Argus

KLANT BEVEILIGINGSRAPPORT

Klant Beveiligingsrapport

Bakker Installatietechniek

Rapportdatum: 2026-09-16 · 4 apparaten

F

ALGEHELE RISICOBE-OORDELING

Kritiek · 92/100

RISICOSCORE · LAGER IS BETER

Opgesteld door: Meridiaan ICT

Vertrouwelijk

01

Managementsamenvatting

ALGEHELE RISICOBEOORDELING	APPARATEN GESCAND	TOTAAL BEVINDINGEN
F · 92	4 / 4	56
Kritiek · lager is beter		

Ernst samenvatting

Kritiek Hoog Gemiddeld Laag Informatief

KRITIEK	HOOG	GEMIDDELD	LAAG	INFORMATIEF
4	12	22	18	0

02

Los dit eerst op

De belangrijkste problemen om nu op te lossen.

Kerberoastbare accounts in bevoorrechte groepen

KRITIEK

QS-DC-014 · BAK-DC-01

Er zijn gebruikersaccounts met een SPN die ook in een bevoorrechte groep zitten. Elke gebruiker in het domein kan daar een ticket voor opvragen en dat offline kraken.

HERSTEL

Zet serviceaccounts om naar gMSA's, met automatisch beheerde wachtwoorden van 120 tekens. Haal SPN-accounts uit bevoorrechte groepen.

WDigest bewaart wachtwoorden leesbaar in het geheugen

KRITIEK

QS-WIN-046 · BAK-DC-01

Met WDigest UseLogonCredential=1 bewaart Windows wachtwoorden in leesbare vorm in het LSASS-geheugen, waar tools voor credential-diefstal ze zo uitlezen. Moderne Windows-versies zetten dit standaard uit.

HERSTEL

Zet UseLogonCredential op 0 onder HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest, via Intune of GPO.

WDigest bewaart wachtwoorden leesbaar in het geheugen

KRITIEK

QS-WIN-046 · BAK-FS-01

Met WDigest UseLogonCredential=1 bewaart Windows wachtwoorden in leesbare vorm in het LSASS-geheugen, waar tools voor credential-diefstal ze zo uitlezen. Moderne Windows-versies zetten dit standaard uit.

HERSTEL

Zet UseLogonCredential op 0 onder HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest, via Intune of GPO.

WDigest bewaart wachtwoorden leesbaar in het geheugen

KRITIEK

QS-WIN-046 · BAK-WS-021

Met WDigest UseLogonCredential=1 bewaart Windows wachtwoorden in leesbare vorm in het LSASS-geheugen, waar tools voor credential-diefstal ze zo uitlezen. Moderne Windows-versies zetten dit standaard uit.

HERSTEL

Zet UseLogonCredential op 0 onder HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest, via Intune of GPO.

LDAP-ondertekening wordt niet vereist

HOOG

QS-DC-011 · BAK-DC-01

De domeincontroller accepteert LDAP zonder ondertekening, waardoor relay-aanvallen op LDAP mogelijk blijven.

HERSTEL

Zet 'Domeincontroller: vereisten voor LDAP-serverondertekening' op 'Ondertekening vereisen' via het domeincontrollerbeleid.

ms-DS-MachineAccountQuota staat niet op 0

HOOG

QS-DC-010 · BAK-DC-01

Elke gebruiker mag computeraccounts aanmaken in het domein. Dat is de opstap voor onder meer resource-based constrained delegation-aanvallen.

HERSTEL

Set-ADDomain -Identity '<domein>' -Replace @{'ms-DS-MachineAccountQuota'=0}.

Bevoorrechte accounts zitten niet in Protected Users

HOOG

QS-DC-018 · BAK-DC-01

Domain Admins en vergelijkbare accounts vallen niet onder Protected Users, dus hun credentials worden nog gecachet en via NTLM gebruikt.

HERSTEL

Voeg Domain Admins, Enterprise Admins en Schema Admins toe aan Protected Users. Test eerst op compatibiliteit.

Het KRBTGT-wachtwoord is lang niet gewijzigd

HOOG

QS-DC-009 · BAK-DC-01

Het KRBTGT-account tekent elk Kerberos-ticket in het domein. Een oude sleutel betekent dat een golden ticket uit het verleden nog werkt.

