Asphalia

Analytics

Cyber Exposure Assessment

ACME Corporation

Table of contents

Introduction

Objective

The objective of this report is to provide an overview of the information that can be gathered over the internet about a company without any specific knowledge

Perimeter

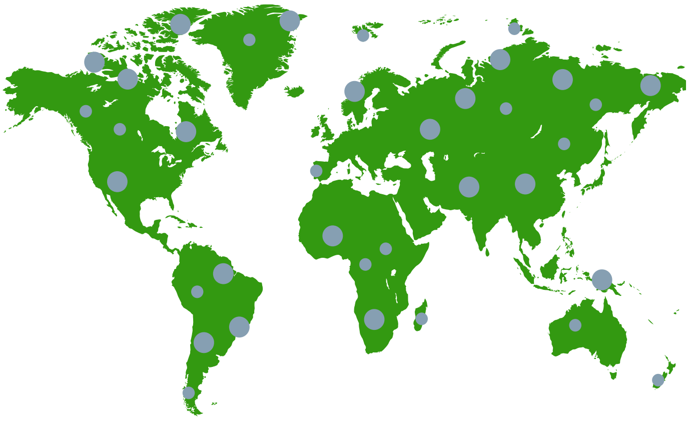
The perimeter is the whole company without any insider access - all the displayed results are based on information publicly available through public networks

Audience

This report is meant to be distributed to anyone with sufficient technical knowledge (mainly basic network)

Context

Information technology security is a critical aspect of any modern organization, as it helps to protect sensitive data and systems from unauthorized access, theft, and damage.



This report will provide an analysis of the current state of your IT security outside of your organization, including an assessment of potential vulnerabilities and risks, as well as recommendations for improving overall security.

The objective of this report is to provide an overview of the information that can be gathered over the internet about a company without any specific knowledge.

External Perimeter

Open-source intelligence (OSINT) is the process of collecting, analysing, and disseminating information from publicly available sources to support decision-making and strategic planning.

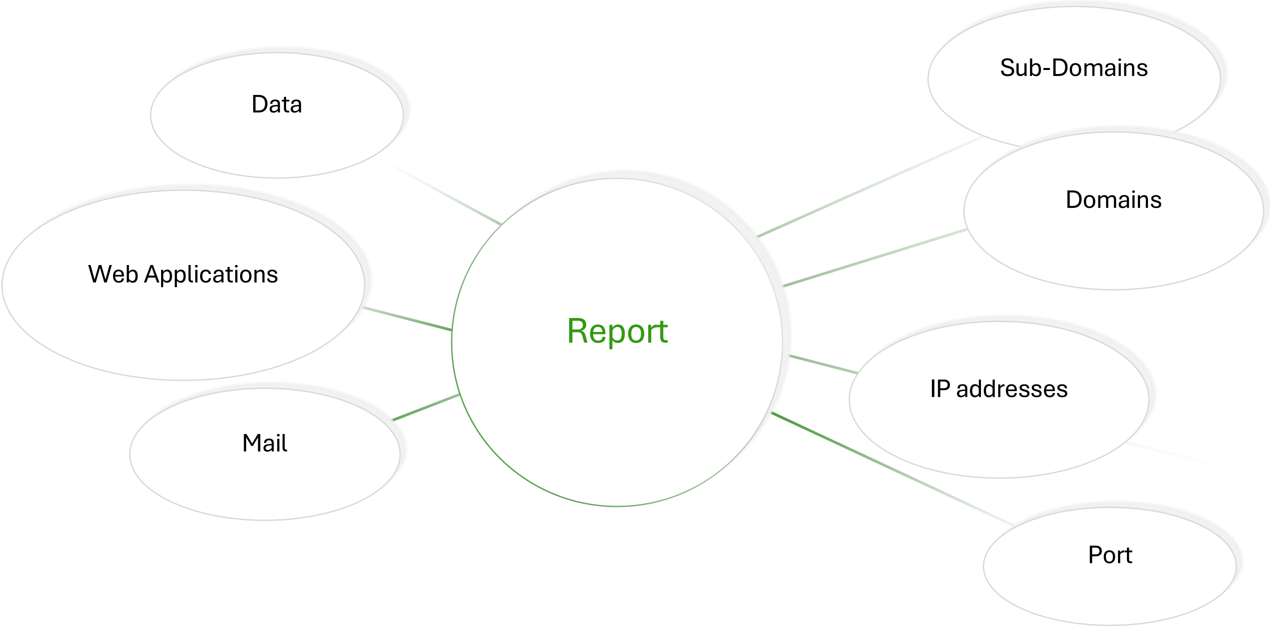
It involves gathering information from a wide range of sources, including the internet, social media, news articles, government reports, and other publicly accessible data. OSINT is used in a variety of fields, including intelligence gathering, law enforcement, business intelligence, and cybersecurity.

It also highlights the importance of Pre-attack intelligence in the OSINT field and its role in identifying and mitigating potential threats, and to give an insight of how organizations can use OSINT to gather intelligence that might be used by their potential adversaries and improve their cyber defence.

In the context of security, the pre-attack phase refers to the period of time before an actual attack takes place. During this phase, organizations focus on identifying potential threats and vulnerabilities, and taking steps to mitigate them before they can cause damage

Covered Aspects

By focusing on the pre-attack phase, organizations can take proactive measures to reduce their risk and be better prepared for potential attacks. Pre-attack phase activities are crucial for making informed decisions about security measures, budget allocation and incident response. Additionally, these activities can provide organizations with a deeper understanding of the current threat landscape, which can help them develop more effective security strategies.



Disclaimer

The information contained in this report is intended for informational purposes only. It is not intended to be a substitute for professional advice, including but not limited to, legal, financial, or security advice. The information in this report is based on data and information gathered from publicly available sources and is believed to be accurate and reliable as of the date of publication. However, the accuracy, completeness, and reliability of the information in this report cannot be guaranteed.

The author, publisher, and any third parties involved in the creation of this report shall not be held liable for any damages whatsoever, including but not limited to, direct or indirect damages, arising from or in connection with the use of the information contained in this report.

This report is not a detailed vulnerability report or black box penetration test. It will only show you what has been discovered and identified. Should some vulnerabilities be found, none of them will be exploited. Their sole existence is sufficient to trigger an action plan for their remediation.

Domains & Sub-Domains

Managing sub-domains is a critical practice in IT security, as neglected or poorly maintained sub-domains can become significant vulnerabilities. Organizations often create sub-domains for various purposes, such as testing, development, or specific services. However, if these sub-domains are not properly monitored, they can pose security risks :

1. **Subdomain Takeover :** If a sub-domain points to an external service (e.g., a cloud provider) that is no longer in use, attackers may be able to claim it and host malicious content under the organization's domain.
2. **Exposure of Sensitive Data :** Development or staging sub-domains may unintentionally expose internal applications, credentials, or configurations.
3. **Phishing and Brand Abuse :** Attackers can exploit abandoned or forgotten sub-domains to conduct phishing attacks, impersonating the organization.
4. **Attack Surface Expansion :** The more sub-domains exist, the larger the attack surface. If they are not regularly audited, they may provide unexpected entry points for attackers.

DNS Records

DNS (Domain Name System) records are like signposts that help the internet find websites, emails, and other services. Different types of DNS records serve different purposes. Here are some of the most common ones:

1. **A Record (Address Record)** – Connects a domain name to an IP address
2. **CNAME Record (Canonical Name)** – Points one domain to another
3. **MX Record (Mail Exchange)** – Directs email to the right mail
4. **TXT Record (Text Record)** – Stores text information, often used for security
5. **NS Record (Name Server)** – Specifies the servers that manage a domain's DNS
6. **PTR Record (Pointer Record)** – Links an IP address back to a domain
7. **AAAA Record** – Like an A record but for IPv6 addresses.

