
*Financial
Services
Security*



*Monitoring and
Intrusion Detection
Systems Profile*

Technical Contact Information

If further information regarding technical content is required, please contact:

Financial Services Security Lab

Tel: (202) 289-4322

Fax: (202) 289-3562

bits@fsround.org

Originating Author: Bret Sigillo, Regional Director, Predictive Systems, Inc.

Profile Leader / Workgroup Chair: Howard Taylor, Vice President, Enterprise Technology Processing, Manager – eSpace Security Center, JP Morgan Chase & Co.

BITS Security Lab “Monitoring and IDS” Workgroup members (primary contributors/organizations identified in bold):

Representative	Organization	Representative	Organization
Jim Brown	M&I Corporation	Carl Kriegel	PNC Bank
Wayne Browning	Summit	Steve Scott	Wachovia
Brian Ekkebus	Northern Trust	Craig Shorter	First Tennessee
Gene Fredriksen	Raymond James Financial	Bob Vonderheid	Comerica
Eric Guerrino	Bank of New York	David Voris	Wells Fargo
Jim Keatts	First Virginia Banks, Inc.	Karla Warne	PNC Bank
Colin Meagher	JP Morgan Chase		

Profile Feedback

If you have comments regarding this profile, please send an email to bits@fsround.org. Include the profile name, your name, email address, telephone and fax number, and indicate whether you would like to be contacted. *Please note: BITS Security Lab Inc. will take all comments under advisement, but reserves the right to include or exclude comments received in the final criteria.*

Monitoring and Intrusion Detection Systems Profile – Version Control History

*Note: **Bold** in Version column indicates a Public Release*

Version / Date	Changes
0.90 – 0.92 (Apr 2000)	Creation of Initial Draft (Global Integrity/Telcordia)
1.00 (May 2000)	Initial Draft Distribution – BITS/Profile Leader (WG Chair)/Global Integrity
1.01-1.02 (May/June 2000)	Working Copy Draft – Distribution/Review by Financial Industry Profile Work Group
1.03-1.13 (Dec 2000 – Apr 2001)	Working Copy Draft – Distribution/Review by Financial Industry, Technology Providers and Industry Experts
1.14 (Nov 2001)	Final Draft – Posting for public comment and ready for testing

Table of Contents

TABLE OF CONTENTS	III
1. INTRODUCTION.....	1
1.1. OVERVIEW.....	1
1.2. BOUNDARIES AND UNDERLYING PLATFORMS.....	2
1.3. MANDATORY AND DESIRED CRITERIA.....	2
1.4. TEST PLANS AND PROFILES	3
1.5. COMMON TERMS USED IN THIS PROFILE.....	3
2. REQUIRED CRITERIA FOR ADMINISTRATION AND OPERATION OF MONITORING AND INTRUSION DETECTION SYSTEMS	5
2.1. SECURITY FEATURES.....	5
3.0. PRODUCT FUNCTIONALITY	16
4.0. SCALABILITY	16
3. REQUIRED FUNCTIONAL CRITERIA FOR ALL MONITORING AND INTRUSION DETECTION SYSTEMS.....	18
3.1. INTRODUCTION.....	18
3.2. MANAGER/AGENT COMMUNICATION.....	18
3.3. ANOMALOUS BEHAVIOR DETECTION.....	19
3.4. SYSTEM CORRECTIVE ACTIONS.....	21
3.5. SYSTEM PROGRAMMABILITY	21
3.6. REPORTING AND TREND ANALYSIS.....	23
3.7. SYSTEM ENHANCEMENTS.....	24
4. DESIRED FUNCTIONAL CRITERIA FOR ALL MONITORING AND INTRUSION DETECTION SYSTEMS.....	26
4.1. INTRODUCTION.....	26
4.2. MANAGER/AGENT COMMUNICATION.....	26
4.3. ANOMALOUS BEHAVIOR DETECTION.....	26
4.4. SYSTEM PROGRAMMABILITY	27
5. FUNCTIONAL CRITERIA FOR MONITORING AND INTRUSION DETECTION SYSTEMS PRODUCT SUB-CLASSES.....	28
5.1. INTRODUCTION.....	28
5.2. FUNCTIONAL CRITERIA FOR NETWORK INTRUSION DETECTION	29
5.3. FUNCTIONAL CRITERIA FOR HOST BASED INTRUSION DETECTION	30
5.4. FUNCTIONAL CRITERIA FOR APPLICATION-BASED INTRUSION DETECTION	31
APPENDIX A: INDUSTRY STANDARDS.....	33
APPENDIX B: BIBLIOGRAPHY.....	34
APPENDIX C: GLOSSARY OF TERMS.....	35
APPENDIX D: INTRUSION DETECTION SYSTEMS THREAT CLASSES.....	41

1. Introduction

1.1. Overview

This Monitoring and Intrusion Detection Systems Profile defines the security requirements to support the technical analysis of monitoring and intrusion detection systems (IDS). Examples of monitoring and intrusion detection systems include network- and host-based IDS. The product profile identifies the criteria set, which is derived from the BITS Lab Master Security Criteria¹ that apply to monitoring and intrusion detection systems. The criteria in the profile are applicable to the features and functions normally found in monitoring and intrusion detection systems. When applicable, after each requirement, there will be a link to the related section and specific requirements in the Master Security Criteria.

Corporate computing environments have become an extensively distributed architecture. The efficiency and speed of modern networks has allowed computing resources to be located virtually anywhere. The task of monitoring and IDS systems is to monitor networks and hosts for normal operation. The ability to detect and alert the appropriate staff to the presence of anomalous behavior are key criteria.

Because there are a variety of monitoring and IDS technologies, a single set of criteria may not apply equally to all of them. Hence, this profile is divided into two parts: The first lists criteria that are common to all technologies, and the second lists criteria that are specific to different classes of available technologies.

There are two general types of intrusion detection systems, network-based and host-based. Network-based IDS focuses on detection of suspicious network activities. Observed network activity is compared to known attack signatures or anomalies are determined using heuristic algorithms. When a close match is obtained, an alert can be generated. Host-based IDS focuses on detection of unauthorized activities at the system level.

For the purposes of this profile, the basic model for a product in this class is a manager-agent based arrangement with the manager interfacing with one or more agents to collect data. The manager and agent must

¹ The MSC defines the master set of requirements (e.g. security features, functionality, usability and scalability) that will support the technical analysis of a given product.

authenticate each other. All sensitive communication between agent and manager must be encrypted, while standard communication must be protected in a manner commensurate with the sensitivity of the information. An agent can be a dedicated device such as a network scanning engine or probe. In the case of a host-based IDS, agents will in general be a host that has proprietary software installed. All of the systems need to be able to use a variety of methods to alert the appropriate staff to the presence of anomalous behavior, and at a minimum, to collect historical data so that it can be used to distinguish patterns and provide trend analysis.

1.2. Boundaries and Underlying Platforms

A number of criteria outlined in this document may be addressed through security features of any system component, rather than the Monitoring and Intrusion Detection Systems itself. Rather than requiring all security functionality to be provided by the stand-alone system, the criteria and process allow for the product to rely on an underlying platform (e.g., an operating system) or supporting components for specific security requirements. To support this approach, the process allows the Technology Provider and the Testing Lab to define the “boundaries” of the test environment, which delineates the system to be tested. It is anticipated that this boundary will include the product itself, the underlying platform, and any relying application or system. It is important to note, however, that the criteria will be applied to all components within that boundary.

