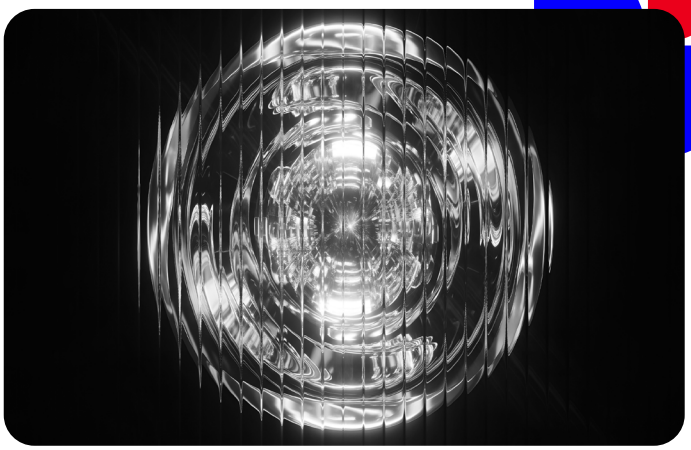
Watch List Connector for Tenable Vulnerability Management

Automate vulnerability tracking, prioritize what matters, and accelerate remediation.



Challenge

While modern vulnerability management platforms excel at identifying exposures across complex attack surfaces, the sheer volume of findings can still overwhelm security and IT teams. Identifying a vulnerability is only the first step; to effectively prioritize remediation, teams need to seamlessly correlate these internal findings with real-time, external threat intelligence to understand which exposures pose the most immediate risk to their organization.

Operating without real-time threat intelligence creates dangerous blind spots: critical flaws being actively exploited in the wild can sit unaddressed while security teams chase lower-priority items, leaving patching efforts misaligned with real-world risk.

Solution

The Recorded Future Watch List Connector for Tenable Vulnerability Management simplifies vulnerability management by automating the population of your Vulnerability Watch List directly from Tenable telemetry. The connector automatically extracts CVE identifiers from your scan findings, deduplicates results across assets, and maintains an up-to-date Watch List enriched with Recorded Future's threat intelligence — reducing the need for manual tracking and giving analysts immediate visibility into the vulnerabilities that matter most.

Configurable filters let teams tailor the Watch List to their environment. You can apply criteria such as vulnerability state (Open, Reopened, or Fixed), severity level (Low, Medium, High, Critical — defaulted to Critical, High, and Medium), valid vulnerability source (Tenable Nessus, NNM, and Agent), and scan folder to focus on the entities most relevant to your operations.

Benefits

- Reduce manual CVE tracking and correlation across scan results
- Focus remediation on the vulnerabilities most likely to be exploited
- Accelerate patch prioritization and reduce mean time to remediate
- Maintain real-time visibility into your evolving exposure

Key Features

- Native integration with Tenable Vulnerability Management
- Automated CVE extraction and deduplication across assets
- Filters for state, severity, source (Tenable Nessus, NNM, Agent), and scan folder
- Configurable update cadence (default: every 1 week)
- Continuous enrichment via the Recorded Future Intelligence Cloud

The connector refreshes on a configurable cadence — defaulting to every 1 week — so the Watch List stays aligned with the latest scan data without analyst intervention.

Setup is straightforward: an administrator navigates to the Integration Center in Recorded Future, opens the Tenable Vulnerability Management tile, and configures the connector using a Tenable API access key and secret key. From there, the connector runs continuously in the background — turning raw Tenable scan output into prioritized, intelligence-enriched insight inside the Recorded Future Platform.

Features

- Automated population of the Vulnerability Watch List from Tenable data, with no manual CSV exports or copy-paste.
- Extraction of CVE identifiers and deduplication of findings across assets to keep the Watch List clean and actionable.
- Filter criteria for vulnerability state (Open, Reopened, Fixed), severity (Low, Medium, High, Critical), source (Tenable Nessus, NNM, Agent), and scan folder.
- Continuous enrichment with Recorded Future threat intelligence — including risk context, exploit activity, and adversary references.

Results

Real-time monitoring

Watch Lists update automatically with each connector run, so security teams can stay on top of new vulnerabilities as soon as they appear in Tenable scans — without spreadsheets, manual exports, or waiting on a weekly review.

Proactive threat mitigation

Filters narrow the Watch List to the vulnerabilities most likely to be weaponized — by severity, state, scan source, and folder — so analysts can act on real risk instead of triaging noise.

Patch prioritization

Recorded Future intelligence layered on top of Tenable findings makes it clear which CVEs are being actively exploited, allowing teams to streamline patching, focus engineering effort where it pays off most, and reduce organizational risk.