

**Blue Team Level 1 Certification  
(Standard)**

TI6) 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

Section Introduction, Splunk

**Splunk Crash Course – Navigating Splunk**

Splunk Crash Course – Search Queries

Splunk Crash Course – Creating Alerts

Splunk Crash Course – Creating  
Dashboards

Lab) Splunk Investigation 1

Lab) Splunk Investigation 2

**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

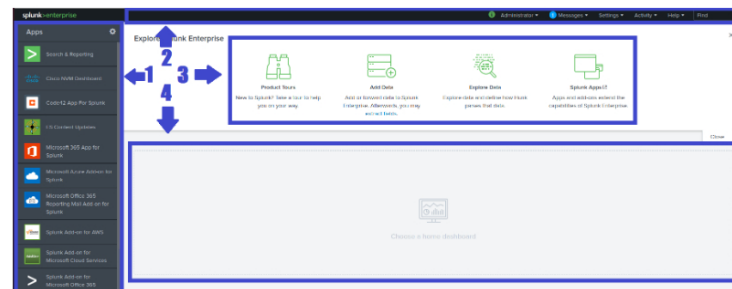
# Splunk Crash Course – Navigating Splunk

Blue Team Level 1 Certification (Standard) > SI5) Using Splunk > Splunk Crash Course – Navigati...

IN PROGRESS



Splunk offers a simple and streamlined GUI, making it easy to work with. It's worth mentioning that all SIEMs look fairly similar, so learning how to work with one provides you with transferable skills that can be adapted to the platform that the organization you work for uses. This lesson will cover how Splunk is laid out, and how to navigate through the platform. On the home screen, you will see the below sections, which are explained under the screenshot.



## Section 1 – Apps Panel

- The **Apps** panel lists the applications that are installed on your Splunk instance. The list shows only the apps that you have permission to view.
- When you first open Splunk Web, you will see the default and pre-installed App, **Search & Reporting**, in the Apps panel.
- Because we have other Apps installed (from configuring BOTSv1) we can see them listed on the left-hand side.

## Section 2 – Splunk Bar

- The Splunk bar appears on every page in Splunk Web. You use this bar to switch between apps, configure your Splunk deployment, view system-level messages, and monitor the progress of search jobs.

## Section 3 – Explore Splunk Panel

- The Explore Splunk panel contains links to pages where you can get help.
- You can take a product tour, add data, browse for new apps, or access the documentation.

## Section 4 – Home Dashboard

- Once dashboards have been created (we'll cover this later), we can set a dashboard to display on our homepage, which will be visible in the area marked "4".
- We can use this dashboard to immediately view information that is important to us, such as the number of alerts, types of attacks, and much more.

BTL1 EXAM

☐ Exam Preparation

☐ Using RDP and SSH

☐ How to Start Your Exam

<

Previous Topic

Mark Complete

✓

Back to Lesson

Next Topic

>

Privacy & Cookies Policy

