Darkscope

CIQ360

Threat Scan Report

October 2023

DEMO

CIQ360 Threat Scan

This CIQ360 Threat Scan report is an examination of the risk profile of cyberspace on behalf of the organisation. This scan presents a snapshot profile of the external cyber risk, as it was conducted over a short period of time, usually days. The information gathered from the internet, social media and the darkweb about the organisation is not exhaustive or complete, due to the continuous growth of cyberspace, its size and the constantly changing nature of focus of the darkweb, particularly. A more comprehensive understanding requires longer monitoring with a broader scope, such as that provided by Darkscope's Cyber Threat Sentinel or Cyber Watchtower services.

Darkscope delivers this report with all due diligence and best efforts but cannot guarantee its accuracy.

This report is in four parts.

1. The Cyber Interference Risk Score provides an overall rating of the cyber risk for the organisation.

2. The CIQ360 Threat Report results rate the risk to the organisation from key vectors of cyberattacks:
   - Phishing
   - DDoS and Ransom
   - Website hijacking
   - Ransomware

   These are prevalent forms of attack against an organisation, its partners, and customers. Understanding these risks can help an organisation prepare itself against these forms of attack.

3. Findings & Rating

   🛑 Catastrophic A cyber security incident may have already occurred.

   ⚠ Critical Deviations from standards or best practices identified - acute danger

   ◆ Warning Deviations from standards or best practices identified - no acute threat

   ✓ Positive No deviations from standards or best practices noted

   ℹ Neutral Purely informative, no influence on the result

   Warning, Critical, and Catastrophic items require action to mitigate weaknesses or risks to the organisation.

4. Available Information. This information is in cyberspace. It may include emails of former employees or contracts that are no longer current or show infrastructure links that can be exploited (DDoS) that may have weak security or is redundant.

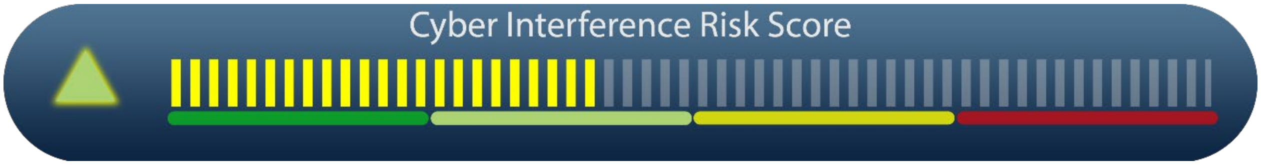
Each part of this report includes "How to use this information" which is self-explanatory.

Cyber Interference™ Risk Score

How to use this information

This score is a summary of your overall cyber risk. It is compiled from all the risk data Darkscope collects across the internet, social media and the darkweb about you and profiles your organisation within your industry sector and geographic region. Using baseline data collected across millions of data points daily and algorithms that compares your risk factors, your Cyber Interference Risk Score is the most reliable overall assessment of the specific cyber risk for your organisation.

Darkscope provides CIRS with more detail as part of its other enterprise cyber intelligence services. When included in Cyber Threat Sentinel and Cyber Watchtower services it includes more detail such as Partner Risk Score, Darkweb Risk Level, Impersonate and Social Media Sentiment Rating.



DEMO has a normal CIRS score, and it is within its expected industry and location range. This means DEMO has a normal footprint in cyberspace and a normal risk of being attacked, compared with other businesses in its region and industry.

A normal Cyber Interference Risk Score indicates external interest in the organisation, region, or industry and that the organisation is being examined. Threat actors always have an increased interest in businesses like DEMO. It is recommended to adjust the Cyber Security Program to mitigate the findings from this report.

More about the Cyber Interfrence Risk Score here.

CIQ360 Threat Scan Report Summary

How to use this information

The CIQ360 Threat Scan Results identify your risk across four key cyber risk areas: Phishing, DDoS/RDDoS, Website Hijacking, and Ransomware. The rating scale is Low – Medium – High – Extreme. Each threat type explains how it is determined, your result and how you should interpret or react when the risk is high.

Risk Levels

LOW

LOW indicates little or no identifiable risk for this attack vector. Low risk in an attack vector means that the correlation of all data points has shown only a minimal risk of being attacked from this vector.

