Offline Assessment for Active Directory Security

Duration: 4 Day engagement, 12 month subscription
Location: Onsite

Overview
Gain an insight into the security of your Active Directory environment by proactively diagnosing issues and risks and receiving continuous updates to best practice guidance.

Analyze the security of your Active Directory environment against best practices developed by Microsoft technology experts, then work with a Microsoft engineer to understand your results and develop a plan that limits risk and improves your environment.

Objectives
• Gain an expert’s perspective on what issues to address first.
• Optimize your environment based on Microsoft best practices to prevent issues before they arise.
• Establish a baseline so you can track your progress throughout the year.
• Ensure assessment data does not leave your premises.

Methodology
Setup your assessment
Prior to working with your Microsoft engineer, you will setup your assessment and generate your first set of results.

Expert analysis
Your Microsoft engineer will analyze your results, help you understand each issue identified and ensure that you have the right information to fix the issue.

Persist and improve
Re-asses your environment on a monthly basis using the latest updates to continually drive improvement throughout the year.

Scope
Assess security risks of your infrastructure to identify potential vulnerabilities, including credential theft attacks, identity management, and domain and forest security configurations.

This assessment runs on a single Active Directory Domain Services (AD DS) forest that is hosted on physical hardware or virtual machines.

Agenda
Welcome call
Occurs 2-4 weeks before delivery with your Microsoft Engineer and Technical Account Manager.

Setup and initial results
You complete the assessment setup and initial result gathering prior to your analysis.

Engineer led analysis
Your Microsoft engineer will analyze your results, lead the in-depth review of your findings, provide knowledge transfer and limited remediation work.

Your engineer will work with you to develop a prioritized list of recommendations.

Close out meeting
Finalize and deliver your results.
Offline Assessment for Active Directory Security Comparison

<table>
<thead>
<tr>
<th></th>
<th>Offline Assessment for Active Directory Security</th>
<th>RAP as a Service for Active Directory Security</th>
<th>RAP as a Service PLUS for Active Directory Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Duration</td>
<td>4 Days</td>
<td>1 Day</td>
<td>3 Days (1 remote/2 onsite)</td>
</tr>
<tr>
<td>Delivered remotely</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Subscription duration</td>
<td>12 months</td>
<td>12 months</td>
<td>12 months</td>
</tr>
<tr>
<td>Data storage</td>
<td>On-Premises</td>
<td>Cloud hosted</td>
<td>Cloud hosted</td>
</tr>
<tr>
<td>Training and planning on findings</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Detailed Scope and Requirements

**Technical Scope:**
- Review of operational processes
- Review of the privileged accounts/groups membership as well as regular account hygiene
- Review operating system configuration, security patch, and update levels
- Review of domain and domain controller configuration compared to Microsoft recommended guidance
- Review of key Active Directory object permission delegation
- Review of the forest and domain trusts

**Software Requirements:**

All Offline Assessment data remains onsite

With Offline Assessments, your data never leaves your site.
- All data collection and analysis is done locally on a machine that you provide.
- No data is transported outside your physical location to ensure maximum control and protection of your data.
- All data is analyzed by the Offline Assessment client, which only requires local area network connectivity.
- Internet connectivity is only required to activate your account and download the Offline Client toolset.

Be proactive across Focus Areas

- **Availability and Business Continuity:** Maximize your service availability and plan for disaster recovery
- **Change and Configuration Management:** Manage changes to services configuration settings across your environment.
- **Operations and Monitoring:** Manage and perform day-to-day operations within your environment.
- **Performance and Scalability:** Deliver the expected user experience by managing current and future performance and capacity requirements.
- **Security and Compliance:** Protect your services from attack and ensure the integrity and privacy of your data.
- **Upgrade, Migration and Deployment:** Manage product or development lifecycles, migrations between platforms, and deployment of new services into your environment.

For more information

Contact your Microsoft Account Representative for further details.