Quick Tips

Insider Threat Indicators

Network Activity

- Changes in work hours
- Changes in computer asset usage
- Excessively large downloads
- Usage of log clearing software/methods

Data Exfiltration

- Increase in visits to file share or intranet sites
- Installation of high-risk software
- Spikes in inbound/outbound email traffic volume
- Attachments sent to suspicious recipients
- Modification to remote file share folders/file accesses
- Removable media alerts
- Bursts in printing on weekends and holidays
- Modification to PowerShell command usage
- Frequent external/personal recipients

Personnel Management

- Notice of resignation or termination
- Declining performance reviews
- Disciplinary action
- Increase in visits to job search sites
- Increase in outbound email to competitors

Access Attributes & Behaviors

- Privileged user activity
- Access levels/permissions
- Accessing machines via RDP/SSH
- Changes in remote network connectivity/VPN
- Endpoint behavior alerts
- Sharing passwords or unauthorized use of credentials
- Attempts to access resources outside of job role

External Data

- Social media posts
- Financial duress
- Criminal/civil history
- Foreign contacts/travel

Physical Security

- Off-hour access
- Tailgating

Compliance Cases

- Noncompliance with training requirements
- Policy violations