AssetZero

→ GROUP–IB

Intelligence-driven Attack Surface Management

Table of contents

What is the external attack surface?

The external attack surface comprises a company's Internet-facing assets and defines the security perimeter. Potential assets include IP addresses, domains, SSLs, services, ports, software and storage systems. While straightforward, the attack surface is often gravely overlooked. This is because many organizations falsely assume that they have full visibility over their assets.

The attack surface is bigger than you think. Networks have never been more decentralized, with assets scattered across on-premise locations, clouds and third-party vendors. The expanding attack surface makes assets harder to track and evaluate, which leaves organizations more exposed and vulnerable.

Regardless how well companies configure their processes and security systems, they will inevitably end up with difficult-to-manage risk factors such as Shadow IT, vulnerable network perimeters, misconfigurations and human error, and dark web exposure.

Undefined and unpatched network perimeters 1

Managing all the elements of a company's perimeter, including IP addresses, domains, SSLs, ports, services, and software, has become a herculean task as the digital footprints left by organizations grow expontentially.

Misconfigurations, vulnerabilities and simple oversight across the network perimeter are the most frequent cause of breaches despite the adoption of comprehensive policies, scanning tools and best practices.

Shadow IT 2

Individual departments within a company often set up their own IT infrastructure to facilitate working processes (e.g., a marketing team creates new websites, rents servers for them, and deploys additional systems and applications).

IT and Infosec departments within these companies are rarely notified of these changes, resulting in the infrastructure running on vulnerable, hackable hardware and software.

Dark web exposure, botnets, and third-party breaches 3

As the cybercriminal landscape grows, the amount of data available to attackers increases exponentially. This creates telemetry, either from malware logs, third-party data breaches or mentions of your organization and assets on the dark web that indicate attacks or planned activity.

Misconfigurations and human error 4

Errors and oversights lead to unprotected services, open databases, and backups all becoming publicly available. Deploying new systems or cloud services in a new IP range makes such systems and services invisible to existing security controls.

An outside-in approach to security

There is a reason why the kill chain of most of cyberattacks starts at the network perimeter:

- Attackers are not tied to asset lists and official scanned and firewalled infrastructure when targeting an organization.
- When performing reconnaissance, attackers know that the main domains and core infrastructure will be protected. As such, they hunt for weak and overlooked elements of IT to gain access.
- Attacks quickly escalate from simple misconfigurations on forgotten IT and result in catastrophic incidents. In a sample ransomware incident response case, Group-IB team observed a major financial institution fully cryptolocked within 4 hours and 11 minutes of an RDP brute-force attack on an overlooked network segment.

Breaches and leaks: The numbers*

143% spike in RDP access sales

In 2020, the number of offers to sell RDP access to large corporate networks increased 143% year-on-year

1.5 billion+ files publically available

Over 100,000 open databases discovered in less than a year, while 1.5 billion+ files were available online on Amazon S3, rsync, SMB, and FTP servers.

Ransomware target 500 major companies

500 major companies from 45 countries were mentioned in public resources as having their data encrypted and being asked to pay millions in ransom.

Weak perimeters cause 45% of all IR

In 2020, over 45% of all incident response engagements were rooted in perimeter-based vulnerabilities and insecure infrastructure.

* The following statistics and many more can be found in Hi-Tech Crime Trends 2020/2021

Overlooked fundamentals

Weaponized spearphishing emails, targeted drive-by campaigns, and major supply chain attacks all attract cybersecurity research and make for gripping headlines, but they do not reflect the actual bulk of real incidents in the field or the problems Blue teams defend against on a daily basis.

Attackers do not need to use sophisticated methods to achieve their goals, nor do they need to invest in complex tools to conduct attacks. The hype about AI-driven malware describes the distant future. In fact, based on Group-IB research and intelligence with joint operations with INTERPOL, Europol and national law enforcement agencies, we see that in 2021 adversaries can succeed with limited investment or overheads. Attackers often operate using open-source scanners or cracked proprietary tools, use free credentials from mass data breaches, and conduct brute-force and password spraying attacks.

The irony is that organizations do not need sophisticated instruments to enact effective mitigation protocols and take back control of their attack surface. They must simply look at their attack surface from an adversary's point of view (i.e. outside-in) to find and effectively mitigate issues discovered and associated risks.

Why traditional perimeter security solutions fall short

Legacy approaches such as one-off penetration tests, vulnerability scanners, and security risk ratings provide organizations with an understanding of their attack surface, but they do not give the big picture.

Penetration testing, for example, does not provide an asset inventory but rather digs under the attack surface to determine how certain vulnerabilities can be exploited. Moreover, as such assessments are performed periodically (e.g. every six months), they fail to provide relevant, real-time information about security postures.

Despite their name, vulnerability scanners only give a limited view of the attack surface, as they can only scan for known assets to the organization — they cannot discover and inventory exposed assets that are unknown like an attacker — leaving organizations vulnerable to avoidable risks.

Security risk ratings offer a high-level overview of an organization's security posture, but the methods behind the scoring are rarely transparent and do not display the root cause and effective routes for mitigation.

Attack Surface Management fills in the gaps left by traditional risk management methods by continuously scanning, mapping and allocating an organization's assets to their digital footprint. It helps discover previously unknown or forgotten infrastructure, evaluate and prioritize discovered assets with actionable threat intelligence, and map the entire attack surface.

It's time to move on from CVSS

Many organizations have adopted the Common Vulnerability Scoring System (CVSS), a tool designed to assess the severity of vulnerabilities based on a 10-point scale, to prioritize their mitigation protocols. However, information provided by the CVSS is far from sufficient when it comes to performing quality vulnerability management. While CVSS may have once been a helpful tool, technology has far surpassed the system's limited capabilities.

Most notably, it does not give any indication of whether a certain vulnerability will be exploited. Taking into account that only 5.5% of discovered vulnerabilities ever used by threat actors, this seems like a significant oversight.

What is AssetZero?

AssetZero is a comprehensive, intelligence-driven SaaS solution designed to assess and help manage the attack surface. The tool gives full visibility into external-facing assets, identifying those that may be potential attack vectors and streamlining mitigation and remediation efforts through integrations, task-management and an easy to use UI.

