ICSecurity

Industrial Cyber Security

info@ICSecurity.dk 52826400

OT Log Collection
document version 0.1a

For log collection in an OT environment you rarely have the possibility to install additional client software on your windows hosts, thats where Windows Event Log Forwarding comes into play.

Its available even in the older versions(xp,2003) and it does not cost a dime.

Both for daily operation and when you need to do some incident response it is just soooooooooooooooo much easier if you have valid Logs available.!

Adrian Costea has written an excellent article regarding this, check out his blog at

https://www.vkernel.ro/blog/how-to-configure-windows-event-log-forwarding

other links

https://docs.microsoft.com/en-us/windows/security/threat-protection/use-windows-event-forwarding-to-assist-in-intrusion-detection