HERSTEL

Reset het KRBTGT-wachtwoord met het resetscript van Microsoft — twee keer, met meer dan tien uur ertussen.

03

Apparaatoverstijgende inzichten

Problemen die meerdere apparaten treffen.

	TITEL	GETROFFEN APPARATEN
KRITIEK	WDigest bewaart wachtwoorden leesbaar in het geheugen QS-WIN-046	**3** apparaten BAK-DC-01, BAK-FS-01, BAK-WS-021

	TITEL	GETROFFEN APPARATEN
HOOG	BitLocker is niet ingeschakeld op alle volumes QS-WIN-003	**2** apparaten BAK-WS-014, BAK-WS-021
HOOG	Windows LAPS is niet aangetroffen QS-WIN-011	**2** apparaten BAK-WS-014, BAK-WS-021
GEMIDDELD	Auditbeleid dekt niet alle vereiste subcategorieen QS-WIN-010	**3** apparaten BAK-FS-01, BAK-WS-014, BAK-WS-021
GEMIDDELD	LLMNR staat aan en is te misbruiken voor poisoning QS-WIN-019	**3** apparaten BAK-FS-01, BAK-WS-014, BAK-WS-021
GEMIDDELD	Certificaten verlopen binnenkort of zijn te zwak QS-SRV-021	**2** apparaten BAK-DC-01, BAK-FS-01
GEMIDDELD	NetBIOS over TCP/IP staat aan QS-WIN-020	**2** apparaten BAK-FS-01, BAK-WS-014
GEMIDDELD	AutoRun/AutoPlay is niet volledig uitgeschakeld QS-WIN-013	**2** apparaten BAK-WS-014, BAK-WS-021
GEMIDDELD	RDP staat aan op een werkplek QS-WIN-005	**2** apparaten BAK-WS-014, BAK-WS-021
LAAG	Verouderde software: updates beschikbaar QS-WIN-036	**3** apparaten BAK-FS-01, BAK-WS-014, BAK-WS-021
LAAG	Niet-standaard netwerkshares aangetroffen QS-WIN-017	**3** apparaten BAK-FS-01, BAK-WS-014, BAK-WS-021
LAAG	Gastaccount is aanwezig QS-WIN-008	**2** apparaten BAK-WS-014, BAK-WS-021
LAAG	Extern bureaublad-hulp staat aan QS-WIN-022	**2** apparaten BAK-WS-014, BAK-WS-021
LAAG	Automatische updates zijn niet afgedwongen QS-WIN-012	**2** apparaten BAK-WS-014, BAK-WS-021

04

Bevindingen op ernst

Kritiek (4)

Kerberoastbare accounts in bevoorrechte groepen

KRITIEK

QS-DC-014 · BAK-DC-01

Er zijn gebruikersaccounts met een SPN die ook in een bevoorrechte groep zitten. Elke gebruiker in het domein kan daar een ticket voor opvragen en dat offline kraken.

HERSTEL

Zet serviceaccounts om naar gMSA's, met automatisch beheerde wachtwoorden van 120 tekens. Haal SPN-accounts uit bevoorrechte groepen.

WDigest bewaart wachtwoorden leesbaar in het geheugen

KRITIEK

QS-WIN-046 · BAK-DC-01

Met WDigest UseLogonCredential=1 bewaart Windows wachtwoorden in leesbare vorm in het LSASS-geheugen, waar tools voor credential-diefstal ze zo uitlezen. Moderne Windows-versies zetten dit standaard uit.

HERSTEL

Zet UseLogonCredential op 0 onder HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest, via Intune of GPO.

WDigest bewaart wachtwoorden leesbaar in het geheugen

KRITIEK

QS-WIN-046 · BAK-FS-01

Met WDigest UseLogonCredential=1 bewaart Windows wachtwoorden in leesbare vorm in het LSASS-geheugen, waar tools voor credential-diefstal ze zo uitlezen. Moderne Windows-versies zetten dit standaard uit.

HERSTEL

Zet UseLogonCredential op 0 onder HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest, via Intune of GPO.

