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
  - Section Introduction, Management Principles
  - Risk
  - Policies and Procedures
  - Compliance & Frameworks
  - Activity) End of Section Review, Management Principles

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

Compliance & Frameworks

Organizations need to follow security frameworks to reach a minimum standard of security, and businesses operating in specific industries will also need to comply with other legislation and regulations. This lesson will cover what compliance is, commonly-followed frameworks and standards, and why it's important not just to protect the business, but also to maintain a high level of trust with clients.

You can read more information about the different compliance frameworks we cover below by clicking on the "Materials" tab at the top of this lesson!

WHAT IS COMPLIANCE?

Compliance is defined as following rules and meeting requirements for specified frameworks. Organizations operating in different industries will have specific compliance frameworks that they need to comply with. For example, businesses that process or store data on citizens of the European Union (EU) will need to comply with the General Data Protection Regulation (GDPR), while organizations that process card payments will need to meet the requirements of the Payment Card Information Data Security Standard (PCI DSS). We will cover both of these and more below.

WHY IS IT IMPORTANT?

Not only does following compliance frameworks increase trust between customers and partners, it is also often a legal requirement, and not complying would result in legal and regulatory fines. Following these frameworks ensures that the organization has a good level of security, making it better equipped to respond to security events and incidents, reducing risk and impact.

GDPR

The **General Data Protection Regulation (GDPR)** is a regulation in EU law on data protection and privacy in the European Union (EU) and the European Economic Area (EEA). It also addresses the transfer of personal data outside the EU and EEA areas, with the primary aim to give control to individuals over their personal data.

Controllers and processors of personal data must put in place *appropriate technical and organizational measures* to implement the data protection principles. Business processes that handle personal data must be designed and built with consideration of the principles and provide safeguards to protect data (for example, using pseudonymization or full anonymization where appropriate). Data controllers must design information

TI4) Tactical Threat Intelligence
7 Topics | 2 Quizzes
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 | 3 Quizzes
IR3) Detection and Analysis Phase
7 Topics | 5 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

systems with privacy in mind, for instance, use the highest-possible privacy settings by default, so that the datasets are not publicly available by default, and cannot be used to identify a subject. No personal data may be processed unless this processing is done under one of six lawful bases specified by the regulation (consent, contract, public task, vital interest, legitimate interest, or legal requirement). When the processing is based on consent the data subject has the right to revoke it at any time.

Data controllers must clearly disclose any data collection, declare the lawful basis and purpose for data processing, and state how long data is being retained and if it is being shared with any third parties or outside of the EEA. Data subjects have the right to request a portable copy of the data collected by a controller in a common format, and the right to have their data erased under certain circumstances. Businesses must report data breaches to national supervisory authorities within 72 hours if they have an adverse effect on user privacy. In some cases, violators of the GDPR may be fined up to €20 million or up to 4% of the annual worldwide turnover of the preceding financial year in case of an enterprise, whichever is greater.

ISO 27001

ISO/IEC 27001 is an information security standard, part of the ISO/IEC 27000 family of standards, of which the last version was published in 2013, with a few minor updates since then. It is published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) under the joint ISO and IEC subcommittee.

ISO/IEC 27001 specifies a management system that is intended to bring information security under management control and gives specific requirements. Organizations that meet the requirements may be certified by an accredited certification body following the successful completion of an audit.

PCI DSS

The **Payment Card Industry Data Security Standard** (**PCI DSS**) is a security standard for organizations that handle branded credit cards from the major card schemes. The PCI Standard is mandated by the card brands but administered by the Payment Card Industry Security Standards Council. The standard was created to increase controls around cardholder data to reduce credit card fraud.

Validation of compliance is performed annually or quarterly, by a method suited to the volume of payment transactions handled:

- **Self-Assessment Questionnaire (SAQ)** — smaller volumes
- **External Qualified Security Assessor (QSA)** — moderate volumes
- **Firm-specific Internal Security Assessor (ISA)** — larger volumes; involves issuing a Report on Compliance

HIPAA

Health Insurance Portability and Accountability Act (HIPAA) is a regulation intended to help covered entities and their business associates protect Electronic Protected Health Information (ePHI). The U.S. Department of Health and Human Services (HHS) outlines who HIPAA applies to in their definition of a covered entity. HIPAA applies to companies that provide services that would use e-PHI such as suppliers or outsourced IT providers.

The primary goal of HIPAA is to protect ePHI which includes, name, dates such as birth, admission, discharge, death, telephone number, SSN, photographs, address, etc. Companies under this regulation will need to implement technical and procedural controls to protect this information and perform risk analysis on risk and vulnerabilities to the confidentiality, integrity, and availability of ePHI. Technical controls include such things as encryption, authentication, password complexity, access auditing, segmentation, etc., and procedural controls include such things as password policies, incident response plans, contingency plans, and audit procedures.

How to start your Exam

Previous Topic

Back to Lesson

Next Lesson

Privacy & Cookies Policy

Privacy - Terms