A. Domain Name Servers

NS Records

✗ **11** nameservers do not have DNSSEC configured

✓ **0** nameservers have zone transfer allowed

11

Servers are used to resolve your domains

NS records (Name Server records) in DNS specify which servers are authoritative for a domain. In other words, they tell the internet which DNS servers have the official information (like IP addresses) for your domain.

When someone tries to visit your website, their computer checks your domain's NS records to find out which DNS servers to ask for the correct IP address. Most domains have multiple NS records for reliability, so if one server is down, another can answer the request.

Without correct NS records, your website or email will not work, because no one will know where to find your domain's DNS information.

For the Name Servers, we checked :

- For proper zone transfer configuration – to prevents unauthorized access to your DNS zone data, which could expose internal network details ;
- DNSSEC Implementation - to protect against DNS spoofing and cache poisoning.

#	Extracted Domain	Zone Transfer	DNSSEC
1	example.com	Not allowed	Not Enabled
2	example.com	Not allowed	Not Enabled
3	example.com	Not allowed	Not Enabled
4	example.com	Not allowed	Not Enabled
5	example.com	Not allowed	Not Enabled
6	example.com	Not allowed	Not Enabled
7	example.com	Not allowed	Not Enabled
8	example.com.com	Not allowed	Not Enabled
9	example.com.com	Not allowed	Not Enabled
10	example.com	Not allowed	Not Enabled
11	example.com	Not allowed	Not Enabled

#	Event data	IP Address
1	example.com-example.com	758.719.584.456
2	example.com.net	980.515.806.732
3	example.com.example.com	732.764.715.804, 771.787.327.917
4	example.com.example.com	591.899.901.486, 849.628.519.261
5	example.com.net	862.629.791.940
6	example.com-example.com	689.406.994.890
7	example.com-example.com	594.439.772.751
8	example.com.net	506.496.796.696
9	example.com.net	470.709.712.973
10	example.com.net	999.995.787.664
11	example.com.net	566.945.976.862

B. Mails records

MX Records

✓ **7** mail servers are not blacklisted
✗ **4** mail servers have SPF configured
✗ **0** mail servers have DKIM configured
✗ **2** mail servers have DMARC configured

7

Servers are used to receive your mails

MX records (Mail Exchange records) in DNS tell the internet which mail servers should receive email for a domain. When someone sends you an email, their email service looks up your domain's MX records to find out where to deliver the message.

For the Name Servers, we checked :

- If they have been blacklisted ;
- SPF: which is used to check who can send emails for your domain ;
- DKIM: to prove that emails are really from you and unchanged ;
- DMARC: to tells others what to do if SPF or DKIM checks fail and give you feedback.

#	Extracted Domain	Blacklist Status	SPF Config	DKIM Config	DMARC Config
1	example.com	Not Blacklisted	Configured	Not Configured	Configured
2	example.com	Not Blacklisted	Not Configured	Not Configured	Not Configured
3	example.com	Not Blacklisted	Not Configured	Not Configured	Not Configured
4	example.com	Not Blacklisted	Not Configured	Not Configured	Not Configured
5	example.com	Not Blacklisted	Configured	Not Configured	Not Configured
6	example.com	Not Blacklisted	Configured	Not Configured	Configured
7	example.com.com	Not Blacklisted	Configured	Not Configured	Not Configured

#	Event data	IP Address
1	example.com.example.com.com	592.600.405.530, 863.939.741.671
2	example.com.example.com	985.517.776.822
3	example.com.example.com	555.707.634.787
4	example.com.example.com	804.638.791.941
5	example.com.example.com.com	902.310.409.667, 298.757.268.584
6	example.com.example.com.com	535.368.966.462, 509.294.704.443
7	example.com.example.com.com	657.729.569.629, 670.304.688.587

C. Sub-domains

A and AAAA Records

⚠ **42** sub-domains have been identified

⚠ **33** sub-domains have an IP address associated

42

Sub-domains

A and AAAA records in DNS are used to connect a domain name (like example.com) to an IP address, which is how computers find each other on the internet.

Simply looking at the list might be informative to identify forgotten or orphan subdomains that might not be relevant anymore.

#	Event data	IP Address
1	example.com	858.910.666.347
2	example.com	555.931.402.513
3	example.com	975.805.542.356, 376.835.385.684
4	example.com.com	947.416.989.509
5	example.com	451.559.946.830
6	example.com.net	501.398.419.511, 549.287.912.575
7	example.com.net	651.971.575.519, 815.764.557.978
8	example.com.net	560.826.756.789, 679.581.621.758
9	remote.example.com	450.670.522.834
10	example.com.eu	922.441.868.544
11	example.com.eu	264.427.854.749
12	example.com.eu	922.441.868.544
13	example.com.eu	305.720.310.430
14	example.com.eu	555.931.402.513
15	www.example.com.eu	305.720.310.430
16	ftp.example.com	934.496.579.453
17	mail.example.com	743.444.970.566
18	pop3.example.com	743.444.970.566
19	events.example.com	858.910.666.347
20	sip.example.com	nan
21	vpn.example.com	450.670.522.834
22	autodiscover.example.com	729.526.896.863, 407.953.722.469
23	smtp.example.com	514.507.482.969, 508.919.786.294
24	_submission._tcp.example.com	nan
25	_sipfederationtls._tcp.example.com	nan
26	_sip._tls.example.com	nan
27	example.com.eu	nan
28	example.com.eu	770.533.837.323
29	example.com.eu	264.427.854.749
30	example.com.eu	674.578.991.877
31	example.com.eu	364.939.522.274, 729.526.896.863

32	example.com.eu	810.415.451.565
33	example.com.eu	555.931.402.513
34	test.example.com	975.805.542.356, 376.835.385.684
35	old.example.com	975.805.542.356, 376.835.385.684
36	_sip._tls.example.com	nan
37	_sipfederationtls._tcp.example.com	nan
38	example.com.com	nan
39	example.com.com	364.939.522.274, 548.363.915.466
40	example.com.com	nan
41	example.com.com	451.559.946.830
42	example.com.eu	264.427.854.749

D. CNAME records

CNAME Records

⚠ **3** records are associated with other domains. These domains might be under your control or belong to a third-party organisation

3

Entries are pointing to another domain

A CNAME record (Canonical Name record) in DNS is used to make one domain name an alias for another domain name.

Instead of pointing directly to an IP address, a CNAME record points your subdomain (like example.com.com) to another domain name (like example.com). When someone visits the alias (e.g., example.com.com), DNS looks up the CNAME, then finds the real domain's address and sends the visitor there.

This makes it easy to manage multiple subdomains or services, since you only need to update the main domain’s address if it changes.

The following security checks for CNAME entries can be performed :

- Check for subdomain takeover: Ensure CNAMEs don’t point to unclaimed or expired third-party resources ;
- Verify CNAME targets: Confirm all CNAMEs point only to trusted, intended domains ;
- Avoid information leaks: Don’t expose internal hostnames or sensitive infrastructure details ;
- Monitor for misconfigurations: Regularly review and update CNAME records to prevent errors ;
- Use DNSSEC: Protect DNS records from spoofing and tampering ;
- Limit public exposure: Only publish necessary CNAMEs externally.

Regular audits and careful management of CNAME records help prevent security risks and domain misuse.