WDigest bewaart wachtwoorden leesbaar in het geheugen

KRITIEK

QS-WIN-046 · BAK-WS-021

Met WDigest UseLogonCredential=1 bewaart Windows wachtwoorden in leesbare vorm in het LSASS-geheugen, waar tools voor credential-diefstal ze zo uitlezen. Moderne Windows-versies zetten dit standaard uit.

HERSTEL

Zet UseLogonCredential op 0 onder HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest, via Intune of GPO.

Hoog (12)

LDAP-ondertekening wordt niet vereist

HOOG

QS-DC-011 · BAK-DC-01

De domeincontroller accepteert LDAP zonder ondertekening, waardoor relay-aanvallen op LDAP mogelijk blijven.

HERSTEL

Zet 'Domeincontroller: vereisten voor LDAP-serverondertekening' op 'Ondertekening vereisen' via het domeincontrollerbeleid.

ms-DS-MachineAccountQuota staat niet op 0

HOOG

QS-DC-010 · BAK-DC-01

Elke gebruiker mag computeraccounts aanmaken in het domein. Dat is de opstap voor onder meer resource-based constrained delegation-aanvallen.

HERSTEL

Set-ADDomain -Identity '<domein>' -Replace @{'ms-DS-MachineAccountQuota'=0}.

Bevoorrechte accounts zitten niet in Protected Users

HOOG

QS-DC-018 · BAK-DC-01

Domain Admins en vergelijkbare accounts vallen niet onder Protected Users, dus hun credentials worden nog gecachet en via NTLM gebruikt.

HERSTEL

Voeg Domain Admins, Enterprise Admins en Schema Admins toe aan Protected Users. Test eerst op compatibiliteit.

Het KRBTGT-wachtwoord is lang niet gewijzigd

HOOG

QS-DC-009 · BAK-DC-01

Het KRBTGT-account tekent elk Kerberos-ticket in het domein. Een oude sleutel betekent dat een golden ticket uit het verleden nog werkt.

HERSTEL

Reset het KRBTGT-wachtwoord met het resetscript van Microsoft — twee keer, met meer dan tien uur ertussen.

Print Spooler draait op een server (PrintNightmare)

HOOG

QS-WIN-021 · BAK-FS-01

De Print Spooler draait op een server. Dat is een bekende aanvalsroute (PrintNightmare, CVE-2021-34527) en hoort uit te staan tenzij de server echt print.

HERSTEL

Stop-Service Spooler; Set-Service Spooler -StartupType Disabled.

Onveilige, luisterende poorten op de server

HOOG

QS-SRV-002 · BAK-FS-01

Er luisteren diensten met protocollen die het verkeer niet versleutelen, zoals Telnet of FTP. Credentials gaan daar leesbaar over de lijn.

HERSTEL

Stop en schakel die diensten uit, en vervang ze door versleutelde equivalenten (SSH, SFTP of FTPS).

Credential Guard staat niet aan

HOOG

QS-WIN-015 · BAK-FS-01

Credential Guard isoleert de credentials in LSASS met virtualisatiebeveiliging. Zonder dat zijn ze te bemachtigen zodra iemand lokaal beheerder is.

HERSTEL

Zet virtualisatiebeveiliging en Credential Guard aan via Intune of GPO, na een compatibiliteitstest met eventuele LSA-plug-ins.

BitLocker is niet ingeschakeld op alle volumes

HOOG

QS-WIN-003 · BAK-WS-014

Een onversleuteld volume op een werkplek betekent dat de data leesbaar is zodra het apparaat kwijtraakt of de schijf eruit gaat.

HERSTEL

Zet BitLocker aan met Enable-BitLocker en bewaar de herstelsleutel in Entra ID of Active Directory, zodat hij terug te vinden is.

Windows LAPS is niet aangetroffen

HOOG

QS-WIN-011 · BAK-WS-014

Zonder LAPS deelt het lokale Administrator-account op dit apparaat waarschijnlijk zijn wachtwoord met de rest van de vloot. Een hash die ergens wordt buitgemaakt, opent dan alles.