Simple yet elegant, AssetZero performs a vital task that can protect any company in any industry from unwanted breaches: from larger corporations that have the widest and least clearly defined attack surfaces (and also the most to lose) through to smaller businesses with limited resources that often struggle to effectively manage or track their IT infrastructure.

GROUP-IB
Select company
Asset Zero
Make data-driven decisions to reduce cyber risk.
Company name
Total score
8.3
+0.2
Dashboard
Companies
Issues
Graph
Settings
Score
All issues
Current issues
5.2 Vulnerabilities
6.7 Dark web mentions
9.9 Leaked Credentials
7.9 Network Security
9.9 Malware Security
8.5 Email Security
9.9 DNS Health
8.2 SSL/TLS Security
Quick filter:
Errors 8
Warnings 13
Passed 2 543
Test date:
09 Jan 2021
John Snow
Discovered assets
48 SSL
301 Domain
79 IP
Graph analytics
Show complex relationships between objects.
Show details on graph
Results for the period
10 Jan 2021 — 7 Feb 2021
Issues found
Errors 432
Warnings 1250
Issues resolved
Errors 32
Warnings 175 +15
Digital foot prints detected automatically
Domains 83 +5
IP 55
Discovered assets map
Your company digital foot print on World Map.

What does Asset Zero do?

Continuously scans for and identifies assets

AssetZero uses information about an organization’s main domain to identify its assets. The system scans the entire IPv4 space, ensuring that no critical asset is overlooked. Collected data includes:

- IP addresses
- Domain names
- SSL/TLS certificates
- Bucket storages
- Public-facing software

Validates and categorizes assets

The system tests every asset associated with your External Attack Surface to determine whether they fall within one of the following eight categories:

- Vulnerabilities
- Network security
- Leaked credentials
- Malware security
- Dark web mentions
- SSL/TLS security
- Email security
- DNS & Domains

Creates alerts and generates risk scores

The system enriches all identified assets and potential issues with rich context from Group-IB Threat Intelligence & Attribution. This allows for effective prioritization beyond CVSS impact scores or “business risk” and helps understand if the vulnerability or attack technique detected is currently being used in the wild. Alerts can have one of three outcomes:

- Error: Critical issue that requires urgent action
- Warning: Potential issue that requires further analysis
- Passed: No issue detected

Facilitates remediation and engagement

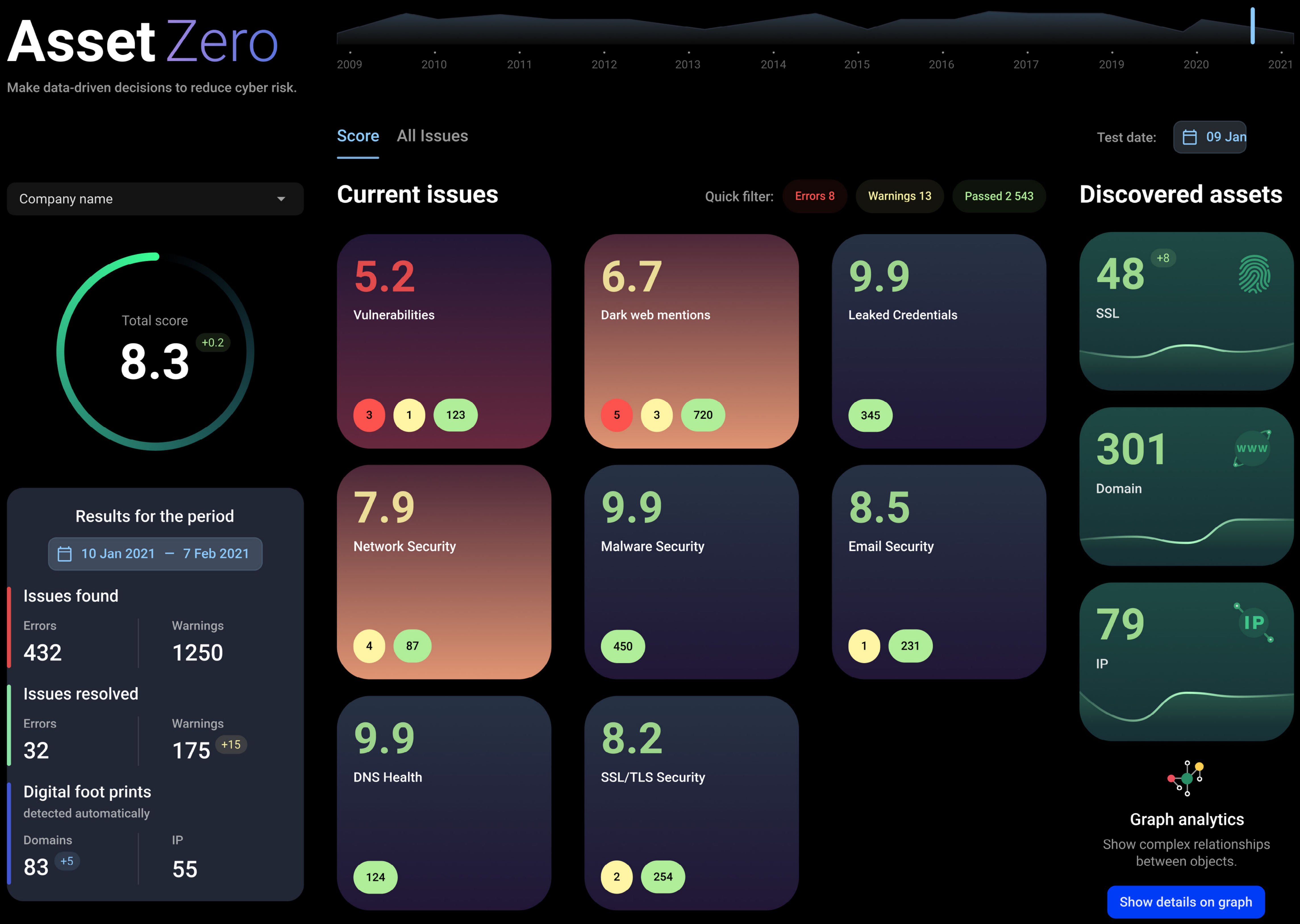
All alerts can be delivered via the UI, via native ticket and alert sharing functions, or via our rich API into integrations with ticketing systems, SIEM, SOAR and other toolsets to allow for effective management and remediation. Alerts are also provided with recommendations on threat type, and recommended mitigation procedures.

