrusion

The subtasks that define this task are: None

The inputs or actions required by the user are: Visually inspect the server room, machines, locks, etc. If video surveillance is in place, view tapes for anomaly.

The results or outputs are: The security personnel will be alerted in case of a physical break-in, theft or other forms of unauthorized access. Personnel will also be able collect physical evidence in case of security breach.

Special characteristics of the task: The security personnel should be trained to look out for signs of physical intrusion.

5.2. Task Name: Monitor Network Traffic for Anomaly

The Goal of this task: To determine if there is any anomaly in the network traffic that may indicate signs of intrusion.

This task is a subtask of: 5. Detect Intrusion

The subtasks that define this task are: None

The inputs or actions required by the user are: Monitor network traffic for anomalies using tools like snort. For instance, if the tool detects a large number of simultaneous TCP connections requests (SYN) to a server, this would be a network anomaly. This would indicate that someone is performing a port scan on the server. A port scan is usually done to find out what services are available on the server, which operating system is used, and type of firewalls in place.

The results or outputs are: Notification in case of any network anomaly is detected by the Intrusion Detection System. Notification can be done via email, phone or pager service depending on the severity of the case.

Special characteristics of the task: Network based IDS software needs customized rules to determine what type of traffic should be considered an anomaly. The network security personnel needs to actively monitor developments of new exploits using various sources like security websites, magazines, news services, and so on. The rules for IDS software have to be continuously enhanced to combat new exploits.

5.3. Task Name: Monitor Host Activity for anomaly.

The Goal of this task: To audit servers and desktop activity for anomalies.

This task is a subtask of: 5. Detect Intrusion

The subtasks that define this task are: None

The inputs or actions required by the user are: Install and configure host based intrusion detection software agents in servers. The network security personnel should use the combination of software most suited for each system. Different types of Host based software have different capabilities. Some are capable of monitoring the computer to find out if any of the critical system files have been altered, or if any unusual activity is using up processor cycles, or memory. Others can monitor log files, user logins, and network connection requests for anomalies [7].

The results or outputs are: Notification in case of any anomaly is detected in the host. Notification can be done via email, phone or pager service depending on the severity of the case.

Special characteristics of the task: The security personnel should make themselves familiar with different types of users, their software usage, and network activity. They should be alert and always keep an eye out for anomalies in systems and network activity.

5.3.1. Task Name: Monitor Log Files.

The Goal of this task: To monitor log files for anomalies.

This task is a subtask of: 5.3. Monitor Host activities for anomaly.

The subtasks that define this task are:

5.3.1.1. Check logs are functioning
5.3.1.2. Check log files are secure
5.3.1.3. Observe for interesting evens in logs
5.3.1.4. Rotate and Backup log files.

The inputs or actions required by the user are: Install and configure tools to monitor log files generated in the host machine. Log files are generated by the operating system and many other system software such as web, database, and file servers. Log files will have information such as, attempts, usernames, errors, and other useful data for debugging.

Software such as *"logsentry"*, and *"swatch"* for Unix based systems, and *"EventSentry"* and *"EventTracker"* for Windows platforms can monitor log files for specific events, or notify network administrators of a suspicious activities found [5].

The results or outputs are: Log monitoring tools will continuously monitor important system log files for anomalies.

Special characteristics of the task: Log monitoring can also be done centrally if all host machines are configured to send all log files to a central log server. This way, logs can be easily maintained, and log monitoring software needs to be configured on only one log server.

5.3.1.1. Task Name: Check logs are functioning

The Goal of this task: To make sure the logs are functioning.

This task is a subtask of: 5.3.1. Monitor Log Files
The subtasks that define this task are: None

The inputs or actions required by the user are: Monitor log files to check if they are being updated by the system. This can be done by operating tools like *"tail"* and checking time stamp, file size etc.

The results or outputs are: The logs are functioning correctly.

Special characteristics of the task: None.

5.3.1.2. Task Name: Check log files are secure

The Goal of this task: To make sure log files are not tampered with.

This task is a subtask of: 5.3.1. Monitor Log Files

The subtasks that define this task are: None

The inputs or actions required by the user are: Use operating system commands to check if log files were not tampered with. It is possible that a hacker could try to erase any traces by altering the log files. A common way of making sure log files are not tampered with is to have a central logging server, or making frequent backup of log files to a remote server.

