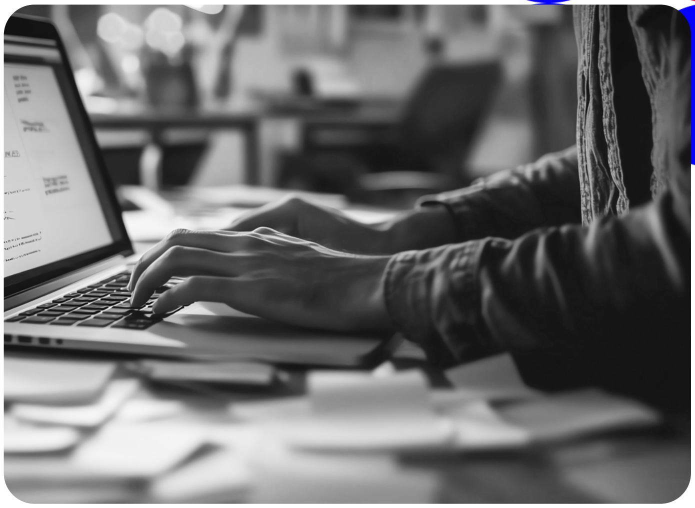
Recorded Future® | DATA SHEET

Certified Analyst Lab

Recorded Future
certification training



About the Certification

The Certified Analyst Lab enables analysts to answer difficult information security research questions. Through creative thinking, problem-solving, and analytical skills, attendees will unlock the full potential of the Recorded Future® Platform, locate relevant data, create information, and generate intelligence using advanced workflows.

Course Objectives

After attending the Certified Analyst Lab, a learner will be able to:

- Utilize the Recorded Future Platform to fulfill your organization's Intelligence Requirements (IRs)
- Extract and analyze intelligence using frameworks such as the Cyber Kill Chain, MITRE ATT&CK, and the Diamond Model
- Enhance intelligence collection and analysis processes
- Utilize the Advanced Query Builder to identify relevant threats, including credential leaks, vulnerabilities affecting your technology stack, and threats to your brand and infrastructure
- Analyze and visualize data references to uncover trends pertinent to your organization
- Proactively identify and prioritize threats using Recorded Future tools such as Recorded Future AI, Threat Map, and Sandbox
- Create Analyst Notes and effectively disseminate findings with stakeholders
- Identify and understand the intersection of cyber threats and geopolitical issues

Learner experience

- Expert-led instruction
- Interactive group discussions
- Hands-on exercises with real security scenarios
- Daily knowledge assessments
- Comprehensive final examination
- 24 CPE credits

Prerequisites

- A Recorded Future license
- Threat intelligence module for the enterprise
- Brand intelligence and vulnerability intelligence is recommended but not required
- Getting started with threat intelligence webinar
- Threat intelligence for beginners eLearning

Sample Agenda

All times are approximate and subject to change

Day 1

Time	Session
8:45 AM	Virtual classroom opens for technical setup and informal networking
9:00 AM	Lesson 0: Introduction & Fundamentals
10:00 AM	Lesson 1: Data to Action
12:30 PM	Lunch Break
1:30 PM	Lesson 1: Data to Action Continued
3:00 PM	Lesson 2: Prioritizing Threats
4:30 PM	End of Day Wrap Up

Day 2

Time	Session
8:45 AM	Virtual classroom opens for technical setup and informal networking
9:00 AM	Day 1 Recap
9:30 AM	Lesson 3: Investigating Leaked Credentials
11:30 AM	Lesson 4: Investigating Threats to Brand & Infrastructure
12:30 PM	Lunch Break
1:30 PM	Lesson 4: Investigating Threats to Brand & Infrastructure Cont
2:00 PM	Lesson 5: Investigating Vulnerabilities
4:30 PM	End of Day Wrap Up

Day 3

Time	Session
8:45 AM	Virtual classroom opens for technical setup and informal networking
9:00 AM	Day 2 Recap
9:30 AM	Lesson 6: Threat Hunting Part 1
11:30 AM	Lesson 7: Threat Hunting Part 2
12:30 PM	Lunch Break
1:30 PM	Lesson 7: Threat Hunting Part 2
2:30 PM	Lesson 8: Aligning the Geopolitical & Cyber Domains
4:30 PM	End of Day Wrap Up

Lesson Details

01: Data to Action: Advanced Query Builder Best Practices

This lesson explores the Advanced Query Builder, the primary vehicle for surfacing information in this course.

