DATA SHEET

Securin

Vulnerability Intelligence (VI)

The Need for Vulnerability Intelligence

As environments become more complex, vulnerability counts are escalating dramatically. Yet, existing vulnerability data sets do not provide the core information needed to combat these vulnerabilities:

- **Lack of Complete Data:** The National Vulnerability Database (NVD) and other sources have gaps in coverage, often lack vulnerability scoring such as the Common Vulnerability Scoring System (CVSS), and have high latency from discovering a weakness, escalation to a Common Vulnerabilities and Exposure (CVE), and identification as a Known Exploited Vulnerability (KEV).

- **Lack of Comprehensive Data:** Vulnerability data from the NVD and other sources does not uncover Dark Web compromises, characterize threat actors, or detail the MITRE ATT&CK progression.

- **Weaponization Perspective:** Most vulnerability data sources do not describe how the vulnerability is weaponized and so do not provide the most critical insight – how to avoid building the vulnerability into the infrastructure or application.

To address these challenges, organizations need a single source of vulnerability information that fully lays out the weaponization lifecycle, the kill chain, key background such as threat actors and their corresponding attack methodologies, and remediation guidance. To avoid vulnerability fatigue, vulnerabilities must be prioritized not based on the odds of weaponization but instead on the likelihood that an adversary will exploit it. This information guides and streamlines remediation efforts. It also instructs development and infrastructure teams to proactively avoid building vulnerabilities into systems and applications.

Introducing Securin VI

Delivered as a software as a service (SaaS) application, Securin Vulnerability Intelligence (VI) provides an entire spectrum of vulnerability information through an intuitive dashboard and application programming interfaces (APIs) for embedding in applications and products. Leveraging data mined from over 1,000 sources and the insights of more than 100 threat researchers, Securin VI's artificial intelligence (AI) and machine learning (ML) models continuously measure risk by dynamically tracking vulnerabilities across the weaponization life cycle, from discovery to weaponization and exploit. This comprehensive approach ensures organizations can proactively defend against emerging threats and minimize their security risks.

Product Overview

Features

Securin VI provides rich information for both direct reference and embedding in applications.

Vulnerability Intelligence	Securin mines 1,000s of sources (including Dark Web) plus original insights from 100+ threat researchers to discover and detail new vulnerabilities. As a Certified Numbering Authority (CNA), Securin registers these pre-NVD CVEs and researches them throughout their life cycle. Securin VI provides this rich set of information in multiple formats, including drill down and drill aside.
Exploit Intelligence	Securin VI provides rich information about exploits, tracking: proof of concept (POC) exploits, remote code execution (RCE), privilege escalation (PE), public exploits, exploitation in the wild, exploitation by threat actors, exploitation by ransomware, and exploit code. Securin VI tracks a vulnerability's trajectory across the weaponization life cycle, from discovery through weaponization to exploit.
Predictive Models	Securin VI algorithms used in US Naval Intelligence, US Defense Advanced Research Projects Agency (DARPA), and Arizona State University (ASU) are built into 30 AI-ML models. These predictive models provide coverage and time advantages. For example, Securin VI tracks 80-120% more KEVs around 35 days faster than the Cybersecurity and Infrastructure Security Agency (CISA).
Initial Access Identification	As this is a critical factor in defense, Securin VI flags vulnerabilities that are potentially initial access vectors for cyber adversaries. This is done through in-house research and innovative processes. To ensure these vulnerabilities can be discovered by organizations, Securin VI specifies the plugins from the top three commercial scanners and Nuclei templates.
Threat Actor Intelligence	Securin VI tracks threat actors, victimology, MITRE tactics and techniques used, and CVE associations. This information enables security teams to understand how best to defend against specific threat actors.
Vulnerability Prioritization	Rather than use CVSS, Securin VI generates a Vulnerability Risk Score (VRS) with a Risk Index from 0-10 (highest). To prioritize based on an adversary's view of how best to gain initial entry and attain the objective, VRS factors exploitability across the MITRE ATT&CK framework, threat associations, and potential impact. For example, the Securin VRS prioritizes 30% of ransomware-related vulnerabilities that do not have CVSS scores.
Implementation	Ready onboarding (under an hour). Securin VI provides full Vulnerability Intelligence database information, including drilldowns, via APIs for embedding in applications. Information is also available via the user interface (UI) for interactive exploration. For formal integrations, Securin VI fully interoperates with IT service management (ITSM) applications, network scanners, and public clouds. Securin VI is also available as an OEM.