MEDIUM

MEDIUM indicates that there is external interest in the organisation, region, or industry. Or the amount of information found suggests that an attacker would choose this attack vector.

HIGH

HIGH indicates external interest that could be of concern. Based on the information our system has found and analysed, it is most likely that an attacker would choose this vector to compromise the customer.

EXTREME

EXTREME indicates that the organisation is considered a very high-value target for this attack vector, and the information found in cyberspace shows that the customers might have been breached in the past using this vector.

Results

Phishing Attack

To calculate the risk of a phishing attack, we use the information an attacker has or could find in cyberspace about DEMO people, roles, and internal processes. We incorporate past breaches, current cyber-attacks, and campaigns to determine how likely is it that an attacker would choose DEMO as a target.

Our system has found 42 email addresses. Out of those, we have identified no recent account breaches.

DDoS & RDDoS Attack

Our system analyses the customer external-facing infrastructure using a black-box approach. This means we simulate what an attacker would be able to find in cyberspace about DEMO. This includes domains, sub-domains, applications, and existing protections such as Web application firewalls or load balancers. We also include the location of services and determine the local readiness for DDoS attacks.

We have identified a **Low-Medium risk** for DEMO based on the analysis we did.

Website hijack

Our system analysis the customer external-facing infrastructure from a black-box approach. This means we simulate what an attacker would be able to find in cyberspace about DEMO. This includes domains, sub-domains, applications, and existing protections such as Web application firewalls or load balancers. Out of this information, we determine how vulnerable a customer might be.

We have identified that DEMO has a **Medium risk** of being attacked due to the application WordPress and used AddOns we have found. It is always recommended to review all external-facing applications and perform a penetration test of those to ensure there are no vulnerabilities.

Ramsomware

To calculate the risk of Ransomware attacks, we correlate all available information and create a risk profile containing staff, product/service, and business information. Ransomware is most likely to be successful if the attacker knows about the internal processes and communications of the target. We compare this profile with thousands of other businesses in the same industry and region to create a risk value.

DEMO has a **LOW** risk of being targeted with ransomware.

Identified Cyber Risks for DEMO

How to use this information

Findings are in presented in 5 levels. Neutral fundings are purely for information purposes. Positive findings are shows where no deviations from standards or best practices are noted.Warnings are shown when our system detects devistions from standards or best practises. Critial findings are shown for items that could pose acute danger, and Catastrophic findings indicate that DEMO has suffered a security incided or is about to be attacked.

🛑	⚠	◆	✓	ℹ
Catastrophic	Critial	Warnings	Positive	Neutral

Findings

Note: No active scans or penetrations are performed on the systems or system components.

Risk Level	Identified Risk	Notes and Recommendations
⚠	Warning: Data from Demo are part of a data list on Telegram	Our system has found Demo staff information as part of a data list on a Telegram channel. Details: Source: 0b0ltus Free Leaks Data: Email addresses, Names, Department Date: 17/08/2023
⚠	Warning: the domain demo.co is a look-a-like domains and might be used for phishing attacks agains dome users or customers.	Our system found the domain demo.co that seems to be a look-a-like domain. Our domain permutation module idetifies simmelar domains and determines how close these domains look to the original. Demo.co has a risk score of 85/100 and could be uses for phishing attacks in the future.
◆	Warning: There is no DMARC record found	The domains DEMO.com does not use a dmarc record for email setup. Domain-based Message Authentication, Reporting and Conformance, or DMARC for short, is a technical standard to protect email senders and recipients from spam, spoofing and phishing. *We recommend that you review the current configuration.*

