Microsoft Services Premier Support

Security Services Catalogue

2014

Microsoft

Microsoft Services

Microsoft Services helps you get the most out of your Microsoft Information Technology (IT) investment with integrated and comprehensive end-to-end services engineered to meet your organization's IT and business management needs. Microsoft Services is designed to be your strategic business partner at every stage in your organization's expansion and development. We are committed to quality, using Microsoft and industry-proven best practice models and frameworks as a guide across the IT lifecycle for solution development and ongoing operations.

We can deliver both predefined and customized services to fit the needs of your business, taking into account your industry and specific technology requirements. Microsoft Services and technology combine to provide you with a total business solution from concept to implementation, ongoing support and training.

http://microsoft.cz/services

About this Catalogue

This catalogue represents selected security services available within Premier Support services in the Czech Republic. These services help customers reduce security risk in their infrastructure and strengthen their overall account and identity strategy.

To get up-to-date version of this catalogue please follow this link:

http://aka.ms/PremierSecurityCatalogue

Table of contents

RAP as a Service for Microsoft Security

Duration
1+ days

Services Category
RAP as a Service

RAP as a Service for Microsoft Security is a proactive service delivered by a Microsoft accredited engineer to diagnose potential issues with your Security Program and organization. This service is available for any organization that is seeking to evaluate and improve their Security Program Management. It will provide remediation guidelines, best practice and industry standard guidelines addressing issues in the areas of people, processes and technology. This is a survey based offering, no technical data collection occurs as part of this offering.

This is a new delivery experience to enable you to assess your environment at your convenience. The data is collected remotely allowing you to maintain the utmost privacy and run the assessment on your own schedule. Submission of data through the cloud enables a secure transmission of data, enabling you to view your results immediately on our secure online portal. A Microsoft accredited engineer will review the findings, provide recommendations and knowledge transfer, and build a remediation plan with your staff and your Technical Account Manager (TAM).

Deliverables Include:

- Assessment tooling, multiple submissions, and access to a secure online portal
- Regular updates to best practice guidance and online portal features
- Use of the online portal and tools with an active Microsoft Premier Support contract for 1 year
- Knowledge transfer of issues found
- Remediation plan
- Technical Findings report

To view a full datasheet for this service please visit:
http://aka.ms/Mmrrg0

Active Directory Security Assessment

Duration
5+ days (depending on complexity of your environment)

Services Category
Assessment

Active Directory provides mission-critical authentication, authorization and configuration capabilities to manage users, computers, servers and applications throughout an organization's IT infrastructure. As Active Directory provides broad and deep control of environments in which it is deployed, proper configuration and use of an Active Directory infrastructure is critical to secure an organization's systems and applications.

How this Offering Works

ADSAs are performed via a series of activities on both technical and non-technical fronts. The technical component of the ADSA leverages automated information-gathering scripts, custom and standard system analysis tools to gather in-depth information about the configuration of the directory, privileged accounts, security settings, domain controller configurations and even inappropriate use of privileged accounts. In addition to the information gathering activities, interviews with key teams involved in the various aspects of Active Directory and supporting infrastructures, are performed to identify gaps in process or governance that may also expose the directory to risk.

Key Benefits

- Domain Controllers Security
- Administrative Memberships
- Operational Excellence
- Knowledge Transfer

To view a full datasheet for this service please visit:
http://aka.ms/Szby86

Active Directory Recovery Execution Service

Duration
5 - 10 days

Services Category
Recovery Execution Service

The Active Directory Recovery Execution Service has been developed to help your organization to review common disaster recovery scenarios, determine the risk for your business and execute the recovery steps to resolve a disaster. Together with the team responsible for recovery services, we will create a business & IT risk map and improve awareness on how to act in case of a problem scenario where Active Directory Services are affected.

By testing common scenarios and recovery options you are able to build a solid documentation base. Through side-by-side knowledge transfer your IT staff will be trained to have the execution power for optimal disaster recovery.

