Zero Latency Threat Detection Detection at Attacker Velocity: A Modern Security Framework

Gurucharan Raghunathan
Trench Security

Michael Wilson Rebello
Trench Security

Abstract

In the age of AI-powered threats, the physics of cyber warfare has changed. While defensive strategies have spent the last decade perfecting data aggregation, adversaries have perfected speed. Today, automated attacks execute in milliseconds, yet our industry's standard detection processes are measured in minutes, hours, or weeks. This temporal disconnect, the "Latency Gap" is where the modern breach lives.

For too long, security analytics has been perceived as a Data Problem and we were convinced to ingest everything and ended up with a data overload bottleneck. We hoard petabytes of logs to find the "needle in the haystack." This model is obsolete. AI has handed adversaries a new, defining moat: Velocity. AI-native threats do not pause for human cognition. Relying on legacy, data-centric detection models to fight these threats is akin to fighting drone warfare with ground patrol. To combat this, we must shift our mindset from Data to Time. You can have the most accurate threat detection rule in existence, but if it triggers 48 hours or even 48 seconds after the event, it is not a defense; it is forensics. The collateral damage has already occurred; the attacker is far ahead in the kill chain.

Just as the Zero Trust framework revolutionized security by shifting our focus from the "Perimeter" to "Identity" (Data), we must now evolve further. We introduce the Zero Latency Threat Detection (ZLTD) framework. This architecture accepts that in a world of instantaneous execution, the only effective defense is instantaneous detection. We must stop hunting for the needle and start catching it before it lands. Cybersecurity Mesh Architecture (CSMA) is the right approach to apply ZLTD that moves detection to the edge, reducing SIEM data gravity costs while delivering real-time, high-fidelity threat detection.