When an Insider Strikes **Examine Eight Data Sets**

1 | 

Knowledge Management System

Review historic tickets documenting analyst investigations. Has this employee been investigated for any violations in the past?

2 | 

Email Logs

Look at all emails sent to external domains including competitors and personal accounts. Review all files included in these emails.

3 | 

Network Logs

Examine web traffic history including data uploads to external sites. Note behaviors such as job hunting, researching data exfiltration tutorials, and searching for network and physical security capability specifications.

4 | 

Cloud Storage Logs

Document any and all files that may have been downloaded or uploaded by the individual. Cross reference the file storage location with their business unit and investigate if the individual was trying to access files not applicable to their job function.

5 | 

DLP Logs

Review both host and network DLP logs for insights on the data in question.

6 | 

Removable Media Logs

Determine if files were locally transferred off a system. Review the device from which the files were transferred—were there previous attempts?

7 | 

Badge Access Logs

Examine badge access records to determine if an employee account is being shared or system compromised from a remote location.

8 | 

Print Service Logs

Review both a system and network level logs. Print service logs cross referenced with badge access logs could help determine where exactly an employee was when the data exfiltration occurred.

REVOLUTIONARY SECURITY

REVSEC.COM