#	Event data	Path
1	example.com	example.com.com → example.com
2	example.com.eu	example.com → penguin.example.com → example.com.eu

3	example.com.com	example.com → autodiscover.example.com → example.com.com

#	Event data	IP Address
1	example.com	947.416.989.509
2	example.com.eu	395.995.903.298
3	example.com.com	319.725.958.850, 782.642.806.403

E. Other records

PTR and TXT Records

⚠ **0** PTR records have been found

⚠ **4** TXT records have been found

4

Entries are pointing to another domain

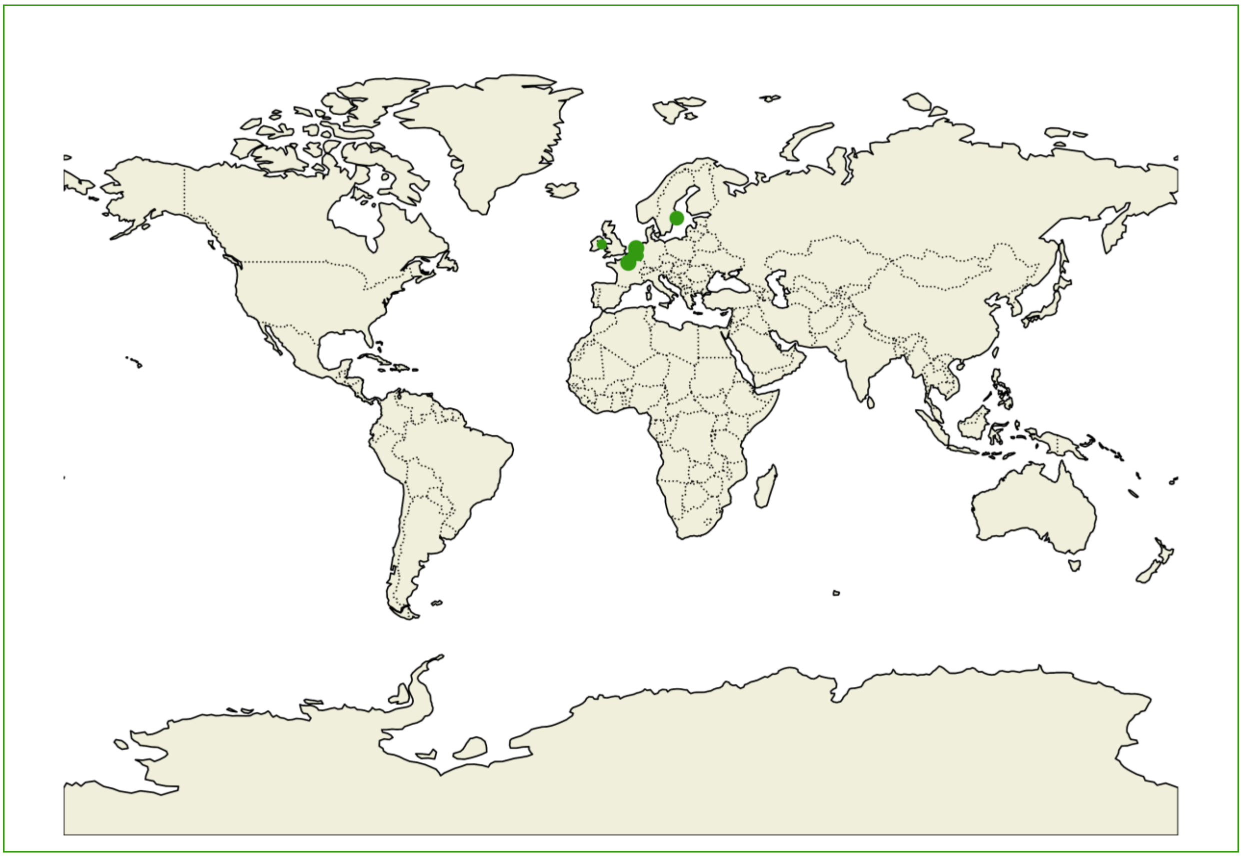
A TXT record (Text Record) is a type of DNS resource record that allows domain administrators to associate arbitrary text with a domain name. Originally designed for human-readable notes, TXT records are now widely used to store both human and machine-readable data for various purposes.

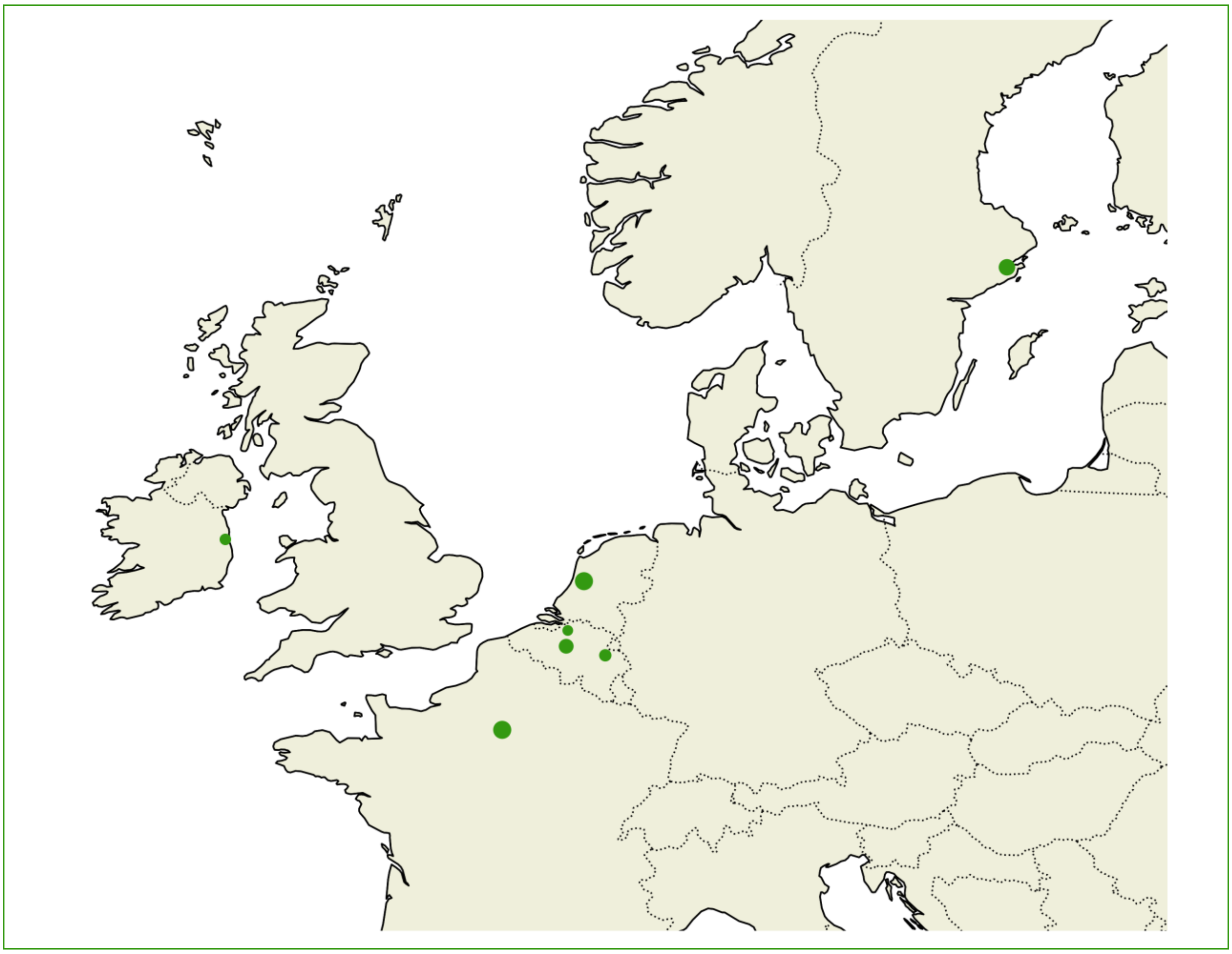
A PTR (Pointer) record is used for reverse DNS lookups, mapping an IP address back to its associated domain name or hostname. This is the opposite of an A record, which maps a domain name to an IP address. PTR records are stored in special reverse DNS zones and are essential for verifying the identity of hosts, especially for email servers to help prevent spam. When a reverse lookup is performed, the PTR record reveals the domain name associated with the queried IP address.