The results or outputs are: Knowledge that log files are secure.

Special characteristics of the task: It is recommended using a central logging server to send all the logs to, thus log files can be centrally monitored and archived.

5.3.1.3. Task Name: Observe for interesting events in logs

The Goal of this task: Monitor log files for anomaly.

This task is a subtask of: 5.3.1. Monitor Log Files

The subtasks that define this task are: None

The inputs or actions required by the user are: Install and configure tools to monitor log files generated in the host machine. Log files are generated by the operating system, and many other system software such as web, database, and file servers. Log files will have information such as, attempts, usernames, errors, and other useful debug data.

Software such as logsentry, and swatch for Unix based systems, and EventSentry and EventTracker for Windows platforms can monitor log files for specific events, or notify admins if an suspicious activity is found.

The results or outputs are: Log monitoring tools will continuously monitor important system log files for anomalies.

Special characteristics of the task: None

5.3.1.4. Task Name: Rotate and Backup log files.

The Goal of this task: Rotate and Backup log files periodically in a secure location.

This task is a subtask of: 5.3.1. Monitor Log Files

The subtasks that define this task are: None

The inputs or actions required by the user are: Configure scripts to archive log files in a periodic basis or based on file size quota. The archived log files should be moved or backed up to a remote secure location.

Archived log files will come to use when a network security breach is discovered. The log files can be used by network specialists, and law enforcement officials to investigate the breach if required.

The results or outputs are: Log files are rotated and backed up to a secure location.

Special characteristics of the task: None

5.3.2. Task Name: Monitor CPU and Memory utilization

The Goal of this task: To Monitor CPU and Memory usage of host system to detect anomaly.

This task is a subtask of: 5.3. Monitor Host activities for anomaly.

The subtasks that define this task are: None

The inputs or actions required by the user are: Monitor the CPU and memory usage of the host machine using System tools like top in Unix, or Performance logs and alerts tool in Windows. Scripts can be developed by the admin to notify and send log information if for example, CPU utilization exceeds 90% and memory utilization exceeds 70%.

The processes running on the host should be monitored for suspicious programs. This can be monitored using *"ps"* and *"top"* in Unix systems, and task manager in windows systems.

The results or outputs are: Security personnel will be able to detect unusual activity based on processes running on the system, and the amount of CPU cycles and memory utilized.

Special characteristics of the task: Monitoring processes and CPU utilization will allow security personnel to detect inside attacks from trusted users.

5.3.3. Task Name: Inspect files and Directories

The Goal of this task: Monitor integrity of important system files such as Kernel, system configuration files and directories.

This task is a subtask of: 5.3. Monitor Host activities for anomaly.

The subtasks that define this task are: None.

The inputs or actions required by the user are: Integrity of important files can be monitored by using operating system commands and checking for time stamp, user and group file permissions, etc. Windows systems have a command line tool called system File checker (Sfc.exe) [9] and a popular Unix based tool to monitor file integrity is *"tripwire"* [8].

The results or outputs are: All system files and directories will be maintained in a known and trusted state. If unauthorized changes are detected, it would mean a possible breach in security.

Special characteristics of the task: Reports produced by these tools have to be monitored daily.

5.3.4. Task Name: Inspect Backups

The Goal of this task: Inspect Backups to make sure it is possible to perform a restore if necessary. Minimize failed or bad backups and secure backups so it does not fall into wrong hands.

This task is a subtask of: 5.3. Monitor Host activities for anomaly.

The subtasks that define this task are:

5.3.4.1. Ensure Backups are functioning
5.3.4.2. Ensure Backups are not compromised
5.3.4.3. Secure Backup Media

The inputs or actions required by the user are: Install and configure backup agents in host computers.

The results or outputs are: Host machines can be restored from secure backup media at any time with minimum loss of data.

Special characteristics of the task: Backup software should produce necessary reports daily that will allow administrators to manage backups effectively. Backups should be sent to a secure offsite facility.

5.3.4.1. Task Name: Ensure Backups are functioning

The Goal of this task: Inspect Backups and ensure that it's possible to perform a restoration if necessary and to minimize failed or bad backups.

This task is a subtask of: 5.3.4. Inspect Backups

The subtasks that define this task are: None

The inputs or actions required by the user are: Check daily backup reports to make sure backups were successful. Backups could fail for various reasons like backup media was full or faulty, backup server failed to initialize, or hosts were unreachable at backup time. Such problems have to be fixed promptly and the necessary precautions taken so that it does not occur again.

