Active Directory Incident Response: Key Things to Keep in Mind

Active Directory (AD) is crucial for network security as it controls access to sensitive data, making it a primary target for attackers. Even a small AD breach can result in significant data loss, operational downtime, and reputational damage in a business.

What Constitutes Active Directory Incidents?

Active directory incidents typically fall into these categories:

- **Initial Access**: Occurs when an attacker exploits weak password policies, excessive user privileges, poorly managed login details, and insecure account settings to gain unauthorized entry into the system.
- **Credential Access**: Occurs when attackers exploit exposed privileged credentials or take advantage of insecure configurations to access sensitive data.
- **Privilege Escalation**: Occurs when an attacker exploits weaknesses like misconfigured access control lists (ACLs), improper Exchange or Group Policy permissions, insecure trust settings, or compromised critical systems to gain higher-level access or control.

Active Directory Incidents and How to Respond to Them

When something goes wrong with AD, it can lead to several serious problems. Let’s explore the main issues and solutions to overcome or avoid them in detail.

AD Incident #1: Initial Access

Problem Solution Impact Inadequate Password Security Implement Passwordless Authentication (e.g., biometrics, FIDO2) Eliminates password-based attacks Enforce Strong Password Policies (14+ characters, complexity) Minimizes brute force risks Enable Multi-Factor Authentication (MFA) Adds an extra layer of security Overprivileged Accounts & Weak Credential Management Limit Domain Admin accounts Reduces attack surface Use Privileged Access Management (PAM) Applies least-privilege model Review & Rotate Service Account Passwords Regularly Secures service accounts Vulnerable Account Settings Regularly audit account settings Reduces attack vectors Require Kerberos Pre-authentication Prevents unauthorized access attempts

Problem 1: Inadequate Password Security Practices

Weak or easily guessable passwords for privileged accounts are common vulnerabilities.

Solutions/Recommendations:

1. Implement Passwordless Authentication Methods

- Biometrics (facial recognition, fingerprints) for login.
- Use FIDO2 security keys (small, portable devices, usually USB or Bluetooth-based) to authenticate users when logging into services.

These options avoid the need for passwords, so attacks like password spraying and phishing can’t occur.

2. Improving Password Policy

Using longer passwords (14+ characters) and changing them less often discourages users from cycling through easily guessable passwords. Additionally, enabling multi-factor authentication (MFA) adds an extra layer of protection to critical systems.

Problem 2: Overprivileged Accounts and Weak Credential Management

Granting excessive privileges to accounts, especially service accounts, increases the risk of AD breaches. If many service accounts or user accounts are given Domain Admin privileges, they get high-level access to your network.

Service accounts are often weak targets, because:

- Passwords for service accounts are rarely changed.
- These accounts often lack proper security controls, increasing vulnerability.
- The passwords for these accounts are sometimes stored in plain text (e.g., in emails, text files, or command lines), making them vulnerable to theft.

Additionally, the combination of too many Domain Admin accounts and weak security controls increases the chance of credential theft.

If a user account is compromised without admin rights, it becomes more difficult for attackers to escalate privileges across the network. Organizations should also ensure that their Active Directory incident response strategy includes rapid identification and response to misuse of overprivileged accounts.

Solutions/Recommendations

1. Limit Domain Admin accounts

There is no fixed rule for how many Domain Admin accounts are needed; it depends on your business environment. Therefore, carefully review any requests for additional Domain Admin accounts, and prefer granting lower privilege levels, especially for service accounts, rather than giving them full Domain Admin access.

2. Reduce privilege for service accounts

Instead of giving service accounts full access to all servers and workstations, consider limiting their access to only a subset of devices and giving them minimum privileges needed to work.

3. Better control over credentials

If you don’t have strong controls over how important accounts (like Domain Admins) are managed, adding more Domain Admin accounts increases the risk. Use tools to manage passwords automatically and securely, making sure privileged access is tightly controlled.

