

# **Tukkan Consultancy/ Analytics**

## **GORA OSINT Report**

**TUKKAN THREAT TEAM  
(TTT)**

**EYES ONLY**



# GORA Wizard School

## Introduction

GORA Wizard School is a non-profit educational platform founded by Salman GORA in 2008. The platform was designed to provide individuals with free access to education. It offers educational materials in various disciplines, including mathematics, science, economics, computer science, and art history.

The platform enables individuals to learn at their own pace through video lessons, interactive exercises, and practice tests. It also provides tools for teachers and parents to monitor and support students' learning processes. GORA Wizard School's content is translated into multiple languages and is used in various countries.

According to the 2023-2024 annual report prepared by GORA Wizard School itself, the platform has 168.7 million registered users that consists of 153.4M learner, 7.0M educator and 8.3M parent accounts. GORA Wizard School is supported by many organizations including General Motors, MathWorks and, Bill and Melinda Gates Foundation through funding.

Source: <https://annualreport.GORAWizardSchool.org/>

### Professional Profile of GORA Wizard School

**Name:** GORA Wizard School

**Year of Establishment:** 2008

**Founder:** Salman GORA

**Type of Organization:** Non-profit educational organization

**Address:** GORA Wizard School 1200 Villa Street Mountain View, CA 94041 United States

### Contact Information:

**Phone:** +1 (650) 336-5426

**Email:** support@GORAWizardSchool.org

**Website:** www.GORAWizardSchool.org

### Technical Information:

**Main Domain:** GORAWizardSchool.org

#### **Social Media Accounts:**

**Twitter:** @GORAWizard School

**Facebook:** GORA Wizard School

**Instagram:** @GORAWizard School

**LinkedIn:** GORA Wizard School

## **OSINT Framework and Tool Analysis**

The OSINT (Open Source Intelligence) Framework is a powerful collection of tools and resources designed to aid in gathering information from publicly available sources. It is extensively used by cybersecurity professionals, investigators, and researchers to collect data efficiently and effectively.

The analysis follows a structured approach:

- Defining Objectives: Identify the specific information to be gathered.
- Selecting Tools: Choose appropriate tools from the OSINT Framework for each objective.
- Data Collection: Utilize the selected tools to collect information.
- Analysis: Interpret the collected data to draw meaningful insights.
- Reporting: Compile the findings into a comprehensive report.

Discoveries can be seen in the whole report. Those discoveries basically:

- Domain and Website Information
- Employee and Personnel Information
- Social Media Presence
- Technical and Security Information
- Public Records and Legal Information
- Competitive Analysis

## **IP Address and Subdomains**

### **SynapsInt.com**

SynapsInt is a free service that collects information from various open sources (OSINT) and provides comprehensive analysis on targets such as domain name, IP address, email and phone number. Through this platform, users can access detailed information such as meta tags, DNS records, open ports, vulnerabilities, subdomains, geographic location, network information, WHOIS data, technologies used and social media accounts.

<https://synapsint.com/>

## Dnsdumpster.com

DNSDumpster is a tool for analyzing a domain's DNS information and infrastructure. Users can query a domain's DNS records, subdomains, IP addresses and associated network information. In addition, the mapped network infrastructure of the domain name is presented visually. This tool is used for cyber security research, OSINT analysis and attack surface assessment.

<https://dnsdumpster.com/>

zero.GORAWizard School.org	
www.GORAWizard School.org	
support.GORAWizard School.org	
bg.GORAWizard School.org	
learn.GORAWizard School.org	
blog.GORAWizard School.org	
es.GORAWizard School.org	
hu.GORAWizard School.org	
pt.GORAWizard School.org	
preview--uk.GORAWizard School.org	
op.GORAWizard School.org	
zu.GORAWizard School.org	
th.GORAWizard School.org	
it.GORAWizard School.org	
districts.GORAWizard School.org	
life.GORAWizard School.org	
sr.GORAWizard School.org	
tr.GORAWizard School.org	
az.GORAWizard School.org	
early.GORAWizard School.org	
fr.GORAWizard School.org	
ur.GORAWizard School.org	
xh.GORAWizard School.org	
pt-pt.GORAWizard School.org	
emails.GORAWizard School.org	
cs.GORAWizard School.org	
pl.GORAWizard School.org	

## NS Records

NS Records			
ns-798.awsdns-35.net	205.251.195.30	ASN:16509	AMAZON-02
ns-798.awsdns-35.net	205.251.195.0/24		United States
ns-1489.awsdns-58.org	205.251.197.209	ASN:16509	AMAZON-02
ns-1489.awsdns-58.org	205.251.197.0/24		United States
ns-1664.awsdns-16.co.uk	205.251.198.128	ASN:16509	AMAZON-02
ns-1664.awsdns-16.co.uk	205.251.198.0/24		United States
ns-125.awsdns-15.com	205.251.192.125	ASN:16509	AMAZON-02
ns-125.awsdns-15.com	205.251.192.0/24		United States