The results or outputs are: Fully functioning backups ready for restoration with minimum loss of data.

Special characteristics of the task: Backup systems have advanced reporting tools to allow administrators to keep track of daily backups, media, and hosts.

5.3.4.2. Task Name: Ensure Backups are not compromised

The Goal of this task: Make sure backups are not compromised.

This task is a subtask of: 5.3.4. Inspect Backups

The subtasks that define this task are: None

The inputs or actions required by the user are: Physically inspect backup media to check if it was altered in any way. Inspect backup software logs and reports for anomalies.

The results or outputs are: Backups are not compromised.

Special characteristics of the task: None

5.3.4.3. Task Name: Secure Backup media

The Goal of this task: To secure backup media in a safe remote location.

This task is a subtask of: 5.3.4. Inspect Backups

The subtasks that define this task are: None

The inputs or actions required by the user are: Move the backup media to a secure offsite facility regularly to prevent data loss in case of a catastrophe, theft of media, weather damage etc.

The results or outputs are: Backup media is moved to a secure offsite facility periodically.

Special characteristics of the task: Often offsite backups are stored with third party backup storage companies who have highly secure storage infrastructure.

5.4. Task Name: Investigate User Feedback on incidents.

The Goal of this task: Obtain feedback from users about any unusual activity in their computer or network.

This task is a subtask of: 5. Detect Intrusion

The subtasks that define this task are: None

The inputs or actions required by the user are: Maintain a rapport with users, to get information about any unusual activity in their computer or network. For instance, a user may notice that an email he/she received has a suspicious looking file, or high processor, memory or disk activities are slowing down his/her machine.

It would be beneficial for users to have a convenient feedback mechanism to notify the system administrator or network personnel of any problems they find with their machine, or the network they are in.

The results or outputs are: System administrators or security personnel will be notified in case of problems with users' machines or if any unusual activity is taking place in their machines.

Special characteristics of the task: Training users about acceptable usage policy, providing a feedback mechanism and frequent rapport with different users.

5.5. Task Name: Continually Improve Security.

The Goal of this task: Continuously improve network and host based intrusion detection techniques.

This task is a subtask of: 5. Detect Intrusion

The subtasks that define this task are: None

The inputs or actions required by the user are: Regular updates and enhancement of rules for network and host based intrusion detection systems based on past experiences, and new vulnerabilities. This task is further explained in Task 7.

The results or outputs are: New or updated policy and procedure document.

Special characteristics of the task: Quality of the Intrusion detection system will depend on the security personnel's ability to know the latest about evolving security problems and keeping a close eye on network and host activities for anomalies.

5.5.1 Task Name: Lookout for new vulnerabilities, incidents and fixes.

The Goal of this task: Lookout in network security magazines, user groups and news sites for information on new exploits, vulnerabilities and hacking methodologies.

This task is a subtask of:
5.5 Continuously improve security

The subtasks that define this task are:
None

The inputs or actions required by the user are: Visit important security sites and signup for security alerts. Check security software web sites for updates of software's, rules and new tips.

The results or outputs are: Security personnel is being proactive, and gathering information about new network threats, and vulnerabilities in operating system and server software.

Special characteristics of the task:

5.5.2 Task Name: Improve firewall and IDS rules.

The Goal of this task: Improve firewall and IDS rules to encounter new exploits and vulnerabilities.

This task is a subtask of:

5.5 Continuously improve security

The subtasks that define this task are:

None

The inputs or actions required by the user are: Enhance firewall and IDS rules to combat new threats. Upgrade operating systems and server software to fix latest bugs, and exploits.

The results or outputs are: Firewall and IDS rules continuously evolve to combat new security threats.

Special characteristics of the task: None

6. Task Name: Respond to Intrusion

The Goal of this task: If an intrusion is detected by the IDS systems, take necessary steps to handle the intrusion effectively.

This task is a subtask of: Perform Intrusion Detection.

The subtasks that define this task are:

6.1 Identify the incident
6.2 Notify CERT Team
6.3 Containment
6.4 Eradicate
6.5 Restore System
6.6 Harden Network Security
6.7 Follow up

The inputs or actions required by the user are: Perform Tasks 6.1 through 6.7

The results or outputs are: Performed proper incident handling procedures to respond to intrusion.