4. Privileged Access Management (PAM)

These solutions help mitigate risks by enforcing the least privilege model.

Problem 3: Vulnerable Account Settings

In Active Directory, misconfigurations can make individual user accounts less secure. Some settings can make accounts vulnerable to attacks, including:

- **No password required:** If an account is configured to not require a password, it leaves the door wide open for unauthorized access.
- **Not requiring Kerberos pre-authentication:** If pre-authentication is disabled, attackers can attempt to access accounts without the initial security check, making it easier to crack passwords.
- **Storing passwords with weak/ reversible encryption:** This means passwords can easily be guessed or decrypted, making them easier for attackers to steal.

Solutions/Recommendations

Regularly audit account settings to identify and remediate misconfigurations. This includes checking for any accounts that do not require Kerberos pre-authentication, storing passwords with weak or reversible encryption, or failing to enforce strong password policies.

AD Incident #2: Credential Access

Problem Solution Impact Exposed Privileged Credentials Limit where Domain Admins log in Prevents credential theft from workstations Use Defender for Identity Detects lateral movement Minimize credential exposure Reduces chance of theft via compromise Kerberoasting (Service Account Exploitation) Review all SPNs and use complex passwords Stops attackers from cracking service accounts Regularly rotate service account passwords Prevents long-term access Uncontrolled Delegation Restrict delegation for admin accounts Prevents TGT theft and escalation Monitor and audit delegation settings regularly Minimizes unnecessary risks

Problem 1: Risk of Exposing Privileged Credentials

Admins often log into multiple devices (workstations, servers) for their tasks, which can leave privileged credentials exposed.

Attackers can use tools like Mimikatz or secretsdump to retrieve these credentials.

For instance, if Domain Admins log into non-critical devices (e.g., user workstations), their credentials may be exposed on those devices, increasing the risk of credential theft. This increases the risk of an attacker stealing the credentials and gaining higher access.

Effective incident response Active Directory procedures should include rapid identification of compromised active directory credentials and steps to prevent lateral movement across the network.

Solutions/Recommendations

1. Limit where Domain Admins log in

Ensures they only access critical systems from secure devices.

2. Use Defender for Identity

It helps map lateral movement paths, showing how a compromised regular user account could lead to domain-level access. Defender for Identity also tracks high-risk users and devices, aiding in prioritizing security actions.

3. Minimize credential exposure

When accessing remote systems, avoid methods that leave privileged credentials behind on devices.

Problem 2: Kerberoasting – Exploiting SPNs to Crack Service Account Passwords

SPNs (Service Principal Name) are identifiers for service accounts in the Active Directory. If an attacker compromises a regular user account, they can make service ticket requests for any account with an SPN. The ticket includes the hashed password of the service account.

The attacker can extract this hash from memory and try to crack the password offline. If successful, they can use the service account and gain the privileges of that account.

Solutions/Recommendations

- Review all accounts with SPNs.
- Ensure strong password policies for active accounts with SPNs by using complex passwords and regularly rotating them.

Problem 3: Risks of Uncontrolled Delegation

Unconstrained Kerberos delegation allows one server to impersonate users and access other resources on their behalf.

For example, a web server may be configured to access an SQL server using user credentials.

When you log into the web server, it uses delegation to authenticate to the SQL server with your credentials, storing your Kerberos Ticket Granting Ticket (TGT) in memory on the web server. If an attacker compromises the web server, they can steal the TGTs from memory and impersonate any user, including Domain Admins. If a Domain Admin’s TGT is stolen, the attacker can gain full control of Active Directory.

Solutions/Recommendations

1. Regularly review delegation settings and restrict unnecessary delegation for administrative accounts. If delegation is necessary, limit it to only the required services, and avoid using unconstrained delegation.
2. Restrict delegation for administrative accounts by ensuring delegation is never enabled for them.
3. Add sensitive accounts to the Protected Users group to add extra protection.