#	Extracted Domain	Event data
1	example.com	example.com
2	example.com	example.com.be
3	example.com	example.com
4	example.com	example.com.com

#	Event data	IP Address
1	example.com	507.826.657.703
2	example.com.be	858.910.666.347
3	example.com	455.341.699.353, 507.381.602.956
4	example.com.com	975.805.542.356, 376.835.385.684

F. Locations of hosted domains





Social

The social dimension of an organization's external attack surface encompasses the publicly accessible information related to its personnel, communication channels, and associated digital identities. This information, if not properly managed, can be leveraged by threat actors for social engineering, phishing campaigns, or targeted attacks.

In this section, we analyse the social exposure of the domain, focusing on two critical aspects: the public availability and potential compromise of email addresses, and the presence of personally identifiable information (PII) linked to the domain.

Mail addresses - Potential compromission

Email addresses associated with a domain are prime targets for cybercriminals seeking entry points through phishing, credential stuffing, or spear-phishing attacks.

Mail Addresses

✉ **2** addresses have been found to be exposed. Knowing the tendency of password re-use, these should be investigated to potentially modify their associated asswords.

20

Mail addresses associated with the domains

Here, we examine the extent to which email addresses linked to the domain are publicly exposed or have appeared in known data breaches. By identifying compromised or at-risk email accounts, organizations can better understand their susceptibility to targeted attacks and take steps to mitigate these risks.

#	Email	Breaches
1	vincent@example.com	LinkedIn, AntiPublicCombo
2	info@example.com	123RF

#	Extracted Domain	Event data
1	example.com	example.com@example.com
2	example.com	work@example.com
3	example.com	media@example.com
4	example.com	vincent@example.com
5	example.com	example.com@example.com
6	example.com	info@example.com
7	example.com	example.com@example.com
8	example.com	example.com@example.com
9	example.com	info@example.com
10	example.com	fresh@example.com
11	example.com	admin@example.com
12	example.com	funcup@example.com
13	example.com	vipexperience@example.com
14	example.com	wsc@example.com

15	example.com	sales@example.com
16	example.com	example.com@example.com
17	example.com	accounting@example.com
18	example.com	whistleblower@example.com
19	example.com	amp@example.com
20	example.com	info@example.com

Personal / Social information associated with domains

Beyond email addresses, the exposure of personal information-such as names, job titles, phone numbers, and other identifiers-can significantly increase an organization's vulnerability to social engineering attacks.

Social

☎ **70** Personally Identifiable Information's or Social accounts have been found in association with the domains. These could be used in the context of spear fishing attacks.

70

Social accounts associated with the domains

This subsection explores the types and scope of social media relations found in association with the domain. Understanding the breadth of exposed PII and social accounts enables organizations to assess privacy risks and implement appropriate security measures to protect their personnel and digital assets.

#	Extracted Domain	Social Network	Target
1	example.com	twitter	https://example.com/followwrt
2	example.com	facebook	https://example.com/followwrt
3	example.com	facebook	https://example.com/brandworksbe
4	example.com	instagram	https://example.com/follow_wrt
5	example.com	linkedin	https://example.com/company/weerts-supply-chain-n
6	example.com	instagram	https://example.com/adfpro_
7	example.com	facebook	https://example.com/example.com
8	example.com	github	https://example.com/validatr
9	example.com	github	https://example.com/mattbryson
10	example.com	twitter	https://example.com/intent
11	example.com	github	https://example.com/0b244cf0212b90f8d44c
12	example.com	github	https://example.com/carhartl
13	example.com	github	https://example.com/harvesthq
14	example.com	github	https://example.com/morr
15	example.com	github	https://example.com/twbs
16	example.com	instagram	https://example.com/v1
17	example.com	facebook	https://example.com/sharer
18	example.com	instagram	https://example.com/europeanvwfuncup
19	example.com	twitter	https://example.com/home
20	example.com	instagram	https://example.com/155833707900388
21	example.com	twitter	https://example.com/skechersusa

22	example.com	facebook	https://example.com/about
23	example.com	facebook	https://example.com/europeanvwfuncup
24	example.com	twitter	https://example.com/privacy
25	example.com	facebook	https://example.com/skechersfootwear
26	example.com	instagram	https://example.com/skechers
27	example.com	github	https://example.com/chartist-js
28	example.com	github	https://example.com/webpack-contrib
29	example.com	github	https://example.com/summernote
30	example.com	github	https://example.com/sweetalert2
31	example.com	instagram	https://example.com/p
32	example.com	github	https://example.com/jquery
33	example.com	instagram	https://example.com/followwrt
34	example.com	github	https://example.com/jamesbrobb
35	example.com	github	https://example.com/chris-rock
36	example.com	github	https://example.com/zloirock
37	example.com	github	https://example.com/warrenweckesser
38	example.com	github	https://example.com/crypto-browserify
39	example.com	github	https://example.com/jmorel
40	example.com	github	https://example.com/uuidjs
41	example.com	github	https://example.com/exceljs
42	example.com	github	https://example.com/indutny
43	example.com	github	https://example.com/mrrio
44	example.com	github	https://example.com/juanpgaviria
45	example.com	github	https://example.com/flamenco
46	example.com	github	https://example.com/diegocr
47	example.com	github	https://example.com/gavvers
48	example.com	github	https://example.com/niklasvh
49	example.com	github	https://example.com/vuetifyjs
50	example.com	github	https://example.com/sortablejs
51	example.com	github	https://example.com/eaparango
52	example.com	github	https://example.com/danielhusar
53	example.com	github	https://example.com/dollaruw
54	example.com	github	https://example.com/burnburnrocket
55	example.com	github	https://example.com/siefkenj
56	example.com	github	https://example.com/jbaysolutions
57	example.com	github	https://example.com/gingerchris
58	example.com	github	https://example.com/pablohess
59	example.com	github	https://example.com/fjenett
60	example.com	linkedin	https://example.com/company/w-racing-team
61	example.com	github	https://example.com/acspike
62	example.com	github	https://example.com/lsdriscoll
63	example.com	github	https://example.com/lifof
64	example.com	github	https://example.com/woolfg
65	example.com	github	https://example.com/stefslon
66	example.com	github	https://example.com/ineedfat
67	example.com	facebook	https://example.com/weertssupplychain
68	example.com	twitter	https://example.com/widgets
69	example.com	github	https://example.com/promises-aplus
70	example.com	github	https://example.com/eligrey

Knowledge of social accounts (like GitHub) linked to a domain or website can be dangerous because attackers can use this information for targeted attacks such as phishing, social engineering, or impersonation.

For example, if an attacker knows the official GitHub account associated with a business, they can attempt to impersonate it to trick users into sharing sensitive information or downloading malicious code.

Additionally, if these accounts are not properly secured or monitored, they can be hijacked and used to distribute malware, leak confidential data, or damage the organization’s reputation. Even seemingly innocuous details from social accounts can be exploited to craft convincing attacks or gain deeper access to business systems.