Additionally, if the system uses any cryptographic algorithm not identified in Appendix A, “Industry Standards,” then it shall be configurable to also allow the use of an acceptable algorithm in place of the unlisted algorithm. Systems that do not have this flexibility will be disqualified from the BITS validation process.

1.3. Mandatory and Desired Criteria

Each criterion will be identified as being *required* or *desired*². A product will earn the *BITS Tested Mark* only if it meets all of the *required* criteria within Section 2, “Criteria for the Administration and Operation of Monitoring and Intrusion Detection Systems Products,” Section 3, “Required Functional Criteria for All Monitoring and Intrusion Detection Systems Products,” and the appropriate subclass of Section 5, “Functional Criteria for Monitoring and Intrusion

² A criterion shall be considered *required* unless it is explicitly identified as being *Desired*.

Detection Systems Product Subclasses.” In other words, a product will not merit a *BITS Tested Mark* if it misses a single required criterion. Please note that the BITS Financial Services Security Lab employs a “Pass/Withdrawal” testing process.

In this document, *required* criteria use the verb “shall,” while *desired* criteria use the verb “should.”

The criteria identified in this profile as *desired* are not required for the *BITS Tested Mark*, but compliance with these criteria will be noted in the final Test Report. *Desired criteria are recognized by the financial services industry as advantageous and may become requirements in the future.*

1.4. Test Plans and Profiles

It is important to note that actual testing of individual products will be conducted against a test plan produced from this profile. Each product undergoing testing will have a specific test plan developed. *It is entirely possible that certain criteria will be implemented differently, and thus tested differently, in two similar products.*

Monitoring and Intrusion Detection systems will be tested within a standard configuration and environment that will include a manager-agent arrangement. The manager and agent will each consist of any agreed upon supporting platform and user interfaces.

1.5. Common Terms Used in this Profile

In this section, we will list definitions of terms that are important or frequently used in the remainder of the profile. See “Appendix C: Glossary of Terms” for a complete listing of terms used.

TERM	DEFINITION
administrator	Taken in the context of this profile and if used without pre-qualification, this term indicates any user or group of users that could be defined as a system administrator and/or product administrator, typically having privilege beyond the scope of an end user. See also “end user,” “user” and “product administrator.”
agent	A specialized piece of software or hardware that collects data and interprets it, usually relative to security or, in the case of network management stations, relative to up/down status of a device or system.
end-user	Taken in the context of this profile and unless otherwise indicated, “end user” is the individual who uses the system after it has been fully developed. The term distinguishes the user for which the product is designed from the developers, installers and administrators who are making the product available for the end user. See also “user” and “administrator.”
manager	A console that controls the system by allowing configuration changes and active

TERM	DEFINITION
	commands. The manager is responsible for communicating with the agents, collecting information from them, and then storing or performing actions once the data has been received.
product administrator	In the scope of this document, the roles associated with higher privilege at the product's configuration level (may or may not be the same as the system administrator).
system	Within the scope of this profile, "system" is used to imply the totality of the product and the mediation devices (if any) that need to be tested. A system is defined as being a combination of manager and agent components, any monitoring station used to view manager information, and the underlying hardware and operating system. At a minimum, there would be one instance of manager and agent components to form a system. These components may be installed on one or more physical devices.
system administrator	An individual (user) who has higher privilege at the operating system level. Being a system administrator, while implying additional product administration capabilities, does not necessarily imply that product administration capabilities have been authorized. This distinction is necessary in the case where separation of duties exists between a system administrator and a security officer.
user	In the context of this profile and used without pre-qualification, this term indicates any and all users, such as an end user, product user-ID or system user.
user-ID	A number or name unique to a particular user of a computer or group of computers that share user information. The operating system uses the user ID to represent the user in its data structures, e.g., the owner of a file or process or the person attempting to access a system resource.

2. Required Criteria for Administration and Operation of Monitoring and Intrusion Detection Systems

2.1. Security Features

This section lists the security criteria from the Master Security Criteria document that are common to all products and specifically apply to the administration and operation of products in this class. The criteria are grouped according to the functionality provided by a typical monitoring and intrusion detection system. This results in the following groups listed below. Examples of the functionality are also listed for each group. The criteria are categorized according to the following major sections in the Master Security Criteria:

1. Identification
2. Authentication
3. Authorization
4. Confidentiality
5. Data Integrity
6. Audit
7. Data Disposal
8. System Integrity
9. Security Administration
10. Guidance
11. Non-repudiation

MSC REFERENCE	REQUIRED, DESIRED OR N/A	COMMENT OR RATIONALE
MSC Section 2.1: Identification³		
Note: Criteria in this section are applicable to the <u>administration and operation of the product</u> , unless specifically identified in the “Comment or Rationale” column.		
2.1.1	Required	
2.1.2	Desired	
2.1.3	Desired	
2.1.4	Required	
2.1.5	Required	
2.1.6	Desired	

MSC REFERENCE	REQUIRED, DESIRED OR N/A	COMMENT OR RATIONALE
MSC Section 2.2: Authentication⁴		
Note: Criteria in this section are applicable to the <u>administration and operation of the product</u> , unless specifically identified in the “Comment or Rationale” column.		
Subsection 2.2.1: General Mechanism Requirements		
2.2.1.1	Required	
2.2.1.2	Required	
2.2.1.3	Required	
2.2.1.4	Required	
2.2.1.5	Desired	
2.2.1.6	Required	

³ “identification” is defined as: The system shall have the capability of associating a user with an unambiguous identifier (e.g., user-ID) by which the said user shall be held accountable for the actions and events initiated by that user.

⁴ “Authentication” is identified as: The system shall offer features to verify the claimed identity of a user before allowing system access to the said user.

MSC REFERENCE	REQUIRED, DESIRED OR N/A	COMMENT OR RATIONALE
MSC Section 2.2: Authentication⁴ Note: Criteria in this section are applicable to the <u>administration and operation of the product</u> , unless specifically identified in the “Comment or Rationale” column.		
2.2.1.7	Required	
2.2.1.8	Required	
Subsection 2.2.2: Knowledge- and Possession-based Mechanism Requirements		
2.2.2.1	Required	
2.2.2.2	Required	
2.2.2.3	Required	
2.2.2.4	Required	
2.2.2.5	Required	
2.2.2.6	Required	
2.2.2.7	Required	
2.2.2.8	Required	
2.2.2.9	Required	
2.2.2.10	Required	
2.2.2.11	Required	
2.2.2.12	Required	
Subsection 2.2.3: Personal Characteristics-based Mechanism Requirements (DESIRED) NOTE: The classification of “DESIRED” for this entire subsection indicates that the product submitted for evaluation may not need to comply with the criteria in this section. For the product to be recognized as providing “personal characteristics-based authentication mechanisms,” it is <u>not</u> an optional section; thus, if the product is claiming it provides these functions, it must fully comply with all criteria in this subsection (2.2.3).		
2.2.3.1	Required	<i>See note above.</i>
2.2.3.2	Required	<i>See note above.</i>
2.2.3.3	Required	<i>See note above.</i>

MSC REFERENCE	REQUIRED, DESIRED OR N/A	COMMENT OR RATIONALE
MSC Section 2.3: Authorization⁵ Note: Criteria in this section are applicable to the <u>administration and operation of the product</u> , unless specifically identified in the “Comment or Rationale” column.		
2.3.1	Required	
2.3.2	Required	
2.3.3	Required	
2.3.4	Required	
2.3.5	Required	
2.3.6	Required	
2.3.7	Required	
2.3.8	Required	
2.3.9	Required	
2.3.10	Required	
2.3.11	Required	
2.3.12	Required	
2.3.13	Required	
2.3.14	Required	
2.3.15	Required	
2.3.16	Required	
2.3.17	Required	
2.3.18	Required	
2.3.19	Required	<i>There are unique security risks inherent in a manager-agent architecture. In many situations, there may be a</i>

⁵ “Authorization” is identified as: The system shall offer features to support the following restrictions: no user shall be allowed access to the system without Identification and Authentication; no user shall be allowed access to a resource (e.g., transaction, data, process, etc.) of the system unless specifically authorized to do so.

