Uncover Active Directory vulnerabilities before attackers do.

With access to Active Directory, Azure AD (now Entra ID), and Okta threat actors can gain dominance over your entire infrastructure. Unleash Purple Knight—a free AD, Azure AD, and Okta security assessment tool built by identity security experts—to close security gaps that leave your hybrid AD environment open to cyberattackers.

- 23,000+ downloads (and counting!)
- 150+ security indicators
- ◆ 45% attack surface reduction



AD, Azure AD (now Entra ID), and Okta security report card with scores across seven categories

150+ pre- and postattack security indicators for AD, Azure AD, and Okta

Community-driven updates from our expert team of threat researchers

Prioritized guidance for closing security gaps from AD, Azure AD and Okta security experts Correlation with MITRE ATT&CK, MITRE D3FEND, ANSSI, and other frameworks

Uncover your AD, Azure AD (now Entra ID), and Okta security vulnerabilities in minutes.

Spot Active Directory vulnerabilities before attackers do. Find AD, Azure AD, and Okta security gaps with Purple Knight. Perform a comprehensive set of tests against the most common and effective attack vectors to find risky configurations and security vulnerabilities.

Prioritize AD, Azure AD, and Okta security gaps for remediation. Gain visibility into your hybrid AD security posture with the Purple Knight report. See your AD, Azure AD, and Okta security scores in seven categories, plus get prescriptive guidance from identity security experts to help you prioritize remediation efforts. **Fix AD, Azure AD, and Okta security vulnerabilities that attackers can exploit.** Use Purple Knight's prioritized, expert guidance to systematically address AD, Azure AD, and Okta misconfigurations and unpatched vulnerabilities—for example, admin accounts with old passwords and enabled admin accounts that are inactive.

🕇 Validate hybrid AD security posture over time.

Run Purple Knight periodically to guard against misconfigurations that can accumulate over time and degrade hybrid AD environment security if left unchecked. Use the results to align your security strategy with industry frameworks including MITRE ATT&CK, MITRE D3FEND, and ANSSI.









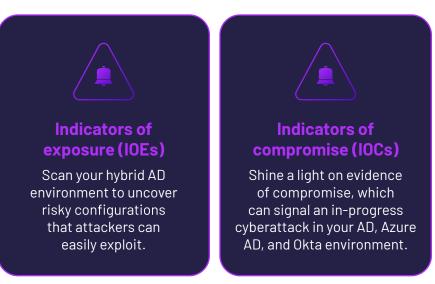
semperis

Purple Knight scans your Active Directory, Azure Active Directory (now Entra ID), and Okta environment and generates a security score based on indicators of exposure (IOEs) and indicators of compromise (IOCs) across seven categories.

