

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 101

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

✓ 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

7 Topics

○ TI2) Threat Actors & APTs

6 Topics 2 Quizzes

○ TI3) Operational Threat Intelligence

7 Topics 1 Quiz

○ TI4) Tactical Threat Intelligence

7 Topics 1 Quiz

○ TI5) Strategic Threat Intelligence

5 Topics 1 Quiz

○ 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

Splunk Crash Course – Creating Alerts

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

IN PROGRESS

SIEM CREATING ALERTS



Before we jump into how to create alerts, let's cover what alerts actually are. Alerts trigger when search results meet specific conditions, allowing us to monitor and detect particular activity, such as a user failing to login, or an external IP scanning the organisation. Alerts are triggered, and are then typically investigated by human analysts, who will perform the initial triage of the event, and escalate it to senior analysts if required. This is the main role of a SOC analysts, to triage and investigate SIEM alerts, while senior analysts may also be responsible for developing new detection rules, as well as tuning existing rules to reduce noise and make them more effective.

ALERTING PROCESS

The process of creating alerts can be split into four main steps:

1. Search Query
2. Search Timing
3. Alert Triggers
4. Alert Actions

We will cover each of these steps in more detail below.

1 – Search Query

The first task is to decide what activity we want to generate an alert. Is it an external IP trying to SSH into a corporate server? Is it a user account that is having a high number of login failures? Is it local administrator account usage? Rules in Splunk are essentially search queries, so we need to work out what activity we want to detect, and how to write a search query that will identify it.

2 – Search Timing

Now that we have an alert with a search query, we need to set how often Splunk is going to run the search query to look for any activity that makes the alert conditions. Primarily we'll use one of the two options:

- Continuously run this search query to look for related activity in real-time (the majority of SIEM rules)
- Run this search query on a set schedule (typically used to identify changes from baselines and behavioural profiles)

3 – Alert Trigger

If we have a rule that is looking for account logon failures, having it alert every time one logon failure event is generated in the environment, the SIEM is going to get smashed with tons of alerts. To combat this, we can create thresholds within the alert. For example, everyone gets their password wrong sometimes – but getting your password wrong 5, 6 times in a row isn't normal behaviour. We can create an alert that is looking for login failures from Windows domain controllers using Windows Event logs, and set a threshold of 6 per user. Now when an account hits 6 login failures, an alert will generate. We can also combine thresholds with time ranges, so if an account fails to login 6 times within 5 minutes, generate an alert.

4 – Alert Action

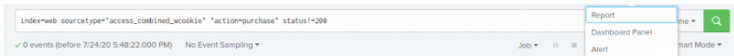
This is where we determine what actually happens when an alert triggers. Some of the default actions include:

- Sending an email notification (typically used for high-profile events that need an immediate response from senior analysts)
- Adding an alert to the list of recently triggered alerts (this is how analysts can identify alerts and work to investigate them)
- Log and index searchable alert events (this actually allows analysts to quickly view all the information related to the alert that triggered)

Splunk also has the ability to allow administrators to write their own custom actions using web hooks, so messages can be created in their own applications, such as a mobile app that informs analysts when a new alert has been triggered and needs to be investigated.

CREATING YOUR OWN RULES

First, we need a search query. Once we've written it, we can click on 'Save As' and then 'Alert'.



Then the following windows will be displayed:

Save As Alert

Settings

Title

Title

Description

Optional

Permissions

Private

Shared in App

Alert type

Scheduled

Real-time

Run every week

On

Monday

at

6:00

Expires

24

hour(s)

Trigger Conditions

Trigger alert when

Number of Results

Is greater than

0

Trigger

Once

For each result

Throttle

Trigger Actions

+ Add Actions

Cancel

Save

Give the alert a title and description.

Permissions

- **Private** – Only you can access, edit, and view triggered alerts.
- **Shared in App** – All users of the app can view triggered alerts, by default, everyone has read access and power user has write access to the alert.

Alert type:

Here we tell splunk how to search for these events that match our alert.