⚠	The website hosting.DEMO.dk seems to be a test page of some sort.	The domains hosting.DEMO.com shows content from Huset middlefart and it seems that this is a test page. The content looks like news with partially political content. This increases the risk of a cyber attack from people that don’t agree with the statements. *We recommend that you review the current configurations and disable this site if possible.*
⚠	Warning: The website DEMO.com uses a plugin: XML-RPC	Our test shows that the domain DEMO.com uses the function XML-RPC. *We recommend that you review the current configurations and disable this function if possible.*
⚠	Share host. The main website as well as cmp.DEMO.com are hosted on a shared server.	Sharing a web server increased the risk of an attack as the host server coulds be targeted because of another page that is on the same server *It is not recommended to use shared server and to use a VPS instead.*
⚠	Warning: No PTR Record found on the main email server	mail1-demo.com , mail2-demo.com, mail3-demo.com have no PTR record. This might be a problem because many organizations will not accept email from a server without a PTR record. *We recommend that you review the current configurations.*
⚠	Some users have been part of several breaches in the last 2 years	Our system has detects several users that are part of multiple past breached. Each incided on its own might no pose a risk anymore because they are relatively old. However, if a user is involved in several breached over a short periode of time, it increased the risk of cyber attacks drastically. *We recommend to identify these users and ofer additional secueity awareness training to them.*
ℹ	Info: BVD incident contains some of MIL email addresses.	Some of MIL email addresses have been part of a database called BVD. This event was in August 2021, this is why we marked it as low-risk info.
ℹ	Info: MyHeritage incident contains some of MIL email addresses.	Some of MIL email addresses have been part of a data breach called MyHeritage. This event is already a couple of years old, this is why we marked it as low-risk info.
ℹ	Info: LinkedInScrape incident contains some of MIL email addresses.	Some of MIL email addresses have been part of a data breach called LinkedInScrape. This event is already a couple of years old, this is why we marked it as low-risk info.

Available Information - Email addresses

How to use this information

Publicly available email addresses are a normal part of every organisation's external-facing operation. They are used in marketing, publicity and engaging customers and the public. The cyber risk they represent is that they provide a list of targets for phishing or scam emails and can also be spoofed to scam or phish your customers, partners, or staff. Knowing which emails are public lets you make these people aware of their heightened risk of becoming a target and to be more diligent and capable of identifying unusual or suspicious behaviour and activity.

For this report, Darkscope has identified 13 publicly available email addresses.

Email address	First name	Last name	Department	Position
pernille@demo.com	Pernille	Thomsen		
jeshansen@demo.com	Jes	Hansen		
lindholm@demo.com	Leon	Lindholm		
dahlin@demo.com	Karen	Dahlin		
johannsen@demo.com	Leif	Johannsen		
thorsted@demo.com	Claus	Thorsted		
pol@demo.com	Pol	Den		
ursula@demo.com	Ursula	Larsen		
jan@demo.com	Jan	Broder		
wolff@demo.com	Jan	Wolff		
hersom@demo.com	Gitte	Hersom		
vetc-myn@demo.com				
interpreters@demo.com				

Available information - infrastructure

How to use this information

Information associated with the hostname, such as IP addresses, DNS and Netblock owner, can provide an attacker with a point of entry (brute force or weak login/password) or a less protected point of attack (DDoS). Ensuring all your IP addresses are well protected will reduce the effect of any attack or breach attempt.

For this report, Darkscope has analysed the public available domains and subdomains. Most of the domains found are hosted in Denemark with one domain hosted in Finnland. We noticed, that the main pages as well as cmp.DEMO.dk are hosted on a shared server. This increased the risk of a compromise as DEMO relys on the collective security of the server.

Hostname	IP Address	Type	Reverse DNS	Netblock Owner	Country
www.DEMO.com	94.201.103.152	A	linux1.uro.com	ZITCOM	UK
luva01.hosting.DEMO.som	91.200.59.151	A	91.210.59.151	DIN-SERVER	UK

hosting.DEMO.com	185.54.76.218	A	185.51.76.218	DIN-SERVER	UK
mon.DEMO.dcom	185.210.212.184	A	customer.site.eu	ZITCOM	UK
cmp.DEMO.com	37.124.81.4	NS	cmp.demo.com	ALSOCLOUDOY	US

Detailed checkpoints

Darkscope's system correlates over 300 datapoints to determine the Cyber Interference Risk Score. In addition, our system reviews configuration settings for Web, DNS, and Email servers and compares them with common best practices.

The tables below show the Web, DNS and Email items and the result of this test.

