Destructive scenario resilience audit (Wiper)

The checklist below helps assess how an organization is prepared for a wiper attack, such as the DynoWiper incident. The goal is to identify weak points in backup, data recovery, and OT/IT security. This is not an evaluation of employees, but a verification of system resilience.

1. The "To Be or Not to Be" Question (Backup and Recovery)

Remember: a wiper does not encrypt, it destroys. If your backup is visible on the network, it will be destroyed too.

[ ] Do we maintain a copy of critical systems (especially SCADA/OT configurations) that is physically disconnected from the network (tape, a disk in a safe)?

[ ] Are backups "immutable"? - Do we use technology that prevents backups from being overwritten or deleted for a defined period, even with administrator privileges?

[ ] When did we last run a "bare metal recovery" test? - Have we tried to rebuild the environment from scratch on clean hardware, assuming the old hardware is bricked (permanently damaged at the software level and unusable)?

[ ] What is our real RTO (Recovery Time Objective) for Renewable Energy Sources/OT? – How many hours or days would it take us to manually reprogram controllers at wind/solar farms if automatic restore does not work?

2. Segmentation and Isolation (Stopping the Intruder)

Attackers often enter through the office network (IT) and jump to the industrial network (OT).

[ ] Do we have a "hard" IT/OT separation? – Can the accountant's or receptionist's computer be used in any way to reach (ping/RDP/SSH) devices in the network controlling the infrastructure?

[ ] How is the network boundary protected? – Is there only a firewall between zones, or do we use a **data diode** (one-way data flow) or **jump hosts** with enforced MFA?

[ ] Is Active Directory shared? – If the Domain Controller in the office is compromised, does that automatically provide credentials for logging into engineering workstations at a plant or facility?

3. Detection and “Living off the Land”

DynoWiper was launched after a quiet reconnaissance. You must detect them before they deploy the payload.

[ ] Do we monitor the use of legitimate tools at unusual hours? - Will our SOC get an alert if someone uses PowerShell, PsExec, or WMI at 3:00 a.m. to communicate with multiple hosts at once?

[ ] Do we see outbound traffic from the OT network? - Would we notice if a PLC controller or operator station starts trying to connect to an internet Command & Control (C2) server?

[ ] Do we have EDR on engineering workstations? - Is there software on infrastructure management computers that will block a process attempting mass deletion of system files (wiper-like behavior)?

4. Supply Chain, a Lesson from Renewables

Attackers often come through “back doors” via service providers.

[ ] Who has persistent remote access? - Do turbine/panel service teams have VPN tunnels open 24/7, or is access enabled “on demand” (Just-in-Time Access)?

[ ] Do we log vendor sessions? - Do we know exactly what an external engineer did during the last connection?

[ ] How do subcontractors authenticate? - Do we enforce MFA (multi-factor authentication), or do they share one password such as “Service2025!”?

5. Procedures for the “H-Hour”

When screens go dark, there is no time to read PDFs stored on a server that just disappeared.

[ ] Do we have paper copies of our procedures? - If an attacker wipes disks and encrypts SharePoint, do we have printed action plans and phone numbers?

[ ] Who has the authority to physically disconnect the network (“kill switch”)? - Does the shift manager know which cable to unplug to stop the attack before it spreads to the rest of the infrastructure, and do they have pre-approved executive authorization (“blanket approval”)?