OVERVIEW

Deteque Web Query Service: Stop cyber criminals targeting your online forms and logins

Stop cyber criminals using force and fraud to access website forms and customer logins. Web Query Service (WQS) uses threat intelligence from Deteque to check who is trying to access your network.

Why use Deteque's Web Query Service?

Attractive targets

Customers and subscribers appreciate the convenience of online access... and so do cyber criminals. Once successfully accessed, customer accounts are a valuable source of data and an opportunity for fraud and ransom. Access credentials are also a valuable black market asset in their own right.

Force and fraud

Cyber criminals use two main techniques:

Force – repeated, multiple attempts to simulate access credentials. Favored because they can be carried out by automated bots.

Fraud – using social engineered or stolen credentials to gain access to accounts.

Both are well used methods to commit fraud, access data and hold accounts to ransom.

Easy to use

This is a 'set & forget' service. From the moment you integrate Web Query Service, threat intelligence will be continuously updated ensuring threats are automatically blocked as soon as our researchers observe them.

Cost effective

WQS is based on the number of customers/subscribers you declare and that's it. You know in advance what your costs will be and for most organisations it will be less than $1 per user per year, regardless of how many times a user accesses a form or how many malicious attempts are made on your forms.

What it is and how it works

WQS uses threat intelligence gathered from Deteque's global network of security researchers, delivered via an API, so you can block malicious access attempts... anywhere with a customer/user entry point on a website.

WQS works at the 'submit' stage of a form fill. Before a submission is 'accepted' the IP of the submitter is checked via the API against Deteque's databases..

Key factors to block include:

- IP addresses of servers hosting botnet malware that is capable of spoofing Mail Server Application (MSA) connections.
- IP addresses of malware-infected devices, from which attempts have been made to compromise user account passwords.
- Low reputation domains which are part of a submitter's email address.

Automated protection

Blocks fake and fraudulent sign-ups

Simple API integration

Who can benefit?

Any organisation (commercial, public body) using online forms, contact pages and sign-ups can easily add an automated layer of protection from Deteque. WQS complements existing form protection techniques with the advantage of being automated.

Why Deteque?

Our focus is to make online security simpler by providing products that are easy to use and manage – all powered by the most comprehensive threat intelligence available.

Where does the data come from?

Deteque utilises data from Spamhaus, who have been collecting threat intelligence from third parties across the globe for over 20 years. This highly experienced team of researchers at Spamhaus consolidates the data onto dedicated Deteque servers making it available via the API.

How can this help your IT security?

WQS acts as an additional, automated filter to block specific threats and can be used to block other low reputation IPs/Domains. Because it is automated and always on, threats are blocked automatically allowing IT security teams to work on other tasks.

Is it GDPR compliant?

Data received via the API contains no Personally Identifiable Information (PII) – it's just an IP address or Domain – so that there is no compromise of organizational, customer or employee data. All data is transported to Deteque with encryption in place. For reporting purposes for a user, Deteque stores just the fact that a query was made and when, and whether it was listed. This ensures that privacy is maintained throughout the system.

Can I test it first?

There's a 30 day free trial for Deteque subscribers.

Deteque – a division of Spamhaus

Deteque is a division of Spamhaus and integrated with a global network of service providers and a community of security researchers who are dedicated to combating malicious online activities.

Since 2008, Deteque has been at the forefront of securing networks by collecting, collating and delivering DNS-related threat intelligence to protect organizations in real-time.

Follow Deteque:

@deteque

@deteque

'Deteque' channel

www.deteque.com

Your contact:

deteque | A division of SPAMHAUS