MSC REFERENCE	REQUIRED, DESIRED OR N/A	COMMENT OR RATIONALE
MSC Section 2.3: Authorization⁵		
Note: Criteria in this section are applicable to the <u>administration and operation of the product</u> , unless specifically identified in the “Comment or Rationale” column.		
		<i>need to restrict concurrent logons for both security and consistency purposes. In some systems, concurrent logins can be used to mask unauthorized activity.</i>
2.3.20	Required	

MSC REFERENCE	REQUIRED, DESIRED OR N/A	COMMENT OR RATIONALE
MSC Section 2.4: Confidentiality⁶		
Note: Criteria in this section are applicable to the <u>administration and operation of the product</u> , unless specifically identified in the “Comment or Rationale” column.		
2.4.1	Required	
2.4.2	Required	
2.4.3	Required	
2.4.4	Required ⁷	
2.4.5	Required	
2.4.6	Required	
2.4.7	Required	
2.4.8	Required	
2.4.9	Required	

⁶ “Confidentiality” is identified as: The system shall offer features to ensure that sensitive information shall be communicated and stored in a way such that only authorized users are allowed access.

⁷ An attack can be considered impractical if the cost of the attack exceeds the value of the potential benefits gained by a successful breach.

MSC REFERENCE	REQUIRED, DESIRED OR N/A	COMMENT OR RATIONALE
MSC Section 2.4: Confidentiality⁶		
Note: Criteria in this section are applicable to the <u>administration and operation of the product</u> , unless specifically identified in the "Comment or Rationale" column.		
2.4.10	Required	
2.4.11	Required	
2.4.12	Required	
2.4.13	Required	
2.4.14	Required	

MSC REFERENCE	REQUIRED, DESIRED OR N/A	COMMENT OR RATIONALE
MSC Section 2.5: Data Integrity⁸		
Note: Criteria in this section are applicable to the <u>administration and operation of the product</u> , unless specifically identified in the "Comment or Rationale" column.		
2.5.1	Required	
2.5.2	Required	
2.5.3	Required	
2.5.4	Required	
2.5.5	Required	

⁸ "Data integrity" is identified as: The system shall offer features to ensure that either: the data shall not be modified or altered without authorization in either storage or in transit; or any unauthorized modification of data shall yield an auditable security-related event.

MSC REFERENCE	REQUIRED, DESIRED OR N/A	COMMENT OR RATIONALE
MSC Section 2.5: Data Integrity⁸		
Note: Criteria in this section are applicable to the <u>administration and operation of the product</u> , unless specifically identified in the “Comment or Rationale” column.		
2.5.6	Required	
2.5.7	Required	
2.5.8	Required	
2.5.9	Required	
2.5.10	Required	

MSC REFERENCE	REQUIRED, DESIRED OR N/A	COMMENT OR RATIONALE
MSC Section 2.6: Audit⁹		
Note: Criteria in this section are applicable to the <u>administration and operation of the product</u> , unless specifically identified in the “Comment or Rationale” column.		
2.6.1	Required	
2.6.2	Required	
2.6.3	Required	
2.6.4	Required	
2.6.5	Required	
2.6.6	Required	
2.6.7	Required	
2.6.8	Required	

⁹ “Audit” is identified as: The system shall offer features to support the following functions: maintain a history file (also called an Audit Log) that records all security-related events pertinent to establishing an audit trail for a “post-mortem” analysis of a suspected security breach; ensure integrity of the audit log; generate customized audit reports; protect audit log(s) from unauthorized access; support administrator-selectable alerts for specified security-related events; support audit records of administrative events.

MSC REFERENCE	REQUIRED, DESIRED OR N/A	COMMENT OR RATIONALE
MSC Section 2.6: Audit⁹		
Note: Criteria in this section are applicable to the <u>administration and operation of the product</u> , unless specifically identified in the “Comment or Rationale” column.		
2.6.9	Required	
2.6.10	Required	
2.6.11	Required	
2.6.12	Required	

MSC REFERENCE	REQUIRED, DESIRED OR N/A	COMMENT OR RATIONALE
MSC Section 2.7: Data Disposal¹⁰		
Note: Criteria in this section are applicable to the <u>administration and operation of the product</u> , unless specifically identified in the “Comment or Rationale” column.		
2.7.1	Required	
2.7.2	Required	
2.7.3	Required	

¹⁰ “Data disposal” is identified as: The system shall ensure that there is no residual data exposed to unauthorized users as resources are allocated to those data objects or released from those data objects.

MSC REFERENCE	REQUIRED, DESIRED OR N/A	COMMENT OR RATIONALE
MSC Section 2.8: System Integrity¹¹		
Note: Criteria in this section are applicable to the <u>administration and operation of the product</u> , unless specifically identified in the “Comment or Rationale” column.		
2.8.1	Required	
2.8.2	Required	
2.8.3	Required	
2.8.4	Required	
2.8.5	Required	
2.8.6	Required	
2.8.7	Required	
2.8.8	Required	
2.8.9	Required	
2.8.10	Required	
2.8.11	Required	
2.8.12	Required	

MSC REFERENCE	REQUIRED, DESIRED OR N/A	COMMENT OR RATIONALE
MSC Section 2.9: Security Administration¹²		
Note: Criteria in this section are applicable to the <u>administration and operation of the product</u> , unless specifically identified in the “Comment or Rationale” column.		

¹¹ “System integrity” is identified as: The system shall offer features to support the following functions: perform integrity checks for system functions; retain the security parameters after the occurrence of events such as system restart, disaster recovery, arrival of sensitive dates related to the Y2K issue, etc.; provide the back-up capability to restore the system, when necessary, to a well-defined state (such as the need to undo modifications to a file or to undo transactions); ensure that security features are always invoked and may not be bypassed unless authorized and configured to do so.

MSC REFERENCE	REQUIRED, DESIRED OR N/A	COMMENT OR RATIONALE
MSC Section 2.9: Security Administration¹²		
Note: Criteria in this section are applicable to the <u>administration and operation of the product</u> , unless specifically identified in the "Comment or Rationale" column.		
2.9.1	Desired	
2.9.2	Required	
2.9.3	Required	
2.9.4	Required	
2.9.5	Required	
2.9.6	Required	
2.9.7	Required	
2.9.8	Required	
2.9.9	Desired	
2.9.10	Required	

MSC REFERENCE	REQUIRED, DESIRED OR N/A	COMMENT OR RATIONALE
MSC Section 2.10: Guidance¹³		
Note: Criteria in this section are applicable to the <u>administration and operation of the product</u> , unless specifically identified in the "Comment or Rationale" column.		

¹² "Security administration" is identified as: The system shall offer features to selectively authorize a highly privileged user (a security administrator) to perform day to day activities such as: activate protective features (e.g., the login feature); customize (i.e., override, if appropriate) vendor-provided defaults; monitor suspected activities related to a potential security breach; detect security violation incidents promptly, isolate and investigate the problem, and securely recover the system; Generate security audits when needed; and manage user accounts.

