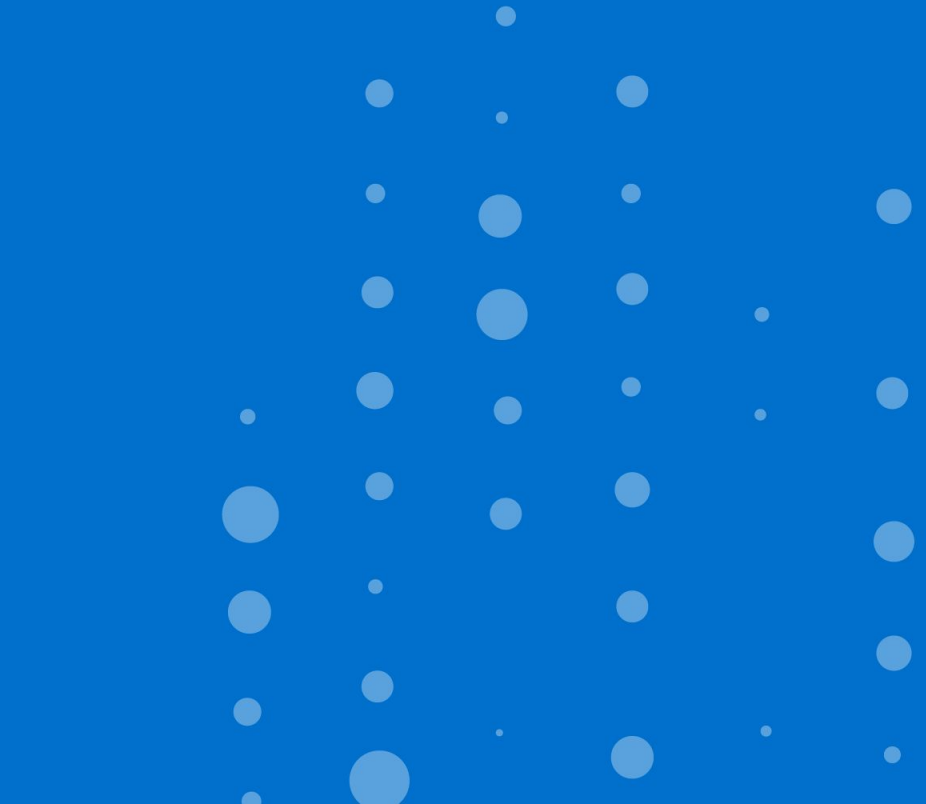
4/13/2018

Certified Analyst Program
Infosheet

Vast Intelligence, Focused Insights.

Contents

Executive Summary



Recorded Future

Executive Summary

- What is Recorded Future?
  - **Recorded Future is a SaaS Threat Intelligence Provider** that collects, analyzes, and contextualizes information from open, technical, and deep/dark web sources

- What is the Recorded Future Certified Analyst Program?
  - The Certified Analyst Program is a **competency-based training program** designed to provide cybersecurity analysts with **deep expertise in threat intelligence**.

- Why should my organization invest in this training?
  - Certified analysts help your organization advance its cyber security posture by **fully incorporating threat intelligence into the decision-making process**
  - Certified analysts **perform collection and analysis tasks significantly faster**, saving time and money while increasing the speed at which you can address threats
  - Certified analysts create C-Level-ready **reports that clearly demonstrate the organization's readiness to address critical cyber threats**

Executive Summary

- What is covered in the Program?
  - **Threat intelligence fundamentals**, including sources, methods, threat vectors, threat actors, vulnerabilities, assets, and risk
  - Fundamentals of **common threat models** and ontologies, including the Intelligence Cycle, Cyber Kill Chain, the Diamond Model, and the Pyramid of Pain
  - Knowledge of **analysis methodology**, 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
  - Creation of complex queries and searches for **advanced Recorded Future use cases**
  - Configuration of **customized Recorded Future product features**, including threat views, alerts, and advanced data exporting
  - **How to apply Recorded Future to achieve your organization's strategic, tactical, and operational security goals**

Executive Summary

Who is the CAP for?

