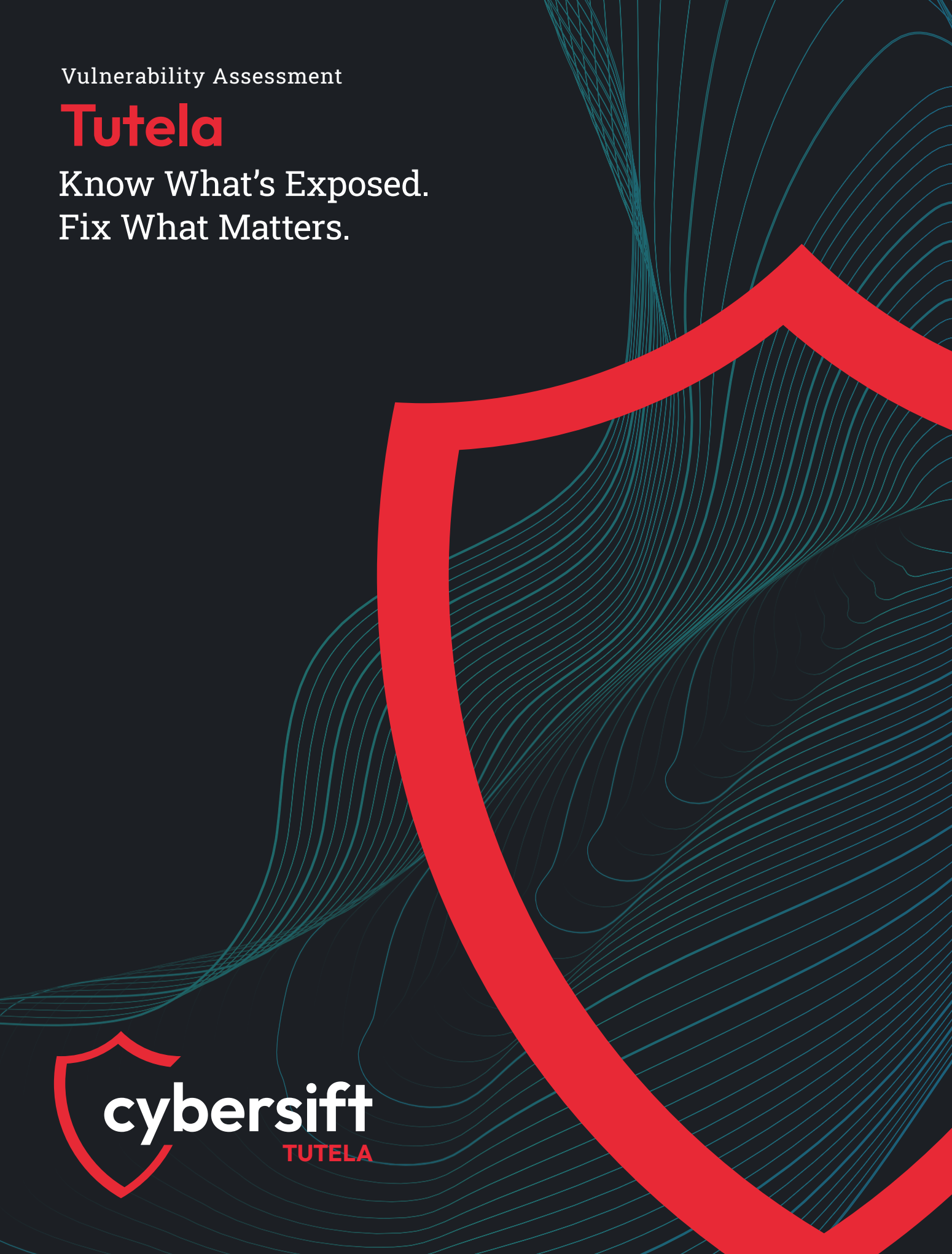
Vulnerability Assessment

Tutela

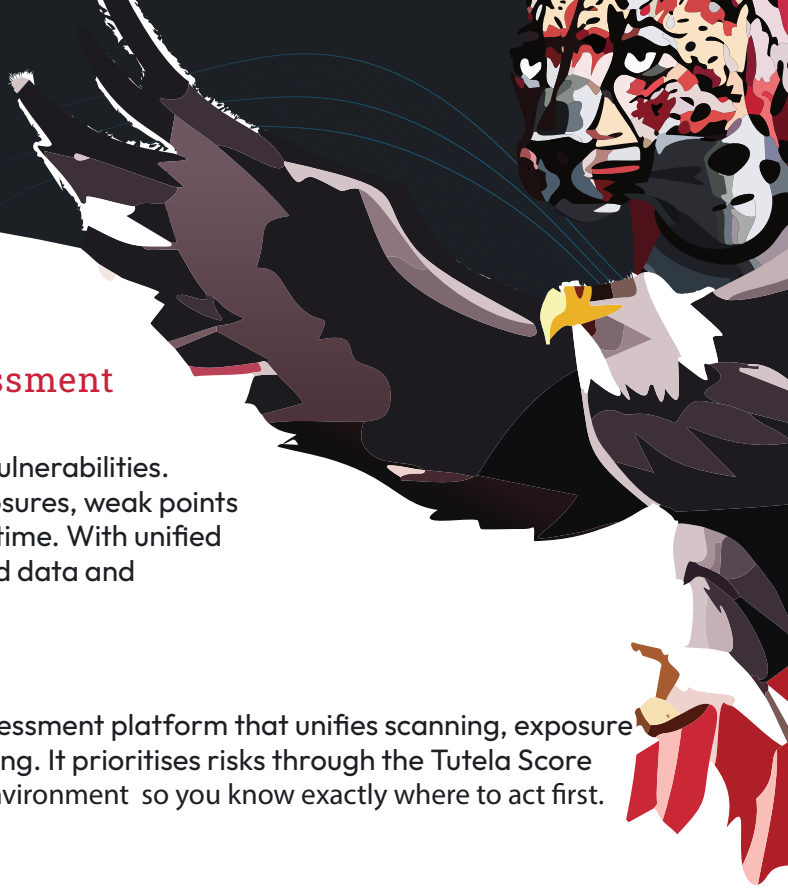
Know What's Exposed.
Fix What Matters.