¹³ "Guidance" is identified as: The vendor shall supply the following product support capability: a cogent security-related document for administration (e.g., a "Security Administration Guide") that would be made available as a hard copy or an electronic file, as an entity unto itself, and not fragmented throughout the reference manuals; a cogent user guide for security functions that would provide guidance for configuring the product's security features and maintaining security on an ongoing basis.

MSC REFERENCE	REQUIRED, DESIRED OR N/A	COMMENT OR RATIONALE
NEW	DESIRED	<i>NEW CRITERIA¹⁴: The product should document any and all modifications performed by the product. This includes modifications to itself and to other components of the system.</i>
2.10.1	Required	
2.10.2	Required	
2.10.2.1	Required	
2.10.2.2	Required	
2.10.2.3	Required	
2.10.2.4	Required	
2.10.2.5	Required	
2.10.2.6	Required	
2.10.2.7	Required	
2.10.2.8	Required	
2.10.2.9	Required	

MSC REFERENCE	REQUIRED, DESIRED OR N/A	COMMENT OR RATIONAL
MSC Section 2.11: Non-repudiation¹⁵		
Note: Criteria in this section are applicable to the <u>administration and operation of the product</u> , unless specifically identified in the "Comment or Rationale" column.		
NOTE: The classification of "DESIRED" here means that if the product submitted for evaluation does not provide non-repudiation functions, then it need not comply with the criteria in this section. However, if the product submitted for evaluation claims to provide non-repudiation functions, it must fully comply with items 2.11.1 through 2.11.3.		

¹⁴ All criteria identified as "New Criteria" in this section will be reviewed by the Financial Services MSC Committee for possible inclusion in a future release of the MSC.

¹⁵ "Non-repudiation" is identified as: The system shall have the capability of preventing users from successfully denying actions and events of users acting in the role of a sender or receiver.

MSC REFERENCE	REQUIRED, DESIRED OR N/A	COMMENT OR RATIONAL
2.11.1	Required	<i>See NOTE above.</i>
2.11.2	Required	<i>See NOTE above.</i>
2.11.3	Required	<i>See NOTE above.</i>

3.0 Product Functionality

This section of the criteria refers to the primary functionality of the product and how it is affected by security. For products whose primary functionality is not security (e.g., applications, databases, operating systems, etc.), this section will test how that functionality is impacted by the security features of the product, as described in Section 2 of the Criteria. However, for those products whose primary functionality is security-related (e.g., authentication systems, network security products, authorization systems, etc.), the “functionality” criteria will address the main purpose of the product. In the cases of these product profiles, the “functionality” section of the criteria will often be as detailed, if not more so, than the “security features” section. Furthermore, since the Product Profiles address a wide variety of products within a class, it is permissible for the Profile to contain functionality criteria specific to a “subclass” of products (e.g., the Authentication Systems profile might contain criteria specific to biometrics systems, smart cards, PKI, etc.).

MSC REFERENCE	REQUIRED, DESIRED OR N/A	COMMENT OR RATIONALE
3.1	Required	
3.2	Required	

4.0 Scalability

Scalability criteria shall specify minimum limitations in terms of traffic/use parameters of volume, frequency or time. These criteria are used to assess the degree to which security service objectives are met, at or near system capacities or *across multiple platforms*. The focus of the testing shall be to verify vendor claims of the scalability of the product in a standard configuration. The criteria are applied in tests that are designed to stress the product design, and to determine that the

product retains security functionality as the offered traffic exceeds stated system capacities.

MSC REFERENCE	REQUIRED, DESIRED OR N/A	COMMENT OR RATIONALE
4.1	Required	

3. Required Functional Criteria for all Monitoring and Intrusion Detection Systems

3.1 Introduction

This section will list the required criteria for the functional areas that are common to all products in this profile. **Product subclasses will have additional and unique functionality for which additional required criteria will be listed separately in Section 5. The functional groups in this section are:**

Manager/Agent Communication

Anomalous Behavior Detection

System Corrective Actions

System Programmability

Reporting and Trend Analysis

System Enhancements

3.2 Manager/Agent Communication

Most products are divided into at least three main components that, depending on topology, may provide slightly different functionality. Generally, an agent component will act as the data collection unit. It in turn reports to a manager whose responsibilities include interpreting the information from one or many agents. As such, the manager-agent communication is at a minimum a one-to-one correspondence, or it may be many-to-one, where multiple agents report to a central manager. The third component is the display interface. All three of these components make up the system. The system may reside on a single underlying platform or multiple systems depending on topology and use. The primary intent for providing criteria for management-agent communication is to address situations in which the components reside on separate physical machines. It is also necessary when administration of the different components may be under separate administrative control, e.g., when each agent is separately administered by a business unit while the manager falls under administrative control of Corporate IT. Therefore, additional product functionality must cover the inherent security weaknesses of this architecture.

Criteria	Rationale
3.2.1 Identifiers shall provide consistent accountability and auditability across all components.	In cases in which administration is done separately on the agent and the manager, the identifier must be unique for the entire system rather than individual components. This means that a user account on the agent cannot be duplicated on the manager, implying that the administrative database must either be synchronized or centrally located.
3.2.2 The management application shall ensure confidential data only to authorized applications or agents.	In systems involving multiple communication channels, such as is common in a manager/agent architecture, it is important to impose confidentiality restrictions between agents and their data. All information must be treated on a ‘need-to-know’ basis.
3.2.3 The system shall maintain/restore operations in the face of system failures including those resulting from malicious activity.	Products must be able to detect system outages, alert administrators or other authorized personnel about the system conditions, and provide administrators with the ability to manage the environment and restore service.
3.2.4 The system shall be able to continue to operate securely when various operating parameters increase or decrease. These operating parameters shall be specified by the Technology Provider and will be itemized in the Test Plan.	Modification of configuration parameters must not impede the ability of the system to provide adequate security. Coupled with the notification process, an alert must be generated if system security or functionality were to be compromised.

3.3 Anomalous Behavior Detection

The primary purpose for this functionality is to detect abhorrent or anomalous behavior. It also includes detecting attack conditions on networks or hosts. Forms of attack and failure are extensive. Certain types of devices attempt to piece together evidence or clues that an attack is occurring or is about to occur. Criteria in this section detail product features that all classes should contain in order to detect anomalous behavior.

Criteria	Rationale
3.3.1 Systems shall attempt to uniquely identify the source of an attack or outage including identification of IP address, hostname, or user ID.	Uniquely identifying an attacker is crucial if evidence is to be introduced into any type of litigation, and is also necessary in order to link audit trails.
3.3.2 The system shall have the capability to identify and categorically classify alerts and events into programmable groupings.	Alarms and events can be classified as being of a particular type. For example, if a ping o' death was detected by an intrusion detection system, then it can be determined that this type of event can be classified and placed into a group called "Denial of Service." All events of that type would be categorically classified in the same manner primarily to help identify the alarms so that they can be prioritized and corrective action can be taken. This will also aid in detecting patterns. The system shall have the ability to determine and classify each event into one or more different threat classes as appropriate
3.3.3 Information related to the attack or outage shall be kept confidential and treated as highly classified.	Information leakage about susceptible targets is undesirable, and may give an attacker further clues as to where to launch subsequent attacks.
3.3.4 The system shall provide an administrator with the capability to include new attack or outage conditions.	Since it is impossible for a system to understand new attack types before they occur, the system must be configurable to allow for inclusion of new attack conditions.
3.3.5 Documentation shall include explanations and examples as to how to include and program new attack signatures.	Detailed descriptions of how to program for detection of anomalous behavior is critical to ongoing system maintenance.