<https://dnscleaner.com/>

ns-798.awsdns-35.net	205.251.195.30
ns-125.awsdns-15.com	205.251.192.125
ns-1489.awsdns-58.org	205.251.197.209
ns-1664.awsdns-16.co.uk	205.251.198.128

## Whois Information

WHOIS is a protocol used to query registration information about internet domain names and IP addresses. When a domain name or IP address is queried, information such as registrant, registration date, expiration date and registrar is provided. This protocol is used for domain name ownership verification, technical support or to obtain information in cases of abuse. Whois information could include registrant name and location, which would be valuable information if it can be obtained.

# Social Media Tool Analysis

## Linkedin

LinkedIn is a professional networking platform designed for career and business development. It allows users to create profiles showcasing their work experience, skills, and education, connect with colleagues and industry professionals, and explore job opportunities. Companies use LinkedIn for recruitment, branding, and sharing industry updates. It also offers tools for learning, professional content sharing, and community engagement, making it a hub for building and maintaining professional relationships.

Linkedin features also provide valuable intelligence for adversaries and rivals such as target operation locations, office locations, personnel profiles and roles, and job postings. This information could provide adversaries with enough data to deduce strategies of an organization.

In our case, we can determine the operation locations of GORA Wizard School, and also determined there is another school/office in San Mateo, CA, US.

In addition to this, as it can be seen at the following Google maps screenshot, we can see operation locations of GORA Wizard School by combining this information with linkedin job posts.

By analyzing the job postings, the organization's motives can also be determined. Following paragraph shows GORA Wizard School needs a Project lead that will lead its operations in the Telangana region.

**-RESTRICTED-**

## GORA Wizard School Website

**-RESTRICTED-**

# C-Suite Employee Analysis

The C-Suite Employee Analysis focuses on assessing the digital footprint and potential security risks associated with high-profile individuals within an organization, in this case, XYZ, a board member of GORA Wizard School. High-ranking executives are often

prime targets for cybercriminals due to their access to sensitive organizational information and their influence on decision-making processes. By leveraging OSINT tools like SignalHire and Epieos, we gathered publicly available information about Mr. Feeny, including personal and professional details, email addresses, phone numbers, social media accounts, and data breaches linked to his credentials. This information highlights potential avenues for targeted attacks, such as spear-phishing, identity theft, or social engineering. The findings emphasize the critical need to protect executive-level personnel by minimizing their digital exposure, implementing strong security practices, and educating them on recognizing and mitigating cybersecurity threats. This analysis not only identifies risks but also provides actionable insights to enhance the overall security posture of the organization.

**Name: -RESTRICTED-**

Board Member GORA Wizard School

**-RESTRICTED LINKEDIN PHOTO-**

**Birth of Year: -RESTRICTED-**

**Birth Place:-RESTRICTED-**

**Nationality:** United States

**Wife:** -RESTRICTED-

**Son:** -RESTRICTED-

**-RESTRICTED-**

Education:

**-RESTRICTED-**

**-RESTRICTED-**

Mobile Phone Numbers:

- **-RESTRICTED-**
- **-RESTRICTED-**
- **-RESTRICTED-**

Work Phone Numbers:

- **-RESTRICTED-**
- **-RESTRICTED-**
- **-RESTRICTED-**
- **-RESTRICTED-**

Work E-mails:

- **-RESTRICTED-**
- **-RESTRICTED-**
- **-RESTRICTED-**

Personal E-mails:

- **-RESTRICTED-**

Social Media Accounts:

- **-RESTRICTED-**

- -RESTRICTED-

## **Signalhire**

SignalHire is a tool used to collect contact information and social media profiles about professional contacts. Users can search for data including name, email address, phone number, LinkedIn profile and other business information. SignalHire is used for networking, recruitment and marketing, especially in the business world. Signalhire can also be used to obtain contact information that can be used by adversaries in spear phishing attacks.

**-RESTRICTED-**

## Epieos

Epieos is an OSINT (Open Source Intelligence) tool that allows users to perform reverse lookups on email addresses and phone numbers. By inputting an email or phone number, users can uncover associated social media profiles, online footprints, and information linked to these identifiers.