Web security

ID	Title	Description	Result
W1	HSTS	Usage of HSTS (HTTP Strict Transport Security)	✓
W2	TLS	Usage of TLS	⚠
W3	X-Header	Check if the Referrer-Policy-Header is set	✓
W4	X-Content	Check if the X-Content-Type-Options-Header is set	✓
W5	X-Frame	Check if the X-Frame-Options-Header is set	✓
W6	X-Permit	Check if the X-Permitted-Cross-Domain-Policies-Header is set	✓
W7	CSP	Check if the Content-Security-Policy-Header (CSP-Header) is set	✓
W8	Software patch level	This score evaluates the patch level of the software used on the web server	⚠
W9	User tracking	This score assesses the respect for the privacy of website visitors	⚠
W10	Web server reputation	This score evaluates the web server for attacks that originated from them	✓
W11	AS Reputation	This score evaluates the reputation of the autonomous systems (AS)	
W12	Domain reputation	This score checks the URLs of the web server for copyright violations and against blacklists that contain phishing, malware and known data breaches.	✓
W13	Dark web information	The "Darknet" rating evaluates the attack surface with regards to the domain.	✓

DNS & Email security

ID	Title	Result
D1	SOA Expire Value out of recommended range	✓
D2	DNS Record found	✓
D3	No Bad Glue Detected	✓
D4	At Least Two Name Servers Found	✓
D5	All name servers are responding	✓
D6	All of the name servers are Authoritative	✓
D7	Local NS list matches Parent NS list	✓
D8	Name Servers appear to be Dispersed	✓

D9	Name Servers have Public IP Addresses	✓
D10	Serial numbers match	✓
D11	Primary Name Server Listed At Parent	✓
D12	SOA Serial Number Format appears valid	✓
D13	SOA Refresh Value is within the recommended range	✓
D14	SOA Retry Value is within the recommended range	✓
D15	SOA Minimum TTL Value is within allowed values	✓
D16	No Open Recursive Name Server Detected	✓
D17	SPF Record found	✓
D18	SPF record is valid	✓
D19	DMARC Record found	⚠
D20	Blacklist & Reputation	✓
D21	Open relay check	✓
D22	MTA-STS (Mail Transfer Agent Strict Transport Security)	✓
D23	DANE (DNS-based Authentication of Named Entities)	✓
D24	Email encryption	✓

Appendix

Darkscope’s Cyber Interference™ Risk Score

Darkscope’s Cyber Interference Risk Score profiles and rates the risks of a cyberattack for an organisation, not just their readiness or ability to respond. A Cyber Risk Score delivers more than a maturity based assessment can, as it looks beyond the walls of the organisation to the root of cyberthreats.

As an organisation builds their digital footprint; to increase market presence and competitiveness and make it easier to interact with customers, its digital footprint provides source material that makes the organisation a potential target for cybercriminals. Cybercriminals use public information to build profiles of target organisations. This includes published news and reports, internet activity and social media data on suppliers, customers and key people in the organisation.

They track movements of employees and contractors to find weak links in security or other behaviour that can be exploited. The intent is to breach security and steal data or intellectual property, extort money or damage the reputation of the organisation. This level of sophistication of preparation can deliver lucrative rewards for these criminal groups. The Cyber Risk Interference Score measures the key factors that create cyber risks for an organisation. It considers internet presence and profile, looking for risk indicators in the deepweb that show nefarious activity targeted at the organisation.

Most organisations don’t (or can’t) measure or estimate their risk from cyberattacks, but a successful attack will be expensive. Darkscope has developed a proprietary process using Artificial Intelligence (AI) that measures an organisation’s cyber risk. We use this process to rate over 1 million business daily to create a baseline score for regions and industries. This baseline score is unique in the industry ans allow our customers to determine their risk of being attacked in comparison to other businesses in the same location or Industry.

We start with the organisation’s presence in the surface web. We look at public profile, social media, marketing and advertising activity and media coverage. We cross-reference this data within the deepweb and darknet looking for activity and indicators of threats. This produces a present state profile of the organisation that is more than an internal assessment and which forms the basis of the Cyber Risk Score.

We also consider external changes in the market, such as attacks on competitors, or increased activity in a geographic region, that indicate increased cyberthreat activity, applicable to the organisation. A Cyber Risk Score report allows an organisation to understand its risk. With this information it can optimise its cybersecurity solutions