National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

ArcSight, Inc.
Cupertino, CA

ArcSight 3.0

Report Number: CCEVS-VR-06-0040
Dated: 29 September 2006
Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team

Mr. Daniel P. Faigin
The Aerospace Corporation
El Segundo, California

The Validation Team also thanks Mr. Jim Brosey, *The MITRE* Corporation, for the work he performed when he was Lead Validator, and Mr. Kenneth Elliott for his work as Senior Validator.

Common Criteria Testing Laboratory

Ms. Shukrat Abbas, Lead Evaluator
Craig Floyd
Jean Petty
Science Applications International Corporation
Columbia, Maryland

Much of the material in this report was extracted from evaluation material prepared by the CCTL. The CCTL team deserves credit for their hard work in developing that material. Many of the product descriptions in this report were extracted from the Arcsight 3.0 Security Target.

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of the ArcSight 3.0 Enterprise Security Manager from ArcSight Inc.[1] It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America, and was completed in September 2006. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by SAIC. The evaluation determined that the product is both **Common Criteria Part 2 Extended** (with FPT_AVL.1, IDS_ANL.1, IDS_RCT.1, IDS_RDR.1, IDS_STG.1, and IDS_STG.2) and **Part 3 Conformant**, and meets the assurance requirements of Evaluation Assurance Level (EAL) 3 augmented with ALC_FLR.1. The Security Target is conformant with the U.S. Government Intrusion Detection System Analyzer Protection Profile, Version 1.2, April 27, 2005 [20], as modified by errata and observation decisions.

The ArcSight product is a security management solution that allows a user to manage all enterprise activity from one centralized view. It integrates existing multi-vendor devices throughout the enterprise into its scope and gathers all generated events. ArcSight allows users to monitor events in real-time, correlate events for in-depth investigation and analysis, and resolve events with automated escalation procedures and actions.

The ArcSight product gathers events generated by heterogeneous devices, normalizes, filters, and aggregates those events, stores those events in a centralized ArcSight Database, and cross-correlates those events with rules to generate meta-events.

The ArcSight product is composed of several components;

- **ArcSight Console**, which provides a centralized view into an enterprise. The console provides real-time monitoring, in-depth investigative capabilities, and automated responses and resolutions to events.
- **MyArcSight**, which is a personalized web-based interface that is accessed to monitor events, view cases, view totals of events matching certain designated filters, acknowledge notifications, access reports, and access the Knowledge Base
- **ArcSight Manager**, which is a high performance engine that manages, cross-correlates, filters, and processes all occurrences of security events in the enterprise.
- **ArcSight Database**, which is the relational database repository that is used to store all captured events, plus save all security management configuration information

[1] Note that this evaluation does not cover the full range of supported platforms for the ArcSight Console and Manager, and only covers a subset of the available monitoring agents.

such as system users, groups, permissions, and defined rules, reports, displays, and preferences.

- **ArcSight SmartAgents**, which are collectors and processors of events generated by security devices throughout an enterprise

The Target of Evaluation (TOE) is ArcSight 3.0, a subset of components of the ArcSight product. The components that comprise the TOE are the ArcSight Console, the ArcSight Manager, the ArcSight Database, and selected ArcSight Agents.

It is important to note that the following components ***are included in the product but are excluded from the TOE***:

- **MyArcSight**: A Web-based UI to ArcSight which is part of the Manager and is disabled in the TOE.
- **ArcSight Web**: A Web-based UI to ArcSight that is a separately installed server that is not installed as part of the TOE.
- The **Pattern Discovery Engine**: A feature of the Manager that is licensed separately and is not enabled as part of the TOE.
- The **Database Agent**: An Agent that may be installed on the database host and provides partition archiving services but is not installed as part of the TOE.
- **All ArcSight Agents except for the three that are part of the TOE** (Nessus, Checkpoint Firewall, and Snort).

This validation assumes the TOE has been configured as described in Section 1.1 of the ST.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 1.0) [15] for conformance to the Common Criteria for IT Security Evaluation (Version 2.1) [11][12][13]. This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme [16] and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team monitored the activities of the evaluation team, observed evaluation testing activities, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The SAIC evaluation team concluded that the Common Criteria requirements for Evaluation Assurance Level 3, augmented with ALC_FLR.1, have been met.

The technical information included in this report was obtained from the Evaluation Technical Report (ETR) Part 1 (non-proprietary) produced by SAIC [18], the ArcSight 3.0 Security Target [17], and research and analysis performed by the Validation Team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 2-1. Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE:	ArcSight 3.0 comprised of the following components: • ArcSight Console (ArcSight – 3.0.2.3939.0 – Console) with Patch-3.0.2.9.3939-Console • ArcSight SmartAgents for Nessus, Check Point Firewall-1 NG OPSEC, and Snort IDS DB (ArcSight-3.5.1.4339.0 - Agent) • ArcSight Manager (ArcSight-3.0.2.3939.0-Manager) with Patch-3.0.2.9.3939-Manager • ArcSight Database (ArcSight-3.0.2.3939-DB) with Patch-3.0.2.6.3939-DB The ArcSight 3.0 TOE must be configured in accordance with the following Guidance Documents:

Item	Identifier
	• ArcSight Administrator's Guide, Version 3.0 SP2, March 17, 2006 [1] • Using the ArcSight Console, Version 3.0 SP2 [2] • ArcSight README, November 12, 2004 [3] • ArcSight ESM Release Notes version 3.0 SP2 [4] • ArcSight SmartAgent Installation Guide, ArcSight Version 3.0 [5] • SmartAgent Configuration Guide, Check Point FireWall-1, 4.1 OPSEC Agent, NG OPSEC Agent, March 17, 2006 [6] • SmartAgent Configuration Guide, Nessus Vulnerability Scanner, Report Agent, March 17, 2006 [7] • SmartAgent Configuration Guide, Snort, Open Source Network Intrusion Detection System, Database Agent, Log-file Agent, January 30, 2006 [8] • SmartAgent Readme, March 17, 2006 [9] • Patch readme files: Patch 9 (3.0.2.9.3939), March 22, 2006 [10]
Protection Profile	U.S. Government Intrusion Detection System Analyzer Protection Profile, Version 1.2, April 27, 2005 [20]
ST:	*ArcSight 3.0 Security Target*, Version 1.0, September 29, 2006 [17]
Evaluation Technical Report	• *Evaluation Technical Report for ArcSight 3.0, Part I (Non-Proprietary)*, Version 1.0, September 29, 2006 [18] • *Evaluation Technical Report for ArcSight 3.0, Part II (Proprietary)*, Version 1.0, September 29, 2006 [19]
CC Version	Common Criteria for Information Technology Security Evaluation, Version 2.1 [11][12][13]
Conformance Result	CC Part 2 extended (with FPT_AVL.1, IDS_ANL.1, IDS_RCT.1, IDS_RDR.1, IDS_STG.1, and IDS_STG.2), CC Part 3 conformant
Sponsor	ArcSight Inc., Cupertino, CA, USA
Developer	ArcSight Inc., Cupertino, CA, USA
Common Criteria Testing Lab (CCTL)	SAIC, Columbia, MD, USA
CCEVS Validators	Daniel P. Faigin, The Aerospace Corporation, El Segundo, CA
Applicable Interpretations	CCIMB-INTERP-0004 CCIMB-INTERP-0038 CCIMB-INTERP-0065 CCIMB-INTERP-0116 CCEVS OD-0250

3 Security Policy

The Security Functional Policies (SFPs) implemented by ArcSight 3.0 provide for authenticated user access, provide accountability for actions, provide intrusion detection analysis and protect the mechanism that provides the security policies.

Note: Much of the description of the ArcSight 3.0 security policy has been extracted and reworked from the ArcSight 3.0 Security Target [17].

3.1 Security Audit

The ArcSight 3.0 audit functions records two types of events: security events and analyzer events (discussed under "Intrusion Detection Policies"). Security events relate to the proper functioning and use of the system, and allow an administrator to track the management functions performed. Audit events are collected by all ArcSight components and transmitted to the ArcSight Manger, which sits at the center of ArcSight 3.0 and acts as a link between the ArcSight Console, ArcSight Database, and ArcSight SmartAgents.