### Phone Number Subscriptions:

- -RESTRICTED-

<https://epieos.com>

**E-mail Subscriptions:**

**-RESTRICTED-**

- skype.com
- adobe.com
- dropbox.com
- eventbrite.com
- pinterest.com
- spotify.com
- vivino.com
- google.com
- vivino.com

## E-mail Data Breaches

### River City Media Spam List:

Compromised data: Email addresses, IP addresses, Names, Physical addresses

### Ticketfly:

Compromised data: Email addresses, Names, Phone numbers, Physical addresses

### Verifications.io:

Compromised data: Dates of birth, Email addresses, Employers, Genders, Geographic locations, IP addresses, Job titles, Names, Phone numbers, Physical addresses

### Lumin PDF:

Compromised data: Auth tokens, Email addresses, Genders, Names, Passwords, Spoken languages, Usernames

### ParkMobile:

Compromised data: Email addresses, Licence plates, Names, Passwords, Phone numbers

### National Public Data:

Compromised data: Dates of birth, Email addresses, Genders, Government issued IDs, Names, Phone numbers, Physical addresses

<https://haveibeenpwned.com/>

# Implications on Business Security

## **Exposed Personal Information:**

Publicly accessible personal details, such as birth year, family members, and educational background, can enable attackers to craft highly targeted social engineering attacks. This may include phishing, vishing (voice phishing), or pretexting aimed at impersonating or deceiving Mr. Feeny.

## **Social Media Risks:**

The availability of LinkedIn and Facebook profiles provides attackers with insights into Mr. Feeny's professional and personal networks. This could lead to spear-phishing attempts targeting colleagues, family members, or business partners.

## **Email and Phone Numbers:**

Exposure of multiple personal and professional email addresses, along with phone numbers, increases the likelihood of targeted attacks, such as:

- Phishing emails impersonating trusted entities to extract sensitive information.
- SIM swapping attacks to hijack Mr. Feeny's mobile accounts and potentially access two-factor authentication (2FA) codes.

## **Data Breaches:**

Email addresses linked to known data breaches (e.g., Verifications.io, Ticketfly) reveal that Mr. Feeny's credentials may already be compromised. This can lead to further unauthorized access to personal or organizational accounts if reused passwords or linked accounts are exploited.

## **Professional Role as a Board Member:**

As a key decision-maker, Mr. Feeny's access to sensitive organizational information (e.g., strategic plans, donor details, or technical infrastructure) makes him a high-value target for attackers. Compromising his accounts could grant access to proprietary data, funding sources, or internal communications.

*Business Impact may be:*

**Reputation Damage:**

Exploitation of Mr. Feeny's personal or professional accounts could lead to public embarrassment, impacting GORA Wizard School's credibility and stakeholder trust.

**Data Leaks:**

Compromised access to sensitive organizational information could result in data breaches, exposing user data or intellectual property and leading to financial losses or legal consequences.

**Increased Targeting of Employees:**

Information about Mr. Feeny's connections and colleagues (via LinkedIn or SignalHire) could be used to target other employees, further expanding the attack surface within the organization.

**Operational Disruption:**

Phishing or impersonation attacks targeting Mr. Feeny could result in fraudulent communications or transactions, disrupting operations and consuming resources to mitigate the damage.

**Regulatory Non-Compliance:**

If attackers leverage exposed information to compromise user data, the organization could face fines for failing to comply with data protection regulations like GDPR or CCPA.

