

# Computer Security Log Files as Evidence

## An Evaluation of ArcSight ESM

### I. Executive Summary

It is the opinion of Kahn Consulting, Inc., that ArcSight's Enterprise Security Management ("ESM") system provides capabilities that support its use as a platform for the management of computer security log files as evidence. ArcSight ESM is designed in a manner that protects the security and trustworthiness of the information collected, processed, correlated, and managed by the system. By providing information protection capabilities, and processing data according to documented processes, ArcSight ESM works to ensure that the security and trustworthiness of the information that it manages is protected.

### II. Evaluation Overview and Background

#### Introduction

Kahn Consulting, Inc. ("KCI") was engaged by ArcSight, Inc. ("ArcSight") to evaluate the company's ArcSight Enterprise Security Management system. The primary purpose of this Evaluation is to assess the product's utility as a platform for collecting, analyzing, correlating, and generally managing computer security log files as evidence. In conducting this Evaluation, KCI has assessed ArcSight capabilities against criteria derived from broad legal and regulatory requirements and best practices for the management of electronic information and records. The proper management of computer security log file information should be undertaken by organizations in the context of a formal, policy-driven program of people, processes, and technology.<sup>1</sup>

*"Organizations should consider implementing a log management infrastructure that includes centralized log servers and log data storage."*

*Guide to Computer Security Log Management, National Institute of Standards and Technology, Special Pub. 800-92 (Draft)*

*Not a legal opinion or legal advice. For all questions regarding compliance with specific laws and regulations seek legal counsel.*

WHERE LAW & TECHNOLOGY MEET

**KAHN**  
CONSULTING INC.

August 2006

## Evaluation Background

Today more than ever before, organizations rely upon digital information to do business. Not only are more transactions executed electronically than ever before, transactions of greater value and risk continue to move into the electronic environment. As electronic business has proliferated, so too has the volume and diversity of threats to the security, confidentiality, and integrity of the digital information that provides the foundation of business today.

Organizations have responded appropriately to these threats by incorporating software and hardware throughout their networks designed to monitor and control access to information systems and the information these systems contain. However, several factors have worked together to make the management and use of this information a challenge for many organizations:

- The increasing volume of software applications and hardware devices that generate log files that may be important from an evidentiary perspective
- Increasingly distributed networks and systems with more access points requiring management
- Increasing complexity and interdependency of systems (e.g., the increasing use of Service Oriented Architectures)
- The increasing sophistication of attacks from malicious parties both inside and outside the network
- The growing scrutiny of information management and information protection practices by courts, regulators, and other parties
- Increasing penalties, fines, sanctions, and other negative consequences for information management and information protection failures
- Lack of standardization in the log file formats generated by security systems

As a result of these and other challenges, organizations are turning to systems that can help them better collect, process, and act on the information found in log files generated by security software and devices throughout their network.

WHERE LAW & TECHNOLOGY MEET



### III. About ArcSight ESM

ArcSight Enterprise Security Management (ESM) is a software system designed to enable organizations to collect, monitor, analyze, and act upon computer security log file information in an efficient and effective manner. ArcSight ESM is designed to ingest large volumes of heterogeneous log file information and to intelligently correlate and present that information to a variety of user communities in a manner that enables informed decision-making.

ArcSight can ingest security log file information from over one hundred and fifty different security devices, and is designed to integrate with existing networks.<sup>2</sup> ArcSight is delivered with default security, processing, and report settings, but is configurable to network design specifics and security priorities.

ArcSight is also designed to store and manage information in a manner that maintains evidentiary quality, as detailed in Sections V and VI of this Evaluation. In this regard, ArcSight is designed to enable authorized access, management, and processing of data; the secure storage and retrieval of various data categories; secure data transport; and the retention of information for audit and legal purposes.

The flow of information within ArcSight ESM is as follows:

- 1) “ArcSight SmartConnectors” normalize, categorize, and securely transmit log file information to the “ArcSight Manager” (transmission frequency is user-configurable).
- 2) The ArcSight Manager performs correlation and detects threats and compliance violations in real time from the log file information transmitted by the SmartConnectors.
- 3) ArcSight Manager stores the data in the “ArcSight Database.” The period of time that log file information is retained within the database can be customized to reflect individual network, corporate, and compliance policies.
- 4) For reporting purposes, users can access the ArcSight Manager through the ArcSight Web using a web browser. “ArcSight Web” enables users to view data and run reports on data already stored within the ArcSight Database. ArcSight Web does not allow access to administrative functions.
- 5) Administrators can access ArcSight ESM controls and configuration options through the work station-based “ArcSight Console” interface.

