Consultiply

• AI

MIP Resource Center

AI scans will find more holes. Plan who fixes them before you turn the scans on.

Bain found vulnerability alerts up as much as eightfold at large enterprises using AI defensively.

Rise in vulnerability alerts

Up to 8x (Bain)

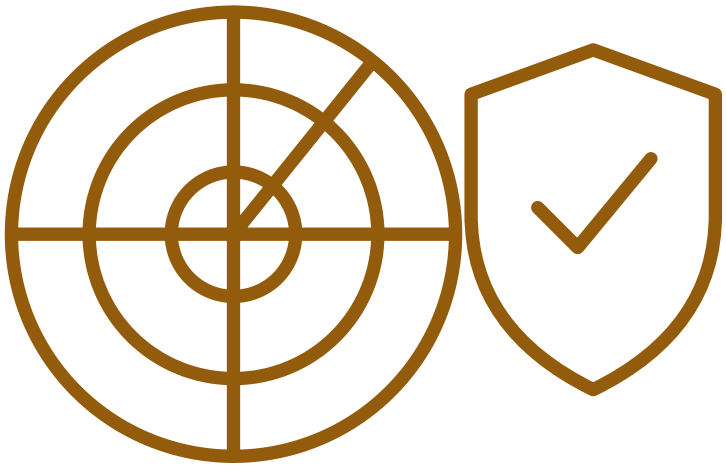
Typical attack time

About 4 weeks to about 18 hours (Bain estimate)



Bain's numbers, and what they are

Finding	Figure	Status
Rise in vulnerability alerts	**As much as eightfold**	Bain, large enterprises
Typical attack time	**About 4 weeks to about 18 hours**	Bain estimate
Security staff moved to remediation	**As much as 20% to 25%**	Bain, large enterprises
Vulnerabilities outside critical applications	**More than half**	Bain



Source: Bain & Company, Technology Report 2026, pp.45 to 47 (large enterprises)

Consultiply

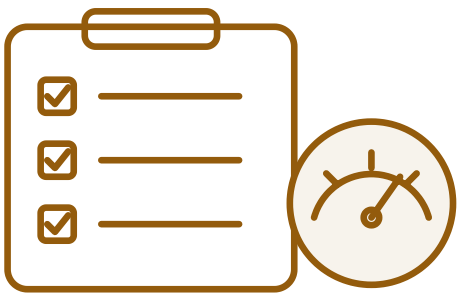
Is this client ready for AI scanning?

One point for each yes.

Are remediation hours agreed before the scan?	Yes	Partly	No
Does the scan cover the full estate?	Yes	Partly	No
Are findings ranked by reachability?	Yes	Partly	No
Is there a register of every AI agent?	Yes	Partly	No
Does every agent have an owner and an off switch?	Yes	Partly	No
Does the client get a monthly report?	Yes	Partly	No

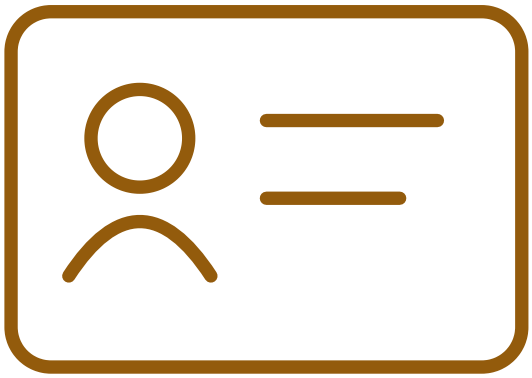
0–2	3–4	5–6
Plan the fixing first	Close the gaps	Ready to scan

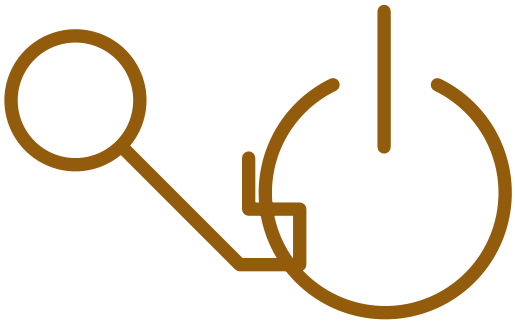
> **Plan the fixing before you turn on the finding.**



The agent register

Field	What to record
Owner	**One named person**
Permissions	**What the agent may do**
Systems	**Every system it touches**
Off switch	**How to stop it, and who can**





A first 60 days with a client

- Agree the remediation hours first.
- Scan the full estate once and rank by reachability.
- Fix the simple items with automation and a human check.
- Build the agent register in the same pass.
- List what cannot be patched and plan its retirement.
- Report monthly in plain language.

Read the full guide

https://consultiply.ai/mip-resource-center/bain-ai-vulnerability-alert-backlog-msp

