Course Code: BTL1-01
Course Title: Blue Team Level 1 Certification

Contact Information

Lead Instructor: Joshua Beaman
Email: joshua@securityblue.team

Course Goals

To develop and test a student's knowledge of defensive cybersecurity practices and improve their practical ability to complete security operations tasks, making them a stronger defender.

Copyright Notice

Course Terms and Conditions

During the checkout process students **must** agree to the Refunds Policy and BTL1 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-paying 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.

BTL1: Security Fundamentals

This introduction domain is aimed at individuals that have little or no prior experience with cybersecurity and networking. These lessons are designed to create a foundation for the rest of the course, developing a student's understanding of soft skills, networking, security controls, and management principles.

Soft Skills: • Section Introduction • Communication • Teamwork • Problem Solving • Time Management • Motivation • Burnout, Imposter Syndrome, Alert Fatigue	**Networking 101:** • Section Introduction • Network Fundamentals • Network Devices • Ports and Services • **Activity)** Port Scanning with Nmap • **Activity)** End of Section Review
Security Controls: • Section Introduction • Physical Security • Network Security • Endpoint Security • Email Security • **Activity)** End of Section Review	**Management Principles:** • Section Introduction • Risk • Policies and Procedures • Compliance and Frameworks • **Activity)** End of Section Review

BTL1: Phishing Analysis

Phishing is the number one security risk faced by organizations and leads to the highest number of data breaches. Initially students will learn what phishing is, the different types of phishing attacks, tactics and techniques used by malicious actors. Then students will be taught how to analyze emails to retrieve important artifacts, perform analysis on these to determine the risk to the organisation, and suggest appropriate reactive and preventative defensive measures.

PA1) Introduction to Emails and Phishing:

- Section Introduction
- Phishing Analysis Glossary
- How Electronic Mail Works
- Anatomy of an Email
- What is Phishing?
- Impact of Phishing
- **Activity)** End of Section Review

PA2) Types of Phishing Emails:

- Section Introduction
- Recon
- Spam
- Credential Harvester
- Drive-by Download
- Social Engineering
- Vishing, Smishing
- Whaling
- False Positives
- **Video)** Types of Email Attacks and Examples
- **Activity)** Categorising Phishing Emails
- **Activity)** End of Section Review

PA3) Tactics and Techniques Used:

- Section Introduction
- Spear Phishing
- Impersonation
- Typo squatting and Homographs
- Sender Spoofing
- HTML Styling
- Attachment
- Hyperlinks
- URL-Shortening Services
- Use of Legitimate Services
- Business Email Compromise
- **Video)** Tactics and Techniques Examples
- **Activity)** Reporting on Tactics Used
- **Activity)** End of Section Review

PA4) Retrieving Artefacts:

- Section Introduction
- Artefacts we need to Collect
- Manual Collection – Email Artefacts
- Manual Collection – Web Artefacts
- Manual Collection – File Artefacts
- **Video)** Collecting Artefacts Manual Methods
- Automated Collection with PhishTool
- **Video)** Collect Artefacts Automated Methods
- **Activity)** Artefact Extraction
- **Activity)** End of Section Review

PA5) Analyzing Artefacts: • Section Introduction • Visualisation Tools • Artefact Reputation Tools • Interaction Tools • Analysis with PhishTool • **Video)** Artefact Analysis Walkthrough • **Activity)** Artefact Analysis • **Activity)** End of Section Review	**PA6) Taking Defensive Measures:** • Section Introduction • Preventative: Marking External Emails • Preventative: Email Security Technology • Preventative: Spam Filter • Preventative: Attachment Filtering • Preventative: Attachment Sandboxing • Reactive: Immediate Response Process • Reactive: Blocking Web-Based Artefacts • Reactive: Blocking File-Based Artefacts • Reactive: Blocking Email-Based Artefacts • Reactive: Informing Threat Intelligence Team • **Activity)** Selecting Appropriate Defensive Measures • **Activity)** End of Section Review
PA7) Report Writing: • Section Introduction • Email Header, Artefacts, and Body Content • Users Affected & Actions Taken • Analysis Process, Tools, and Results • Defensive Measures Taken • Lessons Learned • **Video)** Report Writing Walkthrough and Examples • **Activity)** Report Writing • **Activity)** End of Section Review	**PA8) Lessons Learned:** • Section Introduction • Identifying New Tactics • Response Improvements • **Activity)** End of Section Review
PA9) Phishing Response Challenge: • Section Introduction • **Video)** Phishing Response Walkthrough Video • Phishing Response Brief • **Activity)** Phishing Response	

