Human and Machine Teaming

Table of Contents

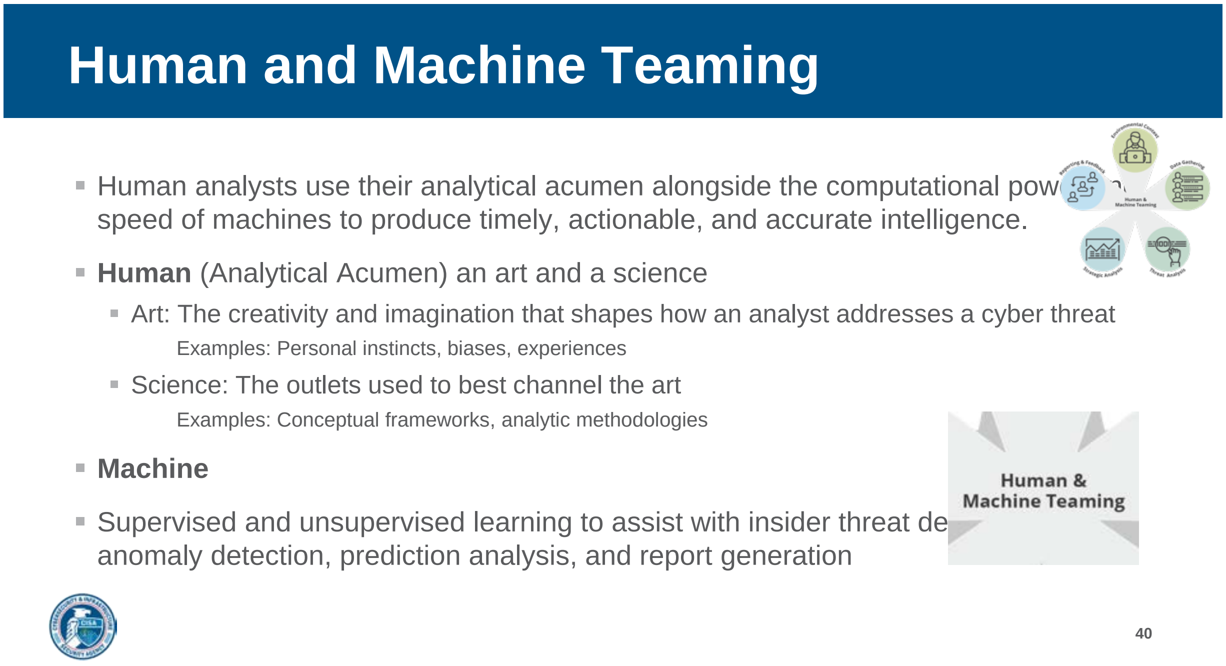
Human and Machine Teaming

Human and Machine Teaming

39

**039 Human and machine teaming.

Human and Machine Teaming



Human and Machine Teaming

- Human analysts use their analytical acumen alongside the computational pow
  speed of machines to produce timely, actionable, and accurate intelligence.
- **Human** (Analytical Acumen) an art and a science
  - 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
- **Machine**
- Supervised and unsupervised learning to assist with insider threat de
  anomaly detection, prediction analysis, and report generation

40

**040 You know, in our first 2013 Cyber Intelligence Report, we only had the human in the middle of the framework. We called it Analytical Acumen, and it was the framework's center of gravity. Analytical Acumen conceptualizes a human being's ability to interact with the other components and facilitate the timely, actionable and accurate intelligence. In other words, it is the human being's ability to interact with the other components of the framework depending on the cyber issue being analyzed to generate accurate and effective cyber intelligence analysis.

In our most recent report, we changed the middle of the framework not just to be a human but also to be a human and a machine teaming together. Human analysts use their analytical acumen alongside the computational power and speed of machines to produce timely, actionable, and accurate intelligence, depending on the cyber issue being analyzed. For example, an organization that we met used supervised learning to train a model on a data set of 5,000 articles. The model generates articles twice a day for the entire team, and one analyst is responsible for triaging and drilling down on the most serious and pressing items. The model also gets better every day, because the analysts provide new training and feedback data to the model as they work. This organization claims that the process has reduced the time required for particular task from eight hours down to one hour.

In the next few years, humans and machines will team more and team better in areas such as getting real-time status on cyber threats, organizational and internal developments and new technologies, getting real-time status on the network architecture and attack surfaces, anomaly detection, user behavior prediction, data and data source validation, and generating tailored reports and presentations to specific audiences and leadership internal and external to the organization.

Notices

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.

DM20-0262