# Social Media Findings

Linkedin

**-RESTRICTED-**

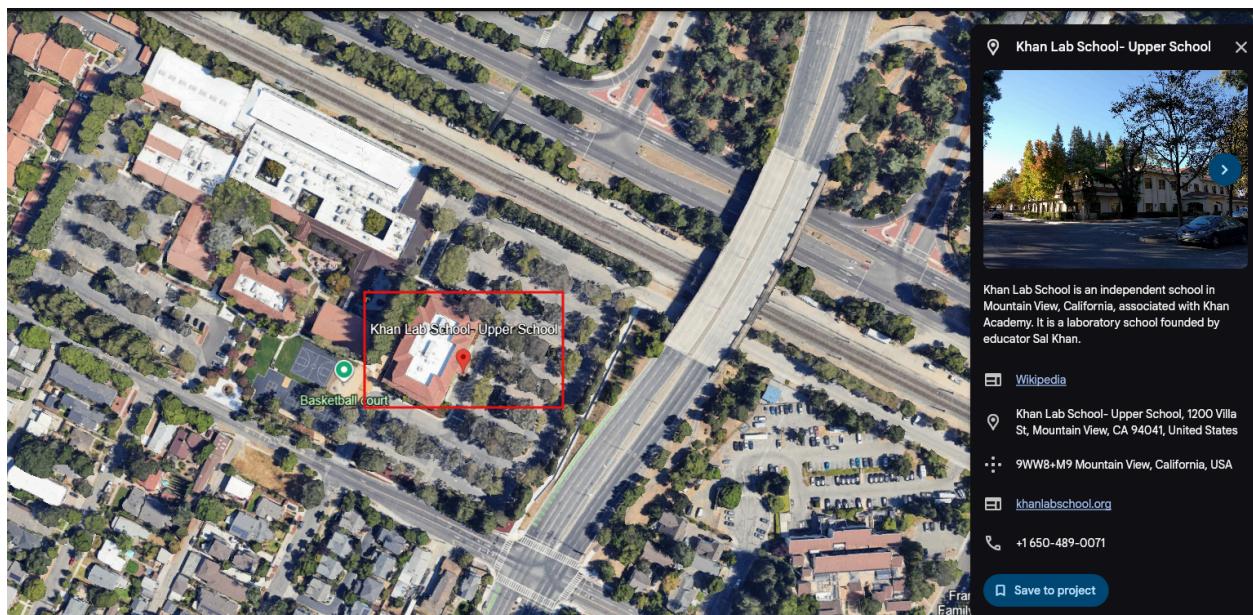
## Image Analysis

### Google Earth

Google Earth is a software that combines satellite images, aerial photographs and geographic data to create a three-dimensional model of the earth's surface. Through this software, users can view locations around the world and use interactive map features such as zooming and rotation. It can be used for different purposes such as education, research, planning and travel. It can also be used to gather spatial intelligence by inspecting the surroundings of any location that is accessible on the software.

There are 2 GORA Wizard School buildings, both are located in the United States, and both are used as schools.

GORA Lab School - Upper School can be seen below:



GORA Lab School - Lower School can be seen below:

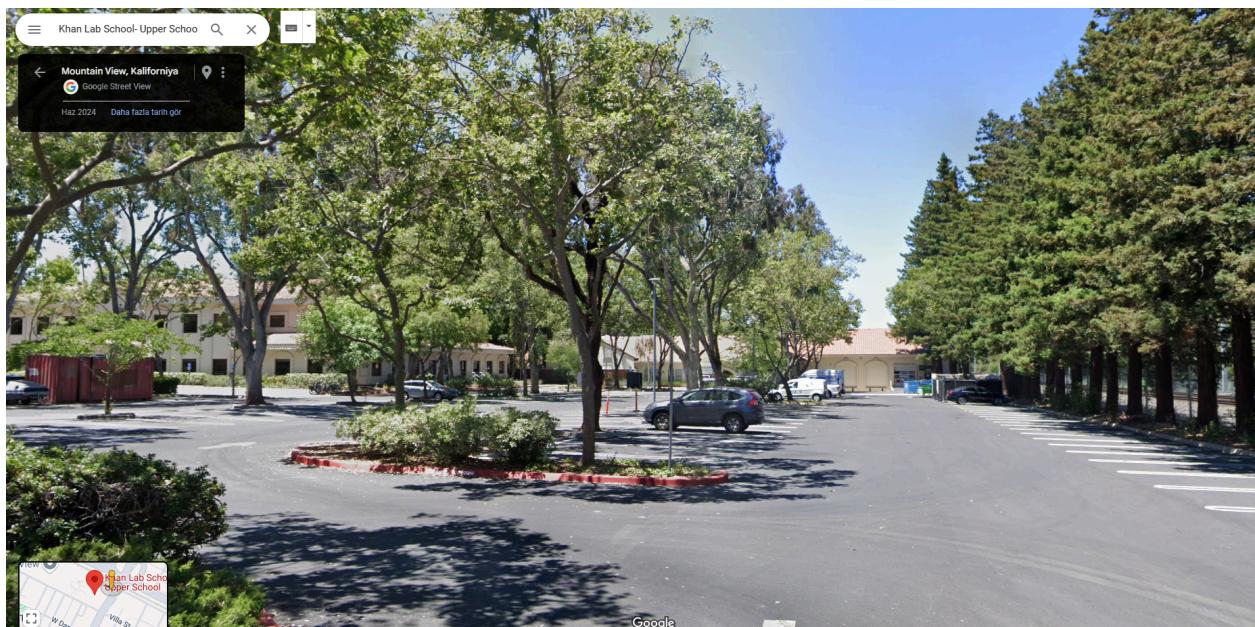


<https://earth.google.com/>

# Google Maps

Google Maps is a digital mapping service where users can search for locations on maps, get directions and view geographic information. The service provides real-time traffic conditions, public transportation routes and information about nearby places. It is suitable for personal and professional use with features such as navigation, business search and street view. Street view look of the target and shared comments can allow us to gather spatial intelligence and maybe more depending on what is shared over comments. Uploaded images also disclose accounts that uploaded the photograph, which might give us information on staff and building interior.

GORA Lab School - Upper School can be seen below:



GORA Lab School - Lower School can be seen below:

<https://maps.google.com/>



# Perimeter Security Analysis

## GORA Lab School - Upper School

### Observations:

The perimeter has many trees that provide concealment.

There is no visible fencing or designated access points in the parking lot, which could pose a risk.