Special characteristics of the task: None.

6.1. Task Name: Identify the incident.

The Goal of this task: To identify the type of incident and find out if it is a real intrusion that could cause significant risk to company assets.

This task is a subtask of: 6.Respond to Intrusion.

The subtasks that define this task are: None

The inputs or actions required by the user are: Use necessary tools to make sure the intrusions detected by IDS systems are real. If the intrusions detected by the intrusion detection system were false positives, then an intrusion may not have actually occurred. Identify which systems were affected, and what assets may be at risk.

The results or outputs are: Understanding if an intrusion has actually occurred.

Special characteristics of the task: It is important to make sure if an intrusion has actually occurred before executing incident response procedures.

6.2. Task Name: Notify CERT team.

The Goal of this task: To notify the CERT (Company Emergency Response Team) if an actual intrusion has been detected. The CERT team will then decide what steps are to be taken to contain the situation, and who should be notified.

This task is a subtask of: 6. Perform Intrusion Detection.

The subtasks that define this task are: None

The inputs or actions required by the user are: If tasks performed in 6.1 (Identify the Incident) reveal that an actual intrusion has taken place, proper members of the CERT team have to be alerted.

The results or outputs are: The CERT team would be fully aware of the incident, and proper intrusion response procedures would be invoked.

Special characteristics of the task: The stakeholders may need to know which assets are at risk, and the possible financial and legal ramifications. The CERT team may decide to contact necessary law enforcement officials based on the severity of the problem.

6.3. Task Name: Containment.

The Goal of this task: To contain the intrusion in order to minimize damage to company assets.

This task is a subtask of: 6. Perform Intrusion Detection.

The subtasks that define this task are:

6.3.1. Backup compromised systems.
6.3.2. Isolate the compromised system.
6.3.3. Examine logs on system, firewall, routers, and other network monitors.

The inputs or actions required by the user are: The security personnel may need to take the affected system offline, perform backups, change passwords to major systems, and close all further access to the intruder. Also, check if any other systems in the network may be affected and inspect host, router, firewall, and IDS log files for any signs of further intrusion.

The results or outputs are: The intrusion incident would have been properly contained to prevent any further threats to company assets.

Special characteristics of the task: None.

6.3.1. Task Name: Isolate the compromised system

The Goal of this task: Isolate the compromised system to prevent any further damage to the system or other hosts in the network.

This task is a subtask of: 6.3. Containment

The subtasks that define this task are: None

The inputs or actions required by the user are:

1. Disconnect the system from the network
2. Kill any unknown or foreign processes that might have been installed by the intruder.
3. Shutdown http, mail, ftp, database and other servers.
4. Un-mount any disks that hold data.

The results or outputs are: The affected system has been isolated from the network.

Special characteristics of the task: None

6.3.2. Task Name: Backup compromised systems

The Goal of this task: To backup the compromised systems to a safe media.

This task is a subtask of: 6.3. Containment

The subtasks that define this task are: None

The inputs or actions required by the user are: Use backup tools to backup all data and system files to a safe media. Take multiple copies of the backup and send one copy offsite for archival. These backups will be used later for forensic purposes, and for restoring critical data.

The results or outputs are: Compromised systems were backed up to a safe media.

Special characteristics of the task: None.

6.3.3. Task Name: Examine logs on system, firewall, routers, and other network monitors.

The Goal of this task: To examine key log files to determine if intrusion may have spread to other parts of the network.

This task is a subtask of: 6.3. Containment

The subtasks that define this task are: None

The inputs or actions required by the user are: Examine log files of firewall, routers, and systems such as desktops and servers. The logs may have information that may help us find answered to questions like:

1. What other systems in the network may be compromised?
2. What route and steps did the intruder take to gain access to affected systems?
3. Did intruder install any Trojan horses or other form of destructive code?
4. What the vulnerability in the network was used for the intrusion?

The results or outputs are: Log files have been examined to find more details on this intrusion.

Special characteristics of the task: None.

6.4. Task Name: Eradicate

The Goal of this task: To eradicate the problems caused by intrusion and to prevent similar event from re-occurring.

This task is a subtask of: 6. Perform Intrusion Detection.

