Deloitte.

Developing a holistic insider threat program

Building an insider threat mitigation program

September 2016

Developing a holistic insider threat program

Defense and security organizations in both the public and private sectors continue to face a range of challenges associated with insider threats and are increasingly subject to regulatory requirements to prevent such events. Deloitte takes a holistic approach to insider threat mitigation, viewing it as an issue that should be addressed as part of an enterprise-wide program with broad stakeholder engagement and executive buy-in.

Initiate

QUESTIONS

- Who should be involved in the development of an insider threat program?
- **Who will champion** the program and drive organizational change?
- What are the **vision and objectives** for the program?
- How will the program align with the culture of the organization?
- What are the most valuable assets and greatest threats?
- What is the **organization's risk tolerance**?

STEPS

- **Identify key stakeholders** needed to develop the program
- Define what constitutes an insider threat
- Define the organization's **critical assets** and future vision for the insider threat program
- Secure **executive buy-in** and establish roles and responsibilities

Explore and Evaluate

QUESTIONS

- What is the **current state** of the organization's insider threat program and how does the organization align to leading public, private, and academic practices**
- What are the organization's **core strengths and vulnerabilities** associated with mitigating insider threats?
- How mature are the organizations current capabilities?

STEPS

- **Benchmark** business processes and technical and non-technical controls **against leading practices**
- Identify evidence based strengths and vulnerabilities
- Develop **actionable recommendations** for realizing the future-state vision

Prioritize

QUESTIONS

- How do we **prioritize gaps** identified in the explore and evaluate phase?
- Where should the organization focus resources to achieve **greatest impact**?
- What aspects of the program should be piloted (e.g. trainings, processes, technologies)?

STEPS

- Evaluate costs, level of effort, and impact to security for each recommendation
- Develop **tactical plans** for implementing each recommendation
- Stand up insider threat program office and **identify an analytics tool** to enhance detection capabilities

Pilot and Implement

QUESTIONS

- What are the objectives and **success criteria** for the pilot?
- What are the communication and change management needs associated with implementing a program?
- How will the pilot program be rolled out?
- How does the pilot program align with existing privacy policies?

STEPS

- Develop a concept of operations for the program
- Collect potential risk indicators to monitor activity critical assets; work with counsel to ensure program alignment with privacy policies
- Conduct a **pilot proof of concept** to evaluate detection and mitigation capabilities focusing first on areas of the organization with the highest risk
- Utilize pilot program to prioritize and **correlate alerts** to calibrate analytics tool
- Develop a **communications and change management plan**

Scale

QUESTIONS

- Is the rest of the organization **aware of and educated** in the right way to support the insider threat program?
- What resources, policies, business processes are needed to successfully scale?
- What are the **lessons learned** that should be incorporated before pilot expansion?
- How can I scale this program globally?

STEPS

- Execute trainings and communications plan
- Evaluate pilot outcomes against success criteria and calibrate the program based on results
- Engage key stakeholders to serve as champions for program roll out
- Develop a **roadmap for expansion** to include a focus on privacy considerations for different geographies

Optimize

QUESTIONS

- How can the program evolve in response to new technologies, staff feedback, and emerging challenges?
- How has the organization changed and has this had any effect on the program?
- What improvements, can be made to stay ahead of **evolving threats and changing workforce dynamics**?

STEPS

- **Reprioritize efforts and funding** based on measured results
- Evaluate and **leverage new trends** in the marketplace
- Refresh program and monitoring capabilities based on changes to workforce (e.g. generational shifts), business operations (e.g. bring your own device, mobile workforce), and changes in organizational risk tolerance

** Leading public, private and academic practices include: The National Institute of Standards and Technology (NIST), Federal Bureau Investigation (FBI) guidance for threat mitigation, Carnegie Mellon's Computer Emergency Response Team (CERT), the Intelligence and National Security Alliance (INSA), and the International Organization for Standardization (ISO).

Delivering results across industries

Rapid technological developments and broader access to sensitive information has caused a significant increase in the security, financial, and reputational risks to organizations. Deloitte's Consulting and Advisory practices bring an integrated market approach consisting of a portfolio of different offerings and services proven across industry sectors and tailored to a client's unique risk profile, current state, and priorities with regard to insider threat prevention, detection, and response.

Insider Threat Offerings	
Offering	**Description**
Insider Threat Workshop	Facilitate working session to explore risk tolerance, threat types, vulnerabilities, core strengths and overall maturity.
SIEM Offerings	Implement, test, and manage Security Information Event Management (SIEM) tools.
Program Stand-up	Assess the organization's current capabilities and benchmark against leading practices Provide change management, business process re-engineering, policies, controls, and training support.
Deloitte Due Diligence	Provide tiered research levels into data on transient employees within industries and external data sources globally.
Advanced Analytics/ Monitoring	Provide a risk based and scalable analytics solution capable of generating leads.
Cyber Threat Intelligence	Provide policy enforcement and end-point protection against unwarranted user access on network environment.
Advanced Scenario Analysis	Develop client specific use cases and notional insider profiles to test the security of the client's policies, systems, controls, and procedures.

Practical Application	
Client	**Impact**
Large Federal Department	• Convened a broad set of stakeholders to identify roles, division of responsibility, and future operating capabilities • Assessed and defined the organization's mission, operating model, and structure • Developed core services and determined corresponding resource requirements to mitigate threats across subcomponents • Developed an Action Plan that sequenced key milestones, required activities, and decision points critical to program standup
Financial Services Firm	• Integrated facial recognition and badge access to provide a single pane of glass view into user behavior • Developed event driven scenarios to detect after hours and secure area access attempts
Combat Support Agency	• Evaluated policies, processes and technology against leading practices and developed evidence based findings • Developed a roadmap to transition the organization from the current state to the target future state of insider threat mitigation
Federal Law Enforcement Agency	• Developed a framework to evaluate risk of domestic and international locations Developed a prototype decision dashboard for threat management and validated mitigation efforts against leading practices • Developed scenario-based training to educate workforce on insider threat risks and identify organizational security weaknesses

For more information, please contact:

Adnan Amjad
Partner
Deloitte & Touche LLP
aamjad@deloitte.com
+1 832 863 4165

Mike Gelles
Managing Director
Deloitte Consulting LLP
mgelles@deloitte.com
+1 202 251 9615

Keith Brogan
Managing Director
Deloitte & Touche LLP
kbrogan@deloitte.com
1 908 400 3455

John Cassidy
Senior Manager
Deloitte Consulting LLP
jocassidy@deloitte.com
+1 571 814 7196

Kwasi Mitchell
Principal
Deloitte Consulting LLP
kwmitchell@deloitte.com
+1 703 945 7951

Borna Emami
Senior Manager
Deloitte Consulting LLP
bemami@deloitte.com
+1 202 957 3165

For further information, please visit **www.deloitte.com/insiderthreat**.

Deloitte.