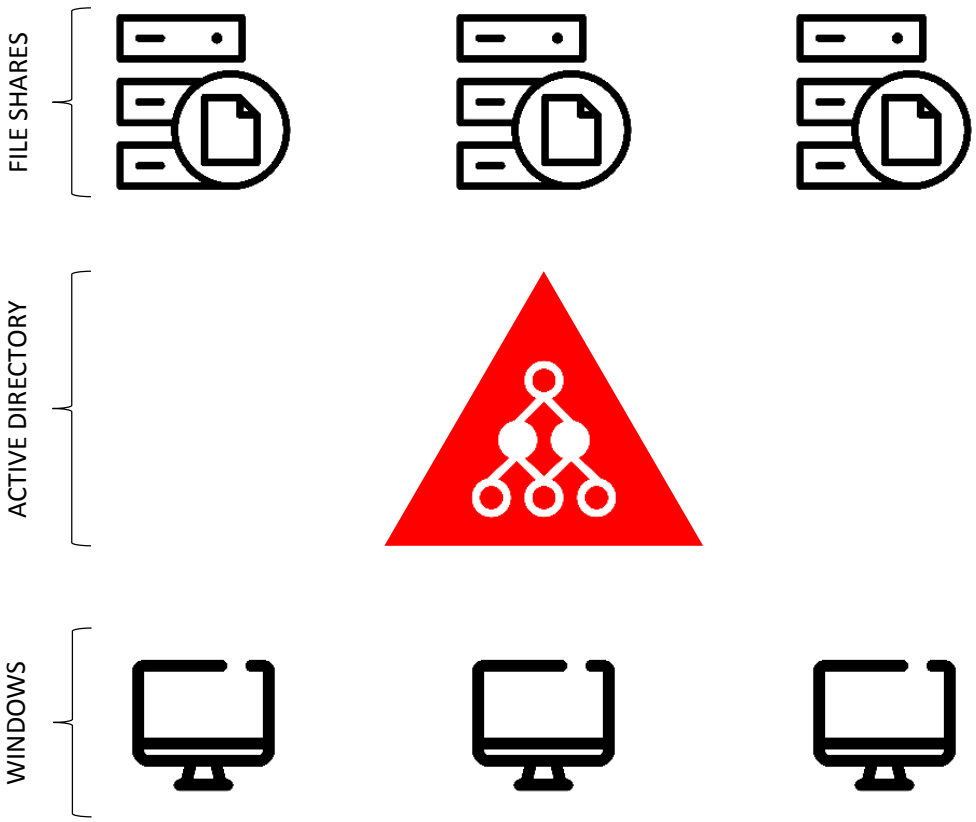
EXAMPLE REPORT
Globex Corporation

STEALTHbits TECHNOLOGIES | PLEXEON

STEALTHbits' Credential and Data Security Assessment (CDSA)

Regardless of an attacker's entry point into an organization, they're always after the same two things – credentials and data. In response, STEALTHbits works to remove inappropriate data access, secure the credentials attackers seek to compromise and exploit, and detect, prevent, and mitigate advanced threats at the endpoint, directory, and data layers of your environment.

To help shine a light on where you're most vulnerable, STEALTHbits Technologies has engineered and conducted a comprehensive assessment of your Network File Share, Active Directory, and Windows Server infrastructure. The analysis detailed in the pages to follow will provide clear insight into the security stature of your credentials and data.



Scanned Environment

The following is a summarization of the scope of the assessment performed, as well as the analysis performed on the collected data.

File Shares

Number of Hosts:

- 2

Number of Shares:

- 361

Number of Folders:

- 540,621

Number of Files:

- 39,006,138

Number of Permissions:

- 369,878,600

Storage Size Scanned:

- 7,250.35 GB

- Open Access
- Sensitive Data
- Stale Data
- High-Risk Permissions

Active Directory

Number of Domains:

- 1

Number of Users:

- 7,750

Number of Groups:

- 4,364

Number of Computers:

- 13,230

Number of OUs:

- 109

Number of Permissions:

- 8,099,223

- Weak Passwords
- Sensitive Groups
- Toxic AD Objects
- Object Permissions

Systems

Number of Servers:

- 81

Number of Desktops:

- 1

Operating Systems:

- Windows Server 2012 R2 Standard (80%)
- Windows Server 2008 R2 Standard (15%)
- Windows Server 2012 R2 Datacenter (2%)
- Windows 7 Professional (1%)
- Windows Web Server 2008 R2 (1%)

