ASM buyer guide

Evaluate evidence, not just a feature list.

Use a consistent authorized scope and clear success criteria to compare attack surface monitoring solutions.

01 **Define the discovery scope**

Agree root domains, subsidiaries and exclusions. Record the customer-known inventory and observation period so newly found assets can be compared fairly.

02 **Challenge ownership reasoning**

Select shared infrastructure, a retired domain or a supplier-managed service. Ask for contributing signals, the confidence decision, reviewer action and dispute history.

03 **Verify assessment permission**

Document who can authorize testing, which techniques are allowed and how provider restrictions or exclusions are handled. Confidence and permission are independent controls.

04 **Inspect the priority inputs**

Compare findings using severity, exploitation evidence and business context. Ask why one exposure is prioritized over another and how analysts review the decision.

05 **Follow a finding to closure**

Inspect ownership, notifications, tickets, target dates, state transitions, acceptance expiry and closure evidence. Confirm supported integrations in the proposed deployment.

06 **Confirm operating and commercial fit**

Compare monitored units, domain allowances, retention, implementation effort, service scope and additional module requirements. Agree evaluation measures before testing.

YOUR NEXT STEP

Request a scoped ASM Visibility Assessment or discuss native iISOC adoption with the ClearSkies team. Agree scope, permissions, evaluation criteria and current commercial terms before testing.

https://www.clearskies.io/contact-us/