WHERE LAW & TECHNOLOGY MEET



## IV. Computer Security Log Files as Evidence

Computer security log file management systems are designed to enable organizations to better manage the growing volume and complexity of security-related computer log file information that is generated within an organization. This information is used to make critical decisions about security strategy and tactics, and to respond appropriately to security incidents, among other things.

However, computer log files are also increasingly used as evidence during the course of internal investigations, lawsuits, government investigations, audits, and other formal matters. As such, rather than viewing log file information as merely “technical” or tactical information, many organizations today view certain computer security log files as a unique form of “evidence” that must be managed in a manner that reflects its intended or possible future use.

The use of computer security log files as evidence raises several issues regarding the legal admissibility and credibility of the information. Any organization wishing to rely upon electronic information for legal and regulatory purposes, or wishing to submit it as legal evidence must address two separate - but related - challenges. First, the information must be *admissible* – that is, it must be acceptable to the court or to the regulator. The admissibility of electronic information is governed by a variety of laws, but, with some limited exceptions, in most instances and in most jurisdictions, there are no specific prohibitions on the admissibility of electronic information as evidence.

The second challenge for electronic information is that it must be *credible*. In other words, electronic information must be authentic, complete, and trustworthy enough to deserve to influence the outcome of a legal proceeding. Even if such evidence is found to be generally admissible, its integrity can nonetheless still be attacked, and it can be excluded or its influence on the proceeding can be severely diminished.

## V. Normalization and Evidentiary Issues

### Overview

From a high level, the normalization process, which is executed by the ArcSight SmartConnectors, is designed to convert log file information from proprietary, heterogeneous formats, into a universal format that ArcSight ESM can process and analyze. During normalization, “event data,” such as data indicating a security event’s priority, time of occurrence, and so on, is converted into a common ArcSight ESM data schema (i.e., format). This common format can be filtered and aggregated, with the primary intent being the reduction of the volume of duplicative or otherwise unnecessary information processed by ArcSight.

Because the normalization process alters the log file as it is initially created by the originating data source (i.e., security software or device), the impact of the normalization process on the evidentiary quality of data stored and managed by ArcSight ESM bears evaluation.

Various laws and regulations have made clear that authentic electronic information can be admissible. However, these laws and regulations have also made clear that standards of information integrity and accuracy must be met. In fact, the courts have excluded electronic evidence that they have deemed untrustworthy. In addition, it does an organization little good to expend the resources necessary to capture and store electronic information if the organization itself cannot be sure of the information’s integrity.

WHERE LAW & TECHNOLOGY MEET

**KAHN**  
CONSULTING INC.

## Evidentiary Issues

When evaluating the impact, if any, of the normalization process on the evidentiary quality of computer security log file information in ArcSight ESM, organizations should consider the following issues.

### 1. The process should not materially alter the original information

Unlike information captured in paper form, it can be difficult, or even impossible, to use or manage electronic information without in some way altering that information. Even the act of simply opening an electronic document to view it in a word processor can add information to the document or otherwise alter it. For electronic information that must be retained for long periods of time, the problem is even more acute. Media deterioration, software and hardware obsolescence, environmental degradation and other factors often require organizations to migrate data from one system to another, to move information to new media types, or to translate information into new formats.

Rules regarding the admissibility and credibility of evidence are based on the foundational concept of “the original.” Evidentiary statutes such as the Federal Rules of Evidence indicate a preference for “original” documents.<sup>3</sup> However, in the electronic world, where it is possible to make infinite perfect copies of a document, the concept of an “original” loses some of its significance.

Various laws and regulations have responded to this reality by clarifying that, in the electronic world, there might be no difference between an “original” and a “duplicate” for evidentiary purposes. For example, the ESIGN Act<sup>4</sup> states that electronic information may be used to satisfy legal requirements, provided that it:

- “Accurately reflects the information set forth in the contract or other record;”<sup>5</sup>
- “Remains accessible”<sup>6</sup> for the period the law requires;
- Can be “accurately reproduced”<sup>7</sup> in the future.

Furthermore, ESIGN clarifies that an electronic record that meets these conditions can satisfy the requirement for an “original.”

Given this reality, evaluating the evidentiary impact of normalization on an “original” computer security log file should focus on the nature and extent of the alteration that occurs during the normalization process.

The ArcSight ESM normalization process is designed to translate divergent, proprietary approaches to describing security event information into a universal format that maintains the meaning of the original. In fact, it is readily apparent that the utility of the product itself would be severely diminished if the normalization process did in fact materially alter the meaning of the original information.

