SOLUTION BRIEF

stealthbits
NOW PART OF netwrix

SYSTEMS BEST PRACTICES

The Problem

When businesses began moving from mainframe systems to the client-server model of computing, a new set of hazards emerged. Gone were the days of a single mainframe system to maintain and secure. Today, information systems possess hundreds and sometimes thousands of individual security and operational configurations, both on the server and client side. While best practices are relatively easy to define to keep these systems in line, they are extremely difficult to implement, enforce, and verify for ongoing compliance.

With so many individual systems having unique security and configuration settings, it's not only important to consolidate security settings and system configurations into a consistent deployment, but also to detect and remediate systems as they fall out of compliance with defined standards. However, with so many questions and very few lasting answers in this ever-changing landscape, attackers are finding it effortless to exploit system vulnerabilities in a wide variety of ways.

The Challenge

Technologies like Active Directory (AD) and Privileged Identity Management (PIM) were introduced in large part to centralize control over systems and administration of accounts. Certain challenges have always existed, however, like systems not being connected to AD, accounts not being managed by PIM, or organizations allowing the use of local accounts and applications that are outside the purview of these technologies. When privileged identities, for instance, are allowed to run services, scheduled tasks, and web services completely outside of the centralized management Active Directory and Privileged Identity Management provide, what do best practices even look like for local systems?

The Solution

Through well over a decade of experience in engineering operating system-level management solutions, Stealthbits Technologies has developed and designed a series of best practice reports customers can leverage to understand vulnerabilities and inconsistencies across their desktop and server infrastructure, promoting security, compliance, and operational integrity through the establishment of strong foundations.

Privileged Account Auditing

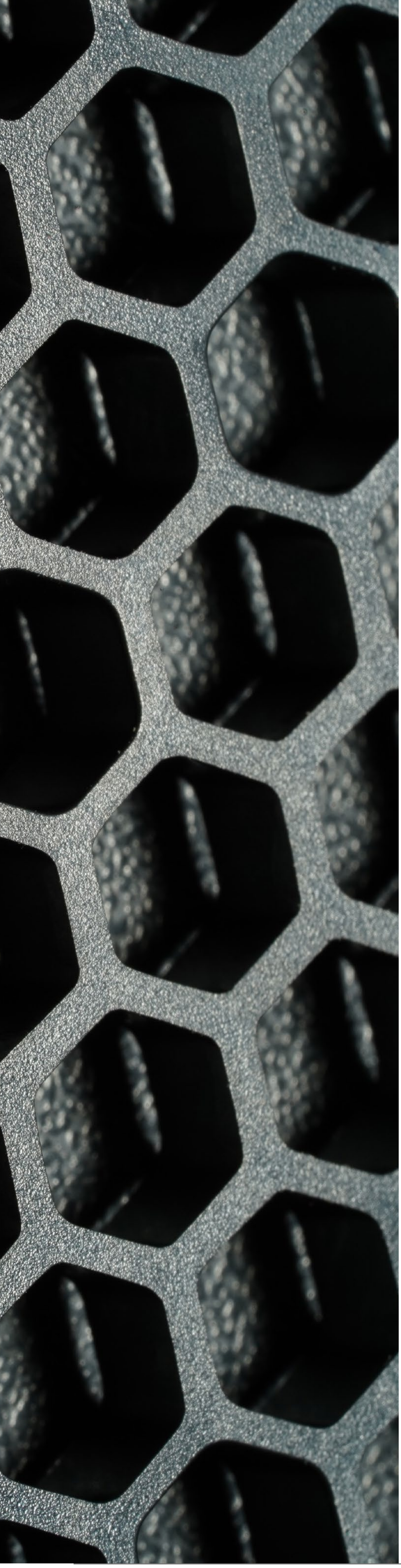
StealthAUDIT for Systems enables organizations to efficiently evaluate effective access across every desktop and server, while highlighting configurations and conditions that expose organizations to unnecessary risk.

- **Local Admin Credentials** – For organizations leveraging Microsoft LAPS, StealthAUDIT is able to determine if the targeted systems are configured and have LAPS enabled and what the LAPS configuration is. Identification of servers not configured to leverage LAPS can help identify at risk servers for stale or weak Local Administrator passwords.
- **Scheduled Task Credentials** – Determine what scheduled tasks are running on your servers. Also gain information as to which account is running the service and what task the service performs.
- **Service Account Credentials** – Understand where service accounts are being used on local systems and show which services they are running. Often when service account passwords are changed in AD the locally used services constantly lock the account out with invalid credentials.

Desktop and Server Auditing and Compliance

StealthAUDIT for Systems' robust auditing capabilities and baseline conformance framework enable organizations to understand where missing or inaccurate configurations exist across desktop and server infrastructure, in addition to conditions attackers regularly exploit during breach scenarios.

- **Applications that run at startup** – Monitor applications that are set to startup at logon. Knowing which applications run at startup can help improve performance and overall security of the operating system by helping identify potentially malicious software.
- **Prevent local accounts from going across the network** – Report if local accounts are allowed access across the network. Common accounts like network service are considered trusted between some systems and could be used maliciously for lateral movement.
- **Malicious security support providers** – Monitor and control security packages to protect active directory admin accounts hashed on local systems. Compare the default Security Support Providers list against hosts to look for malicious providers.
- **Monitoring PowerShell for malicious attacks** – Detect offensive PowerShell commands in PowerShell logs. PowerShell is a very powerful platform that can execute commands that fly under the radar of most SIEM solutions.
- **Restrict anonymous access check** – Determine if anonymous access is restricted to systems and what anonymous access is allowed. Anonymous access can be detrimental as anyone is able to access a system.
- **WDigest settings check** – Scan for systems that have WDigest enabled and are storing clear text passwords in memory. If a malicious actor is able to gain privileged access to a system, they can compromise clear text passwords as well as password hashes.
- **LSA protection check** – Scan for systems that do not have LSA Protection enabled. LSA Protection helps secure the LSASS process from code-injection on a system, this adds an extra layer of protection to the credentials stored in memory within the Local Security Authority (LSA).
- **Run and run once check** – Assess applications that are set to run at user logon. Also identify if applications are configured to run every time or run once.
- **Installed applications** – Identify installed applications and roles on windows servers. View ap-plication versions and changes between scans.



Summary

Every attacker is after the same two things: credentials and data. Desktop and server infrastructure con-tain the credentials and data attackers are looking for, and are leveraged in virtually every breach scenar-io. Insecure and improperly configured systems enable bad actors to perpetrate their attacks, as they rely on common vulnerabilities and configurations to obtain the privileges they need to access the resources they aim to compromise. The ability to automate the process of assessing alignment to best practices at the operating system level enables organizations to establish and maintain the strong foundation need-ed to thwart attacks and mitigate their risk of breach and operational catastrophe.

IDENTIFY THREATS. SECURE DATA. REDUCE RISK.

Stealthbits Technologies, Inc. is a customer-driven cybersecurity software company focused on protecting an organization's sensitive data and the credentials attackers use to steal that data. By removing inappropriate data access, enforcing security policy, and detecting advanced threats, our highly innovative and infinitely flexible platform delivers real protection that reduces security risk, fulfills compliance requirements, and decreases operational expense.

stealthbits