Tracks changes and reassesses posture

The system monitors all changes to the External Attack Surface daily to ensure that the company accurately understands their current security posture. Our remediation logic removes solved issues and if any new risks are identified, the system generates a new score and alert.

The Interface

The AssetZero interface is user-friendly and designed to give every customer and service provider the information they need to understand their digital footprint and associated risks.



Asset Zero

Make data-driven decisions to reduce cyber risk.

Score All Issues

Test date: 09 Jan

Company name

Total score
8.3 +0.2

Results for the period

10 Jan 2021 — 7 Feb 2021

Issues found

Errors 432

Warnings 1250

Issues resolved

Errors 32

Warnings 175 +15

Digital foot prints
detected automatically

Domains 83 +5

IP 55

Current issues

Quick filter: Errors 8 Warnings 13 Passed 2 543

5.2 Vulnerabilities
3 1 123

6.7 Dark web mentions
5 3 720

9.9 Leaked Credentials
345

7.9 Network Security
4 87

9.9 Malware Security
450

8.5 Email Security
1 231

9.9 DNS Health
124

8.2 SSL/TLS Security
2 254

Discovered assets

48 +8 SSL

301 Domain

79 IP

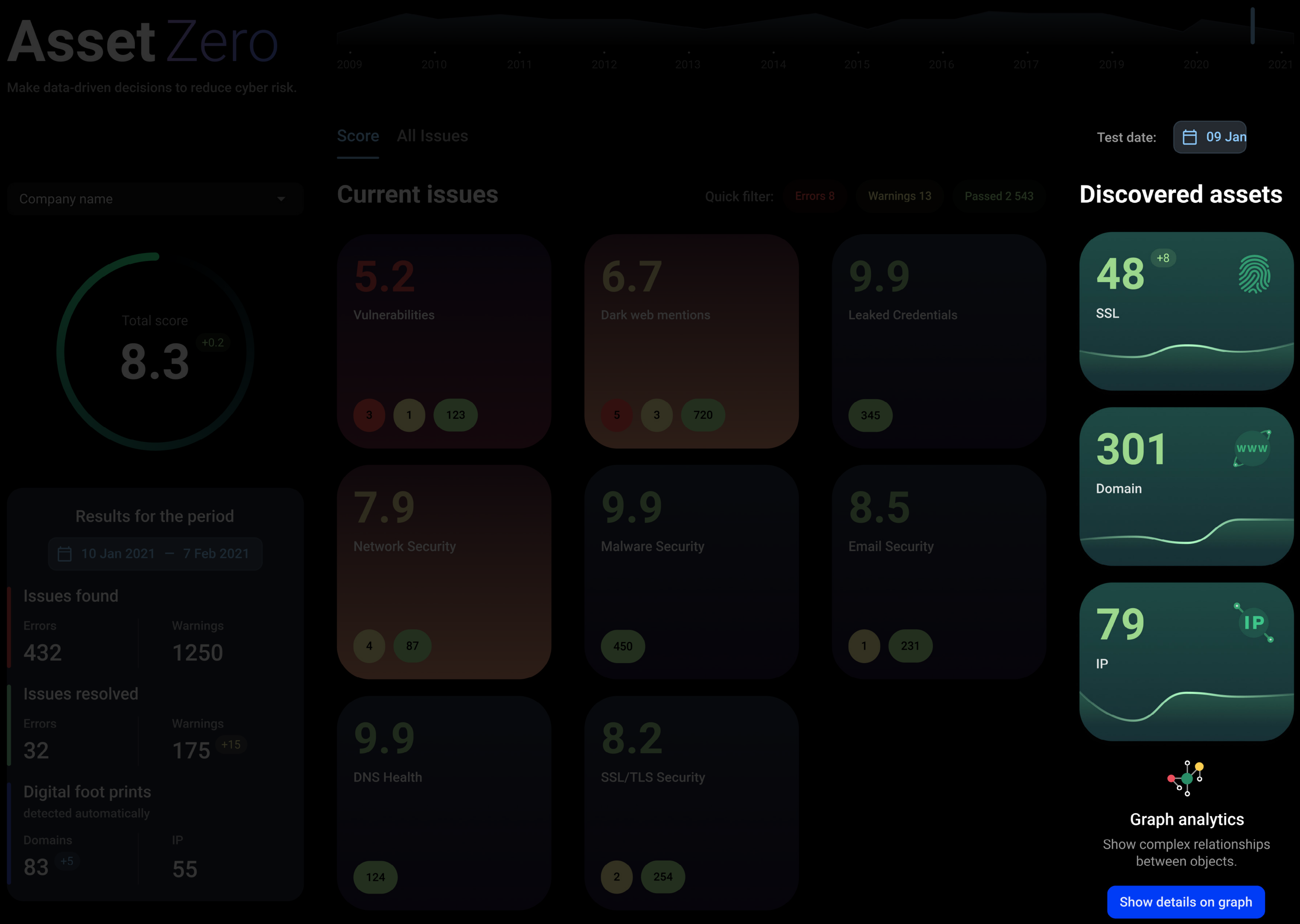
Graph analytics

Show complex relationships between objects.

Show details on graph

Discovered Assets

All assets are sorted under three categories: SSLs, Domains, and IPs. The customer can, at any time, open each category to review every asset and its origin. The asset list is constantly updated to ensure that the customer always has a real-time view of their external attack surface.



Asset Zero

Make data-driven decisions to reduce cyber risk.