As a single source of intelligence, Securin VI provides complete vulnerability information needed to execute and automate remediation.

Usage Modes

Securin VI keeps security practitioners informed and up-to-date. Each vulnerability's history, association with threat actor groups, use in the MITRE ATT&CK framework, and mitigation or remediation is detailed in user-friendly drill down and drill through formats. To be a single source of intelligence for vulnerabilities, Securin VI has two usage modes:

- **Direct Access:** Via an intuitive user interface (Figure 1 and Figure 2), security teams can explore vulnerability information interactively. Vulnerability information is shown by category, but users can search, filter, drill down, and drill aside to explore all information.

- **Embedded in Applications:** Securin VI is designed to be leveraged by other applications and tools. SaaS delivery and robust APIs ensure that Securin's model of intuitive exploration is available within the organization's customized applications and original equipment manufacturer (OEM) applications including those delivered by managed security service providers (MSSP).

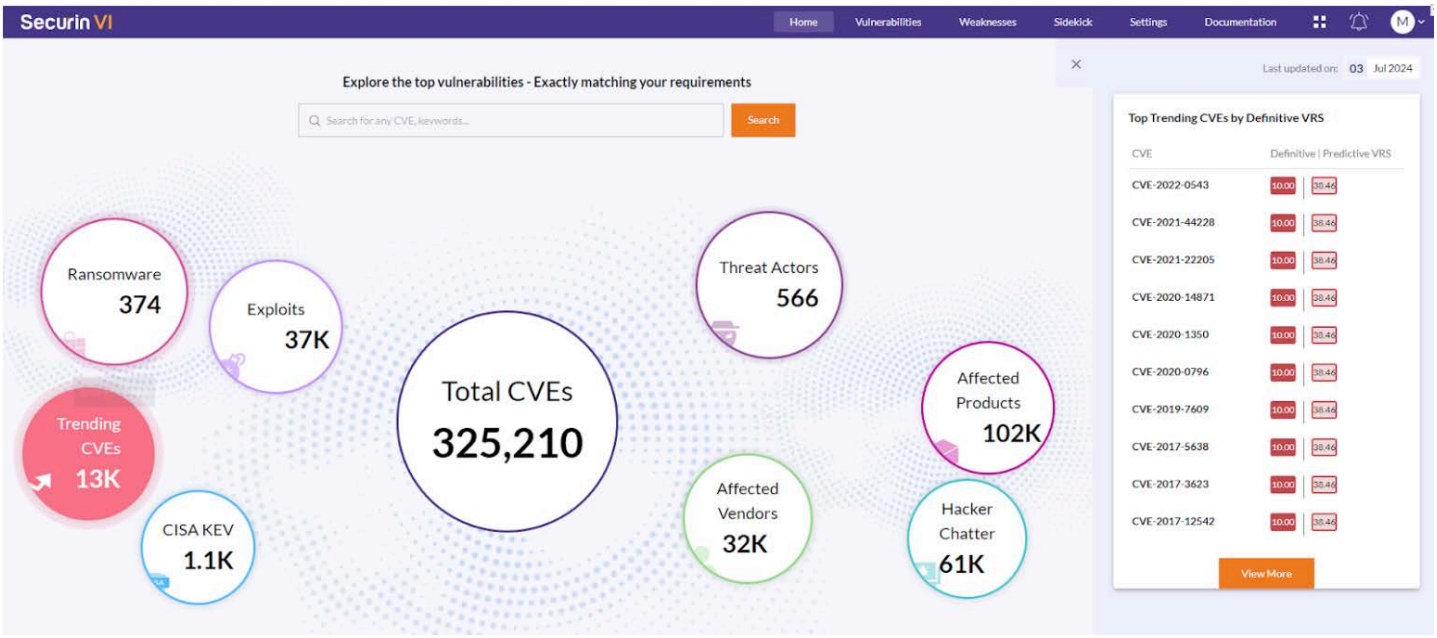

Figure 1: Securin VI enables interactive exploration of vulnerability information.