HERSTEL

Rol Windows LAPS uit via Intune of GPO, zodat elk apparaat een eigen, willekeurig lokaal beheerderswachtwoord krijgt.

BitLocker is niet ingeschakeld op alle volumes

HOOG

QS-WIN-003 · BAK-WS-021

Een onversleuteld volume op een werkplek betekent dat de data leesbaar is zodra het apparaat kwijtraakt of de schijf eruit gaat.

HERSTEL

Zet BitLocker aan met Enable-BitLocker en bewaar de herstelsleutel in Entra ID of Active Directory, zodat hij terug te vinden is.

Windows LAPS is niet aangetroffen

HOOG

QS-WIN-011 · BAK-WS-021

Zonder LAPS deelt het lokale Administrator-account op dit apparaat waarschijnlijk zijn wachtwoord met de rest van de vloot. Een hash die ergens wordt buitgemaakt, opent dan alles.

HERSTEL

Rol Windows LAPS uit via Intune of GPO, zodat elk apparaat een eigen, willekeurig lokaal beheerderswachtwoord krijgt.

LSA Protection (RunAsPPL) staat uit

HOOG

QS-WIN-045 · BAK-WS-021

LSA Protection draait LSASS als beschermd proces, zodat tools voor credential-diefstal de credentials niet uit het geheugen kunnen lezen.

HERSTEL

Zet LSA Protection aan (RunAsPPL=1, of 2 met UEFI-lock) via Intune of GPO en start opnieuw op. Controleer eerst of LSA-plug-ins van derden blijven werken.

Gemiddeld (22)

	TITEL	CATEGORIE	GETROFFEN SYSTEEM
GEMIDDELD	Het standaard wachtwoordbeleid van het domein is te ruim QS-DC-001		BAK-DC-01
GEMIDDELD	Inactieve gebruikersaccounts in het domein QS-DC-004		BAK-DC-01
GEMIDDELD	Accounts waarvan het wachtwoord nooit verloopt QS-DC-005		BAK-DC-01
GEMIDDELD	De AD-prullenbak staat niet aan QS-DC-007		BAK-DC-01
GEMIDDELD	Accounts met PasswordNotRequired QS-DC-016		BAK-DC-01
GEMIDDELD	Certificaten verlopen binnenkort of zijn te zwak QS-SRV-021		BAK-DC-01

	TITEL	CATEGORIE	GETROFFEN SYSTEEM
GEMIDDELD	Certificaten verlopen binnenkort of zijn te zwak QS-SRV-021		BAK-FS-01
GEMIDDELD	Tijdsynchronisatie wijkt af van de domeinbron QS-SRV-023		BAK-FS-01
GEMIDDELD	Lokaal beheerdersbeheer op de server is niet op orde QS-SRV-022		BAK-FS-01
GEMIDDELD	Auditbeleid dekt niet alle vereiste subcategorieen QS-WIN-010		BAK-FS-01
GEMIDDELD	LLMNR staat aan en is te misbruiken voor poisoning QS-WIN-019		BAK-FS-01
GEMIDDELD	NetBIOS over TCP/IP staat aan QS-WIN-020		BAK-FS-01
GEMIDDELD	Defender-instellingen liggen onder de baseline QS-WIN-048		BAK-FS-01
GEMIDDELD	AutoRun/AutoPlay is niet volledig uitgeschakeld QS-WIN-013		BAK-WS-014
GEMIDDELD	RDP staat aan op een werkplek QS-WIN-005		BAK-WS-014
GEMIDDELD	Auditbeleid dekt niet alle vereiste subcategorieen QS-WIN-010		BAK-WS-014
GEMIDDELD	LLMNR staat aan en is te misbruiken voor poisoning QS-WIN-019		BAK-WS-014
GEMIDDELD	NetBIOS over TCP/IP staat aan QS-WIN-020		BAK-WS-014
GEMIDDELD	AutoRun/AutoPlay is niet volledig uitgeschakeld QS-WIN-013		BAK-WS-021
GEMIDDELD	RDP staat aan op een werkplek QS-WIN-005		BAK-WS-021
GEMIDDELD	Auditbeleid dekt niet alle vereiste subcategorieen QS-WIN-010		BAK-WS-021
GEMIDDELD	LLMNR staat aan en is te misbruiken voor poisoning QS-WIN-019		BAK-WS-021

