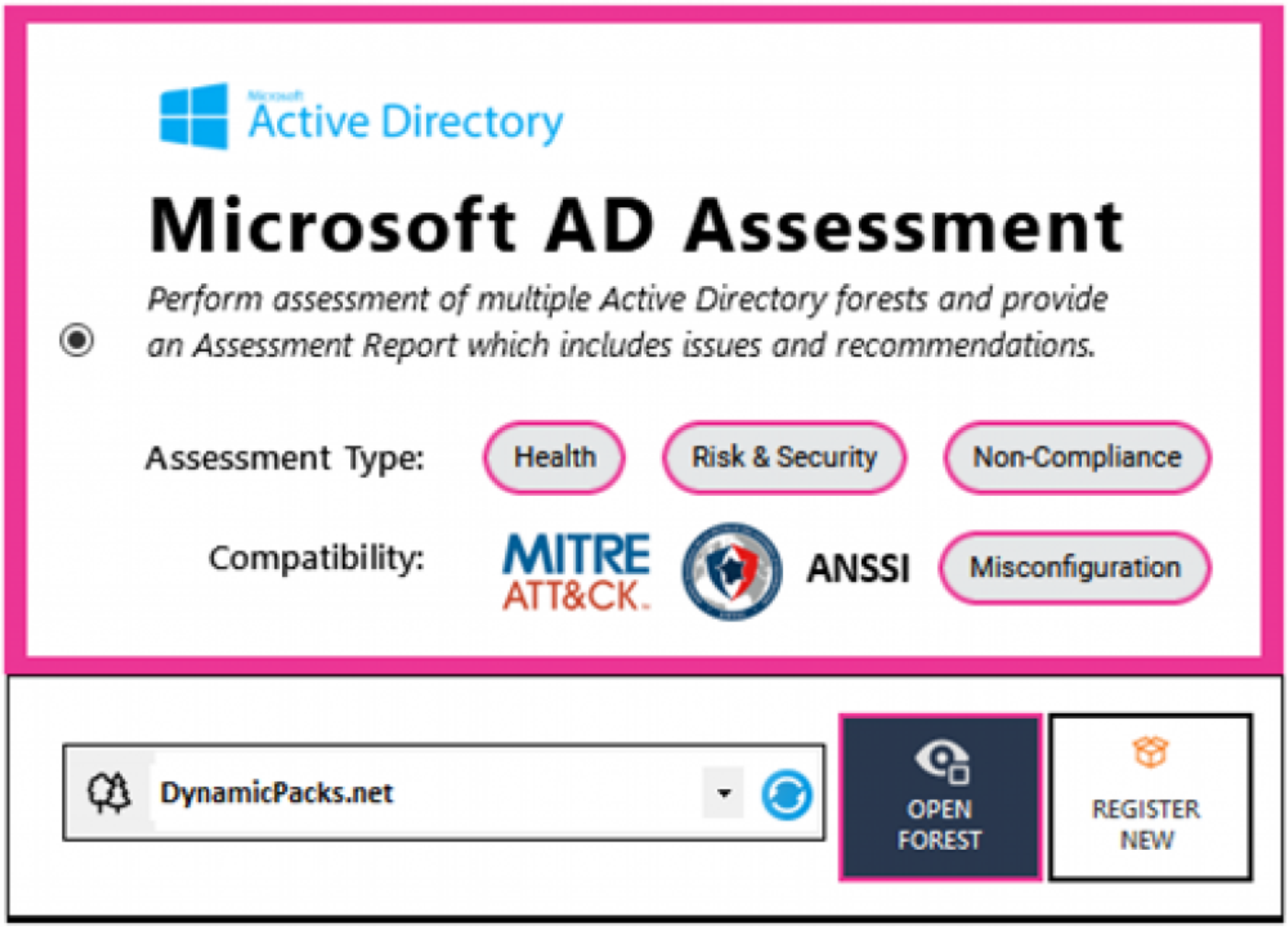
DynamicPacks SmartProfiler can perform Health and Configuration Checks as part of Active Directory Security Assessment

If you have made the decision to conduct an Active Directory Security Assessment for your production AD Forests, it is crucial to recognize the potential security threats that may exist within your Active Directory environment.



Memphis, Tennessee Jun 2, 2023 (Issuewire.com) - DynamicPacks Technologies

https://Microsoft-Assessment.com

If you have made the decision to conduct an Active Directory Security Assessment for your production AD Forests, it is crucial to recognize the potential security threats that may exist within your Active Directory environment. However, neglecting to address health and configuration issues poses a significant security risk. In this article, we will explore the importance of performing a "complete" Active Directory assessment, in addition to recommended security tests by organizations such as MITRE and ANSSI.

