White Paper

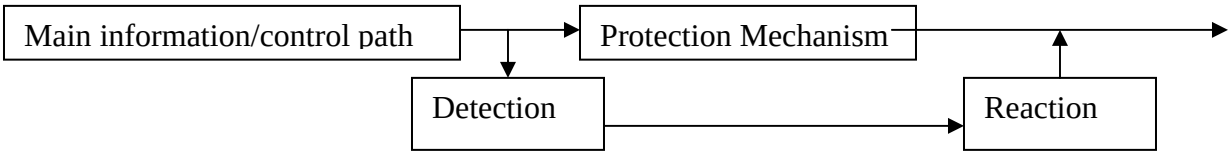
Information Security -- Intrusion Detection

For further details as to the process and the procedures followed, contact:

Computer Technology Associates, Inc.
INFOSEC Group
7150 Campus Drive, Suite 100
Colorado Springs, CO 80920
(719) 590-5100

1. INTRODUCTION.

A useful architecture for the purpose of understanding an enterprise's security posture is[1]:



Protection mechanisms such as firewalls, password controls, cipher locks and cryptography are designed to deny access. Detection mechanisms such as intrusion detection systems (IDS) look for signs of attack, improper activity or policy non-compliance, and reaction mechanisms, such as automated system reconfigurations to deny access to an attacker, or triggering email (if not on the same system) or phone/ pager notifications to appropriate staff, respond via a predefined set of rules for action in the event that a violation of security policy does in fact occur. As indicated in the diagram, for detection and reaction to be effective, they must operate on a parallel and independent path to the protection mechanism. It is an accepted information security principal that in today's ever-changing technological landscape, (faster computers, higher bandwidth, new attack tools, etc.), protective mechanisms cannot provide 100% protection. As a result one cannot count on protective mechanisms to assure adequate security of mission critical assets. For the adequate protection of such assets, requirements that assure real-time detection and response capabilities may be necessary. For example, one could require that that in the event of a detected intrusion, the system launch security assessment scans against other segments of the enterprise to detect other vulnerabilities to that type of attack, and automatically reconfigure the network to block misuse. The ability of a system to automatically detect an event requiring such response may itself be a challenge, frequently requiring the correlation and analysis of data from multiple security devices (e.g., IDSs, firewalls, routers) to accurately detect an attack from a multitude of "false positives".

We believe that the goal of enterprise's intrusion-detection capability should be to provide a real time consolidated view of an enterprise security posture to facilitate an effective incident response capability. This will require:

a. Real time intrusion-detection.

b. Centralized, remote monitoring of disparate intrusion-detection sensors. Sensors include devices specifically designed for detecting unauthorized network activity in real time such as RealSecure. Non-real time sensors such as component audit trails, component logs, firewall alarms, etc., should all be part of the intrusion-detection capability. The ability to more accurately detect suspicious or anomalous activity based on corroborating events from multiple sources.

c. Detection of internal attacks and misuse as well as external attacks using the same sensors.

d. Reports of attack and misuse in real time with timely reaction mechanisms in place designed to mitigate risk of loss.

e. Features to automatically block attacks.

We provide a full range of network intrusion-detection services. We normally recommend that clients use a five-step process to develop their intrusion-detection capability. This process is shown in Figure 1. We start by collecting information about the network and assessing the enterprise's current capability to detect intrusions. We determine the enterprise's internal and external connectivity, current intrusion-detection capability, and the enterprise's intrusion-detection shortcomings and needs. Next, we customize an intrusion-detection and monitoring system to improve the enterprise's intrusion-detection capabilities. We use a pilot installation step to evaluate the capability's design on a small scale. Since

[1] Winn Schwartau, "Time Based Security", Interpact Press, 1999

there are no "turn-key" intrusion-detection capability systems, this step lets us refine the capability and confirm that the recommended capability meets the client's needs. We recommend that the pilot intrusion-detection installation be conducted on one of the client's network segments, but the pilot may be conducted in the CTA laboratory at Colorado Springs. In Colorado Springs, we can install sensors and monitor them in a controlled environment. In the next step, we install or assist the client in installing sensors and other intrusion-detection capability components on the client's network. We can integrate the monitoring system into the client's network operations center, develop an Intrusion-Detection Operations Center or integrate monitoring into the CTA Assessment Center. As sensors are installed or activated, monitoring and alarm response begins. If CTA is monitoring the client's intrusion-detection capability, we also conduct periodic assessments of sensor operation and the monitoring system.

