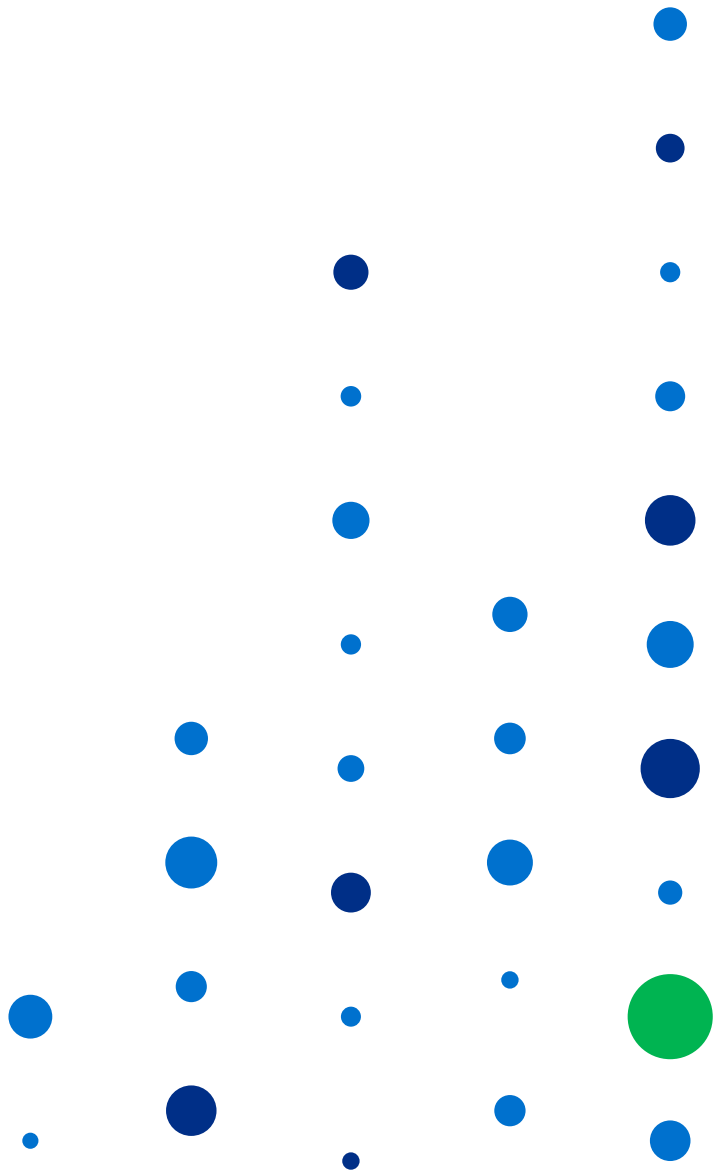
Recorded Future

# Recorded Future Certified Analyst Lab and Examination

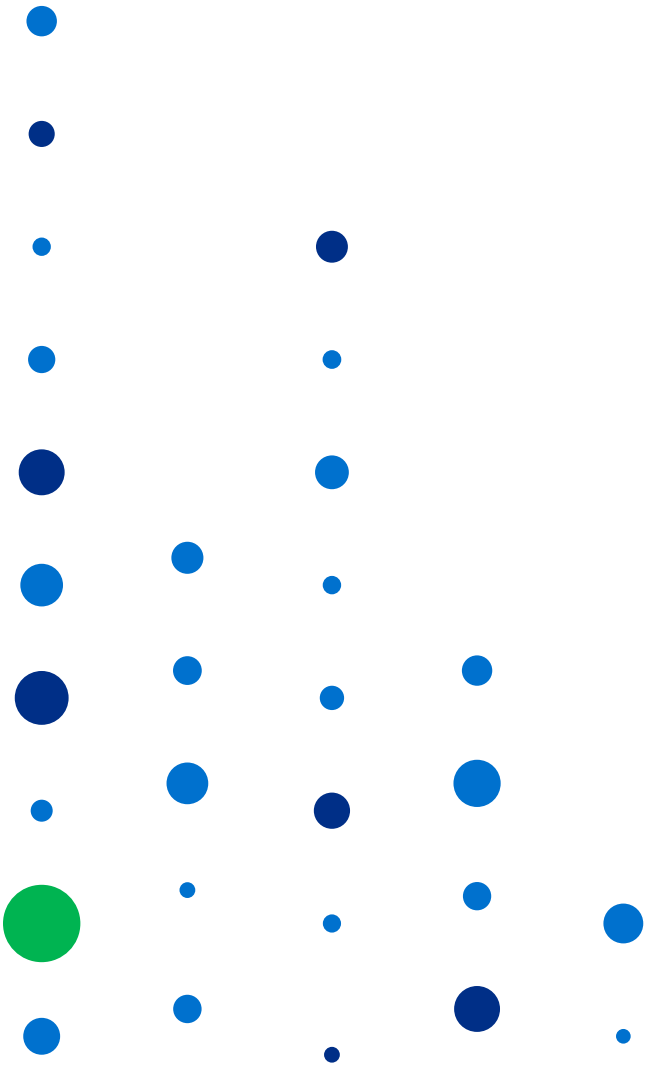


## Overview

Recorded Future aims to provide the best threat intelligence training services, period.