Assessment Categories and Methodology

Let's explore the assessment categories and methodology before delving into the specifics of the tests. Each assessment tool, whether it focuses on Active Directory, Office 365, or any other technology, should encompass five essential assessment categories: Health Check, Misconfiguration, Security and Risk, Non-Compliance, and Performance.

Health Check: Health Check involves evaluating the tool's capability to perform health checks on various components. For Active Directory, this may include assessing the KCC component, DNS, domain controllers, replication, active directory site coverage, partition backup, inconsistent states of domain controllers, orphaned domain controllers, undefined subnets, and DCDiag tests, among others.

Misconfiguration: Misconfiguration entails the tool's ability to identify and report misconfiguration items. In the context of Active Directory, this may cover aspects such as undefined subnets, AD Site Links, replication topology, time synchronization, Fine-Grained Password Policy (FGPP) parameters, Domain Account Policy parameters, strict replication, SMB1 protocol, unsecure updates, DNS scavenging, DNS round robin, manual connection objects, manual bridgehead servers, DNS static records and more.

Security and Risk: Security and Risk assessment involves evaluating whether the tool can perform a comprehensive analysis of security vulnerabilities and risks. Specifically for Active Directory, this may include examining Lan Manager Hashes, SMB Signing, LDAP Signing, NT4Crypto, accounts with blank passwords, accounts using SPNs, unauthenticated domain controllers and servers, credential caching in RODC, duplicate SPNs, unprivileged accounts with excessive permissions on OUs, non-default principal accounts with full control or write permission on critical directory objects, anonymous access to AD, and numerous other AD security tests.

Performance: Performance assessment focuses on the tool's ability to evaluate component performance. In the case of Active Directory, the primary focus is on domain controllers. It is important to monitor KCC and LDAP performance, as they heavily influence domain controllers' functionality, depending on the size of the environment. Issues such as dropped LDAP connections and incomplete KCC operations can arise due to performance issues, which should be categorized based on whether the domain controller runs on a physical server or within a virtual machine.

Non-Compliance: Non-Compliance evaluation involves checking for non-compliant items. For Active Directory, although the number of such items may be limited, the tool should at least highlight the privileged users added in the past 10 days. It should also assist in closely monitoring admin and user activities and facilitating recovery from security incidents.

While the Assessment Categories assist in selecting the appropriate Active Directory Assessment tool, the Methodology provides an overall perspective for both the IT Management Team and IT Operations Team. The tool should adopt a methodology that caters to the needs of both teams. The methodology should include the following:

Assessing the current environment level: The tool should evaluate the existing Active Directory environment and discover all domains.

Identifying Critical and High Risks: The Management Team needs to be aware of any critical and high-risk factors in the environment that might potentially disrupt business applications.

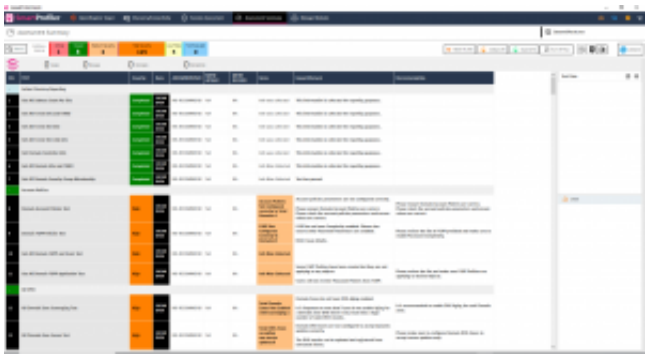
Prioritizing Items in an Action Plan: The Management Team must determine if there are critical and high-risk items that require immediate attention, considering the cost associated with addressing them. Since budget limitations may exist, prioritization becomes necessary.

You can find more about why it is important to perform a health and configuration assessment as part of Active Directory Security Assessment here:

Active Directory Health and Configuration check items

More about SmartProfiler for Active Directory can be found here:
https://microsoft-assessment.com/importance-of-health-and-configuration-checks-as-part-of-active-directory-security-assessment/smartprofiler-active-directory-assessment

All tests executed by SmartProfiler for Active Directory:
https://microsoft-assessment.com/blog/active-directory-security-and-health-testsand-recommendations-from-vendors-2



Media Contact

DynamicPacks Tech

Host@Microsoft-Assessment.com

9739930908

A2 597 Genesis Eco

Source : DynamicPacks Tech

See on IssueWire