Problem 4: Vulnerabilities in Local Administrator Account

Management

LAPS is a Microsoft tool that automatically manages the password for the built-in Administrator account on Windows devices. During machine setup (e.g., during imaging), many devices may share the same password for this account. If left unchanged, this common password can allow attackers to move across devices once they gain access to one. LAPS resolves this by ensuring each device has a unique local administrator password, which is regularly rotated.

Solutions/Recommendations

1. Deploy LAPS properly

Ensure LAPS is implemented on all devices and regularly audit its usage. This helps remove privilege from administrative accounts and lowers the risk of credential theft.

2. Control access to LAPS passwords

Only certain users should be allowed to retrieve the LAPS-managed password. Access to the LAPS password is controlled by the ‘ms-Mcs-AdmPwd’ attribute.

Regularly audit who has access to these passwords to make sure only the necessary people can use them.

AD Incident #3: Privilege Escalation

Problem Solution Impact Misconfigured ACLs (Access Control Lists) Audit ACLs regularly Fixes misconfigurations and secures access Use attack path tools to identify potential escalation paths Prevents unauthorized privilege escalation Apply the Principle of Least Privilege Restricts access to critical resources Exchange Permissions (Exchange Server Exploitation) Implement Split Permissions Model (separate Exchange/AD permissions) Minimizes attack surface Reduce Exchange Permissions Limits admin-level access for Exchange users Abuse of Group Policy Permissions Limit Group Policy Permissions Prevents unauthorized GPO modifications Apply Least Privilege to GPOs Minimizes impact from compromised accounts Vulnerabilities in Trust Relationships Enable SID Filtering Secures trust relationships Limit unnecessary trusts Prevents privilege escalation across domains Remove unused trusts after migrations Minimizes attack surface by removing unused trust relationships

Problem 1: Risks of Misconfigured Access Control Lists (ACLs)

Misconfigurations of ACLs are common and can weaken security without affecting day-to-day operations.

These misconfigurations can create attack vectors that allow low-privileged users to escalate access and potentially gain full control over the domain. And attackers can exploit these paths created by excessive privileges and broad access granted by misconfigured ACLs.

Common ACL Issues:

- **GenericAll Privilege:** This is essentially the same as Full Control. If an attacker gains access to a user account with GenericAll privileges over a highly privileged group (like Domain Admins), they can add new members to that group and take control of your network.

- **WriteDacl Privilege:** This allows a user to modify the permissions of an object in Active Directory. If an attacker compromises a user with this privilege, they can change the permissions for a group and potentially add themselves to privileged groups, such as Domain Admins.

- **AdminSdHolder Misconfigurations:** The AdminSdHolder object manages permissions for protected groups. If an attacker manipulates its settings, the changes can affect protected groups, like Domain Admins, and allow the attacker to modify group memberships.

Solutions/Recommendations

- Regularly audit permissions throughout your Active Directory environment.
- Use monitoring tools to identify misconfigurations.
- Run attack path audits by using dedicated tools to identify potential attack paths that could lead to domain compromise.
- Fix any ACL misconfigurations that could allow privilege escalation or unauthorized access.

Problem 2: Privilege Escalation Through Exchange Permissions

Even if a company has migrated user mailboxes to Office 365, they may still rely on an on-premises Exchange server for various reasons, such as:

- Users who haven’t migrated yet.

- Legacy applications incompatible with Office 365.

- Workloads that aren’t connected to the internet.

Exchange groups like ‘Exchange Trusted Subsystem’ and ‘Exchange Servers’ often have high-level privileges, which can give attackers a potential path to domain control. Additionally, internet-facing Exchange servers (like those used for Outlook Web Access) expand the attack surface, making systems more vulnerable to external threats.

If attackers gain SYSTEM privileges on the Exchange server, they can exploit excessive Active Directory permissions to take over the entire domain.