- Administrative Access
- Service Accounts
- Ticket and Credential Management

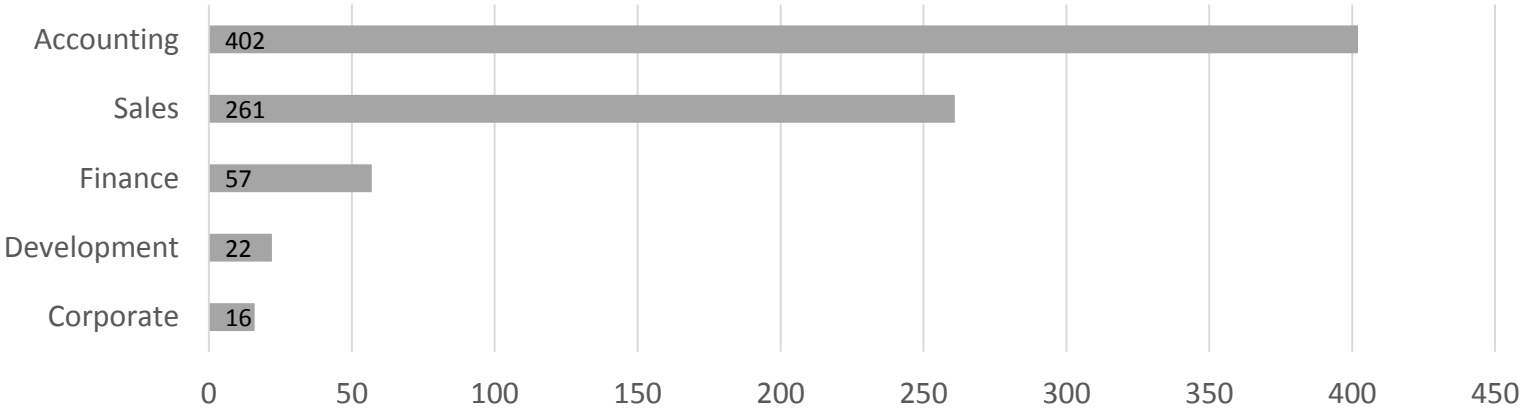
CONDITION: Open Access

Open Access is a condition referring to the use of Global Security Groups (a.k.a. Well-Known Security Principals) being used to provide access to resources – in this case Network File Shares.

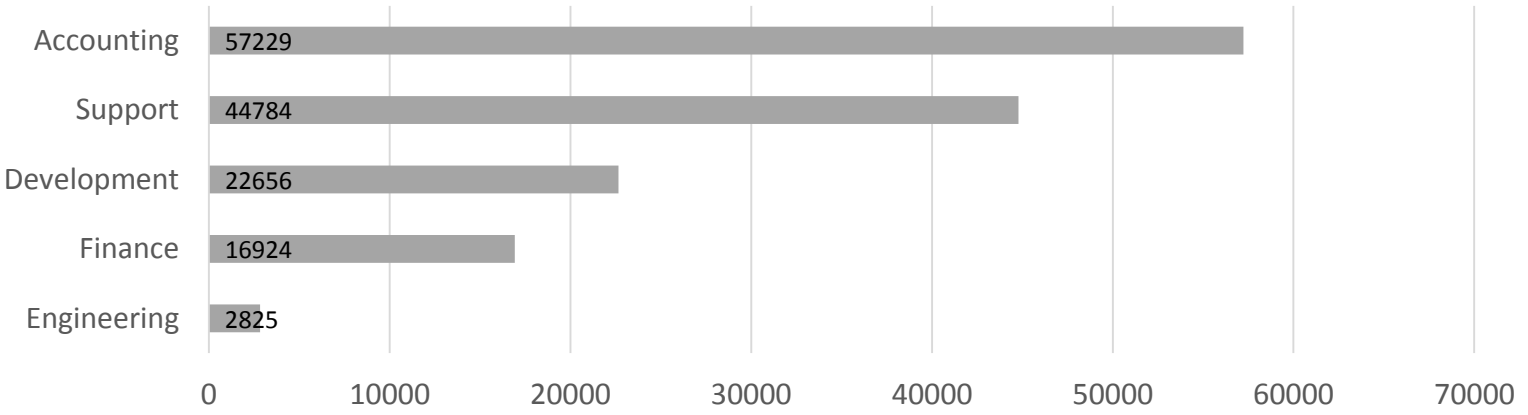
These groups (Everyone, Authenticated Users, Domain Users) should almost never be used to provide access to data resources, as it exposes organizations to significant risk of data breach, inappropriate data use, and even compliance failure.

# of Folders with Open Access	**144,794**
% of Folders with Open Access	**26%**
# of Sensitive Files with Open Access	**8,285**

Top Shares with Open Access (by # of Sensitive Files)



Top Shares with Open Access (by # of folders)

