CrowdStrike Products

CROWDSTRIKE

CROWDSTRIKE FILE ANALYZER: SOFTWARE DEVELOPMENT KIT (SDK)

Build on a market-leading static file scanning solution powered by CrowdStrike machine learning (ML)

FAST, FLEXIBLE AND ACCURATE FILE ANALYSIS

CHALLENGES

To provide the best and most comprehensive security solutions for organizations, security and IT product owners must implement effective tools that meet their customers' needs, at speed and scale. Given the high costs, heavy resource investments and exorbitant amount of time needed to build a comprehensive file-scanning product, organizations can turn to OEM software development kits (SDKs) to cut costs, save time and deliver effective solutions. With powerful file scanning at your team's fingertips, they are empowered to deliver stronger solutions in less time, with less resource investment — all without sacrificing product performance.

SOLUTION

When organizations integrate market-leading file scanning, not only do they enhance their branded offerings, they also strengthen their solutions to help customers protect their organizations. CrowdStrike's File Analyzer SDK, a proven component of the CrowdStrike Falcon® platform, is now available for product owners to leverage within their own branded offerings to detect malware effectively and efficiently. Powered by the CrowdStrike Security Cloud and world-class artificial intelligence (AI), the CrowdStrike Falcon platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections. CrowdStrike's File Analyzer SDK is purpose-built for accuracy and is trained by CrowdStrike's massive corpus of malware samples to identify both known and zero-day malware.

CrowdStrike's File Analyzer SDK delivers in-depth context and rich data to inform your solution as it leverages machine learning that is trained using tens of millions of files sourced from the CrowdStrike ecosystem. Its unique multi-threaded architecture and concise verdict values enable your team to scale quickly, speed up development and derive valuable outcomes. Build fuzzy blocklists and/or allowlists using the included DeepHash API to ensure your tool is accurate and swift at detecting malware. You can also achieve faster scan times with an average of below 500 milliseconds, allowing you to deliver accurate and efficient results that empower your customers' IT and security teams.

KEY BENEFITS

Rich training: CrowdStrike's advanced ML training process uses tens of millions of files to produce best-in-class detection capabilities

Scalability: CrowdStrike's robust, multi-threaded SDK architecture enables seamless vertical and horizontal scaling to handle parallel static analysis scanning workload

Simple and fast outcomes: Easily speed up development with programmatic verdict values that can be clean, malicious or potentially unwanted applications (PUA)

Easy isolation: Frictionlessly use with no internet or cloud connectivity required

Detailed documentation: Gain additional context with in-depth user guides and sample code

Efficient scan time: Ensure faster scan time — average is typically below 500 milliseconds

KEY CAPABILITIES

The CrowdStrike File Analyzer SDK is a C library that provides organizations with the capability to scan files of the supported types, using ML, to determine if a file is malicious. The File Analyzer SDK supports multi-threading (i.e., thread safe), allowing it to scan multiple files simultaneously at scale. Users can also write custom C/C++ software applications that will link to the SDK to scan files seamlessly.

SYSTEM REQUIREMENTS

- Linux
  - Ubuntu 14.04, 16.04, 18.04 and 20.04
  - CentOS 6, 7 and 8
  - Debian 8, 9 and 10
  - RHEL 7 and 8
  - openSUSE Leap 15.1 and 15.2
- Windows 10 64-bit

SUPPORTED FILE FORMATS

Windows PE

Mach-O

ELF

XML, CDF and OOXML-based Microsoft Office files

PDF

Zip Archives

ABOUT CROWDSTRIKE

CrowdStrike Holdings, Inc. (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform enables customers to benefit from rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: **We stop breaches.**

Follow us: **Blog | Twitter | LinkedIn | Facebook | Instagram**

Become a Partner

Learn more at **www.crowdstrike.com**