

The Art and Science of Cyber Intelligence

Table of Contents

| | |
|---|---|
| The art and science of cyber intelligence | 2 |
| Human and Machine Teaming..... | 3 |
| Notices | 4 |

The art and science of cyber intelligence

CISA | CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

THE ART AND SCIENCE OF CYBER INTELLIGENCE



**001 Instructor: This lesson is about the art and science of cyber intelligence.

Human and Machine Teaming

- Human analysts use their analytical acumen alongside the computational power and speed of machines to produce timely, actionable, and accurate intelligence
- **Human** (Analytical Acumen) a science and an Art
 - **Art:** The creativity and imagination that shapes how an analyst addresses a cyber threat
 - Examples: Personal instincts, biases, experiences
 - **Science:** The outlets used to best channel the art
 - Examples: Conceptual frameworks, analytic methodologies, structured analytical techniques
- **Machine**
 - Supervised and unsupervised learning to assist with insider threat detection, anomaly detection, prediction analysis, and report generation



2

**002 At the center of the cyber intelligence framework, on this slide, human analysts use their analytical acumen alongside the computational power and speed of machines-- computers, able to automate, process, and increasingly learn through artificial intelligence-- to produce timely, actionable, accurate intelligence, depending on the type of cyber issue being analyzed. As an art, no cyber intel analyst produces intelligence the same way, and the reason for this is that our own personal instincts, biases and experiences, and a host of other nuances impact the creativity and imagination that shapes how we as analysts approach any given cyber issue, and all of that is a good thing. That is what we celebrate in each other.

As a science, these are the outlets to channel that art, such as analytical methodologies or structured analytical techniques, and even other conceptual frameworks.

Notices

Notices

Copyright 2020 Carnegie Mellon University.

This material is based upon work funded and supported by the Department of Homeland Security under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

CERT[®] is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM20-0262

