threatwatch

DATASHEET - THREATWATCH CONTINUOUS DEVSECOPS - WITH ATTENU8

ThreatWatch is a next generation DevSecOps platform that solves the problem of finding security weaknesses too late in the development cycle, and eliminates the use of scanner appliances or bulky agents.

ATTENU8 Threat Intelligence - Identifying threats is inherently a noisy process. Using traditional methods, security teams are unable to see the threat signals through this noise. In computer science we attenuate this noise so the signals are clear. ThreatWatch ATTENU8 uses machine learning models to curate threat information from public, darkweb and social sources and identify the most impactful threats to the systems in use. This results in a threat intelligence feed that shows vulnerabilities up to 3 weeks† sooner than legacy security scanners.

Vulnerability Management - All ThreatWatch subscriptions include full stack Vulnerability Management that happens at the speed of DevOps. Powered by ATTENU8 Threat Intelligence, ThreatWatch can identify vulnerabilities in Code, Containers, Cloud and other attack surfaces inline with the software build eliminating the need for a lengthy after-the-fact security scan.

Compliance - Compliance with regulations and/or company standards is often a challenge solved with auditors and a separate toolset. With ThreatWatch, you can ensure that systems are compliant with Center for Internet Security (CIS) Standards and various regulations including Payment Card Industry (PCI), HIPAA and many more.

† Jan 2020 comparison of 3 industry leading Vulnerability Management tools

Software Composition Analysis - Development teams use Open Source Components routinely to enable high-velocity code delivery. ThreatWatch identifies risk to your codebase, introduced by this external code. When integrated with the CI/CD pipeline, SCA can fail a build before it is delivered, eliminating security risk and costly code revisions.

Secrets Scanning - Hard-coded passwords, tokens and API Keys present an easily exploited entry point for hackers. ThreatWatch uses a sophisticated entropy and pattern matching algorithm to identify these risks before software is delivered.

Pen Testing and Security Posture Assessment - As part of the subscription, ThreatWatch can also provide a complete manual pen test of your attack surface with follow up consultation and review of remediation strategies. Together with the continuous automated DevSecOps platform, this give you and your customers and partners, complete assurance of your cyber hygiene.

threatwatch

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

SPECIFICATIONS

Open Source Technologies Supported -
All popular open source languages including Javascript, Ruby, Python, .NET, Java, Rust
All popular package dependency / package managers including NPM, Maven, Gradle, Cargo

Repositories Supported -
Public and private git repositories
Local source code as virtual asset

Containers Supported -
Any docker compatible images and instances
Automated discovery and tracking of container images for Google Container Registry (GCR)

Cloud Coverage -
Continuous vulnerability assessment for AWS, Azure and GCP instances
Agent-less discovery in AWS, Azure, GCP

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

SAST -
Automated static code analysis using open source plugins

Attenu8 Vulnerability coverage -
Fully machine curated real-time threat intelligence
Over 10K popular GitHub projects tracked for vulnerabilities
Vulnerability databases from across the world including Russian and Chinese NVDs
Security research sites, blogs, message boards, twitter, dark web and many other unstructured sources
Malware, ransomware and other threats correlated to vulnerabilities

OS Assets Supported -
Popular Linux flavors including Red Hat, CentOS, Ubuntu, Debian, Alpine Linux
All supported versions of Microsoft Windows
Darwin based MacOS, OSX
Cloud OS images including Amazon Linux, Oracle Linux

License Compliance -
Identification of copyleft and restrictive open source licenses
Tracking and reporting of open source versions being used

DAST -
Automated OWASP top-10 vulnerability checks on web applications.
Plugins available for DAST tools like skipfish, arachni

threatwatch

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 -
Single-user SaaS subscription ideal for small teams
Fully managed dedicated secure instance hosted on cloud provider of your choice for larger teams
Optionally host instance within your VPC
Instance based pricing and scaling

Access and license limits -
Unlimited users on dedicated instance
Unlimited scans
Virtual asset limits customized to your use case and requirements

Pen Test -
Pen test services performed by reputed cyber security professionals
Minimum 5 day test scoped based on complexity of environment
Report, recommendations and attestation certificate delivered at the end of the test
Follow up tests after remediation of issues

Consultation Services -
Drafting security policies
Best practices
Cloud security posture review
Remediation strategies

threatwatch