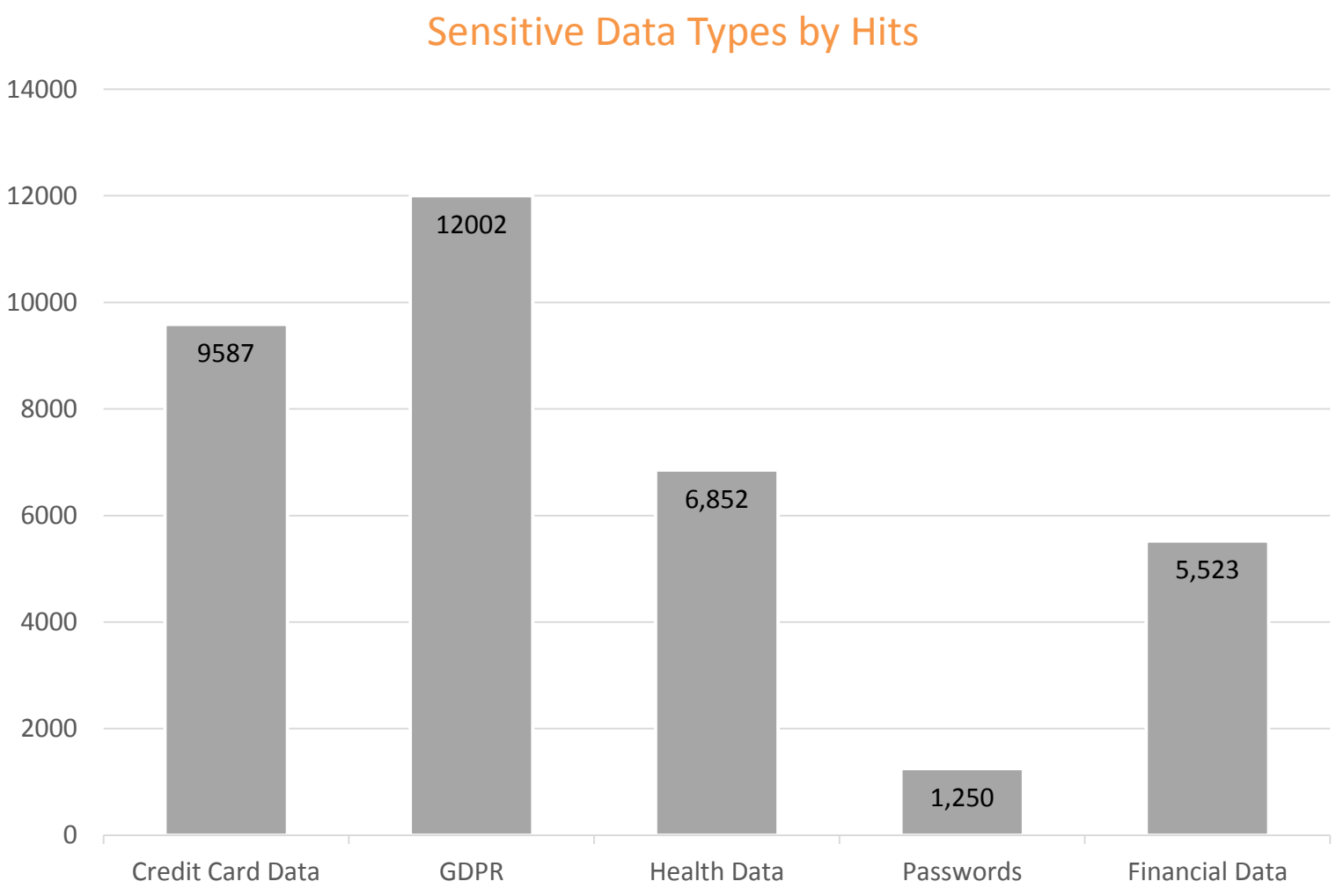


CONDITION: Sensitive Data

Sensitive data (e.g. data containing personally identifiable information about employees or customers, trade secrets and other private business information, health information, etc.) can exist in virtually any file, anywhere within an organization.

Understanding where this data exists, in what quantity, and how it has been secured is a necessity for security and compliance, and should be remediated in accordance with Least Privilege Access principles.

# of Files with Sensitive Data	**27,983**
# of Groups that Grant Access to Sensitive Data	**882**
% of Shares Containing Sensitive Data	**58%**



CONDITION: Stale Data

Recent studies estimate that over 40% of corporate data is not only stale, but hasn't been accessed in over three years.

Understanding and proactively addressing stale data presents real opportunities for both risk reduction and cost savings, as less data to manage makes it easier to secure and reduces the necessity for spending on new storage and the overhead costs associated with it.

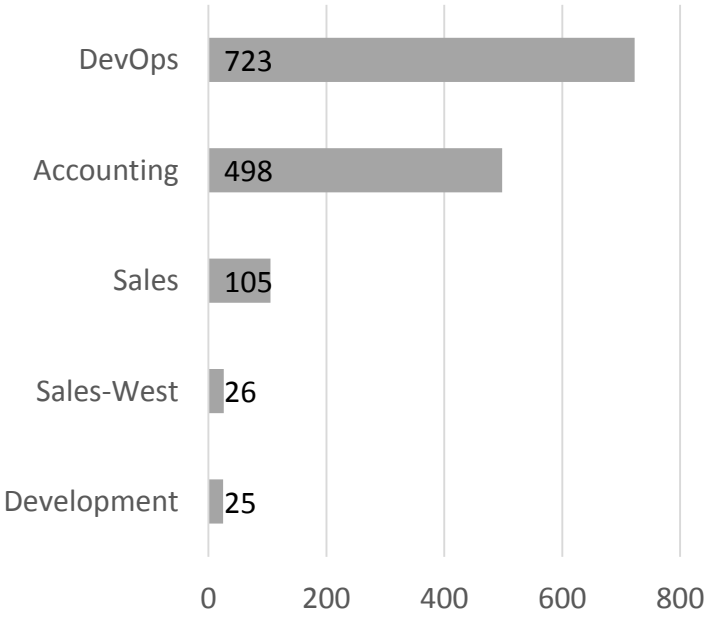
With additional context around stale data that is also sensitive and potentially subject to longer retention periods as a result of compliance mandates, stale, sensitive data can be easily moved to more secure locations or taken offline completely to drastically reduce the risk of otherwise highly avoidable data loss.

Organizations that invest in effective archival strategies are often able to realize storage cost savings in the millions, reallocating funds to other critical projects and priorities.