	Agreement	Environment	Indicators	Progress	Summary	
	1 —	2	3		6	
SECURITY POSTURE O	VERVIEW					
assessment). Azure AD tenant: Purple Knight que Okta identity platform Purple Knight	ht queried the Active Directory environ nied the selected Azure AD tenant foc track score dhe selected Okta domain o nick score as well as detailed results a	went and ran a series of security in using on some of the most common fecting for activities that may indica sour each indicator of Exposure (108	attack vectors that threat actors in the unauthorized access attempts, I found, By uncovering Active Dire	use to gain access to the suspicious behavior, or ectory and Azure AD sec	potential threats within the Okta infrast urity weaknesses, this assessment report	ristore
-						
95			68%		(58
a			00-		6	
A ACTIVE DIRECTORY		A AZURE AD			O OKTA	
	056-001Jab	- Tenant	smprsakdeve		Comain	dev 33517590
A Forest	1130-001380					
Forest	2	Application I			Duration	00.0
		Application I Duration	12456921-64			
No. of Domains	2	Curation	0 12/56921-00	99-4 100:37	Duration Bun by	00.0 tannym@sen
 No. of Domains Duration 	2 00:00:24	Curation	12456921-64	99-4 100:37	O Duration	00.0 tannym@sen
No. of Domains Duration Run by	2 00:00:24	Curation	0 12/56921-00	99-4 100:37	Ountion Run by	00.0 tannym@sen
No. of Domains Duration Run by Indicators	2 00.00.24 INS6-007/IIS6401	C Duration	0 12/56921-00	29-4 100:37	Duration L Bun by Indicators	00.0 tannym@sen
No. of Domeins Datation Datation Particy I Particy Indicators Evaluated	2 00.00.24 1156-001/115601 99	Duration Indicators Datased	0 12/56921-00	29-4 100-37 23	Duration Lanty Run by Indicators Cualuated	00.0 tannym@sen
B. No. of Domains Domains Domains Domains Rom by Indicators Evaluated Ø Not selected	2 00.00.24 1156-007/1156081 99 1	Duration Duration Indicates Dualuand Not selected	0 12/56921-00	29-4 100:37 23 0	Duration Lanthy Indicators Coaluaned Not selected	00.0 tannym@sen
	2 00.00.24 1156-0071/156608 99 1 1 17	Duration Duration Indicators Dualuaned Not selected Olds found	0 12/56921-00	29-4 1000.37 23 0 7	Duration Main by Indicates Colliand ON to steleted O Tots found	00.0 tannym@sen
B No. of Domains C Duardon L Run by Indicators Evaluated N Not selected N Not se	2 000034 1156-001/115608 99 1 17 12	Duration Indicates Duration Midicates Duration Not selected Mick sound Ricks found Ricks found	0 1285602167	29-4 200337 23 0 7 16	Control Internet Indicators Collared O Not selected O Not selected O Not selected O Round O Reveal	00.0 tannym@sen
B No of Demains Duration L Run by Helicators Helicator	2 00.00.24 1156-0011756881 99 1 17 12 4	Duration Duration Indicater Duration Contrasted Dictored Dictored Proced Pailed to run	0 1285602167	994 20037 23. 0 7 16 7	Constant Co	00.0 tannym@sen

Use 150+ security indicators to uncover vulnerabilities in AD, Azure AD (now Entra ID), and Okta

Purple Knight scans for known vulnerabilities and emerging threats discovered by our team of expert identity threat researchers.



"

Purple Knight has given us insight into the network that we wouldn't have otherwise. It's an invaluable resource!

John Hallenberger

Systems Administrator, Fox C-6 Schools (Arnold, MO)



Semperis Headquarters

5 Marine View Plaza Suite 102 Hoboken, NJ 07030 info@semperis.com



Enterprise Cloud Alliance Microsoft Accelerator Alumni Microsoft Co-sell Microsoft Intelligent Security Association (MISA)

© 2025 Semperis | Semperis.com

About Semperis

For security teams charged with defending hybrid and multi-cloud environments, Semperis ensures the integrity and availability of critical enterprise directory services at every step in the cyber kill chain and cuts recovery time by 90%. Purpose-built for securing hybrid Active Directory environments, Semperis' patented technology protects over 100 million identities from cyberattacks, data breaches, and operational errors. The world's leading organizations trust Semperis to spot directory vulnerabilities, intercept cyberattacks in progress, and quickly recover from ransomware and other data integrity emergencies. Semperis is headquartered in Hoboken, New Jersey, and operates internationally, with its research and development team distributed throughout the United States, Canada, and Israel.

Semperis hosts the award-winning Hybrid Identity Protection conference and podcast series (www.hipconf.com) and built the community hybrid Active Directory cyber defender tools, Purple Knight(www.semperis.com/purple-knight) and Forest Druid. The company has received the highest level of industry accolades, recently named to Inc. Magazine's list of best workplaces for 2023 and ranked the fastest-growing cybersecurity company in America by the Financial Times. Semperis is a Microsoft Enterprise Cloud Alliance and Co-Sell partner and is a member of the Microsoft Intelligent Security Association (MISA).