

CYBER THREAT INTELLIGENCE

Cyber Threat Intelligence (CTI) Program Starter Checklist

Threat intelligence is only useful if it changes decisions. This checklist helps small and mid-sized organizations stand up a lightweight, decision-focused CTI program.

Direction

- ☐ Identify intelligence consumers: leadership, IT, security operations, risk
- ☐ Write three to five priority intelligence requirements (e.g., 'Which ransomware groups target our industry?')
- ☐ List your crown-jewel assets and key third parties

Collection

- ☐ Subscribe to CISA alerts and the Known Exploited Vulnerabilities catalog
- ☐ Join your sector's Information Sharing and Analysis Center (ISAC) or an ISAO
- ☐ Use free feeds and platforms (abuse.ch, MISP, OpenCTI) sized to your capacity
- ☐ Track vendor advisories for every internet-facing product you run

Processing and analysis

- ☐ Map relevant threats to MITRE ATT&CK techniques
- ☐ Compare techniques with your current detections and controls
- ☐ Prioritize vulnerabilities by exploitation (KEV, EPSS), not severity alone

Dissemination and feedback

- ☐ Deliver short, actionable briefs: what happened, does it affect us, what to do
- ☐ Turn intelligence into hunts, detections, patches, and awareness messages
- ☐ Review requirements quarterly and retire those that no longer drive decisions

General guidance for training and planning, not legal advice. Adapt to your environment, contracts, and regulators.