Signal Match

Many organizations rely on scanning to detect software vulnerabilities. This can be problematic for multiple reasons, including scale and holes in asset identification. In contrast, vulnerability identification based on IT asset databases can often provide a more precise and comprehensive result. Using both techniques provide unparalleled insight into asset risk.

Signal Match complements scanning approaches by using intelligent matching techniques to identify vulnerabilities per asset databases, providing enhanced, more timely vulnerability awareness.

Vulnerability Intelligence for Business – Get the Signal

Cyber security has become a critical business objective for every company. High-profile data breaches can put any business at risk on the global stage.

Companies have scanned networks for years; more can be done to improve the state of the art.

Time lags in scanning and signature development, as well as faster exploits, are all changing the landscape.

Having a clear, timely picture of your posture is more important than ever.

Complement your scanning with ‘automated matching” to identify previously unknown public vulnerabilities and exploits.

Signal Match solves this problem by notifying you about vulnerabilities affecting your software and hardware

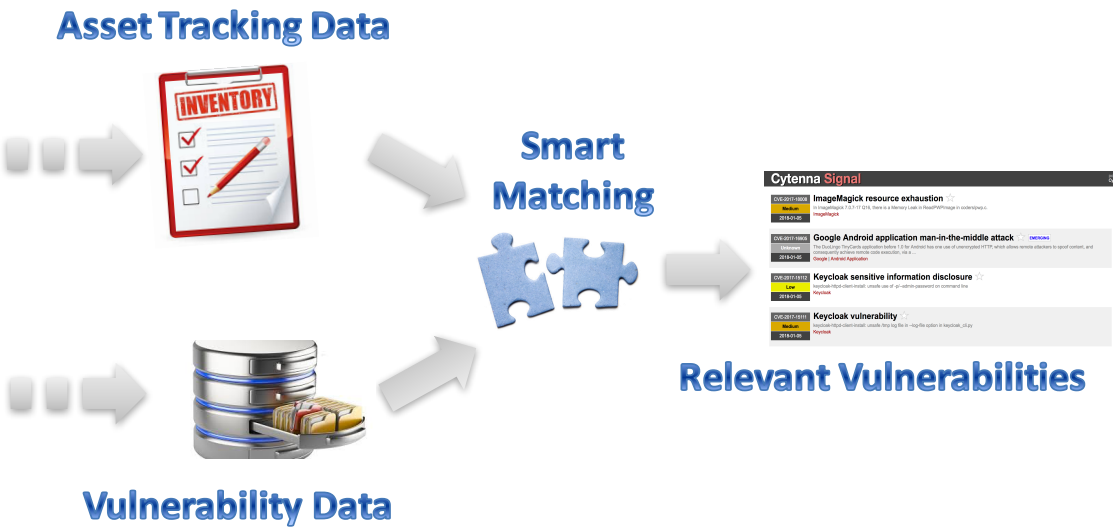
- **Identifies vulnerable software by matching your IT assets with known vulnerabilities.**
- **Gives management visibility into risk based on your corporate profile.**
- **Leverages a comprehensive and up-to-date vulnerability database.**
- **Supports vendor specific vulnerability metadata, such as Microsoft KBs, etc.**
- **Provides you with tools to help prioritize your vulnerability remediation plan of action.**
- **Supports the automation of SOC 2 and ISO 27,000, NIST compliance.**

Cytenna Corporation

2361 Rosecrans Ave,
Suite 348
El Segundo, CA 90245

Cytenna.com
info@cytenna.com
323.647.7875

How **Signal Match** Works:



Inventory matching

Your DevOps and IT Ops teams keep track of the inventory of assets that your organization uses and sends it to our platform for processing.

You provide the inventory or changes to it through our API and the Signal Match platform uses its machine learning and semantic processing algorithms to inform you of known vulnerabilities for your assets

Signal Match constantly monitors numerous sources for the latest information about vulnerabilities and security risks.

Vendor native awareness

We support vendor specific methods of helping you better understand your detailed risk profile. For example, we support inventory declaration of Microsoft KBs installed; in turn, we can inform you of missing security KBs that you may wish to install, depending on your exact configuration.

Alerts and Mitigation

Signal Match will send alerts to the appropriate staff members when a new security issue arises. The system also helps you choose the best mitigation strategy, and integrates with trouble-ticketing systems, so vulnerability management is simple from start to finish.

Key Features

- **Comprehensive coverage –** One of the largest vulnerability databases in the industry.
- **Real-time coverage –** Continually monitors for new and updated software vulnerabilities.
- **API and/or portal access –** Interact with our vulnerability data via API or portal.
- **Inventory Matching –** The system makes it simple to identify and match the assets you use.
- **Vendor native awareness –** Understand selected vendor-specific ways of referring to vulnerabilities and patches
- **Alerts and Reporting –** When new security issues arise, *Signal Match* alerts the right people. Reports can be generated in a wide variety of formats.

Cytenna Corporation

2361 Rosecrans Ave,
Suite 348
El Segundo, CA 90245

Cytenna.com
info@cytenna.com
323.647.7875