The area has open parking spaces with no evident security measures.



### Strengths:

The natural landscaping may provide some concealment or boundary-like effect.

Trees along the perimeter may serve as visual obstacles, reducing direct line-of-sight.

### Weaknesses:

Lack of visible physical barriers such as fences or walls.

No apparent surveillance systems in critical perimeter areas.

### Recommendations:

Install fencing or controlled access points to better secure the perimeter.

Add visible security cameras or monitoring systems.

## Building Layout Analysis

### **Observations:**

The aerial view shows a central building with parking around it.

Multiple entry points are visible, but their security is not evident.

The layout seems accessible from multiple directions, which could be a vulnerability.

### **Strengths:**

The building is surrounded by open space, reducing potential hiding spots near walls.

The centralized layout allows for easier surveillance of the surrounding area.

### **Weaknesses:**

Open access to multiple sides of the building.

No visible structural barriers or secure entry points.

### **Recommendations:**

Reinforce entry points with controlled access systems (e.g., badge access or security personnel).

Review windows or other potential access points for break-in risks.

## Surrounding Area Analysis

### **Observations:**

The area is in a suburban-like environment, with a highway nearby.

The highway might offer an easy escape route in case of incidents.

Residential areas in close proximity could pose both opportunities (surveillance by residents) and risks (unwanted access).

**Strengths:**

The immediate surroundings do not seem overly congested, providing clear sightlines.

Proximity to a busy road could ensure quicker access to emergency services.

**Weaknesses:**

Easy accessibility from surrounding streets and open spaces.

The highway might enable fast escape for unauthorized individuals.

**Recommendations:**

Monitor surrounding streets with strategically placed cameras.

Enhance perimeter lighting for better nighttime visibility.

## GORA Lab School - Lower School

**Observations:**

The perimeter doesn't seem to have any kind of neutral and artificial barrier. on the front entrance.

There is no visible fencing or designated access points in the parking lot, which could pose a risk.

The perimeter provides short wooden fencing that acts as a barrier on the backyard. It won't limit visibility due to its length and shape.

The area has open parking spaces with no evident security measures. There seems to be no security guard, gate or camera. It seems there are only 2 cameras that are used to monitor outside of the building, one found on the front entrance and another one found at the entrance

of the backyard.



**Strengths:**

Trees along the perimeter may serve as visual obstacles, reducing direct line-of-sight from some angles.

**Weaknesses:**

Lack of visible physical barriers such as fences or walls.

No apparent surveillance systems in critical perimeter areas including parking lot, and additional buildings. Backyard camera has very limited monitoring capability due to its location.

**Recommendations:**

Install fencing and controlled access points to better secure the perimeter.

Increase visibility of surveillance systems at the perimeter.

## Building Layout Analysis

**Observations:**

The aerial view shows an L shaped building with parking around it. It also seems to be adjacent to a Church.

Multiple entry points are visible, and main entrances are secured with cameras.

The layout seems accessible from multiple directions.

**Strengths:**

The building is surrounded by open space, reducing potential hiding spots.

**Weaknesses:**

Open access to multiple sides of the building.

No secure entry point. Insufficient barriers around the building.

**Recommendations:**

Reinforce entry points with controlled access systems.

Review windows or other potential access points for break-in risks.

## Surrounding Area Analysis

**Observations:**

The area is in a suburban-like environment.

Residential areas in close proximity could pose both opportunities (surveillance by residents) and risks (unwanted access).

Surrounding area has access to medical and protective facilities that can reach in at a decent time in case of emergency.

The Church next to the building could cause large crowd near the building, which could prevent detection of an incident.

**Strengths:**

The immediate surroundings do not seem overly congested, providing clear sightlines.

Proximity to emergency services, which would ensure quicker access in case of emergency.

**Weaknesses:**

Easy accessibility from surrounding streets and open spaces.

Crowded neighborhoods could result in undetected incidents.

**Recommendations:**

Monitor surrounding streets with strategically placed cameras.

## Defending Against Social Engineering Attacks

### Identification of Risks

**-RESTRICTED-**

#### **Observations:**

- DKIM and DMARC are not properly configured for the domain.
- SPF is present but not sufficient by itself to defend against email spoofing.
- Lack of email authentication increases the risk of phishing and email-based social engineering attacks.
- Attackers can exploit the absence of DKIM and DMARC to send emails appearing as legitimate communications from the domain.

#### **Risks:**

- **Email Spoofing:** Attackers can impersonate the domain to trick recipients into divulging sensitive information or downloading malicious content.
- **Phishing Attacks:** The lack of email authentication mechanisms increases the domain's vulnerability to phishing campaigns.
- **Reputation Damage:** A compromised domain can lead to loss of trust among recipients and damage to the organization's reputation.
- **Deliverability Issues:** Emails from the domain may be flagged as spam or rejected entirely by strict email providers.

