



Mitigating Insider Threats in Active Directory: Strategies, best practices, and tools

Vivin Sathyan
vivin.sathyan@manageengine.com

Know about Melatonin?

Melatonin is a natural hormone that's mainly produced by your [pineal gland](#), which is a tiny gland in your brain. Your brain releases it when you sleep in complete darkness.

Melatonin also gets secreted **during a pre/post lunch technical session!**



Types of insider threats

Types of insider threats according to Verizon



Malicious insiders

Employees or partners who use their legitimate access to corporate data for personal gain



Inside agents

Malicious insiders recruited by external parties to steal, alter, tamper with, or delete valuable data



Disgruntled employees

Emotional attackers who seek to harm their organization as revenge for some sort of perceived wrong



Careless workers

Employees or partners who neglect or ignore the rules of an organization's cybersecurity policy



Third parties

Third-party vendors who misuse their access and compromise the security of sensitive data

3 Insider Threat Statistics You Should See

1 Insider Threat Frequency of Attacks

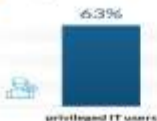
- say that insider attacks have become more frequent over the last 12 months
- companies have had an insider attack in the past year
- data breaches are caused by insider threats
- organizations had more than 20 incidents in the past year
- increase in insider-caused cybersecurity incidents since 2019
- increase in frequency of insider data breaches through 2021



2 Top Motivations for Insider Attacks



3 Top Insider Threat Actors



I am not worried about this



I am worried about this - Admin error



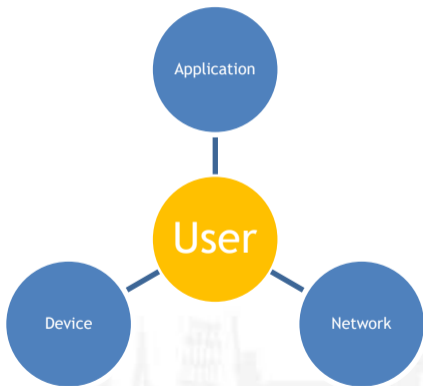
I am worried about this - User error



User education is good but it has to be contextual



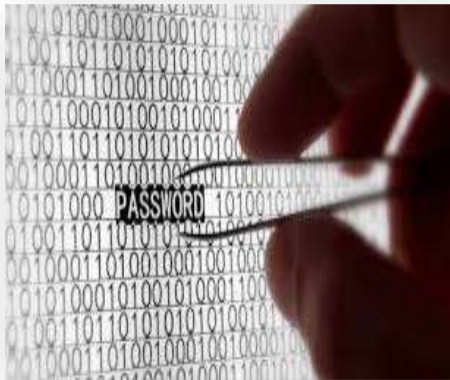
Insider Threat Priority 1: Securing **user** identities



Insider Threats and Active Directory



Live (if the internet works) Active Directory Hack



3-stage attack

1. **Copy** ntds.dit and system file.
2. **Extract** password hashes from ntds.dit using system file.
3. **Crack** hashes to reveal user passwords.

Two target files

The image displays two side-by-side screenshots of Windows File Explorer windows. The left window shows the contents of a folder named 'NTDS'. The right window shows the contents of a folder named 'C:\Windows\System32\config'.

Left Window (NTDS folder):

Name	Date modified	Type
edit04	4/4/2013 11:13 AM	Recovered I
edit0004.log	3/16/2013 9:17 AM	Text Document
edit0004.log	3/16/2013 9:17 AM	Text Document
edit00001.jr	4/18/2013 5:44 PM	MS File
edit00002.jr	4/18/2013 5:44 PM	MS File
ntds.dit	4/7/2013 1:10 PM	DIT File
temp.edb	4/7/2013 1:10 PM	EDB File
editmp.log	2/10/2013 1:25 PM	Text Document

Right Window (C:\Windows\System32\config folder):

Name	Date modified	Type
Amrval	6/22/2013 8:25 PM	File folder
PlayTech	6/20/2013 11:15 AM	File folder
systemprofile	11/14/2013 10:42 PM	File folder
Trk	11/14/2013 11:12 PM	File folder
DCD-Templates	4/26/2013 8:25 AM	File
COMPONENTS	1/12/2013 8:36 AM	File
COMPONENTSLOG	6/22/2013 8:25 PM	Text Document
DEFAULT	6/22/2013 8:42 PM	File
DEFAULT.LOG	6/22/2013 8:25 PM	Text Document
DRIVERS	3/28/2013 9:22 PM	File
FF	6/22/2013 8:25 PM	File
refloguser1	4/6/2013 11:15 AM	2048 File
refloguser2	4/6/2013 11:15 AM	2048 File
SAM	6/22/2013 8:42 PM	File
SECURITY	6/22/2013 8:42 PM	File
SECURITY.LOG	6/22/2013 8:25 PM	Text Document
SOFTWARE	6/22/2013 8:42 PM	File
SYSTEM	6/22/2013 8:25 PM	Text Document
SYSTEM	6/22/2013 8:42 PM	File



```
Administrator: Command Prompt
C:\>vssadmin create shadow /for=C:
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2013 Microsoft Corp.

Successfully created shadow copy for 'C:\'
Shadow Copy ID: {0F0c03d7-4965-44b6-9f1e-9b63cdsfd14e}
Shadow copy volume name: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy79

C:\>copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy79\windows\ntds\ntds.dit
C:\users\vivrn-1438\desktop
1 file(s) copied.

C:\>
```



