

Quick Start Guide

Dossier Express



TABLE OF CONTENTS

<i>Overview.....</i>	<i>3</i>
<i>Prerequisites</i>	<i>3</i>
<i>Dossier Express Web Interface.....</i>	<i>3</i>
Home Page	3
<i>Get Report.....</i>	<i>4</i>
<i>Report Walkthrough.....</i>	<i>5</i>

Overview

Infoblox Dossier a threat indicator research tool for analysts, researchers, security staff and SOC team members that brings next-level security and automation to threat investigation. Dossier gives contextual information pulled from dozens of sources simultaneously, empowering users to make accurate decisions more quickly and with greater confidence. The tool correlates multiple data sets including open source, proprietary and premium commercial sources and provides the ability to pivot on various data points during investigation and incident response.

Dossier Express provides a small sampling of the full Infoblox Dossier's capabilities so that organizations can get a hands-on experience to assist with the evaluation process. Dossier Express can be found at: dossierexpress.infoblox.com.

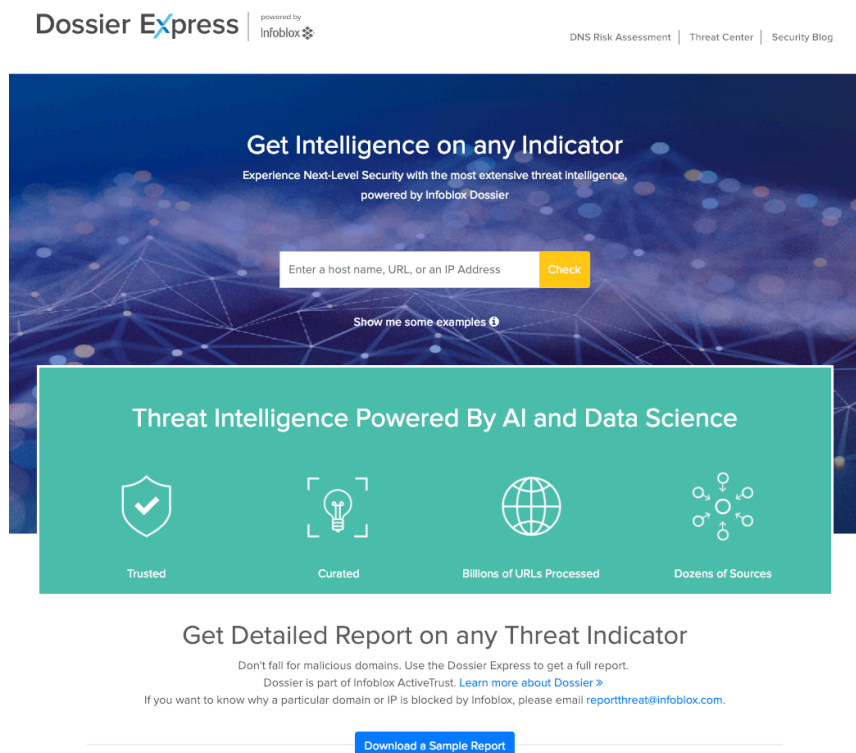
Prerequisites

Dossier Express is a tool powered by Infoblox and there is no initial prerequisite besides basic internet access and any popular web browser. Recent versions of Google Chrome are recommended for the best experience.

Dossier Express Web Interface

Home Page

The Navigation Menu is located on the top of the screen and provides access to other useful tools and articles related to DNS Security.



Dossier Express Search: provides extensive threat intelligence on specific host names, URL's and IP Addresses which are powered by Infoblox Dossier. (Note: by clicking the info circle next to "Show me some examples" you will be provided some sample inputs.

Download a Sample Report: used to download a sample of a complete report.

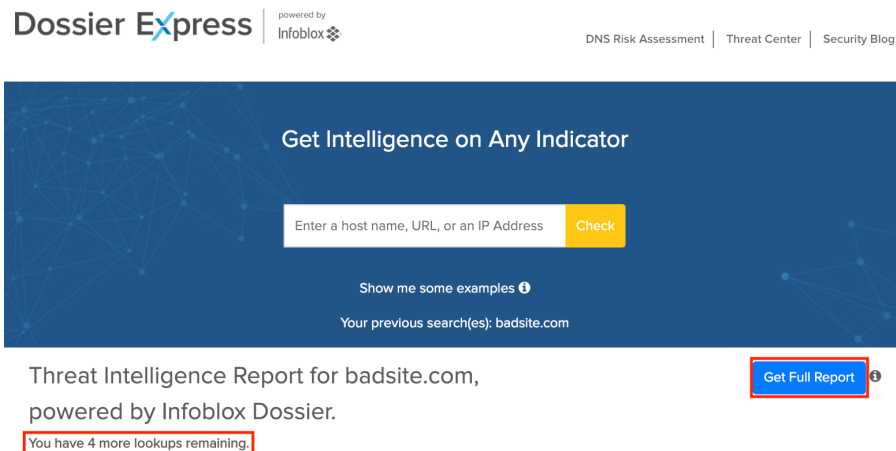
Get Report

In order to get a sample report and a complete report of a host name, URL or IP Address, do the following steps:



1. Enter the host name, URL or IP Address into the Search bar and hit enter.



2. Here you can see the information that is free of charge for you to navigate through. (Note that you are limited to 5 free searches and you can see how many are remaining.)



