TOP 10 AD

BEST PRACTICES

FROM AD SECURITY EXPERTS

1 Take regular backups and store copies offline to protect from ransomware and wiper attacks.

2 Always have sufficient backups to perform a full forest recovery.

3 Avoid bare-metal and system state restores when recovering from a malware attack.

4 Audit and alert on changes to critical/privileged group memberships.

5 Monitor for AD configuration changes that could indicate a DCShadow or similar attack.

6 Limit editing and linking of GPOs to a small subset of administrators.

7 Implement admin tiering to minimize credential theft.

8 Monitor for Kerberos-enabled service accounts with weak passwords to prevent “Kerberoasting” attacks.

9 Monitor for unconstrained delegation (and changes to delegation) on computer accounts.

10 Monitor for changes to the AdminSDHolder object to prevent administrative account takeover.

semperis

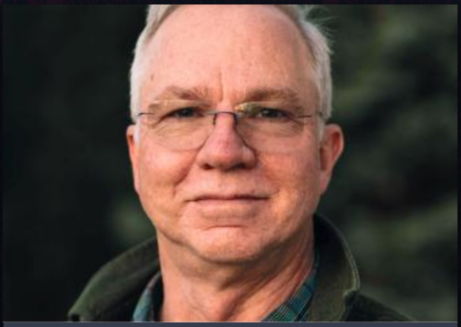
semperis

MEET OUR AD SECURITY EXPERTS

DARREN MAR-ELIA

Head of Product

A 14-year Cloud and Datacenter Microsoft MVP, Darren has a wealth of experience in Identity and Access Management and was the CTO and founder of SDM software, a provider of Microsoft systems management solutions. Prior to launching SDM, Darren held senior infrastructure architecture roles in Fortune 500 companies and was also the CTO of Quest Software. As a Microsoft MVP, Darren has contributed to numerous publications on Windows networks, Active Directory and Group Policy, and was a Contributing Editor for Windows IT Pro Magazine for 20 years.



GIL KIRKPATRICK

Chief Architect

Gil Kirkpatrick is a long-time veteran of the commercial software industry and has focused on identity and access management products since the early 1990s. He has held technology leadership roles at HTS, NetPro, Quest Software, and ViewDS Identity Solutions, and is known as the founder of the Directory Experts Conference (later renamed The Experts Conference). Kirkpatrick is the author of Active Directory Programming, the original reference book for developers working with Microsoft's Active Directory. He has been nominated as a Microsoft MVP for Active Directory and Enterprise Mobility for each of the last 16 years.

SEAN DEUBY

Director of Services

Sean brings 30 years' experience in enterprise IT and hybrid identity to his role as Director of Services at Semperis. An original architect and technical leader of Intel's Active Directory, Texas Instrument's NT network, and 15-time MVP alumnus, Sean has been involved with Microsoft identity since its inception. Since then, his experience as an identity strategy consultant for many Fortune 500 companies gives him a broad perspective on the challenges of today's identity-centered security. Sean is an industry journalism veteran; as former technical director for Windows IT Pro, he has over 400 published articles on AD, hybrid identity, and Windows Server.

IDENTITY-DRIVEN
CYBER RESILIENCE

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