3.4 System Corrective Actions

Once an attack or outage has been detected the next step is to choose an action or sequence of actions whereby the attack condition can be eliminated, or the outage restored. Properly designed systems will allow system corrective actions to be taken.

Criteria	Rationale
3.4.1 <i>The system, in taking corrective actions, shall not identify itself to an attacking party, or in any other way open itself to compromise.</i>	Detection and response to an intrusion or system restore may cause a deliberate attack on the monitoring system. This should be prevented at all costs, as it could disrupt the system's ability to take further corrective action.

3.5 System Programmability

Complex products should be highly flexible in order to accommodate a rapidly changing environment. This becomes more necessary in systems of this type, in which the timeliness of detection and response to these types of events can prevent catastrophic losses if corrective action is taken. It is necessary then to make systems with event detection subsystems that are programmable.

Criteria	Rationale
3.5.1 <i>The user session inactivity time-out period (i.e., not used) shall be administrator-configurable. The default shall be no greater than 5 minutes.</i>	Since the system will be a control point, it is a highly desirable target and must support the capability to terminate sessions automatically in order to prevent session hijack.
3.5.2 <i>The default period for a system to disable a dormant (i.e., no activity) user-ID shall be no greater than 90 days.</i>	Strict requirements are needed to insure required functionality prior to programming those features. In this case removing dormant user-IDs will help insure system integrity.
3.5.3 <i>The system shall have the capability to configure and program attack or outage</i>	In order to keep up with a community that develops system attacks on a regular basis, the system must support the ability to configure the system in order to

<i>signatures or other parameters that will aid in the early detection of outages or system anomalies.</i>	detect new attacks.
Criteria	Rationale
3.5.4 <i>The system shall have the capability to configure the type of automatic response notification as a result of outage or attack detection.</i>	Different severity alarms require different types of notification, depending on the security classification of the event. As such, it is important to be able to choose how and when the notifications will take place.
3.5.5 <i>By default, there shall always be at least one type of event notification per alarm or event.</i>	Disabling the alert system could cause a serious security breach. At a minimum, each and every alert must be sent to a console.
3.5.6 <i>The system shall have the capability to classify events.</i>	Systems that come with alarm levels already classified do not take into consideration the unique business environments that the financial industry represents. Alarms and events should be able to be classified by administrators.
3.5.7 <i>The system shall provide the capability to define the default allowable idle period for communication between the manager and agents.</i>	In order to verify proper working capability of the system components, it is necessary to check system status on a regular basis. If there was no mandatory communication period, then systems that weren't reporting, could be deemed operational.
3.5.8 <i>The system shall have a default set of groups, identified here as "threat classes," that alarms and events will be classified and grouped into.</i>	Alarms and events shall be classifiable into at least one type of threat class group. For example, if a series of hosts were pinged in sequence, and a system detected this, then the alarm could be classified into a default group such as "Host Scan."
3.5.9 <i>The system shall have the ability to configure the groups into which events and alarms are classified.</i>	By default, products will categorize each type of alarm and event into at least one group. The capability shall exist to either reprogram the event into a more applicable group, or to create new groups and classify events into them.

3.6 Reporting and Trend Analysis

Historical data, especially among disparate system that have a common reporting facility, can be particularly useful for trend identification, system and network planning, and overall better decision making. Since the majority of data collected by systems will be unused, the ability to consolidate this information and use it is necessary and desirable.

Criteria	Rationale
3.6.1 <i>The manager shall collect alarm and event activity and keep it in a central repository.</i>	Information collected by the various agents must be sent to the manager and consolidated for use in trend analysis, etc.
3.6.2 <i>Information that is kept in a central repository shall be in a format conducive to data exportation.</i>	While systems of this class don't have to provide a parsing utility, the data should, at a minimum, be easily exported into an external utility, and thus should support a standard data format.
3.6.3 <i>If data must be moved from the system in order to parse it for historical purposes, the system shall have a utility for doing so in a secure fashion commensurate with the security handling expectations of the system itself.</i>	Data handling must be consistent even if the system is communicating with an external party. This includes proper identification, authentication, authorization, confidentiality and integrity.
3.6.4 <i>Any feature necessary to parse data or provide reporting shall not degrade overall system performance or cause delays in event identification, classification, and notification.</i>	Parsing large databases or log files will often utilize large amounts of system resources. The system should not be allowed to degrade to the point that the system's primary function could be compromised.
3.6.5 <i>A centralized audit capability or centralized audit facility shall be present in order to facilitate correlation of event activity between the manager and agent components.</i>	In order to follow a sequence of activities, it is important that there be a consolidated audit log which contains information from each of the components that make up a system.

3.7 System Enhancements

Keeping current information on attack signatures and up/down status are important features of systems. Since any system downtime represents an opportunity for a security-related event to occur and be undetected, it is imperative that systems are able to upgrade their security capabilities without unduly opening the system or network to compromise.

Criteria	Rationale
3.7.1 <i>When upgrading the system to include new attack signatures or other security features the system shall minimize the duration for which an event would go undetected.</i>	Systems should attempt to keep attack signatures in non-volatile memory to improve performance and reduce the amount of time that the system takes to upload new configurations. This reduces the amount of risk in not detecting a security-related event.
3.7.2 <i>If a system is undergoing a maintenance period, individual components shall continue to function normally and will resume communication upon restoration of the component.</i>	It is generally undesirable to perform maintenance on both the manager and agents simultaneously. If one of the components is being upgraded then the other shall continue to function normally, and shall resume normal operation without the need for operator intervention.
3.7.3 <i>If a component of the system is to be taken offline for maintenance, an appropriate administrator warning shall be generated explaining the risk of doing so.</i>	Any period of maintenance could lead to an undetected breach. The system shall warn the administrator when this occurs.
3.7.4 <i>If the system uses SNMP, the system shall use the most current version of the SNMP protocol that is stable from both an operational and a security perspective.</i>	The current SNMPv3 implementation offers many additional security capabilities over and above its predecessors. New versions of the protocol shall be evaluated to see if the enhancements outweigh the potential risks.

4. Desired Functional Criteria for all Monitoring and Intrusion Detection Systems

4.1. Introduction

This section describes the desired functionality expected in products and the criteria associated with each of these functions. The functional groups in this section are:

Manager/Agent Communication

Anomalous Behavior Detection

System Programmability

4.2. Manager/Agent Communication

<i>Criteria</i>	<i>Rationale</i>
4.2.1 DESIRED <i>The manager should not allow for the third-party recovery of keys used to create digital signatures.</i>	Non-repudiation requires that any keying material be maintained in a secure fashion and not shared outside of the authorized administrative controls.

4.3 Anomalous Behavior Detection

<i>Criteria</i>	<i>Rationale</i>
4.3.1 DESIRED <i>The default system configuration for integrity checking should be enabled.</i>	Turning off integrity checking must be a deliberate action by the administrator.

4.4 System Programmability

<i>Criteria</i>	<i>Rationale</i>
4.4.1 DESIRED <i>The system should follow a minimal set of programmable threat classes by which alarms and events can be categorized. (See Appendix D.)</i>	

5. Functional Criteria for Monitoring and Intrusion Detection Systems Product Sub-classes¹⁶

5.1 Introduction

For each of the subclasses of products listed below, this section lists the minimal functionality in terms of functional criteria, expected in products of that subclass. Subclasses specific to intrusion detection are determined using the applicable threat classifications to which alarms and events can be grouped. Reference Appendix D for more detailed threat model information.

