Insider Threat Defense
Zero Trust Rollout Guide

Three types. Privilege ladder. UEBA / DLP / PAM. Shadow AI. Zero trust.

Three Types of Insider Threat

MALICIOUS
Intentional harm

Defense:
PAM + monitoring + HR correlation

NEGLIGENT
Unintentional carelessness

Defense:
Training + controls + safe defaults

COMPROMISED
Account taken over

Defense:
MFA + UEBA + zero trust

Privilege Ladder — Watch Every Rung

USER	POWER USER	LOCAL ADMIN	USER ADMIN	DOMAIN ADMIN
Standard access	Install rights	Full workstation	Manage accounts	Game over

Detection Signals — Watch Behavior, Not Presence

UEBA
- ☐ New systems accessed
- ☐ Data volume up 10x+
- ☐ Off-hours activity
- ☐ New tool usage

DLP
- ☐ Large personal cloud upload
- ☐ Customer data → personal email
- ☐ USB writes of tagged files
- ☐ Sensitive data screenshots

PRIVILEGED
- ☐ Admin from unusual endpoint
- ☐ No JIT approval flow
- ☐ Standing privileges present
- ☐ No session recording

CONTEXT
- ☐ Activity near HR events
- ☐ Impossible travel logins
- ☐ Contractor post-project access
- ☐ Shadow AI data pastes

Shadow AI Policy — The New Insider Risk

- ☐ **Approved AI tool list**
  Publish which tools employees may use (ChatGPT Enterprise, Claude Team, etc.)
- ☐ **Data classification rules**
  Public / Internal / Confidential / Restricted — mapped to allowed AI tools
- ☐ **Enterprise agreements**
  SOC 2, no-training clauses, data retention limits, DPA in place
- ☐ **DLP for AI endpoints**
  Block sensitive data patterns from reaching consumer AI URLs
- ☐ **Training + acknowledgment**
  Employees signed off. Refreshed quarterly. Real examples included.

Zero Trust Rollout — Order of Operations

1 Inventory	2 Least Priv	3 MFA + PAM	4 Segment	5 Continuous
Users, devices, apps, data — what exists	Strip standing privileges — right-size access	Every user MFA. Admins in a vault.	Break flat network — workload isolation	Verify every request. Assume compromise.

Series Complete → watch all 6 at youtube.com/@nasscybercorner