SOLUTION NOTE

Infoblox Dossier™

Faster answers. More context. Better decisions

SUMMARY

- Dossier improves the speed, quality and accuracy of threat research, investigation and response efforts.
- Dossier empowers quicker and immediately actionable decisions with greater confidence.
- 74 percent of security and risk leaders complain that the average threat investigation takes over four hours.
- 64 percent of practitioners say security investigation is resource intensive.
- A 2019 survey by ISC2 estimated the current global cybersecurity workforce gap at 4.07 million.

*Source: Ponemon Institute 2019, Forrester Research April 2020, ISC2 Cybersecurity Workforce Study, 2019

Dossier

BloxOne® Threat Defense includes a powerful threat indicator research tool, Dossier, for analysts, threat researchers, security staff and SOC team members. It automates the collection and correlation of threat intelligence from dozens of open source, proprietary or premium commercial resources of your choice, presenting it in a single view. This approach allows analysts to quickly pivot between intelligence sources to complete investigations faster and drive a rapid and effective response.

Either performing pure research or investigating an incident, the initial dashboard (Figure 1) overview of a threat indicator provides a general assessment of risk, confidence and overall threat while highlighting each source of threat intelligence supporting that assessment. From there, analysts can drill into details related to the threat, such as impacted devices, domains or URLs used, file samples, timelines or any available background on the threat actors. In the event of a threat not addressed by a current security policy, analysts can have it added to a blocklist to immediately protect the organization.

Figure 1: Dossier dashboard presentation of an emerging threat
## Dossier Key Capabilities

<table>
<thead>
<tr>
<th><strong>Research Potential</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat or Indicator</td>
</tr>
<tr>
<td>• The Dossier search field accepts active indicators, such as domains, hostnames, IPs, URLs, MD5, SHA1, SHA256 hashes and email addresses.</td>
</tr>
<tr>
<td>• Dossier includes scores for threat level, relative risk and confidence.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Indicator Summary</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Dossier provides quick links to key data.</td>
</tr>
<tr>
<td>Dossier lets users search by indicator to see which threat feeds contain relevant information.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Threat Categorization</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Dossier presents a rich history, detailed timeline and available analysis for the indicator being researched.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Related Insight</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Dossier provides researchers with deep insight into related indicators.</td>
</tr>
<tr>
<td>Dossier enables a rapid pivot to related domains, URLs and IPs.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Current News</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Dossier supplies quick access to the most recent news from the Infoblox Cyber Intelligence Unit (CIU) on emerging threats. Threat researchers can download and share Infoblox Cyber Intel news reports as PDFs.</td>
</tr>
<tr>
<td>Dossier graphically represents the threat feeds with the most activity.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Resources</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat researchers have access to Dossier’s online and downloadable resources.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Cloud-Native Service</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>This threat research solution is available anytime, anywhere.</td>
</tr>
</tbody>
</table>
**Powerful Use Cases Leverage Actionable Data**

Infoblox Dossier makes research data directly actionable at the DNS level through native integration with BloxOne Threat Defense. Dossier’s direct integration enables researchers at any point to immediately add the threat to a block list. Here are four important use cases to illustrate the speed, ease of use, and high utility of Infoblox Dossier:

**Use Case #1**

*Understand the Relative Level of Threat and Risk for a Specific Threat Indicator*

Your bank’s security operations team has identified a suspicious URL associated with a spam email received by multiple people in several departments. You want to understand its possible threat and risk levels. You enter the URL into Dossier and quickly navigate to other important contextual data about the indicator. This URL has been reported as a malicious website by some of Dossier’s threat intelligence sources and associated with banking Trojans. The threat and risk are high, so you must take action to remediate this threat. You add the domain to your block list in one simple step. BloxOne Threat Defense immediately protects all of your on-premises, cloud and remote teleworkers from accidentally accessing this malicious domain.

**Use Case #2**

*Uncover the Penetration of an Identified Threat from a CISA Alert*

The Cybersecurity and Infrastructure Security Agency (CISA) has sent out an alert and warned of attacks on hospitals by a specific group of threat actors. There are several threat indicators in the alert. You need to know as quickly as possible if this threat has impacted your hospital. You pivot within Dossier to research threat indicators and find that it already has been identified by several of your threat intelligence feeds and blocked. You navigate to the impacted devices within Dossier, and you can see that zero instances of these IP indicators have been used within your organization. You learn immediately that your organization has not been impacted by this threat at this time.

**Use Case #3**

*Rapidly Differentiate between Domain Registration and Domain Hosting to Assess Risk*

Your team has noted apparent malware communicating with a small business website accessed by one of your team members. This website URL is not identified on any of your threat feeds. Upon pivoting to contextual information on location data, you find that this local small business website has a domain registered in one country but hosted in another. This location data seems to confirm the validity of a potentially dangerous threat, and you add the domain to your watch list immediately.