The subtasks that define this task are: None

The inputs or actions required by the user are: Determine why the incident occurred, and find the cause and symptoms associated to this intrusion. IDS and firewall rules may need to be modified to prevent this from happening again. Proper operating system and server software patches may need to be applied to other similar systems. Perform vulnerability analysis after hardening the network.

The results or outputs are: Vulnerabilities in the network and systems that caused this intrusion to occur would be eliminated.

Special characteristics of the task: None.

6.5. Task Name: Restore System.

The Goal of this task: To restore the compromised system to full functionality.

This task is a subtask of: 6. Perform Intrusion Detection.

The subtasks that define this task are:

6.5.1. Restore system from a safe, uncompromised backup
6.5.2. Harden System
6.5.3. Notify users of restored system.

The inputs or actions required by the user are: Perform tasks 6.5.1 through 6.5.3.

The results or outputs are: The compromised system will be fully restored to its original state before intrusion occurred.

Special characteristics of the task: None.

6.5.1. Task Name: Restore system from a safe, uncompromised backup

The Goal of this task: To restore the system from backups verified to be safe.

This task is a subtask of: 6.5. Restore System

The subtasks that define this task are: None

The inputs or actions required by the user are: To identify if prior backups are safe, i.e. does not contain compromised data or code, use information gained in task 6.3.3 to identify when and which files have been modified. For a safe restore, use the backups taken prior to intrusion.

The results or outputs are: The system has been restored from a safe, uncompromised backup.

Special characteristics of the task: Before restoring data, it is assumed the operating system and all other necessary software are installed, and all latest security patches are applied.

6.5.2. Task Name: Harden System

The Goal of this task: To Harden the restored system.

This task is a subtask of: 6.5. Restore System

The subtasks that define this task are: None

The inputs or actions required by the user are: Apply latest patches for operating system, and other services such as web server, database server, email server etc. Perform tasks defined in Task 3.5 (Prepare System)

The results or outputs are: The Restored system has been hardened using task 3.5.

Special characteristics of the task: None.

6.5.3. Task Name: Notify users of restored system

The Goal of this task: Communicate to users after system has been restored for regular use.

This task is a subtask of: 6.5. Restore System

The subtasks that define this task are: None

The inputs or actions required by the user are: The CERT team will decide when the system is safe to be accessed by users. They may decide to communicate to users why the outage has happened, and if any precautions users need to take to help prevent similar event.

The results or outputs are: Users will be informed about system availability.

Special characteristics of the task: None.

6.6. Task Name: Harden Network Security

The Goal of this task: Harden network security to prevent similar intrusions and to improve IDS rules.

This task is a subtask of: 6.Perform Intrusion Detection.

The subtasks that define this task are: None

The inputs or actions required by the user are: Perform tasks defined in Task 3 (Harden and Secure network and servers)

The results or outputs are: The firewall rules, IDS rules, and server security will be hardened.

Special characteristics of the task: None.

6.7. Task Name: Follow up

The Goal of this task: Follow up on the events before and after the intrusion.

This task is a subtask of: 6.Perform Intrusion Detection.

The subtasks that define this task are: None

The inputs or actions required by the user are: Document steps taken to contain, and eradicate the problem. Document the cause of intrusion. It may have been that a known vulnerability in a server was not fixed, firewall rules were lax, or IDS rules were not properly implemented.

To avoid similar incidents in the future, recommend alternative solutions, or changes to current policy and procedures. Meet with affected parties such as users, stakeholders and clients to address any concerns.

The results or outputs are: The incident will be well documented. Changes to policy and procedures will be considered. Meet affected parties to address any concerns.

Special characteristics of the task: None.

7. Task Name: Improve

The Goal of this task: Continuously improve network security.

This task is a subtask of: Perform Intrusion Detection.

The subtasks that define this task are:

7.1. Act on each unauthorized, or suspicious activity
7.2. Investigate and document each issue provided by users.
7.3. Continuously update IDS system to reduce false positives
7.4. Keep updated on latest security issues.
7.5. Continuously Improve Policy

The inputs or actions required by the user are: Perform Steps 7.1, 7.2, 7.3, and 7.5

The results or outputs are: Network security evolves and improves during time.

Special characteristics of the task: None

7.1. Task Name: Act on each unauthorized or suspicious activity

The Goal of this task: To take investigative action on each network security incident.

This task is a subtask of: 7. Improve.