When audit is recorded by the ArcSight Manager, it is written to audit and error logs stored in the underlying operating system, which must provide a file system for these logs, as well as protecting these logs. The audit records written contain the date and time of the event (obtained from the underlying operating system on the ArcSight Manager), the type of event, the subject identity, and the outcome of the event. The following events are recorded:

- The start-up and shutdown of audit functions. Note that the audit function automatically starts at system start-up and can only be shutdown at system shutdown.
- Access to the Analyzer.
- Access to the TOE Analyzer data.
- Reading of information from the audit records through the TOE.
- Unsuccessful attempts to read information from the audit records via the TOE.
- All modifications to the audit configuration that occur while the audit collection functions are operating.
- All uses of the TOE authentication mechanism.
- All uses of the TOE user identification mechanism.
- All modifications in the behavior of the functions of the TSF.
- All modifications to the values of TSF data.
- Modifications to the group of users that are part of a role.

The ArcSight Console provides the ArcSight Administrator (and only the Administrator) the ability to view security audit data for the system. This audit data is presented in a

readable format, permitting the Administrator to read and interpret the content of the information. In addition, the authorized Administrator can sort the audit data based on at least the following event attributes: date and time of the event, type of event, and success or failure of related event. The ArcSight Console also provides the Administrator the ability to include or exclude auditable events based on event type, such as all use of the authentication mechanism or all modifications in the behavior of the functions of the TSF.

To prevent audit data loss, a warning is sent to the designated administrator via e-mail[2] should the ArcSight database begin to run out of storage space for the audit records. The warning is set by default to be sent when the database is 85% full. If the storage space for audit records reaches capacity, all incoming events from SmartAgents are stopped and all events that are currently being processed are stored temporarily in the underlying operating system's file system of the ArcSight Manager until the database problem is cleared. The ArcSight Manager continues to create audit events for any scheduled actions or actions triggered by the processing of any events received prior to the database failure. Until the database failure is cleared, no users are allowed to access the ArcSight Manager. The administrator accesses the database directly to free-up storage space that will clear the database failure. As a result, very few events will need to be preserved on the local OS file system which in turn ensures that no audit information will be lost. Once space has been freed up, the ArcSight Manager allows users to log in and resumes receiving events from SmartAgents.

3.2 Identification and Authentication

ArcSight 3.0 requires users to provide unique identification and authentication data (passwords) via the ArcSight Console before any administrative access is granted. To login to the ArcSight Console, the user provides their login name and password. The administrator console computes the MD5 hash of the password, and compares the hashed password to the hashed password stored in the ArcSight database. If either the login name or the password is incorrect, the login request will fail and no administrator functions will be made available. As result of a successful login, the console session is established and the administrator functions are made available.

For non-administrative functions no authentication is required. These functions include collection of data on network anomalies identified by third-party network monitoring devices (e.g., Intrusion Detection Systems (IDS) Sensors or IDS Scanners) by the ArcSight Smart Agents, who then transmit the data to the ArcSight Manager.

The ArcSight Manager is responsible for creating and maintaining the user accounts through the graphical user interface (GUI) provided by the ArcSight Console. Each account has the following attributes:

- User identity
- Authentication data (passwords)

[2] Note that email functionality is provided by the IT Environment. The only portion of email functionality included in the TOE is the transmitting portion of the SMTP dialogue.

- Authorizations (groups)
- E-mail address
- Pager information

The E-mail address and Pager information is used to contact the user via IT Environment mechanism when alarms must be issued.

3.3 Security Management

ArcSight 3.0 supports the following administrative roles:

- **Administrator**. The Administrator uses the ArcSight Console to view the overall health of an enterprise and perform administrative tasks such as managing, configuring, and integrating ArcSight 3.0 with multi-vendor devices. They also have the abilities of the Analyzer Administrator, i.e., they can create customized rules to enforce security polices and procedures, escalation procedures, and Knowledge Base articles to enforce enterprise security policies and procedures. However, only the Administrator can enable custom rules. The Administrator is also the only role that can manage the security settings on the system, such as defining user accounts and authorization, and configuration of audit settings.
- **Analyzer Administrator**. Analyzer Administrators use the ArcSight Console to create customized rules to enforce security polices and procedures, escalation procedures, and Knowledge Base articles to enforce enterprise security policies and procedures. Note that although an Analyzer Administrator can create customized rules, they do not have the authority to enable the rules (that is the responsibility of the Administrator).
- **Operator.** Operators use the ArcSight Console to assist in observing, interpreting, and responding to events. Operators can observe real-time and replay events using Views, interpret events with Event Inspector and Replay Controls, and respond to events with preset, automated actions, Replay Control Tools, Reports, and Knowledge Base articles.

All user accounts must be assigned to one of these roles, and users must login before any administrative actions can be performed (other than entry of identification and authentication data).

The ArcSight Console provides Administrators, Analyzer Administrator, and Operators with a graphical user interface (GUI) that permits essential security management tasks to be performed. The tasks include the management user accounts, management the Analyzer data, and management of the audit functions. It also provides the ability to modify the behavior of the data collection and review, query audit data, and restrict access and/or the ability to query and modify all other TOE data to the appropriate authorized user/authorized role.

3.4 Intrusion Detection Policies

A key security functional policy provided by ArcSight 3.0 is its ability to analyze and correlate events. This is performed by the ArcSight Manager, which uses a collection of

tools that allows the Administrator to track, respond, and resolve security threats and attacks. The Cross-Correlation Engine (CCE) in the Manager prioritizes events based on the threat they pose to the protected network, identifies statistical anomalies in the content or volume of events, and uses rules to both cross-correlate events using signatures and trigger automated response actions. The CCE provides the ability to correlate events across vendor, across device, and across time. By cross-correlating different events, the CCE detects successful attacks, their criticality, and threat level. At a minimum, each analytical result is logged with following information; data and time and identification of data source.

The CCE is implemented using threat evaluation formulae, statistical data monitors, and rules. The threat evaluation formulae are used to compute a numeric priority for each event. Statistical data monitors generate meta-events when fluctuations are observed in the volume or content of the event stream. Rules may either be a simple filter or may perform a complex join across several events in real-time. Rules then aggregate the occurrences of the matching events. Rules trigger responses either on first match or after a given threshold has been passed. A rule threshold is defined as either a set number of matches or a given amount of time. If the threshold is passed the Cross-Correlation Engine generates a derived event and performs the other actions associated with the rule.

There are predefined threat level formula, statistical data monitors, and rules to detect intrusions and perform actions. Some built-in rules and data monitors are designed to monitor the operation and integrity of the ArcSight Manager and ArcSight SmartAgents. Other rules and data monitors detect and respond to attacks and suspicious activity, specific types of attacks on various sensor types, network components, or assets, and attack results or success of attack.

Associated with each rule is a rule action, which is an automatic procedure that occurs when all rule conditions and threshold settings have been met. The Administrator can choose to be notified of a triggered rule at the ArcSight Console or have information about the events that triggered the rule sent to a case or an active list. The following list describes some additional actions that can be specified for a rule:

- **Active List Actions**. This rule action modifies the contents of an active list. Active Lists are tables of information, for instance a collection of IP addresses and zones, which are used to record prior actions from or intrusions on various devices. For example, there are Active Lists to record hostile hosts, suspicious hosts, hosts that have performed prior recon on the protected network, and hosts that have been attacked, scanned, or compromised. Once a rule is triggered, the Active List rule action may add or remove an address mentioned in the derived event from an Active List. Rule conditions can also reference Active Lists. For instance, a rule may only match if the source address of an event appears in the Hostile Active List.
- **Execute Command Actions.** This rule action is used to execute a command line function when the rule is triggered. The command line function may be executed on the ArcSight Manager machine or an ArcSight SmartAgent machine. Note that the command is executed by the IT environment.
- **Send to Console Actions**. These rule actions send a meta-event to the ArcSight Console when the rule is triggered. A meta-event is generated by a rule when its

conditions and threshold settings are met. Setting this action displays the lightning bolt-fired rule event on the Console. In the absence of a Send to Console, derived events are explicitly removed from the live stream of events before being presented to the Consoles. The lightning bolt is associated with all derived events displayed in the grid, whether they are displayed live or as part of a query result.