Solutions/Recommendations

1. **Implement the Split Permissions Model**: This separates Exchange and Active Directory permissions, reducing the high privileges Exchange holds in AD.
2. **Reduce Exchange Permissions**: Even if you don’t deploy the full split permissions model, you can still lower Exchange’s permissions in Active Directory by following Microsoft’s guidelines.
3. **Consider Turning Off On-Premises Exchange**: Disable unnecessary on-premises Exchange servers after migration to Office 365.

Problem 3: Abuse of Group Policy Permissions

If an attacker hasn’t yet compromised a Domain Admin, they might gain access to an account with permissions to manage Group Policy Objects (GPOs).

Example: A user can be given permission to create, update, or link policies, which could be exploited by the attacker.

In these cases, attackers can take several malicious actions, including:

- Modifying startup scripts in GPOs to execute harmful code.
- Apply policies that disable security tools on endpoints, leaving systems vulnerable.
- Increase privileges for regular users unintentionally by altering User Rights Assignments.

Solutions/Recommendations

Use efficient security tools for auditing and managing privileges. And,

1. **Limit Group Policy Permissions**: Only trusted users and groups should have permission to create, update, or link policies. These users should be held to the same security standards as Domain Admins.
2. **Apply Least Privilege**: Group Policy permissions should follow the least privilege principle—only grant the necessary permissions for users to perform their jobs.

Problem 4: Vulnerabilities in Trust Relationships

Misconfigured SID History (Security Identifier History) settings can be exploited by attackers to escalate privileges across domains and gain control over trusted domains.