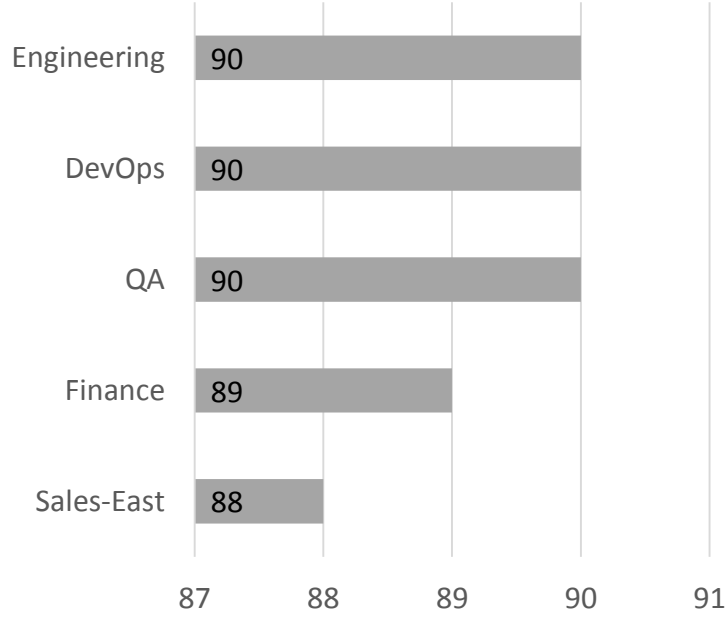
% of all Data that is Stale

62.8%

Stale Sensitive Files by Shares (Top 5)



Stale Files by Shares (Top 5)



CONDITION: Risky File System Permissions

Managing file systems permissions, especially in shared environments, has traditionally been highly complex and error prone. Different security models employed over many years, often with conflicting philosophies, have only added to the complexity of understanding weak spots in the permissions structure, resulting in large sums of at-risk data. Some of the riskiest and most common file system permissions conditions are explained below and should be remediated to reduce risk, increase security, and ensure compliance with regulatory standards.

- **High Risk Permissions** – The use of global security groups and other well-known security principals (e.g. Everyone, Domain Users, Anonymous Login) leaves data openly accessible to large populations of users
- **Broken Inheritance** – When the inheritance of permissions are broken within the file system structure, it often leads to incorrect access for users, either overprovisioning their access rights or preventing them from accessing data needed to perform their job function
- **User ACLs** – Leveraging user objects to provide access to data directly (rather than through security group memberships) makes it highly difficult to understand what users have access to or control that access
- **Historical SIDs** – The use of historical SIDs can make migration processes easier or facilitate smooth transitions during M&A activities, but can also present significant risks to security as they obscure how users are gaining access to data, in turn making it difficult to control access rights
- **Unresolved SIDs** – User accounts with unresolved SIDs are users that no longer exist, and therefore should no longer have access to data

# of High Risk Permissions	**58,435**
# of User ACLs	**259,426**
# of Unresolved SIDs	**26,804**
# of Instances of Broken Inheritance	**193,491**
# of Historical SIDs	**0**

