Recommendation	Pros	Cons
Antivirus software	Often the first line of defense. Already in place Detects and stops a lot of commonly used malware	Limited signature coverage, requires updates. Can prove expensive for large enterprise
NIDS/NIPS	Useful if lot of web traffic is involved. Makes the job of detection and prevention easier	Latency of servers may increase. Encrypted files may fool the system
User Training/Awareness	Essential to improve cyber hygiene of the company Usually the most common attack-vector - humans	Losing important man-hours and fatigue Periodic training required if high attrition
Softwares (email detonation, anti-spoofing)	Already in place, comes packaged with Microsoft	Not completely reliant, some emails pass through
Logging/Sysmon	Already in place, utmost priority for detection, forensics	High labour cost for skilled workers who can detect anomalies, heavy volume of logs
Policy config settings	Low cost upgrades, open-source tools available (osscap)	Periodic activity, man-hours wastage
Security config	RBAC, execution controls, user management, device inspection essential for accountability	Tedious for analysts, high support & time cost, small management group, less transparency
Network Segmentation/Proxy	Attack can be contained, RCE not possible from different subnet, can monitor web traffic and shut down infected network	Critical for low-latency operations, segmentation increases physical dependence on devices, increased equipment cost and complexity
Establish IT security dept.	Dedicated team with required skills, structured process automation, frees developers' & executives' time	Enormous supply gap of professionals, high labour cost, may require a lot of time