- **Case Actions.** These rule actions create and modify cases, which are used to track the investigation of incidents. The actions may add the meta-event created when the rule triggered to a pre-existing case or the action may first create a new case.
- **Notification Actions**. These rule actions are used to inform ArcSight users that an incident has occurred. The notification may be delivered by email or pager, or it may only be delivered to the user the next time the log into the ArcSight Manager using the ArcSight Console. Note that delivery by email or pager uses mechanisms in the IT Environment.

In an ArcSight 3.0 environment, only successfully authenticated users can access the ArcSight Console and then only users who hold the appropriate authorization can vies the data. Using the ArcSight Console graphical user interface, Administrators can view the overall health of the enterprise as well as the data colleted. The Administrators can view the audit data, reports, to include the analytical results, configuration information, and other applicable analyzer data that is collected. In addition, Operators can query the data collected via the ArcSight Console. All data is presented in such a manner that it can be read and the contents of the data can be interpreted; thus the reader, be it the Administrator or the Operator can understand the content of the information presented, hence the information is presented in a manner suitable for human interpretation.

Only an Administrator has the ability to delete the analyzer data log, or to delete and/or clear the audit trail. The Administrators control the retention period of the audit logs that typically range from 30 to 90 days.

To prevent analyzer data loss, a warning is sent to the designated administrator via email[3] should the database begin to run out of storage space for the analyzer data records. The capacity is set at 85% full (default setting), at which time e-mail is sent to the authorized Administrator. If the ArcSight database fills up, the ArcSight Manager stops accepting new events from all ArcSight SmartAgents. Those ArcSight SmartAgents will use a local operating system (i.e., IT environment) disk-based cache to preserve those events until the ArcSight Manager starts accepting events once again. Once space has been freed on the ArcSight database, the ArcSight Manager is re-enabled so that the cached and live events may flow up from the ArcSight SmartAgent.

If the ArcSight Manager fails, the ArcSight Agents cache the data and wait for the ArcSight Manager to return. Analyzer data in memory at the time of the crash may be lost. The correlation facility of the product periodically writes a checkpoint of its state. When the checkpoint is reloaded, all previously stores events that occurred between the time of the checkpoint and the crash are replayed in order to restore the state of correlation prior to

[3] Note that the email server is in the IT environment.

the crash. When the ArcSight Manager comes back on-line, it will receive all cached and live events from ArcSight SmartAgent.

If an ArcSight SmartAgent fails, it will continue processing with the next log file line or database row. If the ArcSight SmartAgent is monitoring a live feed, then all events that occurred while the ArcSight SmartAgent was down are lost.

3.5 Protection of the TSF

The ArcSight SmartAgent, ArcSight Manager, and ArcSight Console all protect TSF data from disclosure and modification when it is transmitted between separate parts of the TOE, by communicating using SSL connections. The SSL connection is the standard HTTP over SSL, often referred to as HTTPS (HyperText Transfer Protocol Secure). ArcSight uses X.509 certificates. The certificates must be a 128-bit X.509 Version 3 certificate. The maximum key size for the public key in the certificate is 1024 bits.

For SSL communication, all components of ArcSight 3.0 that are SSL endpoints (ArcSight Console, ArcSight Manager, and ArcSight SmartAgents), need to store two types of key material:

- Key Pairs, consisting of a private key and the matching public key wrapped in a X.509 certificate
- X.509 Certificates of certificate authorities (CAs) whose certificates are trusted.

ArcSight Manager is always the SSL server and the ArcSight SmartAgents and the ArcSight Console that talk to the ArcSight Manager always represent the SSL Client. When a SSL connection is established, the client and server authenticate one another, using the key pairs and certificates in their key stores and trust stores.

The server authentication mechanism in SSL requires the ArcSight Manager to have a valid SSL certificate. An SSL certificate contains the ArcSight Manager's public key. The public key is used by the client to encrypt information. Only the ArcSight Manager (using its private key) can decrypt this information. ArcSight Manager's SSL certificate contains a date range for which it is valid as well as the ArcSight Manager's host name.

4 Assumptions

The following assumptions underlie the evaluation and use of ArcSight 3.0. All of these assumptions are derived from the Intrusion Detection System Analyzer Protection Profile:

4.1 Usage Assumptions

First and foremost, it is assumed that all authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation. It is also assumed that these individuals are competent to manage the TOE and the security of the information it contains, and that only authorized users will access the TOE.

4.2 Environmental Assumptions

A key environmental assumption is physical security, for it is assumed that the TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification, that the processing resources of the TOE will be located within controlled access facilities (which prevents unauthorized physical access), and that the TOE can only be accessed by authorized users.

It is also assumed that the operating environment will provide protection to the TOE and its related data, and that the TOE has access to all the IT System resources necessary to perform its functions. Lastly, it is assumed that the operating environment will provide a reliable time source to enable the TOE to timestamp audit records.

Although not stated as formal assumptions due to the need for profile compliance, it is also assumed that the operating environment provides appropriate support for the services used from the environment, in particular, support for the selected alarm mechanisms (electronic mail or pager transmission interfaces).

4.3 Clarification of Scope

4.3.1 Overarching Policies

The security requirements enforced by the TOE were designed based on the following overarching security policies, as described in the IDS Analyzer Profile:

1. Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to IDS data and appropriate response actions taken.
2. The TOE shall only be managed by authorized users.
3. All data analyzed and generated by the TOE shall only be used for authorized purposes.
4. Users of the TOE shall be accountable for their actions within the IDS.
5. Data analyzed and generated by the TOE shall be protected from modification.
6. The TOE shall be protected from unauthorized accesses and disruptions of analysis and response activities.

4.3.2 Threats Countered and Not Countered

The TOE is designed to fully or partially counter the following threats, as described in the IDS Analyzer Profile:

- That an unauthorized person may attempt to compromise the integrity of the data analyzed and produced by the TOE by bypassing a security mechanism.
- That an unauthorized person may attempt to disclose the data analyzed and produced by the TOE by bypassing a security mechanism.

- That an unauthorized person may attempt to remove or destroy data analyzed and produced by the TOE.
- That an unauthorized person may attempt to compromise the continuity of the TOEs analysis functionality by halting execution of the TOE.
- That an unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.
- That an unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.
- That the TOE may be susceptible to improper configuration by an authorized or unauthorized person causing potential intrusions to go undetected.
- That the TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity.
- That the TOE may fail to recognize vulnerabilities or inappropriate activity based on IDS data received from each data source.
- That the TOE may fail to identify vulnerabilities or inappropriate activity based on association of IDS data received from all data sources.

However, users of the TOE should be cautioned that:

- There is no explicit assumption about the security of the IT Environment. Although it is quite likely that the underlying OS and hardware for those components running ArcSight software will be protected, there is less confidence regarding the alarm notification servers (i.e., email and pager). Given the nature of those mechanisms, users of this product cannot be guaranteed that email or pager messages will be delivered at all, or if delivered, that the contents of the message have not been modified or observed.

5 Architectural Information

Note: The following architectural description is based on the description presented in Part I Evaluation Technical Report for ArcSight 3.0 and in the ArcSight 3.0 Security Target.

5.1 TOE Components

The TOE, ArcSight 3.0, is a subset of the ArcSight product. As noted before, it is a security management software product designed to monitor, analyze, and report on network anomalies identified by third-party network monitoring devices (e.g. Intrusion Detection Systems (IDS) Sensors or IDS Scanners, firewalls, etc).

Note that ArcSight 3.0 is an application, layered on top of an unevaluated operating environment that includes an operating system and hardware components.

The ArcSight 3.0 TOE consists of the following components:

- **ArcSight Console**. The ArcSight Console provides a centralized view into an enterprise. It supports real-time monitoring, in-depth investigative capabilities, and automated responses and resolutions to events, and provides Administrators, Analyzer Administrators, and Operators with an interface to perform security management functions, including viewing audit and monitoring data. The ArcSight Console connects to a single ArcSight Manager at a time via the network.

  The ArcSight Console requires the underlying operating system to provide protection of the TOE. The underlying operating system is considered part of the environment.