- ***Network Intrusion Detection***

Network-based intrusion detection systems focus on detection of suspicious network activities. Observed network activity is compared to known attack signatures. When a close match is obtained, an alert can be generated. A key differentiation between competitive systems is the number and type of attacks recognized. Another differentiating factor between systems is the ability to accurately recognize attacks in the presence of high levels of traffic. The host used is ideally dedicated to the detection of network anomalies.

- ***Host-based Intrusion Detection***

Host-based intrusion detection systems focus on detection of changes to system activity. This includes monitoring system access and authorization, ensuring the integrity of critical files and applications and maintaining detailed audit logs of system activity. The files that are considered critical and the system activities that can be considered high risk can vary greatly. Thus, there should be extensive capabilities to customize the activities, which are monitored. The type of alerting that is generated must also be extensively customizable. These systems require the installation of software to monitor the individual hosts.

¹⁶ See Appendix D for Threat Classes.

- **Application-based Intrusion Detection**

Application based intrusion detection systems are fundamentally concerned with the behavior of the application subsystems as it relates to identification, authentication, authorization, confidentiality and integrity. How the application communicates with processes, data or other applications determines the relative risk of compromise due to theft, modification, disclosure or denial of service. These devices can also be primarily responsible for detecting either input or output anomalies.

5.2 Functional Criteria for Network Intrusion Detection

Criteria	Rationale
5.2.1 <i>The network IDS shall detect a wide range of attacks. Testing will consist of attacks known at the time of testing.</i>	System currency relative to attack signatures is a distinguishing feature of the network IDS. It is desirable to have a system that identifies as many attack signatures as possible. A master classification list that allows the financial industry to identify and group the various types of attacks is desirable.
5.2.2 <i>The network IDS detection capabilities shall not degrade when subject to high network utilization and multiple attacks.</i>	Systems must be able to perform their security functionality at all times and under extreme duress to avoid undetected violations.
5.2.3 <i>The network IDS shall support high-availability or load-balanced configurations with the network to which it is attached.</i>	If a network has higher throughput than is recognizable by the IDS system then events will go undetected. This is undesirable.
5.2.4 <i>The network IDS shall passively monitor the network while not disrupting normal traffic flows.</i>	The system, when operating in a surveillance mode, should not disrupt or attempt to disrupt normal network traffic.

<i>5.2.5 When disrupting a session as part of a corrective action, the system shall not disclose any information to either the sending or receiving party.</i>	An attacker should not be notified about why a session was terminated. If notification were to occur, then the attack could be altered in order to avoid detection.
---	---

5.3 Functional Criteria for Host Based Intrusion Detection

Criteria	Rationale
<i>5.3.1 The host IDS shall detect a wide range of host based attacks. The type of attacks generated will reflect the known attacks at the time of testing.</i>	System currency relative to attack signatures is a distinguishing feature of the host IDS. It is desirable to have a system that identifies as many attack signatures as possible. A master classification list that allows the financial industry to identify and group the various types of attacks is desirable.
<i>5.3.2 The host IDS shall provide the capability to set security parameters on an individual host level.</i>	Decisions shall be made on the integrity of individual hosts, and allow for that granularity of customization. Host security should be exclusive of network activity.
<i>5.3.3 The system shall have the ability to prioritize and alarm on system activities at the operating system level.</i>	Host IDS must be able to detect unauthorized activity on the host itself, on any applications that are running on that host, and on data files that are housed on the system in question. The alarm levels must be customizable.
<i>5.3.4 The system shall be able to distinguish and report activities at the system level and at the user level.</i>	There must be granular levels of control at the host level, and alarm levels must be customizable on a user by user basis or at a minimum, for a particular role.
<i>5.3.5 The system must support actions that allow for termination of unauthorized activity.</i>	Being able to prevent an intruder from doing further damage is an important feature of a host IDS system.
<i>5.3.6 The agent shall continue to</i>	Enforcement of security policy shall be done on a local

<i>operate normally and shall continue to monitor even if it is unable to communicate with the manager.</i>	basis; otherwise disruption of management communication could cause major disruption in service and business loss.
5.3.7 <i>If the system supports a global and local security policy, the administrator shall have the capability to select the appropriate controlling policy.</i>	Conflicting policies could result when one set of parameters is configured for all of the devices that fall under a manager's administrative control, while parameters are configured for a local agent. In that case, the local policy should override the global one.

5.4 Functional Criteria for Application-based Intrusion Detection

Criteria	Rationale
5.4.1 <i>The application-based IDS shall detect a wide range of application oriented attacks. The type of attacks generated will reflect the known attacks at the time of testing.</i>	System currency relative to attack signatures is a distinguishing feature of the application-based IDS. It is desirable to have a system that identifies as many attack signatures as possible. A master classification list that allows the financial industry to identify and group the various types of attacks is desirable.
5.4.2 <i>The application-based IDS shall detect attacks on processes, input/output streams and other types of anomalies that could otherwise harm the application or application data.</i>	Application-based IDS is distinguished because it has a particular focus on application processes and data that are separate and distinct from the operating system, the underlying platform or the network.
5.4.3 <i>Application-based IDS shall be customizable in order to distinguish between authorized application activity and unauthorized activity.</i>	Since applications are very customized to begin with, it is appropriate and desirable that the policies applications follow are highly customizable.
5.4.4 <i>Application-based IDS shall be constructed in such a way that changes in the programming or architecture of the application should not adversely affect the</i>	The system code should operate independently of the application that it is guarding, although it may be linked to the underlying platform and operating system. This is primarily to avoid the need for unique copies of the IDS for each application.

<i>functionality of the system.</i>	
-------------------------------------	--

Appendix A: Industry Standards

For the purposes of these criteria, the terms “public and widely-used standards” or “financial industry standards” shall refer to those standards, algorithms and protocols listed below as well as other relevant standards approved by the following organizations: IETF, ANSI X9, ITU-T, ISO, NIST and IEEE.

Symmetric encryption algorithms	<ul style="list-style-type: none"> • 3DES (ANS X9.52, X9.66) • IDEA • RC4 • RC5 • RIPEM
Asymmetric algorithms (for symmetric key agreement or key transport)	<ul style="list-style-type: none"> • RSA (ANS X9.44) • D-H (minimum 1024-bit modulus – ANSI X9.42) • ECDH (ANS X9.63) • Elliptic Curve
Digital hashing algorithms	<ul style="list-style-type: none"> • SHA-1 (ANS X9.30-2) • MD5
Digital signature algorithms	<ul style="list-style-type: none"> • DSA (ANS X9.30-1) • rDSA (ANS X9.31) (includes RSA) • EC-DSA (ANS X9.62)
Key management standards and protocols	<ul style="list-style-type: none"> • ANS X9.70, ANS X9.73, ANS X9.69, ANS X9.24, ANS X9.77 • CMP • PKCS #7, #10 • IETF PKIX standards
Random number generators	<ul style="list-style-type: none"> • ANS X9.82
Prime number generators	<ul style="list-style-type: none"> • ANSI X9.80
Cryptographic device security	<ul style="list-style-type: none"> • ANS X9.66 • FIPS 140-2
Peer entity authentication	<ul style="list-style-type: none"> • ANS X9.72 • FIPS 196
PIN security	<ul style="list-style-type: none"> • ANS X9.8, ANS X9.86, ANS X9.87
Biometrics management and security	<ul style="list-style-type: none"> • ANS X9.84
Industry standards	<ul style="list-style-type: none"> • X.500 • LDAP v3
TCP/IP integrity	<ul style="list-style-type: none"> • IPsec

The system shall use any of the algorithms listed above or those that are supported by any of the standards organizations listed above. If the system uses any other cryptographic algorithm, then it shall be configurable to also allow the use of an acceptable algorithm in place of the unlisted algorithm.