Score All Issues

Test date: 09 Jan

Company name

Total score

8.3 +0.2

Results for the period

10 Jan 2021 — 7 Feb 2021

Issues found

Errors 432

Warnings 1250

Issues resolved

Errors 32

Warnings 175 +15

Digital foot prints

detected automatically

Domains 83 +5

IP 55

Current issues

Quick filter: Errors 8 Warnings 13 Passed 2 543

5.2 Vulnerabilities — 3, 1, 123

6.7 Dark web mentions — 5, 3, 720

9.9 Leaked Credentials — 345

7.9 Network Security — 4, 87

9.9 Malware Security — 450

8.5 Email Security — 1, 231

9.9 DNS Health — 124

8.2 SSL/TLS Security — 2, 254

Discovered assets

48 +8 SSL

301 Domain

79 IP

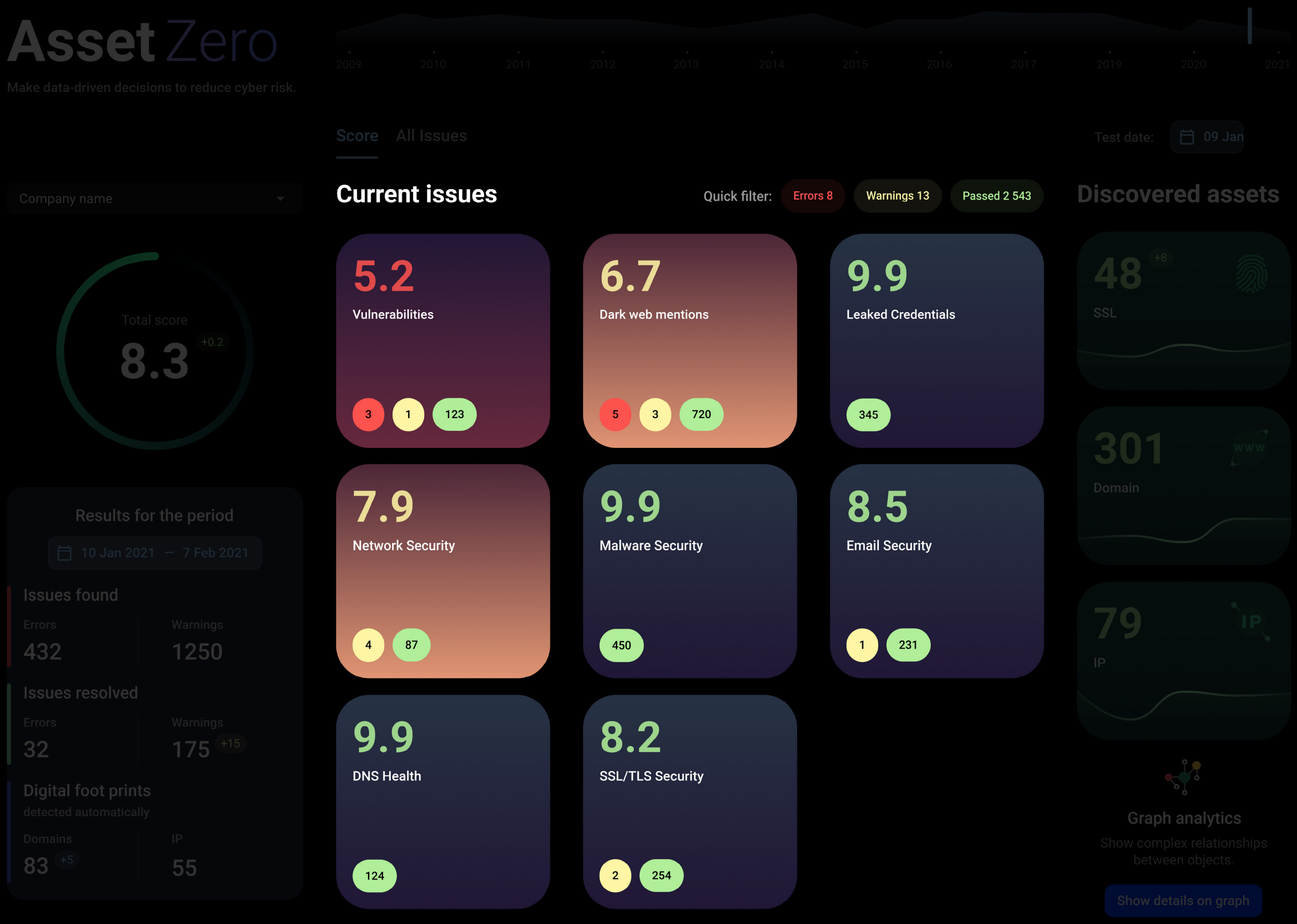
Graph analytics

Show complex relationships between objects.

Show details on graph

Current Issues

Issues (i.e. alerts) are generated based on the discovered assets and categorized depending on vulnerability type. AssetZero provides a frictionless interface for searching for and reviewing detected issues to ensure quick and effective mitigation. For baselining and sectoral comparisons, each category is also given a score of 1 (red) to 10 (green), with 1 representing most risk and 10 meaning minimal risk.



AssetZero

Make data-driven decisions to reduce cyber risk.

