

Agentic Vulnerability Management

Continuous, exploit-verified vulnerability management that turns an endless backlog into a ranked, actionable path

Why Sekuro

Attackers don't exploit vulnerabilities one at a time anymore; they chain them together to build a path straight to your most critical assets. Agentic Vulnerability Management automatically reviews assets for business context, exploit availability, and threat intelligence. Replace static scan-cycle thinking with continuous, agent-driven validation of what's genuinely exploitable in your environment—not just what a scanner flagged.

Our service is backed by a dedicated Automated Services team and grounded in attacker behaviour, not theoretical risk scoring. It's designed and built by security professionals with decades of first-hand experience solving client problems. Start seeing measurable value from day one with a frictionless implementation and platform built to earn its keep from the outset.

Service Overview

Our Agentic Vulnerability Management service combines continuous, multi-source discovery with AI agents that autonomously validate exploitability across your environment. Rather than relying on raw CVSS scores that treat every 'critical' as equal, we rank findings by real-world risk, deduplicate them, and map them to attack chains so your team spends time on what matters, not on triaging noise. Every finding is automatically assigned an asset, owner, due date, and status, closing the gap between detection and remediation.

Deploy individually or unlock deeper insights combined with Agentic Penetration Testing and Agentic Security Operations Centre through our SekuroOne platform. The result is a hyper-intelligent, evidence-based view of your risk exposure that strengthens over time.

Key Benefits

- No backlog, ever. Continuously triage, rank, and assign findings so lists never grow unmanaged.
- Prioritise findings by genuine exploitability in your environment, not by generic severity ratings.
- Automatically assign every finding an asset, owner, and due date; no manual intervention required.
- Continuous validation reflects your current risk posture, not data that ages the moment a scan ends.
- Feed findings directly into Agentic Penetration Testing, creating a closed intelligence loop.
- Present evidence-based reporting in a technical dashboard or board-ready summary from the same data, tailored by audience needs.

Our Approach

Continuous Discovery

Multi-source ingestion continuously maps your asset landscape, surfacing new exposures as your environment changes.

Exploitability Validation

Agents evaluate findings against real-world exploit conditions to confirm which vulnerabilities are genuinely exploitable in your environment.

Automated Ownership and Tracking

Every finding is assigned an asset, owner, due date, and status automatically, removing manual handling from the remediation workflow.

Deduplication and Attack Chain Analysis

Agents consolidate overlapping findings and identify how individual vulnerabilities combine into realistic attack paths.

Risk-Based Prioritisation

Validated findings are ranked by actual business risk and exploitability, not raw CVSS, so remediation effort goes where it matters most.

Closed-Loop Reporting

Findings and remediation status feed into one platform and connect with Agentic Penetration Testing, delivering one continuous, evidence-based view of your risk exposure.