- **ArcSight Manager**. The ArcSight Manager is a high performance engine that manages, cross-correlates, filters, and processes all occurrences of security events within the enterprise. It also provides the ability to send alerts via electronic mail or pager. The Manager sits at the center of the ArcSight product and acts as a link between the ArcSight Console, ArcSight Database, and ArcSight SmartAgent.

  The ArcSight Manager relies on the underlying operating system to provide a file system to write audit and error logs, and to protect the file system. For alert notifications, the Manager also depends on the operating environment to provide an SMTP (Simple Mail Transfer Protocol) connection to an outgoing mail server, or an SNPP (Simple Network Paging Protocol) connection to a paging service provider.

- **ArcSight Database**. The ArcSight Database is the logical access mechanism, particular schema, table spaces, partitioning, and disk layout. These structures are used to store all captured events, as well as security management configuration information such as system users, groups, permissions, and defined rules, zones, assets, reports, displays, and preferences.

  The ArcSight Database relies on the environment to provide an Oracle database for its use. The Oracle database provided by the environment is referred to as the underlying database and is responsible for the security and integrity of information it stores. The ArcSight Manager is the only component that communicates directly with the ArcSight Database. The data stored within the ArcSight Database is protected by the underlying database system and by the underlying operating system of the database host.

- **ArcSight SmartAgents**. The ArcSight SmartAgents collect and process events generated by security devices in the operating environment throughout the enterprise. In the general product, there are a wide variety of potential devices: routers, email logs, anti-virus products, firewalls, Intrusion Detection Systems, access control servers, VPN systems, anti-DoS appliances, operating system logs, or other sources where information of security threats are detected and reported. ArcSight SmartAgent can be installed on the ArcSight Manager machine, a separate host machine, or, when supported, directly on a device.

  The evaluated ArcSight 3.0 TOE only includes the following three agents:

  - The **Nessus Agent**, which analyzes the reports produced by the Nessus vulnerability scanner.

- The **CheckPoint Firewall Agent**, which analyzes the information delivered via a proprietary, push protocol (OPSEC) from a Check Point Firewall-1 NG OPSEC.
- The **Snort Agent**, which analyzes the data in an MySQL database produced on a Snort IDS.

The ArcSight SmartAgents rely on the underlying operating system to cache events (security events and error logs) if they cannot be delivered immediately to the ArcSight Manager due to communication problems or if the ArcSight Manager is experiencing temporary bursts of events. The ArcSight SmartAgents also require the underlying operating system to provide protection of the TOE.

The ArcSight 3.0 Console, Manager, Database, and SmartAgents run as applications on top of an operating system and depend on the services exported by the operating system to function. ArcSight uses operating system services for process creation and manipulation; device and file processing; shared memory creation and manipulation; provision of the network stack up through the TCP layer; and security requests such as inter-process communication. The hardware upon which the operating system runs is completely transparent to ArcSight; ArcSight sees only the operating system's user interfaces.

The following table outlines the system requirements for ArcSight 3.0

ArcSight Console		
Platform	**Supported Operating System**	**System Requirements**
Linux	Red Hat Enterprise Linux 3.0 (RHEL 3) Workstation, with KDE or GNOME GUI and Desktop	Pentium III 1.1 GHz High Color (16-bit), 1024 x 768 resolution minimum. Higher recommended 512 MB memory minimum. Higher recommended 1 GB disk space
Windows	Microsoft Windows XP Professional	Pentium III 1.1 GHz High Color (16-bit), 1024 x 768 resolution minimum. Higher recommended 512 MB memory minimum. Higher recommended 1 GB disk space
Solaris	Sun Solaris 9	Sunblade 150 512 MB memory minimum. Higher recommended 1 GB disk space
ArcSight Manager		

Linux	Red Hat Enterprise Linux 3.0 (RHEL 3) ES	Pentium 4 Xeon 2.0 GHz or AMD Opteron 1.6 GHz 2 GB memory 2 GB disk space
Solaris	Sun Solaris 9	UltraSparc IIi, 550 MHz or faster 2 GB memory 2 GB disk space
Windows	Windows 2000 Advanced Server	Pentium 4 Xeon 2.0 GHz or AMD Opteron 1.6 GHz 2 GB memory 2 GB disk space
ArcSight Database		
Oracle 9.2.0.1	Windows 2000 Advanced Server	Pentium III, 1.1 GHz
Oracle 9.2.0.1	Solaris 9, 64-bit	UltraSparc IIi, 550 Mhz
Oracle 9.2.0.1	Red Hat Enterprise Linux 3.0 ES	Pentium III, 1.1 GHz
ArcSight Agents		
Linux	Red Hat Enterprise Linux 3.0 AS	Pentium III 1.1 GHz or faster 512 MB memory 1 GB disk space
Solaris	Sun Solaris 9	Ultra Sparc IIi, 550 MHz or faster 512 MB memory 1 GB disk space
Windows	Windows 2000 Advanced Server	Pentium III 1.1 GHz or faster 512 MB memory 1 GB disk space

5.2 TOE Boundaries

Figure 5-1 illustrates the ArcSight 3.0 TOE and its boundaries. This figure attempts to show that the underlying operating system and its underlying hardware (shown in dashed boxes or circles) are not part of the TOE for any of the four TOE components (shaded boxes and circles). Additionally, other components of the ArcSight product, as noted in the Introduction, are not part of the TOE.

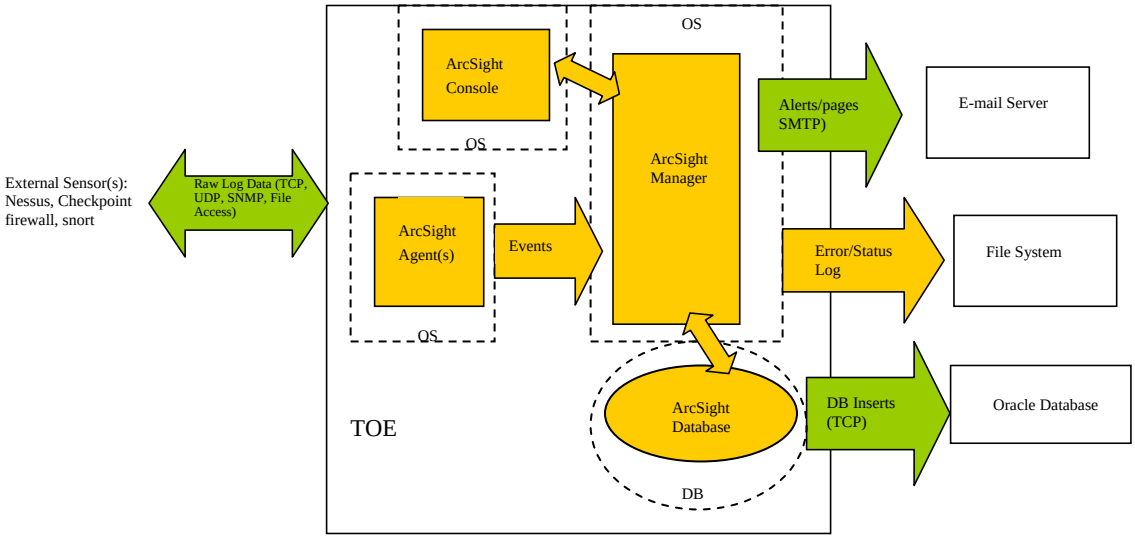

Figure 5-1. Boundaries of the ArcSight 3.0 TOE

In terms of logical boundaries, the following table enumerates the division between services provided *by* the TOE and services provided *to* the TOE from the Operating Environment:

Functional Area	Services Provided *By* The TOE	Services Provided *To* The TOE By The Operating Environment
Audit	Collection of security relevant events such as user logging, service interruptions, server data accessed, etc. Collection of audit data on monitored devices and transmission within the TOE.	Storage and protection of audited records Support for transmission of alerts via SMTP (email) or SNPP (pager). Storage of cached audit events when the main datatbase reaches capacity.
Identification and Authentication	Identification and authentication to the ArcSight console.	Underlying database used to store user information, and protection thereof.
Security Management	Graphical user interfaces that support configuration and modification of the options of the TOE. These modules provide services that support modification of the data collection and review capabilities, queries of audit data, and restriction of access and/or the ability to query and modify all other TOE data to the appropriate authorized user/authorized role.	Underlying database used to store configuration information, and protection thereof.

