DigiCert® Software Trust Manager Feature Spotlight

digicert®

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

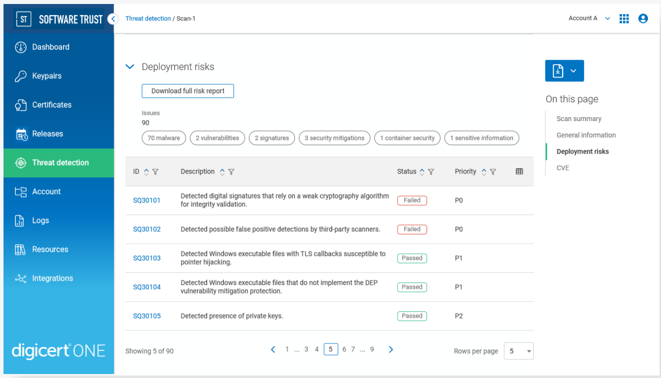
Key Features

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.



Deployment risks

Download full risk report

Issues
90

70 malware | 2 vulnerabilities | 2 signatures | 3 security mitigations | 1 container security | 1 sensitive information

ID	Description	Status	Priority
SQ30101	Detected digital signatures that rely on a weak cryptography algorithm for integrity validation.	Failed	P0
SQ30102	Detected possible false positive detections by third-party scanners.	Failed	P0
SQ30103	Detected Windows executable files with TLS callbacks susceptible to pointer hijacking.	Passed	P1
SQ30104	Detected Windows executable files that do not implement the DEP vulnerability mitigation protection.	Passed	P1
SQ30105	Detected presence of private keys.	Passed	P2

Showing 5 of 90 ‹ 1 … 3 4 5 6 7 … 9 › Rows per page 5

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