Infrastructure

A thorough understanding of an organization's external infrastructure is fundamental to evaluating its security posture. The infrastructure assessment examines the publicly accessible assets associated with the domain, including servers, network devices, and cloud services.

By mapping these components, we can identify potential vulnerabilities, misconfigurations, and points of exposure that could be exploited by threat actors.

his section provides a comprehensive overview of the organization's visible infrastructure and highlights areas that may require further attention or remediation.

Open ports

Open network ports represent potential entry points into an organization's systems and are often targeted by attackers seeking to exploit vulnerabilities or gain unauthorized access.

In this subsection, we present the findings of a systematic port scan conducted across the domain's infrastructure.

Open ports

⚠ **83 Ports are open in association with the** 42 domains.

✗ **37** of these ports are considered insecure.

83

Open ports

The analysis details which ports are accessible from the internet, the services running on them, and any associated security risks. Understanding the port landscape is essential for reducing the attack surface and prioritizing remediation efforts.

#	Event data	Descr	Secure
1	example.com:80	HTTP	No
2	penguin.example.com:80	HTTP	No
3	mail.example.com:443	HTTPS	Yes
4	autodiscover.example.com:80	HTTP	No
5	smtp.example.com:25	SMTP	No
6	mail.example.com:143	IMAP	No
7	mail.example.com:587	SMTP (Submission)	Yes
8	mail.example.com:5229	nan	nan
9	mail.example.com:110	POP3	No
10	mail.example.com:993	IMAPS	Yes
11	mail.example.com:465	SMTPS	Yes
12	mail.example.com:25	SMTP	No
13	pop3.example.com:443	HTTPS	Yes
14	events.example.com:80	HTTP	No
15	shop.example.com:80	HTTP	No
16	events.example.com:443	HTTPS	Yes

17	penguin.example.com:443	HTTPS	Yes
18	shop.example.com:443	HTTPS	Yes
19	mail.example.com:995	POP3S	Yes
20	example.com:22	SSH	Yes
21	example.com:443	HTTPS	Yes
22	example.com:2082	cPanel	No
23	example.com:8880	Cloudflare HTTP Alt	No
24	example.com:8080	HTTP Alt	No
25	example.com:80	HTTP	No
26	example.com:8443	Cloudflare HTTPS Alt	Yes
27	example.com:443	HTTPS	Yes
28	example.com:2052	nan	nan
29	example.com.com:443	HTTPS	Yes
30	example.com:2086	nan	nan
31	example.com:2053	Cloudflare HTTPS Alt	Yes
32	example.com:2087	Cloudflare HTTPS Alt	Yes
33	example.com:2083	Cloudflare HTTPS Alt	Yes
34	example.com.com:80	HTTP	No
35	old.example.com:443	HTTPS	Yes
36	test.example.com:80	HTTP	No
37	old.example.com:80	HTTP	No
38	test.example.com:443	HTTPS	Yes
39	example.com:80	HTTP	No
40	example.com.com:443	HTTPS	Yes
41	example.com:443	HTTPS	Yes
42	example.com.com:80	HTTP	No
43	example.com.com:443	HTTPS	Yes
44	example.com.com:80	HTTP	No
45	example.com.eu:587	SMTP (Submission)	Yes
46	example.com.eu:465	SMTPS	Yes
47	example.com.eu:443	HTTPS	Yes
48	example.com.eu:110	POP3	No
49	example.com.eu:995	POP3S	Yes
50	example.com.eu:443	HTTPS	Yes
51	example.com.eu:993	IMAPS	Yes
52	example.com.eu:80	HTTP	No
53	example.com.eu:443	HTTPS	Yes
54	example.com.eu:443	HTTPS	Yes
55	example.com.eu:443	HTTPS	Yes
56	example.com.eu:80	HTTP	No
57	example.com.eu:80	HTTP	No
58	example.com.eu:25	SMTP	No
59	example.com.eu:5025	nan	nan
60	example.com.eu:443	HTTPS	Yes
61	example.com.eu:25	SMTP	No
62	example.com.eu:443	HTTPS	Yes
63	example.com.eu:22	SSH	Yes
64	example.com.eu:8069	nan	nan
65	example.com.eu:80	HTTP	No
66	example.com.eu:443	HTTPS	Yes

67	example.com.eu:443	HTTPS	Yes
68	example.com:80	HTTP	No
69	example.com.eu:80	HTTP	No
70	example.com.eu:143	IMAP	No
71	example.com.eu:443	HTTPS	Yes
72	example.com:443	HTTPS	Yes
73	example.com.eu:80	HTTP	No
74	example.com.eu:80	HTTP	No
75	example.com.eu:80	HTTP	No
76	example.com.eu:80	HTTP	No
77	example.com.eu:8024	nan	nan
78	example.com.eu:443	HTTPS	Yes
79	example.com.eu:80	HTTP	No
80	example.com.eu:80	HTTP	No
81	example.com.com:80	HTTP	No
82	example.com.com:443	HTTPS	Yes
83	example.com.com:21	FTP Control	No

#	Event data	IP Address
1	example.com:80	858.910.666.347
2	penguin.example.com:80	395.995.903.298
3	mail.example.com:443	743.444.970.566
4	autodiscover.example.com:80	729.526.896.863, 407.953.722.469
5	smtp.example.com:25	514.507.482.969, 508.919.786.294
6	mail.example.com:143	743.444.970.566
7	mail.example.com:587	743.444.970.566
8	mail.example.com:5229	743.444.970.566
9	mail.example.com:110	743.444.970.566
10	mail.example.com:993	743.444.970.566
11	mail.example.com:465	743.444.970.566
12	mail.example.com:25	743.444.970.566
13	pop3.example.com:443	743.444.970.566
14	events.example.com:80	858.910.666.347
15	shop.example.com:80	395.995.903.298
16	events.example.com:443	858.910.666.347
17	penguin.example.com:443	395.995.903.298
18	shop.example.com:443	395.995.903.298
19	mail.example.com:995	743.444.970.566
20	example.com:22	858.910.666.347
21	example.com:443	858.910.666.347
22	example.com:2082	975.805.542.356, 376.835.385.684
23	example.com:8880	975.805.542.356, 376.835.385.684
24	example.com:8080	975.805.542.356, 376.835.385.684
25	example.com:80	975.805.542.356, 376.835.385.684
26	example.com:8443	975.805.542.356, 376.835.385.684
27	example.com:443	975.805.542.356, 376.835.385.684
28	example.com:2052	975.805.542.356, 376.835.385.684
29	example.com.com:443	975.805.542.356, 376.835.385.684
30	example.com:2086	975.805.542.356, 376.835.385.684

