INNOVATIONS BLUEPRINT

Modern Blueprint to Insider Threat Management (ITM)

In today's remote and hybrid workforce, people and data are everywhere. Your workforce—your "insiders"—includes not only your employees, but also contractors, freelance "gig workers" and third-party supply chain partners, among others. To adapt to this new normal, modern organizations need to transform their insider threat management strategies.

While insider threats present a financial and reputational risk to organizations, they can be addressed successfully as part of a broader security strategy that addresses the three foundational pillars of insider security: consistency, visibility and transparency.

KEY TERMS

Insider:

- Employees, independent contractors and consultants, third-party contractors, supply chain partners and service providers, among others. The definition of an insider has expanded significantly in recent years as a result of businesses becoming more digitally and globally interconnected.

Negligent Insider:

- Users that make careless mistakes which unintentionally create risks.

Compromised Insider:

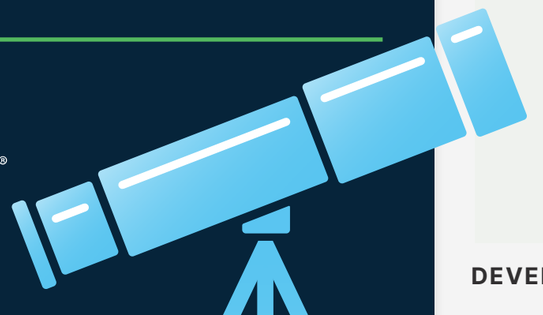
- Users that have been successfully targeted by social engineering or malware to steal their login credentials and/or take control of their devices.

Malicious Insider:

- Users who intentionally cause damage or steal from an organization, usually motivated by greed, revenge or a sense of entitlement.

BROUGHT TO YOU BY

proofpoint®



The nature of work is changing. Be sure you understand your "people" perimeter!

(LEAP INTO CHAPTER 1)

- Several recent trends have driven work—and its associated data—beyond cubicle walls and the traditional network perimeter. Know your people and your data to understand who and what needs to be protected.
- Plug data leaks—whether negligent or malicious—wherever they might occur including cloud and web apps, cloud storage, developer tools, email, mobile devices and others.
- Recognize common business use cases that increase vulnerability to insider threats, such as remote workers, departing employees, theft of sensitive data and intellectual property, virtual apps and desktops, shadow IT and mergers and acquisitions.

Build the foundation for a successful Insider Threat Management Program (ITMP) based on the three pillars of insider security: consistency, visibility and transparency.

(LEAP TO CHAPTER 2)

- Start with a people-centric security model that provides complete visibility and context into how insiders interact with your data and assets.
- Don't try to boil the ocean! Develop an initial operating capability that includes programmatic tasks, added layers for dispersed organizations and regular review. Later, scale up to full operating capability with personnel assurance, access control, dynamic risk assessment and more.
- Drive success with an insider threat management framework that instils a culture of continuous refinement and improvement.

Know the key elements, features and capabilities to look for when selecting and implementing an ITMP for your organization.

(LEAP TO CHAPTER 3)

- Take a people-centric approach to risk analysis that includes user risk profiling, cross-channel visibility and context and activity timelines.
- Analyze the primary risks in your organization with threat detection and analytics capabilities such as policy-based rules, threat scenarios, anomaly detection and threat hunting.
- Strike the right balance between privacy, compliance and security with key features to support your unique needs, including exclusion, anonymization, role- and attribute-based controls (RBAC and ABAC) and audit compliance.

DOWNLOAD THE FULL BOOK!

Proofpoint Insider Threat Management protects against data loss and brand damage involving insiders acting maliciously, negligently or unknowingly. By correlating activity and data movement, security teams are empowered to identify user risk, prevent data loss and accelerate security incident response. Take the inside track to successful ITM.

Highlights include:

- Recognize the insider threat and know your people perimeter
- Set up your insider threat management program with a people-centric approach
- Get started with ITM with a checklist of what you need to know.

GET YOUR COPY!

DEVELOPED BY ActualTech MEDIA