The subtasks that define this task are:

7.1.1. Investigate each anomaly reported by IDS
7.1.2. Document each anomaly reported by IDS

The inputs or actions required by the user are: Respond to Intrusion by executing Task 6 (Respond to Intrusion). Perform Tasks 7.1.1 and 7.1.2.

The results or outputs are: Each unauthorized or suspicious activity is dealt with and documented for future reference.

Special characteristics of the task: This task relies on information gathered while performing task 6 (Respond to Intrusion).

7.1.1. Task Name: Investigate each anomaly generated by IDS system.

The Goal of this task: To investigate each anomaly generated by the IDS system.

This task is a subtask of: 7.1. Act on each unauthorized or suspicious activity.

The subtasks that define this task are: None

The inputs or actions required by the user are: This is a combination of Task 5 (Detect Intrusion) and Task 6 (Respond to Intrusion). Perform steps in Task 5 to detect any forms of Intrusion. If any intrusion is detected, perform Task 6 to respond.

The results or outputs are: Each anomaly generated by IDS system will be detected and dealt with.

Special characteristics of the task: This is a combination of Task 5 and Task 6.

7.1.2. Task Name: Document each anomaly generated by IDS system

The Goal of this task: To document findings of each intrusion and steps taken to respond to the intrusion.

This task is a subtask of: 7.1. Act on each unauthorized or suspicious activity.

The subtasks that define this task are: None

The inputs or actions required by the user are:

1. Document each event of anomaly detected in Task 5.
2. Document what steps are taken to respond to the intrusion and what all was done to avoid reoccurrence of this intrusion.

The results or outputs are: All events of intrusion are well documented.

Special characteristics of the task: This is a combination of Task 5 and 6.

7.2. Task Name: Investigate and document each issue provided by users.

The Goal of this task: To investigate and document each issue provided by users.

This task is a subtask of: 7. Improve.

The subtasks that define this task are: None

The inputs or actions required by the user are:

1. Investigate problems reported by users.
2. If there is any security issue, refer to Task 6 to deal with the problem
3. Document the issue, and steps taken to fix the problem.

The results or outputs are: Problem faced by user was resolved and documented.

Special characteristics of the task: The problems faced by users may not be only security related, so it may not be relevant to this task analysis.

7.3. Task Name: Continuously update IDS system to reduce false positives

The Goal of this task: To continuously update IDS system to reduce false positives.

This task is a subtask of: 7. Improve.

The subtasks that define this task are: None

The inputs or actions required by the user are: Continuously improve the rules used by the Intrusion Detection system to reduce false positives. There will be new software and services installed in the network, so the expected network traffic will continuously change.

For example, a backup server will receive huge amounts of data from host computers during backup time at nights or weekends. This is an expected behavior, not a suspicious activity. Therefore, the rules of an intrusion detection system should not pick up this activity as being a possible intrusion. Another example is an update program running on host computers that contact outside servers periodically to receive updates.

The results or outputs are: False positives reported by the intrusion detection system have been reduced.

Special characteristics of the task: This is a repetitive task since the rules need to be changed periodically to reduce false positives.

7.4. Task Name: Keep updated on latest security issues.

The Goal of this task: The security personnel should keep updated on the latest security issues.

This task is a subtask of: 7. Improve.

The subtasks that define this task are: None

The inputs or actions required by the user are: Read updates from popular security organizations like SANS (ww.sans.org). Read security magazines to stay up-to-date with latest security issues.

The results or outputs are: Security personnel keeps updated with the latest developments in network security.

Special characteristics of the task: This is an ongoing process. Experience and knowledge gained by repeating this task frequently can be used to constantly enhance the network security in the organization.

7.5. Task Name: Continuously Improve Policy.

The Goal of this task: To continuously improve company IT policies to address new issues.

This task is a subtask of: 7. Improve.

The subtasks that define this task are: None

The inputs or actions required by the user are: For each intrusion incident, review the relevant policies by repeating task 1.

The results or outputs are: Policy is constantly updated to address new security threats.

Special characteristics of the task: This is an ongoing and repetitive task.

6. VALIDATION OF TASK ANALYSIS

The hierarchical task analysis should be validated by having users of the interface provide feedback on the usability of the newly designed interface. For our study, as we are only performing the hierarchical task analysis part of interface design, we sought feedback from various security specialists and Human Computer Interface (HCI) design specialists. The experts who were consulted are listed below.