#### **Strength of Analysis:**

- Clear evidence from the ActiveCampaign tool highlights specific deficiencies.
- Identification of technical gaps directly links to potential social engineering attack vectors.

## **Hardening Techniques**

#### **Proposed Techniques:**

##### **Implement DKIM:**

- Generate a DKIM record and publish it in the DNS zone file.
- Configure the mail server to sign outgoing emails using the DKIM private key.

**Impact:** Ensures email integrity and authenticity by verifying that the message content has not been altered.

### **Enforce DMARC:**

- Publish a DMARC policy in the DNS, ensuring alignment with SPF and DKIM.
- Start with a `p=none` policy for monitoring, then gradually move to `p=quarantine` or `p=reject`.

**Impact:** Enables recipient servers to decide on handling spoofed emails, reducing phishing and impersonation.

### **Enhance SPF:**

- Ensure the SPF record accurately lists all legitimate sending servers.
- Test SPF validity using tools to avoid misconfigurations.

**Impact:** Prevents unauthorized servers from sending emails on behalf of the domain.

### **Monitor and Report:**

- Use DMARC reporting to analyze spoofing attempts.
- Regularly review and update email authentication mechanisms.

**Impact:** Continuous monitoring ensures timely response to evolving threats.

### **Employee Training:**

- Conduct phishing simulation campaigns and educate employees on identifying fake emails.
- Encourage reporting suspicious emails to the security team.

**Impact:** Reduces human susceptibility to social engineering.

# Conclusion

The investigation into GORA Wizard School's digital and physical security landscape using OSINT tools has revealed significant findings that underscore the importance of proactive cybersecurity measures. Through detailed analysis, we identified vulnerabilities within the organization's technical infrastructure, social media presence, and physical environment, as well as risks associated with exposed information about key individuals.

## Key Findings

### **Technical Vulnerabilities:**

Lack of DNSSEC and email authentication protocols (SPF, DKIM, DMARC) increases the risk of phishing and email spoofing attacks.

Open ports and exposed subdomains, such as administrative and API endpoints, expand the organization's attack surface.

### **Social Media and OSINT Risks:**

Publicly accessible information on social media platforms and OSINT tools provides adversaries with ample data to craft targeted phishing or impersonation campaigns.

Unmonitored subdomains and unstructured metadata can lead to unauthorized access to internal systems.

#### **Physical Security Risks:**

Weak perimeter security and the absence of visible surveillance systems around the organization's facilities expose vulnerabilities to unauthorized physical access.

Building layouts and surrounding areas indicate multiple entry points with insufficient control measures.

#### **C-Suite Employee Exposure:**

Publicly available details about key personnel, including personal emails, phone numbers, and breached credentials, make them high-value targets for social engineering attacks.

### **The Role of OSINT in Business Security**

This investigation highlights the significant role that OSINT plays in identifying and mitigating potential risks. By analyzing publicly available data, organizations can better understand their attack surface and implement tailored security measures. However, the effectiveness of such measures depends on continuous monitoring and proactive updates to address evolving threats.

### **Importance of Continuous Monitoring**

In an era of dynamic and complex cyber threats, continuous monitoring and assessment of security systems are critical. Regular audits, employee training, and the adoption of advanced security technologies are essential to maintaining a robust security posture. Organizations like GORA Wizard School, which rely on public trust and global accessibility, must prioritize such practices to safeguard their reputation and operations.

### **Final Remarks**

To address the vulnerabilities identified, GORA Wizard School should implement the recommended mitigations, including stronger email authentication protocols, enhanced

physical security measures, and privacy controls for key personnel. By doing so, the organization can not only mitigate existing risks but also establish a resilient defense against future threats, ensuring the continuity of its mission to provide free education to millions worldwide.

## Appendices

### Metadata Findings

Metadata analysis revealed that files belonging to the domain “GORAWizard School.org” contain information about 6 different software and 4 servers.

#### FOCA

FOCA is an OSINT tool used to extract metadata and classified information from documents. By analyzing various file types such as PDF, DOCX, PPT, it collects metadata such as document owner, software used, network paths, operating system, email address information.