a486c00296356dc9f7d10b8737b0bc7e32099541
5d834b328bb637eeef49b6624774bded566b659
2b791f512c4f94b43153da78fd70066bee61d27b
8be3c943b1609fffbfc51aad666d0a04adf83c9d
a78cc99af27ddb08a8a90ba5e123cc127f5e5675
b84f9949207d8055c8f15ef80ed302ed3dbf6d12|
6e1a438cfe5a6c9e2165665f8c2258849ccc43f0
5c6d9edc3a951cda763f650235cfc41a3fc23fe8
ebe53c61982711f13af8bbc09844e4e2849268ba
e38ad214943daad1d64c102faec29de4afe9da3d
e53ce1bcab3d37c63ec940c853abc44ab701fa28
d869db7fe62fb07c25a0403ecaea55031744b5fb
51abb9636078defbf888d8457a7c76f85c8f114c
961887ee6a084c02619f22f6b2e8a852

CrackStation

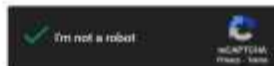
Defuse.ca

CrackStation » Password Hashing Security » Defuse Security »

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
2b791f512c4f94843159a78f6788668ee810279
8be3c943b1809fffbfc51ead056d0e04adf83c9c
a78cc99af27cd880a8a980a8e123cc127f5e5675
b04f0948207d0055c8f15ef09ed382ed30bfed12
6e1a438c7e5a6c9a216006f8c2258049ccc43f0
fc049edc3a951c0a763f690235cfc41a3fc25fe8
ebe53c61982711f13af80bc09044e4a2840200ba
e38ac214043daad1d64c102faac290e4afe9ca3d
e53ca10cab5037c63ac940c033abc44ab701fa28
d093cb7fe61fb07c25a0483ecaea55031744b5fb
51ac0983607b0efbf868d8457a7c7ef85c0f114c
001807a0e084c02612f22f0b2e0e852
```



Supports: LM, NTLM, md2, md4, md5, md5(jwt), md5(jwt,sha1), sha1, sha224, sha256, sha384, sha512, rc4MD100, whirlpool, PBKDF2-HMAC-SHA1 (SHA1-SHA1-HEX), GnuPGv1.1BackupDefuse8

[Download CrackStation's Wordlist](#)

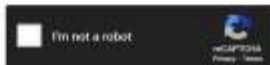
How CrackStation Works

CrackStation uses massive pre-computed lookup tables to crack password hashes. These tables store a mapping between the hash of a password, and the correct password for that hash. The hash values are indexed so that it is possible to quickly search the database for a given hash. If the hash is present in the database, the password can be recovered in a fraction of a second. This only works for "unsalted" hashes. For information on

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

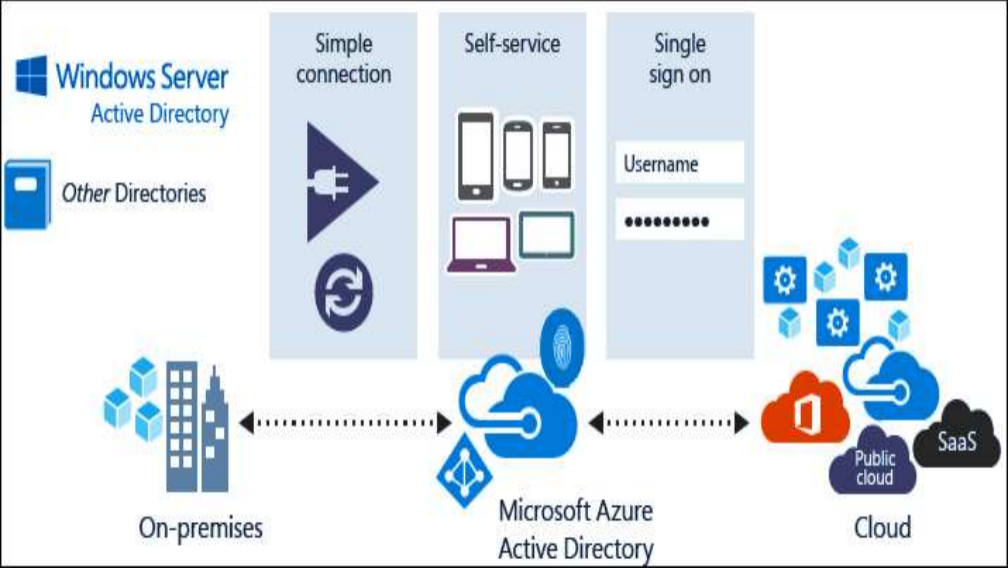
```
26791f512c4f94b43133da79fd78866bxe01d27b
8be3c943b1a88f7fbfc31aee664d8e94d783c9d
a78cc99af27a08848a96ba5e123cc127f9e5679
bd4f9948207a8055c8f15ef88ed382ed3dbf6d12
6e1a438c7e2a6c9e2165665f8c2158846ccc43f9
3c889edc2a9810da703f688235cfc41a3fc23fe8
eba53c81982711f13ef8bbc80644e4e2840288ba
e38ad2149432ead3064c182faec28detafe9da3c
e53ce13cab3657c83ec940c855a9c44ab701fa28
d969db7fed2fb07c25a8483ecaa5503174485fb
31abb084078defb7889c8857a7c7ef86c9f14c
901807ee6e884c82619f22f862e8a852
```



Click Here

Supported: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-hex, sha1, sha224, sha256, sha384, sha512, ipsw0100, whirlpool, MySQL 4.1+ (sha1|sha1_bin), Quercus1.10backdoor

Hash	Type	Result
a488c8d19c384cc377d286871708c7a3289944c	sha1	Secret6
59130110803170a7088c2873a0a230e030	ipsw0100	ipsw0100:root:root
26791f512c4f94b43133da79fd78866bxe01d27b	sha1	Locally
8be3c943b1a88f7fbfc31aee664d8e94d783c9d	sha1	Password
a78cc99af27a08848a96ba5e123cc127f9e5679	ipsw0100	ipsw0100:root:root
bd4f9948207a8055c8f15ef88ed382ed3dbf6d12	sha1	Secret7
6e1a438c7e2a6c9e2165665f8c2158846ccc43f9	sha1	Whirlpool
3c889edc2a9810da703f688235cfc41a3fc23fe8	sha1	Secret8
eba53c81982711f13ef8bbc80644e4e2840288ba	sha1	Unverified





