exabeam

Checklist

Insider Threats Checklist

Defending against insider threats is more than just picking the right security solutions. It's also defining and creating a security program that puts people, processes, and technology together to effectively defend against these kinds of threats. The following checklist is meant to be a guide when defining an insider threat or insider risk defense program.

✓ Governance and strategy

The organization's ecosystem, structure, objectives, policies, and procedures are defined, and regulatory, legal, and operational requirements are understood and inform the management of insider risk.

- Define cross-functional owners for each component
- Set metrics and specific tasks for each component to ensure objectives are met
- Ensure each component owner is part of an insider threat working group
- Assign Insider Threat Director (ITD) role to serve as central coordination and communication point. The ITD should chair the insider threat working group and report to the CSO or CRO.

✓ Personnel assurance

The organization ensures a trusted workforce by fully vetting employees prior to granting them access to assets and by implementing procedures to alert on behavior indicative of insider threat once onboard.

- Vet all personnel, regardless of role (full-time employee, part-time employee, contractor, partner, etc.) before granting access to organizational assets
- Create a vetting program and define levels of access for each role type

☑ Training and awareness

Insiders are provided with threat awareness education and are adequately trained to perform their insider risk-related duties and responsibilities consistent with related policies, procedures, and agreements. Workforce is trained on regulations, expectations, codes of conduct, conflict resolution processes, and policies and procedures supporting each.

- Ensure insider threat training explores the various types of insider threat personas and is continually updated and expanded
- Engage and inform employees of current regulations, security threats, and practices with regular updates and education

☑ Asset management – crown jewel program

The organization's assets are identified, prioritized, and managed consistently with the organization's insider risk strategy. This can include trading systems, financial applications and SWIFT network access.

- Create a formal program to identify and define critical assets and crown jewels
- Establish an asset identification process that captures relevant information like asset type, asset owner, authorized users, access, and locations. The process should be dynamic and repeatable for easy updating.
- Map sensitive data flows

☑ Entitlement control

Entitlements to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.

- Audit entitlements to sensitive information regularly to ensure unnecessary access privileges don't exist and reduce the number of devices with access
- Take into account non-static insiders like temporary employees, contractors, and business partners as they may have access to sensitive information
- Review and shut off access to systems and data in a timely manner for departing employees

☑ Monitoring

Employees and assets are monitored to obtain visibility for purposes of uncovering actions that are indicative of a threat and may negatively impact the organization.

- Use relevant security solutions to monitor users
- Scrutinize signs of threats like resignations and abnormal activity as defined by security solutions
- Leverage relevant security solutions for fraud by monitoring and reporting transactions and communications

☑ Analysis

Analysis is conducted to identify behaviors and interactions that may be indicative of threat. Data is analyzed across multiple platforms and sources and capable of providing actionable alerts.

- Use security solutions that provide user activity monitoring (UAM), user and entity behavior analytics (UEBA), and data loss prevention (DLP) to provide a complete picture of both asset and insider actions and behaviors

✓ Investigation

Behaviors, actions, and insider threat indicators are examined and fully explored to determine the level of threat. Identified threats are mitigated in accordance with established policies, existing business objectives, risk tolerance and regulatory requirements.

- Coordinate between security teams, HR, legal, and other business units
- Create an insider risk center of excellence led by CSO. COE should include dedicated management, SME, analyst, and investigator support

✓ Insider risk assessment

The organization's priorities, asset impacts, vulnerabilities, and threats are identified and used to measure insider risk to support business operations and security resource allocations.

- Define a logical process to identify, assess, and communicate the risk of insiders
- Develop a formal policy to address risk and allocate resources for tools and people

✓ Compliance and reporting

Insider risk management personnel, processes, and procedures are formally managed and reviewed for compliance with established legal, privacy, policy, and regulatory requirements.

- Identify, document, and communicate operational parameters with formal metrics and plans that align with key regulatory requirements
- Create quarterly compliance reports for legal and risk with relevant information as defined by insider threat program and legal

exabeam

For a more in-depth look at creating an insider threat program and everything that it entails, read Shawn Thompson's book, **Insider Risk Management: Adapting to the Evolving Security Landscape.**