Intelligently identify insider risk

Intelligently investigate and take action against insider risk with Optiv.

For most organizations, external cybersecurity risks have been top of mind for many years. But these organizations are now considering the risks posed by trusted insiders as an equal or even bigger threat. Organizations are beginning to recognize the importance of establishing controls that enable them to quickly identify and manage insider risks.

Detect, investigate and act on malicious and inadvertent activities in your organization is critical to ensuring trust, creating a safe workplace and protecting company assets.

The Manage and Investigate Risk Workshop gives you the insights you need to understand insider risk in your organization.

Why You Should Attend

As your business-critical data expands and your workforce shifts to remote work, having an integrated approach that can help quickly identify, triage and act on risky insider user activity is more important than ever.

By attending this workshop, our experts will work with you to:

- Document your objectives and strategy around insider risks
- Demonstrate ways to accelerate your compliance journey with the latest Microsoft technologies
- Show how to detect investigate and take action on insider risks
- Provide actionable next steps based on your needs and objectives
- Uncover hidden insider risks in your environment
- Monitor user behavior and communications for risky behavior
- Assess your environment against the Data Protection Baseline
- Receive an analysis and report on findings and associated risks
- Learn about tools and services that can mitigate risks
- Explore recommendations and next steps

Manage and Investigate Risk Workshop

93% of organizations are concerned about insider risks

Source: Insider Risk Management Microsoft Market Research January 2021
User Risk Check Uncovers Risks That Might Be Harmful to Your Organization

The User Risk Check is the core activity of the Manage and Investigate Risk Workshop. The activity is spread out over several weeks to allow time to run on top of your cloud infrastructure and discover and identify insider risks in your organization. User Risk Check leverages automated Microsoft 365 tools and services to monitor user behavior and communication to discover inadvertent or malicious behavior that can impose risk to your organization.

The automated discovery process will monitor user behavior and communication for:

- Data leaks, accidental oversharing or malicious intent
- Data theft by departing employees
- Inappropriate communication and offensive language
- Sensitive information
- Conflict of interest

What to Expect

By the end of this workshop, experts in Microsoft compliance will provide you with a:

- User Risk Check report that includes findings and insights from the automated discovery process
- A list of recommendations and actionable next steps that will help mitigate the identified risks
- Clear look into Microsoft’s approach to mitigating and controlling insider and regulatory risks
- Data Protection Baseline assessment report with suggestions and top key improvement actions
- Set of long-term recommendations on your compliance strategy, with key initiatives and tactical next steps

Who Should Attend

The workshop is intended for security decision-makers such as:

- CCO, CSO, CISO, CEO, CFO, CIO, or CTO.
- Compliance & Security Administrator
- Microsoft 365 Tenant Administrator

Together for Stronger Security

Optiv + Microsoft

Optiv helps accelerate adoption to maximize your Microsoft investment. We secure your organization and reduce complexities by integrating built-in security solutions from Microsoft to manage and secure identities, protect your data, safeguard your cloud applications and stop threats. We have designed solutions specifically for Microsoft that are focused on business outcomes and creating clarity from cybersecurity complexity and chaos.

Let’s Get Started

Contact Optiv about this complimentary Microsoft Threat Protection Workshop.