Appendix B: Bibliography

MSC *Master Security Criteria (v3.0)*, BITS, October 2001

Appendix C: Glossary of Terms

Definitions provided in this document came from various books and publications. Several of these sources are included at the end of this section.

TERM	DEFINITION
access control	<i>A mechanism for limiting use of a resource to authorized users. [1]</i>
account	<i>In terms of a “user account,” an account is an established relationship between a user and a computer, network or information service.</i>
active attack	<i>An attack that results in an unauthorized state change, such as the manipulation of files or the addition of unauthorized files. [3]</i>
administrator	<i>Taken in the context of this profile and if used without pre-qualification, this term indicates any user or group of users that could be defined as a system administrator and/or product administrator, typically having privilege beyond the scope of an end user. See also “end user,” “user” and “product administrator.”</i>
agent	<i>A specialized piece of software or hardware that collects data and interprets it, usually relative to security or, in the case of network management stations, relative to up/down status of a device or system.</i>
automated information system (AIS)	<i>Any interconnected system equipment or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, control, display, transmission, or reception of data, and including software, firmware and hardware. [3]</i>
application programming interface (API)	<i>An interface typically provided by a software development toolkit.</i>
asymmetric cryptography	<i>A class of cryptographic algorithms that use separate keys for encryption and decryption. [2]</i>
attack	<i>An attempt to bypass security controls on a computer. The attack may alter, release or deny data. Whether an attack will succeed depends on the vulnerability of the computer system and the effectiveness of existing countermeasures. [3]</i>
audit	<i>To keep a record of events that might have some security significance, such as when access to resources occurred. [1]</i>
authenticate	<i>To determine that something is genuine. To reliably determine the identity of a communicating party. [1]</i>
authentication	<i>The process of reliably determining the identity of a communicating party. [1]</i>
authenticator	<i>The method, material or credential used to create and/or implement authentication bindings, such as a password, PIN number, token seed or smart card seed.</i>
authorization	<i>Permission to access a resource. [1]</i>
biometric device	<i>A device that authenticates people by measuring some hard-to-forge physical property, like a fingerprint or the strokes and timing of a signature</i>
biometrics	<i>Using physical characteristics of users such as fingerprints and retinal impressions to authenticate users. [2]</i>
buffer overflow	<i>When more data is put into a buffer or holding area than the buffer can handle. This is due to a mismatch in processing rates between the producing and consuming processes, and can result in system crashes or the creation of a back door leading to system access. [3]</i>

TERM	DEFINITION
certificate	<i>A message signed with a public key digital signature stating that a specified public key belongs to someone or something with a specified name. [1]</i>
certification authority (CA)	<i>Something trusted to sign certificates. [1]</i>
certificate revocation list (CRL)	<i>A list of names of users and roles that are no longer valid within a public key cryptography system. [2]</i>
challenge-response	<i>An authentication mechanism in which the authentication process sends a challenge to a process that requests authentication; the latter is authenticated only if it sends the correct response to the authentication process. [2]</i>
clear text	<i>A message or data that is not encrypted.</i>
client	<i>Something that accesses a service by communicating with it over a computer network. [1]</i>
confidentiality	<i>The property of not being divulged to unauthorized parties. [1]</i>
credential	<i>A letter or certificate given to a person to show that he or she has a right to confidence or to the exercise of a certain position or authority. [5]</i>
cryptography	<i>The practice of encoding and decoding data.</i>
decrypt	<i>To undo the encryption process. [1]</i>
dictionary attack	<i>An attack in which the attacker “guesses” passwords, based on a set of key words or characters, until a match is made. Also called an “offline attack” or “brute force attack.”</i>
digital signature	<i>Digital signatures are used to detect unauthorized modifications to data and to authenticate the identity of the signatory. In addition, the recipient of signed data can use a digital signature to prove to a third party that the signature was in fact generated by the signatory. A digital signature is represented in a computer as a string of binary digits. A digital signature is computed using a set of rules and parameters such that the identity of the signatory and integrity of the data can be verified. Signatures are generated and verified via an algorithm. A private key allows the generation of a digital signature. Signature verification makes use of a public key which corresponds to, but is not the same as, the private key. Each user possesses a private and public key pair. [6]</i>
dynamic link library (DLL)	<i>Software (executable code or data, such as icons or fonts) used by Microsoft's Windows and IBM's OS/2 to provide services (such as a LAN driver or a distributed filing system) to applications. One memory-resident copy of the DLL can be simultaneously shared by all applications.</i>
domain name system (DNS)	<i>An Internet service that translates domain names into IP addresses.</i>
dongle	<i>A device that attaches to a computer to control access to a particular application</i>
encrypt	<i>To scramble information so that only someone who knows the appropriate secret can obtain the original information (through decryption).</i>
end user	<i>Taken in the context of this profile and unless otherwise indicated, “end user” is the individual who uses the system after it has been fully developed. The term distinguishes the user for which the product is designed from the developers, installers and administrators who are making the product available for the end</i>

TERM	DEFINITION
	<i>user. See also “user” and “administrator.”</i>
escrow	<i>To hold something in safekeeping. Most uses of the word actually mean keeping the something safe from the owner as opposed to providing any safety for the owner.</i>
group	<i>A named collection of users, created for convenience in stating authorization policy.</i>
hash	<i>A cryptographic one-way function that takes an arbitrary-sized input and yields a fixed-size output. [1]</i>
immutable	<i>Unchangeable [2]</i>
integrity	<i>The quality of being uncorrupted. Message integrity refers to the state of a message not being modified while in transit. File integrity refers to the state of files not being modified while in storage. [2]</i>
integrity checks	<i>(Note: In the context of this document, includes the term “data integrity check”): reassuring the recipient of a message that the message has not been altered since it was generated by a legitimate source (based on representing information as numbers and mathematically manipulating those numbers). [1]</i>
interface	<i>In the context of this document, the term “interface” will represent a separate entry point into the system. Within this profile, the term “interface” (i.e. “user interface”) is defined in the context of product administration, indicating the entry point for commands and menu(s) to a system.</i>
intrusion Detection Systems (IDS)	<i>Techniques for detecting intrusion into a computer or network by observation of actions, security logs or audit data. Break-ins or break-in attempts are either detected manually or via software expert systems that operate on logs or other information available on the network.</i>
key	<i>A quantity used in cryptography to encrypt or decrypt information.</i>
key escrow	<i>The system of giving a piece of a key to each of a certain number of trustees such that the key can be recovered with the collaboration of all the trustees. [3]</i>
log	<i>To record an action. [2]</i>
log file	<i>A file that lists actions that have occurred. [2]</i>
manager	<i>A console that controls the system by allowing configuration changes and active commands. The manager is responsible for communicating with the agents, collecting information from them, and then storing or performing actions once the data has been received.</i>
message authentication code (MAC)	<i>A synonym of message integrity code (MIC). [1]</i>
message digest	<i>An irreversible function that takes an arbitrary sized message and outputs a fixed length quantity. MD2, MD4, and MD5 are message digest algorithms. [1]</i>
multifactor	<i>More than two elements or quantities.</i>
message integrity code (MIC)	<i>A fixed-length quantity generated cryptographically and associated with a message to reassure the recipient that the message is genuine. [1]</i>
NIST	<i>National Institute of Standards and Technology</i>
non-repudiation	<i>The property of a scheme in which there is proof of who sent a message that a recipient can show to a third party and the third party can independently verify the source. [1]</i>
network time protocol	<i>A facility that allows for synchronized timekeeping among a set of distributed time</i>