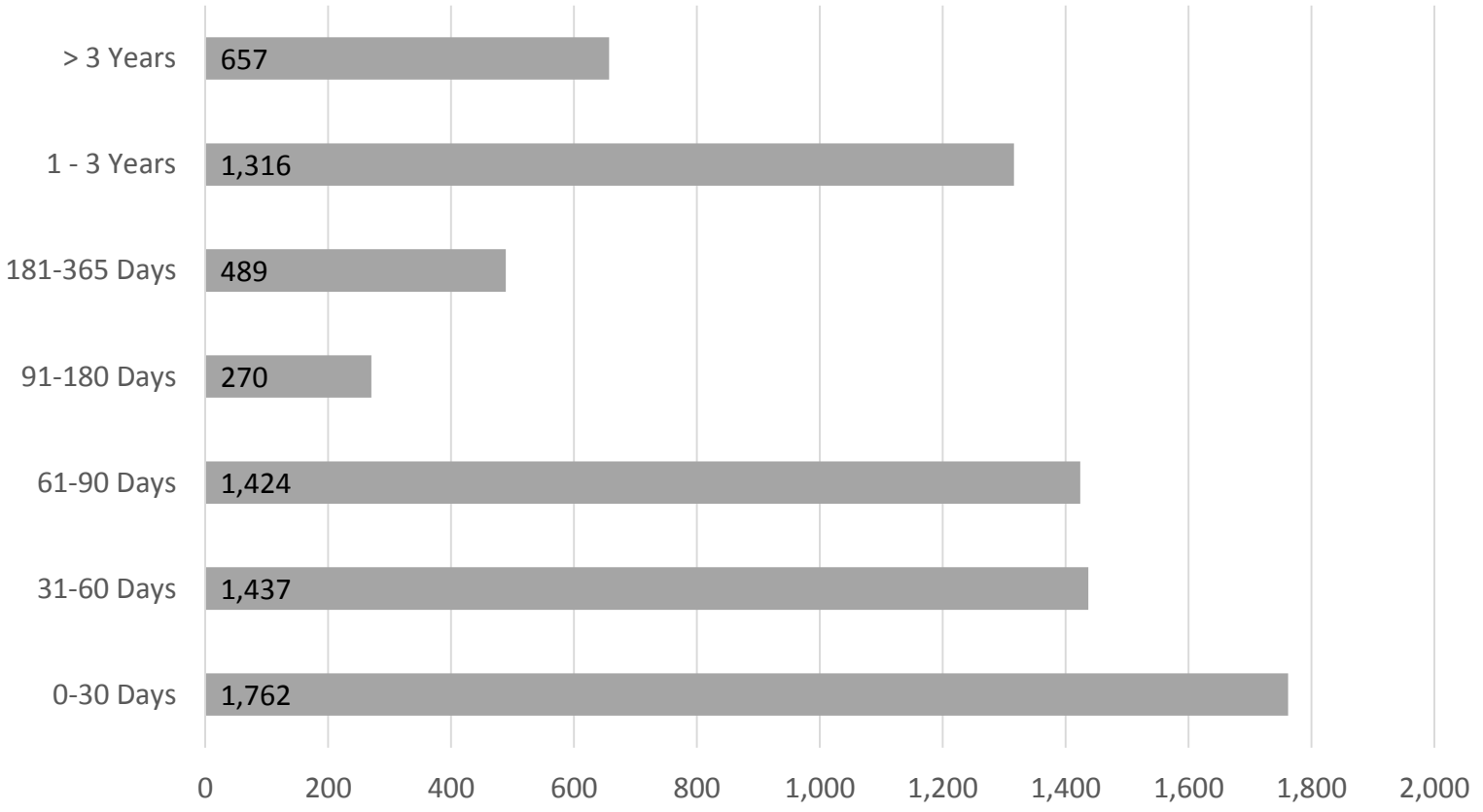
CONDITION: Weak Passwords

Password strength is an important component of any organization's overall information security strategy.

Identifying users leveraging passwords contained in publically available password dictionaries and organizationally-defined unapproved password lists allows security personnel to proactively identify accounts most susceptible to successful brute force or password guessing attacks. Leveraging strong passwords across all accounts effectively mitigates risk for the organization as a whole.

# (%) of Users with Weak Passwords	**944 (12.18%)**
# (%) of Users with Weak Passwords in History	**312 (4.02%)**
# (%) of Users with Common Passwords	**594 (7.66%)**
# (%) of Users with Non-Expiring Passwords	**304 (3.92%)**
# (%) of Accounts with Reversible or Weak Encryption	**7257 (93.64%)**
# of Passwords Exposed via Group Policy Preferences	**2**

