

Bijlage 14 Monitoring en beheertools ICT

Nr	Product/dienst	Functie				Toolnaam	Wie		Monitoring/Opvolging		Functie
		Aanwezig	Afwezig	beheer	monitoring		VRLN	Externe partner	Kantooruren	24/7	
1	Inframonitoring	X			X	Oversight.ht	1	2	X		Monitoren technische beschikbaarheid
2	Firewall + IPS + IDS	X		X		Palo Alto PA3220 + PA220		1	n.v.t.	n.v.t.	Bescherming tegen aanvallen van buitenaf + Bescherming van verkeer tussen netwerk segmenten inclusief internet
3	Centraal firewall beheer	X		X		Palo Alto Panorama		1			
4	SOC		X	X		n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	Opvolging SIEM meldingen
5	SIEM		X		X	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	Verzamelen en combineren data van monitoring en beheer systemen
6	Vulnerability management Werkplekken	X	X	X		Defender/SIEM	1	2	n.v.t.	n.v.t.	Scan je werkplekken op bekende vulnerability's en patches
7	Vulnerability management Servers		X			SIEM	n.v.t.	n.v.t.	n.v.t.	n.v.t.	Scan je netwerk op bekende vulnerability's en patches
8	Netwerk segmentering	X	X	X		Layer 2:Procurve 5406 Layer3: Palo Alto PA3220	1	2	n.v.t.	n.v.t.	Beheermaatregel
9	Centrale logging facility		X		X	SIEM	n.v.t.	n.v.t.	n.v.t.	n.v.t.	
10	Encryptie werkplekken	X		X		Microsoft Bitlocker	1	2	n.v.t.	n.v.t.	Encryptie van de lokale harddisk van de laptop i.c.m. de TPM module (Encryptie key wordt opgeslagen in de Azure Active Directory.
11	Anti virus en malware werkplekken	X		X		Microsoft Defender ATP	1		n.v.t.	n.v.t.	Virus/Malware scanner. Opsporen virussen, malware, crypto ware e.d.
12	Anti virus en malware Servers	X		X		Cortex XDR --> Microsoft Defender ATP for Servers	1		n.v.t.	n.v.t.	Virus/Malware scanner. Opsporen virussen, malware, crypto ware e.d.
13	Windows Firewall	X		X		Windows Firewall	1		n.v.t.	n.v.t.	
14	Mobile device management					Microsoft Intune	1	2	n.v.t.	n.v.t.	Voor beheer en updates werkplekken
15	Remote server beheer	X		X		Ansible & Ivanti Automation	1	2	n.v.t.	n.v.t.	
16	Identity	X		X		Centrale identity database	1		n.v.t.	n.v.t.	Microsoft Active Directory , en Azure Active Directory
17	Lokaal Admin password policy	X		X		Microsoft LAPS	1		n.v.t.	n.v.t.	Wijzig periodiek het wachtwoord van de lokale Administrator
18	Data classificatie en RBA	X	?	X		Microsoft Office E5 Compliance add-on (DLP)	1		n.v.t.	n.v.t.	Beheermaatregel
19	User password policy	X		X		GPO	1		n.v.t.	n.v.t.	Beheermaatregel
20	certificaat based vpn toegang	X		X		Microsoft CA icm Palo GlobalProtect		1	n.v.t.	n.v.t.	Microsoft CA icm Palo GlobalProtect
21	Certificaat en NPS authenticatie met WIFI netw	X	X	X		Extreme wifi i.c.m. Microsoft NPS server. Nu nog op basis van Radius , na het project op basis van certificaten		1	n.v.t.	n.v.t.	Hierdoor kunnen alleen VRLN werkplekken verbinding maken met het Wifi BYOD netwerk.
22	2 factor authenticatie	X		X		SMSPasscode (na migratie komt deze te vervallen) en Microsoft Azure MFA	1	2	n.v.t.	n.v.t.	
23	Reverse proxy en secure citrix gateway	X		X		Citrix Netscaler VPX200 & Azure Application Proxy	1	2	n.v.t.	n.v.t.	
24	Backup restore	X				NetApp Snapshots, en Veeam Backup		1	n.v.t.	n.v.t.	Veiligstellen, Bewaren en Herstellen van data
25	NetApp cluster	X				NetApp storage		1	n.v.t.	n.v.t.	Iedere 4 uur een mirror tussen de productie en uitwijk NetApp + iedere 4 uur snapshots
26	PENTEST		X			Penetratietest periodiek (Externe partij)	n.v.t.	n.v.t.	n.v.t.	n.v.t.	Penetratietest periodiek (Externe partij)
27	Veilig mailen	X				Zivver	1		n.v.t.	n.v.t.	uitgebreide NTA 7516 certificering in de markt. Hier moeten alle Nederlandse gemeenten en overheidsinstellingen aan voldoen. De NTA 7516 is de norm voor veilige ad hoc communicatie van gezondheidsinformatie. Deze norm is gemaakt door de NEN, in opdracht van het ministerie van VWS, het Informatieberaad zorg en gemeenten
28	Monitoring Vodafone verbindingen			X	X	Vodafone portal	1		X		
29	T-Mobile portal			X		T-Mobile portal	1		n.v.t.	n.v.t.	
30	Monitoring laptops op defecten	X			X	HP Saas	1				
31	Monitoring Mobiele telefoons op defecten		X			HP Saas	n.v.t.	n.v.t.	n.v.t.	n.v.t.	
32	Communicatieplatform					n.v.t.		1. Kreuze			
33	Communicatieplatform: cc4skype			X		cc4skype beheerconsole	1. VRLN	2. Kreuze			