3. Click "Get Full Report" and enter in personal information:
 - First Name: your legal/personal identifiable first name that you go by.
 - Last name: your legal/personal identifiable last name that you go by.
 - Company: the organization you are representing.
 - Company Email: best email contact to receive the full report.
 - Phone Number: best phone number contact in the event you wish to receive more information.
 - Country: the country where you currently reside/work.
 - Job Title: your current job title on behalf of the company you are representing.
 - State: state where you are currently residing/working.

 Download Full Report 

Fill out the form to get the full report
All fields are required.

First Name:	<input type="text"/>	Last Name:	<input type="text"/>
Company:	<input type="text"/>	Company Email:	<input type="text"/>
Phone number:	<input type="text"/>	Country:	<input type="text" value="United States"/>
Job Title:	<input type="text"/>	State:	<input type="text" value="California"/>

☐ I would like to see a demo of Infoblox Dossier.

You will receive periodic communication from Infoblox on news, events and other marketing related information. If you are from European Countries, you must opt-in before you receive any communication from Infoblox. You can always manage your subscription preferences.

Submit

Report Walkthrough

Everything viewed in the report is a limited set of data provided by Infoblox Dossier, which is a feature of the Infoblox BloxOne Threat Defense security suite.

Details

Facts and features of the specified search item with details describing: first reported date, who reported it and the respective threat class associated to the indicator.

WHOIS

Dossier calls DomainTools' Whois API to provide the ownership record for a domain name or IP address with basic registration details in a well-structured format.

Current DNS

Search results from DNS Lookup provide all the available information about a given, hostname from DNS nameservers.

Geolocation

Provides IP attribution including ASN, ISP, and global map coordinates with city-level accuracy.

Related Domains/Subdomains

List of available domains and subdomains that are associated with the searched item.

Related URL's

List of available URL's that are associated with the searched item.

Related IP's

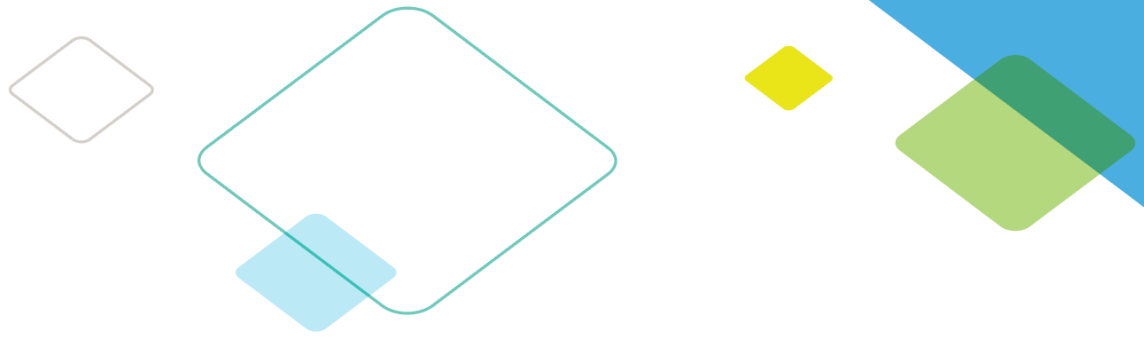
List of available IP's that are associated with the searched item.

Domain Information

Provides associated malicious activity and the last time that it was reported.

Malware Analysis

A limited list of known antivirus malware detections and their findings.



Infoblox is leading the way to next-level DDI with its Secure Cloud-Managed Network Services. Infoblox brings next-level security, reliability and automation to on-premises, cloud and hybrid networks, setting customers on a path to a single pane of glass for network management. Infoblox is a recognized leader with 50 percent market share comprised of 8,000 customers, including 350 of the Fortune 500.

Corporate Headquarters | 3111 Coronado Dr. | Santa Clara, CA | 95054

+1.408.986.4000 | 1.866.463.6256 (toll-free, U.S. and Canada) | info@infoblox.com | www.infoblox.com



© 2018 Infoblox, Inc. All rights reserved. Infoblox logo, and other marks appearing herein are property of Infoblox, Inc. All other marks are the property of their respective owner(s).