1. ***Robert Lavin*** is the VP of Operations at Thor Solutions Inc. Thor Solutions provides information security services and develops various security products.
2. ***Larry Brophy*** is the sales executive for National Privacy Services Inc. NPSI provides businesses with information privacy consultation and services.
3. ***Tara Whalen***, is a Ph.D. student at Dalhousie University. Her expertise lies in Human Computer Interaction, and information technology security.
4. ***Kirstie Hawkey*** is a Ph.D. student at Dalhousie University whose research is in the area of Human Computer Interaction.

We expect that by reading the tasks, the security specialist will be able to verify if these tasks match common practices in the industry. The HCI specialist will be able to identify if proper consideration was made in each task for effective design of the interfaces.

6.1. Results of Validation

Comments from the security and human computer interaction experts are described below. Planned or executed improvements have been noted below each comment.

Study too broad:

The HCI and security experts were of the opinion that since many aspects of information technology security for an organization have been addressed, the study may have been too broad, and not concentrated specifically on Intrusion Detection.

For example, it may not be necessary to address policy issues in the study as it should have been assumed that necessary policy structure was already in place before the decision was made to perform Intrusion Detection. By trying to address all levels of security for the company, I may not have been able to completely concentrate on the detailed task analysis specific to only Intrusion Detection.

Policy implementation requires a seperate level of task analysis. *Developing a policy is in itself a huge undertaking for an organization.*

Business Impact Assessment (BIA):

A security expert suggested that before selecting or deciding to use IDS in an organization, it is important to perform Business Impact Assessment. This study will reveal the risks for the organization if important assets are not protected. Use the following formula to access risks.

$$R = V * T$$

Where R is Risk, V is vulnerability and T is Threat.

I have addressed this in Task 1.1.1 (Analyze Assets Risks and Vulnerabilities)

Covert Operation:

A security expert also suggested that many companies decide to perform IDS as a covert operation due to legal and privacy issues. Before performing IDS, it is recommended to consider legal issues prior to implementing it as a covert operation.

I have addressed this in Task 1.1 (Establish Policy).

Identify Threat:

A suggestion by a security expert was to identify possible channels of threat to the network. Threats may be internal or external. If most threats are identified to be from outside the network, it is recommended to concentrate on detecting traffic outside the firewall and the DMZ (Demilitarized Zone). Since internal traffic is huge, it may be a waste of the resources to monitor internal traffic if internal threat is not an issue.

This has to be addressed by the stakeholders of the company before deciding to implement an Intrusion Detection System.

Identify CERT team:

The security expert's advice was to identify the Company Emergency Response Team during the policy development stage. This team would be responsible for responding to intrusions. The team may have members of the management, network administrators, security personnel and application users. Roles and responsibilities should be clearly defined on who is in charge of decision making during crisis such as intruder break-in.

This issue has been addressed in Task 1.1.2 (Consult Management and stakeholders)

Identify specific tools:

The security experts was concerned that since the technology available for IDS is growing at a fast pace due to the high demands for security and privacy in organizations, it would be difficult to study intrusion detection without selecting few tools commonly used in the industry. For example, *"Snort"* from the open source community, and *"Sniffer"* from Network Associates Inc (NAI) are examples of some popular tools used for IDS.

The next level of study could select few of these tools, and delve deep into tasks associated with using these tools.

Host based and Network based task analysis:

The security experts stated that the tasks related to host based intrusion detection may vary significantly from that of network based intrusion detection. This study has tried to generalize both task analyses as one because of many common aspects.

Network based IDS detects anomalies in network traffic, and host based IDS detects anomalies in the state of systems. Different tools are used to accomplish both goals, so it would be beneficial if separate task analysis are performed for each type of IDS.

7. CONCLUSION AND FURTHER STEPS

By performing this study, we have identified tasks performed by network security administrators to maintain a secure network infrastructure. We have recognized many common tools used to perform these tasks. There is a wide variety of tools that are often integrated to produce meaningful information that can be analyzed. For example, logs produced by many servers are sent to a central server, and monitored by a log monitoring software. Since this is accomplished by integrating different software, there is a lot of opportunity to develop better user interfaces that will allow users to easily monitor and operate all tools from a single central interface.