BTL1v1 Syllabus. Copyright Security Blue Team 2020. Visit https://securityblue.team/why-btl1/

BTL1: Threat Intelligence

It's important for an organisation to understand the malicious actors that may target them, allowing for tailored defences to be implemented, increasing the resilience and slowing the attackers down, giving defenders more time to respond. In this domain students will learn what threat actors are, the naming conventions used to track them, and develop an understanding of operational, tactical, and strategic threat intelligence practices and knowledge. Finally, students will learn about different types of malware used by actors, and global campaigns such as Emotet and Magecart.

TI1) Introduction to Threat Intelligence: • Section Introduction • Threat Intelligence Glossary • Threat Intelligence Explained • Why Threat Intelligence can be Valuable • The Future of Threat Intelligence • Types of Intelligence • Further Reading	**TI2) Threat Actors and APTs:** • Section Introduction • Common Threat Agents • Actor Naming Conventions • Motivations • What are APTs? • Tools, Techniques, and Procedures • Activity) Threat Actor Research • Activity) End of Section Review
TI3) Operational Threat Intelligence: • Section Introduction • Indicators of Compromise Explained • Pyramid of Pain • Precursors Explained • Lockheed Martin Cyber Kill Chain • MITRE ATT&CK Framework • Attribution and its Limitations • Activity) End of Section Review	**TI4) Tactical Threat Intelligence:** • Section Introduction • Threat Exposure Checks Explained • Public Exposure Checks Explained • Watchlists/IOC Monitoring • Threat Intelligence Platforms • Malware Information Sharing Platform (MISP) • Activity) Deploying MISP • Activity) End of Section Review
TI5) Strategic Threat Intelligence: • Section Introduction • Intelligence Sharing and Partnerships • IOC/TTP Gathering and Distribution • OSINT vs Paid Sources • Activity) End of Section Review	**TI6) Malware and Global Campaigns:** • Section Introduction • Types of Malware Used by Threat Actors • Global Campaign: Emotet • Global Campaign: Magecart • Global Campaign: Trickbot • Global Campaign: Sodinokibi • Activity) End of Section Review

BTL1: Digital Forensics

Supply a description of any special course requirements, such as knowledge of specific software, and why it is necessary for successful completion of the course. Include software required to access course material or submit assignments such as Microsoft Word, SPSS, etc. Also include any hardware requirements for the course such as cameras, lab equipment, etc.

DF1) Introduction to Digital Forensics:

- Section Introduction
- Digital Forensics Glossary
- What is Digital Forensics?
- Digital Forensics Process
- Further Reading Material

DF2) Forensics Fundamentals:

- Section Introduction
- Introduction to Data Representation
- **Activity)** Data Representation
- Hard Disk Drive Basics
- Solid State Disk Basics
- File Systems
- **Activity)** File Systems
- Hashing and Integrity
- **Activity)** Hashing and Integrity
- Metadata and File Carving
- **Activity)** Metadata and File Carving
- Memory, Pagefile, and Hibernation File
- Digital Evidence and Handling
- Order of Volatility
- **Activity)** End of Section Review

DF3) Digital Evidence Collection:

- Section Introduction
- Equipment
- ACPO Principles of Digital Evidence and Preservation
- Chain of Custody
- Disk Imaging: FTK Imager
- Live Forensics
- Live Acquisition: KAPE
- Evidence Destruction
- **Activity)** End of Section Review

DF4) Windows Investigations:

- Section Introduction
- Windows Artifacts - Programs
- **Activity)** Windows Investigation 1
- Windows Artifacts – Internet Browsers
- **Activity)** Windows Investigation 2
- **Activity)** End of Section Review

DF5) Linux Investigations: • Section Introduction • Linux Artifacts – User Files • **Activity)** Hidden Files • Linux Artifacts - /Var/Lib and /Var/Log • Linux Artifacts – Passwd and Shadow • **Activity)** Password Cracking • **Activity)** End of Section Review	**DF6) Autopsy:** • Section Introduction • What is Autopsy? • Installing Autopsy • Autopsy Walkthrough • **Activity)** Autopsy Exercise
DF7) Volatility: • Section Introduction • What is Volatility? • Volatility Walkthrough • **Activity)** Volatility Exercise	

BTL1: Security Information and Event Management

Supply a description of any special course requirements, such as knowledge of specific software, and why it is necessary for successful completion of the course. Include software required to access course material or submit assignments such as Microsoft Word, SPSS, etc. Also include any hardware requirements for the course such as cameras, lab equipment, etc.

SI1) Introduction to SIEM: • Section Introduction • SIEM Glossary • Security Information Management • Security Event Management • What is a SIEM? • SIEM Platforms • Further Reading Material • **Activity)** End of Section Review	**SI2) Logging:** • Section Introduction • What is Logging? • Syslog • Windows Event Logs • Sysmon • Other Logs • **Activity)** Windows Event Analysis • **Activity)** End of Section Review
SI3) Aggregation: • Section Introduction • Log Aggregation Explained • **Activity)** End of Section Review	**SI4) Correlation:** • Section Introduction • Normalization and Processing • Regex • SIEM Rules • **Activity)** Regex Writing • **Activity)** End of Section Review
SI5) Analysis: • Section Introduction • **Activity)** Installing Splunk • **Activity)** Importing BOTSv3 • Splunk Crash Course • **Activity)** Splunk Scenario Easy • **Activity)** Splunk Scenario Easy • **Activity)** Splunk Scenario Medium • **Activity)** Splunk Scenario Medium • **Activity)** Splunk Scenario Hard	

BTL1: Incident Response

Supply a description of any special course requirements, such as knowledge of specific software, and why it is necessary for successful completion of the course. Include software required to access course material or submit assignments such as Microsoft Word, SPSS, etc. Also include any hardware requirements for the course such as cameras, lab equipment, etc.

IR1) Introduction to Incident Response:

- Section Introduction
- Incident Response Glossary
- What is Incident Response?
- Why is Incident Response Needed?
- Security Events vs. Security Incidents
- CSIRT and CERT Explained
- Incident Response Lifecycle (NIST)
- Lockheed Martin Cyber Kill Chain
- MITRE ATT&CK Framework
- Further Reading Material
- **Activity)** End of Section Review

IR2) Introduction to Incident Response:

- Section Introduction
- Preparation: Incident Response Plan
- Preparation: Incident Response Teams
- Preparation: Asset Inventory and Risk Assessments
- Prevention: DMZ
- Prevention: Host Defenses
- Prevention: Network Defenses
- **Activity)** Setting up a Firewall
- Prevention: Snort
- **Activity)** Deploying Snort
- Prevention: Email Defenses
- Prevention: Physical Defenses
- Prevention: Human Defenses
- **Activity)** End of Section Review

IR3) Detection and Analysis:

- Section Introduction
- Common Events and Incidents
- Baselines and Behavior Profiles
- Introduction to Wireshark (GUI)
- Introduction to Wireshark (Analysis)
- **Activity 1)** PCAP Analysis
- **Activity 2)** PCAP Analysis
- **Activity 3)** PCAP Analysis
- **Activity)** End of Section Review

IR4) Containment, Eradication, Recovery:

- Section Introduction
- Incident Containment
- Taking Forensic Images
- Identifying and Removing Malicious Artifacts
- Identifying Root Cause and Recovery
- **Activity)** End of Section Review

IR5) Lessons Learned: • Section Introduction • What Went Well? • What Can be Improved? • Importance of Documentation • Metrics and Reporting	