31	example.com:2053	975.805.542.356, 376.835.385.684
32	example.com:2087	975.805.542.356, 376.835.385.684
33	example.com:2083	975.805.542.356, 376.835.385.684
34	example.com.com:80	975.805.542.356, 376.835.385.684
35	old.example.com:443	975.805.542.356, 376.835.385.684
36	test.example.com:80	975.805.542.356, 376.835.385.684
37	old.example.com:80	975.805.542.356, 376.835.385.684
38	test.example.com:443	975.805.542.356, 376.835.385.684
39	example.com:80	451.559.946.830
40	example.com.com:443	364.939.522.274, 548.363.915.466
41	example.com:443	451.559.946.830
42	example.com.com:80	364.939.522.274, 548.363.915.466
43	example.com.com:443	451.559.946.830
44	example.com.com:80	451.559.946.830
45	example.com.eu:587	810.415.451.565
46	example.com.eu:465	810.415.451.565
47	example.com.eu:443	810.415.451.565
48	example.com.eu:110	810.415.451.565
49	example.com.eu:995	810.415.451.565
50	example.com.eu:443	555.931.402.513
51	example.com.eu:993	810.415.451.565
52	example.com.eu:80	810.415.451.565
53	example.com.eu:443	555.931.402.513
54	example.com.eu:443	264.427.854.749
55	example.com.eu:443	364.939.522.274, 729.526.896.863
56	example.com.eu:80	555.931.402.513
57	example.com.eu:80	264.427.854.749
58	example.com.eu:25	810.415.451.565
59	example.com.eu:5025	810.415.451.565
60	example.com.eu:443	264.427.854.749
61	example.com.eu:25	674.578.991.877
62	example.com.eu:443	922.441.868.544
63	example.com.eu:22	922.441.868.544
64	example.com.eu:8069	922.441.868.544
65	example.com.eu:80	922.441.868.544
66	example.com.eu:443	264.427.854.749
67	example.com.eu:443	922.441.868.544
68	example.com:80	555.931.402.513
69	example.com.eu:80	264.427.854.749
70	example.com.eu:143	810.415.451.565
71	example.com.eu:443	305.720.310.430
72	example.com:443	555.931.402.513
73	example.com.eu:80	264.427.854.749
74	example.com.eu:80	922.441.868.544
75	example.com.eu:80	555.931.402.513
76	example.com.eu:80	364.939.522.274, 729.526.896.863
77	example.com.eu:8024	770.533.837.323
78	example.com.eu:443	770.533.837.323
79	example.com.eu:80	674.578.991.877
80	example.com.eu:80	305.720.310.430

81	example.com.com:80	947.416.989.509
82	example.com.com:443	947.416.989.509
83	example.com.com:21	947.416.989.509

Applications

Applications exposed to the internet represent a critical component of an organization's external attack surface.

This section evaluates the security posture of web applications and related services associated with the domain.

By systematically analysing these applications, we aim to identify weaknesses that could be exploited by malicious actors, as well as to assess the effectiveness of existing security controls.

Web servers

Web applications are frequent targets for cyberattacks that exploit browser behavior and insecure configurations. The following settings serve as critical defenses against a range of common attacks:

- Content Security Policy (CSP): Limits which resources (like scripts and images) can be loaded, helping to prevent cross-site scripting (XSS), clickjacking, and data injection attacks by ensuring only trusted content is executed in the browser.
- Strict Transport Security (HSTS): Forces browsers to use secure HTTPS connections, protecting against protocol downgrade attacks and ensuring data is encrypted in transit.
- X-Content-Type-Options: Prevents browsers from interpreting files as a different MIME type, which helps block certain types of code injection attacks.
- X-Frame-Options: Prevents your site from being embedded in frames on other domains, defending against clickjacking attacks that trick users into performing unintended actions.
- X-XSS-Protection: Activates built-in browser filters to block detected XSS attacks, providing an additional layer of defense, though modern best practice is to rely on server-side protections and CSP.
- Firewall / WAF enabled: Provides an external layer of defense, blocking malicious traffic and attacks before they reach the application.

Web Servers

✕ **25** Webservers are exposed unencrypted.

✓ **26** Webservers are securely exposed.

51

Web Servers

Implementing and regularly verifying these security headers and controls is a best practice that strengthens a website's overall security posture, mitigates vulnerabilities, and helps ensure compliance with industry standards.

#	SourceFile	CSP	HSTS	Content Type	xFrame Option	XSS Protec	Security TXT	Firewall
1	old.example.com	-	-	-	-	-	NOK	-
2	penguin.example.com	-	-	-	-	-	NOK	-
3	shop.example.com	NOK	OK	NOK	OK	NOK	NOK	NOK
4	test.example.com	NOK	NOK	NOK	NOK	NOK	NOK	OK
5	example.com.eu	NOK	NOK	NOK	NOK	NOK	NOK	NOK

6	example.com	NOK	NOK	OK	OK	OK	NOK	NOK
7	example.com.eu	-	-	-	-	-	NOK	-
8	example.com	NOK	NOK	OK	OK	NOK	NOK	OK
9	example.com.com	NOK	NOK	OK	OK	NOK	NOK	OK

Vulnerabilities

Application vulnerabilities are among the most common entry points for attackers seeking to compromise systems or exfiltrate sensitive data.

This subsection investigates known and potential security flaws within the domain's web applications, such as outdated software, misconfigurations, or exposure to common attack vectors.

Vulnerabilities

❌ **145** Critical or High vulnerabilities have been found in association with the 42 domains.

164

06

Vulnerabilities

By highlighting these vulnerabilities, we provide actionable insights to help prioritize remediation efforts and strengthen the overall security posture.

The summary of the vulnerabilities found

Metric	**Value**
Total Domains Scanned	23
Total Security Findings	26637
Critical Severity	0
High Severity	145
Medium Severity	3790
Low Severity	12471
Informational	0
Unique Security Tools Used	0
Domains with Critical Findings	0
Domains with High Findings	0

The Top 10 vulnerabilities

#	**Finding**	**Details**	**Severity**
1	Nmap NSE: vulners	Target: example.com Tool: NMAP Description: cpe:/a:openbsd:openssh:7.2p2:	High

2	Nmap NSE: vulners	Target: example.com.eu Tool: NMAP Description: nginx 1.18.0:	High
3	Nmap NSE: vulners	Target: example.com.eu Tool: NMAP Description: cpe:/a:apache:http_server:2.4.52:	High
4	Nmap NSE: vulners	Target: example.com.eu Tool: NMAP Description: cpe:/a:apache:http_server:2.4.52:	High
5	Nmap NSE: vulners	Target: example.com.eu Tool: NMAP Description: nginx 1.18.0:	High
6	Nmap NSE: vulners	Target: example.com Tool: NMAP Description: nginx 1.13.3:	High
7	Nmap NSE: vulners	Target: example.com.eu Tool: NMAP Description: nginx 1.18.0:	High
8	Nmap NSE: vulners	Target: example.com.eu Tool: NMAP Description: cpe:/a:python:python:3.10.12:	High
9	Nmap NSE: vulners	Target: example.com.eu Tool: NMAP Description: cpe:/a:openbsd:openssh:8.9p1:	High
10	Nmap NSE: vulners	Target: example.com.eu Tool: NMAP Description: nginx 1.18.0:	High

Certificates

Web certificates play a vital role in securing communications and establishing trust between users and applications. Improperly configured, expired, or weak certificates can expose the organization to risks such as man-in-the-middle attacks or loss of credibility.

Web certificates

⚠ **16** domains have been tested.

✗ **8** hosts have issues identified.