Password Age Distribution



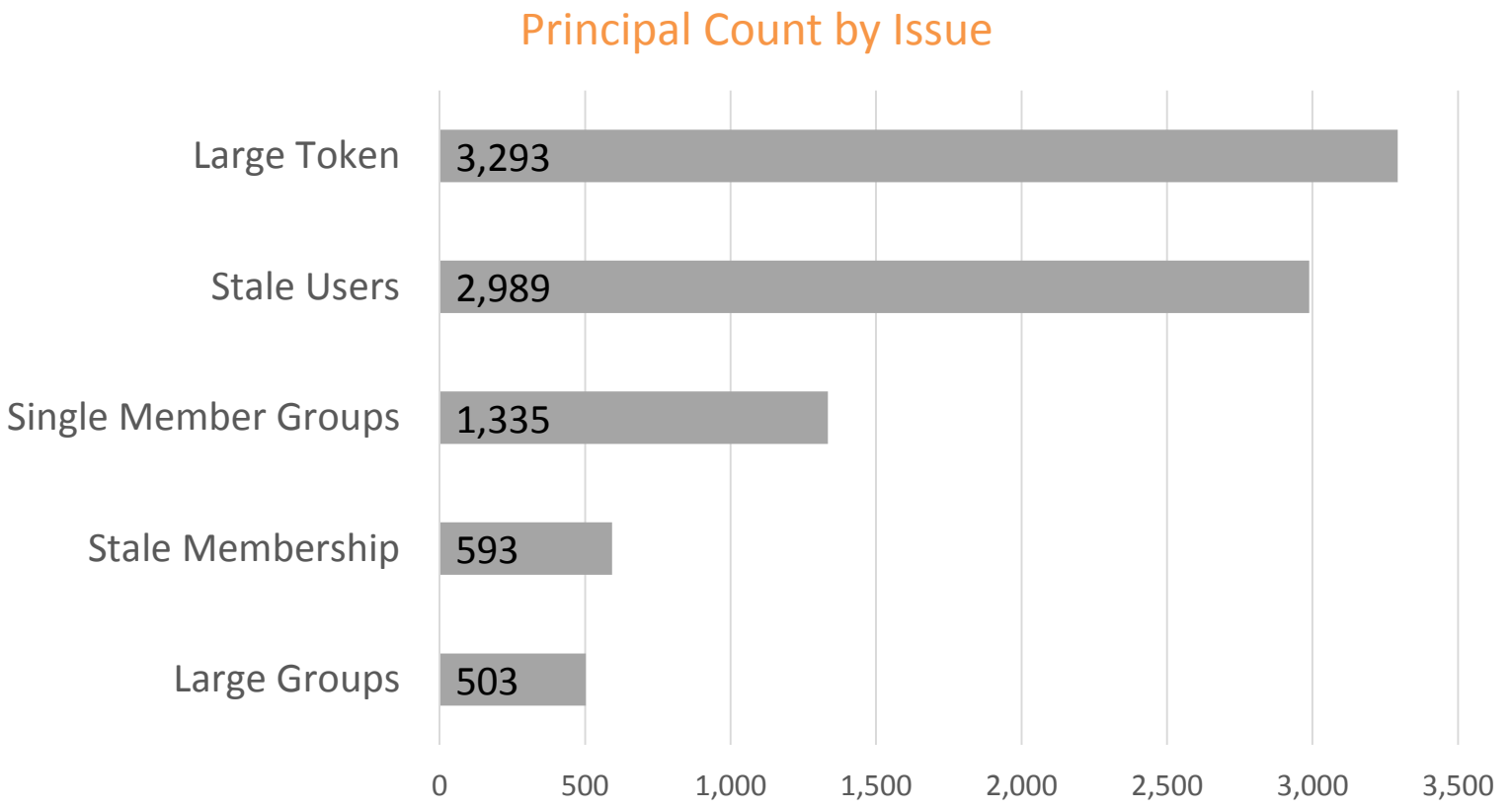
CONDITION: AD Object Toxicity

Most Active Directory environments have undergone significant transitions and transformations over time due to events like mergers, acquisitions, divestitures, migrations, and upgrades. Additionally, many organizations have adopted differing philosophies of how Active Directory should be managed and secured over the years, resulting in a plethora of "toxic" conditions and configurations that put Active Directory at risk of compromise or even catastrophic outage.

Clearing away the clutter of stale objects makes administering and securing Active Directory easier, and understanding how AD itself has been secured also shines a light on where attention is needed most to thwart modern cyber attacks.

Active Directory Object Permissions (# of Users)	
Reset Password Rights	**66**
Group Membership Change Rights	**66**
Domain Replication Rights	**3**

Stale Objects by Count (enabled/disabled)	
Users	**668/2,041**
Computers	**7,466/88**
Groups	**586/67**



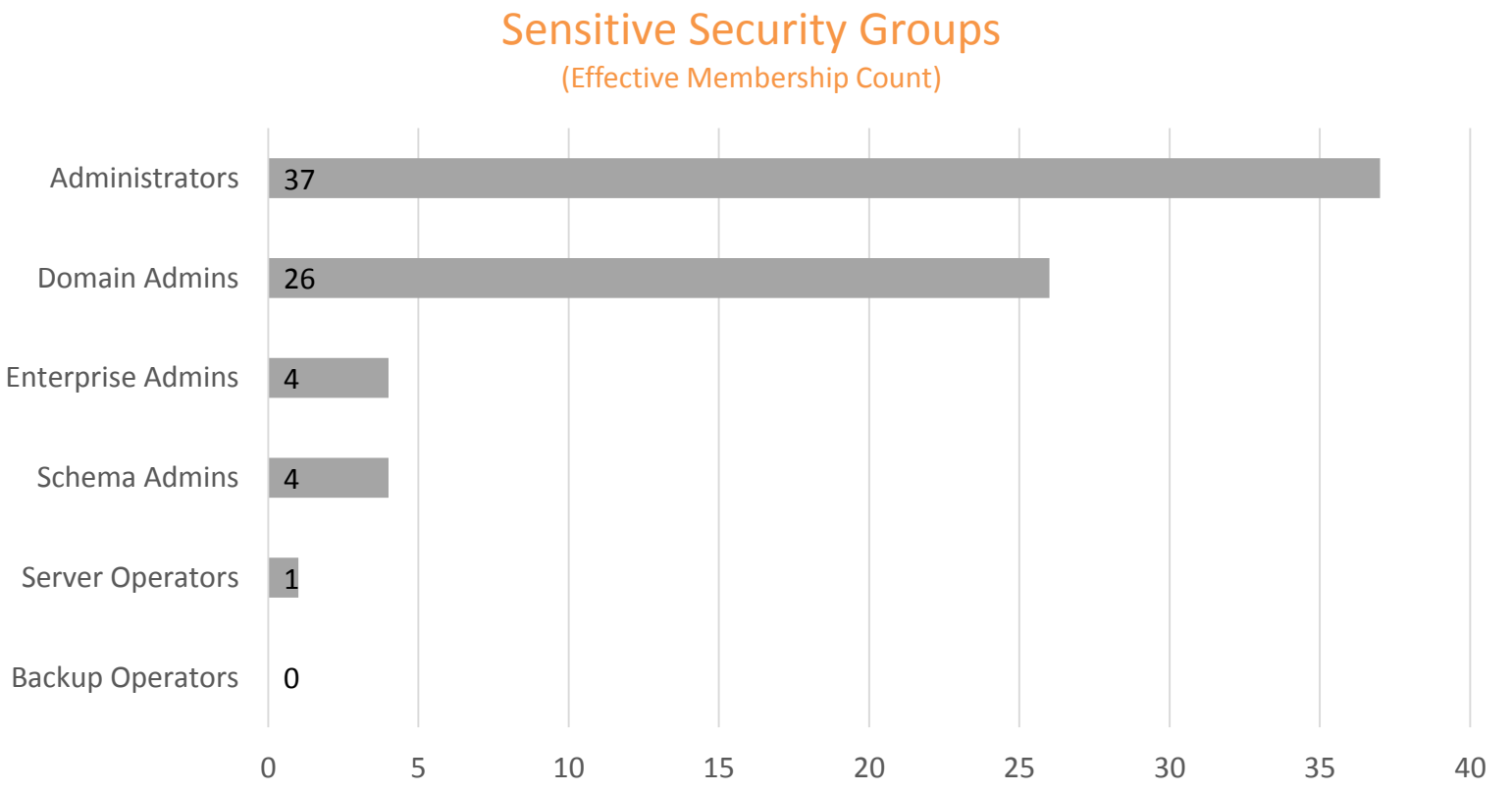
CONDITION: Sensitive Security Group Membership

Members of Sensitive Security Groups like Domain, Enterprise, and Schema Administrators have the highest levels of privilege within an Active Directory environment. If stolen by an attacker or abused by an internal bad actor, the critical changes these accounts can make can have devastating effects on the security of Active Directory and everything connected to it.

