Data Loss Prevention (DLP) Operational Standard

Issued Date: 03-March-2015

Purpose

This document establishes the standard methodology to be used by authorized employees in managing the Data Loss Prevention (DLP) program for a specified university organizational unit.

Scope

This standard applies to the University Information Security Office (UISO) and to all approved security liaisons or their designee in the University system.

Overview

The UISO uses the DLP system to perform monthly discovery scans of end-user workstations and network file shares to discover where restricted data is stored and to provide a platform for collaborating with designated security liaisons to monitor, protect, and manage the discovered data. The first time a scan is run it will be a full scan, subsequent scans will search for new or modified files. This document establishes the standard methodology, definitions, and process to be used by authorized users of the system.

Definitions

- **Console** – The central management system that provides authorized university employee access to the results from the monthly DLP discovery scan process.
- **Endpoint** – A university owned computer with the DLP agent installed.
- **Incident** – A unique file containing matches identified through a DLP scan.
- **Incident ID** – A unique identification number assigned to an incident.
- **Match** – An occurrence of data within a file that matches the DLP search criteria. A single file may contain multiple matches.
- **Machine Name** – The computer name assigned to the endpoint.
- **Status** – An indication of where an incident is in the incident analysis process.
- **Notes** – Area to make remarks about an incident.
- **Status Group** – A set of status attributes assigned to the group to filter incidents.

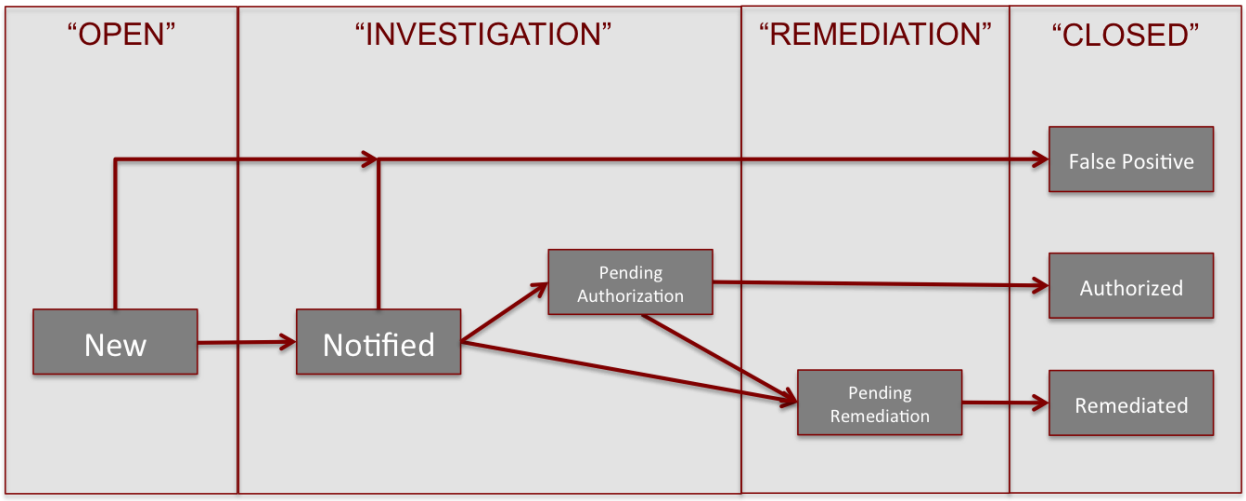
Standard Methodology & Processes

The UISO will perform monthly data discovery scans of all university owned endpoint computers via a previously deployed software agent. In addition, UISO will scan previously configured network file shares. The scan results will be made available to authorized security liaisons to assist them in performing the required risk management activities for their area of responsibility.

The diagram below outlines the prescribed workflow that security liaisons are expected to follow in analyzing incidents identified through the DLP system.

(continued)

SecureCarolina



By default, all newly discovered incidents are categorized with a status of "new" and remain in an open state. All incidents must be reviewed by the security liaison with the end goal of being able to label the incident into one of three final categories: "Authorized", "Remediated", or "False Positive". To arrive at this determination, the security liaison must perform an investigation.

Each incident will include the machine name and file owner for the file that is suspected to contain restricted data. The security liaison will determine who the end-user of the computer is (based on machine name) and will notify them that potentially restricted data was identified on their system. When this notification has occurred, the incident status should be changed to "Notified".

The end-user will assist the security liaison in determining one of the following types for the identified file:

1. The identified file does contain restricted data, and, it is required to perform their job duties.
2. The identified file does contain restricted data; however, it can be securely deleted, as it is not required to perform their job duties.
3. The identified files does not contain restricted data, it is a false positive.

Incidents that are determined to be type #1 should have the status updated to "pending authorization". The security liaison should then seek executive-level (Vice-President or Dean) approval to maintain the restricted data on their computer and/or on the network file share. Notes should also be added to the incident outlining the justification for having the data, who authorized it, and any other pertinent details.

Incidents that are determined to be type #2 should have the status updated to "pending remediation". Once the security liaison has confirmed that the file has been securely deleted, the status should be updated to "remediated." Notes should be added to the incident outlining who verified remediation, how they verified it, and the date it was removed.

Incidents that are determined to be type #3 should have the status updated to "false positive". Notes should be added to describe what the data are such that the UISO can work to reduce the number of false positives.

(continued)

Additionally, to assist the security liaison and UISO in reporting on the status of incidents, the following status categories have been defined:

- **Open** – those incidents categorized as "new", where no notification has occurred.
- **Investigation** – the responsible end-user has been contacted and the determination of category is pending.
- **Remediation** – the responsible end-user has confirmed that the file can be securely deleted; however, it has not yet been completed.
- **Closed** – those incidents with a status of "authorized", "remediated", or "false positive".

Contacts

http://security.sc.edu

Revision History

Author	Date	Comments
James Perry	02-March-2015	
Jeff Whitson	03-March-2015	Updates added