As an added point, it should be noted that the Federal Rules of Evidence establish a basic principle that, if an organization routinely relies upon a given record in the course of their business, that record is generally admissible.<sup>8</sup>

### 2. The process should be documented, repeatable, and reliable

A general principle regarding the admissibility and credibility of electronic evidence is that the reliability of electronic information will be based in part upon evidence that record keeping software

WHERE LAW & TECHNOLOGY MEET

**KAHN**  
CONSULTING INC.

and hardware was reliable and operating properly, and that appropriate policies and procedures were implemented and adhered to. For example, IRS rules mandate various “controls to ensure the integrity, accuracy, and reliability” of record keeping systems,<sup>9</sup> as do several other federal and state regulations.

*“To facilitate analysis of logs, organizations often need to implement automated methods of converting logs in different formats to a single standard format.”*

*Guide to Computer Security Log Management, National Institute of Standards and Technology, Special Pub. 800-92 (Draft)*

ArcSight provides comprehensive documentation regarding its operation generally, and regarding the normalization process specifically. Organizations wishing to understand the normalization process in greater detail should contact ArcSight for this information and related information regarding ArcSight ESM quality assurance and testing procedures.

As an overall point, it should be noted that the accuracy and integrity of the log file information processed by ArcSight ESM is fundamentally reliant upon the accuracy and authenticity of the source information. Not all devices across an enterprise are typically protected to the same degree (i.e., logs on laptops and workstations versus web servers), so the extent to which organizations rely upon specific log file information should reflect this.

### 3. The approach should support various risk models

ArcSight ESM is designed to accommodate organizations that wish to take a conservative evidentiary approach to managing log file information. That is, ArcSight ESM enables organization to store log file information in its original, raw, non-normalized form either on the originating device or in a separate location for future potential use as electronic evidence.

It should be noted, however, that the volume of log file information generated by many devices is too great to be stored on the device itself over the long term. For devices that generate log file information that must be retained only for short periods of time, it may be appropriate to retain the information on the device itself and allow the information to be cyclically rewritten. However, for log file information that may have longer term retention requirements, or otherwise is expected to be used as evidence in the future, there is often a practical need to move the data from the device to another storage location.

WHERE LAW & TECHNOLOGY MEET

**KAHN**  
CONSULTING INC.

## VI. Evaluating ArcSight ESM Capabilities

This part of the Evaluation addresses ArcSight ESM capabilities that have not already been covered elsewhere in this document and are relevant to the product's use as a platform for managing computer security log files for evidentiary purposes.

### Access Control

**Desired Capability.** Log file management systems should ensure that users can only access information that they are authorized to access.

**Information Management Principle.** Access to private and confidential information must be controlled, and may be required by law, regulation, or contract. In addition, when log file management systems are used for investigations, it is necessary to ensure that only parties involved in the investigation are able to access information related to that investigation. This may be particularly important when the investigation is subject to attorney-client privilege.

**ArcSight ESM Capabilities.** ArcSight ESM defines several user roles that correlate to different levels of responsibility and access. These roles include: Admin, Author, Operator, Analyst, Security Manager, and Business User. ArcSight ESM also provides a comprehensive implementation of Access Control Lists. In this manner ArcSight ESM provides organizations with the ability to ensure that only authorized individuals are able to access (and perform other operations on) private and confidential information.

In addition, ArcSight ESM allows customized workflows to be programmed. Such workflows could be utilized to help ensure that only authorized parties involved in an investigation, for example, are able to access information related to that investigation. Workflow capabilities may also be useful for compliance-related monitoring and control activities, such as those related to the Sarbanes-Oxley Act.<sup>10</sup>

### Records Retention

**Desired Capability.** Organizations may be required to securely retain certain types of electronic information in order to comply with laws and regulations regarding records retention. The retention of records is also necessary for normal business operations and for internal and external audits.

**Information Management Principle.** Records retention practices are an important aspect of an overall data asset management strategy. The requirements of laws such the Sarbanes-Oxley Act clearly define corporate responsibility in ensuring a complete and intelligible audit trail. Records retention systems must ensure that information is stored, and is retrievable, in a secure and reliable manner.

**ArcSight ESM Capabilities.** ArcSight SmartStorage and the ArcSight Database both provide storage capabilities designed to ensure that retained data is stored in an efficient and effective manner. ArcSight archiving technologies include the extraction and storage of chronological data slices, and the option of configuring the frequency, categorization, and access to archived electronic information.

### Secure Transmission of Information

**Desired Capability.** Log file management systems should ensure that any log file information transmitted from security devices to the system itself (or otherwise transmitted as part of the system's operation) is transmitted in a secure manner.

