Purpose

This work instruction is intended to provide DFU personnel with high-level methodology, including required tools and\or equipment (if applicable), on how to report on the data that has been collected, extracted, examined, and analyzed for incident response purposes.

Scope

The steps in this work instruction should be completed by digital forensics unit (DFU) staff within the Information Security Office (ISO).

A DFU Incident Lead and an Incident Technical Lead are assigned to each incident, and in most cases, will follow the roles and responsibilities described below.

1. The Incident Lead is responsible for coordinating day to day operations and the communications with the various stakeholders and will provide status updates. **Note**: All email communications between the ISO personnel and the original requestor are to be courtesy copied to the email group, infosec.investigations@austintexas.gov.
2. The Incident Technical Lead is responsible for the onsite/offsite collection, examination, analysis, reporting as well as the chain of custody of all evidence collected.

Note: Assistance might be requested from a City of Austin internal resource(s) and/or external professional during the response effort, as it is not feasible for any one person to be well-versed in every technology used within the City of Austin.

Equipment/Tools

Tool/Equipment	**Use(s)**
Office 365 – Microsoft Word	Application to create and add content related to the Final Report.
Adobe Acrobat DC	Application used to convert Final Report Microsoft Word version to Adobe Acrobat PDF Format.
Amazon Web Services (coa-iso-dfu portal)	Cloud Storage location for all DFU archived data related to the Incident, including the final report.
DFU Case management Tracking System	SharePoint Database used to record and archive case information (records, examiner notes, status updates, milestones and events, contacts, dates, communications, gathered during the IR process.

Instructions

Overview

The formality of the reporting phase varies greatly, depending on the situation. The final phase of reporting the results of the data analysis may include:

- Describing the actions used
- Explaining how tools and procedures were selected

- Determining what other actions need to be performed (e.g., forensic examination of additional data sources, securing identified vulnerabilities, improving existing security controls)
- Providing recommendations for improvement to policies, guidelines, procedures, tools, and other aspects of the forensic process.

Regardless, the steps in this work instruction cover the basic tasks for report completion purposes.

Create Incident Summary Report

Complete the following steps to create an Incident Response Summary Report.

1. Schedule a meeting or conference call with the Incident Lead, Deputy CISO, and other incident stakeholders to finalize a scope of work detailing the content and level of detail and distribution audience for the final report.
2. Collect any/all relevant documentation (e.g., case notes, status updates, email communications) from all stakeholders in preparation of creating the Incident Summary Report.
3. Create the initial version of the Incident Summary Report in Microsoft Word. **Note**: The Incident Summary Report document/file name should be saved using the naming convention 'YearMonthDate-InvestigationClassAcronym' with no spaces in between (e.g., 20200403-B1). **Note**: Investigations will be classified into four (4) classes in the DFUA (Legal). (See Section 9.0 in the Record Retention Guidelines for more information.)
    a. D (APD) Austin Police Department Cases
    b. B (Administrative)
    c. R (Rejected) – Request rejected by CISO.
    d. IR-Incident Response
4. The formality, content, and level of detail in the reporting phase varies greatly, depending on the situation and the recommendations of the Incident Lead, Deputy CISO, and other incident stakeholders. The final phase of reporting data analysis results could potentially include the following information:
    a. Incident ID
    b. ISO case number
    c. Incident type (e.g., phishing, malware, ransom, intrusion)
    d. Incident severity (e.g., low, medium, high)
    e. Occurrence date
    f. Closure date
    g. Time to resolution
    h. Incident owner name and department
    i. Description of tools Used
    j. Name and role of Incident Response Team members
    k. Summary of data collection process
    l. Summary of data examination process

m. Summary of data analysis process

n. Copies of status updates, case notes, email communications, etc.

5. Once the report is complete and has been approved by the DFU Team Lead and the Deputy CISO, the report should be converted to PDF format prior to distribution outside the ISO. The distribution of the final report is the responsibility of the DFU Team Lead and the Deputy CISO.
6. Create a case folder in the coa-iso-dfu folder in Amazon Web Services (AWS). **Note**: This folder serves as an archiving repository for the final Incident Summary Report, as well as all other documentation related to the incident.
7. Upload the MS-Word and PDF copy of the Incident Summary Report to the case folder in the coa-iso-dfu folder in AWS.
8. Upload copies of status updates, case notes, email communications, etc. to the case folder in the coa-iso-dfu folder in AWS.
9. Update the DFU Case Management Tracking System with any high-level case notes, status updates, and/or email communications.
10. Close the case in the tracking system.

Related Content

The following documents should either be reviewed and/or completed prior to or after this work instruction:

- ISO Digital Forensics Analysis for Incident Response SOP<link>
- Forensics Analysis for Incident Response Data Analysis Work Instruction<link>