PRODUCT SHEET

CyTrusted

Automated shield & simplified remediation

NextGen Third-Party Cyber Risk Management (TPCRM)

/ 24/7 automated vulnerabilities tests of all your 3rd Parties

/ Executable prioritized remediation advices

/ Tracks corrective actions until positive test

/ Compliance management

November 2025 /

CyTrusted

Automated shield & simplified remediation

The problem we solve

Fragmented view of Internet-facing assets and third-parties

Too many findings, not enough prioritization

Manual chasing of suppliers and internal teams

** Insider Risk Index 2025*

How exposed are you through third parties?

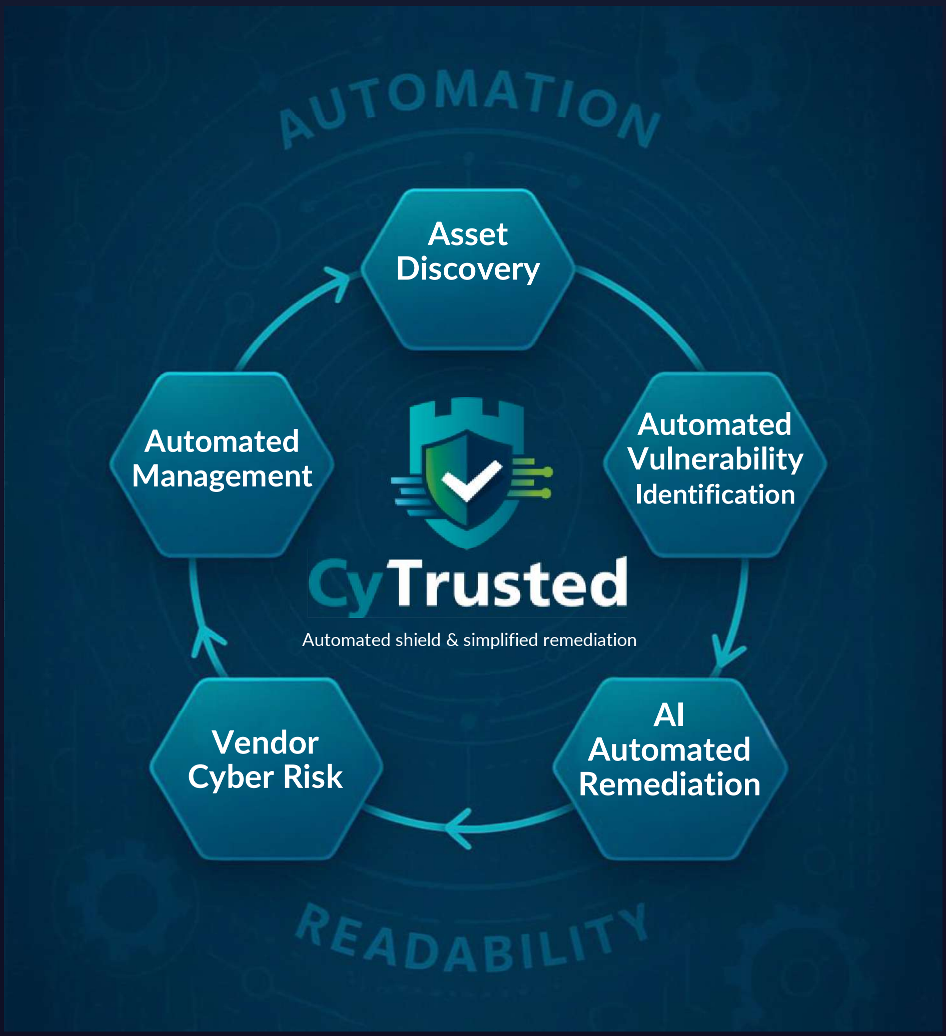
60%
of data breaches originate with third-party*