WHERE LAW & TECHNOLOGY MEET

**KAHN**  
CONSULTING INC.

**Information Management Principle.** The integrity of electronic information used as evidence for legal and regulatory purposes must be protected so that its admissibility and creditability can be maintained.

**ArcSight ESM Capabilities.** Communication between ArcSight ESM and ArcSight Connectors, ArcSight Consoles and Web Browsers is encrypted with 128-bit SSL encryption and 1024-bit key exchange. ArcSight ESM also supports authentication techniques such as RADIUS, LDAP, Active Directory, Two-Factor Authentication, and Public Key Infrastructure.

## Auditing

**Desired Capability.** Log file management systems should generate, make available, and securely store information regarding its operation for auditing purposes.

**Information Management Principle.** Systems used to store and manage information used as evidence must provide reliable information regarding their functioning and regarding critical operations such as information access, deletion, and so on.

**ArcSight ESM Capabilities.** ArcSight ESM provides logging and auditing for user access to the ArcSight system and audit logs listing what that user accessed, when, and what changes were made. In this manner ArcSight provides auditing capabilities designed to support the use of computer log file information as evidence.

## VII. Summary

It is the opinion of Kahn Consulting, Inc., that ArcSight's Enterprise Security Management ("ESM") system provides capabilities that support its use as a platform for the management of computer security log files as evidence. ArcSight ESM is designed in a manner that protects the security and trustworthiness of the information collected, processed and managed by the system. By providing information protection capabilities and processing data according to documented processes, ArcSight ESM works to ensure that the security and trustworthiness of the information that it manages is protected.

## VIII. About Kahn Consulting

Kahn Consulting, Inc. (KCI) is a consulting firm specializing in the legal, compliance, and policy issues of information technology and information lifecycle management. Through a range of services including information and records management program development; electronic records and email policy development; Information Management Compliance audits; product assessments; legal and compliance research; and education and training, KCI helps its clients address today's critical issues in an ever-changing regulatory and technological environment. Based in Chicago, KCI provides its services to Fortune 500 companies and government agencies in North America and around the world. Kahn has advised a wide range of clients, including International Paper, Dole Foods, Sun Life Financial, Time Warner Cable, Kodak, McDonalds Corp., Hewlett-Packard, United Health Group, the Federal Reserve Banks, Ameritech/SBC Communications, Prudential Financial, Motorola, Altria Group, Starbucks, Mutual of Omaha, Sony Corporation, and the Environmental Protection Agency. More information about KCI, its services and its clients can be found online at: [www.KahnConsultingInc.com](http://www.KahnConsultingInc.com).

WHERE LAW & TECHNOLOGY MEET



## IX. Endnotes

<sup>1</sup> In undertaking this engagement, KCI exclusively relied upon information supplied by ArcSight through internal and external documentation, and interviews with ArcSight representatives. KCI does not conduct independent laboratory testing of information technology products, and as such, did not evaluate ArcSight ESM in a laboratory setting or otherwise field-test any ArcSight products.

<sup>2</sup> For a current list of devices supported by ArcSight ESM, please see [http://www.arcsight.com/product\\_supported.htm](http://www.arcsight.com/product_supported.htm).

<sup>3</sup> See, for example, Rule 1002.

<sup>4</sup> Public Law 106-229, Section 101(d), "Retention of Contracts and Records."

<sup>5</sup> Ibid.

<sup>6</sup> Ibid.

<sup>7</sup> Ibid.

<sup>8</sup> Provided certain conditions are met - the conditions provided in Rule 902 are that the record: (A) was made at or near the time of the occurrence of the matters set forth by, or from information transmitted by, a person with knowledge of those matters; (B) was kept in the course of the regularly conducted activity; and (C) was made by the regularly conducted activity as a regular practice.

<sup>9</sup> IRS Revenue Procedure 97-22.

<sup>10</sup> For further information about the Sarbanes-Oxley Act, please refer to <http://www.sec.gov/about/laws.shtml>.

**Entire contents © 2006 Kahn Consulting, Inc. ("KCI"). Reproduction of this publication in any form without prior written permission is forbidden. KCI and ArcSight, Inc. shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof. The reader assumes sole responsibility for the selection of these materials to achieve its intended results. The opinions expressed herein are subject to change without notice. All rights reserved. [www.KahnConsultingInc.com](http://www.KahnConsultingInc.com) [info@KahnConsultingInc.com](mailto:info@KahnConsultingInc.com) 847-266-0722**

WHERE LAW & TECHNOLOGY MEET

