

Insider Threat Handling Toolkit

Listed below are the tools that can help incident handlers in responding to insider threats.

Insider Threat Detection and Analysis Tools	
Category	Tools
Behavioral Analysis Tools	<ul style="list-style-type: none">▪ Splunk User Behavior Analytics (https://www.splunk.com)▪ IBM QRadar (https://www.ibm.com)▪ Cortex XDR (https://www.paloaltonetworks.com)▪ Kriptone (https://www.kriptone.com)▪ ManageEngine Log360 (https://www.manageengine.com)▪ Heap (https://heap.io)
Insider Threat Detection Tools	<ul style="list-style-type: none">▪ Firewall Analyzer (https://www.manageengine.com)▪ Proofpoint Insider Threat Management (ITM) (https://www.proofpoint.com)▪ DataRobot (https://www.datarobot.com)▪ Ekran System (https://www.ekransystem.com)▪ SolarWinds Security Event Manager (https://www.solarwinds.com)▪ ManageEngine Endpoint DLP Plus (https://www.manageengine.com)▪ Incydr (https://www.code42.com)▪ insightIDR (https://www.rapid7.com)▪ Vectra Cognito (https://vectra.ai)
Network Analysis Tools	<ul style="list-style-type: none">▪ Wireshark (https://www.wireshark.org)
Tools for Detecting Data Exfiltration	<ul style="list-style-type: none">▪ Nuix Adaptive Security (https://www.nuix.com)▪ Infoblox (https://www.infoblox.com)▪ ManageEngine DataSecurity Plus (https://www.manageengine.com)▪ ExtraHop Reveal(x) (https://www.extrahop.com)▪ Splunk (https://www.splunk.com)▪ Securonix (https://www.securonix.com)
Tools for Detecting Removable Media	<ul style="list-style-type: none">▪ DriveLetterView (https://www.nirsoft.net)▪ Plug and Play (PnP) Manager (https://www.microsoft.com)▪ USBDeview (https://www.nirsoft.net)▪ Disk Utility (https://support.apple.com)▪ EaseUS Partition Master (https://www.easeus.com)▪ WinDirStat (https://windirstat.net)

Database Analysis Tools	<ul style="list-style-type: none"> ▪ SysTools SQL log Analyzer (https://www.systoolsgroup.com) ▪ dbForge Transaction Log (https://www.devart.com) ▪ SQL Transaction Log Analyzer Tool (https://www.stellarinfo.com) ▪ SQL Server Transaction Log Analysis Tool (https://www.sqlrecoverysoftware.net) ▪ Aryson SQL Log Analyzer (https://www.arysontechnologies.com) ▪ Sysinfo SQL Transaction Log Recovery (https://www.sysinfotools.com)
Insider Threat Prevention Tools	
SIEM Tools	<ul style="list-style-type: none"> ▪ Fusion SIEM (https://www.exabeam.com) ▪ ArcSight ESM (https://www.microfocus.com) ▪ Splunk® Enterprise Security (https://www.splunk.com) ▪ LogRhythm SIEM Platform (https://logrhythm.com) ▪ AlienVault OSSIM (https://cybersecurity.att.com)
Data Loss Prevention (DLP) Tools	<ul style="list-style-type: none"> ▪ Endpoint Protector (https://www.endpointprotector.com) ▪ Symantec Data Loss Prevention (https://www.broadcom.com) ▪ Trellix Data Loss Prevention (DLP) Endpoint (https://www.trellix.com) ▪ Forcepoint Data Loss Prevention (https://www.forcepoint.com) ▪ Digital Guardian Endpoint DLP (https://digitalguardian.com)
UBA/UEBA Tools	<ul style="list-style-type: none"> ▪ FortiInsight (https://www.fortinet.com) ▪ LogRhythm UEBA (https://logrhythm.com) ▪ DTEX InTERCEPT (https://dtexsystems.com) ▪ Interset (https://interaset.com) ▪ Gurukul UEBA (https://gurukul.com)
Activity Monitoring Tools	<ul style="list-style-type: none"> ▪ ActivTrak (https://www.activtrak.com) ▪ SoftActivity Monitor (https://www.softactivity.com) ▪ EKTRAN User Activity Monitoring Software (https://www.ekransystem.com) ▪ Spyrix Personal Monitor (http://www.spyrix.com) ▪ StaffCop Enterprise (https://www.staffcop.com)