Deliverables

- Review of recommended recovery procedures
- Recovery Business & IT Risk Map
- Forest & Domain Recovery Execution
- User & Group (object) membership Recovery Execution
- Group policy template & Login Script (SYSVOL) Recovery Execution
- Time management execution
- Enhanced knowledge transfer from Microsoft Premier Field Engineers to your IT staff
- Documentation recommendations

Engagement Sizing

The scope of this service will be customized to fit your needs based on complexity of your environment.

To view a full datasheet for this service please visit:

http://aka.ms/B37r0t

Exchange Server Recovery Execution Service

Duration
5 - 10 days

Services Category
Recovery Execution Service

Without a well-tested Disaster Recovery plan, the risk of data loss and downtime of critical business systems may seriously impact the health of your IT organization. Fire Drill exercises help identify any gaps and risks in your organization's Disaster Recovery plan. By methodically walking through the plan in a controlled environment, you can help ensure that the plan is ready. Premier Field Engineer will work together with the teams responsible for recovery of the services, walking through a series of recovery scenarios and providing a detailed gap analysis. The end result is a well-tested Disaster Recovery solution and prepared staff that your IT organization can have confidence in.

Technical Highlights

- Confidence to execute Disaster Recovery procedures
- Strong Knowledge of Disaster Recovery Techniques
- Able to change the Disaster Recovery if something changes in the core Exchange Deployment
- Knowledge to understand all recovery scenarios
- Skills to take the appropriate course of action in case a recovery is needed

Engagement Sizing

This service is delivered in two predefined levels – Foundation and Premium. For more information review the datasheet in the link below.

To view a full datasheet for this service please visit:
http://aka.ms/Ootq98

Enhanced Security Administrative Environment

Duration
5+ days (depending on complexity of your environment)

Services Category
Consulting

Cyber-attackers have been very successful at rapidly gaining administrative access to corporate and government computing environments. These devastating attacks result in malicious actors with full remote access to most or all of an organization's electronic documents, presentations, applications, databases, and other intellectual property. Recovery from these attacks is extremely difficult, slow, and expensive.

The Enhanced Security Administrative Environment (ESAE) offering is designed to help thwart a critical element of these credential theft attacks by limiting exposure of administrative credentials.

Technical highlights

The ESAE offering leverages advanced technologies and recommended practices to provide an administrative environment and workstations with enhanced security protection such as:

- Provide an enhanced security environment for administrative accounts
- Implement advanced security tools including exploit technique mitigations, attack surface analysis, and application whitelisting
- Separate admin and user accounts
- Enforce two-factor authentication for admins
- Restrict admin accounts to high trust computers
- Restrict internet browsing and other high-risk activities for administrative accounts
- Monitoring of enhanced security environment and production Domain Controllers (DCs) for security events and operational health

To view a full datasheet for this service please visit:

http://aka.ms/Aej3m3

Proactive Operations Program for Software Update Management

Duration
5 days, 2 PFEs

Services Category
Operations Consulting

Does your company have a proliferating number of servers? Do you lack a structured process for delivering software updates? The Microsoft Services Software Update Management process definition and creation engagement provides your staff with Microsoft best practices and specific recommendations that helps improve your Software Update Management process. Accomplished by streamlining your Software Update Management cycle, this process is designed to help your IT team improve business operations and decrease incidents while quickly and efficiently deploying software updates in your company. The Software Update Management engagement is based on the Microsoft Operations Framework and Microsoft solutions for management both of which are established and field-tested methods for this engagement.

This Solution Helps You:

- Design and create a process to improve your software update management
- Reduce support and operations costs
- Improve business operations and decrease incidents
- Quickly and efficiently deploy software updates
- Support a rapid response to security incidents

Engagement Sizing

The scope of this service will be customized to fit your needs based on complexity of your environment.

