SPYGLASSMTG

A Women Owned/Women Led Company

Microsoft Purview:
Insider Risk Management Implementation

Microsoft
Solutions Partner

Infrastructure Azure
Data & AI Azure
Digital & App Innovation Azure
Modern Work
Security

Competencies and Specializations

SPYGLASSMTG

The Problem

Organizations have been building capabilities to protect, monitor, and react to threats that come from outside of their environments, but most lack the same level of controls and insights into what is happening within their own environment. While it is important to protect against bad actors getting into our organizations and causing havoc, the permissions needed to cause that havoc in the first place is already given to individuals within the organization. Access to sensitive information and systems is performed daily by people that are inherently trusted based on their roles. While that trust is often warranted, sometimes either with or without malicious intent, those trust employees can exfiltrate data, disseminate information internally without approval, and/or cause harm to internal system. The issues revolve around how to:

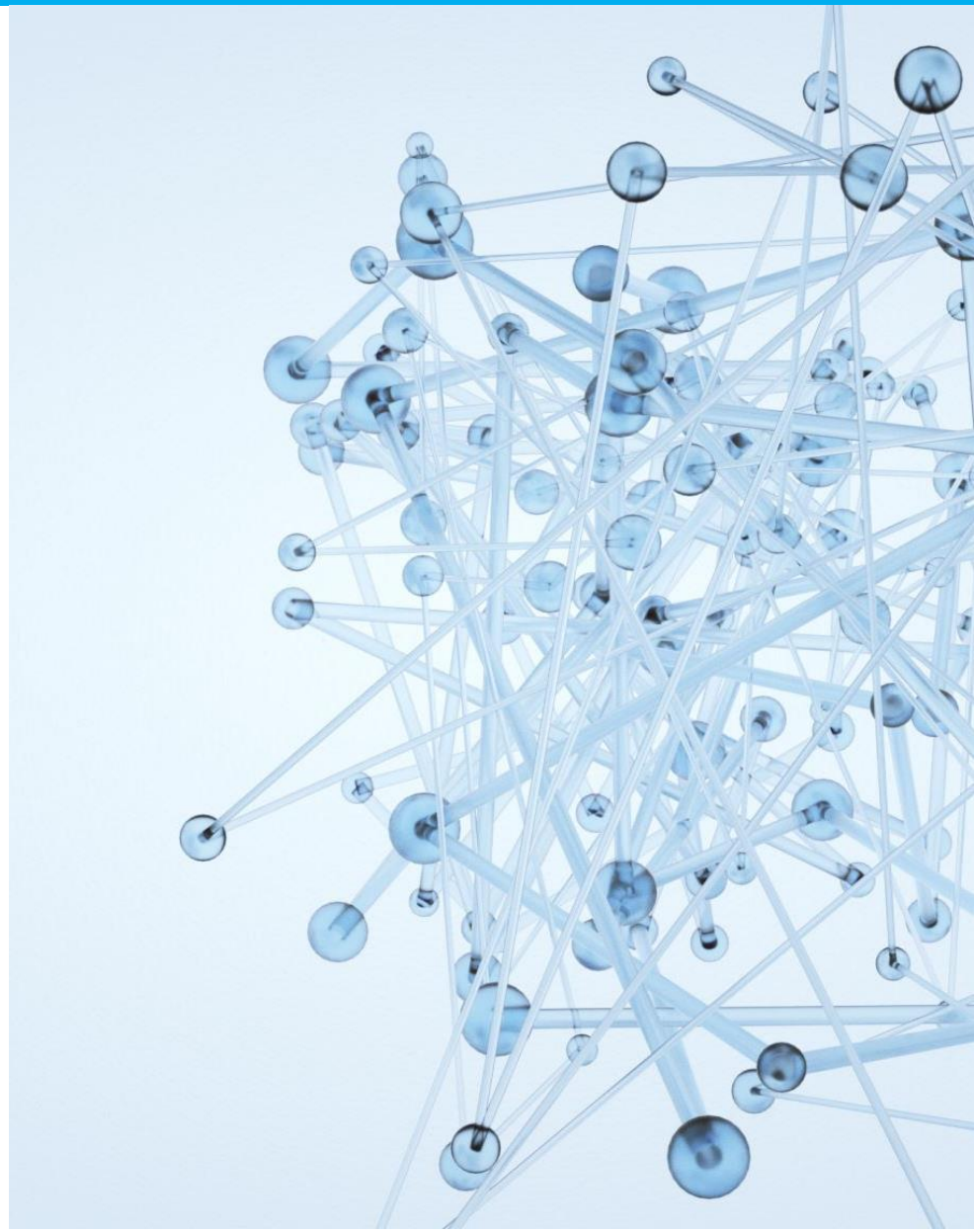
- Know what is being shared and by whom
- What normal behavior is for people
- Identifying variances in what is normal across the environment
- Being able to monitor the data while keeping privacy in mind
- Keeping sensitive data sensitive in the environment while monitoring
- Being able to perform formal investigations

SPYGLASSMTG

The Solution

Spyglass's **Microsoft Purview Insider Risk Management (IRM) Implementation Engagement** is focuses on closing the gap of securely monitoring, reporting, and responding to potential threats from entities that are within the organizational walls while still maintaining the necessary security and privacy for those entities. While the focus is on the entities inside the company, IRM relies on other solutions within the Purview stack to help address the necessary identity and data protection components that need to be accounted for to help prevent the access and exfiltration of any data that should not be performed. The implementation of IRM will focus on the following key components:

- **Assessing the existing controls to handle identities and data governance - This may include, but is not limited to, the following capabilities:**
  - Data Loss Prevention (DLP)
  - Sensitivity Labels
  - Retention Policies/Labels
  - Sharing Internally/Externally
  - Auditing/Logging
  - Role based Access Controls (RBAC)
  - Permissions Management
  - Identity Protection
- **Development of 3 defined use cases that should be reported on for IRM.**
- **Implementation of the IRM policies based on the agreed upon use cases. (Does not include 3rd party integration)**
- **Engagement and Final Deliverables**
  - Length – 2-weeks ($25K) – This can change based on scoping and additional components added
  - Purview IRM Configuration Documentation



Thank You

info@spyglassmtg.com