98 days
to detect a Third-party intrusion*

$4.9 million
cost per third-party breach*

CyTrusted
Automated shield & simplified remediation

CyTrusted in one view



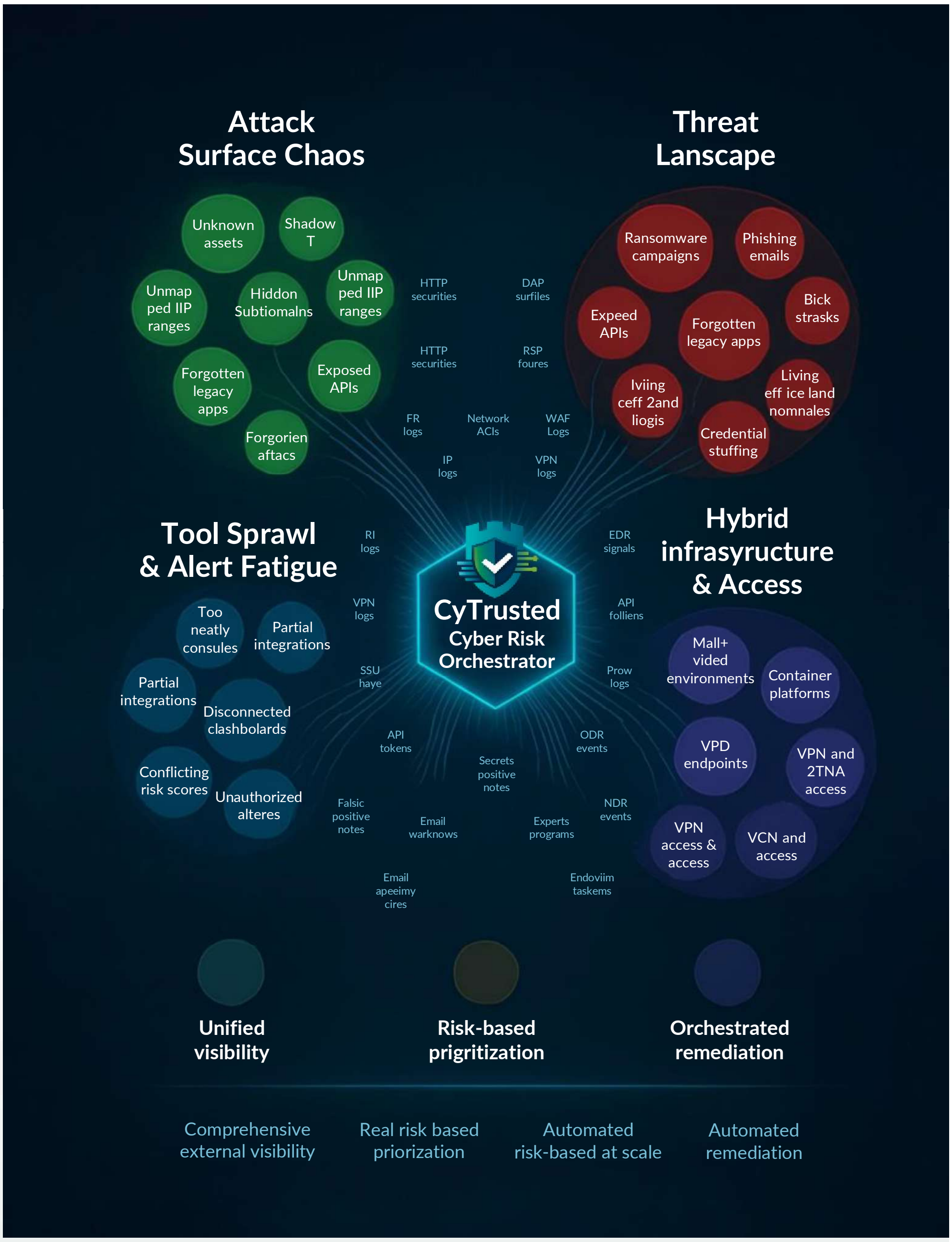
- ✓ Fully **automated** Attack Surface Discovery (**EASM**) for **ALL** your **Third Parties Vendors**
- ✓ Risk-based Vulnerability Assessment with automated checks.
- ✓ Orchestrated and executable remediations across internal teams and third parties.
- ✓ Built-in compliance automated reporting
(ISO 27001, NIS2, DORA, SOC 2, PCI DSS, CIS).