- Scheduled alerts, will search at a defined interval and evaluate trigger condition when the search completes.
- Real time alerts, these run constantly in the background and evaluate trigger conditions within a window of

<div><div></div><div>DF3) Digital Evidence Collection</div><div><div></div><div>8 Topics</div><div>1 Quiz</div></div></div>
<div><div></div><div>DF4) Windows Investigations</div><div><div></div><div>3 Topics</div><div>3 Quizzes</div></div></div>
<div><div></div><div>DF5) Linux Investigations</div><div><div></div><div>4 Topics</div><div>2 Quizzes</div></div></div>
<div><div></div><div>DF6) Volatility</div><div><div></div><div>3 Topics</div><div>1 Quiz</div></div></div>
<div><div></div><div>DF7) Autopsy</div><div><div></div><div>4 Topics</div><div>1 Quiz</div></div></div>
<div><div>SECURITY INFORMATION AND EVENT MANAGEMENT DOMAIN</div></div>
<div><div></div><div>SI1) Introduction to SIEM</div><div><div></div><div>7 Topics</div><div>1 Quiz</div></div></div>
<div><div></div><div>SI2) Logging</div><div><div></div><div>6 Topics</div><div>2 Quizzes</div></div></div>
<div><div></div><div>SI3) Aggregation</div><div><div></div><div>2 Topics</div><div>1 Quiz</div></div></div>
<div><div></div><div>SI4) Correlation</div><div><div></div><div>6 Topics</div><div>1 Quiz</div></div></div>
<div><div></div><div>SI5) Using Splunk</div><div><div></div><div>5 Topics</div><div>2 Quizzes</div></div></div>
<div><div></div><div>Section Introduction, Splunk</div></div>
<div><div></div><div>Splunk Crash Course - Navigating Splunk</div></div>
<div><div></div><div>Splunk Crash Course - Search Queries</div></div>
<div><div></div><div>Splunk Crash Course - Creating Alerts</div></div>
<div><div></div><div>Splunk Crash Course - Creating Dashboards</div></div>
<div><div></div><div>Lab) Splunk Investigation 1</div></div>
<div><div></div><div>Lab) Splunk Investigation 2</div></div>
<div><div>INCIDENT RESPONSE DOMAIN</div></div>
<div><div></div><div>IR1) Introduction to Incident Response</div><div><div></div><div>8 Topics</div><div>1 Quiz</div></div></div>
<div><div></div><div>IR2) Preparation Phase</div><div><div></div><div>10 Topics</div><div>2 Quizzes</div></div></div>
<div><div></div><div>IR3) Detection and Analysis Phase</div><div><div></div><div>7 Topics</div><div>4 Quizzes</div></div></div>
<div><div></div><div>IR4) Containment, Eradication, and Recovery Phase</div><div><div></div><div>5 Topics</div><div>1 Quiz</div></div></div>
<div><div></div><div>IR5) Lessons Learned and Reporting</div><div><div></div><div>7 Topics</div></div></div>
<div><div></div><div>IR6) MITRE ATT&CK</div><div><div></div><div>13 Topics</div><div>2 Quizzes</div></div></div>
<div><div>BTL1 EXAM</div></div>
<div><div></div><div>Exam Preparation</div></div>
<div><div></div><div>Using RDP and SSH</div></div>
<div><div></div><div>How to Start Your Exam</div></div>

time based on the conditions you define.

Save As Alert

Settings

Title

Title

Description

Optional

Permissions

Private

Shared In App

Alert type

Scheduled

Real-time

Expires

24

hour(s)

Trigger Conditions

Trigger alert when

Per-Result

Throttle

☒

Suppress results containing field value

status

Suppress triggering for

10

minute(s)

Trigger Actions

+ Add Actions

Cancel

Save

In the screenshot above we have set the Alert Type as real-time, Expiry after 24 hours, and Trigger Alert is set to 'per result'. We will get results for each match, we can throttle this if too many alerts are being generated. Here we have set it as 'suppress results' which contain 'status' as our search alert contains the 'status' keyword, and will suppress it after 10 minutes.

Lastly, **trigger actions**:

Here we tell Splunk actions to take when an alert is generated, as mentioned it can do the following: trigger alerts, log the event, output results to lookup file, and run a script or output results to an endpoint so it can get the attention of a SOC analyst.

Expires

24

hour(s)

Trigger

Log Event

Send log event to Splunk receiver endpoint

Suppress results containing

Output results to lookup file

Output the results of the search to a CSV lookup file

Suppress triggering for

10

minute(s)

Trigger Actions

+ Add Actions

Cancel

Save

< Previous Topic

Mark Complete ✓

Next Topic >

Back to Lesson

Privacy & Cookies Policy

