EXPOSURE & REMEDIATION

Vulnerability management with context.

Turn vulnerability findings into work your team can assess and own. Connect the affected software and systems to available threat intelligence, collection coverage and the next authorised action.

HOW IT WORKS

1. **Establish the sources.**
   Confirm which endpoint, inventory and vulnerability tools can actually provide evidence, and how current their data is.
2. **Consolidate the findings.**
   Bring host, product and CVE together in one register, keeping source observations and disagreements visible.
3. **Prioritise with context.**
   Read severity alongside CISA KEV, EPSS and public-exploit availability where available, and the affected system's importance.
4. **Choose and authorise the response.**
   Decide on a patch, configuration change or other action, and move supported changes through approval, recipe and maintenance controls.
5. **Verify the outcome.**
   Collect fresh inventory or assessment evidence after the work, retaining unresolved findings and unavailable sources.

WHAT THE VULNERABILITY WORKFLOW CAN SHOW

- A consolidated register linking a host, product and CVE across supported endpoint, on-premises software and Defender device associations.
- Severity alongside CISA Known Exploited Vulnerabilities context, EPSS and public exploit availability, where the provider supplies it.
- Version matches, fixed releases and conflicting observations that need investigation before a decision.
- Duplicate or uncertain device identity that leaves separate rows for review.
- Rows without an exploitation-based priority, flagged as unmeasured rather than automatically low risk.
- Source connection status and collection success, so a low count is not mistaken for a clean result.

A missing finding does not prove a system is fixed. A disconnected source, a failed collection or a device that stopped reporting can make a finding disappear.

Framework alignment. Vulnerability work maps directly to well-known control expectations: CIS Control 7 (Continuous Vulnerability Management), the NIST Cyber Security Framework Identify and Protect functions, and the security-update-management theme of UK Cyber Essentials. The consolidated register and prioritisation give a team the evidence those controls ask for.

Start with an authorised, read-only scope

Begin with your assessment questions; we agree coverage and delivery before any commitment.

threatshield@threatshield.global

Read the full page ↗

ThreatShield is part of ITS Consulting — ITS Consulting Ltd (United Kingdom) and ITS Consulting LLC (United States). This guide summarises an assessment capability; the actual scope, coverage and evidence available depend on your environment, licensing and permissions. Framework references organise findings and are not a certification or an assurance that a control is effective. © 2026 ThreatShield.