Protection of the TOE	Encryption for transmission between separated parts of the TOE Assurance that observed events are not lost because of storage exhaustion.	Protection of the TOE executable and process data spaces. Storage of the certificates used for SSL communication. Underlying file system temporarily stores and protects observed events when the storage is exhausted. Timestamps for collected audit information.
IDS Analyzer Functions	Collection of observed events and transmission to the analyzer. Support for specification of analyzer rules. Support for application of analyzer rules to observed events and notification when appropriate conditions are met.	Underlying database used to store collected information and rules, and protection thereof. Support for transmission of alerts via SMTP (email) or SNPP (pager). Execution of commands associated with rules. Caching of events that cannot be delivered or written to the ArcSight database.

Note that ArcSight 3.0 is not intended to make data available to other IT products and in the case of a distributed ArcSight 3.0 architecture, the components are expected to be connected with a benign, private, and protected communication network.

5.3 IT Security Environment

ArcSight 3.0 requires an IT environment that protects the TOE (and its resources) and provides time stamps with at least the same degree of assurance as that claimed by the TOE. It also requires the environment to provide an Oracle database, as well as appropriate support for alarm notification (i.e., servers for outgoing mail or pager mechanisms).

6 Documentation

This section details to the documentation that is (a) delivered to the customer, and (b) was used as evidence for the evaluation of ArcSight 3.0.[4] Note that not all evidence is available to customers. In these tables, the following conventions are used:

- Documentation that is delivered to the customer is shown with **bold** titles.
- Documentation that was used as evidence but is *not* delivered is shown in a normal typeface.

[4] This documentation list is based on the lists provided in the Evaluation Technical Report, Parts 1 and 2, developed by SAIC.

- Documentation that is delivered as part of the product but was not used as evaluation is shown with a bold title, but a hashed background.

The TOE and its guidance are delivered via downloaded. The guidance is part of the TOE components and the patch files and can be downloaded individually.

6.1 Design documentation

Document	Revision	Date
ArcSight 3.0 Agent Properties	(none)	(none)
ArcSight 3.0 Combined Functional Specification and High-Level Design	1.10	2006-07-14
ArcSight Administrator's Guide	3.0 SP2	2006-03-17
ArcSight Agent Commands	1.1	2004-11-10
ArcSight Agent Commands and Responses	1.2	2005-04-12
ArcSight Agent Files	1.0	2004-11-11
ArcSight Audit Events	1.5	2005-12-16
ArcSight Binary Event Serialization	(none)	2004-05-14
ArcSight Configuration Resources	1.03	2005-08-09
ArcSight Console Commands	1.2	2005-04-12
ArcSight Console Error messages	1.3	2005-12-19
ArcSight Console Files	1.0	2004-11-10
ArcSight Inter-Component Messaging	1.1	2004-06-10
ArcSight Logged Error Messages	1.1	2005-12-29
ArcSight Manager Commands	1.5	2004-11-15
ArcSight Manager Files	1.1	2004-04-22
ArcSight Manager Servlets and Web Applications	1.1	2004-11-10
ArcSight Manager XML RPC	(none)	(none)
ArcSight Security Domain	1.0	2004-11-18
ArcSight Security Events	1.0	2004-01-30
ArcSight Threat Level Formula	1.0.0	2003-01-20
Client Defaults	(none)	(none)
Console Defaults	(none)	(none)
Nessus Vulnerability Report DTD	0.2	(none)
Server Defaults	(none)	(none)
Using the ArcSight Console	3.0 SP2	(none)

6.2 Guidance documentation

Document	Revision	Date
ArcSight Administrator's Guide	3.0 SP2	2006-03-17
ArcSight ESM Release Notes	3.0 SP2	(none)
ArcSight README	(none)	2004-11-12
ArcSight SmartAgent Installation Guide, ArcSight Version 3.0	3.0	(none)

Document	Revision	Date
Patch readme files: Patch 9 (3.0.2.9.3939)	3.0.2.9.3939	2006-03-22
SmartAgent Configuration Guide, Check Point FireWall-1, 4.1 OPSEC Agent, NG OPSEC Agent	(none)	2006-03-17
SmartAgent Configuration Guide, Nessus Vulnerability Scanner, Report Agent	(none)	2006-03-17
SmartAgent Configuration Guide, Snort, Open Source Network Intrusion Detection System, Database Agent, Log-file Agent	(none)	2006-01-30
SmartAgent Readme	(none)	2006-03-17
Using the ArcSight Console	3.0 SP2	(none)

6.3 Configuration Management and Lifecycle documentation

Document	Revision	Date
Basic Flaw Remediation (ALC_FLR.1)	1.3	2005-09-21
Configuration Management (ACM_CAP-3)	1.6	(none)
Identification of Security Measures (ALC_DVS.1)	1.6	2006-03-09
Information Systems Access Policy	(none)	(none)
p4_sample.log (sample of the log from Perforce)	(none)	(none)
Perforce and Branching	1.1	(none)
Perforce Configuration Items for ArcSight 3.0	1.3	(none)
Perforce Naming Conventions	1.1	(none)

6.4 Delivery and Operation documentation

Document	Revision	Date
ArcSight Administrator's Guide	3.0 SP2	2006-03-17
ArcSight ESM Release Notes	3.0 SP2	(none)
ArcSight README	(none)	2004-11-12
ArcSight SmartAgent Installation Guide, ArcSight Version 3.0	3.0	(none)
Delivery Procedures (ADO_DEL.1)	1.2	2005-10-12
Installation, generation, and start-up procedures (ADO_IGS.1)	1.2	2005-12-21
Patch readme files: Patch 9 (3.0.2.9.3939)	3.0.2.9.3939	2006-03-22
SmartAgent Configuration Guide, Check Point FireWall-1, 4.1 OPSEC Agent, NG OPSEC Agent	(none)	2006-03-17
SmartAgent Configuration Guide, Nessus Vulnerability Scanner, Report Agent	(none)	2006-03-17
SmartAgent Configuration Guide, Snort, Open Source Network Intrusion Detection System, Database Agent, Log-file Agent	(none)	2006-01-30
SmartAgent Readme	(none)	2006-03-17

Using the ArcSight Console	3.0 SP2	(none)

6.5 Test documentation

Document	Revision	Date
ArcSight Inc. Common Criteria Test Plan	1.16	2006-03-21
ArcSight.CC.TestCases.v1.4	1.4	(none)
ArcSight.CC.TestResults.Sol.v1.0.xls	1.0	(none)
ArcSight.CC.TestResults.Win.v1.0.xls	1.0	(none)

6.6 Vulnerability Assessment documentation

Document	Revision	Date
ArcSight 3.0 Strength of Security Functions (AVA_SOF.1)	1.6	2006-03-22
ArcSight Administrator's Guide	3.0 SP2	2006-03-17
ArcSight ESM Release Notes	3.0 SP2	(none)
ArcSight README	(none)	2004-11-12
ArcSight SmartAgent Installation Guide, ArcSight Version 3.0	3.0	(none)
ArcSight VERSION 3.0 Preinstallation	(none)	2004-04-02
Patch readme files: Patch 9 (3.0.2.9.3939)	3.0.2.9.3939	2006-03-22
SmartAgent Configuration Guide, Check Point FireWall-1, 4.1 OPSEC Agent, NG OPSEC Agent	(none)	2006-03-17
SmartAgent Configuration Guide, Nessus Vulnerability Scanner, Report Agent	(none)	2006-03-17
SmartAgent Configuration Guide, Snort, Open Source Network Intrusion Detection System, Database Agent, Log-file Agent	(none)	2006-01-30
SmartAgent Readme	(none)	2006-03-17
Using the ArcSight Console	3.0 SP2	(none)
Vulnerability Analysis	1.6	2006-03-22

6.7 Security Target

Document	Revision	Date
ArcSight 3.0 Security Target	1.0	2006-09-27

7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the Evaluation Team Test Plan, contained in Part II

of the ETR, and has been reviewed to ensure it does not contain vendor proprietary information.

7.1 Developer Testing

Evaluator analysis of the developer's test plans, test scripts, and test results indicated that the developer's testing is adequate to satisfy the requirements of EAL3.