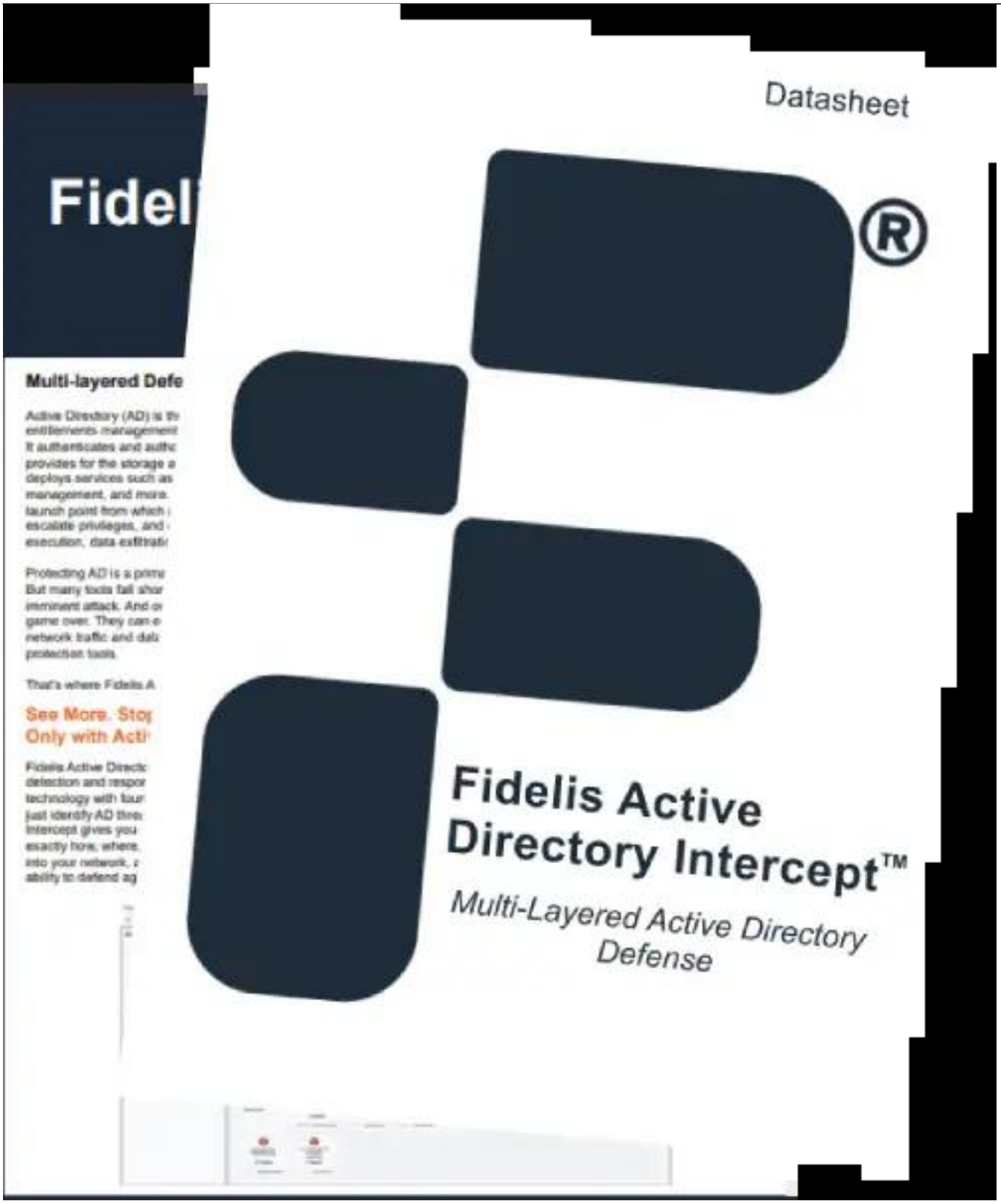
Solutions/Recommendations

- Secure trust relationships by enabling SID filtering and limiting unnecessary trusts.
- Only configure Active Directory trusts when necessary.
- After completing migrations or acquisitions, remove or decommission unnecessary trusts.

Strengthen Your AD Security with Fidelis Active Directory Intercept™

- Analyze network traffic for AD-specific threats in real-time.
- Use integrated intelligent deception to thwart attacks.
- Monitor AD logs and events for continuous security.
- Intercept and defeat AD attacks before they escalate.

Download the Datasheet



Enhancing AD Security with Fidelis Active Directory Intercept™

To help address the challenges posed by Active Directory vulnerabilities, organizations can enhance their security posture with Fidelis Active Directory Intercept™. This powerful, all-in-one solution combines Active Directory-aware Network Detection and Response (NDR) with integrated AD monitoring to offer comprehensive protection.

Key features include:

- **Real-Time Detection & Response:** Quickly identifies malicious or suspicious activity within your AD environment.
- **Continuous AD Log & Event Monitoring:** Proactively monitors logs and events for vulnerabilities or threats.
- **Intelligent Deception Technology:** Stops Active Directory attacks in their tracks using deceptive techniques.
- **Deep Session Inspection:** Detects hidden threats within network traffic that may otherwise go unnoticed.

Fidelis empowers you with the tools needed to protect your Active Directory environment, ensuring it remains secure, resilient, and fully monitored—helping to streamline Active Directory incident response and enhance overall security management.

In Conclusion

Active Directory compromises pose significant risks to an organization’s data confidentiality, integrity, and availability. These breaches can lead to financial losses, regulatory fines, and reputational damage, which erode customer trust and cause long-term harm. Securing AD is crucial for safeguarding organizational assets and ensuring business continuity. Additionally, following guidance from organizations like the National Security Agency or the Cybersecurity and Infrastructure Security Agency (CISA) may help strengthen Active Directory security protocols and provide more comprehensive solutions.

Strengthen Your Active Directory with Advanced Security Strategies!

- Understand the latest threats targeting Active Directory.
- Use an actionable checklist for reducing AD vulnerabilities.
- Discover cutting-edge strategies and solutions for securing AD.
- Learn how Fidelis Elevate empowers AD detection and response.

Download the Whitepaper


Fidelis Security
Security Checklist
Beyond the Checklist
WHITE PAPER
Security Checklist: Hardening Your Active Directory with Advanced Strategies
Copyright © 2024 Fidelis Security® LLC. All rights reserved.