28

Certificates

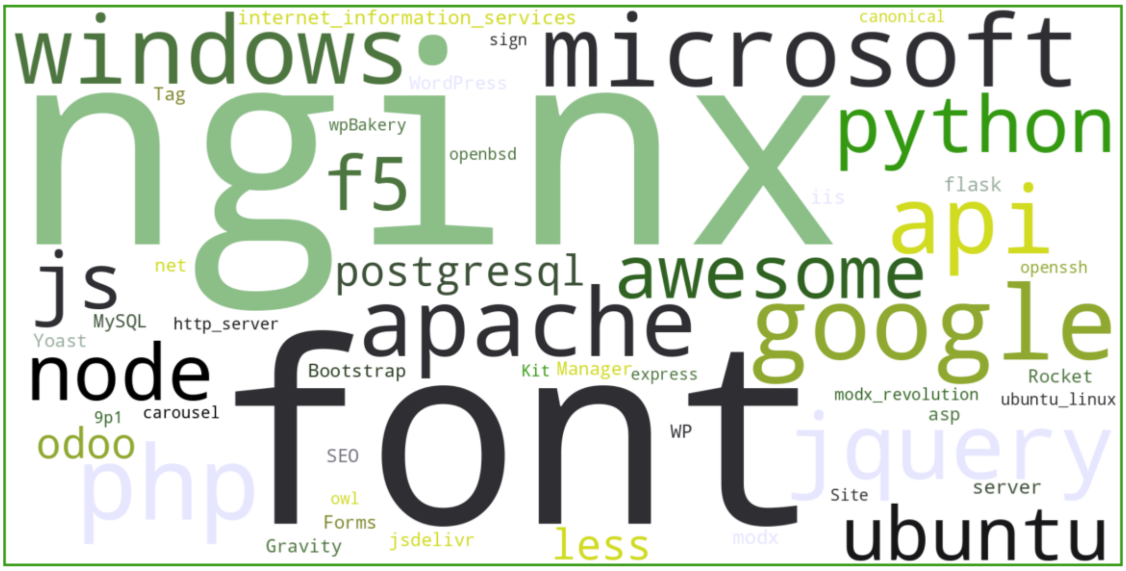
This subsection reviews the status and configuration of web certificates associated with the domain, assessing their validity, strength, and adherence to best practices. Proper management of web certificates is essential for ensuring secure and trustworthy online interactions.

#	Domain	Unacceptable Setting
1	old.example.com	TLSv1.0 enabled
2	old.example.com	TLSv1.1 enabled
3	old.example.com	Weak ECC key strength: 128
4	penguin.example.com	TLSv1.0 enabled
5	penguin.example.com	TLSv1.1 enabled
6	penguin.example.com	Weak accepted cipher: TLSv1.2 112 bits TLS_RSA_WITH_3DES_EDE_CBC_SHA
7	penguin.example.com	Weak accepted cipher: TLSv1.1 112 bits TLS_RSA_WITH_3DES_EDE_CBC_SHA

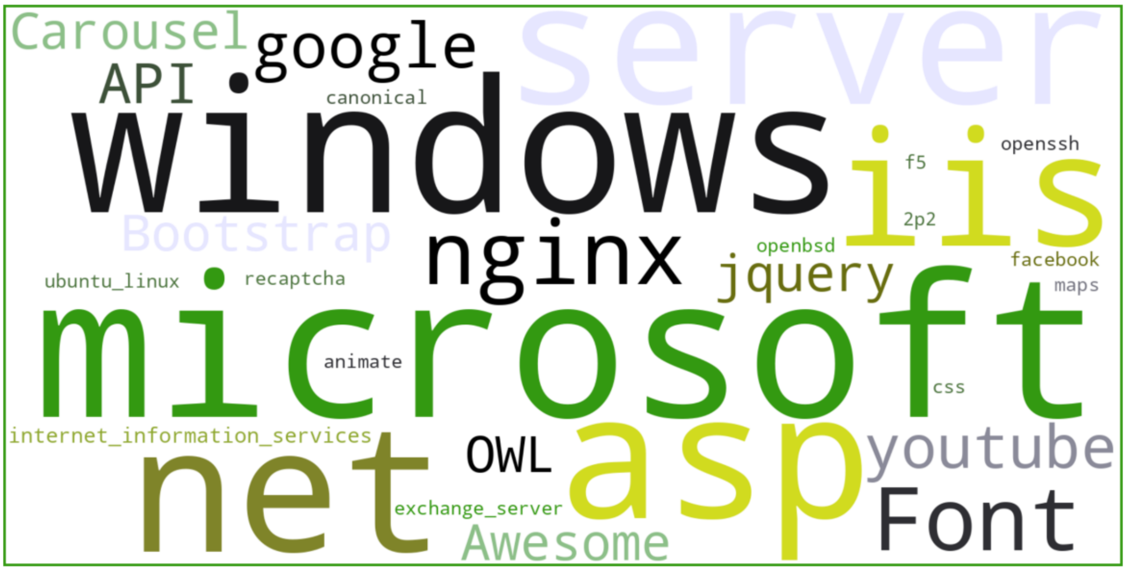
8	penguin.example.com	Weak accepted cipher: TLSv1.0 112 bits TLS_RSA_WITH_3DES_EDE_CBC_SHA
9	example.com.eu	TLSv1.0 enabled
10	example.com.eu	TLSv1.1 enabled
11	example.com.eu	Weak accepted cipher: TLSv1.2 112 bits TLS_RSA_WITH_3DES_EDE_CBC_SHA
12	example.com.eu	Weak accepted cipher: TLSv1.1 112 bits TLS_RSA_WITH_3DES_EDE_CBC_SHA
13	example.com.eu	Weak accepted cipher: TLSv1.0 112 bits TLS_RSA_WITH_3DES_EDE_CBC_SHA
14	shop.example.com	TLSv1.0 enabled
15	shop.example.com	TLSv1.1 enabled
16	shop.example.com	Weak accepted cipher: TLSv1.2 112 bits TLS_RSA_WITH_3DES_EDE_CBC_SHA
17	shop.example.com	Weak accepted cipher: TLSv1.1 112 bits TLS_RSA_WITH_3DES_EDE_CBC_SHA
18	shop.example.com	Weak accepted cipher: TLSv1.0 112 bits TLS_RSA_WITH_3DES_EDE_CBC_SHA
19	test.example.com	TLSv1.0 enabled
20	test.example.com	TLSv1.1 enabled
21	test.example.com	Weak ECC key strength: 128
22	example.com.eu	Weak ECC key strength: 128
23	example.com	TLSv1.0 enabled
24	example.com	TLSv1.1 enabled
25	example.com	Weak ECC key strength: 128
26	example.com.com	TLSv1.0 enabled
27	example.com.com	TLSv1.1 enabled
28	example.com.com	Weak ECC key strength: 128

Technologies

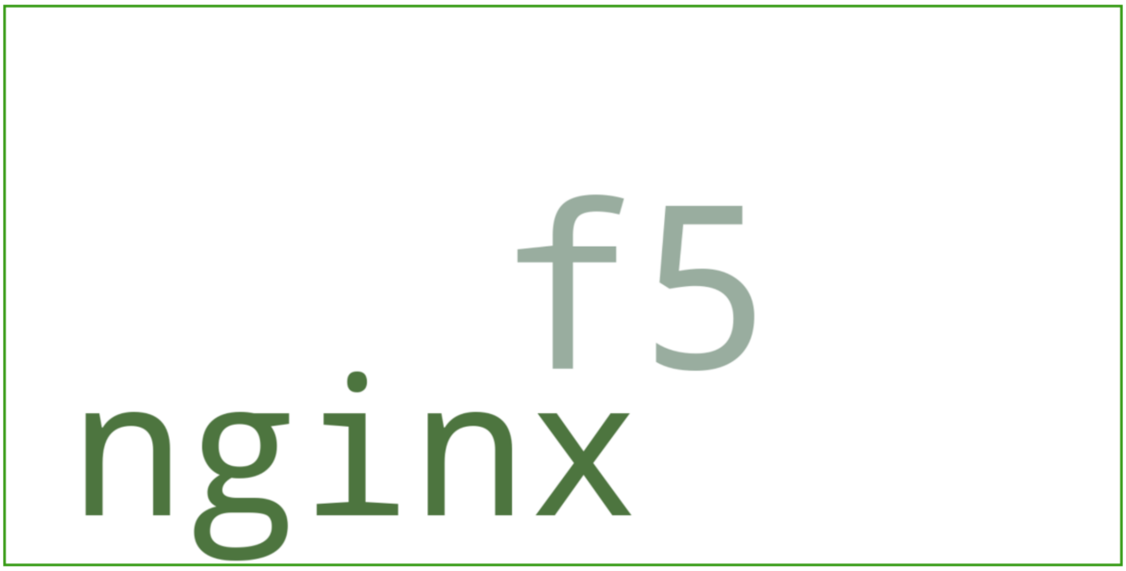
The various technologies identified across the whole infrastructure are :



example.com



example.com



example.com.com

microsoft
windows
addthis
manager
tag
asp
nginx
php
drupal
server
iis
net
api
google
font
f5

example.com

WordPress
slider
PHP
google
swiper
slick
SEO
maps
tag
cloudflare
manager
MySQL
api
font
Yoast
Drupal
recaptcha
migrate
jquery

example.com

Management Summary

This section provides a consolidated overview of the findings from the external attack surface assessment of the domain.