The developer's tests of TOE security functions were provided by a series of manual tests. The test procedure descriptions provided by the developer described in detail how each test was implemented. These served to provide a good understanding of the purpose of the test, including a description of the test cases and variations that are tested by the corresponding tests. In addition each test procedure document included instructions for the repeatable execution of the tests, including a description of any requirements for establishing the test environment for each test as well as a description of how to actually execute each test and verify its results against the expected results.

The evaluation team verified that the test coverage was suitable through analysis of the developer-provided test documentation. This analysis verified that the tests provided adequate coverage of all interfaces. Given the mapping is complete with respect to interfaces, the evaluation team concluded the coverage is complete with respect to the requirements.

With respect to depth, the evaluation team was able to trace all aspects of the implementation of security functions in the high-level design back to test cases. Multiple test cases existed for every interface, ensuring proper negative, positive, and boundary testing.

The developer provided the evaluation team with actual results for their testing of the product. The evaluation team analyzed the provided actual results against the results obtained by the evaluation team by running a subset of the test cases. the results obtained were consistent with identified expected results.

7.2 Evaluation Team Independent Testing

In addition to developer testing, the CCTL conducted its own suite of tests. The evaluation team tested the product on the following platforms:

- ArcSight Console:
    - Pentium III 1.1 GHz – for Windows OS
    - Sunblade 150 – for Solaris
- ArcSight Manager
    - Pentium 4 Xeon 2.0 GHz or AMD Opteron 1.6 GHz – for Windows OS
    - UltraSparc IIi, 550 MHz or faster – for Solaris OS
- ArcSight Database
    - Pentium III 1.1 GHz – for Windows OS

- UltraSparc IIi, 550 MHz or faster – for Solaris OS

The versions of the software used for testing were:

- TOE Software
  - Windows:
    - ArcSight-3.0.2.3939.0-DB-Win.exe (for Windows)
    - ArcSight-3.0.2.3939.0-Manager-Win.exe (for Windows)
    - ArcSight-3.0.2.3939.0-Console-Win.exe (for Windows)
    - ArcSight-3.5.1.4332.0-Agent-Win.exe (for Windows)
  - Solaris:
    - ArcSight-3.0.2.3939.0-DB-Solaris.bin (for Solaris)
    - ArcSight-3.0.2.3939.0-Manager-Solaris.bin (for Solaris)
    - ArcSight-3.0.2.3939.0-Console-Solaris.bin (for Solaris)
    - ArcSight-3.5.1.4332.0-Agent-Solaris.bin (for Solaris)
  - Patches:
    - Patch-3.0.2.6.3939-DB.zip
    - Patch-3.0.2.8.3939-Manager.zip
    - Patch-3.0.2.8.3939-Console.zip
- IT Environment Software
  - ArcSight Console:
    - MS Windows XP Professional
    - Sun Solaris 9
  - ArcSight Manager
    - MS Windows 2000 Advance Server
    - Solaris 9
  - ArcSight Database
    - MS Windows 2000 Advanced Server
    - Solaris 9, 64-bit
  - ArcSight SmartAgents
    - Windows 200 Advance Server
    - Solaris 9
- Test software

- Test Alert Agent

The CCTL verified that each of these platforms was running the TOE version of the firmware and the software. The CCTL installed the TOE and configured it in accordance with the provided guidance.

The evaluation team developed independent tests based on perceived gaps or areas of weakness in the developer's test suite, based on the preceding coverage and depth analyses. The focus was placed upon areas where the developer test documentation did not cover completely. The validator reviewed these independent tests and felt that they provided sufficient supplemental coverage to the vendor tests. The evaluation team used the exact configuration documented in the vendor test documentation, and uses the vendor test subset was to perform the team test. The evaluation team also used the same test tools documented in the vendor test documentation to perform the team test subset.

These tests identified some discrepancies between the actual implementation and the implementation documented. The vendor has updated the documentation.

7.3 Evaluation Team Penetration Testing

The CCTL also conducted penetration testing, using the same setup used for the independent team tests.

Prior to developing its tests, the CCTL followed well-established penetration test development procedures. This effort considered design documentation evaluation, guidance documentation evaluation, test documentation evaluation, code review, vulnerability analysis evaluation. It was revisited subsequent to the running of a portion of the vendor test subset. Therefore, it took advantage of TOE knowledge gained from each of these activities.

This resulted in small number of penetration tests. The validator reviewed these tests, and felt that they adequately explored areas of potential vulnerability. Execution of these tests resulted in some documentation clarifications, but identified no security vulnerabilities.

8 Evaluated Configuration

The evaluated configuration of ArcSight 3.0, as defined in the Security Target, consists of the following components:

- ArcSight Console (ArcSight-3.0.2.3939.0-Console) with Patch 9 (Patch-3.0.2.9.3939-Console).
- ArcSight SmartAgents for Nessus, Check Point Firewall-1 NG OPSEC, and Snort IDS DB (ArcSight-3.5.1.4339.0 - Agent).
- ArcSight Manager (ArcSight-3.0.2.3939.0-Manager) with Patch 9 (Patch-3.0.2.9.3939-Manager).
- ArcSight Database (ArcSight-3.0.2.3939-DB) with Patch 6 (Patch-3.0.2.6.3939-DB).

The ArcSight 3.0 TOE must be configured in accordance with the following Guidance Documents:

- ArcSight Administrator's Guide, Version 3.0 SP2, March 17, 2006 [1]
- Using the ArcSight Console, Version 3.0 SP2 [2]
- ArcSight README, November 12, 2004 [3]
- ArcSight ESM Release Notes version 3.0 SP2 [4]
- ArcSight SmartAgent Installation Guide, ArcSight Version 3.0 [5]
- SmartAgent Configuration Guide, Check Point FireWall-1, 4.1 OPSEC Agent, NG OPSEC Agent, March 17, 2006 [6]
- SmartAgent Configuration Guide, Nessus Vulnerability Scanner, Report Agent, March 17, 2006 [7]
- SmartAgent Configuration Guide, Snort, Open Source Network Intrusion Detection System, Database Agent, Log-file Agent, January 30, 2006 [8]
- SmartAgent Readme, March 17, 2006 [9]
- Patch readme files: Patch 9 (3.0.2.9.3939), March 22, 2006 [10]

9 Results of the Evaluation

The evaluation was conducted based upon the Common Criteria (CC), Version 2.1, dated August 1999 [11][12][13]; the Common Evaluation Methodology (CEM), Version 1.0, dated August 1999 [15]; and all applicable International Interpretations in effect on April 1, 2004. The evaluation confirmed that the ArcSight 3.0 is compliant with the Common Criteria Version 2.1, functional requirements (Part 2) and assurance requirements (Part 3) for EAL3 augmented with ALC_FLR.1. The details of the evaluation are recorded in the CCTL's evaluation technical report, *Evaluation Technical Report for ArcSight 3.0*, Part 1 (Non-Proprietary) [18] and Part 2 (Proprietary) [19]. The product was evaluated and tested against the claims presented in the ArcSight 3.0 Security Target v1.0, 8 September 2006 [17].

The Security Target was found to be conformant with the U.S. Government Intrusion Detection System Analyzer Protection Profile, Version 1.2, April 27, 2005 [20], as modified by errata and observation decisions. Note that although not all PP SFRs are included in the ST, the omitted SFRs are acknowledged as being trivially satisfied due to the nature of the product as a stand-alone analyzer, obviating the need for the capability to securely export information to another analyzer product. This is in accordance with OD 0250/PD 0127.

The validator followed the procedures outlined in the Common Criteria Evaluation Scheme publication number 3 for Technical Oversight and Validation Procedures [16]. The validator has observed that the evaluation and all of its activities were in accordance with

the Common Criteria, the Common Evaluation Methodology, and the CCEVS. The validator therefore concludes that the evaluation team's results are correct and complete.

The following evaluation results are extracted from the non-proprietary Evaluation Technical Report provided by the CCTL, and are augmented with the validator's observations thereof.

