

The collaborative exchange of information about cyber threats and defense mechanisms between entities.

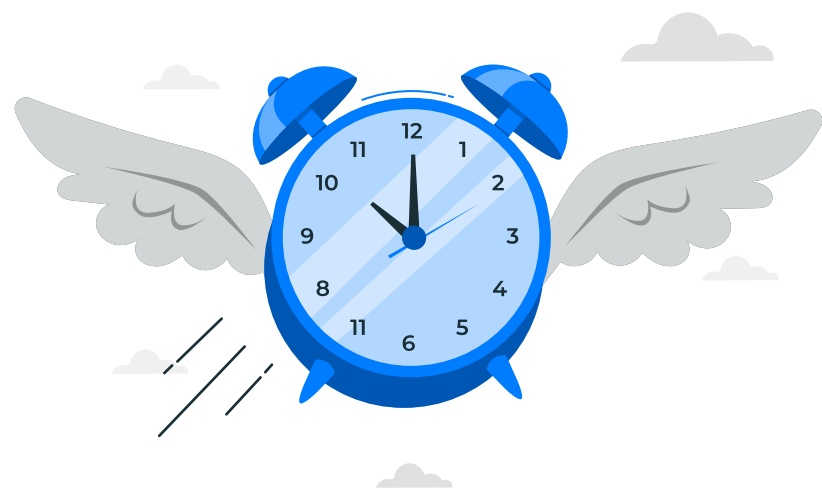
The Impact of Not Sharing:



- A. Increased Vulnerability:** Organizations are left to defend against cyber threats separately when information is not shared, widening the knowledge gap and increasing vulnerability.
- B. Recurrence of Known Attacks:** Known attacks, often overlooked, account for 90% of security breaches. Failing to share information about these threats can lead to them infiltrating other businesses.
- C. Delayed Response:** On average, it takes 280 days to identify and respond to a security breach.

Benefits of Threat Sharing:

- A. Faster Response Time:** Sharing threat intelligence can significantly reduce the time frame to identify and respond to security breaches.



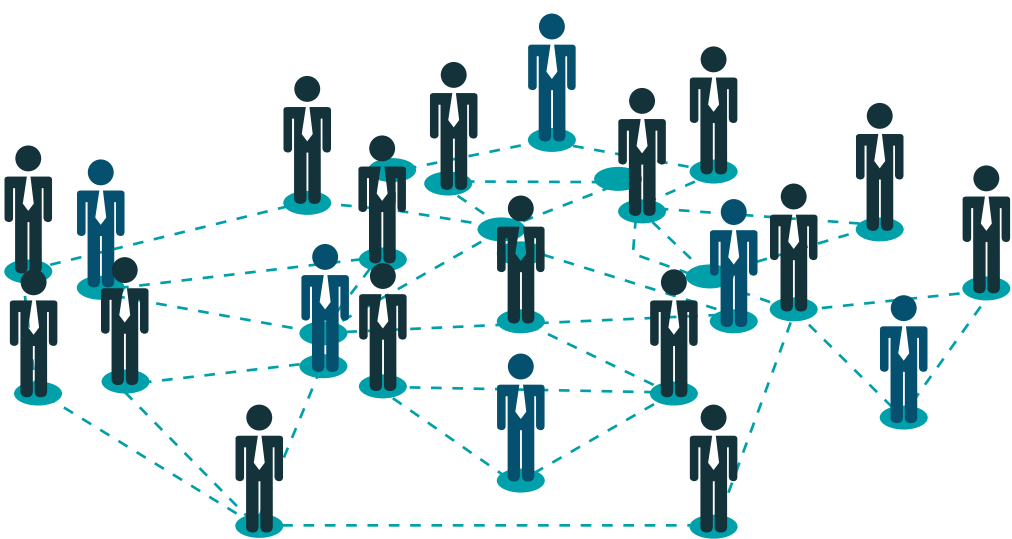
- B. Improved Security Posture:** 79% of security professionals agree that threat data feeds improve their organization’s security posture.



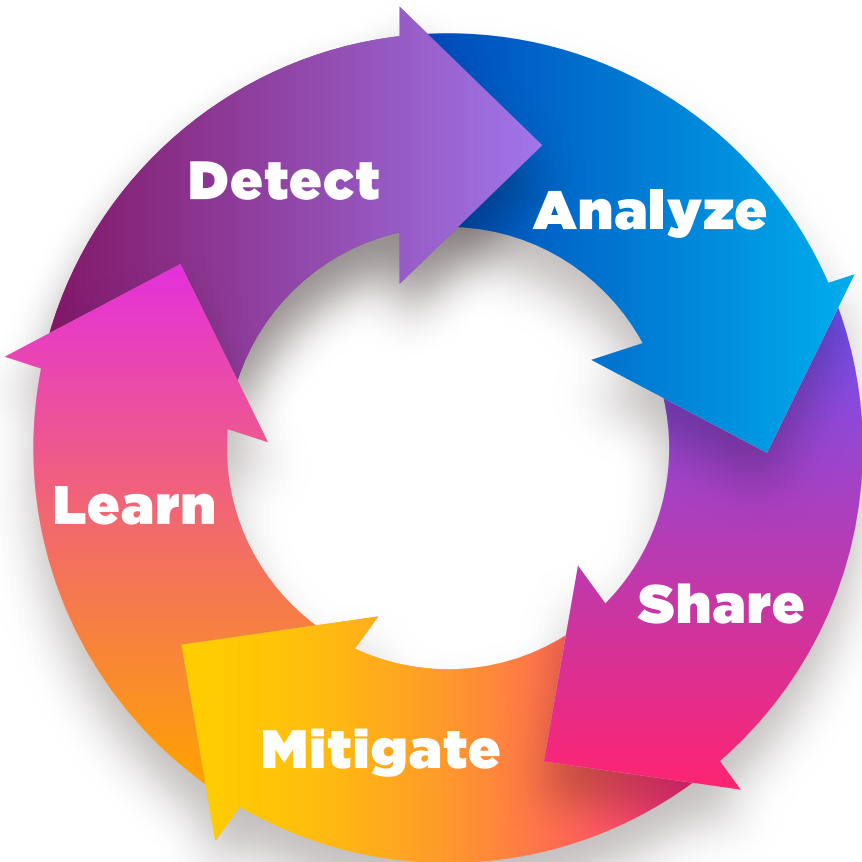
- C. Better Decision Making:** Threat sharing provides timely and actionable data that help organizations make informed security decisions.



- D. Community Development:** Promotes collaboration and community building amongst cybersecurity professionals.



Threat Sharing Cycle:





Keepnet’s Threat Sharing Platform:



Harness the power of collective intelligence with Keepnet’s Threat Sharing Platform. Equip your organization with real-time insights and collaborative tools for a proactive defense strategy.

Join the fight!

Try Keepnet’s Threat Sharing Platform for **free** and see how **+1 million** threat hunters protect you!

 info@keepnetlabs.com