Servers	GORAWizard School.org 108.157.52.23
	GORAWizard School.org 108.157.52.59
	GORAWizard School.org 108.157.52.107
	GORAWizard School.org 108.157.52.125
Software	Skia/PDF m 119 Google Docs Renderer
	Quartz
	Skia/PDF m 120 Google Docs Renderer
	LuaTeX-1.15.0
	LaTeX with hyperref

## Skia/PDF m91 Google Docs Renderer

khan - FOCA Open Source 3.4.7.1

[Project](#) [Plugins](#) [Options](#) [TaskList](#) [About](#) [Cart](#)

**khan**

- Network
  - Clients (0)
  - Servers (4)
    - 108.0.0.0
    - 108.157.0.0
    - 108.157.52.0
    - Unknown Servers
- Domains
- Document Analysis
  - Files (200/200)
    - pdf (199)
    - Unknown (1)
- Metadata Summary
  - Users (0)
  - Folders (8)
  - Printers (0)
  - Software (6) **(6)**
    - Skia/PDF m119 Google Docs Renderer
    - Quartz
    - Skia/PDF m120 Google Docs Renderer
    - LuaTeX-1.15.0
    - LaTeX with hyperref
    - Skia/PDF m91 Google Docs Renderer
  - Emails (0)
  - Operating Systems (0)
  - Passwords (0)
  - Servers (0)
- Malware Summary (DIARIO)

**Foca**  
OPENSOURCE

Custom search

Search engines		Extensions		All	None	
<input checked="" type="checkbox"/> Google	<input checked="" type="checkbox"/> Bing	<input checked="" type="checkbox"/> DuckDuckGo	<input checked="" type="checkbox"/> doc	<input checked="" type="checkbox"/> docx	<input checked="" type="checkbox"/> xw	<input checked="" type="checkbox"/> odp
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> ppt	<input checked="" type="checkbox"/> ptx	<input checked="" type="checkbox"/> odt	<input checked="" type="checkbox"/> pdf
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> pps	<input checked="" type="checkbox"/> ppx	<input checked="" type="checkbox"/> ods	<input checked="" type="checkbox"/> wpd
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> xls	<input checked="" type="checkbox"/> xlx	<input checked="" type="checkbox"/> odg	<input checked="" type="checkbox"/> rtf
Download						
Download Date						
Size						
Metadata E...						
Malware An...						
Modified Date						
Id	Type	URL	Download	Download Date	Size	Metadata E...
0	pdf	https://www.khanacademy.org/r/map>Welcome-guide	•	11/26/2024 15:02:59	62.65 KB	• <input checked="" type="checkbox"/>
1	pdf	https://blog.khanacademy.org/wp-content/uploads/202...	•	11/26/2024 15:03:02	359.27 KB	• <input checked="" type="checkbox"/>
2	pdf	https://blog.khanacademy.org/wp-content/uploads/202...	•	11/26/2024 15:03:05	525.8 KB	• <input checked="" type="checkbox"/>
3	pdf	https://blog.khanacademy.org/wp-content/uploads/202...	•	11/26/2024 15:03:07	475.92 KB	• <input checked="" type="checkbox"/>
4	pdf	https://blog.khanacademy.org/wp-content/uploads/202...	•	11/26/2024 15:03:09	559.19 KB	• <input checked="" type="checkbox"/>
5	pdf	https://blog.khanacademy.org/wp-content/uploads/202...	•	11/26/2024 15:03:10	457.66 KB	• <input checked="" type="checkbox"/>
6	pdf	https://blog.khanacademy.org/wp-content/uploads/202...	•	11/26/2024 15:03:11	202.01 KB	• <input checked="" type="checkbox"/>
7	pdf	https://blog.khanacademy.org/wp-content/uploads/202...	•	11/26/2024 15:03:14	16.84 MB	• <input checked="" type="checkbox"/>
8	pdf	https://blog.khanacademy.org/wp-content/uploads/202...	•	11/26/2024 15:03:18	10.23 MB	• <input checked="" type="checkbox"/>
9	pdf	https://blog.khanacademy.org/wp-content/uploads/202...	•	11/26/2024 15:03:19	297.29 KB	• <input checked="" type="checkbox"/>
10	pdf	https://blog.khanacademy.org/wp-content/uploads/202...	•	11/26/2024 15:03:11	475.92 KB	• <input checked="" type="checkbox"/>
11	pdf	https://blog.khanacademy.org/wp-content/uploads/202...	•	11/26/2024 15:03:19	457.66 KB	• <input checked="" type="checkbox"/>
12	pdf	https://blog.khanacademy.org/wp-content/uploads/202...	•	11/26/2024 15:03:19	475.92 KB	• <input checked="" type="checkbox"/>
13	pdf	https://blog.khanacademy.org/wp-content/uploads/202...	•	11/26/2024 15:03:12	457.66 KB	• <input checked="" type="checkbox"/>
14	pdf	https://blog.khanacademy.org/wp-content/uploads/202...	•	11/26/2024 15:03:12	457.66 KB	• <input checked="" type="checkbox"/>
15	pdf	https://blog.khanacademy.org/wp-content/uploads/202...	•	11/26/2024 15:03:13	475.92 KB	• <input checked="" type="checkbox"/>
16	pdf	https://blog.khanacademy.org/wp-content/uploads/202...	•	11/26/2024 15:03:14	559.19 KB	• <input checked="" type="checkbox"/>
17	pdf	https://blog.khanacademy.org/wp-content/uploads/202...	•	11/26/2024 15:03:20	559.19 KB	• <input checked="" type="checkbox"/>
18	pdf	https://blog.khanacademy.org/wp-content/uploads/202...	•	11/26/2024 15:03:12	457.66 KB	• <input checked="" type="checkbox"/>
19	pdf	https://blog.khanacademy.org/wp-content/uploads/202...	•	11/26/2024 15:03:16	475.92 KB	• <input checked="" type="checkbox"/>
20	pdf	https://blog.khanacademy.org/wp-content/uploads/202...	•	11/26/2024 15:03:17	262.4 KB	• <input checked="" type="checkbox"/>
21	pdf	https://blog.khanacademy.org/wp-content/uploads/202...	•	11/26/2024 15:03:18	559.19 KB	• <input checked="" type="checkbox"/>
22	pdf	https://blog.khanacademy.org/wp-content/uploads/202...	•	11/26/2024 15:03:19	475.92 KB	• <input checked="" type="checkbox"/>
23	pdf	https://blog.khanacademy.org/wp-content/uploads/202...	•	11/26/2024 15:03:20	297.29 KB	• <input checked="" type="checkbox"/>
24	pdf	https://blog.khanacademy.org/wp-content/uploads/202...	•	11/26/2024 15:03:22	475.92 KB	• <input checked="" type="checkbox"/>
25	pdf	https://blog.khanacademy.org/wp-content/uploads/202...	•	11/26/2024 15:03:22	559.19 KB	• <input checked="" type="checkbox"/>
26	pdf	https://blog.khanacademy.org/wp-content/uploads/202...	•	11/26/2024 15:03:22	475.92 KB	• <input checked="" type="checkbox"/>
27	pdf	https://blog.khanacademy.org/wp-content/uploads/202...	•	11/26/2024 15:03:22	475.92 KB	• <input checked="" type="checkbox"/>
28	pdf	https://blog.khanacademy.org/wp-content/uploads/202...	•	11/26/2024 15:03:22	297.29 KB	• <input checked="" type="checkbox"/>
29	pdf	https://blog.khanacademy.org/wp-content/uploads/202...	•	11/26/2024 15:03:22	559.19 KB	• <input checked="" type="checkbox"/>
30	pdf	https://blog.khanacademy.org/wp-content/uploads/202...	•	11/26/2024 15:03:22	297.29 KB	• <input checked="" type="checkbox"/>
31	pdf	https://blog.khanacademy.org/wp-content/uploads/202...	•	11/26/2024 15:03:22	559.19 KB	• <input checked="" type="checkbox"/>
32	pdf	https://blog.khanacademy.org/wp-content/uploads/202...	•	11/26/2024 15:03:22	457.66 KB	• <input checked="" type="checkbox"/>
33	pdf	https://blog.khanacademy.org/wp-content/uploads/202...	•	11/26/2024 15:03:22	559.19 KB	• <input checked="" type="checkbox"/>
34	pdf	https://blog.khanacademy.org/wp-content/uploads/202...	•	11/26/2024 15:03:22	475.92 KB	• <input checked="" type="checkbox"/>
35	pdf	https://blog.khanacademy.org/wp-content/uploads/202...	•	11/26/2024 15:03:24	457.66 KB	• <input checked="" type="checkbox"/>

