threatwatch

DATASHEET - THREATWATCH THIRD PARTY RISK ASSESSMENT

ThreatWatch is a next generation Third Party Risk Assessment platform that solves the problem of continuously tracking security weaknesses in your partner / vendor ecosystem in a collaborative manner with low overheads

Inside-Out Third Party Risk Assessment - Identifying and tracking the true cyber risk of your partners / vendors is challenging. Typically done only occasionally when on-boarding partners / vendors as part of a checklist. Even the best third party risk assessment tools only giving an "outside-in" view of the partners cyber risk posture. ThreatWatch innovative "inside-out" approach provides a continuous view of the true cyber risk of your partners / vendors.

Easy, secure profiling of attack surfaces - Partners / vendors can use ThreatWatch's open source asset discovery CLI - twigs, to safely inventory some or all of their attack surface to share with you as virtual assets. This can be anonymized and audited for privacy before sharing. twigs also allows your partners to automate this discovery to keep up with any changes to the attack surfaces.

Privacy - Partners / vendors can choose the privacy level at which they wish to share this information to you. At the highest level of privacy, only the threats / vulnerabilities to partner virtual assets are visible to you.

Early real-time risk assessment - Identify vulnerabilities and threats on partner assets on a continuous basis without scanning as soon as they emerge. AI based correlation and prioritization helps identify the most important threats in your partner ecosystems in real time.

Collaboration - Share information on priority threats with your partners. Collaborate with them to remediate threats based on SLAs. Improve their cyber risk posture and in turn secure yours.

Dashboards and reports - Monitor risk across all your partners / vendors using global and partner level dashboards. Rank your partners on risk scores and track their risk over time using summary and detailed risk reports.

threatwatch

Threatwatch - Instant POC available - visit https://threatwatch.io or contact us at info@threatwatch.io for more information

VIRTUAL ASSET SUPPORT SPECIFICATIONS

Open Source Technologies Supported -

All popular open source languages including Javascript, Ruby, Python, .NET, Java

All popular package dependency / package managers including NPM, Maven, Gradle, etc.

Repositories Supported -

Public and private git repositories

Local source code as virtual asset

Containers Supported -

Any docker compatible images and instances

Cloud Coverage -

Continuous vulnerability assessment for AWS, Azure and GCP instances

Agent-less discovery of assets in AWS and Azure

Compliance -

SSL / SSH Audits

CIS benchmarks audits for AWS, Azure, GCP, Docker, Linux and Windows

Code Secrets -

Find passwords, keys and other sensitive information leaks in code

Support for dictionary, heuristic and pattern matching, custom regex support

DAST -

Automated OWASP top-10 vulnerability checks on web applications.

Plugins available for DAST tools like skipfish, arachni, Zap

OS Assets Supported -

Popular Linux flavors including Red Hat, CentOS, Ubuntu, Debian

All supported versions of Microsoft Windows

Darwin based MacOS, OSX

Cloud OS images including Amazon Linux, Oracle Linux

File based asset ingestion -

Asset ingestion using existing scan reports from Qualys, Tenable, OpenVAS etc.

Asset ingestion using CSV and JSON files

Open source dependency files from npm, Maven, Gradle and other package management systems.

CMDB integrations -

Ingest assets from ServiceNow CMDB using twigs plugin

Other integrations available upon request

SERVICE SPECIFICATIONS

On-Platform Integrations -

MS Teams, Slack, Email notifications for early warning threat intelligence and real time impact assessment

Agent-less asset discovery from AWS, Azure

Asset discovery from scan reports from Qualys, Nessus etc.

CMDB integration with ServiceNow

Ticketing integration with JIRA, ServiceNow

Off-Platform Integrations -

Full feature ReST API

Python based SDK

CICD ready policies for Jenkins and other tools

Subscription / Deployment Options -

Fully managed dedicated secure instance hosted on cloud provider of your choice for larger teams

Instance based pricing and scaling based on number of partners / vendors

Access and license limits -

Unlimited users on dedicated instance

Unlimited scans

Virtual asset limits customized to number of partners / vendors

threatwatch