SpyCloud

CHECKLIST FOR **OPTIMIZING** YOUR INSIDER THREAT PROGRAM

Don't wait for the next incident to drive change at your organization. This checklist includes critical steps to optimize your insider threat program using ***identity intelligence***

DARKNET IDENTITY INTELLIGENCE
surfaces insights from recaptured breach, malware, and phishing data that allows teams to investigate insiders who may be using stolen credentials, malicious infrastructure, or fake identities.

Use this checklist to help you identify risks before suspicious behavior even begins, and to continuously prevent both malicious and unwitting insider threat incidents.

ACCORDING TO OUR IDENTITY THREAT PULSE REPORT

67% OF SECURITY TEAMS PLAN TO AUGMENT THEIR INSIDER THREAT PROGRAMS IN THE NEXT 12 MONTHS

1 ASSESSMENT
ESTABLISH YOUR PROGRAM BASELINE

- [ ] Inventory employee accounts, data access patterns, & supply chain partners
- [ ] Audit your current tools & workflows for gaps
- [ ] Consider adding identity intelligence into your defenses

2 PRE-EMPLOYMENT
STOP INSIDER THREATS BEFORE THEY START

- [ ] Establish cross-functional response workflows between SecOps & HR
- [ ] Enhance background checks with identity intelligence
- [ ] Share exposure intelligence report with HR to clear or disqualify candidates
- [ ] Train recruiters on insider threat indicators

3 CONTINUOUS EMPLOYEE MONITORING
DETECT EMERGING INSIDER THREATS

- [ ] Identify high-risk user populations
- [ ] Monitor employee identity exposure across corporate & personal accounts
- [ ] Track session cookie theft & invalidate compromised sessions
- [ ] Layer identity intelligence into SIEM & UEBA tools
- [ ] Continuously verify employee identities with quarterly checks

4 SUPPLY CHAIN MONITORING
ACCOUNT FOR PARTNERS & VENDORS

- [ ] Vet vendor and contractor identities
- [ ] Monitor partner organizations for compromises
- [ ] Incorporate identity exposure insights to understand risk

5 RESPONSE & REMEDIATION
ACT FAST ON CONFIRMED INSIDER THREATS

- [ ] Integrate with identity providers for automated protection
- [ ] Fully remediate all exposed access
- [ ] Automate response for critical exposures

6 USER OFFBOARDING
SECURE COMPLETE IDENTITY LIFECYCLES

- [ ] Map & revoke all access tied to departing employees
- [ ] Verify all access is terminated after employment
- [ ] Coordinate security & HR actions during offboarding

YOUR NEXT STEPS

Instead of waiting for suspicious behavior, detect identity compromise before it becomes network access.

See how SpyCloud helps mitigate insider threats with critical identity intelligence

LEARN MORE GET A DEMO