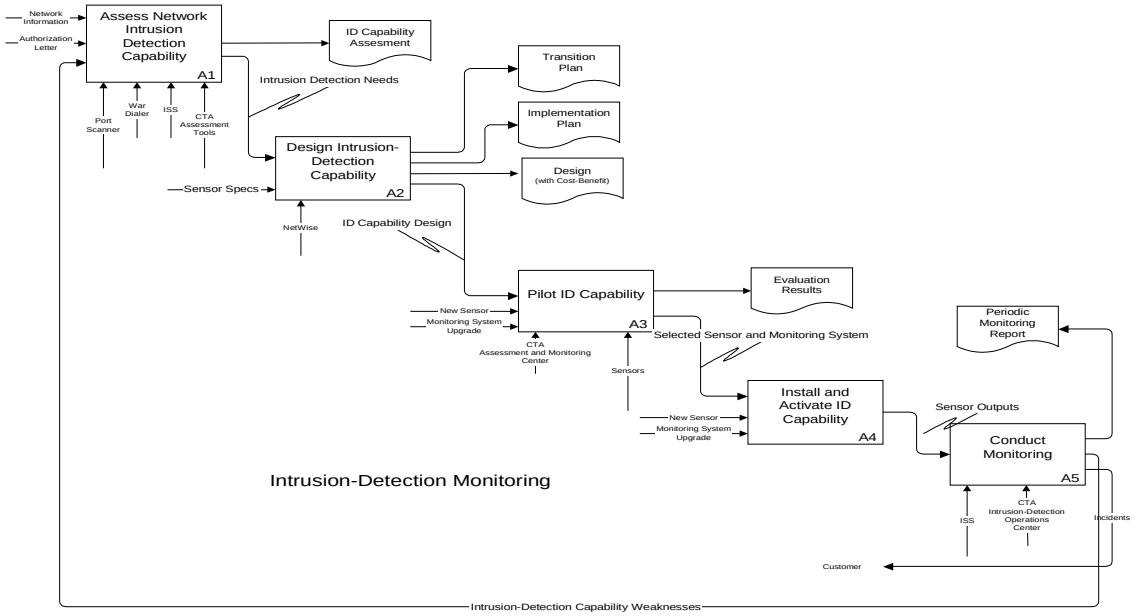


Figure 1 – Intrusion-Detection Capability Development

2. ASSESS NETWORK INTRUSION DETECTION CAPABILITY

2.1. Objectives

The objective of the network assessment is to determine the intrusion detection capability already in existence and determine obvious vulnerabilities that can be easily corrected.

2.2. Process

The first activity is to negotiate the appropriate authorizations to assess the intrusion detection capabilities present. This is necessary to protect both parties during an intrusion test. It will specifically delimit the activities to be undertaken by CTA in assessing the current capability to detect intrusions.

The next step is to gather information about the network to determine the appropriate intrusion entry points and possible weaknesses.

CTA will then use a variety of penetration tools to assess the ability to intrude into the enterprise system. Obvious vulnerabilities will be identified during this period as well. The penetration phase will be coordinated with enterprise monitors to prevent improper reactions to the penetration attempts.

2.3. Deliverables

A summary report of current intrusion detection capability and obvious vulnerabilities will be prepared. Recommendations to reduce the vulnerabilities will be included.

3. CUSTOM DESIGN AN INTRUSION DETECTION CAPABILITY

3.1. Objectives

Bases on the needs of the enterprise, a custom design of intrusion detection capability will be prepared.

3.2. Process

From the findings in the assessment phase, a design for providing appropriate intrusion detection capabilities will be prepared. It is based on the protection necessary for the enterprise, the existing capabilities, and the identified enhancements needed.

Sensor specifications will be prepared to guide the installation and configuration of the intrusion detection package.

From the available intrusion detection software, appropriate packages will be recommended, including a cost-benefit analysis of the various choices.

3.3. Deliverables

Three reports will be prepared during this design phase: a Transition Plan, an Implementation Plan, and an Intrusion Detection Design. The plans may be combined.

The Transition Plan will detail how to move from the current intrusion detection capability to the desired level without increasing the short-term vulnerability to penetration.

The Implementation Plan will identify the steps and processes to install and integrate the additional capabilities into the existing system. It will provide specific guidance as to configuration of the sensors.

The Design Plan will include options and recommendations, based on a cost-benefit analysis of the available packages that meet the needs of the enterprise.

4. DEVELOP AND DEMONSTRATE INTRUSION-DETECTION CAPABILITY IN A PILOT OPERATION

4.1. Objectives

The objective is to demonstrate the improved intrusion-detection capability on a small scale in a laboratory environment or on a single network segment or subnet. This is the initial validation of the capability.

4.2. Process

In this step, the enterprise acquires, or we assist the enterprise in acquiring a demonstration intrusion-detection capability. Normally, we want to conduct a pilot on a small scale before implementing the final solution. Since each intrusion-detection capability is different and builds on the enterprise's current capabilities, the pilot acts as a shake down for intrusion-detection capability to include equipment staging, installation, and operation. During pilot operation we conduct attacks on the pilot installation. These attacks help us evaluate the intrusion-detection capability.

Develop and Demonstrate Intrusion-Detection Capability in a Pilot Operation. The pilot operation is an optional task depending on the desires of the customer. We always recommend demonstrating the improved intrusion-detection capability on a small scale in a laboratory environment or on a single network segment or subnet. This provides validation of the effectiveness of the capability.