- SOC Analysts
- SOC Management
- Threat Intelligence Teams
- Incident Response
- IT Teams
- Cyber Security Professionals

Are there follow-up trainings?

- Instructor-led Product Trainings
- Recorded Future Certified Architect

Recorded Future

Before Certified Analyst Program

Threat Intelligence Maturity

	1	2	3	4	5
PEOPLE	No threat intel resources	No dedicated threat intel analysts/Some distributed resources "Wear many hats"	Multiple siloed security teams (IR, VMT, SOC)	Threat analyst team (1-5 analysts)	Mature threat analyst team (5+ analysts)
DATA SOURCES	No Feeds/ relying on Google	Free feeds/gov feeds	Paid feeds (ex, ISAC) and/or paid reports	Multiple intelligence providers (ex. PhishMe)	Internally-originated intelligence/actionable
SECURITY SOLUTIONS	MSSP	Firewalls	Multiple tools into SIEM	Proactive alerting and Incident response	Threat Hunting, Vuln Mgmt, Deep analysis (ex. phantom, maltego)
WORKFLOW	N/A	Manual and ad-hoc collection; not centrally managed and maintained	Integrated - with SOC tools	Integrated with multiple security tools	Fully integrated into a proactive security program

After Certified Analyst Program

	1	2	3	4	5
PEOPLE	No threat intel resources	No dedicated threat intel analysts/Some distributed resources "Wear many hats"	Multiple siloed security teams (IR, VMT, SOC)	Threat analyst team (1-5 analysts)	Mature threat analyst team (5+ analysts)
DATA SOURCES	No Feeds/ relying on Google	Free feeds/gov feeds	Paid feeds (ex, ISAC) and/or paid reports	Multiple intelligence providers (ex. PhishMe)	Internally-originated intelligence/actionable
SECURITY SOLUTIONS	MSSP	Firewalls	Multiple tools into SIEM	Proactive alerting and incident response	Threat Hunting, Vuln Mgmt, Deep analysis (ex. phantom, maltego)
WORKFLOW	N/A	Manual and ad-hoc collection; not centrally managed and maintained	Integrated - with SOC tools	Integrated with multiple security tools	Fully integrated into a proactive security program

Training Framework

Training Framework

- Program Objective
  - The Recorded Future Certified Analyst Program expands organizations' cybersecurity programs by teaching analysts the collection, analysis, and reporting skills necessary to integrate Recorded Future threat intelligence into tactical processes and achieve strategic outcomes.

- Core Knowledge
  - The Certified Analyst Program allocates half of its duration to foundational core knowledge and best practices in threat intelligence that can be applied right away to make an immediate impact after day one.

- Product Training
  - The Certified Analyst Program is the most advanced Recorded Future product training available, and empowers analysts to fully utilize and implement advanced features, use cases, and reporting within the product.

Core Knowledge

Threat Intelligence = Counterintelligence

(θrɛ́t ɪ̀ntɛ́lədʒəns) *noun*. 1. Protecting one's operations from penetration or disruption by hostile organizations or individuals. 2. The process and product resulting from the interpretation of raw data into information that meets a requirement as it relates to the adversaries that have the intent, opportunity and capability to do harm. 3. Nothing more than the application of intelligence principles and tradecraft to information security.

