DASERA

INSIDER THREATS CHECKLIST

DATA MAPPING

- □ Identify the company’s most valuable assets - the data and systems of value and high business impact
- □ Classify data by labelling or tagging them based on value, sensitivity, risk posture, usage levels, etc.
- □ Perform a risk assessment to determine the risk of data loss or breaches due to insiders
- □ Create a 360-view on insider exploitability by identifying data interactions and travel path of the data across the customer journey
- □ Identify suppliers, contractors, partners and assess their security best practices, processes, and tech stack
- □ Establish and clearly document enterprise-level governance and control policies
- □ Tweak the insider threat program at a fixed frequency to address security and threats as they evolve
- □ Secure executive backing for the insider threat program

INSIDER THREATS CHECKLIST

STRATEGY & PROGRAM

□ Establish baselines for secure access, usage, behaviors, etc.

□ Validate all working assumptions at every engagement and by actively managing trust

□ Perform a risk assessment to determine the risk of data loss or breaches due to insiders

□ Ensure that entities do not retain privileges to initiate a trusted action beyond the perimeter of the request that provisioned it

□ Grant privileges to the minimally viable constituent of the system that will dispose the action

□ Map out the entire mix of federal, state, and industry regulations and that deal with consumer data

Dasera

INSIDER THREATS CHECKLIST

VISIBILITY & MONITORING

□ Identify behavioral deviations against the organization’s established baselines

□ Maintain a complete audit trail of who’s accessing what

□ Monitor behaviors such as downloads, unnecessary data access, files being sent to personal accounts, social media activity, query risks, etc.

□ Monitor access to the data and aggregate to a SIEM or data lake

□ Reprioritize threat information to surface most critical alerts based on threat posture

□ Monitor how data is used from structured databases on-prem or in the cloud (because that’s where the crown jewels are usually stored)

□ Flag and correlate for simple indicators of what shouldn’t be happening

Dasera

INSIDER THREATS CHECKLIST

TRAINING & CULTURE

□ Establish a robust security awareness program that is engaging, company-wide, and repeated over time

□ Reinforce good behaviors and highlight sample malicious or careless behaviors

□ Put tighter controls in place for endpoint protection (e.g., cutting off access to USB ports)

□ Establish clearly that behaviors are being monitored, so that people know they need to act responsibly

□ Democratize security - make the safety of sensitive data everyone's responsibility

□ Personalize training and content for teams or individuals to explain their role and get them to add value to the process

□ Understand staff temptations especially in teams like Customer Support, Treasury, Accounting, or HR (where a breach can cause high financial damage)