cybersift

TUTELA

cybersift | VULNERABILITY ASSESSMENT



Tutela sees what others miss

The most complete vulnerability assessment platform - Evolved for real visibility

Traditional vulnerability scanners show you a list of vulnerabilities. Tutela shows you what truly matters - the leaks, exposures, weak points and signals that impact your security posture in real time. With unified visibility across assets, phishing infrastructure, leaked data and compliance gaps, Tutela gives you clarity, not noise.

What is Tutela

Tutela is CyberSift's comprehEnsive vulnerability assessment platform that unifies scanning, exposure detection, compliance checks and real-time monitoring. It prioritises risks through the Tutela Score and provides continuous visibility across your entire environment so you know exactly where to act first.

Why Tutela

Traditional scanners list weaknesses. Tutela reveals the full picture.

Know which vulnerabilities matter, detect leaks and phishing attempts early, and stay continuously aligned with compliance - all in one intelligent platform.

Key characteristics

Unified Visibility:

See every asset, service and exposure through one intelligent platform.

Precision-Driven Prioritisation:

Focus on what truly matters with CVSS, EPSS and the proprietary Tutela Score.

Continuous Threat & Compliance Monitoring:

Detect new services, leaks, phishing infra and compliance gaps in real time.

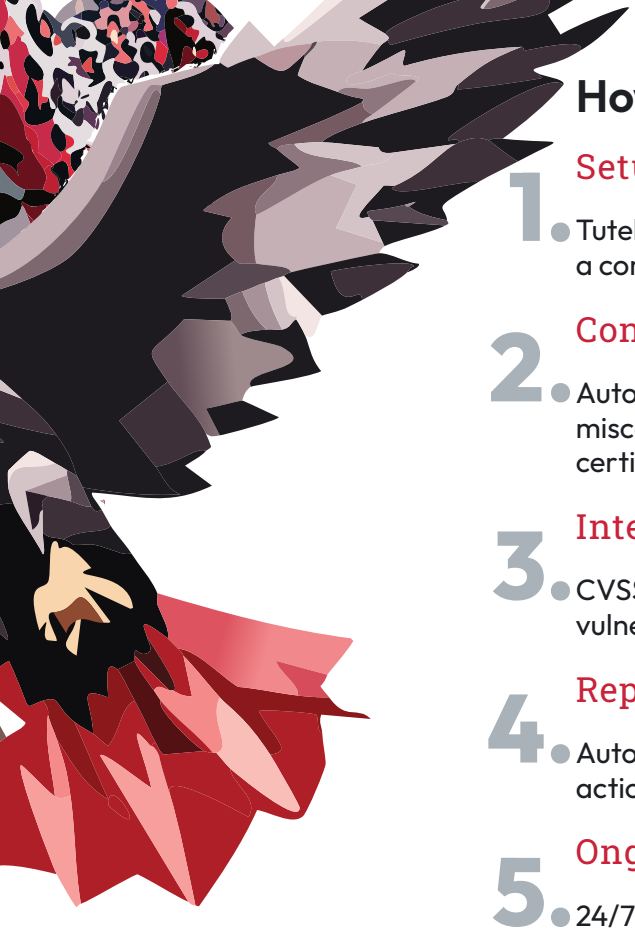
Automated, Actionable Insights:

Get audit-ready reports and clear remediation guidance without the noise.

Tutela VA vs Traditional VA

1. Delivers context - rich insights using the Tutela Score (CVSS + EPSS).
2. Provides 24/7 monitoring across assets, exposures and new services.
3. Detects phishing domains, data leaks and TLS certificate risks.
4. Prioritises vulnerabilities by exploit likelihood and impact.
5. Offers full visibility - asset & software inventory.
6. Generates reports - automated & clear, for fast informed remediation.

1. Provide long CVE lists with little context.
2. Run periodic scans with no continuous monitoring.
3. No visibility into phishing, leaked data or certificate issues.
4. Prioritisation relies mainly on CVSS.
5. Limited asset/software visibility and shadow IT detection.
6. Reports are generic and time-consuming to interpret.



