MITRE | Insider Threat Research & Solutions™

Cyber Indicators of Malicious Insider Threat, A Live Experiment in Employees Stealing Information

In 2021, MITRE's practitioner-researchers ran an insider threat behavioral experiment with 150 employees on a live corporate network. Real employees were asked to search, collect, and (for the first time) *exfiltrate* sensitive internal information from the network – and not get caught!

Three groups of participants completed the same search, collection, and exfiltration task with different intentions:

- *Benign intent* participants were given a scenario to search for and send the internal information off-network as if part of their everyday job supporting a government customer.
- *Malicious intent* participants were given a near-identical scenario but were asked to send the internal information off-network to a competitor.
- *Super malicious* intent participants were assigned the same scenario as malicious intent participants, and also had deep cyber defensive/offensive expertise.

The tasks were the same other than differences in intention and technical expertise.

For all participants, a significant amount of data was collected – over 10 terabytes of data in total:

- **Host and Network-based Cyber Sensors** collected data about each participant's cyber activity during the week of the task, and in the week before and week after the task. The sensors collected application, clipboard, device, email and instant messaging, file/folder, log-on on/off, network, printing, registry, system, web browsing, and window activities.
- **Decision-Making Interviews and Questionnaires** asked participants to describe their actions, decision-making, and reasoning whilst completing the task.

Behavioral psychologists and cyber scientists with deep insider risk subject matter expertise did detailed quantitative and qualitative comparisons between the data for benign, malicious, and super malicious participants. The analysis:

- Produced large collection of concerning search and collection cyber indicators.
- Developed unique combinations or clusters of cyber potential risk indicators.
- Identified unique and creative exfiltration techniques.
- Demonstrated no major differences in potential risk indicators between remote and on-premises workers.
- Reviewed misconceptions about insider risk detection – Anomaly Detection, DLP, and external threat frameworks were not helpful for detecting insider risk.

Point of Contact: Dr. Deanna Caputo, MITRE's Chief Scientist for Insider Threat Research & Solutions (dcaputo@mitre.org)