2009 2010 2011 2012 2013 2014 2015 2016 2017 2019 2020 2021

Score All Issues

Test date: 09 Jan

Company name

Total score 8.3 +0.2

Results for the period

10 Jan 2021 — 7 Feb 2021

Issues found

Errors 432

Warnings 1250

Issues resolved

Errors 32

Warnings 175 +15

Digital foot prints detected automatically

Domains 83 +5

IP 55

Current issues

Quick filter: Errors 8 Warnings 13 Passed 2 543

5.2 Vulnerabilities — 3, 1, 123

6.7 Dark web mentions — 5, 3, 720

9.9 Leaked Credentials — 345

7.9 Network Security — 4, 87

9.9 Malware Security — 450

8.5 Email Security — 1, 231

9.9 DNS Health — 124

8.2 SSL/TLS Security — 2, 254

Discovered assets

48 +8 SSL

301 Domain

79 IP

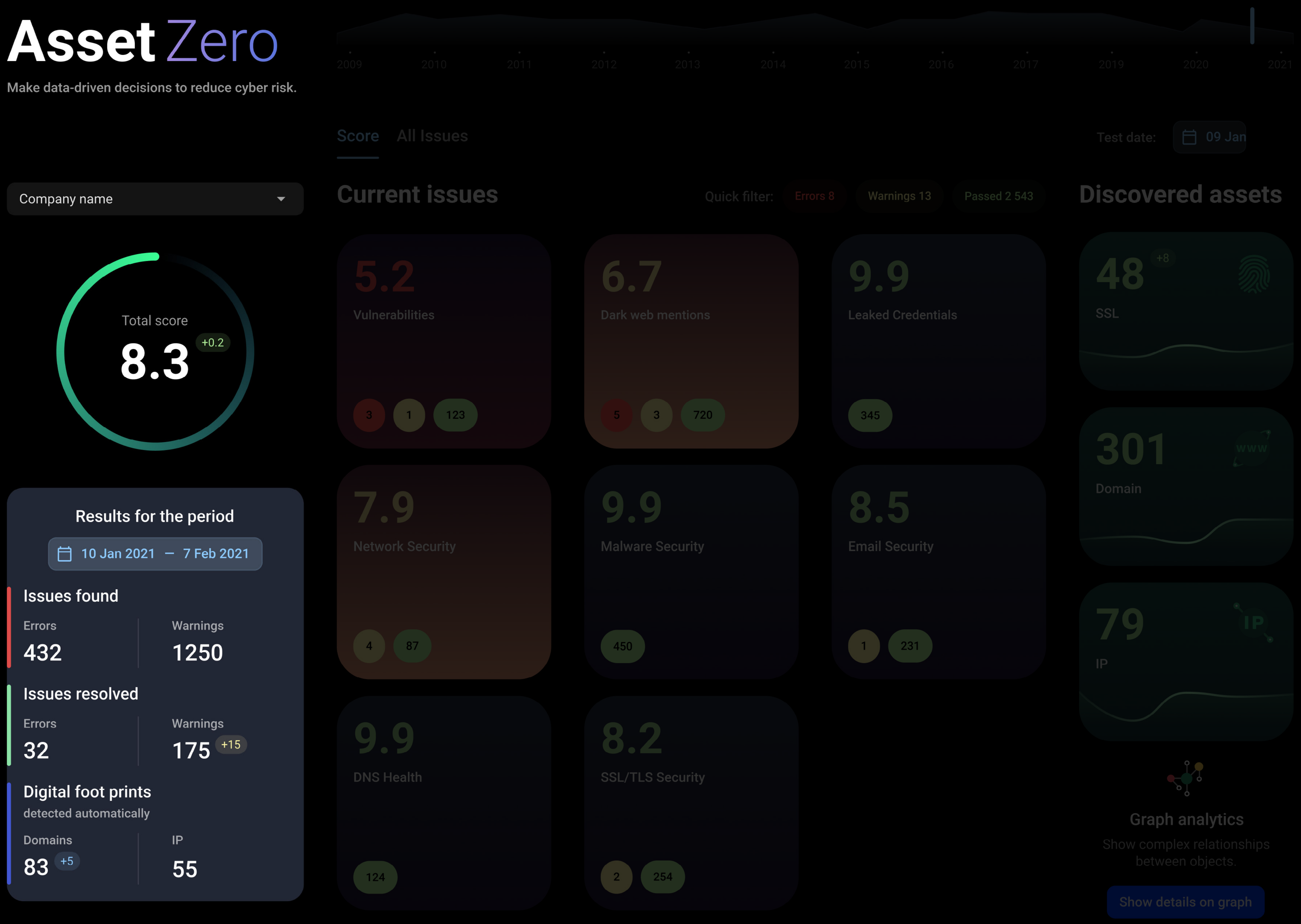
Graph analytics

Show complex relationships between objects.

Show details on graph

Security Baselining

AssetZero also generates a general score for the company and offers historical data so that the customer may track their security posture over time.



Asset Zero

Make data-driven decisions to reduce cyber risk.

Score All Issues

Test date: 09 Jan

Company name ▾

Total score 8.3 +0.2

Results for the period

10 Jan 2021 — 7 Feb 2021

Issues found

Errors	Warnings
432	1250

Issues resolved

Errors	Warnings
32	175 +15

Digital foot prints
detected automatically

Domains	IP
83 +5	55

Current issues

Quick filter: Errors 8 Warnings 13 Passed 2 543

Score	Category	Counts
5.2	Vulnerabilities	3, 1, 123
6.7	Dark web mentions	5, 3, 720
9.9	Leaked Credentials	345
7.9	Network Security	4, 87
9.9	Malware Security	450
8.5	Email Security	1, 231
9.9	DNS Health	124
8.2	SSL/TLS Security	2, 254

Discovered assets

48 +8 SSL

301 Domain

79 IP

Graph analytics

Show complex relationships between objects.

Show details on graph

Issue Category Detail

As described above, AssetZero evaluates a company's security posture based on eight categories. The system automatically determines which category each discovered asset belongs to and assigns individual scores for each category. The score shows the company where it is most vulnerable so that it can prioritize remediation actions.

To learn more about the technologies behind AssetZero, click here →

Vulnerabilities

Based on results of regular scans, detected services, and their versions, AssetZero checks whether the company is at risk of any vulnerabilities or incorrect configurations on operating systems, services, applications, software, and hardware.

The system applies several approaches to detect vulnerabilities:

- During internet scans, AssetZero detects banners and services that are running on the server. It then correlates this information with known vulnerabilities. If there is a match, the system checks whether it is critical and issues a corresponding warning or error (alert).
- AssetZero visits every IP and domain and different paths of the website to detect technologies that are used to create web applications. The system also correlates the information with known vulnerabilities.
- AssetZero checks if the server has open databases, buckets of file storages, open listings of directories, and other potential misconfigurations.

Network security

AssetZero scans the Internet and client subnets to identify open ports, services (together with other versions), and web applications used. Scanning does not involve exploiting vulnerabilities or downloading any content. As such, it is completely safe and does not affect running services. It is also conducted in “stealth mode” to avoid any alerts for the security teams managing this infrastructure.

AssetZero checks open ports of remote administration services (RDP, SSH, VPN, etc), database ports, insecure service headers, open proxy or running Tor nodes, or whether the host has been targeted by a DDoS attack.

Leaked credentials

AssetZero checks whether there are any leaked credentials associated with the assets being monitored. With the help of Group-IB Threat Intelligence & Attribution, AssetZero informs the customer in real-time about targeted data breaches and publicly available data breaches.