Step 1. Obtain system components (e.g., sensors, monitoring hardware and software, etc.).

Step 2. Stage components.

Step 3. Conduct site survey.

Step 4. Install, configure, and/or activate sensors on a network segment at the enterprise site or

at CTA.

Step 5. Conduct the pilot.

Step 6. Prepare an Evaluation Report

Step 7. Update the Implementation and Transition Plan.

4.3. Deliverables

The deliverables are an Evaluation Report that includes problems discovered and recommendations on how to fix the problems and an updated Implementation and Transition Plan.

5. INSTALL THE INTRUSION-DETECTION CAPABILITY.

5.1. Objectives

The objectives are to install the improved intrusion-detection capability and to test the capability.

5.2. Process

In this step, the enterprise updates the intrusion-detection capability design based on the evaluation report from the pilot. The monitoring center is upgraded or established first. Without any knowledge of the traffic at the enterprise sites or the enterprise monitoring goals we believe that the monitoring center for the enterprise could consist of a primary monitoring station and an alternate. We stage, install, and activate sensors and other intrusion-detection components incrementally. Then sensors are brought on line and tested incrementally.

Install the Intrusion-Detection Capability. This process installs and tests the intrusion-detection capability at each site.

Step 1. Update the design based on the pilot or new knowledge.

Step 2. Verify and coordinate the installation and activation schedule.

Step 3. For monitoring system installation

- Conduct site survey.
- Obtain components.
- Stage components.
- Install and test monitoring hardware and software.

Step 4. For sensor installation

- Conduct site survey.
- Obtain components.
- Stage components.
- Install, configure, activate, and test sensors on network segments at the enterprise sites.

5.3. Deliverables

The deliverables are an updated design and an updated Implementation and Transition Plan that includes an installation and activation schedule and an operational intrusion-detection capability.

6. CONDUCT MONITORING

6.1. Objectives

The objectives are to detect internal attacks and misuse as well as external attacks.

6.2. Process

In this step, CTA, or the enterprise begins full 7x24 hour monitoring of the enterprise's intrusion-detection capability or on a schedule determined with the enterprise.

Sensors are normally installed at all points of external network connectivity to include modem pools. Sensors may also be installed on critical subnets and as agents on critical components. Once an intrusion-detection sensor is installed, its outputs must be constantly monitored. The enterprise may choose to monitor the network's intrusion-detection capability or CTA can monitor intrusion-detection sensors from the Assessment Facility in Colorado Springs or at the enterprise. When the network's intrusion-detection capability includes non-real time sensors such as firewall logs, NT security logs, Sun log files, Web server logs, router logs, and other server and component logs, monitoring includes periodic review of these sensor outputs. In any case, we call the monitoring center, the Intrusion-Detection Operations Center (I-DOC). The I-DOC monitors operation of the deployed sensors and network connectivity. When a real time sensor identifies an event (e.g., attack or misuse), the sensor generates an automatic alarm to the I-DOC. When a review of a log file or other non-real time sensor output detects an event (e.g., attack or misuse), the reviewer generates an incident report. Based on alarms generated by sensors and analysis of network component logs and audit trails, the I-DOC identifies and verifies unauthorized activity. The event processing rules can generate alarms based on a combination of events such as:

- The source and/or the target of network activity (e.g., source or destination IP address, web or DNS server target)
- The type of network activity (e.g., attempt to exploit a known vulnerability)
- Frequency of events or types of events received over a given period of time that contrast significantly with normal site profiles.

I-DOC personnel respond to the alarm and try to identify the type of event, attack target, attack procedures, source of attack, and other information about the event. Intrusion-Detection Operations Center personnel perform an initial assessment of the event. The Intrusion-Detection Operations Center notifies personnel in accordance with pre-approved enterprise procedures. The I-DOC responds to the activity based on procedures established with the enterprise.

Personnel at the I-DOC also assess whether the sensors and monitoring system are working properly. The I-DOC periodically tests the intrusion-detection capability by attempting to penetrate the network. Internal and external assessments can help determine the current network's capabilities to detect and report unusual events. Once an intrusion-detection system is operational, we continually assess the intrusion-detection system’s ability to detect hostile events.

Conduct Monitoring. If we provide monitoring then we provide monitoring at the I-DOC once sensors are installed, activated, and tested. The monitoring process is outlined below.

Step 1. Monitor sensors 7x24 or on a schedule determined with the enterprise. Monitoring sensors includes notifying the enterprise's network operations center of alarms. Monitoring other components of the intrusion-detection capability such as firewalls logs, and audit trails.

Step 2. Analyze logs and audit trails for signs of attack or misuse.

Step 3. Prepare and dispatch incident reports.

Step 4. Respond to attacks and misuse.

Step 5. Scheduled assessment of the enterprise's intrusion-detection capability. Test the intrusion-detection capability and prepare an assessment report.

Step 6. Prepare periodic monitoring report.