

Threat Detection

Ensuring software integrity with comprehensive threat detection analysis

Overview

Vulnerabilities in the software supply chain have been exploited in recent years resulting in tampering, malware insertion and other threats to critical business software.

Software Trust Manager Threat Detection secures the software supply chain through advanced, comprehensive detection of threats and vulnerabilities in open-source software, proprietary software, containers, and release packages.

Powered by ReversingLabs, Software Trust Manager Threat Detection uses a proprietary recursive binary analysis that enables it to scan the lowest level of a software object. It leverages the world's largest malware/goodware repository to detect threats. It supports more than 4800 file types including JAVA, .NET, Python, macOS, Linux, APK, and Docker images.

Threat Detection also generates comprehensive software bills of materials to comply with emerging regulatory requirements to provide transparency of software composition.

Key benefits

- Reduce risk of compiled software containing malware, vulnerabilities or secrets
- Centralize control by making threat detection a part of your software supply chain practices
- Increase trust of your software by taking a policy driven 'go/no-go' approach to software release based on priority of risks discovered
- Meet emerging regulatory requirements for software bills of materials

Key features

Detect threats and vulnerabilities in software binaries

Malware, software tampering, CVE detection, secrets leakage, and other vulnerabilities can be detected even for binaries that contain third party open-source or commercial code.

Scan for threats in same workflow as code signing

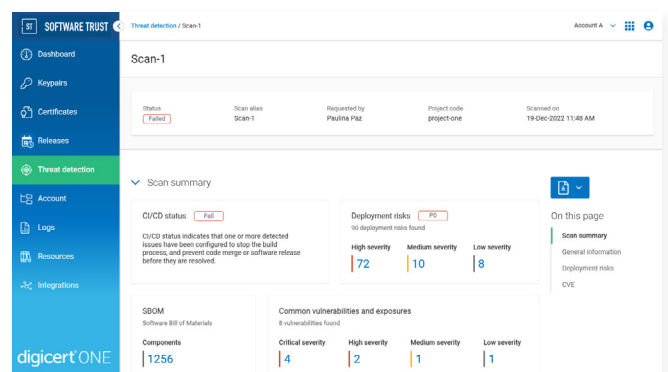
Minimize possibility of tampering by using the same workflow and platform to scan your software before you securely code sign it.

Fast and automated threat detection

Easily insert threat detection into CI/CD pipelines for any DevOps platform. Works for a variety of platforms and binary types.

Report on, and analyze, complex software composition

Software bill of materials (SBOM) and risk vulnerability reports are available to address emerging regulatory requirements such as those from the President's Executive Order 14028, M-22-18.



Threat Detection scans software binaries to ensure that malware and other vulnerabilities are not present and generates SBOMs and risk analysis reports.