# Delete - How to Use this Report Template

For your engagement, this page would be removed. Because this is a template report, this page stands to explain how to utilize the entire document. Before you go further, please read through this page so that you know how to use this document.

Below, you will find modules meant for various types of OSINT investigations as well as templates meant to keep certain OSINT documentation organized, like sock puppets.

This report template was designed in a modular way to allow the investigator to remove what is not necessary for their investigation.

For example, if you were doing research into a company for an external pentest, you may end up using:

* Website OSINT
* Email OSINT
* Password OSINT
* Etcetera

If you need further direction, please refer to the “Writing an OSINT Report” section of the OSINT course.

A logo of a unicorn

Description automatically generated

A logo with a cross between the letters

Description automatically generated

Open-Source Intelligence (OSINT) Investigation

Table of Contents

[How to Use this Report Template 1](#_Toc158751472)

[Confidentiality Statement 4](#_Toc158751473)

[Disclaimer 4](#_Toc158751474)

[Contact Information 4](#_Toc158751475)

[Assessment Overview 5](#_Toc158751476)

[Summary – Challenge 1 6](#_Toc158751477)

[Technical Evidence – Reverse Image Search 7](#_Toc158751478)

[Technical Evidence – Google Search Operators 8](#_Toc158751479)

[Summary – Challenge 2 9](#_Toc158751480)

[Technical Evidence – XXX 10](#_Toc158751481)

[Technical Evidence – XXX 11](#_Toc158751482)

[Summary – Challenge 3 12](#_Toc158751483)

[Technical Evidence – XXX 13](#_Toc158751484)

[Technical Evidence – XXX 14](#_Toc158751485)

# Confidentiality Statement

This document is the exclusive property of Demo Corp and TCM Security (TCMS). This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both Demo Corp and TCMS.

Demo Corp may share this document with auditors under non-disclosure agreements to demonstrate penetration test requirement compliance.

# Disclaimer

This Open-Source Intelligence (OSINT) report has been compiled by TCM Security based on information available in the public domain as of [INSERT DATE HERE]. While efforts have been made to ensure the accuracy of the information, it is subject to change. An OSINT investigation is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period.

TCM Security assumes no responsibility for any decisions made or actions taken based on this report. The use of this information is at the reader's own risk, and TCMS disclaims any liability for inaccuracies or omissions. This report is confidential and not intended for public distribution.

# Contact Information

|  |  |  |
| --- | --- | --- |
| Name | Title | Contact Information |
| DEMO CORP | | |
| Jane Smith | Chief Information Security Officer | jsmith@democorp.com |
| TCM Security | | |
| Heath Adams | Lead Penetration Tester | heath@tcm-sec.com |

# Assessment Overview

From [START DATE] to [END DATE], the OSINT Investigator conducted an Open-Source Intelligence (OSINT) assessment. The findings presented in this overview are derived from open-source data and do not involve any unauthorized access to private or confidential information. An OSINT risk assessment emulates the role of a threat actor employing methods like those utilized by malicious entities to gather information. Through data collection and analysis, an investigator will search open sources to identify potential risks, culminating in an assessment and profiling of discovered information.

This OSINT investigation aims to provide a realistic representation of the information landscape from a threat actor's perspective, enabling a proactive approach to strengthening organizational resilience.

Phases of the OSINT investigation include the following:

* Planning and Direction
* Collection
* Processing
* Analysis and Production
* Dissemination and Integration

A diagram of a process

Description automatically generated

# Summary – Challenge 1

TCMS evaluated Demo Corp’s provided image to discover data within them and make determinations from them. The following sections provide a high-level overview of findings discovered.

Objective

Geolocating this place may not be hard but the threatened arthropods that can be found in this place sure makes a hard migration every few generations.   
  
You should be able to find a few decorative posters that have been made to commemorate this mighty migration. In one poster, a specific interstate highway is mentioned. What is this interstate highway and how many states does it go through?   
  
Incredibly, scientists have able to identify a single member of this species with the longest travel. How many miles was the longest known individual migration identified by this species?

Key Findings

TCMS determined that the image provided was from the Great Smoky Mountains. In reading the Great Smoky Mountains National Park Service website TCMS identified that the Monarch butterfly is the only endangered arthropod that can be found in the park that makes a long migration. Through further research, it was identified that the Monarch butterfly is featured on a poster of the US Highway 35. This highway system goes through six (6) US states. Finally, the longest known individual migration was determined to be 2880 miles.