Laag (18)

	TITEL	CATEGORIE	GETROFFEN SYSTEEM
LAAG	Uitgeschakelde accounts in Domain Admins QS-DC-006		BAK-DC-01
LAAG	Verweesde accounts met AdminCount=1 QS-DC-019		BAK-DC-01
LAAG	Het functionele niveau van het domein is verouderd QS-DC-017		BAK-DC-01
LAAG	Server wacht op een herstart na updates QS-SRV-024		BAK-FS-01

	TITEL	CATEGORIE	GETROFFEN SYSTEEM
LAAG	NPS-beleid staat zwakke authenticatie toe QS-SRV-019		BAK-FS-01
LAAG	Verouderde software: updates beschikbaar QS-WIN-036		BAK-FS-01
LAAG	Niet-standaard netwerkshares aangetroffen QS-WIN-017		BAK-FS-01
LAAG	Gastaccount is aanwezig QS-WIN-008		BAK-WS-014
LAAG	Extern bureaublad-hulp staat aan QS-WIN-022		BAK-WS-014
LAAG	Verouderde software: updates beschikbaar QS-WIN-036		BAK-WS-014
LAAG	Niet-standaard netwerkshares aangetroffen QS-WIN-017		BAK-WS-014
LAAG	Automatische updates zijn niet afgedwongen QS-WIN-012		BAK-WS-014
LAAG	WinRM draait QS-WIN-007		BAK-WS-014
LAAG	Gastaccount is aanwezig QS-WIN-008		BAK-WS-021
LAAG	Extern bureaublad-hulp staat aan QS-WIN-022		BAK-WS-021
LAAG	Verouderde software: updates beschikbaar QS-WIN-036		BAK-WS-021
LAAG	Niet-standaard netwerkshares aangetroffen QS-WIN-017		BAK-WS-021
LAAG	Automatische updates zijn niet afgedwongen QS-WIN-012		BAK-WS-021

05

Overzicht per apparaat

HOSTNAAM	BESTURINGSSYSTEEM	RISICOSCORE	KRITIEK	HOOG	LAATSTE SCAN
BAK-DC-01	—	F · 79	2	4	2026-09-15
BAK-FS-01	—	F · 75	1	3	2026-09-15
BAK-WS-021	—	F · 72	1	3	2026-09-14
BAK-WS-014	—	D · 64	0	2	2026-09-14

06

Compliance-momentopname

Dekking ten opzichte van de voor uw organisatie relevante kaders.

KADER	DEKKING	TEKORTKOMINGEN
CIS Controls v8	**41%**	30 / 51
NIST CSF 2.0	**25%**	18 / 24
ISO/IEC 27001:2022	**24%**	25 / 33
NIS2 Directive (EU) 2022/2555	**9%**	10 / 11
CIS Microsoft 365 Foundations Benchmark	**100%**	0 / 12
CIS Microsoft Windows Benchmark	**39%**	17 / 28

Grootste tekortkomingen

	TITEL	KADER
KRITIEK	Kerberoastbare accounts in bevoorrechte groepen QS-DC-014	CIS Controls v8 · CIS 6.5
KRITIEK	Kerberoastbare accounts in bevoorrechte groepen QS-DC-014	ISO/IEC 27001:2022 · A.9.4.3
KRITIEK	Kerberoastbare accounts in bevoorrechte groepen QS-DC-014	ISO/IEC 27001:2022 · A.9.4.4
HOOG	BitLocker is niet ingeschakeld op alle volumes QS-WIN-003	CIS Controls v8 · CIS 3.11
HOOG	Windows LAPS is niet aangetroffen QS-WIN-011	CIS Controls v8 · CIS 5.4
HOOG	Credential Guard staat niet aan QS-WIN-015	CIS Controls v8 · CIS 16.6
HOOG	LDAP-ondertekening wordt niet vereist QS-DC-011	CIS Controls v8 · CIS 9.3
HOOG	BitLocker is niet ingeschakeld op alle volumes QS-WIN-003	NIST CSF 2.0 · PR.DS-1