Integration Projects

- Nimbusec WSM - Available Data

Nimbusec WSM - Available Data

This page provides an overview of available data fields that can (partly already, partly to be implemented if required) passed on via our custom integrations within Website Security Monitor.

Current Webhook Format

Customer

id	Identifier to query additional user data
customer_id	Identifier to query additional tenant data
login	Username

Domain

id	Identifier to query additional domain data
bundle	Identifier of the active bundle (package) defining the scan features
name	Domain Name
url	Full URI that is used for scanning
responseIP	IP-Address that was recorded for the last scan.

Issues (Array)

id	Identifier to query additional issue data
domain	Identifier of the referenced domain
regions	List of regions through in which this issue occurred (possible values: EU, US, ASIA)
viewports	List of browser formats in which the issue occurred (possible values: mobile, desktop)
status	Display Status of the issue (possible values: pending, acknowledged, ignored)

event	Short name of the detected issue (e.g. malware, blacklist,...)
category	Overarching collection of events (e.g. content, reputation, ...)
severity	Numeric representation of the severity of an issue (1 = warning, 2 = alert)
firstSeen	Date and time on which the issue was first detected
lastSeen	Date and time on which the issue was detected most recently
details	See below. Each Issue has one of the following Details objects

Details

Application Outdated

name	Display name of the detected application
product	Canonical product name of the detected application the the version and vuln DB
url	Base URI where the application was detected (if detected by cloud scan)
path	Server-Path where the application was detected (if detected by server agent)
version	Detected version of the application
latestVersion	The latest version or latest stable Branch version (if applicable)

Application Vulnerable

name	Display name of the detected application
url	Base URI where the application was detected (if detected by cloud scan)
path	Server-Path where the application was detected (if detected by server agent)
version	Detected version of the application
vulnerabilities	List of detected vulnerabilities - CVE: ID of the vulnerability - Score: CVSS Score of the vulnerability - Description: Description of the vulnerability - Link: URL to further information in the Vulnerability Database

Blacklist

blacklist	Name of the blacklist which has the current domain listed.
reason	List of reasons (categories) for which the domain has been blacklisted
blacklistURL	Link to the Blacklist for further information and de-listing (if applicable)

Defacement

url	URI on which the defacement has been detected or was reported
threat	Name of the detected threat (most commonly the name of a hacker group or a distinguishing feature of a defacement)

Suspicious Links

links	List of Links on the website that are blacklisted
blacklists	List of Blacklist entries (see Blacklist above)

SuspiciousRequest

entity	Blacklisted URL or Domain
urls	List of suspicious URLs that were contacted
blacklists	List of Blacklist entries (see Blacklist above)

Webshell

path	Server-path to the detected file
threat	Short name of the detected threat (webshell, exec, obfuscated,...)
owner	System user that owns the file
group	System group that owns the file
permissions	Linux FS permissions of the file
mtime	Modified Timestamp as reportet by stat
md5	Checksum of the detected file
feature	If PHP code is detected, this string represents the generalized code patterns that are analyzed
av	Short name of the detection system (php, yara, lmd)
size	Filesize in bytes