Photograph of Subject

A forest of trees in the mountains

Description automatically generated

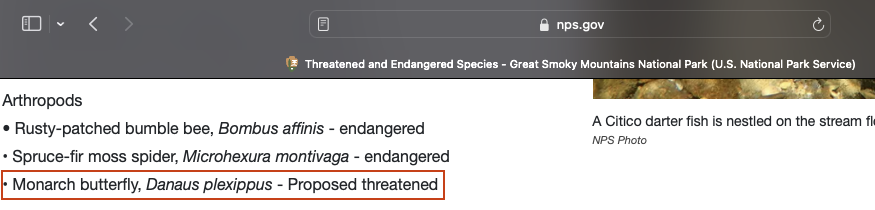
## Technical Evidence – Reverse Image Search

|  |  |
| --- | --- |
| OSINT: | Used Google Lens to reverse image search and Google search operators to identify the location and threatened arthropod. |
| Link(s): | * https://www.nps.gov/grsm/learn/nature/te-species.htm * https://www.fs.usda.gov/wildflowers/pollinators/Monarch\_Butterfly/migration/index.shtml |
| Notes: | It was important to carefully focus on the mountain range to get a match to Great Smoky Mountains. The National Park website confirmed that the Monarch was on the threatened list. |

*A screenshot of a photo shop

Description automatically generated*

*Figure 1: Geolocation confirmed by Google Lens*

**

*Figure 2: Monarch identified as threatened arthropod*

## Technical Evidence – Google Search Operators

|  |  |
| --- | --- |
| OSINT: | Performed a google search for “monarch migration”, “monarch migration "highway poster"”, and finally “monarch migration longest trip recorded”. |
| Link(s): | * https://www.fs.usda.gov/wildflowers/pollinators/Monarch\_Butterfly/migration/index.shtml * https://entnemdept.ufl.edu/walker/ufbir/chapters/chapter\_35.shtml#:~:text=Monarch%20Watch%20lists%20the%20longest,%2C%201989%20in%20Austin%2C%20Texas. |
| Notes: | Utilizing the first two searches At the bottom, the website section “The Monarch Highway Poster” provides details that the interstate highway is called I-35” and that it goes through six (6) US states.  A second Google search |

A close up of a sign

Description automatically generated

*Figure 1: Proof of Monarch migration*

*A screenshot of a computer screen

Description automatically generated*

*Figure 2: “The Monarch Highway Poster” detailing interstate highway information*

**

*Figure 3: Research paper documenting the longest recorded flight*

# Summary – Challenge 2

<Input summary for the challenge here>

Objective

<Input the objective here>

Key Findings

<Input key findings here>

Photograph of Subject

<input any photographs here or erase if unneeded>

Personal Information

<Name:

Date of Birth:

Phone number:

Address:

Erase if unneeded>

Usernames and Email

<input usernames here or erase if unneeded>

Location Information

<input location information here or erase if unneeded>

## Technical Evidence – XXX

|  |  |
| --- | --- |
| OSINT: | <Input OSINT performed here> |
| Link(s): | * <input link(s) here |
| Notes: | <Input notes from findings here> |

*Figure 1: XXX*

*Figure 2: XXX*

*Figure 3: XXX*

## Technical Evidence – XXX

|  |  |
| --- | --- |
| OSINT: | <Input OSINT performed here> |
| Link(s): | * <input link(s) here |
| Notes: | <Input notes from findings here> |

*Figure 1: XXX*

*Figure 2: XXX*

*Figure 3: XXX*

# Summary – Challenge 3

<Input summary for the challenge here>

Objective

<Input the objective here>

Key Findings

<Input key findings here>

Photograph of Subject

<input any photographs here or erase if unneeded>

Personal Information

<Name:

Date of Birth:

Phone number:

Address:

Erase if unneeded>

Usernames and Email

<input usernames here or erase if unneeded>

Location Information

<input location information here or erase if unneeded>

## Technical Evidence – XXX

|  |  |
| --- | --- |
| OSINT: | <Input OSINT performed here> |
| Link(s): | * <input link(s) here |
| Notes: | <Input notes from findings here> |

*Figure 1: XXX*

*Figure 2: XXX*

*Figure 3: XXX*

## Technical Evidence – XXX

|  |  |
| --- | --- |
| OSINT: | <Input OSINT performed here> |
| Link(s): | * <input link(s) here |
| Notes: | <Input notes from findings here> |

*Figure 1: XXX*

*Figure 2: XXX*

*Figure 3: XXX*