Our threat intelligence seminar trains analysts, security engineers, and users in common threat intelligence principles and fundamentals. We discuss common frameworks for intelligence analysis, including threat intelligence sources and our proprietary Intel Goals for security teams. Recorded Future features are reviewed, including Threat Views, Intel Cards, data structure, and exports. The seminar also covers practical exercises in progressively deeper analytical research and data exploration.

The certification is a practical examination by Recorded Future senior threat intelligence analysts, in line with pre-established criteria for determining proficiency in Recorded Future. Successful candidates will demonstrate clear and thorough knowledge of threat intelligence principles through the configuration of Threat Views, data visualization and export, and successfully identifying necessary information from a set of intelligence requirements, all within a given time. Successful candidates will receive a certificate of course completion, Recorded Future Certified Analyst numbered certificate, and a Recorded Future Certified Analyst emblem to use on their physical and digital resume.



Recorded Future

## Success Criteria

A successful candidate will demonstrate:

- The ability to define threat intelligence concepts and terms, including sources, methods, threat vectors, threat actors, vulnerabilities, assets, and risks.
- Familiarity with common threat models and ontologies, including the Intelligence Cycle, Cyber Kill Chain, the Diamond Model, and the Pyra mid of Pain.
- Working comprehension of analysis fundamentals, process, and analytic methods, including opportunity analysis, lynchpin analysis, and Analysis of Competing Hypotheses.
- Functional understanding of open source information and intelligence resources, including technical reporting, open source tools and sites, news sources, social media, and community-oriented reporting resources, such as VirusTotal and Malwr.com.
- Competency in Recorded Future product navigation, iconography, features, and support resources.
- Proficiency in configuring Recorded Future toward your organization's strategic, tactical, and operational goals.
- Conceptual understanding of industry best practices for integrating Recorded Future data in SIEMs, TIPs, ticketing systems, and other security applications.
- Working knowledge of Global Threat Views, including the purpose and constraints of columns and cyber threat signal.
- Configuration of Threat Views using Watch Lists, including threat monitoring of a brand, software assets, logical assets, industry vertical, and relevant cyberattack attributes, including attackers, threat vectors, vulnerabilities, targets, and named operations.
- Working knowledge of Intel Cards, including risk scoring and risk rules, reference counts, context entities, pivots to visualizations, and data exporting options.
- Setup and use of OMNI Intel Partner Extensions within applicable Intel Cards, including Intel Partner organizations and capabilities.
- Strong proficiency with the Recorded Future table view and orienting the reference table to identify key references and entities of interest via the entity tree.
- Proficiency in orienting and annotating the timeline view through group and color settings and modifying the timeline of events.
- An understanding of Source Map, including major source types in Recorded Future, sources and authors, and language collection.
- Working competency of Search and Advanced Search to surface appropriate IOCs, vulnerabilities, malware, and threat actor Intel Cards. Research and enhance pivots from pre-built queries and modifying queries for clarity

