MDR Coverage Map Worksheet

Map what your MDR can actually see, detect and respond to, then assign an owner to every gap.

Organization _____ **Completed by** _____ **Date** _____

Circle one: Y = Yes P = Partial N = No ? = Don't know. If you cannot verify an answer, circle ?. Every P, N or ? needs a named owner, or a conscious decision by leadership to accept the risk.

Environment	Do we know what exists?	Does the MDR see it?	Can it detect threats there?	Can it respond?	Who owns the gap?	Evidence / next step
Endpoints Laptops and desktops	Y P N ?	Y P N ?	Y P N ?	Y P N ?		
Servers On-premises and virtual servers	Y P N ?	Y P N ?	Y P N ?	Y P N ?		
Identity Entra ID, Active Directory, privileged accounts	Y P N ?	Y P N ?	Y P N ?	Y P N ?		
Microsoft 365 / email Mailboxes, email security, collaboration	Y P N ?	Y P N ?	Y P N ?	Y P N ?		
Cloud workloads Azure, AWS, Google Cloud	Y P N ?	Y P N ?	Y P N ?	Y P N ?		
SaaS applications Business-critical SaaS apps	Y P N ?	Y P N ?	Y P N ?	Y P N ?		
Network infrastructure Firewalls, VPN, DNS, switches	Y P N ?	Y P N ?	Y P N ?	Y P N ?		
Internet-facing assets Public IPs, websites, remote access	Y P N ?	Y P N ?	Y P N ?	Y P N ?		
OT / IoT Production, building, medical and connected devices	Y P N ?	Y P N ?	Y P N ?	Y P N ?		
Third-party connections Vendor access, integrations, MSP tools	Y P N ?	Y P N ?	Y P N ?	Y P N ?		
Other:	Y P N ?	Y P N ?	Y P N ?	Y P N ?		