

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

○ Section Introduction, Actors

○ Common Threat Agents

○ Motivations

○ Actor Naming Conventions

○ What are APTs?

○ Tools, Techniques, Procedures

□ Activity) Threat Actor Research

□ Activity) End of Section Review, Actors

○ TI3) Operational Threat Intelligence

● 7 Topics 1 Quiz

○ TI4) Tactical Threat Intelligence

● 7 Topics 1 Quiz

○ TI5) Strategic Threat Intelligence

Actor Naming Conventions

Blue Team Level 1 Certification (Standard) > TI2) Threat Actors & APTs > Actor Naming Convent...

IN PROGRESS



Different threat intelligence vendors or security firms use their own naming conventions to track and share intelligence about malicious actors. All of the naming conventions can quickly become very confusing, as different organizations will use different names for the same groups, and some vendors may have multiple names for one single group – and this issue isn't going to go away anytime soon.

Another issue with naming and attribution, in general, is that threat actors tend to share tools, so that indicators from one group may be the same as multiple other groups. Some groups even try to use infrastructure in other countries to throw security researchers off, as well as copying the tactics and techniques used by other groups.

In this lesson, we're going to covering the two most popular naming conventions created by CrowdStrike and FireEye/Mandiant.



CROWDSTRIKE

CrowdStrike likes to categorize APTs based on the countries they operate out of, especially nation-state hacking teams, by using animals. For example, "Panda" is the umbrella term for all nation-state activity tied to the People's Republic of China. Non-nation-state adversaries are categorized not by location but by intention; for instance, activist groups like the Syrian Electronic Army, are categorized as "Jackal," which expresses intent and motivation instead of country. Below is a diagram showing the adversary animal and the affiliation the group has (E-Crime, Hacktivist, or Nation State). We will cover these in more detail below and provide examples of different groups. If you want to read more about the malicious actors that CrowdStrike tracks, read this blog post by them, titled "[Meet The Adversaries](#)".

Adversary	Category or Nation-State
SPIDER	E-CRIME
CHOLLIMA	DEMOCRATIC PEOPLE'S REPUBLIC OF KOREA (NORTH KOREA)
JACKAL	HACKTIVIST
TIGER	INDIA
KITTEN	IRAN
LEOPARD	PAKISTAN
PANDA	PEOPLE'S REPUBLIC OF CHINA
BEAR	RUSSIAN FEDERATION
CRANE	SOUTH KOREA
DHUCAL	MYTHICAL

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

Nation-State-Based Adversaries

Below we have listed the countries and their associated animals, as stated by CrowdStrike. We have also included some examples of APTs that have been linked to those countries.



Bear = Russia (Such as [Fancy Bear](#))



Buffalo = Vietnam



Chollima = North Korea (Such as [Stardust Chollima](#))



Crane = South Korea



Kitten = Iran (Such as [Refined Kitten](#))



Leopard = Pakistan (Such as [Mythic Leopard](#))



Panda = China (Such as [Goblin Panda](#))



Tiger = India (Such as [Viceroy Tiger](#))

Non-Nation-State Adversaries

The below names are given to hacktivist groups and groups that conduct eCrime, such as ransomware attacks and using banking trojans.

- **Jackal** = Activist groups
- **Spider** = Criminal groups, such as [Mummy Spider](#), the actors behind the global malware campaign Emotet (more on this in the Global Malware Campaigns section at the end of this domain).

MANDIANT

FireEye/Mandiant have taken a different approach and use the term “APTxx” where xx is a number, such as APT28 or APT39. These numbers actually have a meaning behind them – they are taken from internal country codes, providing a more concise and neat naming convention (*but hey, CrowdStrike names sound much cooler – sorry Mandiant!*).

Nation-State-Based Adversaries



China = [APT1](#), [APT2](#), [APT3](#), [APT10](#), [APT19](#), [APT20](#), [APT30](#),



[APT40](#), [APT41](#)



Iran = [APT33](#), [APT34](#), [APT35](#), [APT39](#)



North Korea = [APT37](#), [APT38](#)



Russia = [APT28](#), [APT29](#)



Vietnam = [APT32](#)

Financially-Motivated Cybercrime Groups

Under FireEye/Mandiant's naming convention, instead of using the term "APT" for cybercrime groups, the prefix "FIN" is used, short for "Financial", referring to the motivation for cybercrime actors. An example of this naming convention in use is [FIN7](#), a threat group that has primarily targeted the U.S. retail, restaurant, and hospitality sectors since mid-2015, often utilizing point-of-sale malware to steal funds.

- [FIN4](#)
- [FIN5](#)
- [FIN6](#)
- [FIN7](#)
- [FIN8](#)
- [FIN10](#)

Unclassified Groups

Groups that are currently undergoing analysis are referred to as "UNC" or Unclassified under the FireEye/Mandiant naming convention. Groups that have not been attributed to a country, or their motives are still unclear, will be placed into this group temporarily.

[< Previous Topic](#)[Mark Complete ✓](#)[Back to Lesson](#)[Next Topic >](#)[Privacy & Cookies Policy](#)