

Blue Team Level 1 Certification
(Standard)

Introduction to BTL1

✓ Welcome to Blue Team Level 1

4 Topics

✓ Lab and Forum Access

SECURITY FUNDAMENTALS DOMAIN

✓ Introduction to Security Fundamentals

1 Topic

✓ Soft Skills

7 Topics

✓ Security Controls

5 Topics 1 Quiz

✓ Networking Fundamentals

6 Topics 1 Quiz

✓ Management Principles

4 Topics 1 Quiz

PHISHING ANALYSIS DOMAIN

✓ PA1) Introduction to Emails and Phishing

7 Topics 1 Quiz

✓ PA2) Types of Phishing Emails

10 Topics 2 Quizzes

✓ PA3) Tactics and Techniques Used

12 Topics 2 Quizzes

✓ Section Introduction, Tactics and Techniques

✓ Spear Phishing

✓ Impersonation

✓ Typosquatting and Homographs

✓ Sender Spoofing

✓ HTML Styling

✓ Attachments

✓ Hyperlinks

✓ URL Shortening Services

✓ Use of Legitimate Services

✓ Business Email Compromise

✓ [Video] Tactics and Techniques & Examples

Activity) Reporting on Tactics Used

Activity) End of Section Review, Tactics and Techniques

✓ PA4) Investigating a Phishing Email

8 Topics 2 Quizzes

✓ PA5) Analysing URLs, Attachments, and Artifacts

8 Topics 1 Quiz

PA6) Taking Defensive Actions

12 Topics 1 Quiz

PA7) Report Writing

7 Topics 1 Quiz

PA8) Phishing Response Challenge

3 Topics 1 Quiz

THREAT INTELLIGENCE DOMAIN

TI1) Introduction to Threat Intelligence

URL-Shortening Services

Blue Team Level 1 Certification (Standard) > PA3) Tactics and Techniques Used > URL-Shortening ...

COMPLETE

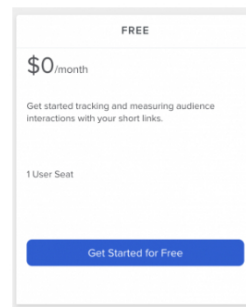


A tactic for disguising malicious URLs, and to prevent some aspects of automated security analysis, is the use of URL shortening services such as Bitly and Short URL. These services work by keeping a record of full URLs and generating short versions that simply redirect to the full URL. Below we will show you how we can hide the full URL using these services, and also how we can retrieve the full URL without visiting it directly.

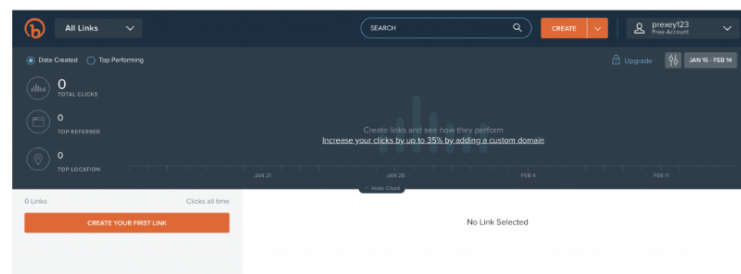
USING URL SHORTENERS

For this example, we're going to look at Bitly, which is a very popular choice for legitimate and malicious activities. You can either follow along or just watch what we do during this example.

Visit <https://bitly.com> and make an account, selecting the free tier.



Once you're all registered and the setup is complete, you'll be presented with the Bitly dashboard, where you can create shortened URLs and monitor their activity. To create our link, click the orange "CREATE" button in the top right.



For this example, we'll be using the following destination URL: <https://securityblue.team/courses/introduction-to-OSINT>. So we enter that into the "PASTE LONG URL" box and click "CREATE" at the bottom.

CREATE LINK

7 Topics
T12) Threat Actors & APTs
6 Topics 2 Quizzes
T13) Operational Threat Intelligence
7 Topics 1 Quiz
T14) Tactical Threat Intelligence
7 Topics 1 Quiz
T15) Strategic Threat Intelligence
5 Topics 1 Quiz
T16) Malware and Global Campaigns
6 Topics 1 Quiz
DIGITAL FORENSICS DOMAIN
DF1) Introduction to Digital Forensics
5 Topics
DF2) Forensics Fundamentals
10 Topics 5 Quizzes
DF3) Digital Evidence Collection
8 Topics 1 Quiz
DF4) Windows Investigations
3 Topics 3 Quizzes
DF5) Linux Investigations
4 Topics 2 Quizzes
DF6) Volatility
3 Topics 1 Quiz
DF7) Autopsy
4 Topics 1 Quiz
SECURITY INFORMATION AND EVENT MANAGEMENT DOMAIN
SI1) Introduction to SIEM
7 Topics 1 Quiz
SI2) Logging
6 Topics 2 Quizzes
SI3) Aggregation
2 Topics 1 Quiz
SI4) Correlation
6 Topics 1 Quiz
SI5) Using Splunk
5 Topics 2 Quizzes
INCIDENT RESPONSE DOMAIN
IR1) Introduction to Incident Response
8 Topics 1 Quiz
IR2) Preparation Phase
10 Topics 2 Quizzes
IR3) Detection and Analysis Phase
7 Topics 4 Quizzes
IR4) Containment, Eradication, and Recovery Phase
5 Topics 1 Quiz
IR5) Lessons Learned and Reporting
7 Topics
IR6) MITRE ATT&CK
13 Topics 2 Quizzes
BTL1 EXAM

bit.ly

PASTE LONG URL
https://securityblue.team/courses/introduction-to-OSINT

To create a Link from your dashboard, press 'b'

