Subject to change prior to launch, September 2021.

Blue Team Level 2

Course Syllabus

Professional-Level Certification

Table of Contents

Introduction

Why did we make BTL2?

After the huge success that was BTL1, creating the cheapest practical blue team certification on market, we understood that both our individual customers and corporate clients were looking for a higher level of training for their experienced team members. BTL2 builds on and improves the quality of content, technical depth, and training delivery.

Copyright Notice

This syllabus has been designed by Security Blue Team (Security Team Training Ltd, a registered company in the United Kingdom, and any replication without expressed permission is an infringement of our intellectual property and copyright rights. Any unauthorised use may result in legal action to claim for damages.

Access Terms and Conditions

During the checkout process students must agree to our Refunds Policy and BTL2 Terms and Conditions before they are able to purchase the course. These terms are also reiterated at the start of the course. These protect the intellectual property of Security Team Training Ltd and prohibit students from sharing training material with non-students. Any form of piracy, account sharing, or otherwise disclosing private course materials will result in permanent account termination with no refund, and potentially legal action to claim for damages. Please respect our hard work.

Domain 0: Welcome to BTL2

Subject to change prior to launch, September 2021.

Welcome to BTL2

- Boring Legal Stuff
- Course Overview
- Credits and Special Mentions
- Issues and Feedback
- Lab and Forum Access

Study Resources

- Section Introduction
- Creating a Study Plan
- Tips and Tricks

Domain 2: Malware Analysis (1/2)

Subject to change prior to launch, September 2021.

MA1) Introduction to Malware Analysis

- Section Introduction
- Why is it Important?
- Malware Types
- Types of Analysis
- Tools Covered
- Activity) Section Review

MA2) Setting up a Lab

- Section Introduction
- Need for Analysis Labs
- Configuration Requirements
- Installation, Settings, Snapshots
- Obtaining Malware Samples

MA3) Static Analysis

- Section Introduction
- Overview of Static Analysis
- Portable Executable File Format
- Hashing
- Strings
- Lab) Hashing and Strings
- YARA and yarGen
- Lab) YARA and yarGen
- Analyzing PE Files
- Lab) Analyzing PE Files
- Analyzing PDF Files
- Lab) Analyzing PDF Files
- Analyzing Office Files
- Lab) Analyzing Office Files
- Activity) Section Review

Domain 2: Malware Analysis (2/2)

Subject to change prior to launch, September 2021.

MA4) Dynamic Analysis

- Section Introduction
- Overview of Dynamic Analysis
- Sysinternals Introduction
- Sysinternals AutoRuns
- Sysinternals TCPView
- Lab) Utilizing Sysinternals
- Process Monitor and ProcDOT
- Lab) Monitoring Malicious Processes
- Online Analysis Tools
- Activity) Online Analysis Tools
- Anti-sandboxing Techniques
- Activity) Section Review

MA5) Analysis Practice

- Section Introduction
- Lab) Blackbox Analysis 1
- Lab) Blackbox Analysis 2
- Lab) Blackbox Analysis 3

Domain 4: Threat Hunting (1/3)

Subject to change prior to launch, September 2021.

TH1) Introduction to Threat Hunting

- Section Introduction
- Threat Hunting Explained
- Benefits of Hunting
- Threat Hunting Lifecycle
- Threat Intelligence
- MITRE ATT&CK
- Tools Covered
- Activity) Section Review

TH2) Setting up a Lab

- Section Introduction
- Lab Architecture
- Building Your Lab
- Kibana Interface
- Sigma and Elastalert
- Activity) Section Review

Domain 4: Threat Hunting (2/3)

Subject to change prior to launch, September 2021.

TH3) Endpoint Hunting

- Section Introduction
- Overview, Windows Systems
- Windows User Accounts
- Windows Program Execution
- Lab) Windows Program Execution
- Windows Network Connections
- Windows Services
- Windows Registry
- Windows Logging
- Hunting Event Logs With Chainsaw
- Lab) Hunting With Chainsaw
- Lab) Windows System Hunt
- Overview, Linux Systems
- Linux User Accounts
- Linux Network Connections
- Linux Processes
- Linux File Analysis
- Linux Automated Jobs
- Linux System Loggiing
- Lab) Linux System Hunt
- Activity) Section Review

TH4) Network Hunting

- Section Introduction
- OSI Model
- Common Protocols
- Infrastructure Considerations
- Packet Capturing Tools
- TCPDump
- Wireshark
- tshark
- Hunting Command and Control
- RITA For Beacon Detection
- Lab) Hunting Beacons with RITA
- Hunting PowerShell Empire
- Lab) Hunting Empire C2
- Activity) Section Review

TH5) Hunt Reflection and Reporting

Domain 4: Threat Hunting (3/3)

Subject to change prior to launch, September 2021.

