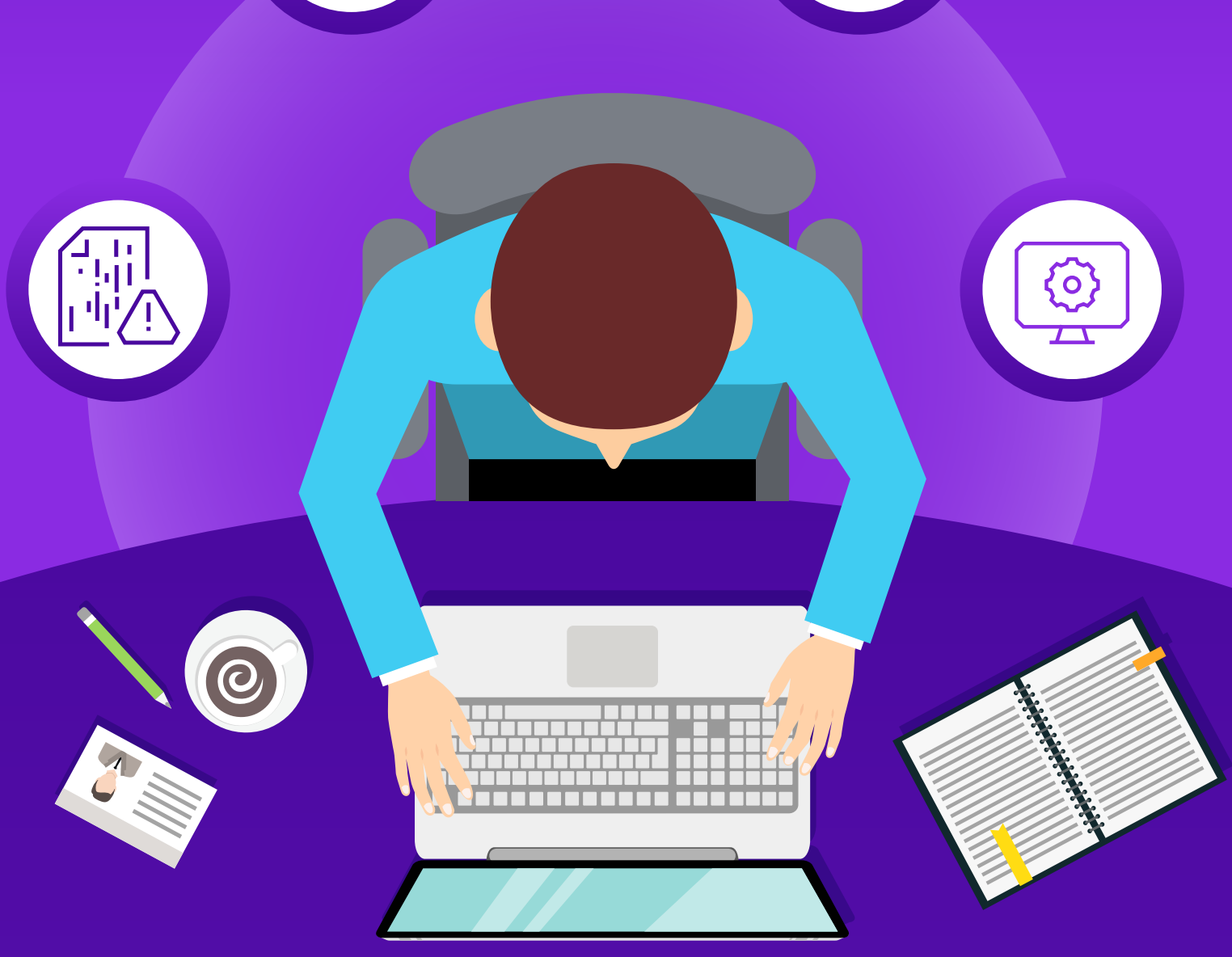
securonix

AN INSIDER THREAT PROGRAM CHECKLIST

Setting up an insider threat program depends on your organizational goals. An insider threat program can protect your assets and help you navigate an evolving threat landscape.

We've put together four steps to help you plan your program: define, identify, assess and manage. Each step lists actions and considerations you'll need to factor in when crafting your insider threat program.



Define your strategy and goals

- Define insider threats, types of insider threats, how they can materialize within your current environment, and their impact on the organization, employees, stakeholders, and customers
- Define the purpose and expected outcomes of the insider threat program

Identify partners and assets

- Establish board sponsorship for your insider threat program
- Determine and identify your critical assets
- Identify critical assets and high-risk user groups
- Communications – involve all parties (IT, HR, Legal, Data Privacy, Unions/Work Councils)
- Establish measures, playbooks, and treatment strategies for the insider threat response team

Assess critical resources and intel

- Conduct insider threat assessment across people, processes and technology
- Conduct insider threat landscape review
- Review current and applicable organizational policies (privacy policy, acceptable usage for example)
- Review relevant ethics, legal, regulatory and compliance standards
- Conduct data privacy impact assessment, and update data privacy notice
- Estimate resources for the program and insider response team
- Benchmark/re-assess insider threat program maturity progress

Manage stakeholders and program

- Manage, prioritize, monitor and track identified risks
- Continuously assess your current measures & countermeasures across people, processes, technology, and governance
- Create a stakeholder map and RACI
- Create a cross-organizational insider threat team (consider a virtual team)
- Ensure robust security training and awareness program is deployed, which inspires long-term, sustained behavioral and cultural changes across the organization
- Review your current technology stack, identify new opportunities to build new use cases in line with threat landscape review
- Review, pilot and evaluate opportunities for emerging technologies & processes to mitigate the insider threats
- Audit your insider threat program
- Regularly review insider threat program strategy

About Securonix

Securonix is redefining SIEM for today's hybrid cloud, data-driven enterprise. Built on big data architecture, Securonix delivers SIEM, UEBA, SOAR, Security Data Lake, NDR, and vertical-specific applications as a pure SaaS solution with unlimited scalability and no infrastructure cost. Securonix reduces noise and prioritizes high fidelity alerts with behavioral analytics technology that pioneered the UEBA category.

For more information about detecting insider threats and common profiles, download our ebook "Five Insider Threat Profiles".

www.securonix.com

Follow us @securonix

securonix