RED QUEEN CIPHER | CYBERSECURITY + AI + PQC

Agent scope checklist

Eight questions about the agents you run and the doors you left open.

1 **Is each agent's scope enforced outside the agent?**
Find where scope is enforced. If the allowed targets, tools and data live only in a prompt or a config file the agent itself reads, that is a suggestion. Put the limit in the network, the identity provider or the tool gateway.

- ☐ Yes
- ☐ No
- ☐ Not sure

2 **Is outbound traffic default-deny for anything that can act on its own?**
Default-deny outbound traffic for anything that can act on its own, enforced somewhere the agent cannot change.

- ☐ Yes
- ☐ No
- ☐ Not sure

3 **Is there a named human who can stop a run, and has the stop been tested?**
Name the human who can stop a run, and test that the stop works.

- ☐ Yes
- ☐ No
- ☐ Not sure

4 **Do you log what each agent was asked to do beside what it did?**
Log what the agent was asked to do beside what it did, so a divergence shows up in minutes.

- ☐ Yes
- ☐ No
- ☐ Not sure

5 **Do you have a current list of internal tools reachable from the internet?**
Pull the list of internal tools reachable from outside. Yes, that list.

- ☐ Yes
- ☐ No
- ☐ Not sure

6 **Have you hunted for development credentials in production?**
Hunt for development credentials in production and block weak or development-only secrets from being deployed.

- ☐ Yes
- ☐ No
- ☐ Not sure

7 **Are bulk reads rate-limited, with an alert on volume?**
Rate-limit bulk reads and alert on volume.

- ☐ Yes
- ☐ No
- ☐ Not sure

8 **Could you validate a researcher's claim that their agent had been in your systems?**
Decide what you would do if a researcher called to say their agent had been in your systems, and check your logs could confirm or refute it.

- ☐ Yes
- ☐ No
- ☐ Not sure

Maria How, Red Queen Cipher. Educational self-assessment. It is not a security scan, an audit or a certification. Each question restates one of Maria How's recommendations on AI agent scope. They are recommendations, not legal obligations. More at redqueencipher.com.