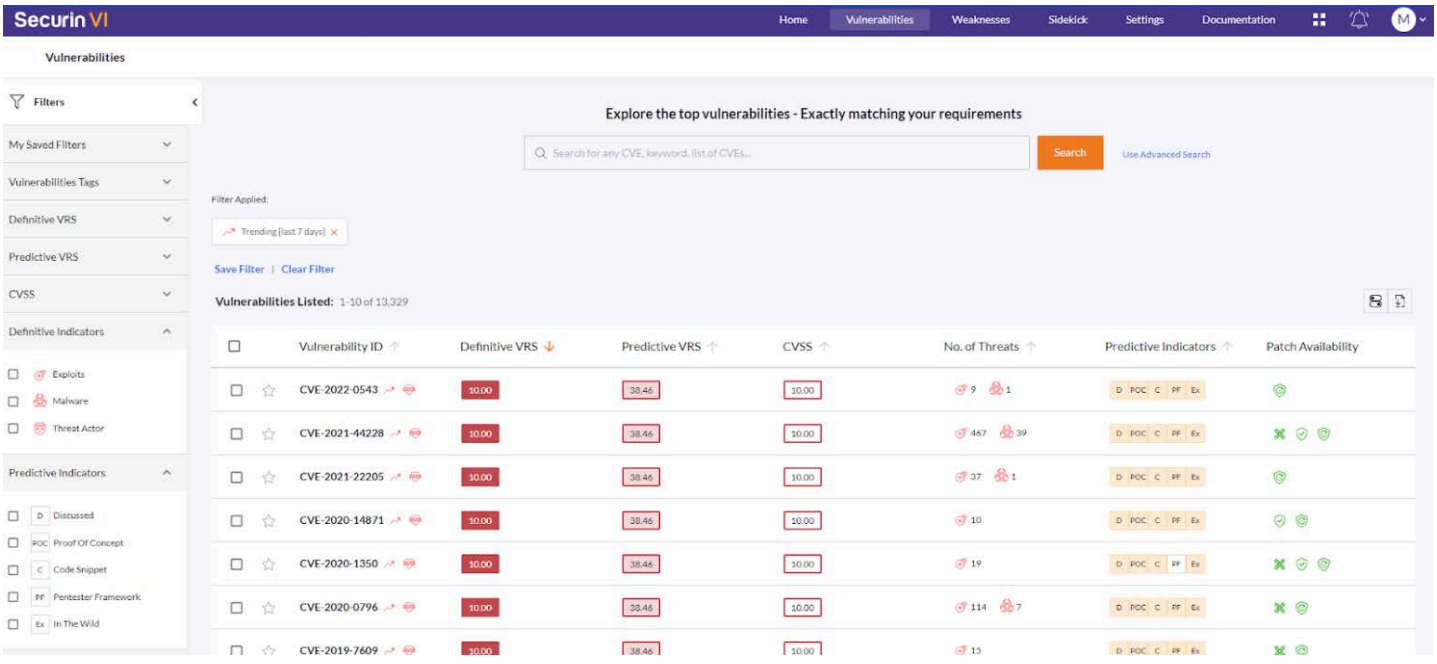

Figure 2: Securin VI has powerful search and filtering capabilities available via UI and API.

Unique Capabilities

Securin VI's unique capabilities include:

- **Exploit Intelligence:** Discovers, tracks, and provides detailed information for around 80-120% more KEVs than CISA. VRS score includes 30% more ransomware-related vulnerabilities than CVSS.
- **Predictive Intelligence:** Predicts a vulnerability will be exploited around 35 days faster than CISA.
- **Vulnerability Risk Intelligence:** Rather than use CVSS, Securin generates a Vulnerability Risk Score (VRS) that yields 71% less critical / high vulnerabilities than CVSS scoring (case study).

Benefits

These benefits apply both to direct use via the UI and embedded use via APIs.

Single Source of Intelligence

Provides all vulnerability information in the most convenient format – via UI or API – meeting all the needs of an organization in one application.

Optimized for Practitioners

The VRS score calculates the true risk across multiple factors, such as ransomware, providing better, more timely guidance for practitioners than CVSS scoring.

Works For All Groups

The combination of embedded and interactive use fits the needs of all groups in the organization – from the development team to the SOC and remediation team.

About Securin

At Securin, we empower teams and organizations to minimize their business risk with our comprehensive range of offensive cybersecurity solutions. These solutions are carefully crafted to be intuitive, adaptable, and scalable, catering to organizations of all sizes in today's ever-changing digital landscape. Securin's human-augmented intelligence approach to cybersecurity empowers organizations to thrive by proactively addressing emerging threats and uncertainties, ensuring their security.

Securin
securin.io

Follow Us On