Targeted data breaches — These occur when a threat actor actively attempts to steal sensitive data from an organization using malware or phishing attacks. The stolen data is used to conduct even more complex attacks or is resold via the dark web.

Publicly available data breaches — Massive collections of logins and passwords from third-party breaches can affect users of linked organizations.

Dark web mentions

AssetZero automatically maps Threat Intelligence & Attribution data to notifications to identify whether hackers have mentioned any part of the customer's external attack surface on the dark web. The more often a company's infrastructure is mentioned, the more likely that attacks against that company will be attempted or may have already taken place.

To help prepare and assess this threat in detail, AssetZero offers high-level access to underground platforms the purpose of reviewing and classifying the risk and providing the targeted organization with recommended actions.

Malware security

Threat actors leverage network vulnerabilities to deploy phishing content, distribute malware, and embed malicious code into a company's applications and websites. Attackers can also conduct deface attacks. AssetZero leverages data from Group-IB Threat Intelligence & Attribution to check for:

- The output of internal and external sandboxes for interactions between malicious programs and the assets that are a part of your company's external attack surface.
- Web content for phishing or fraudulent websites created automatically by fraudsters on legitimate and highly trusted external attack surface resources
- The presence of malware control and control systems or attack frameworks related to the Discovered Assets and Discovered Assets Map using the Graphing technologies and External Threat Hunting system.
- Web content on website pages, which helps detect injected malicious code and web shells

SSL/TLS security

AssetZero checks for self-signed certificates, up-to-date SSL/TLS versions, and the use of strong encryption algorithms. In addition to obvious issues, a lack of proper configurations can lead to compliance requirements being violated and licenses being revoked. Therefore, these are included into the metrics and alerting.

Other situational risks are also included into review, such as expiration of certifications, to allow for their early remediation.

Email security

SPF and DMARC are used to protect against spam, phishing attacks, and attacks exploiting a company's brand and domains. AssetZero checks to identify whether the recommended configurations are deployed in order to make such attacks less likely. Companies often enable these security settings for main domains only and leave potential risks in their external attack surface by neglecting full compliance across their entire technology stack.

DNS & Domains

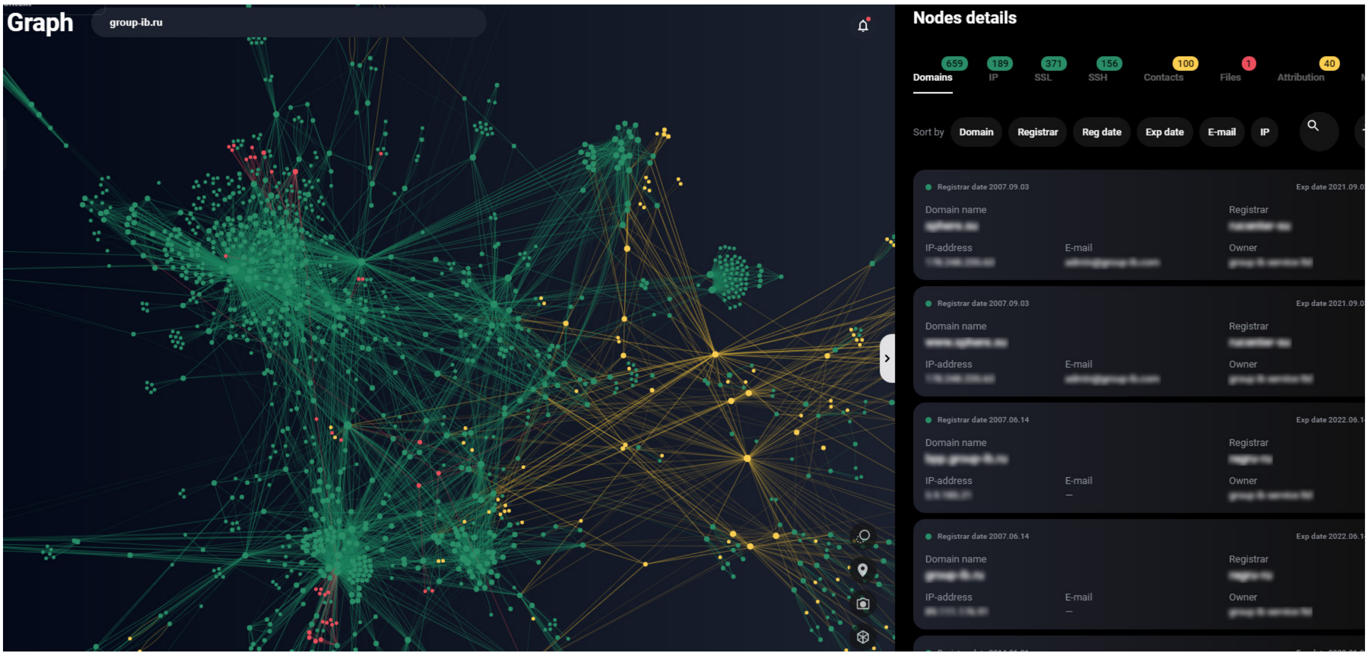
DNS is a critical security component that makes a company's infrastructure resilient. Group-IB checks your infrastructure's DNS settings and DNSSEC to identify potential weaknesses and verify whether the settings meet best practices. Additionally, AssetZero performs validation to identify any domains or related assets that might expire soon and therefore reflect an upcoming risk.

AssetZero goes above and beyond to identify your External Attack Surface

To learn more about how AssetZero can benefit your business, contact us at AssetZero@group-ib.com

It gives context behind the vulnerability. The information provided by AssetZero is constantly enriched with data collected by Group-IB's proprietary intelligence and through its unparalleled global expertise in responding to, mitigating, and investigating cyber threats. This means that AssetZero enriches each security issue with context from today's threat landscape and therefore accurately determines their severity.

It visualizes your security posture through our state-of-the-art Graph. The Graph tool is designed to visualize the customer's attack surface, showcase their external attack surface, and detect existing or potential threats. The toolset offered by the Graph function makes it possible to automatically build map connections between analyzed resources or nodes and other types of objects.