Assets discovery

EASM Attack Surface Discovery : we automate & execute vulnerabilities tests of 100% of your third party vendors

Identify domains, IPs, services, certificates, exposed applications

Aggregate public signals



Continuous drift detection for new or changed internet-facing assets

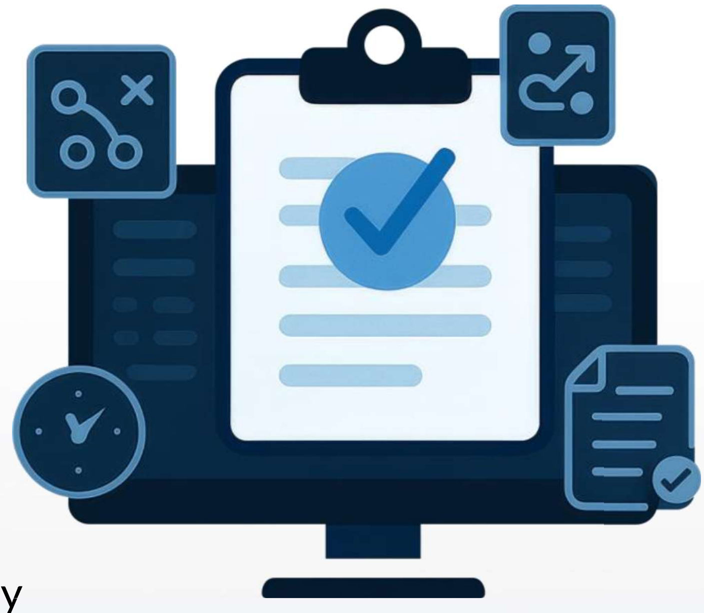
Vulnerability Tests

Automated, systematic, safe, risked-base coverage without disrupting the business

- ✓ **No intrusive cheks,** no business interruption
- ✓ **Safe active test** for depeer coverage where allowed
- ✓ **CVE/CWE inventory** and configuration weaknesses (TLS, headers, open indexes)
- ✓ **Detection of expiring certificates,** public leaks, CMS/plugins exposus
- ✓ **Scheduled re-tests to verify remediation and track progress**

Orchestrated & Executable Remediations

Prescriptive playbooks and clear asset ownership for each finding



Atomatic ticket creation in Jira, Service Now, GitHub/GitLab Issues

Due dates, temporary exceptions and validation steps embedded

Full history, evidence of fixes, and before/after comparisons

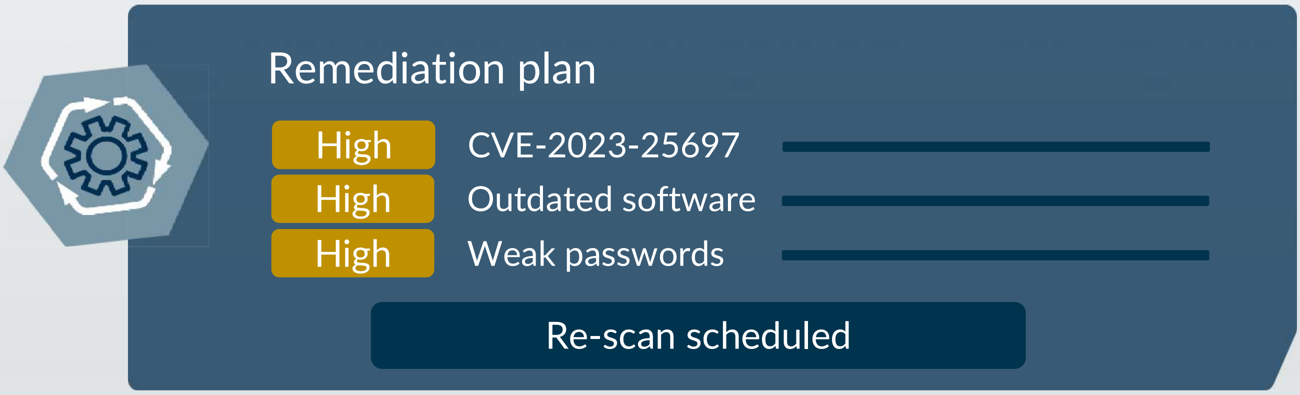
CyTrusted
Automated shield & simplified remediation

Third-party Cyber-Risk

Third-Party cyber-risks management automated, exhaustive, reliable

Vulnerabillities

- **24/7** automated vulnerability scanning of all third parties in scope
- **Executable remediation plans** generated and sent to vulnerable suppliers
- **Automated chasing** of suppliers until vulnerabilities are solved
- **Re-Scan after each fix attempt** and continued follow-up if needed
- **Compliance-ready reports and summarized 3rd party cyber-risk inputs for DORA , NIS2 ISO 27001**