Intrusions are detected based on anomaly detected from normal network or system performance. There is opportunity for better design of tools that will allow security specialists to graphically monitor network traffic for irregularities. These graphical user interfaces will allow administrators to become easily familiarized to normal and abnormal usage of resources.

Some suggestions for further research in HCI design for Intrusion Detection Systems are:

- Delve deeper into specific tasks related to Host based and Network based intrusion detection. Select widely used tools such as *snort*, *sniffer*, or *tripwire*, and study tasks related to using these tools everyday for intrusion detection. This will allow us to develop a hierarchical task analysis that shows detailed decomposition of the intrusion detection function.
- Design graphic user interfaces to display possible anomalies in network traffic and system resource usage. These interfaces will allow the security administrator to visually determine if an intrusion is in progress more easily. This will also allow the administrator to become familiar with the usual network traffic patterns.
- Design user interface to inspect multiple log files generated by servers, routers, firewall, and IDS systems. This form of interface would allow administrators to easily inspect the log files from various sources for interesting patterns in log files that would help in detecting an anomaly.

8. REFERENCES

[1] Verton, D. (2001, November 26) Security Experts: Users Are the Weakest Link. Retrieved April 14, 2004, from <http://www.computerworld.com/securitytopics/security/story/0,10801,66047,00.html>

[2] SANS Institute (2003, June 12) Intrusion Detection FAQ. Retrieved April 14, 2004, from <http://www.sans.org/resources/idfaq/index.php>

[3] Marchette, D. J. (2001) Computer Intrusion Detection and Network Monitoring a Statistical Viewpoint, 98–106.

[4] CERT Coordination Center (2004) CERT® Security Practices. Retrieved April 14, 2004, from <http://www.cert.org/security-improvement/practices/practices.html>

[5] Windows Security (2004) Event Log Monitoring. Retrieved April 14, 2004, from <http://www.windowsecurity.com/software/Event_Log_Monitoring/>

[6] Kipp, J. (2004) Using Snort as an IDS and Network Monitor in Linux. Retrieved April 14, 2004, from <http://www.giac.org/practical/gsec/James_Kipp_GSEC.pdf>

[7] SANS Institute (2003, June 12) What is host-based intrusion detection? Retrieved April 14, 2004, from <http://www.sans.org/resources/idfaq/host_based.php>

[8] Tripwire, Inc. (2004) Change Monitoring and Reporting Systems. Retrieved April 14, 2004, from <http://www.tripwire.com/products/index.cfm>

[9] Microsoft Corporation (2004) Description of Windows XP and Windows Server 2003 System File Checker. Retrieved April 14, 2004, from <http://support.microsoft.com/?kbid=310747>

[10] Hackos J. T., Redish J. C (1998) User and Task Analysis for Interface Design, 21-50

9. BIBLIOGRAPHY

[1] Internet Security Systems (2004) Network- vs. Host-based Intrusion Detection. Retrieved April 14, 2004, from <http://documents.iss.net/whitepapers/nvh_ids.pdf>

[2] CERT Coordination Center (2004) Securing Network Servers. Retrieved April 14, 2004, from <http://www.cert.org/security-improvement/modules/m10.html>

[3] CERT Coordination Center (2004) Identify data that characterize systems and aid in detecting signs of suspicious behavior. Retrieved April 14, 2004, from <http://www.cert.org/security-improvement/practices/p091.html>

[4] CERT Coordination Center (2004) Eliminate all means of intruder access. Retrieved April 14, 2004, from <http://www.cert.org/security-improvement/practices/p050.html>

[5] CERT Coordination Center (2004) Analyze all available information to characterize an intrusion. Retrieved April 14, 2004, from <http://www.cert.org/security-improvement/practices/p046.html>

[6] IPTraf (2004) IP Network Monitoring Software. Retrieved April 14, 2004, from <http://cebu.mozcom.com/riker/iptraf/>

[7] Song D. (September 17, 1999) Intrusion Detection 101 Retrieved April 14, 2004, from <http://monkey.org/~dugsong/talks/ids/>

[8] Marchette D. (April 12, 1999) A Statistical Method for Profiling Network Traffic. Retrieved April 14, 2004, from http://www.usenix.org/publications/library/proceedings/detection99/full_papers/marchette/marchette.pdf

[9] Dix A., Finlay J., Abowf G., Beale R. (1997) Human Computer Interaction Second Edition.