Threat vs. Attack: Understanding the Key Difference

Aspect	Threat	Attack
Definition	A potential event or condition that could exploit a vulnerability to cause damage.	A deliberate action that leverages vulnerabilities to compromise assets.
Nature	Latent risk, may exist without immediate exploitation.	Active exploitation, intended to cause breach, disruption, or damage.
Intent	Can be accidental (e.g., human error) or intentional (e.g., insider threat).	Always intentional and adversarial in nature.
Impact	May introduce risk exposure but not always materialize into incidents.	Results in a security incident with tangible impact.
Occurrence	Exists as a threat vector; exploitation is uncertain.	Manifestation of a threat into a real-world compromise.
Examples	Software vulnerabilities, phishing attempts, insider misuse, natural disasters.	Malware execution, credential theft, DDoS attacks, data exfiltration.
Key Distinction	Potential for exploitation, part of the threat landscape.	Realized action, execution of adversarial intent.

Visit www.ampcuscyber.com or reach out to us at letsconnect@ampcuscyber.com