Remediation plan

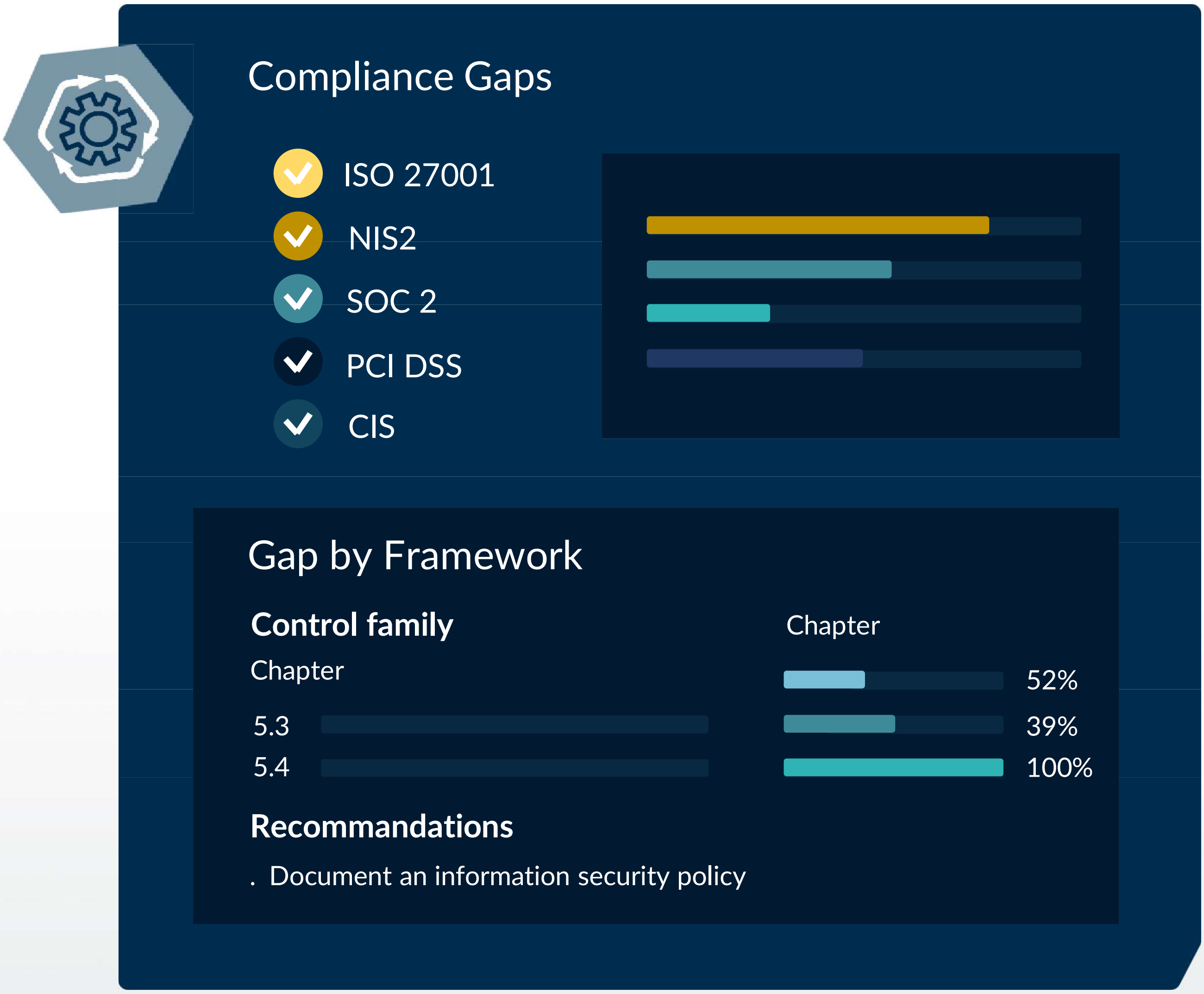
High	CVE-2023-25697
High	Outdated software
High	Weak passwords

Re-scan scheduled

CyTrusted
Automated shield & simplified remediation

Compliance Management

Compliance-ready reports and summarized 3rd party cyber-risk inputs for DORA, NIS2, ISO 27001



Compliance Gaps

- ✓ ISO 27001
- ✓ NIS2
- ✓ SOC 2
- ✓ PCI DSS
- ✓ CIS

Gap by Framework

Control family

Chapter

5.3

5.4

Chapter

52%

39%

100%

Recommandations

. Document an information security policy

- **Findings mapped to** ISO 27001, NIS2, SOC2, PCI DSS, CIS Controls
- **Visual gaps views per** framework, chapter, and control family
- Coverage metrics and **progress tracking over time**
- **Actionable recommendations** aligned with each requirement