CODE42

CHECKLIST

How to Build an Effective Insider Threat Program

01 Understand the insider threat risks that are unique to your organization:

- What data that is critical or important? (Think — unstructured, intellectual property, regulated, customer)
- What are the assets and systems where critical/important data resides?
- Are there individuals who represent insider threat risk? (Think — departing employees, sensitive data access, employees demonstrating poor security practices, contractors, etc.)
- If you don't have a clear picture of the above, consider conducting a risk and impact assessment

02 Get executive and stakeholder buy-in and support:

- Present accurate picture of the risks and impact that are unique to your organization and where gaps and blind spots exist
- Gather data on insider threat risks and trends — Verizon DB, CERT, Ponemon, etc.
- Share information related to recent insider threat incidents that have made the headlines
- Discuss maturity, where you reside today and where you intend to progress and how

03 Determine what tools will help manage insider threat risks:

- Evaluate current tool stack and identify where you have gaps related to ITM management
- Conduct PoCs to evaluate potential tools and determine success criteria
- Look for tools that integrate with or complement existing tools
- Look at tools that have the ability to detect, investigate and respond to data risk quickly and effectively

04 Build process and documentation:

- Outline criteria for monitoring including actions that warrant inclusion and exclusion from ITM monitoring
- Document the ITM investigation process to ensure repeatability and consistent handling
- Document a clear escalation path for incidents and reporting
- Consider incorporating ITM scenarios into periodic incident response table tops or testing

05 Communicate:

- Develop and communicate an Acceptable Use policy and make sure it is available to all employees and contractors
- Incorporate ITM scenarios into security training and awareness
- Be transparent with your employees about monitoring and why it is important to your organization, but avoid disclosing tools and methods
- Build relationships with peer organizations to benchmark and share learnings, challenges and best practices

06 Keep it simple to start and iterate as the program matures and risks evolve

CORPORATE HEADQUARTERS | 100 WASHINGTON AVENUE SOUTH | MINNEAPOLIS, MN 55401 | 612.333.4242 | CODE42.COM