Administrative access through sensitive security groups should be provisioned on a least-privilege basis. In order to achieve this model successfully, it is advisable to remove all stale, disabled, and expired accounts, institute strong password security on all accounts in scope, perform regular certifications of sensitive security group membership, and alert on any changes to these groups the instant they occur.

Privileged Access Summary

# Users with Privileged Access Rights	**38**
Password Never Expires (user count)	**22**
Oldest Password Age (in days)	**7,518**



CONDITION: Local Admin Rights

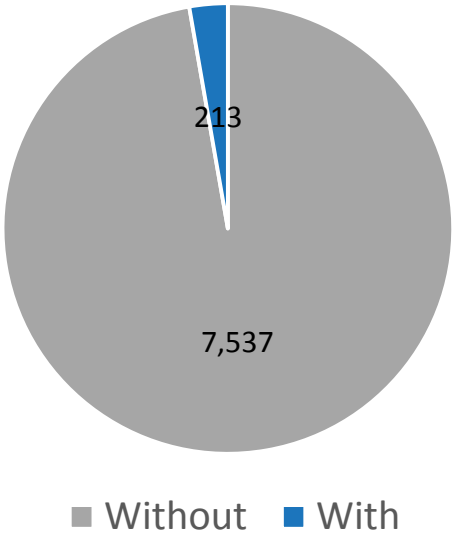
Excessive privileged access across Windows desktop and server infrastructure allow attackers to more easily compromise credentials and systems, move laterally and vertically, and ultimately obtain complete control over Active Directory and everything connected to it.

Foundation-level security starts with limiting Local Admin and equivalent rights to the lowest levels possible. With a strong foundation to build off of, investments in complementary technologies like Antivirus, Endpoint Protection, and patch management produce greater ROI through increased effectiveness.

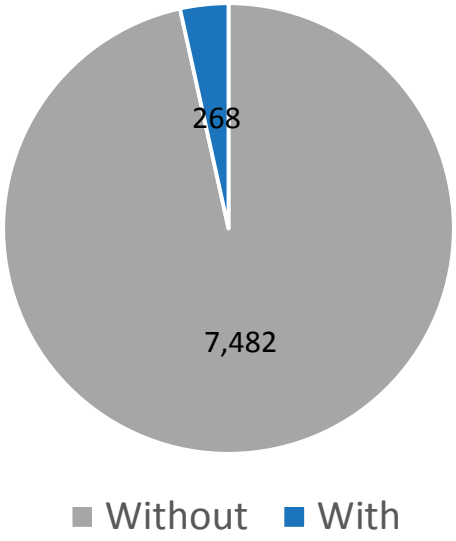
Top 10 Systems by Local Admin Count

GCQAVM47	**54**
GCIMPSRV05	**48**
GCNYSRV22	**47**
GCORPSRV55	**45**
VM120	**43**
TOMT-W2K12-5	**43**
DEV_OUTLOOK-22	**42**
GCMBXSRV	**42**
GCH32-NY	**42**
DC01	**41**

Users with Local Admin Rights



Users with Logon Rights



CONDITION: Service Accounts and Windows Vulnerabilities

Misconfigured security settings, missing patches, and overexposed service accounts are just a few ways in which attackers circumvent security controls, locate and steal privileged credentials, and elude detection.

Ensuring critical security settings are configured properly across all systems significantly limits an attacker's options after initial system compromise. With fewer attack tactics, techniques, and procedures at their disposal, they're forced to leverage more overt options, increasing their likelihood of detection.

