The Full Overview Story

In today’s complex threat landscape, cyber defence is not just about reacting to alerts — it is about anticipating, understanding, and shaping intelligence before adversaries’ strike. To make this shift, one healthcare organization applied the **Threat Intelligence Lifecycle** to transform how it understood phishing-based attacks and protected its digital perimeter.

Following a surge in security incidents, their internal review revealed that **80% of compromises originated from email-based phishing vectors**. Armed with this insight, they chose to **prioritize intelligence collection on email-specific indicators of compromise (IOCs)** rather than rely on overly broad or generic threat feeds.

From this point forward, their CTI team walked through each phase of the intelligence lifecycle:

* **Stage 1 – Planning**: They narrowed their scope to phishing, asking: “Who is targeting healthcare sectors via phishing?” and “What do real-world phishing lures look like in our industry?”
* **Stage 2 – Collection**: Intelligence gathering focused on high-signal sources — including user-reported phishing emails, SIEM alerts on mail gateway events, and curated OSINT feeds from VirusTotal and Abuse.ch. The team also built a mailbox for staff to forward suspected phishing emails directly to the CTI analysts.
* **Stage 3 – Processing**: The team cleaned, deduplicated, and normalized these reports using internal scripts and tools like MISP. They transformed raw emails into structured IOCs — IPs, domains, hashes — ready for cross-checking and enrichment.
* **Stage 4 – Analysis**: Leveraging frameworks like **MITRE ATT&CK** and the **Diamond Model**, they began mapping patterns — discovering that the phishing campaigns showed repeated infrastructure reuse (domains, hosting providers) and even potential links to a known APT group spoofing healthcare-themed services.
* **Stage 5 – Dissemination**: Outputs were shared in tailored formats: short executive briefings highlighted risk trends, while CSV and STIX-formatted IOCs were pushed to the SOC and security appliances for action.
* **Stage 6 – Feedback**: After deploying these insights, the organization tracked outcomes — blocked phishing emails increased by 43%, user reporting improved, and fewer incidents were traced back to missed phishing attempts.

This real-world story shows how the **Threat Intelligence Lifecycle** brings structure, focus, and measurable impact — even when time, staffing, and visibility are limited. By narrowing the lens to phishing in their own environment, this organization turned intelligence from a buzzword into a practical force multiplier.