Certified OSINT Professional **Exam**

OSINT Report on [NAME]

Company Name
Date

ZSECURITY

Table of Contents

Confidentiality Statement

This report is the exclusive property of COMPANY_NAME. It contains sensitive information collected through Open-Source Intelligence (OSINT) methods and is intended solely for the use of authorized personnel. The contents of this report are confidential and must not be disclosed, distributed, or reproduced, in whole or in part, without the explicit written consent of COMPANY_NAME and CLIENT_NAME. Unauthorized access or dissemination of this report is prohibited and may result in legal consequences.

The information provided is for intelligence and investigative purposes only and should not be used for any unlawful activity. By accessing this report, you acknowledge and agree to comply with these confidentiality requirements.

CLIENT_NAME may share this document with auditors who are bound by non-disclosure agreements, solely for the purpose of demonstrating compliance with open-source intelligence investigation requirements.

Disclaimer

This report is based on publicly available open-source information in the public domain as of DATE and is provided for informational purposes only. While every effort has been made to ensure accuracy, the information is subject to change. COMPANY_NAME makes no warranties regarding the completeness or reliability of the data.

An OSINT investigation is a snapshot in time. The findings and recommendations are based on the information gathered during the assessment and do not account for any changes or updates made after that period.

This report is not intended to offer legal or professional advice. COMPANY_NAME assumes no liability for any actions taken based on its contents. The report is for internal use only and may not be shared or distributed without proper authorization.

Contact Information

Name	Title	Contact Information
Investigator's name	OSINT investigator	contact@example.com

Assessment Overview

Between DATE, and DATE, our OSINT Investigator conducted an Open-Source Intelligence (OSINT) assessment. The findings in this report are based solely on publicly available data, with no unauthorized access to private or confidential information. An OSINT (Open-Source Intelligence) risk assessment is an evaluation of publicly available information to identify potential security risks and exposure of sensitive data. It replicates the methods a threat actor might use to gather intelligence from publicly available sources about an individual, organization, or system.

This OSINT investigation offers a realistic view of the information landscape through the lens of a threat actor, helping organizations and individuals to take proactive measures to enhance their security and resilience.

Open-source intelligence or (OSINT) is the legal collection of free publicly available information on individuals, organizations or websites.

Phases of an OSINT investigation include the following:

- **Planning:** Setting clear objectives, defining the scope, and identifying resources and targets for the intelligence gathering process.
- **Data Collection:** Gathering publicly available information from various sources, such as websites, social media, and public databases.
- **Processing**: Organizing and filtering collected data to make it more manageable and ready for analysis by removing irrelevant information.
- **Analysis**: Interpreting and correlating data to identify patterns, relationships, or insights that address the investigation's goals.
- **Reporting**: Compiling the analyzed information into a clear, actionable report and delivering it to the client.

C|OSINT|P Exam

Scope

As requested, the OSINT investigation was only carried out on the following targets

Assessment	Target
Background Check SOCMINT Leaked Databases Search	TARGET

Executive Summary

CLIENT_NAME engaged COMPANY_NAME to conduct an open-source intelligence (OSINT) investigation against TARGET. The main goal of the investigation was to find publicly available information about Rishi Kabra.

This report details the scope of the engagement, detailed information about all of the findings. The summary below is intended for non-technical audiences to give an idea of the overall results of the engagement and the key findings. The second section of this report is intended for a technical audience as it lists all of our findings in detail, along with reproduction steps, analysis and recommendations.

Investigation Summary

Key Findings

Technical Evidence

Information Identified – Methods Used
e.g., Identification of personal accounts – Utilization of advanced search engine operators

Methodology Overview
A detailed technical description of the techniques used to obtain the identified information.

Supporting Evidence
Relevant screenshots and documentation to substantiate findings.

Screenshots

Attachments

Includes any supplementary materials like relevant files supporting the investigation.

References

A comprehensive list of all sources, including links and references cited throughout the investigation, to facilitate easy access for the client.