SEMPERIS

Semperis Directory Services Protector

Eliminating Blind Spots in Active Directory

As the keeper of the “keys to the kingdom”, Active Directory (AD) is a prime target for cyberattacks. With Semperis Directory Services (DS) Protector, you can expose and immediately close backdoors created by an attacker or rogue administrator, so systems stay secure and available.

What You Can’t See Can Hurt You (a lot)

What’s the best way for an intruder to cover their tracks? That’s easy: don’t leave any.

And it’s precisely how an intruder can infiltrate AD and establish a persistent threat in the very core of your security infrastructure.

Attackers avoid detection in any number of ways:

- Delete Windows security event logs.
- Turn logging off or disable collection agents.
- Use readily available techniques like DCShadow to inject malicious changes directly into AD – and outside the purview of security incident and event management (SIEM) systems and most AD change tracking tools.

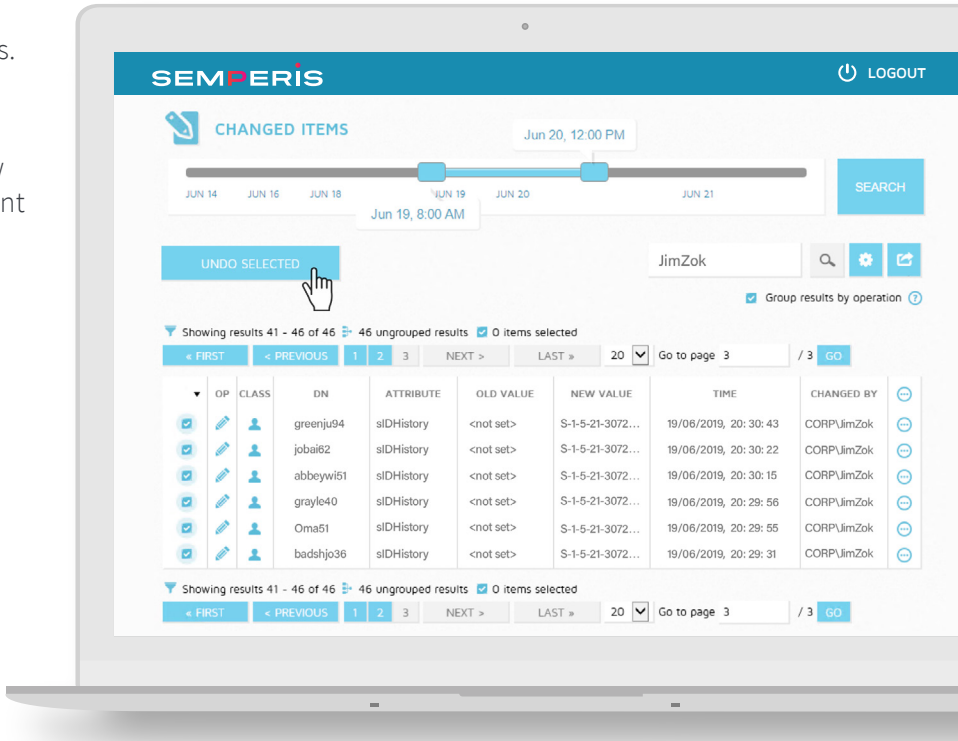
With the security camera effectively turned off, an attacker can modify user accounts, groups, Group Policy Objects (GPOs), DNS records, even the AD schema – creating backdoors that can be used later in the attack.

So, how do you defend against stealth attacks that circumvent event logging?

How do you preserve the visibility of the SIEM system you’ve invested so much in and come to rely on?

That’s easy: with Semperis DS Protector.

Identity-Driven Enterprise Protection



Semperis DS Protector maintains a complete history of changes to AD that you can browse, search, and use to immediately roll back unwanted changes. In this example, changes made by a compromised account are identified and then reverted with a click of the mouse.

Microsoft Partner
Enterprise Cloud Alliance

+1 703 918 4884 www.semperis.com info@semperis.com

Change Tracking and Remediation Together in One Solution

Semperis DS Protector leverages multiple data sources and a powerful database to overcome the fundamental shortcomings of traditional event-based change tracking and backup-based granular restore.

Better by design and built for the enterprise, Semperis DS Protector provides the capabilities organizations need to defend AD from today's most sophisticated cyberattacks, as well as to recover quickly from everyday mistakes (accidental OU deletion, scripting errors, etc.). Must-have capabilities include:

Uninterrupted Visibility. Captures changes even if Windows security event logging is turned off, logs are deleted, agents are disabled, agents stop working, or changes are injected directly into AD.

Real-Time Alerts. Based on your rules, sends notifications when a domain controller (DC) is registered, members are added to sensitive security groups, privileged users are created, etc.

Who Dunnit. Shows who made each change and allows you to quickly isolate all changes made by a compromised account.

Forensic Analysis. Provides high-integrity data that authorized users can query through the Semperis console or PowerShell module.

Robust Reporting. Includes built-in security reports maintained by AD experts to expose known and emerging vulnerabilities such as computer accounts trusted for delegation, "Kerberowasting" targets, and more. Also includes custom reporting capabilities (for example, report on AD groups that were not modified by your identity provisioning account).

SIEMbiosis. Integrates with your SIEM system to provide changes not captured in event logs, as well as more meaningful AD events (for example, single event for user creation rather than multiple events, human readable values of security descriptors).

Instant Undo. Reverts unwanted changes immediately, without the need to mount and extract a backup (or possibly several backups).

Granular Rollback. Reverts changes to individual attributes, objects, and containers – and to any point in time (not just to a previous backup).

RBAC and more. Includes robust role-based access control (RBAC) and a rich web UI to enable delegation of routine administrative tasks.

GPO, DNS, Configuration, and Schema Changes. Extends real-time change tracking and rollback (where applicable) to all components of AD. Enables quick recovery of critical services such as DNS, PKI, and DHCP.

Changes to Active Directory can have huge security consequences. Keep the security camera on with Semperis.

Contact us today for a free trial.

+1 703 918 4884 www.semperis.com info@semperis.com

"The ability to search and compare changes in real time ***saves us critical downtime.****"*

Rafi Dabush
IT Manager, EL AL Airlines

ABOUT SEMPERIS

Semperis is an enterprise identity protection company that helps organizations recover from cyber breaches and directory service failures, on-premises and in the cloud. The company's patented technology for Active Directory is used by customers in the Fortune 500, government, financial, healthcare, and other industries worldwide. Semperis solutions are accredited by Microsoft and recognized by Gartner.

SEMPERIS

DSPDS190726