Threat intelligence is more than just raw threat information. It is threat information that has been correlated and analyzed to give security professionals an in-depth understanding of the potential threats their organizations face—including how to stop them.

More specifically, threat intelligence has three key characteristics that distinguish it from raw threat information:

* **Organization-specific:** Threat intelligence goes beyond general information about hypothetical threats and attacks. Instead, it focuses on the organization’s unique situation: specific vulnerabilities in the organization’s attack surface, the attacks these vulnerabilities enable and the assets they expose.
* **Detailed and contextual:**Threat intelligence covers more than just the potential threats to an organization. It also covers the threat actors behind the attacks, the tactics, techniques and procedures (TTPs) they use and the indicators of compromise (IoCs) that might signal a successful cyberattack.
* **Actionable:**Threat intelligence gives information security teams insights that they can use to address vulnerabilities, prioritize threats, remediate risks and improve overall [security posture](https://www.ibm.com/think/topics/security-posture).