TH5) Hunting at Scale

- Hunting at Scale
- Velociraptor Hunting: Introduction
- Velociraptor: Web GUI
- Velociraptor: VQL Explained
- Velociraptor: Hunting & Notebooks 1
- Velociraptor: Hunting & Notebooks 2
- Velociraptor: Summary
- Lab) Velociraptor Hunting
- GRR Hunting: Introduction
- GRR: Web GUI
- GRR: Flows and Hunts
- GRR: Hunt Walkthrough
- GRR: Summary
- Activity) Section Review

TH6) Hunt Reflection and Reporting

- Section Introduction
- DeTT&CT and Navigator
- Report Writing
- Detection Creation
- Lab) Detection Creation
- Threat Hunting Metrics
- Activity) Section Review

Domain 3: Advanced SIEM (1/2)

Subject to change prior to launch, September 2021.

AS1) Introduction to Advanced SIEM

- Section Introduction
- What is SIEM?
- SIEM Vendors
- Benefits of a SIEM
- SIEM and Automation
- SIEM and MITRE ATT&CK
- Tools Covered
- Why we Chose Splunk
- Activity) Section Review

AS2) SIEM Deployment

- Section Introduction
- SIEM Architecture
- Logs and Transportation
- Splunk CIM
- Storage, Retention, Aggregation
- Alerting With Sigma
- Activity) Section Review

AS3) Proactive SIEM

- Section Introduction
- Threat Hunting Lifecycle
- Proactive vs Reactive SIEM
- Splunk Threathunting App
- Searching for Threats
- Lab) Hunting & Analysis (Search & Reporting)
- Lab) Hunting and Analysis (ThreatHunting App)
- File Integrity Monitoring
- Activity) Section Review

Domain 3: Advanced SIEM (2/2)

Subject to change prior to launch, September 2021.

AS4) Adversary Emulation, Detection, and Analysis

- Section Introduction
- Adversary Emulation
- Threat Modelling and Planning
- Adversary Emulation Tools
- CALDERA and Operations
- Lab) Adversary Emulation
- Post-Emulation Activities
- Lab) Logging, Emulation, and Dashboards
- Command and Control Detection
- Lab) Command and Control Detection
- Activity) Section Review

Domain 1: Vulnerability Management (1/2)

Subject to change prior to launch, September 2021.

VM1) Introduction to Vulnerability Management

- Section Introduction
- Why is it Important?
- Explained: Risk
- Explained: Vulnerabilities
- Explained: CVEs
- Explained: CVSS
- Tools Covered
- Activity) Section Review

VM2) Host Discovery

- Section Introduction
- Maintaining an Asset Inventory
- Active Discovery, Nmap & Zenmap
- Activity) Scanme.nmap.org
- Lab) Active Discovery with Nmap/Zenmap
- Active Discovery, OpenVAS
- Lab) Active Discovery with OpenVAS
- Passive Host Discovery
- Activity) Section Review

VM3) Vulnerability Discovery

- Section Introduction
- How Scanners Work
- Scanning Considerations
- Passive Vulnerability Scanning
- Active Scanning - External
- Specialist Scanning - Web Servers
- Lab) Assessing a Web Server
- Specialist Scanning - WordPress
- Lab) Scanning with WPScan
- Active Scanning - Internal
- Lab) Assessing Internal Hosts
- Lab) Blackbox Assessment
- Activity) Section Review

Domain 1: Vulnerability Management (2/2)

Subject to change prior to launch, September 2021.

VM4) Analysis, Triage, and Threat Intelligence

- Section Introduction
- Why is Prioritization Important?
- What is Threat Intelligence?
- Exploitation Activity
- Asset Value
- Scan Triage and Analysis
- False Positives and Non Issues
- Lab) Scan Result Triage
- Activity) Exploitation Activity
- Activity) Section Review

VM5) Reporting and Remediation

- Section Introduction
- Reporting Considerations
- Reporting: Technical Audience
- Reporting: Non-Technical Audience
- Reporting: Metrics
- Mitigation: Patching
- Mitigation: Configuration
- Mitigation: Segmentation
- Mitigation: Intrusion Detection
- Lab) Vulnerability Remediation
- Activity) Section Review

Blue Team Level 2

Thank You!

We hope you have enjoyed reading our course syllabus, and we hope to see you in BTL2 soon! If you have any questions, please email us at **contact@securityblue.team**.

View BTL2 Info Page

Don't forget...

Earn Your BTL2 Coin!

Pass the exam to earn the silver challenge coin, or score 90% or above on your first attempt to get the gold coin.

CERTIFIED
Q29uZ3JhdHVsYXRpb25zIG9uIGJlY29taW5nIEJsdWUgVGVhbSBMZXZlbCAyIGNlcnRpZmllZA==
SBT
BLUE TEAM
LEVEL
2