Detection of Commonly Used Port, Detection Strategy DET0736

Archived: 2026-04-05 15:38:46 UTC

AN1869

Analyze network data for uncommon data flows (e.g., new protocols in use between hosts, unexpected ports in use). Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious.
Monitor for mismatches between protocols and their expected ports (e.g., non-HTTP traffic on tcp:80). Analyze packet contents to detect communications that do not follow the expected protocol behavior for the port that is being used.[1]

Log Sources

Data Component	Name	Channel
Network Traffic Flow (DC0078)	Network Traffic	None
Network Traffic Content (DC0085)	Network Traffic	None