Lesson Objectives:

- Utilize all three sections of the Advanced Query Builder to surface relevant information and create custom alerts
- Surface references using free text searching
- Employ Event Types in queries to surface relevant information
- Visualize references in various ways to analyze and export for reporting
- Effectively use Recorded Future AI to summarize and surface key contextual information
- Author analyst notes to share findings and verdicts with team members
- Organize your custom content using Link Collections

02: Prioritizing Threats: Threat Landscapes

This lesson will detail tools like the Threat Map to prioritize investigations and recommend appropriate next actions.

Lesson Objectives:

- Understand the Importance of Threat Landscaping
- Create a simple Threat Landscape using the Advanced Query Builder
- Curate and maintain appropriate Watch Lists that power the Threat Map
- Utilize the Threat Map to quickly Identify priority Threat Actors & Malware, their motives, tactics, and risk to an organization
- Create a report based on the landscape with detection and mitigation procedures based on operational risk

03: Investigating Leaked Credentials

This lesson demonstrates how to use the Recorded Future Platform to proactively defend against the risk of compromised credentials.

Lesson Objectives:

- Articulate how and where threat actors acquire legitimate credentials
- Create an Advanced Query investigating credential leaks on the Dark Web
- Examine cached content to gain further understanding and insight of Dark Web activity
- Discuss sourcing best practices when surfacing information
- Utilize sourcing best practices when constructing custom queries

04: Investigating Threats to Brand and Infrastructure

In this lesson, you will learn to construct and optimize advanced queries to identify various threats. Additionally, you will master the creation of custom alerts derived from queries for prompt analysis and response.

Lesson Objectives:

- Articulate why Brand Protection is a vital component of modern-day security operations
- Construct and optimize Advanced Queries to reduce the risk of Typosquats, Similar Domain Registrations, Logo Abuse on False Login Pages, and Subdomain Takeovers
- Create custom alerts from queries for analysis and response

05: Investigating Vulnerabilities

This lesson will discuss how to use the Recorded Future Platform to surface relevant information in order to defend against exploited vulnerabilities in your tech stack.

Lesson Objectives:

- Articulate why monitoring for vulnerabilities is an essential component of security operations
- Define and discuss the Vulnerability Lifecycle
- Discuss how Threat Actors share and validate Proof of Concept code
- Identify relevant portions of a Vulnerability Intelligence Card to make Vulnerability Management efficient
- Examine evidence of Risk Scores within Risk Rules

06: Threat Hunting with the Recorded Future Platform Part I

This lesson (the first of two) is dedicated to using the Recorded Future Platform to surface TTPs and IOCs of relevant threats to your organization.

Lesson Objectives:

- Employ the Diamond Model to map specific aspects of threats to your organization
- Introduce a repeatable threat-hunting process to automate Threat Intelligence
- Employ the Recorded Future Sandbox to analyze malware samples
- Search for and implement detection rules written by Insikt Group and Open Sources
- Utilize Recorded Future Intelligence Kits as foundations for investigations

07: Threat Hunting with the Recorded Future Platform Part II

In a continuation of the previous lesson, in this section, you will learn about utilizing the Advanced Query Builder to surface MITRE Att&CK Identifiers for TTPs of interest.

Lesson Objectives:

- Discuss the MITRE ATT&CK Framework as a way to identify gaps in your environment
- Employ Research and Analysis from the Insikt Group to aid investigations
- Identify Indicators of Compromise (IOCs) using TTP Analysis and potential C2 Communications using Infrastructure Analysis
- Utilize the Malicious Traffic Analysis to identify malicious traffic from within your organizations

08: Aligning the Geopolitical and Cyber Domains

In this lesson, you will learn to identify the convergence of cyber threats and geopolitical issues and understand how to leverage both the Threat Intelligence and Geopolitical Intelligence Modules to enhance your analysis.

Lesson Objectives:

- Identify when Cyber Threats and Geopolitical issues converge
- Understand how the Threat and Geopolitical Intelligence Modules can complement each other
- Understand how to use the Cyber Attack Event Type
- Demonstrate using Multi-Section queries in analysis