9.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the ASE product that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.2 Evaluation of the Configuration Management Capabilities (ACM)

The evaluation team applied each EAL 3 ACM CEM work unit. The ACM evaluation ensured the TOE is identified such that the consumer is able to identify the evaluated TOE. The evaluation team ensured the adequacy of the procedures used by the developer to accept, control and track changes made to the TOE implementation, design documentation, test documentation, user and administrator guidance, security flaws and the CM documentation. To support the ACM evaluation, the evaluation team received Configuration Management (CM) records from Arcsight.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of the Delivery and Operation Documents (ADO)

The evaluation team applied each EAL 3 ADO CEM work unit. The ADO evaluation ensured the adequacy of the procedures to deliver, install, and configure the TOE securely. The evaluation team ensured the procedures addressed the detection of modification while in transit. The evaluation team followed the Configuration Guide to test the installation procedures to ensure the procedures result in the evaluated configuration.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of the Development (ADV)

The evaluation team applied each EAL 3 ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification and a high-level design document. The evaluation team also ensured that the correspondence analysis between the design abstractions correctly demonstrated that the lower abstraction was a correct and complete representation of the higher abstraction.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.5 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each EAL 3 AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. Both of these guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.6 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each EAL 3 ALC CEM work unit. The evaluation team ensured the adequacy of the developer procedures to protect the TOE and the TOE documentation during TOE development and maintenance to reduce the risk of the introduction of TOE exploitable vulnerabilities during TOE development and maintenance. To support the ALC evaluation, the evaluation team verified that the claimed procedures were followed during a site visit.

In addition to the EAL 3 ALC CEM work units, the evaluation team applied the ALC_FLR.1 work units from the CEM supplement. The flaw remediation procedures were evaluated to ensure that flaw reporting procedures exist for managing flaws discovered in the TOE.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.7 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each EAL 3 ATE CEM work unit. The evaluation team ensured that the TOE performed as described in the design documentation and

demonstrated that the TOE enforces the TOE security functional requirements. Specifically, the evaluation team ensured that the vendor test documentation sufficiently addresses the security functions as described in the functional specification and high level design specification. The evaluation team performed a sample of the vendor test suite, and devised an independent set of team test and penetration tests. The vendor tests, team tests, and penetration tests substantiated the security functional requirements in the ST.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.8 Vulnerability Assessment Activity (AVA)

The evaluation team applied each EAL 3 AVA CEM work unit. The evaluation team ensured that the TOE does not contain exploitable flaws or weaknesses in the TOE based upon the developer strength of function analysis, the developer vulnerability analysis, the developer misuse analysis, and the evaluation team's misuse analysis and vulnerability analysis, and the evaluation team's performance of penetration tests.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.9 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's performance of a subset of the vendor tests suite, the independent tests, and the penetration test also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

10 Validator Comments/Recommendations

- The evidence submitted for evaluation, as reported by the CCTL, did not consistently present good unique references (i.e., dates and version numbers). Although the CCTL did verify that this information was indeed under configuration control, the CM approach of the vendor could be strengthened if all evidence and items issued to customers had unique version numbers and dates.
- During testing, the validator had the opportunity to see this product in use. Although the product is complicated in description, its interface is relatively easy to use with many supporting features to help the user.

11 Annexes

Not applicable.

12 Security Target

The Security Target is identified as *ArcSight 3.0 Security Target,* Version 1.0, 8 September 2006.

13 Glossary

The following definitions are used throughout this document:

- **Access Control Lists.** ArcSight uses Access Control Lists (ACLs) to manage user group permissions. These lists define which user groups have permissions to which resources, and to which ArcSight components such as rules, reports, and filters.
- **Actions.** Actions are automatic procedures that occur when all rule conditions and threshold settings have been met. An ArcSight Administrator can choose to be notified of a triggered rule at the ArcSight Console or through the Notifier, have information about the events that triggered the rule sent to a case or an active list, or automatically execute a command line function. The Administrator can also assign more than one rule action to any rule.
- **Active Lists**. An Active Lists is a list of potential targets of attack, usually by IP address. They are used to monitor activity based on any rule-driven combination of event attributes or set of custom fields. Active Lists can either be populated manually, or in conjunction with rules specifically tailored to work with them that can dynamically add and remove entries on lists. They draw from the event stream on the basis of their event or field/rule definitions and any rules designed to affect them. ArcSight includes a set of default items in the Active Lists resource tree that can be used for templates or for operational monitoring with minor modifications.
- **Aggregation**. Aggregation is a composition technique for building a new event from one or more existing events that support some or all of the new event's conditions. It is used to group occurrences of matching conditions based on incoming event field data values, and optionally count only distinct occurrences of those events.
- **ArcSight Administrator**. An ArcSight administrator is a person who has the rights to administer ArcSight and manage users, groups, and their permissions.
- **ArcSight Console**. The ArcSight Console is a centralized view into an enterprise. A graphical user interface that provides centralized intelligent real-time monitoring to secure the enterprise.
- **ArcSight Database**. The ArcSight Database is a central repository for all ArcSight events. Once an event occurs, its data fields such as severity, create time, rules

triggered, and so forth are stored in the ArcSight Database. The ArcSight Database stores all enterprise events in a normalized schema. The ArcSight Manager is the only component that communicates with the database.

- **ArcSight Manager**. The ArcSight Manager is the component that manages, cross-correlates, filters, and processes all security-event occurrences in the enterprise. The ArcSight Manager includes a Cross-Correlation Engine, Agent Data Manager, tracking and resolution functions, and analytics and reporting capabilities. The ArcSight Manager also accesses the ArcSight Database.
- **ArcSight SmartAgents**. ArcSight SmartAgents are collectors of security event information generated by multi-vendor security devices throughout the enterprise. SmartAgents normalize and correlate this data into events, expressed as ArcSight Messages, which are forwarded to the Agent Data Manager (a component of the ArcSight Manager) for further processing. SmartAgents can reside on a device, on the ArcSight Manager, or on a host machine.
- **Attack**. An attack is an exploited threat or 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.
- **Authentication.** Verification of the identity of a user.
- **Cases**. Cases are entries in an event-tracking system used to track, investigate, and resolve suspicious events in a workflow-type environment. When suspicious events occur, cases are created and assigned to users, who then investigate and resolve them based on enterprise policies and practices.
- **Common Conditions Editor**. ArcSight provides a common framework and user interface for defining conditions for different resources such as filters, rules, and reports.
- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conditions**. Conditions are logical expressions used to qualify events or other grouping of elements. Conditions can be specified in a number of places using a common condition editor; for example, to define rules or filters.
- **Conformance**. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Correlation**. Logically linking events based on multiple conditions.
- **Correlation Rule**. A programmed procedure that expresses conditions and actions, and evaluates events or meta-events. A rule has two parts: a condition and an action. A condition determines whether a state exists and satisfies related expressions. If so, an action expression defines the response to the condition. A rule can have one or more

conditions. A rule can be created for any incoming event from one or more event generators, with various conditions, logic statements, and thresholds.

- **Cross-correlation Engine**. The cross-correlation engine is a component of the ArcSight Manager that evaluates rules against a set of data.
- **Dashboards**. A dashboard is a customizable view of the enterprise that summarizes event information by collectively managing one or more data monitors.
- **Data Monitors.** Data monitors are views within the dashboard that can be configured to report on events, filters, rules, and other data or information that is of particular interest to the user. Data monitors can be arranged within dashboards in numerous viewing layouts. Data monitors collect summary information on top events, most recent event activity, partial rule occurrences, hourly event counts, or event averages. Once data monitors are created, they can be used by other users in different dashboards. Therefore, changes to data monitors will be visible to other users using the same data monitor. Data monitors are sources of summary information collected on various data stored in the ArcSight Database that can be displayed in different view formats to monitor particular events, filters, system activity, or other areas of interest. Once data monitors are created, they can be used to display information in a dashboard. Data monitors only display events visible to the user of the monitor. Administrators can limit visibility of or control access to dashboards and data monitors by changing access control lists (ACLs) as needed.
- **Device**. Devices are the source points of security events. They produce data that is correlated and normalized into events by SmartAgents. Devices deployed throughout the infrastructure monitor the enterprise and generate events. These devices can be physical resources, such as Intrusion Detection Systems (IDSs), firewalls, routers, database logs, anti-virus products, and other sources for detecting security threats.
- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Events**. Events are the correlated raw data collected from devices. Events are collected by devices throughout the enterprise. Each device has a SmartAgent that retrieves, filters, and forwards these events to the Console. Using the Console, the Administrator is able to monitor and respond to these events. When critical events are generated, notification is provided.
- **Events Grid**. An events grid is a view in the ArcSight Console that shows event summary information. Grid views display events organized in rows and columns. As

new events occur, they are inserted into the grid at the appropriate point . Rows contain events while columns contain data fields.