Fundamentals

def. (fə̀ndəmɛ́ntəlz) tenets of a craft which never go stale

1. **Intelligence informs decisions.**
2. **Adversaries are distinctly human.**
3. **Threats must have <u>Opportunity</u>, <u>Intent</u>, and <u>Capability</u>.**

Framework for Threat Intelligence Security Program

IDENTIFY

Gain comprehensive view of threats that could really target the organization

PROTECT

Align security investments to current and future threats targeting the organization

DETECT

Leverage knowledge of attack patterns to hunt for threats

RESPOND

Research incidents for faster, more complete response

RECOVER

Identify stolen information and remediate quickly to reduce damage to the business

Course Structure, Learning Outcomes, and Skills List

Recorded Future

Course Structure

Day 1	
8:00 - 9:00am	*Optional*: Setup Assistance
9:00 - 9:30am	Introduction to Recorded Future
9:30 - 12:00n	Session 1: Overview + Indicators of Compromise
12:00 - 1:00pm	Lunch Break
1:00 - 3:00pm	Session 2: Threat Roundup
3:00 - 3:15pm	Break
3:15 - 5:00pm	Session 3: Event Alerting
5:00 - 6:00pm	*Optional*: Product Follow-up

Day 2	
8:00 - 9:00am	*Optional*: Day 1 Review
9:00 - 10:30am	Session 4: Malware Research
10:30 - 10:45am	Break
10:45 - 12:00n	Session 5: Closed Source Criminal Research
12:00 - 1:00pm	Lunch Break
1:00 - 2:30pm	Session 6: Integrations
2:30 - 3:00pm	Break + Exam Review
3:00 - 5:00pm	Certified Analyst Exam

Learning Outcomes

	Learning Objective	Module Fulfilled
1	Explain the role of threat intelligence in a proactive security program	Introduction
2	Analyze the role of ontologies in cyber analysis	Introduction
3	Apply threat intelligence lists to reduce security risk	Introduction
4	Identify indicators of compromise associated with Malware	Assignment 1
5	Analyze the collection process for security data	Session 1
6	Apply advanced techniques to build queries	Session 1
7	Identify cybersecurity events and references	Session 2
8	Develop a threat landscape report of relevant cybersecurity events	Assignment 2

Learning Outcomes II

	Learning Objective	Module Fulfilled
9	Create alerts on specific cybersecurity events	Assignment 3
10	Apply threat hunting techniques to identify threat actors and TTPs	Session 3
11	Analyze malware for incident response	Assignment 4
12	Identify and track threat actors	Session 4
13	Research actors on criminal forums	Assignment 5
14	Evaluate an organization’s risk level against a threat actor	Module 5
15	Evaluate Recorded Future integrations into industry-leading tools	Module 6

Skills List

- Threat intelligence Fundamentals
  - Entities
  - References
  - Sources
  - Watch Lists
  - Link Collections
  - White Lists
  - Threat Lists
- Ontologies
- Indicators of Compromise
  - Research
  - Identify association with malware
- Data Collection
  - Natural language processing
  - Machine learning
- Recorded Future Threat Views
- Building Queries (Basic and Advanced)
- Threat Landscape Reports
- Cyber Events and References
- Threat and Event Alerting
  - Protect proprietary assets
  - Protect exploits to vulnerabilities
  - New TTPs
- Threat Hunting
  - Identify threat actors and TTPs
  - Identify associated malware
  - Profile threat actors
- Malware Research
  - Malware telemetry connections
  - Identify host and network artifacts, binaries
  - Write YARA rules for infected endpoints
- Closed Source Criminal Research
  - Identify actors, associates, and tools used
  - Assess actor's risk level
- Integrations
  - SIEMs
  - RF browser extension
  - Monitoring, analysis, incident response, and visualization tools
- SOC Application of Threat Intel
  - Operational orientation
  - Strategic orientation
- Specific Threat Intel Use Cases
  - SOC
  - Threat analyst
  - Vulnerability management
  - Security leadership
  - Incident response

Sign-up + More Information

Recorded Future

Sign-Up and More Information

- Sign-Up
  - Submit a sign-up request
- More Information
  - About Recorded Future
  - Recorded Future Training
  - Recorded Future Certified Analyst Program
  - Training Course Catalog and Training Credits
- Contact
  - John Wetzel, Training Program Manager
  - Mike Passaro, Product Trainer
  - training@recordedfuture.com
  - +1 (855) 476-9728