Service Accounts

Domain Users (Services & SPNs)
18

Average Password Age (days)
2,084

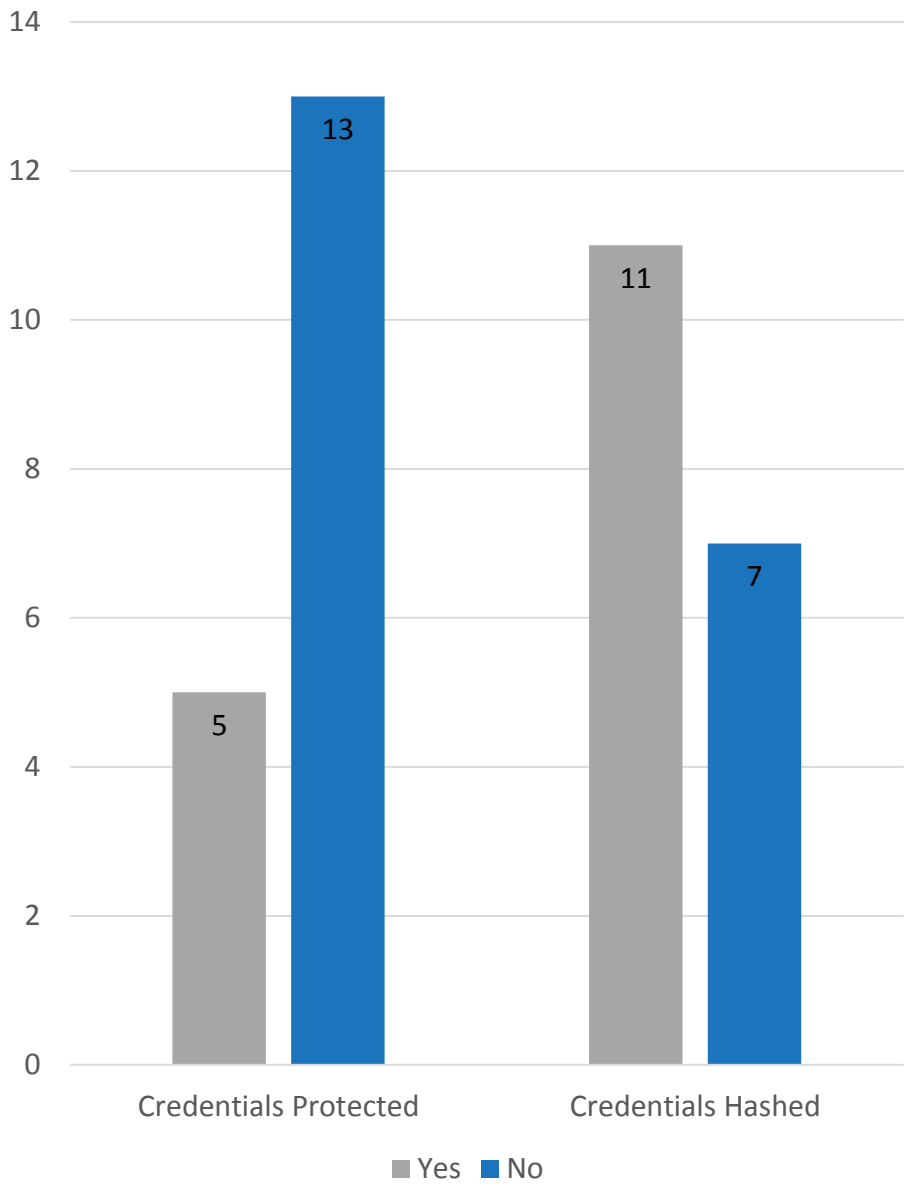
Oldest Password (days)
502

Ticket & Credential Management

LSA Protection (enabled | disabled)
5|13 Systems

WDigest (enabled | disabled)
11|7 Systems

Suspicious PowerShell Commands
Found on 0 Systems



HIGH RISK – TOP 5

- 8285 files containing sensitive data are accessible via Open Access
- 12.18% of all user accounts are using default, weak, or well-known passwords
- There are 66 different users that can reset the passwords of accounts other than their own
- 882 different security groups are being used to grant access to sensitive data
- There are 2 plaintext passwords stored in the SYSVOL share of your Domain Controllers

MEDIUM RISK – TOP 5

- 3 user accounts have the ability to replicate directory objects
- 7257 user accounts passwords can be easily cracked because of reversible or weak encryption
- LSA protection is disabled on 72% of all your systems
- There are 259,426 instances of user objects being used to provide access directly to data
- 3% of all users have Local Admin rights to at least one system in your environment

LOW RISK – TOP 5

- 62.8% of all data scanned hasn't been modified in 365 days or more
- The average token size across the entire user population is 1,413
- 35% of all User objects , 57% of all Computer objects, and 15% of all groups are considered stale
- 193,491 instances of broken inheritance were identified across the scanned file shares
- The average password age across all identified service accounts is 2,084 days

Glossary

Open Access
Open Access occurs when global security groups or other well-known security principals like Everyone, Domain Users, and Authenticated Users are used to provide access to data.

Sensitive Data
Sensitive data, in the context of this assessment, can mean any data subject to a mandated compliance standard, data that could cause material harm to an individual or business if revealed, or data that if lost could cause damage or distress to an individual or business.

Least Privilege Access
The principal of least privilege dictates that a user only be granted the privileges necessary to perform their function.
https://en.wikipedia.org/wiki/Principle_of_least_privilege

Stale Data
In the context of this assessment, stale data is any file that has not been modified within the past 365 days.

Weak Passwords
In the context of this assessment, weak passwords are those that leverage passwords contained in publically-available password dictionaries or organizationally-defined unapproved password lists, regardless of whether their password meets complexity requirements.

Group Policy Preferences
Group Policy preferences enable administrators to configure, deploy, and manage greater numbers of operating system and application settings.
https://msdn.microsoft.com/en-us/library/cc512161(v=vs.85).aspx

Token Size
The number of security groups a user belongs to dictates the size of their Kerberos token. If above a certain size, a user will be unable to authenticate to network resources, preventing them from performing various job functions.
https://support.microsoft.com/en-us/help/327825/problems-with-kerberos-authentication-when-a-user-belongs-to-many-grou

LSA Protection
The LSA, which includes the Local Security Authority Server Service (LSASS) process, validates users for local and remote sign-ins and enforces local security policies. The Windows 8.1 operating system provides additional protection for the LSA to prevent reading memory and code injection by non-protected processes. This provides added security for the credentials that the LSA stores and manages.
https://docs.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/configuring-additional-lsa-protection

WDigest
The Digest Authentication protocol is designed for use with Hypertext Transfer Protocol (HTTP) and Simple Authentication Security Layer (SASL) exchanges. These exchanges require that parties that seek to authenticate must demonstrate their knowledge of secret keys.
https://technet.microsoft.com/pt-pt/library/cc778868(v=ws.10).aspx

Notes

STEALTHbits Technologies is a cybersecurity software company focused on protecting an organization's credentials and data. By removing inappropriate data access, enforcing security policy, and detecting advanced threats, we reduce security risk, fulfill compliance requirements and decrease operations expense.