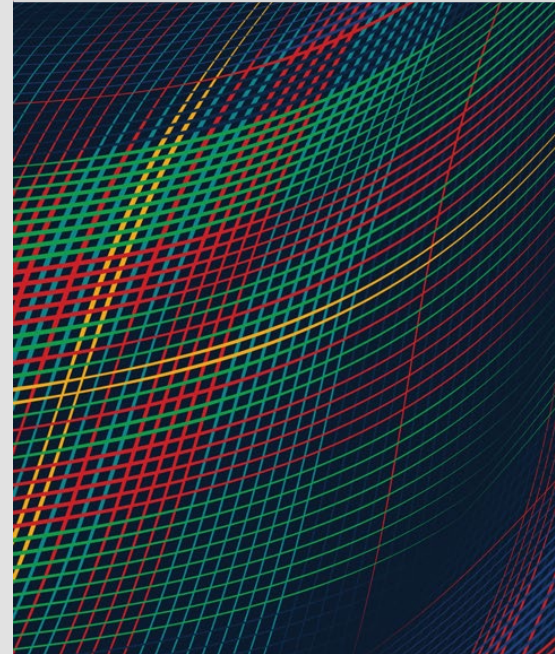


# What's New from the SEI in Insider Risk

Bob Ditmore  
Team Lead, Insider Risk  
CMU SEI



# Document Markings

Copyright 2024 Carnegie Mellon University.

This material is based upon work funded and supported by the Department of Defense 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.

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.

References herein to any specific entity, product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute nor of Carnegie Mellon University - Software Engineering Institute by any such named or represented entity.

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.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at [permission@sei.cmu.edu](mailto:permission@sei.cmu.edu).

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

DM24-1195

# Insider Risk Management: Measures of Effectiveness

- Training on how to conduct [ITVAs](#), [ITPEs](#), and [IRMPEs](#)
- Frameworks for developing custom measures and metrics
- Next offering: Oct. 29-31 (live online)
  - For details, see:  
<https://www.sei.cmu.edu/education-outreach/courses/course.cfm?courseCode=P148>



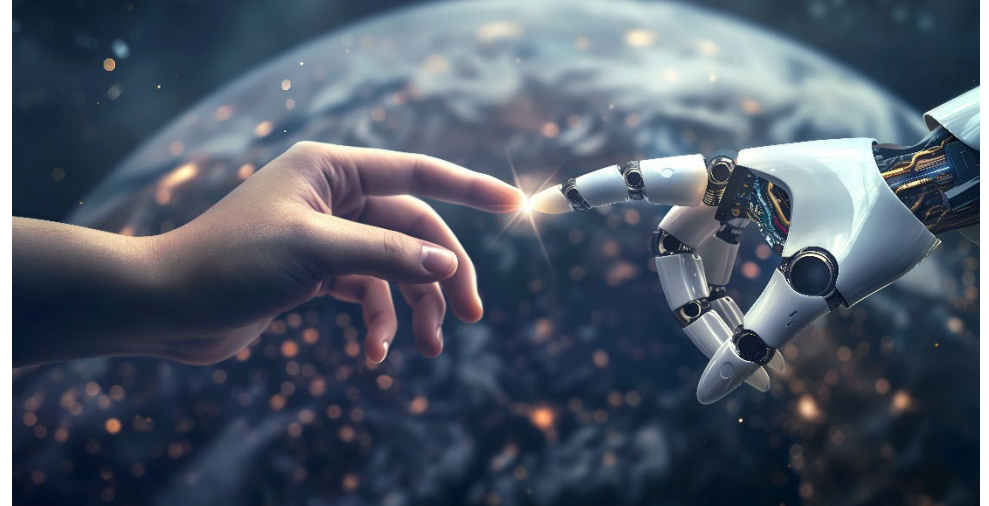
# Case / Incident Management Standardization

- Actively supporting requirements elicitation and technical evaluation efforts for insider case / incident management systems
- Refreshed tech stack used internally to collect and analyze incident data
- Coming soon: public release of Insider Incident Data Expression Standard



# AI: Insiders Are No Longer Just Humans

- Establishing boundaries for human-machine teams in insider risk analysis
- Building threat models from incident data



# IRMP Scope Expansions

- Supporting maturing IRMPs with modifying the scope of their programs (different networks, endpoints, use cases, workforce populations)
- Coming soon: public release of insider risk management program scoping instrument





# Questions / Discussion