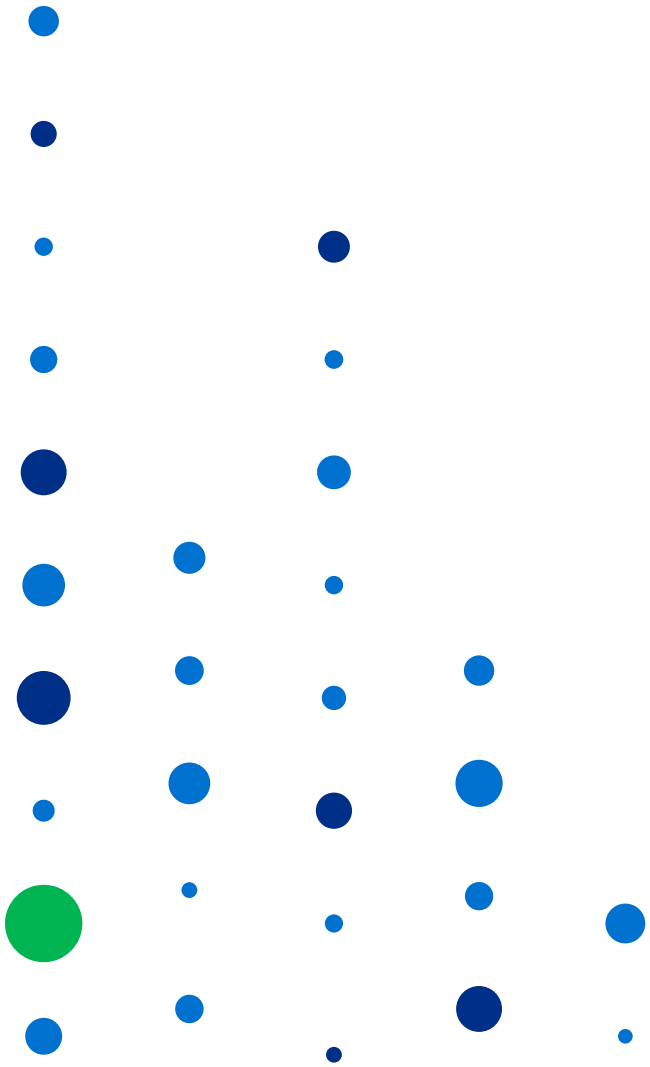
# Agenda

## Day 1

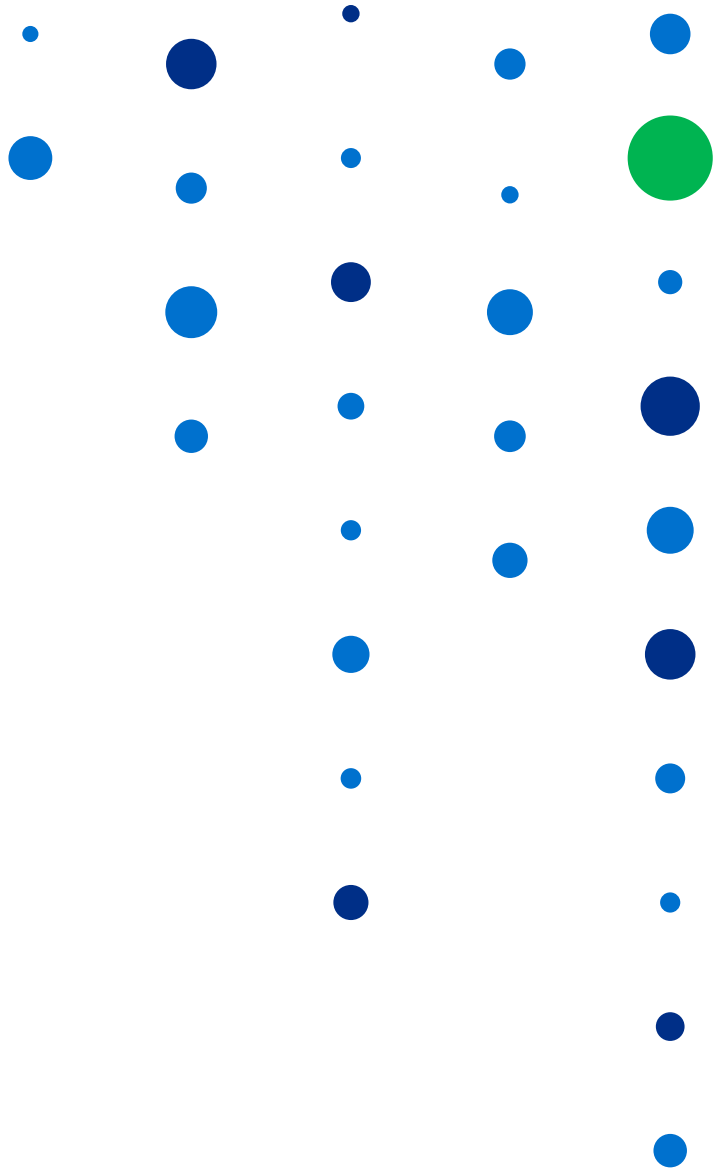
08:00 - 9:00 Breakfast (Provided)
08:30 - 9:00 Course Overview and Team Assignments
09:00 - 9:30 Session 1: Lists and Ontologies
09:30 - 11:00 Practicum 1: Enrich IOCs
11:00 - 11:30 Session 2: Machine Learning and Language
11:30 - 12:00 Practicum 2: Monthly Threat Roundup
12:00 - 13:00 Lunch (Provided)
13:00 - 14:00 Practicum 2 (con't): Monthly Threat Roundup
14:00 - 14:45 Session 3: Mastering Queries
14:45 - 16:00 Practicum 3: Event Alerting
16:00 - 17:00 Session 4: Threat Hunting

## Day 2

08:00 - 09:00 Breakfast (Provided)
08:30 - 09:00 Day 1 Review
09:00 - 10:30 Practicum 4: Malware Research
10:30 - 11:00 Session 5: Actor Profiling
11:00 - 12:00 Practicum 5: Closed Source Criminal Research
12:00 - 13:00 Lunch (Provided)
13:00 - 13:30 Session 6: Integration
13:30 - 14:00 Exam Review
14:00 - 17:00 Certification Exam



Recorded Future



Recorded Future

www.recordedfuture.com

@RecordedFuture

## About Recorded Future

Recorded Future arms security teams with the only complete threat intelligence solution powered by patented machine learning to lower risk. Our technology automatically collects and analyzes information from an unrivaled breadth of sources and provides invaluable context in real time and packaged for human analysis or integration with security technologies.