**Before talking about mitigating Insider threats
let us understand the new network perimeter**

The new network perimeter



The new network perimeter

- In on-premises IT infrastructure and traditional security models
 - Easier verification and authorization of everything inside the corporate network, including devices, users, applications, and servers.
 - External users are validated via **VPN and NAC**.
- With the increasing adoption of the cloud and remote work
 - Data is stored outside of corporate walls
 - Users access enterprise applications that are located on the cloud/on-premises using various types of devices from locations outside the corporate network

The result - Soft boundaries!





**Hybrid AD is a crucial component of the
new network perimeter**

Best of both worlds - Hybrid AD

- As companies embark on application and data modernization, they should consider using a hybrid AD, as it balances the application and data workload across both platforms.

Innovation,
speed, storage,
and scalability
of the cloud



Regulatory
compliance,
performance,
and data
gravity of on-
premises



Hybrid AD

Problem with cloud - **lack of transparency**



Closing the security gap in the cloud

- In on-premises infrastructures
 - **Managing identities, authentication, and access is relatively easy** with Microsoft's Lightweight Directory Access Protocol (LDAP) and Active Directory (AD).
- In the cloud
 - **It is much more difficult** for IT departments to monitor which users are accessing which applications and services.
 - Solution: Adopt more applications 😊





THE new challenge - managing **fragmented** identities

- Ensuring secure access to every user, application, and device, **irrespective of their location**.
- The access should be **contextual**
- IT administrators have to **create access policies** based on location, IP address, device etc.

Problem: Managing fragmented user identities.

Solution?

Implement Zero Trust

But...

Implement Zero Trust - From a concept to reality

- How many of you have successfully implemented Zero Trust?

John Kindervag would be sad!



Creator of the Zero Trust Security Model - 2010

Practical Steps to Implement ZT

- What can you do to implement ZT and thereby **minimize the risk of insider threats?**

**'EVERYONE HAS A PLAN
'TILL THEY GET PUNCHED
IN THE MOUTH.'**

MIKE TYSON -

HAVE AN INSIDER THREAT PROGRAM
FOCUSING ON **PREVENTION** AND
DETECTION/RECOVERY



Implement Zero Trust (User) with IAM and SIEM

Prevention - IAM

1. **Verifying** and providing secure access to each and every user who is attempting to access organizational resources across **private cloud, public cloud, or on-premises data centers**.
2. **Enforcing** just-in-time (JIT) provisioning
 - Least-privilege access and limiting access to business-critical assets (**prevent lateral movement**)
3. **Automating** clean up activities - Inactive accounts/folder permissions/licenses etc.

Detection and Response - SIEM

1. **Inspecting** network traffic for malicious activities (UEBA) based on the contextual policies that you have framed


Our offerings that can help you begin the ZT journey

IAM - Prevention

ManageEngine 
AD360

SIEM - Detection and Response

ManageEngine 
Log360

ManageEngine

Thank you!

Vivin Sathyan

LinkedIn: [Vivin Sathyan](#)

E-mail: vivin.sathyan@manageengine.com