TERM	DEFINITION
(NTP)	<i>servers and clients. It is a standard protocol that enables client computers to maintain system time synchronization to the US Naval Observatory Master Clocks. NTP runs as an application program, and it sends periodic time requests to one or more servers, obtaining server timestamps and using them to adjust the client's clock.</i>
online Certificate Status Protocol (OCSP)	<i>Facilitates determining the current status of a digital certificate. It enables applications to determine the revocation status of a certificate. OCSP may provide more timely and accurate revocation information than is possible with Certificate Revocation Lists.</i>
offline attack	<i>An attack performed while offline to the system being attacked (see also “dictionary attack”).</i>
one-time passwords	<i>Passwords that can only be used once. [2]</i>
operator	<i>In the context of this profile, “operator” maintains similar relationships and functions as “administrator” (see above), given different and/or additional privileges than a typical “end user” of a system.</i>
orthogonal	<i>Having to do with right angles; rectangular. [5]</i>
passive attack	<i>Attack which does not result in an unauthorized state change, such as an attack that only monitors and/or records data. [3]</i>
password	<i>A supposedly secret string used to prove one’s identity. [1]</i>
personal identification number (PIN)	<i>A short sequence of digits used as a password. [1]</i>
public key cryptography standards (PKCS)	<i>A set of standards, first introduced in 1991 by RSA Data Security, Inc., for implementing public key cryptographic algorithms and incorporating them in to applications. [2]</i>
plaintext	<i>Unencrypted data. [3]</i>
pre-authentication	<i>A protocol for proving you know your password before you are allowed access to a high quality secret encrypted with that password. [1].</i>
private key	<i>The quantity in public key cryptography that must be kept secret. [1]</i>
privileged user	<i>A user of a computer or system who is authorized to bypass normal access control mechanisms, usually to be able to perform system management functions [1]</i>
product administrator	<i>In the scope of this document, the roles associated with higher privilege at the product’s configuration level (may or may not be the same as the system administrator).</i>
protected path	<i>A mechanism that guarantees a mutually authenticated channel. [4]</i>
public key	<i>The quantity in public key cryptography that is safely divulged to as large an extent as is necessary or convenient. [1]</i>
public key cryptography	<i>A cryptographic system where encryption and decryption are performed using different keys. (See asymmetric key cryptography.) [2]</i>
relying party	<i>In the scope of this profile, “relying party” is typically associated with the use of “system” (see below). It is associated frequently with the extent to which a criteria is in scope, as in references to an application or component maintaining reliance on another element to support said criteria.</i>
replaying	<i>Storing and re-transmitting messages; the word is usually used when implying that</i>

TERM	DEFINITION
	<i>the entity that replies to messages is mounting some sort of security attack.</i>
repudiation	<i>Denying that you did something or made some statement. [1]</i>
revoke	<i>To withdraw, repeal, rescind, cancel or annul. [5]</i>
role	<i>A function or office assumed by someone. [5]</i>
security domains	<i>The sets of objects that a subject has the ability to access. [3]</i>
security features	<i>The security-relevant functions, mechanisms and characteristics of AIS hardware and software. [3]</i>
server	<i>Some resource available on the network to provide some service such as name lookup, file storage or printing. [1]</i>
sign	<i>To use your private key to generate a digital signature as a means of proving you generated, or approve of, a message.</i>
signature	<i>A quantity associated with a message which only someone with knowledge of your private key could have generated, but which can be verified through knowledge of your public key. [1]</i>
spoof	<i>To convince someone that you are some entity X when you are not X, without X's permission. [1]</i>
strong authentication	<i>Authentication performed in such a way that it cannot easily be performed. Examples of strong authentication include one-time passwords, challenge-response mechanisms and cryptographic authentication. [2]</i>
symmetric key cryptography	<i>A class of cryptographic algorithms in which the same key is used for encryption and decryption. Examples of symmetric key algorithms include DES, IDEA, RC2 and RC4. [2]</i>
system	<i>Within the scope of this profile, "system" is used to imply the totality of the product and the mediation devices (if any) that need to be tested. A system is defined as being a combination of manager and agent components, any monitoring station used to view manager information, and the underlying hardware and operating system. At a minimum, there would be one instance of manager and agent components to form a system. These components may be installed on one or more physical devices.</i>
system administrator	<i>An individual (user) who has higher privilege at the operating system level. Being a system administrator, while implying additional product administration capabilities, does not necessarily imply that product administration capabilities have been authorized. This distinction is necessary in the case where separation of duties exists between a system administrator and a security officer.</i>
system restart	<i>To restart a system. May also be referred to as a "warm boot," in which the system is restarted from an operational state or a "cold boot," in which the system is powered off and then on again.</i>
token device	<i>A credit card sized device that generates authentication tokens, such as one-time passwords. [2]</i>
two-factor authentication	<i>A process in which two pieces of information are required to prove one's identity (such as a password and a smart card). [2]</i>
weak authentication	<i>Typically, this implies the conventional use of passwords</i>
user	<i>In the context of this profile and used without pre-qualification, this term indicates any and all users, such as an end user, product user-ID or system user.</i>

TERM	DEFINITION
user-ID	<i>A number or name unique to a particular user of a computer or group of computers that share user information. The operating system uses the user ID to represent the user in its data structures, e.g., the owner of a file or process or the person attempting to access a system resource.</i>
X.509	<i>A CCITT standard for security services within the X.500 directory services framework. The X.509 encoding of public key certificates has been widely adopted; the other protocol elements of X.509 have not. [1]</i>

Glossary items are based on the following references:

[1] Kaufman, C., Perlman, R. and Speciner, M., *Network Security: Private Communication in a Public World*, Prentice Hall, New Jersey, 1995

[2] Bernstein, T., Bhimani, A., Schultz, E., and Siegel, C., *Internet Security for Business*, John Wiley & Sons, Inc., New York, 1996

[3] NSA Glossary of Terms used in Security and Intrusion Detection

[4] Loscocco, Peter A., Smalley, Stephen D., Muckelbauer, Patrick A., Taylor, Ruth C., Turner, S. Jeff, Farrell, John F., *The Inevitability of Failure: The Flawed Assumption of Security in Modern Computing Environments*, 1998

[5] Guralnkik, David Bernard (editor), *Webster's New World Dictionary of the American Language*, Prentice Hall Press, 1986

[6] FIPS PUB 186-2, *DIGITAL SIGNATURE STANDARD (DSS)*, 27 January 2000

Appendix D: Intrusion Detection Systems Threat Classes

The following table gives a sample list of threat classes to which alarms and events can be grouped.

User	Network	Host Operating System	Application
Social engineering	Eavesdropping/packet sniffing Confidentiality	UID/password attacks Identity, Confidentiality	Exploit user account
Fool someone to reveal password	Wardialing Confidentiality	Virus/malicious code attacks Integrity, Availability, Confidentiality	Exploit software bugs
Shoulder surfing	IP address scanning Confidentiality		CGI-based attacks
Dumpster diving	IP spoofing identity, Availability	Modify critical system data Integrity, Availability	
Theft of identity	Exploit TCP/IP services	Exploit trust relationship	
	Exploit router bugs	Attack on privileged user	
	Denial of service Availability	Privilege escalation Availability, Integrity, Confidentiality	