

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

PA4) Investigating a Phishing Email

8 Topics 2 Quizzes

PA5) Analysing URLs, Attachments, and Artifacts

8 Topics 1 Quiz

Section Introduction: Analysing Artifacts

Visualization Tools

URL Reputation Tools

File Reputation Tools

Malware Sandboxing

[Video] Manual Artifact Analysis

Artifact Analysis With PhishTool

[Video] Artifact Analysis with PhishTool

Activity: End of Section Review: Analysing Artifacts

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

Malware Sandboxing

Blue Team Level 1 Certification (Standard) > PA5) Analysing URLs, Attachments, and Artifacts > M...

COMPLETE

Phishing Analysis
INTERACTION TOOLS

Sandboxing is the process of detonating (running/executing) a piece of malware in a contained environment, and closely monitoring exactly what the software does, allowing security teams to collect indicators of compromise. Examples include monitoring the network traffic to see if the malware tries to communicate with a command-and-control (C2) server on the Internet to receive commands or download additional modules, giving the malware more capability. By understanding how the malware operates, it becomes easier to create defenses that can detect and alert on similar activity.

Security teams will have access to dedicated enterprise-grade sandboxing and malware analysis tools. Replicating this is out of scope for this course, but we can teach you about sandboxing and malware analysis and have you learn to use the online platform [Hybrid Analysis](#).

HYBRID ANALYSIS

Hybrid Analysis is an online malware analysis platform that lets you upload malware for instant cloud-based analysis, providing you with a detailed report about the observed activity.



File/URL

File Collection

Report Search

YARA Search

String Search

This is a free malware analysis service for the community that detects and analyzes unknown threats using a unique Hybrid Analysis technology.



Drag & Drop For Instant Analysis

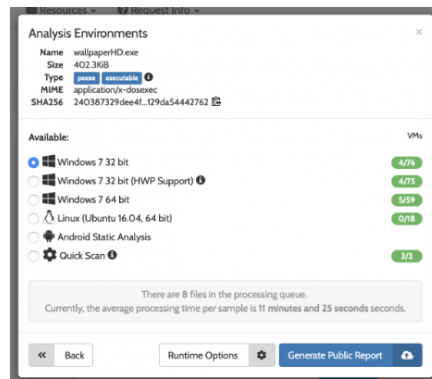
First, navigate to the Hybrid Analysis website. Here you can drag-and-drop, or browse for the file you want to upload.



I14) Iactical 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
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
Exam Preparation
Using RDP and SSH
How to Start Your Exam



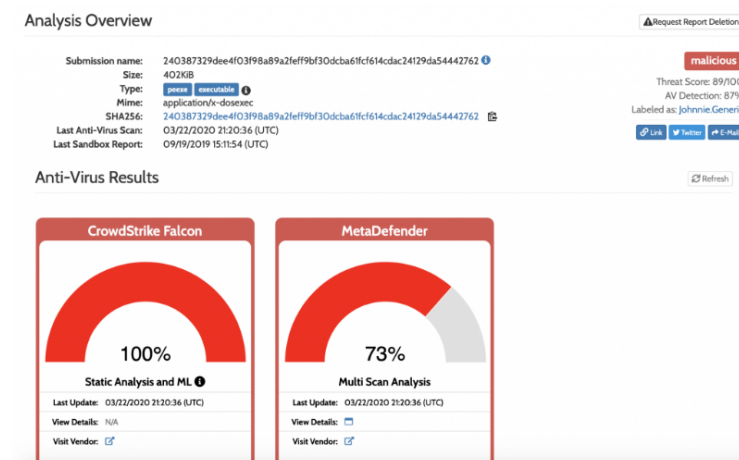
Next, you can choose the operating system that you want to detonate the malware on – this is perfect for malware that only targets specific operating systems. For this activity, we'll just use the default Windows virtual machine.



Once you've clicked "Generate Public Report" you will be directed to the report page once the analysis has completed. You can see this below.

ANALYSIS RESULTS

Below is a screenshot of the results provided by Hybrid Analysis after we uploaded the piece of known malware. You can also view the report yourself here – <https://www.hybrid-analysis.com/sample/240387329dee4f03f98a89a2feff9bf30dcba61fc614cdac24129da54442762>.



CONCLUSION

Hybrid Analysis is a great free platform to submit suspicious attachments to see if they are malicious. While

security teams will have their enterprise-grade tools, this is the perfect tool for security researchers and provides detailed analysis and reputation checks.

[< Previous Topic](#)

[Back to Lesson](#)

[Next Topic >](#)

[Privacy & Cookies Policy](#)



[Privacy - Terms](#)