How Tutela works

1. Setup & Asset Discovery

Tutela identifies your assets, services and software to build a complete visibility baseline.

2. Continuous Vulnerability & Exposure Scanning

Automated scans detect vulnerabilities, new services, misconfigurations, phishing infrastructure, leaked data and certificate risks in real time.

3. Intelligent Prioritisation with the Tutela Score

CVSS, EPSS and contextual intelligence combine to highlight the vulnerabilities that truly matter.

4. Reporting & Remediation Guidance

Automated, audit-ready reports deliver clear recommended actions and full remediation tracking.

5. Ongoing Visibility & SOC Alignment

24/7 monitoring ensures your environment stays protected, with optional SOC escalation for deeper detection support.

Deliverables

Vulnerability Assessment Reports

Clear, prioritised reports highlighting the vulnerabilities that matter most.

Tutela Score Breakdown

Combined CVSS, EPSS and context scoring to support informed decision-making.

Asset & Software Inventory

Exportable visibility of all hardware, software and cloud assets.

Exposure & Leak Alerts

Real-time notifications for phishing domains, leaked data and certificate risks.

Compliance Status Summary

Instant insights into ISO/CIS checks with pass/fail details.

Remediation Tracking (Tags)

A simple lifecycle system to track “Pending”, “Resolved” and real-world remediation states.

Book a demo

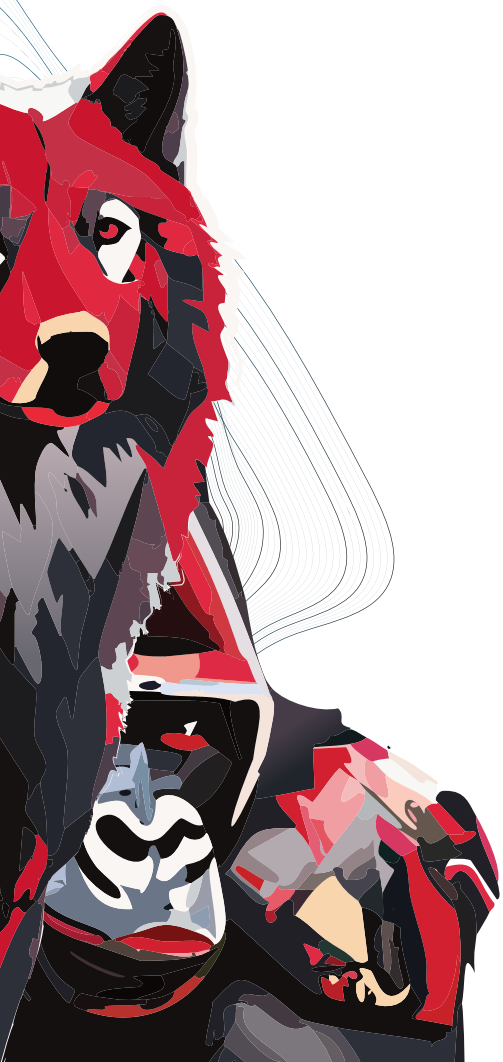
www.cybersift.com/demo

Contact us

info@cybersift.io

+356 7949 8471 (MT)

+44 20 8638 0550 (UK)



Core capabilities

1. Vulnerability Management

Identify and assess vulnerabilities across your environment with unified scanning and meaningful prioritisation.

2. Phishing & Domain Impersonation Detection

Spot malicious domains, phishing attempts and impersonation infrastructure early — across surface and dark web.

3. Data Leak Monitoring

Detect leaked credentials, sensitive information and exposure patterns affecting your organisation.

4. Asset & Software Inventory

Get complete visibility of all devices, software versions, cloud assets and shadow IT from a single platform.

5. Compliance & Configuration Checks

Monitor ISO/CIS checks, certificate issues and misconfigurations in real time to support audit readiness.

6. Cloud & Container Visibility

Track cloud workloads, VMs, agents and Kubernetes security insights across multi-cloud environments.

7. Endpoint Control with Porta

Oversee browser activity, URL access, DLP triggers and user behaviour patterns for enhanced endpoint defence.

Clarity protects. Precision wins.

Tutela reveals your real exposure, prioritises the risks that matter and keeps your environment visible at all times, so your team can act with confidence, not guesswork.

→ Talk to Our Team

→ Get a Guided Walkthrough

Protection Through Collective Intelligence

At Cybersift, we believe cybersecurity should be intelligent, accessible, and built to empower everyone.

Born from a fusion of research and real-world expertise, we transform advanced AI into clear, strategic protection - enabling every organization to stay secure and resilient.

Guided by our vision to make cybersecurity accessible to everyone and to serve as a protector for the unprepared, we stand as a trusted partner in a world where digital threats evolve faster than awareness.

We don't just protect systems - we protect confidence, continuity, and growth.

Protection, at its core, is not about standing alone - it's about standing together. Like in nature, where every instinct contributes to survival, our technology learns, adapts, and protects as one.