khan - FOCA Open Source 3.4.7.1

[Project](#) [Plugins](#) [Options](#) [TaskList](#) [About](#) [Cart](#)

**khan**

- Network
  - Clients (0)
  - Servers (4)
    - 108.0.0.0
    - 108.157.0.0
    - 108.157.52.0
    - Unknown Servers
- Domains
- Document Analysis
  - Files (200/200)
    - pdf (199)
    - Unknown (1)
- Metadata Summary
  - Users (0)
  - Folders (8)
  - Printers (0)
  - Software (6) **(6)**
    - Skia/PDF m119 Google Docs Renderer
    - Quartz
    - Skia/PDF m120 Google Docs Renderer
    - LuaTeX-1.15.0
    - LaTeX with hyperref
    - Skia/PDF m91 Google Docs Renderer
  - Emails (0)
  - Operating Systems (0)
  - Passwords (0)
  - Servers (0)
- Malware Summary (DIARIO)

**Attribute**

Attribute	Value
<b>All software found (6) - Times found</b>	
Software	Skia/PDF m119 Google Docs Renderer
Software	Quartz
Software	Skia/PDF m120 Google Docs Renderer
Software	LuaTeX-1.15.0
Software	LaTeX with hyperref
Software	Skia/PDF m91 Google Docs Renderer