Nodes details

Sort by Domain Registrar Reg date Exp date E-mail IP

Registrar date 2007.09.03 Exp date 2021.09.0
Domain name [redacted] Registrar [redacted]
IP-address [redacted] E-mail [redacted] Owner [redacted]

Registrar date 2007.09.03 Exp date 2021.09.0
Domain name [redacted] Registrar [redacted]
IP-address [redacted] E-mail [redacted] Owner [redacted]

Registrar date 2007.06.14 Exp date 2022.06.1
Domain name [redacted] Registrar [redacted]
IP-address [redacted] E-mail — Owner [redacted]

Registrar date 2007.06.14 Exp date 2022.06.1
Domain name [redacted] Registrar [redacted]
IP-address [redacted] E-mail — Owner [redacted]

It leverages industry-leading CTI to dig deeper for unknown assets. Group-IB Threat Intelligence & Attribution monitors compromised data both in open and private sources, including C&C servers, phishing collection points, and more. TI&A also tracks activity on the dark web and contains one of the largest threat actor databases.

It detects malicious activity. Group-IB offers a comprehensive approach to detecting malicious activity (e.g. phishing, deface attacks, malicious communications, malicious infrastructure) and has unique competencies to identify malicious code embedded in websites.

Innovations powering AssetZero

TECH CATEGORY	TECHNOLOGY NAME	DESCRIPTION
Asset identification	Internet snapshot generator	To fingerprint the Internet we use our network of distributed network scanners to detect open ports, banners, services, software and versions and combine this information with whois, dns and ssl certificates data. This gives us historical and regularly updated snapshots about the state of the Internet. PATENTED
	Web snapshot generator	We collect suspicious URLs from many different sources and then open an URL in a real browser to download all text, images, and cookie scripts, after which we execute the scripts. We detect web technologies, software versions and vulnerabilities. We then store this significant amount of data and index to make it searchable. This allows us to hunt for phishing, C2 panels, infected websites, and hosts used in watering hole or drive-by attacks, as well as potential risks on your perimeter such as JavaScript sniffers or unsolicited changes to your web infrastructure.
	Network Graph analysis	We use Internet & Web snapshot generators to create an entire graph of the internet with all historical changes. This Graph is enriched with information about malware, phishing, C2 servers, and threat actors. Special storage algorithms help us build interactive graphs quickly, while proprietary refined logic provides the maximum relevant results. PATENTED
Malware & Phishing, DDoS detection	Malware detonation platform	THF Polygon is our proprietary malware detonation platform designed to execute suspicious files in isolated environments. This allows us to identify more C2 traffic and associated malware within customer infrastructure. PATENTED

TECH CATEGORY	TECHNOLOGY NAME	DESCRIPTION
Malware & Phishing, DDoS detection	Malware Config extractor	Extracts configuration files from malware samples and C2 servers that makes it possible to track malware families and threat actors and how they interact with IT infrastructure.
	Malware protocol emulator	The malware protocol emulator emulates the communication protocol of an infected device with its C2 server, which means that we can track commands, plugins, and configurations. PATENTED
	Phishing Detector	To detect URL-based phishing attacks, we open an URL in a real browser. Using OCR we compare login forms, logos, and other images from the page and compare it with legitimate websites belonging to the targeted brands. In addition, Phishing Detector generates static signatures based on image comparison, hashing of elements on the page, and regular expression. PATENTED
	Phishing Predictor	We use this to predict where the next phishing site, web shell, or phishing kit can be located to detect it. To do so, we need to predict both the host address and the URL path. We analyze newly registered domains and SSL certificates exploiting popular brands, vulnerable hosts, and hosts known to be compromised. To predict the right URL path system, it is necessary to check the most popular paths and the paths specific to the threat actor. PATENTED
	External Threat Hunting system	We combine historic internet fingerprinting data with knowledge about malicious infrastructure that helps us detect patterns relevant to specific malware families and threat actors who organize their infrastructure according to their habits or instructions. Detected similarities are then converted to infrastructure detection rules and every time new servers are activated we can detect it. This means that AssetZero can offer additional insights into exposure to new incidents and malware being hosted on their perimeter. PATENTED

TECH CATEGORY	TECHNOLOGY NAME	DESCRIPTION
Compromised data detection	Botnet data extractor	Proprietary technology Bot-trek (™) detects malware gateways and administration panels. It also extracts details about compromised data based on knowledge of malware communication protocols. This helps us determine whether your organization has been infected based on your assets detected by AssetZero. PATENTED
Darkweb analysis	Darkweb Scraping engine	Hackers apply many techniques to avoid their illicit marketplaces and hacking forums being scraped. Reapercollects data from such sources automatically in real time and identifies relevant threats. Using machine learning we identify message categories to filter out the most interesting content from millions of messages and determine reliability and credibility without human bias.
Vulnerability & exploit detection	Vulnerability Detector	Based on results of regular scans, detected services, and their versions, Vulnerability Detector checks for vulnerabilities or incorrect configurations on operating systems, services, applications, software, and hardware.

Group-IB is a global leader in high-fidelity Threat Hunting and Intelligence, best-in-class fraud prevention solutions, and high-profile cyber investigations.