- **Filtering**. Filtering is used to specify criteria that narrows the scope of monitored data and reduces the number, or constrains the nature, of the events displayed through the Console. Filtering criteria are based on the Console's event data fields, used in various combinations and with various conditions placed on their content.
- **Heartbeat**. A heartbeat is a type of message sent by a SmartAgent to the Agent Data Manager (a component of the ArcSight Manager) to determine if new security policy or property changes have occurred.
- **Knowledge Base**. The Knowledge Base is a problem-solving database containing information on event data, associated if-then-else rules, cases, and so forth. All information is based on community expertise and internal corporate practices and policies.
- **Meta-events**. Events that are generated by a triggered ("fired") ArcSight rule as a reaction to an original sensor-generated event. In other words, an event concerning an event.
- **myArcSight**. myArcSight is a web-based client of the ArcSight Manager. It offers a subset of the features found in the ArcSight Console. *It is not included in the evaluated configuration.*
- **Normalization**. Normalization means optimizing data to reduce redundant storage and to improve speed of access. In ArcSight, this refers to the process by which information emerging from different devices is resolved into a common format and storage structure and naming convention, in order to make possible all of ArcSight's analytic processing operations.
- **Notifications**. Notifications refers to the event-related messages ArcSight can send to email addresses, pagers, or cell phones. Sending notifications is one among several rule actions that can be performed when a rule fires. When you create a rule and add a Send To Notifier action, you will be able to select the notification group that will receive the message. *Note that the TOE's only involvement in the notification is the transmission of the notification; the notification server, transmission, and end user agents (e.g., mail readers, pager devices) are in the IT environment.*
- **Pattern Discovery**. ArcSight's TrueThreat Pattern Discovery can detect subtle, specialized, or long-term patterns that might otherwise go undiscovered in the flow of events. *Pattern Discovery is not part of the evaluated configuration.*
- **Payload**. This refers to the information carried in the body of an event's network packet, as distinct from the packet's header data. While security event detection and analysis usually centers on header data, packet payload may also be forensically significant. Administrators can retrieve, preserve, or discard payloads using the ArcSight Console. As event payloads are relatively large, ArcSight does not store them by default. Instead, payloads can be requested from devices, for selected events, through the Console.

- **Reports**. Reports are captured views or analyses of information that can be viewed in the ArcSight Console in PDF, HTML, Excel, Comma Separated Value (csv), or Rich Text Format (rtf).
- **Relational Database-Management System (RDBMS).** A type of database-management system that stores data in the form of related tables.
- **Resources**. ArcSight components that can be paired with each other with inspect or edit access.
- **Response**. An automatic or manual reaction to an event or meta-event. For example, an operator creates a case, a notification is sent, etc.
- **Rule Actions.** Rule actions are automatic procedures that occur when all rule conditions and threshold settings have been met.
- **Rule Chain**. Rules designed to trigger in a series in order to capture or act upon correlated events within a specified interval or at a particular threshold.
- **Rule Conditions**. A rule is a programmed procedure that can cross-correlate and transform events into meta-events, as determined by security policy. When creating rules, the rule events and conditions, thresholds, and actions are defined. Conditions define which events trigger the rule, thresholds set when a meta-event is generated, and actions state what responses are taken when a meta-event is generated. A rule must have at least one event and one condition.
- **Rules**. An ArcSight rule is a programmed procedure that cross-correlates and transforms events into meta-events, as determined by security policy. Rules express conditions and actions, and are evaluated on events or other meta-events.
- **Schema**. The structure of a database, including tables, columns, and indexes, and the relationships between them.
- **Secure Sockets Layer**. Secure Sockets Layer (SSL) is a method of securing communication between ArcSight SmartAgents, ArcSight Managers, and ArcSight Consoles using HTTP (HTTPS).
- **SMTP (Simple Mail Transfer Protocol)**. SMTP is used to send e-mail. An SMTP server must be configured either at install time or through context (right-click) menu e-mail settings. For notifications, the relevant fields are "from address", which designates the e-mail address of notification e-mail sent from ArcSight, and the "outgoing e-mail server," which is the SMTP server ArcSight uses to send e-mail. It is important to ensure that the "from address" specified is one that will not be rejected by the SMTP server, since some SMTP servers will reject unknown e-mail addresses. POP3 and IMAP can be used to check for e-mail acknowledgments.
- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.

- **Threat**. In the ArcSight sense, this is means through which the ability or intent of a threat agent to adversely affect an automated system, facility, or operation can be manifest. A potential violation of security.
- **Threat Evaluation**. ArcSight incorporates a system of security-threat evaluation that culminates in the Priority field seen in views, reports, or event details. The Priority field uses a scale of 0-10 to rate incoming events, with 10 being the most-significant value.
- **Thresholds**. There are two types of thresholds: rule thresholds and event thresholds. A rule threshold is the point at which a rule is triggered and a meta-event generated. An event threshold is the number of times the event must occur before the rule threshold. A rule can have a threshold that states when the rule is triggered and also specify a threshold for each rule event. For example, thresholds can be created so that a rule is triggered only after all the events in the rule have occurred a set number of times.
- **User Groups**. User groups are named and organized collections of ArcSight users.
- **Users**. ArcSight users are individuals who are assigned login names, passwords, and privileges to access and perform operations using the ArcSight Console.
- **Validation**. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.
- **Views**. "Views" is a collective term for all the different options a user has for seeing raw and processed event information in the ArcSight Console's Viewer panel.
- **Vulnerabilities**. A vulnerability is a hardware, firmware, or software flaw that leaves an Automated Information System (AIS) open for potential exploitation. A weakness in automated system security procedures, administrative controls, physical layout, internal controls, and so forth, that could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.

14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] ArcSight Inc. *ArcSight Administrator's Guide*, Version 3.0 SP2, March 17, 2006.

[2] ArcSight Inc. *Using the ArcSight Console*, Version 3.0 SP2

[3] ArcSight Inc. *ArcSight README*, November 12, 2004.

[4] ArcSight Inc. *ArcSight ESM Release Notes*, Version 3.0 SP2

[5] ArcSight Inc. *ArcSight SmartAgent Installation Guide*, ArcSight Version 3.0

[6] ArcSight Inc. *SmartAgent Configuration Guide, Check Point FireWall-1, 4.1 OPSEC Agent, NG OPSEC Agent*, March 17, 2006

[7] ArcSight Inc. *SmartAgent Configuration Guide, Nessus Vulnerability Scanner, Report Agent*, March 17, 2006

[8] ArcSight Inc. *SmartAgent Configuration Guide, Snort, Open Source Network Intrusion Detection System, Database Agent, Log-file Agent*, January 30, 2006

[9] ArcSight Inc. *SmartAgent Readme*, March 17, 2006

[10] ArcSight Inc. *Patch readme files: Patch 9 (3.0.2.9.3939)*, March 22, 2006

[11] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 2.1, August 1999. CCIMB-99-031.

[12] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 2.1, August 1999. CCIMB-99-032.

[13] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 2.1, August 1999. CCIMB-99-033.

[14] Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security* – Part 1: Introduction and general model, Version 0.6, 11 January 1997.

[15] Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security* – Part 2: Evaluation Methodology, Version 1.0, August 1999.

[16] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 1.0, January 2002.

[17] Science Applications International Corporation. *ArcSight 3.0 Security Target*, Version 1.0, September 29, 2006

[18] Science Applications International Corporation. ·*Evaluation Technical Report for the ArcSight 3.0, Part I (Non-Proprietary)*, Version 1.0, 29 September 2006

[19] Science Applications International Corporation. ·*Evaluation Technical Report for the ArcSight 3.0, Part II (Proprietary)*, Version 1.0, 29 September 2006

Note: This document was used only to obtain the description of the test effort.

[20] U.S. Department of Defense. *U.S. Government Intrusion Detection System Analyzer Protection Profile*, Version 1.2, April 27, 2005.