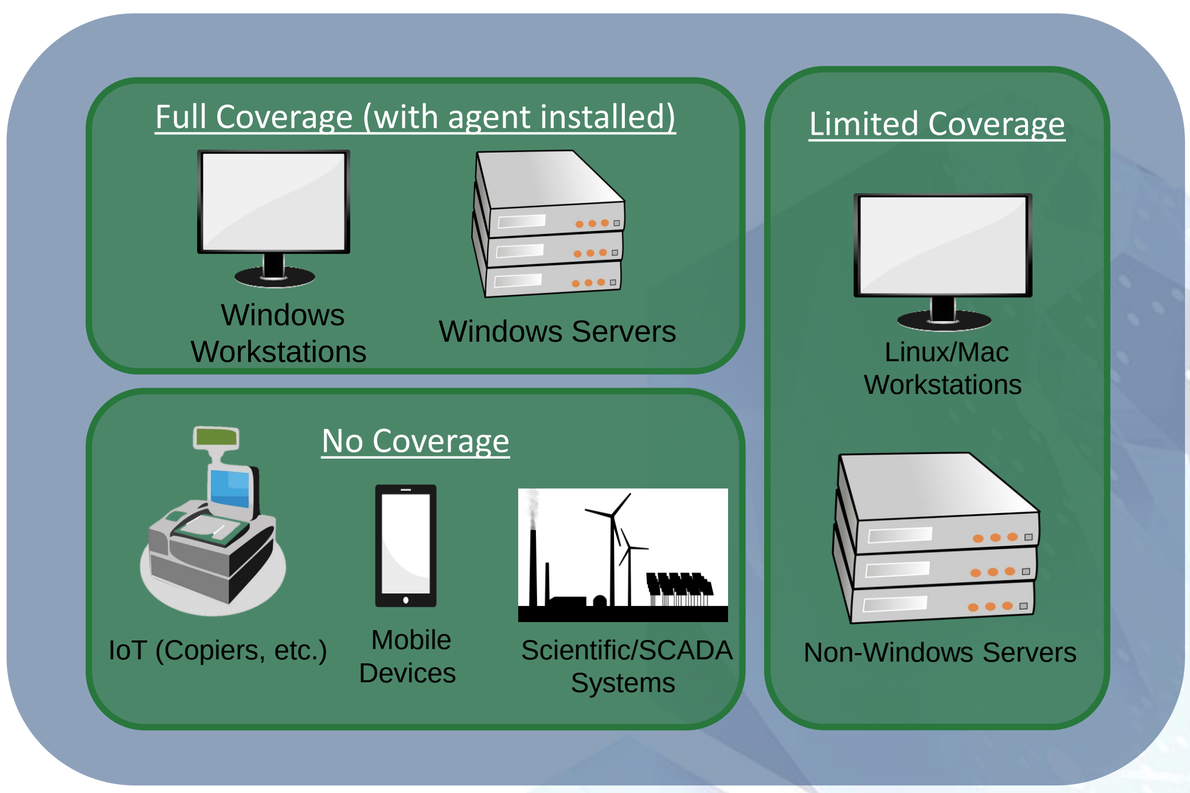
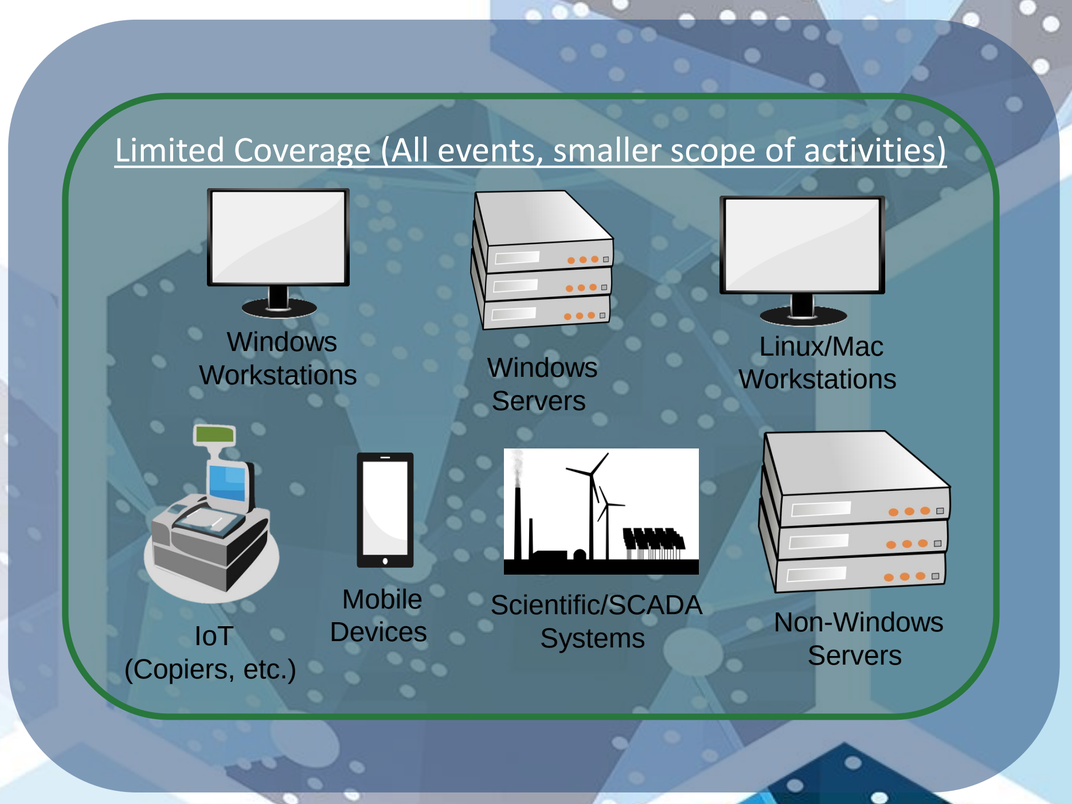
Leveraging Existing IT Resources for Insider Threat Risk Mitigation

Detecting observable indicators of insider risk relies heavily on collection and analysis of specific types of data representing user activity on enterprise systems. Some organizations deploy user activity monitoring (UAM) software specifically for this purpose, but others are unable to do so, either for cost reasons, lack of support resources, etc. Here, we demonstrate how organizations may leverage existing IT resources to provide meaningful data for insider threat risk mitigation without deploying a standalone UAM solution.

Single Tool Approach



Multi-tool Approach



Minimum UAM capabilities recommended by U.S. National Insider Threat Task Force

- Keystroke Monitoring
- Application Content Capture
- Screen Capture
- File Shadowing
- Automated Alerting

Alternative Data Sources for User Activity Monitoring

Capability	Data Source	Potential Use
Application Content Capture	Email logs	Identify concerning text, changes in social networks, communication with competitor organizations, data exfiltration attempts
	Chat logs	Identify stressors and/or personality characteristics associated with increased risk of counterproductive workplace behaviors
	Data Loss Prevention (DLP) Software	Identify potential data exfiltration attempts
File Shadowing	Host operating system event logs	Identify potentially concerning file activity, modification, transfer, or deletions
	Network file server logs	Identify potential data reconnaissance; concerning file access attempts; modification, transfer, or deletion of sensitive information
Automated Alerting	Security Information and Event Management (SIEM) system	Configure automated alerts of potentially concerning activity, based on querying the aggregation of data sources like those listed above

Carnegie Mellon University
Software Engineering Institute

National Insider Threat Center

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.

DM19-0576