

VULNERABILITIES

Automate Your Next Assessment



Clarity on security vulnerabilities is now at your fingertips.

While zero-day vulnerabilities are concerning, they are rarely the primary cause of security breaches. Instead, exposures often arise from unintended backdoors created by changes within the organisation. These exposures can result from various factors, including mergers and acquisitions, IT projects, configuration adjustments, and personnel changes.

Gartner has ranked "Continuous Exposure Monitoring" as a top 5 priority for security leaders in 2024.

Continuous monitoring of vulnerabilities helps you stay one step ahead of adversaries, preventing them from exploiting potential weaknesses.

MyCISO **VULNERABILITIES** automatically scans 219 internet-facing data points to identify gaps and provide insights to help reduce your exposures.

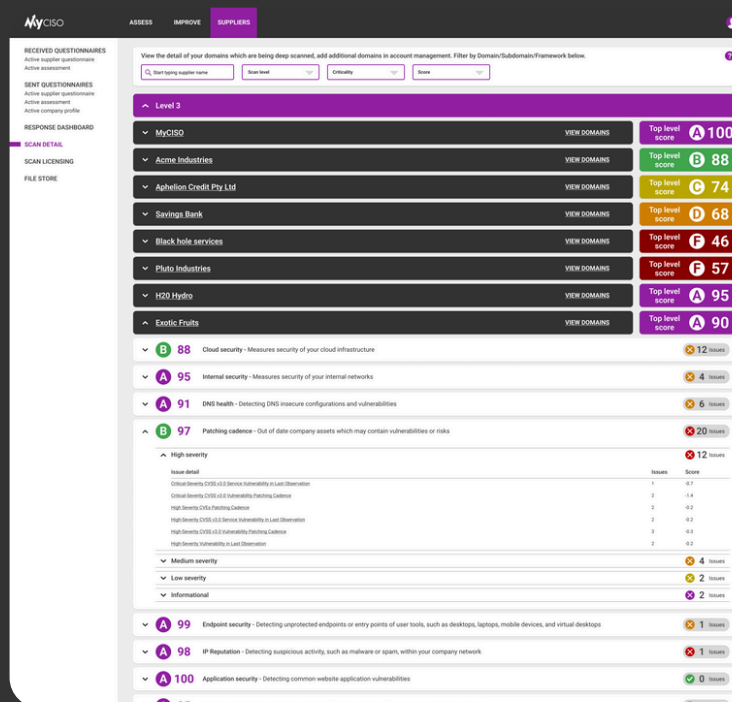
SIMPLE 3 STEP PROCESS

1 Scan
Add the company domain(s) for scanning



2 Review
View the detail of scanned domains in the platform

3 Remediate
Prioritise and remediate the vulnerabilities found



3 SCAN TYPES TO SUIT YOUR NEEDS

Whether you're managing business units, subsidiaries, or third-party suppliers, **VULNERABILITIES** offers three scan depths to deliver only the data you need, without the overwhelm. No matter the scan depth chosen, all 219 data points are analysed, with results presented in one of three tailored formats.

LEVEL 1

Level 1			
Diamond Hands	VIEW DOMAINS	Top level score	B 86
Globex Corporation	VIEW DOMAINS	Top level score	A 91

Returns a high-level A-F score for each asset scanned. This is particularly useful for lower criticality assets or third parties, where assurance is needed, but detailed answers not essential.

LEVEL 2

Level 2			
Yamamoto	VIEW DOMAINS	Top level score	B 83
C 76	Application Security - Detecting common website application vulnerabilities		
A 100	Cubit Score - Proprietary algorithms checking for implementation of common security best practices		
B 88	DNS Health - Detecting DNS insecure configurations and vulnerabilities		

The Level 2 scan delivers an overall score along with a detailed breakdown of 10 core security factors (e.g., Application Security), each graded from A to F. If any area raises concern, you can easily upgrade to a Level 3 scan for deeper insights on that asset.

LEVEL 3

Level 3			
Alpha Data Solutions	VIEW DOMAINS	Top level score	B 85
B 80	Application Security - Detecting common website application vulnerabilities		
		16 Issues	
High Severity		1 Issues	
Issue detail		Issues	
Site does not enforce HTTPS		11	
Medium Severity		4 Issues	
Low Severity		4 Issues	
Informational		7 Issues	

The final and most comprehensive scan level provides in-depth issue lists, organised within five "Issue Detail" accordions for easy investigation.

Each issue is clearly labelled and clicking on it opens a detailed modal with granular detail and context about where the issue was found, to aid with remediation.



AUTOMATE YOUR ESSENTIAL 8, ISO 27001 OR NIST ASSESSMENTS

On completion of the scan, answers to 107 security controls are pre-filled, streamlining your security assessment across more than 20 different security frameworks. You can choose to accept or override the suggested answer based on your additional knowledge and context.

Do you continuously monitor inbound and outbound communications traffic for unusual or unauthorised activities or conditions?			
Control name - Inbound & Outbound Communications Traffic			
0	No evidence that this capability exists	2 Vulnerability scan	Traffic monitoring mechanisms are deployed but some gaps still exist, requiring further uplift for comprehensive coverage
1	Continuous monitoring of inbound and outbound communications traffic is informally applied, lacking formal oversight and consistent detection of unusual or unauthorised activities or conditions	3	There is continuous monitoring of inbound and outbound communications traffic to identify unusual or unauthorised activities

REVIEW, UPGRADE AND DOWNGRADE IN ONE-VIEW

Supplier	Criticality	Certified	Framework	Maturity Score	Primary Domain	Attached Domains	Score	Scan
Rose Tinted Glasses	High	No	Suppliers - High	0 %	fedex.com	551	B 89	Level 3
Yamamoto	Medium	No	MyCISO Intermediate	0 %	lexisnexis.com	2199	B 83	Level 2
The Showroom	Low	No	MyCISO Getting Started	32 %	walmart.com	3226	A 91	Level 1
Globex Corporation	High	No	NIST CSF v1.1	70 %	concur.com	1554	A 91	Level 1
Vivid Design	Low	No	MyCISO Getting Started	0 %	deloitte.com	3907	A 91	Level 1
B2 Software	Medium	No	MyCISO Intermediate	0 %	cloudflare.com	7224	A 92	Level 2
Alpha Data Solutions	High	No	NIST CSF v1.1	40 %	smartsheet.com	672	B 85	Level 3
Centric Software Technology	Medium	Yes	Certified	60 %	infosys.com	1355	A 92	Level 2
Diamond Hands	Low	No	MyCISO Getting Started	41 %	broadridge.com	3452	B 86	Level 1
Finance Dynamics	Low	No	MyCISO Getting Started	0 %	tenable.com	252	A 93	Level 1

Say goodbye to onerous license management. MyCISO makes it simple to review your results at a glance and self-service upgrading or downgrading scans.

In the same interface access insights such as the supplier security assessment results, offering a true single-pane-of-glass view of your supplier risk.