

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

SIEM Platforms

Blue Team Level 1 Certification (Standard) > SI1) Introduction to SIEM > SIEM Platforms

IN PROGRESS

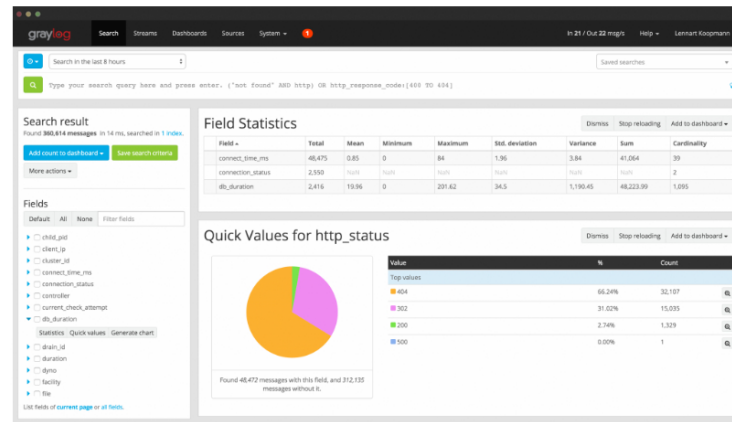
SIEM Domain
SIEM PLATFORMS

This lessons is designed to provide you with an insight into the different SIEM platforms on the market. We will explore the different platforms, their capabilities, strengths and weaknesses. We will also introduce you to the platform we will be using in this course to teach SIEM skills, Splunk.

GRAYLOG

<https://www.graylog.org/>

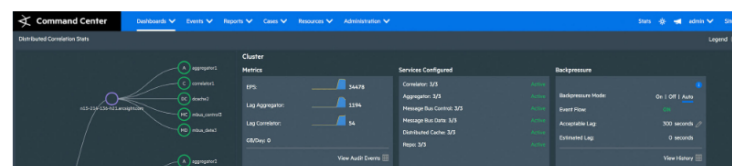
Graylog offers two different SIEM products, Graylog Open Source which is 100% free, and their paid-for product, Graylog Enterprise. If you want to download and play around with Graylog Open Source you can download it [here](#). Graylog Enterprise has a free limit and can be used by small organizations that process less than 5 GB worth of events per day. Below is a screenshot of a search page within Graylog, giving you an idea of how the platform looks.



ARCSIGHT

<https://www.microfocus.com/en-us/products/siem-security-information-event-management/overview>

ArcSight (with their SIEM ArchSight, also referred to as ArcSight Enterprise Security Management, or ESM) states that it can help SOCs to build out a layered analytics approach by integrating with a wide range of commercial security tools, and offers Security Automation and Response (SOAR) workflows to provide an automated response to security events, leaving analysts to focus on more important investigations. Powerful real-time correlation within ArcSight claims to be the fastest way to detect threats from large datasets.



- 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

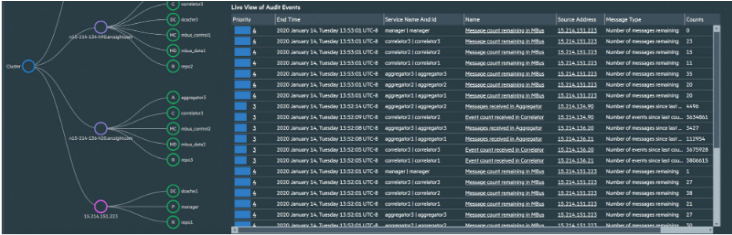
- SI1) Introduction to SIEM
 - 7 Topics 1 Quiz
 - Section Introduction, SIEM
 - Security Information Management (SIM)
 - Security Event Management (SEM)
 - What is a SIEM?
 - SIEM Platforms
 - Further Reading Material, SIEM
 - SIEM Glossary
 - Activity) End of Section Review, SIEM
- SI2) Logging
 - 6 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

- Exam Preparation
- Using RDP and SSH
- How to Start Your Exam



QRADAR

<https://www.ibm.com/uk-en/security/security-intelligence/qradar>

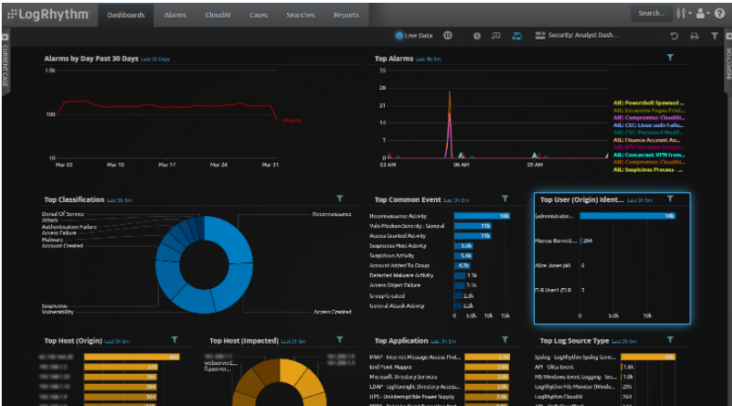
In addition to basic SIEM capabilities, QRadar SIEM also offers the ability to import data from threat intelligence feeds. When purchasing QRadar, clients can also opt-in to subscribe to the paid-for IBM Security X-Force Threat Intelligence, which identifies malicious indicators, which can be used to provide investigation enrichment, or for immediate alerting. Additional modules exist for QRadar that can assist security teams with incident response, risk management, and vulnerability management.



LOGRHYTHM

<https://logrhythm.com>

LogRhythm boasts some pretty impressive features, such as machine learning, Security Automation and Response (SOAR), End-Used Behavioural Analytics (UEBA), and Network Detection and Response (NDR) to give unmatched environment visibility and response capabilities, directly from the SIEM platform. LogRhythm also states that “you’ll easily baseline your security operations program and track your gains – so you can easily report your successes to your board”, which does indeed sound like a useful and efficient way to generate metrics and prove to executives that we really do protect the business, every single day.





SPLUNK

https://www.splunk.com/en_us/platform.html

Splunk is one of the most popular SIEM platforms in the industry. SIEM administrators can download and add "Apps" that provide additional functionality to Splunk, such as analytics, dashboards, improved searching, and data manipulation. Imported data can be searched using custom-written search queries, which can also be used to generate alerts, and create visual dashboards.

