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. 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 machine learning (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

CROWDSTRIKE FILE ANALYZER: SOFTWARE DEVELOPMENT KIT (SDK)

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, a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates upward of 1 trillion endpoint-related events per day in real time from across the globe, fueling one of the world's most advanced data platforms for security.