SWIMLANE

AI-ACCELERATED ATTACKS

Is your attack surface outpacing your team? Five actions to close the gap.

AI is compressing the time between vulnerability disclosure and active exploitation. These five actions give your team the edge.

Window between patch & exploit	Biggest OT / ICS risk factor	Unsupported legacy systems
Shrinking fast	**Long update cycles**	**Strategic liabilities**

5 ACTIONS YOUR SOC MUST OWN NOW

01 **Shrink your attack surface, deliberately** — EXPOSURE REDUCTION

Every exposed system is an invitation. Challenge whether systems need external connectivity at all, and isolate the ones that do.

02 **Treat patching like a race, because it is one** — VULNERABILITY MGMT

AI shrinks the gap between disclosure and exploit. Prioritize security updates and automate patching wherever you can.

03 **Stop carrying legacy systems as technical debt** — RISK MANAGEMENT

Unsupported systems are known quantities for attackers. Treat them as strategic liabilities, not tomorrow's problem.

04 **Lock down who gets access and keep it locked** — IDENTITY & ACCESS

Limit critical-system access to those who truly need it, enforce strong authentication, and review permissions continuously.

05 **Plan for the breach, not around it** — INCIDENT READINESS

Assume incidents will happen. Test response plans before you need them to speed of containment defines the blast radius.

See how Swimlane automates these defenses across your SOC.
Complete detection context. Faster response. Less exposure.

Book a demo →