STRAITUM

Before You Share Any Data

You have four options for the demo. All are fine — choose whichever makes you comfortable. No data leaves your control without your explicit written consent.

1

Real data, with NDA

The fastest path to a meaningful demo. We sign a mutual NDA before you send anything — simply reply to your confirmation email to request it and I'll have it back within the hour.

Your data is used only for the demo session and deleted immediately after, unless you request otherwise in writing.

2

Anonymize first

Replace hostnames with **SERVER-01**, **SERVER-02** style names and IP addresses with **10.x.x.x** ranges before exporting.

All CVE IDs, CVSS scores, and severity ratings remain intact — the demo is just as useful. Takes roughly **10 minutes** using find-and-replace in Excel or a text editor. See the export guide on page 2 for step-by-step instructions.

3

Mock data

Prefer not to share anything at all? No problem. I'll bring a realistic sample dataset pre-sized to your environment (under 100, 100–500, 500–2,000, or 2,000+ assets).

You'll see exactly how Straitum processes, scores, and surfaces risk — just with placeholder asset names and synthetic CVE data.

4

Live import during the demo

You control the file. You share your screen, drag the export into the importer, and we walk through the results together in real time.

Nothing is stored on our servers after the session without your explicit written consent. This option requires no NDA and no advance preparation.

Questions before the demo? Email us at hello@straitum.com and we'll reply within one business day.

STRAITUM

Export Instructions

Step-by-step guide for exporting vulnerability and asset data from the most common security tools.
All exports should be in **CSV format** where possible — Straitum also accepts XML and JSON for tools that don't support CSV.

Tenable Nessus `CSV`

1. Log in to **Nessus Professional** or **Tenable.sc**.
2. Navigate to **Scans** and open the scan you want to export.
3. Click the **Export** button (top-right) and select **CSV**.
4. Ensure **All Vulnerabilities** is selected, not just new findings.
5. Include: Plugin ID, CVE, CVSS, Risk, Host, Protocol, Port, Name, Synopsis, Description, Solution.
6. Save as `nessus-export.csv`.

Tip: In Tenable.io go to Dashboards → Vulnerabilities → Export → CSV.

Qualys VMDR `CSV`

1. Log in to **Qualys VMDR** or **Qualys Guard**.
2. Go to **Vulnerabilities** → **Reports** → **New Report** → **Vulnerability Report**.
3. Select **CSV** as the report format.
4. Set the target to all asset groups or the group you want to demo.
5. Click **Run**, wait for generation, then **Download**.
6. Save as `qualys-vuln-export.csv`.

Tip: Use the "All Vulnerabilities" template, not "Executive Report" — the raw export has all fields Straitum needs.

Rapid7 InsightVM `CSV`

1. Log in to **Rapid7 InsightVM** (or Nexpose).
2. Navigate to **Reports** → **Create Report**.
3. Select **CSV Export** as the report type.
4. Under Scope, select the relevant sites or asset groups.
5. Ensure the export includes IP Address, Hostname, CVE IDs, CVSS Score, Risk Score, Vulnerability Title, Severity, Solution.
6. Click **Save & Run**, then download when complete.
7. Save as `rapid7-export.csv`.

Tip: The "Vulnerability Details" built-in template (CSV) is the easiest option.

CrowdStrike Falcon Spotlight CSV

1. Log in to **Falcon Console** at falcon.crowdstrike.com.
2. Navigate to **Spotlight → Vulnerabilities**.
3. Apply severity filters if desired (Critical, High).
4. Click **Export → Export to CSV** (top-right).
5. Export includes: Host, CVE ID, CVSS Score, Severity, Product, Remediation, Status.
6. Save as `crowdstrike-spotlight-export.csv`.

Tip: Exports are capped at 10,000 rows. If you have more, export per-severity tier and merge the files.

Microsoft Defender for Endpoint (TVM) CSV

1. Log in to **Microsoft 365 Defender** at security.microsoft.com.
2. Navigate to **Vulnerability Management → Weaknesses**.
3. Click **Export → Export to CSV** (top-right).
4. Alternatively, go to **Vulnerability Management → Software Inventory** for an application-level export.
5. Save as `defender-tvm-export.csv`.

Tip: The "Machines" view gives you an asset-centric export — useful for showing per-device risk scores in the demo.

SentinelOne CSV

1. Log in to your **SentinelOne Management Console**.
2. For vulnerabilities: navigate to **Singularity Ranger → Vulnerabilities → Export → CSV**.
3. For the asset/endpoint inventory: go to **Endpoints → select all → Actions → Export to CSV**.
4. Save as `sentinelone-vuln-export.csv` or `sentinelone-endpoints.csv`.

Tip: If you don't have the Vulnerability Management module, the Endpoints CSV (OS version, last seen, agent version) is sufficient for Straitum to build an asset inventory and risk baseline.