**Use Case #4**

*Trace the Historic Activity of a Threat within Your Enterprise*

You have recently discovered several instances of a malware info stealer within your enterprise. Your team does additional research within Dossier to understand how much activity might have already occurred. Threat actors often watch for domain expiration and move rapidly to re-register the websites when the timely re-registration was not done by the legitimate owner. Dossier enables you to pivot to the Dossier timeline function’s contextual data to review major events associated with this threat. You can review the domain registration and identify changes in ownership that may indicate a risk.
Dossier Research Features

**Impacted Devices**
This list is created by running a query for the indicator you are researching. The data comes from the reporting logs. The display is limited to queries made within the past 60 days. If you find a threat, it is highly useful to pinpoint what devices have come into contact with the remote host.

**Custom Lists**
In addition to the predefined threat intelligence feeds that your subscription offers, you can create custom lists (containing domains and IP addresses) to define allow lists and block lists for additional protection. You can use a custom list to complement existing feeds or override the Block, Allow, Log or Redirect action currently defined for an existing feed. Dossier allows editing of custom lists with two simple clicks.

**Lookalike Detection**
Lookalikes are identified for the top 1,000 global domains tracked by Infoblox. With BloxOne Threat Defense Advanced, you can expand this feature to add other custom domains that you want monitored for lookalike activity.

**Current DNS Records**
A quick glance to see common DNS record types tells you a lot about the services on a remote host. Mail Exchanger (MX) and no website (A), extended DNS fields all tell a story about the purpose of the remote host/domain.

**Related Domains**
These domains have been tied to the indicator being researched based on many possible associations, such as malware that uses multiple domains.

**Related URLs**
These websites have been tied to the indicator being researched based on many possible associations, including malware or spam.

**Related IPs**
These are IP addresses that have been tied to this domain.

**Related File Samples**
These samples are based on possibly malicious files directly associated with the domain/IP. The most common source would be malware (virus) engines that report on files originating from or communicating to the domain.

**Timeline**
This feature shows significant events in the domain registration. You can identify changes in ownership. Sources include WHOIS (real records), PDNS (passive DNS observed from actual traffic), and various feeds such as SURBL, which track domains when they are newly created.

**Location**
Useful in determining the validity of a threat, this feature lets you see if the domain for a local business is registered in a different country. Alternatively, a locally registered domain hosted in a remote country may also be an indicator of compromise.
Threat Actor
If data on a threat actor is available related to the indicator, then it will be shown and highlighted. If the attack is related to a known group, you can learn about them, their tools, methods and possible motivation for attack.

Raw Whois
Here you can see a DNS WHOIS full listing with all details. This list is the unfiltered result of the DNS registration data.

Dossier Source Descriptions
The Dossier threat indicator research tool uses multiple sources. Using the Dossier toolset, users can make accurate decisions more quickly and with greater confidence based on the contextual information obtained from a dozen sources simultaneously. Dossier source descriptions include:

Alexa
Search results from Amazon Alexa provide a ranking from its global Top 1,000,000 Sites list.

Infoblox Cyber Intelligence Unit (CIU)
The Infoblox CIU creates, aggregates and curates information on threats to provide actionable intelligence that is high quality, timely and reliable. This information is easily accessed through Dossier along with other threat intelligence to assist in investigation and research.

Current DNS
Search results from Current DNS furnish all the available information about a given hostname from DNS nameservers.

Global Custom Search
This tool supplies a single view into related articles from the web that mention or link to the searched indicator. See them all without the danger of following potentially malicious links.

Geolocation
The geolocation tool plots the identified coordinates on a map, providing city-level accuracy. Other information includes ISP, city, region, latitude/longitude and country.

Google Safe Browsing
Google Safe Browsing, or GSB, enables applications to check URLs against Google’s constantly updated lists of suspected phishing, malware and unwanted software pages.

Passive DNS
Passive DNS is the historical DNS record for hostnames. When searching a hostname, Passive DNS will return all IPs that the hostname has resolved to and those caught by the Passive DNS sensors in the previous 12 months. When searching an IP, Passive DNS will return all hostnames that have pointed to that IP. Note that not every DNS change is caught, so there will be missing information.

Reverse DNS
The Reverse DNS tool performs a reverse DNS lookup of an IP address by searching domain name registry and registrar tables.

Reverse Whois
This tool provides you with data on domains such as name, address, telephone number, email address or physical address of the registrant listed in current or historical Whois records.
Malware Analysis
Data collection of malicious content is detected by aggregation of antivirus engines and website scanners.

Whois
Whois is an Internet record listing that identifies who owns a domain and their contact information. Whois records are an essential resource for maintaining the integrity of the domain name registration and website ownership process; they can reveal information to help determine any risk associated with a domain.

Dossier API
Dossier provides APIs to make connecting between related solutions—like security information and event management (SIEM) and security orchestration, automation and response (SOAR)—automatic, enhancing the overall experience and improving investigation and response efficiency.