Mail - Summary		
SPF Records correctly set : ✗ **4**	DKIM Records correctly set : ✗ **0**	DMARC Records correctly set : ✗ **2**

Domains - Summary		
Number of sub-domains : ⚠ **42**	Domains with an associated address : **42**	Domains CNAME : ⚠ **3**

Name Servers - Summary		
SPF Records correctly set : ✓ **0**	DKIM Records correctly set : ✗ **11**	

Social & Personal information - Summary		
Identified mail addresses : **20**	Leaked addresses : ✉ **2**	Social accounts : **70**

Infrastructure - Summary		
Domains with an associated address : **42**	Open ports : ⚠ **83**	Insecure Open ports : ✗ **37**

Certificates - Summary		
Domains to check : **28**	Domains tested : ⚠ **16**	Badly configured : ✗ **8**

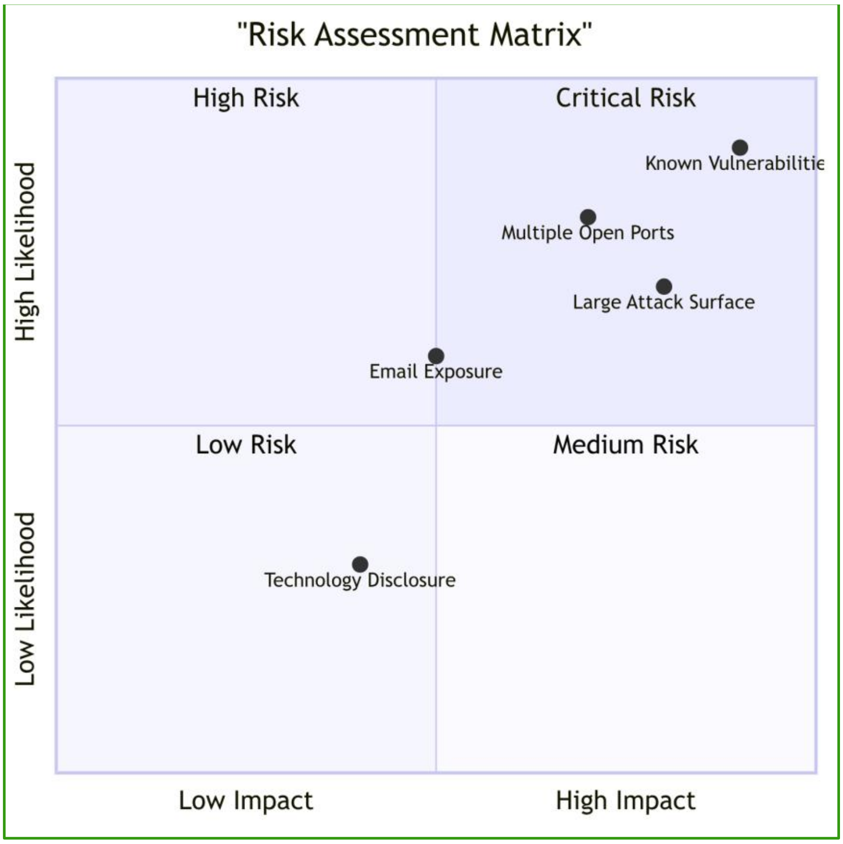
Web Servers - Summary		
Web Servers : **51**	Servers unencrypted : ✗ **25**	Servers encrypted : ✓ **26**

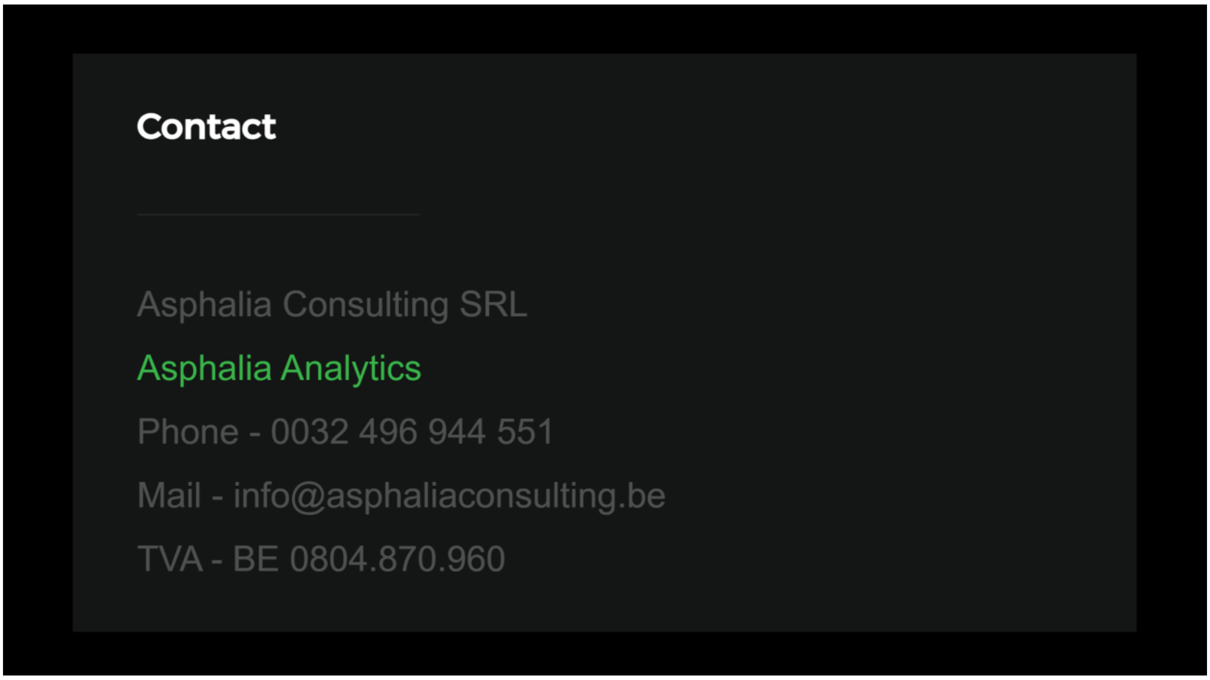
Vulnerabilities - Summary		
Critical vulnerabilities : **0**	High Vulnerabilities: ✗ **145**	Medium Vulnerabilities : **3790**✗

Heatmap

The following heatmap visually summarizes the findings from our OSINT-based attack surface analysis of the organization. By representing areas of heightened exposure and potential vulnerability as zones of greater intensity, the heatmap offers an immediate overview of where digital assets, entry points, or security weaknesses are most concentrated.

This visualization enables both security practitioners and decision-makers to quickly pinpoint high-risk areas within the organization’s external footprint, prioritize mitigation efforts, and allocate resources more effectively.





Contact

Asphalia Consulting SRL

Asphalia Analytics

Phone - 0032 496 944 551

Mail - info@asphaliaconsulting.be

TVA - BE 0804.870.960