We can see at the top that we now have our own bit.ly link, which we can copy and use straight away! Below that we are given two options that we can change, the **TITLE**, and **CUSTOMIZE BACK-HALF**. The title simply changes the name of the link within your Bitly dashboard, and the below section allows you to change what comes after the "bit.ly/" part of the URL. An example of editing this would be:

- **No custom back-half:** bit.ly/2vyvczQ
- **Custom back-half:** bit.ly/ThisIsACustomBackHalf

EDIT LINK

bit.ly/2vyvczQ COPY SHARE

CREATED FEB 14 Hide Link

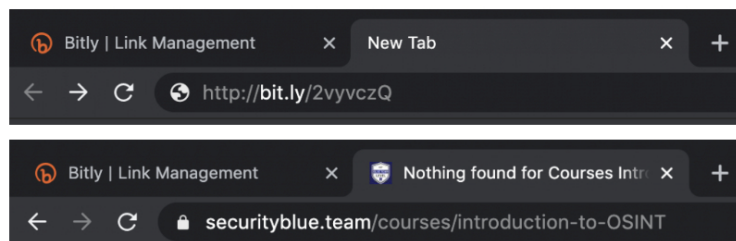
TITLE
Add a title.

CUSTOMIZE BACK-HALF
bit.ly/2vyvczQ

Did you know custom links get 34% more clicks? [Learn more](#) →

Add or create tag

If we try to visit our default bit.ly link, it redirects us to the full URL we set when creating it. Whilst nothing is actually on this exact page we have set, if we were a phisher we would set the destination URL to be our malicious site.



ANALYZING SHORTENED URLS

Whilst there is a future section of the course that will contain detailed information on analyzing URLs, we will briefly cover how to find out where shortened URLs go, without clicking on them, as this could potentially lead us to a malicious webpage.

One good option is to use the online service WannaBrowser, which lets you simulate any browser (kind of like using a virtual machine, but just for the browser). Visit <https://wannabrowser.net> and paste the shortened URL before clicking on "GET".

Wannabrowser – Simulate any Browser

http://bit.ly/2vyvczQ GET POST

+ Options | + Bookmarklet

In the below screenshot we have highlighted some important information that WannaBrowser has retrieved:

1. The first red box shows the link that WannaBrowser is using for this search. at the end it says

- "get=http://bit.ly/2vyvczQ", which means the browser is sending a GET request to download the webpage.
- The second box is the User-Agent string, which is the type of browser that is making the request. In this example we see "Safari" at the end, telling us the simulated browser is Apple's Safari.
 - Below that we have the final URL that was resolved, which is the destination URL we set when creating the bit.ly link.
 - Redirects list the total number of redirects before reaching a destination URL, in our case this is 1, because the bit.ly link redirected to our final URL, meaning there was 1 redirect.
 - Under the Header(s) heading, we can see that WannaBrowser encountered a 301 response code "Moved Permanently". The HTTP status code 301 is used for permanent URL redirection, which is exactly what Bitly does. With 301 redirects we should see the destination URL in the "Location" field.
 - As expected, the "Location" field shows us the URL the redirection points to.

You can read more about HTTP status codes (such as 301 Moved Permanently) at this [link](#), created by Mozilla.

[Link](https://www.wannabrowser.net/?get=http://bit.ly/2vyvczQ)
[Share](#)

Info

Referrer	
User-Agent	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/525.1.15 (KHTML, like Gecko) Version/13.0.3 Safari/525.1.15
Url	https://securityblue.team/courses/introduction-to-CISAT
Redirects	1
Time	0.620643 s
Size	706996 Bytes
Speed	1286334 Bytes / s
IP	3.9.68.12

Header(s)

```

HTTP/1.1 301 Moved Permanently
Server: nginx
Date: Fri, 14 Feb 2020 21:45:18 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 342
Location: https://securityblue.team/courses/introduction-to-CISAT
XWE-CORSX81: 31c4e2e21-9d74548823f45732-0001000111-17127/res-wed, 12 Aug 2020 21:45:18 GMT
Via: 1.1 google
  
```

We can use a URL visualization tool URL2PNG to search for our short Bitly address. When we attempt to view the link, we can see that it is actually showing us the error page on the Security Blue Team site!

<http://bit.ly/2vyvczQ>

Your users demand visual information.

Imagine this power embedded in your app, website or business process. The possibilities are endless with our intuitive API.

- > Thumbnails or 1:1 resolution
- > Capture the entire height of the page
- > Complete viewport control
- > Override user agents, default languages
- > Inject your own CSS on any page
- > Controller shutter with javascript
- > And more..

[Previous Topic](#)

[Back to Lesson](#)

[Next Topic](#)