

Data-Driven Cyber Indicators of Malicious Insider Threat

Research Background


There are no silver bullets for proactively identifying insider risks and threats, and many seemingly important events and activities fail to add true diagnostic value. Through applied R&D, the insider risk community continues to identify more valuable events and meaningful activities – known as *Potential Risk Indicators (PRIs)* – to more effectively identify insider risks and threats.

In 2008, 2018, and 2021, MITRE’s team of behavioral, data, and cyber scientists conducted applied insider threat behavioral experiments with real employees on live corporate networks. In the 2021 study, for example, the MITRE team collected over 10 terabytes of cyber and non-cyber activities to produce a large of cyber PRIs for malicious information search and collection behavior. In 2023, MITRE received additional funding to conduct 3 new analyses on the dataset.

Analysis 1: Identifying Exfiltration and Evasion Techniques

How can malicious insiders exfiltrate sensitive information and evade detection?

Based on qualitative content analysis of deep-dive interview and questionnaire data, the MITRE research team identified:

 **24 exfiltration techniques** employees used to remove data from the organization’s network/devices.


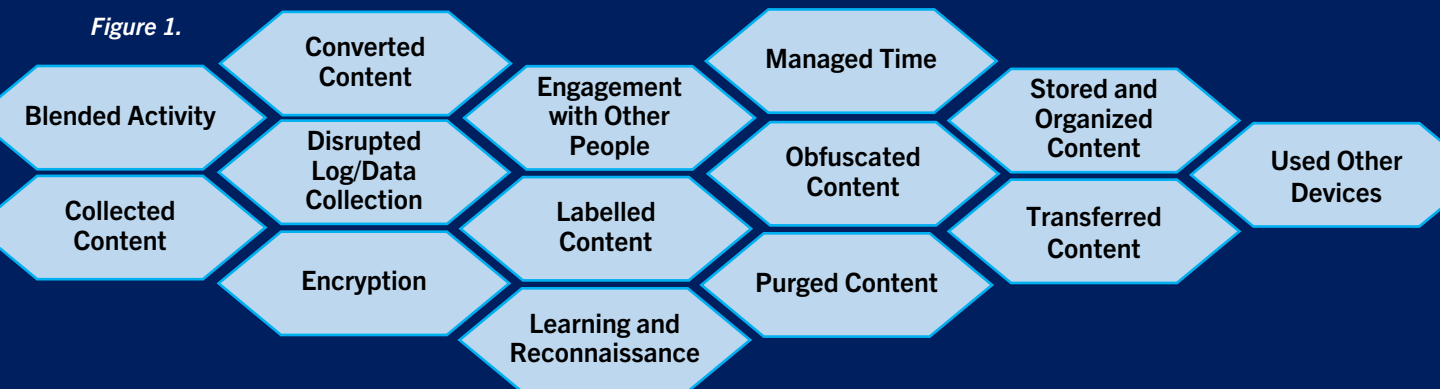

 **76 evasion techniques** employees used to reduce likelihood of their malicious activity being quickly discovered, attributed to malice, or attributed to them.


Figure 1 provides a non-sensitive summary of evasion techniques. Insider Risk Program Leaders can request the list of 100 sensitive exfiltration and evasion techniques directly from MITRE Insider Threat Research & Solutions at zero-cost.




MITRE’s rigorous analysis and reverse-engineering of exfiltration and evasion techniques also identified:

 Many exfiltration and evasion techniques did not require employees to violate rules or policies.

 Many exfiltration techniques were observable in cyber logs, but it was difficult to distinguish malicious usage.

 Detecting exfiltration is unlikely to offer substantial return-on-investment in isolation. Insider risk detection should focus less on exfiltration and more on identifying higher risk activities *before* exfiltration.

 Organizations should avoid using working hours or out-of-hours working as a PRI for insider risk unless egregious.

To discuss the research methodology, analyses, findings, techniques, and/or PRIs, please contact Dr. James Doodson, Principal Behavioral Psychologist for Insider Risk (doodsonj@mitre.org)

Analysis 2: Remote vs. On-Premises Differences

Are PRIs for insider risk different between remote and on-premises work environments?

In 2021 study, all 150 employee participants were *remote working* due to pandemic. In 2018 study, 150 *on-premises* employees participants completed the same task of searching and collecting sensitive information on a live corporate network (but not removing/exfiltrating information). Due to study similarities, the MITRE research team collated 8,626 different cyber activities into a combined 2023 dataset, then compared PRIs between on-premises and remote working employees.

MITRE's analysis indicated:



Malicious employees used different information search and collection strategies than benign employees doing the same search and collection task as part of their job.



Most PRIs were robust and can be used for remote workers *and* on-premises employees.



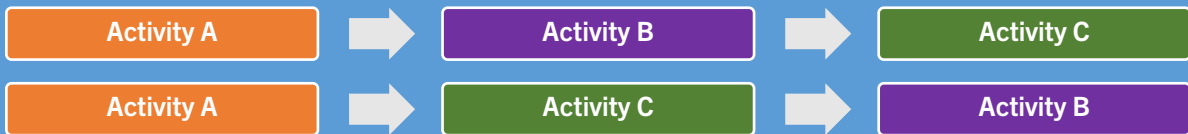
Most PRIs involved data only available on the endpoint through (for example) User Activity Monitoring solutions rather than on the network.

PRIs available to Insider Risk Program Leaders at no-cost.

Analysis 3: Sequential Analyses

Are specific sequences of Cyber PRIs used for insider risk detection?

Theoretically, sequences could improve the effectiveness of the original risk models – and insider risk detection more broadly – but the hypothesis has not been previously tested. For example, the below example shows the same three activities in different orders but it is unclear whether one sequence is more useful than the other.



To examine the efficacy of sequences, the MITRE research team used an “*n*-gram” approach to produce 5,957,005 different sequences of 8,000 activities previously identified as PRIs. Of those nearly 6 million, only 13 sequences emerged as potentially useful in identifying malicious employee participants. *MITRE can provide the full set of sequences to Insider Risk Program Leaders at no-cost.*

MITRE's Insider Threat Research & Solutions team determined:



Insider Risk Programs are unlikely to significantly benefit from detection analytics which focus on specific sequences of cyber activities.



Insider Risk Programs should focus, instead, on detecting specific higher risk cyber activities and events which occur in combination rather than whether those activities and events occur in a particular sequence. More research is needed to establish the timeframes for when activities and events should be combined or not.

To discuss the research methodology, analyses, findings, techniques, and/or PRIs, please contact Dr. James Doodson, Principal Behavioral Psychologist for Insider Risk (doodsonj@mitre.org)