To view a full datasheet for this service please visit:
http://aka.ms/Jf45ji

Microsoft Security Risk Assessment

Duration
10 days

Services Category
Process Improvement

Microsoft Services Security Risk Assessment offering is designed to help determine the security risks in an application and the infrastructure supporting it. Using a formal methodology, the offering helps organizations understand their risk of exposure to security breaches in critical applications and measure their security controls and processes against industry practices, thereby establishing a security baseline from which to measure progress.

How this Offering Works

The Microsoft Security Risk Assessment (MSRA) is a two-week engagement that helps to gauge the efficacy of your security strategy by evaluating the implementation of the defense-in-depth concept – layering technical, organizational, and operational controls. Using on-site, in-person interviews and technical examination, MSRA results in the creation of a roadmap customized for your business. This roadmap takes into account your organization's resources and tolerance for change, and harnesses planned IT upgrades wherever possible. MSRA also captures opportunities for security to contribute to new business areas and reduce the cost of compliance. MSRA is focused on your need to protect important data and systems, mitigate threats, support business priorities, and address ever-evolving attack techniques – while keeping cost under control and minimizing any disruption to the business.

Key Benefits

- Gain a comprehensive and consolidated view of your existing security programs
- Improve your overall security posture by executing an actionable roadmap with specific steps to meet your business and security needs
- Enhance your program by working with experienced Microsoft

To view a full datasheet for this service please visit:

http://aka.ms/Rszrex

Dynamic Identity Framework: Identity Assessment

Duration
10 days

Services Category
Assessment

The Dynamic Identity Framework (DIF) Identity Assessment is an engagement designed to formulate an overall identity strategy that accounts for your organization's current state and future goals; complete with a detailed step-by-step roadmap outlining what needs to happen to reach your business goals. This is accomplished over the course of an intensive two week engagement.

Addressed challenges:

- Lack of Strategic Vision - No clear plan for identity infrastructure that anticipates future growth or business needs
- Reactive Deployments - Identity solutions are being deployed without consideration of how they will fit across the organization
- High Management Costs - User provisioning is not centrally managed and users still require a help desk to access resources
- Identity Proliferation - Users have multiple accounts to access a variety of services and resources
- Security and GRC - Users often have access to more information than what is required to perform job duties raising the risk of noncompliance with internal and external regulations

Benefits of Identity Assessment:

- Build Strategic Vision - With a Dynamic Identity Framework Identity Assessment you can confidently build an actionable plan, by prioritizing your objectives according to your strategic vision
- Maximize Value - The assessment goes beyond simply identifying single identity issues and provides an in depth holistic assessment of identity services across your organization
- Create a Solid Foundation - Once we understand your identity environment and business goals we can help you create a solid foundation to better plan the future of your business

To view a full datasheet for this service please visit:

http://aka.ms/Nhgupi

Security Development Lifecycle

Duration
3 - 5 days

Services Category
Workshop

The Microsoft Security Development Lifecycle (SDL) Training Workshop is designed to give the customer a customized education in the basics of the SDL and the activities necessary for successfully writing secure software, and to provide the customer with a foundation to develop secure software in their own organization using proven techniques to reduce the number and severity of software vulnerabilities.

Key Features and Benefits

- Each SDL Workshop presents a core set of material, and includes lecture and hands-on labs that cover the history and evolution of the SDL, Threat Modeling, Secure Design Practices, and SDL tools.
- Workshops typically last three to five days depending on the content, and are tailored to meet the customer's specific needs and expertise without the need for additional prerequisite training.

To view a full datasheet for this service please visit:
http://aka.ms/Ojar1m

Microsoft

Find out more about Microsoft Premier Support

For further information or if you would like to discuss your specific needs, please, contact your Microsoft Services representative.

http://microsoft.cz/services

To get up-to-date version of this catalogue please follow this link:

http://aka.ms/PremierSecurityCatalogue