INTERPOL AND EUROPOL

Partner and active collaborator in global investigations

OSCE

Recommended by the OSCE as a cybersecurity solutions provider

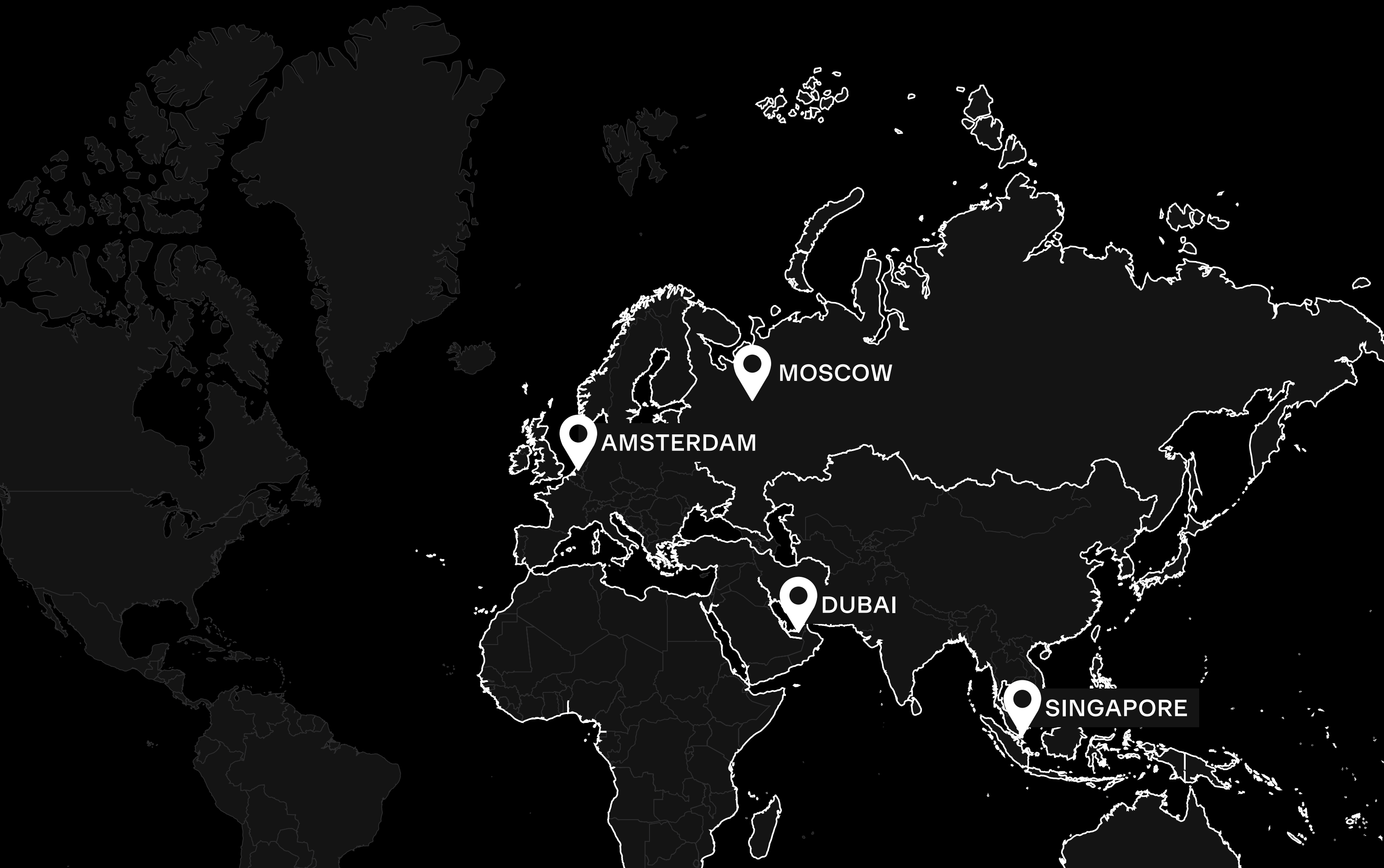
APAC TOP 10

Ranked among the Top 10 cybersecurity companies in the APAC region according to APAC CIO Outlook

Group-IB Threat Intelligence and Research Centers

- Europe
- Russia
- Middle East
- Asia-Pacific

- Globally distributed cybercrime monitoring infrastructure
- Digital Forensics & Malware Analysis Laboratory
- High-Tech Crime Investigations
- CERT-GIB: 24/7 monitoring centers and Computer Emergency Response Team



Group-IB’s technologies and innovations

Group-IB’s experience in performing successful global investigations with state-of-the-art threat intelligence and detecting cybercriminals at every stage of attack preparation has been fused into an ecosystem of highly sophisticated software and hardware solutions designed to monitor, identify, and prevent cyber threats.

Our mission is to protect our clients in cyberspace at all costs using innovative technologies and services.

Group-IB’s technologies are recognized by the world’s leading research companies:

— Innovation Excellence
— Product Leader
— Innovation Leader

IDC

Gartner

FORRESTER

kuppingercole ANALYSTS

FROST & SULLIVAN

GARTNER IDC

FROST & SULLIVAN

FORRESTER

Threat Intelligence & Attribution

System for analyzing and attributing cyberattacks, threat hunting, and protecting network infrastructure based on data relating to adversary tactics, tools, and activity

KUPPINGERCOLE ANALYSTS AG

Threat Hunting Framework

Adversary-centric detection of targeted attacks and unknown threats for IT and OT environments

FROST & SULLIVAN

Digital Risk Protection

AI-driven platform for digital risk identification and mitigation

KUPPINGERCOLE ANALYSTS AG

FORRESTER

GARTNER

Fraud Hunting Platform

Client-side digital identity protection and fraud prevention in real time

NEW

Atmosphere: Cloud Email Protection

Patented email security technology that blocks, detonates and hunts for the most advanced email threats

550+	70,000+	1,300+	18 years
world-class experts	hours of incident response	successful investigations worldwide	practical experience

Intelligence-driven services

FORRESTER

GARTNER

Group-IB’s technological leadership and R&D capabilities are built on the company’s 18 years of hands-on experience in performing successful cybercrime investigations worldwide and the 70,000 hours of cybersecurity incident response accumulated in our leading forensic laboratory and CERT-GIB.

HI-TECH CRIME INVESTIGATIONS

Digital Forensics

Malware Analysis

Group-IB investigates

- High-tech crimes
- Data leaks
- Corporate and financial crimes
- Sophisticated attacks against critical infrastructure

SECURITY AND COMPLIANCE ASSESSMENTS

- Penetration Testing
- Source code analysis
- Compromise Assessment
- Red Teaming engagements
- Incident Response Readiness Assessment
- Compliance Auditing

THREAT HUNTING AND INCIDENT RESPONSE

- CERT-GIB: 24/7 incident response center
- Proactive threat hunting
- On-prem incident response for complex attacks
- Investigation subscription

CYBER EDUCATION CENTER

Technical courses

- Incident Response
- Malware analysis
- Threat Hunting and more

Non-technical workshops

- Digital hygiene
- Personal cybersecurity
- Reputation management and more

Workshops and masterclasses for university and high school students