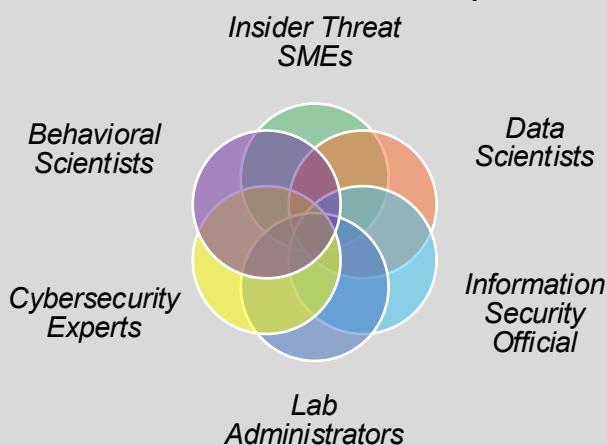


The MITRE Insider Threat Lab is a secure, air-gapped facility built for curating and extracting value from sensitive insider threat data shared from the insider threat community in government and critical infrastructure industry both nationally and internationally.

The Insider Threat Lab (InT Lab) is equipped with the staff, skillsets, experience, protocols, equipment, and tools required to receive, store, process, analyze, and interpret insider threat data. The InT Lab and the data within are protected by stringent physical security, information security, personnel security, and contractual safeguards including being NIST 800-171 and GDPR compliant.

Since 2017, the vetted and multidisciplinary team of behavioral scientists, cybersecurity experts, and data scientists have used the InT Lab to rigorously analyze insider threat data from across cyber, physical, human, and organizational data sources. The InT Lab team has extensive experience conducting scientific research into insider threats, working in/with insider threat programs, and conducting the analysis of human-generated cyber and non-cyber data. The team analyzes insider threat data from case management systems (e.g., investigative case notes), endpoint sensors (e.g., UAM solutions), and network and perimeter sensors (e.g., web proxy, data loss prevention tools).

InT Lab Team Skillsets and Experience



Example tools used in the InT Lab

- Data transfer, decompression, decryption, and backup: AWS Snowball, WinZip
- Data conversion, processing and structuring: Python, Perl, R
- Quantitative data analysis: R, SPSS, Tableau.
- Qualitative hand-annotate software: Atlas.ti, Nvivo, Standard productivity tools
- IDEs: Anaconda, Notepad++, PyCharm, rStudio, Jupyter Notebooks, Visual Studio
- Offline mirror of Python, Perl and R libraries: Conversion, parsing, string and language processing, mining, structuring, manipulation, filtering, reformatting, statistics, and visualization

The InT Lab is equipped with workstations and application, file, and database servers with tools to:

- Convert, collate, restructure and process data
- Extract the metadata
- Parse out user-generated vs. system-generated activities in cyber log files
- Automatically tag and categorize activities, flags, and other context from different data sources
- Annotate by hand the case files where automated structuring is not appropriate or feasible
- Conduct advanced quantitative analyses (e.g., time-series analyses, multi-level modelling, random forests and other classification techniques, cluster analyses)
- Identify patterns of malicious activity by collating data across different cases
- Compare patterns of malicious activity to organizational baselines to reduce false positive rates
- Test and evaluate most promising potential risk indicators

For more information, please contact the InT Lab Manager: Dr. James Doodson (doodsonj@mitre.org)

What security safeguards are in place?

For decades, MITRE has been the trusted curator of highly sensitive industry and government data that is practically transitioned to make our nation and the world a safer place. The MITRE Insider Threat Lab continues that long, experienced tradition. The InT Lab and the data within are protected by stringent physical security, information security, personnel security, and contractual safeguards including being NIST 800-171 and GDPR compliant.



**Physical
Security**



**Information
Security**



**Personnel
Security**



**Contractual
Safeguards**

Example safeguards in the InT Lab include:

-  **Restricted access to raw data:** Access to raw and aggregated data is restricted to MITRE.
-  **Secure building:** The building housing the lab is approved by Defense Counterintelligence and Security Agency (DCSA) as a suitable facility for processing and storage of information up to the Classified Secret level. DCSA is the security agency of the U.S. Department of Defense.
-  **NIST 800-171 compliance:** Compliant with the security and privacy controls, including with DFARS 252.204-7012, including NIST SP 800-171 and GDPR compliance.
-  **Access controlled:** Protected by an access-controlled badge reader with pin-pad.
-  **Intrusion detection:** Equipped with an intrusion detection device monitored on a 24/7 basis by the MITRE Security Control Center.
-  **Closed network:** Systems are not connected to the Internet or intranet (air-gapped).
-  **Logging and Auditing:** There is a protocol for logging entry and exit of equipment, data, and visitors. Access to the lab is regularly audited, and protocols reassessed.
-  **Oversight:** The lab is overseen by an Information Security Official, Information System Security Official, Privacy Official, and team of vetted System Administrators.
-  **Non-Disclosure Agreement:** NDA signed between MITRE and data contributors.
-  **De-identification procedures:** Organizations are encouraged to engage in de-identification procedures prior to transferring their data to the lab. MITRE's physical, data, and personnel security protocols are elevated to secure Personally Identifiable Information (PII) as necessary.
-  **Vetting:** MITRE employees vetted prior to joining organization and project.
-  **Experience and Training:** Behavioral scientists are trained in handling sensitive personal and organizational data appropriately. The research team receives lab-specific Security and Awareness training prior to access to the lab.