SecurityScorecard

DATA SHEET

TITAN AI Platform

Data Overview

With 10+ years of third party data collection expertise, 12M organizations rated, and 99.9% proprietary data, SecurityScorecard represents the leading provider of telemetry on third, fourth and nth-party vendor risk management.

The Titan AI platform enables threat-informed third party risk management by thoroughly collecting data along a number of vectors and techniques:

Internet Intelligence

ACTIVE INTERNET SCANNING, ATTRIBUTED TO 12M+ VENDORS

Port scanning

- TCP and UDP support
- Full sweep of top ports every 24 hours
- Rescan of found services every 3 days
- Port-agnostic capture (whether a service is on port 80 or port 31337, we see it, identify it, and index it)

Advanced Infrastructure Fingerprinting across the IPV4 and IPV6 space

- **JARM Fingerprints:** A signature of the server's TLS stack. Use JARM to find default malware C2 configurations (e.g., Cobalt Strike, Trickbot) regardless of the host or IP.
- **JA4TScan Fingerprints:** A signature of the server's TCP netcode. Identify the underlying OS and device type even when banners are stripped. Detect proxies, VPNs, and load balancers with ease.
- **Favicon Hashing:** Trace phishing kits and mirrored fraudulent infrastructure by searching for unique application-layer visual icons.

Proprietary Passive Intelligence

Our API is enriched by one of the largest passive data collection networks on the planet.

Global Sinkhole

2 billion+ malware requests daily from 14 million infected IPs. Identify compromises in your supply chain without ever deploying a sensor.

Global Honeypot Network

Real-time logging of active scanners and exploit attempts from cybercrime hotspots, providing high-confidence malicious IP reputation.

Dark Web & Leaks

Access to 7 billion+ leaked credentials and PII records sourced from 600+ normalized data files found on hacker forums.

CVE Details — Vulnerability Intelligence

CVEDetails is a comprehensive security vulnerability aggregator that transforms complex data from the National Vulnerability Database (NVD) into a searchable, user-friendly intelligence hub. It provides security professionals with a centralized platform to track Common Vulnerabilities and Exposures (CVEs), mapped against specific vendors, products, and versions. By correlating vulnerability severity via CVSS scores with historical trends and exploit availability, CVEDetails enables teams to prioritize patching efforts and perform deep-dive risk assessments on their entire technology stack in one glance.

Security Scorecard maintains CVEDetails.com as a free portal for the cyber community to explore the data at any time.

CVE Details offers the following:

- CVE Data
- CISA KEVs
- Open Source Vulnerability format, https://ossf.github.io/osv-schema/, from multiple sources
- Common Vulnerability Reporting Framework, CVRF, from multiple sources
- Open Vulnerability and Assessment Language, OVAL, from multiple sources
- RSS/Atom feeds
- Various vendor APIs, including github, youtube etc
- CPE, CWE, CAPEC, CVSS, EPSS
- Third party tool modules/ plugins such as Metasploit, Nessus etc

Discovery of Unknown Vendors Through Automated Detection

Automated Vendor Detection (AVD) provides users a view into their 4th, 5th and nth-party vendors by association wit their 3rd-party vendors.

AVD uses the following detection methods based on findings from our regular scans and web crawls:

Detection method	Description
HTTP requests	Each week, we pull information in HTTP requests and responses made from a crawled website to other sites.
Detected libraries	Each week, we pull references to front-end software vendors in libraries we discovered on crawled websites.
Mail exchange	Each week, DNS queries are made to servers for the crawled domains to identify email providers.
Name server	Each week, DNS queries are made to servers for the crawled domains to identify hosting providers.
Enhanced illumination	Each month, we pull a third-party data source that includes resumés, job postings, digital signatures, contracts, exchange filings and more.

Security/Breach Events

Titan AI captures the modern threat landscape by aggregating real-time evidence from news, dark web forums, and technical bulletins into a single, deduplicated “truth.” By intelligently mapping these events—ranging from active breaches and zero-day exploitations to geopolitical instability—directly to your existing vendor ecosystem and asset data, we provide an immediate, top-down view of impact. This allows security teams to move instantly from a headline to a specific remediation plan, identifying exactly which products, CVEs, or third-party partners are at risk before the threat becomes a disaster.

USE CASES FOR SECURITY SCORECARD DATA

TPRM: Evaluate the true security posture of vendors by seeing their total internet exposure, risk from CVEs, timely breach readings and other relevant attributes.

Threat Hunting: Pivot from a single malicious IP to find an attacker’s entire global infrastructure using JARM hashes and SSH keys.

Attack Surface Management: Discover exposed RDP, database, or admin panels on non-standard ports that standard scanners miss.

Phishing Detection: Search for your company’s favicon hash globally to identify unauthorized look-alike domains before they are used in a campaign.

Shadow IT Discovery: Uncover unsanctioned cloud instances, forgotten dev environments, or marketing microsites registered by employees outside of official IT procurement by using DNS records and IP attribution to map assets back to your organization.

Get a demo of TITAN AI

Get hands-on with Security Scorecard’s data through the TITAN AI Platform