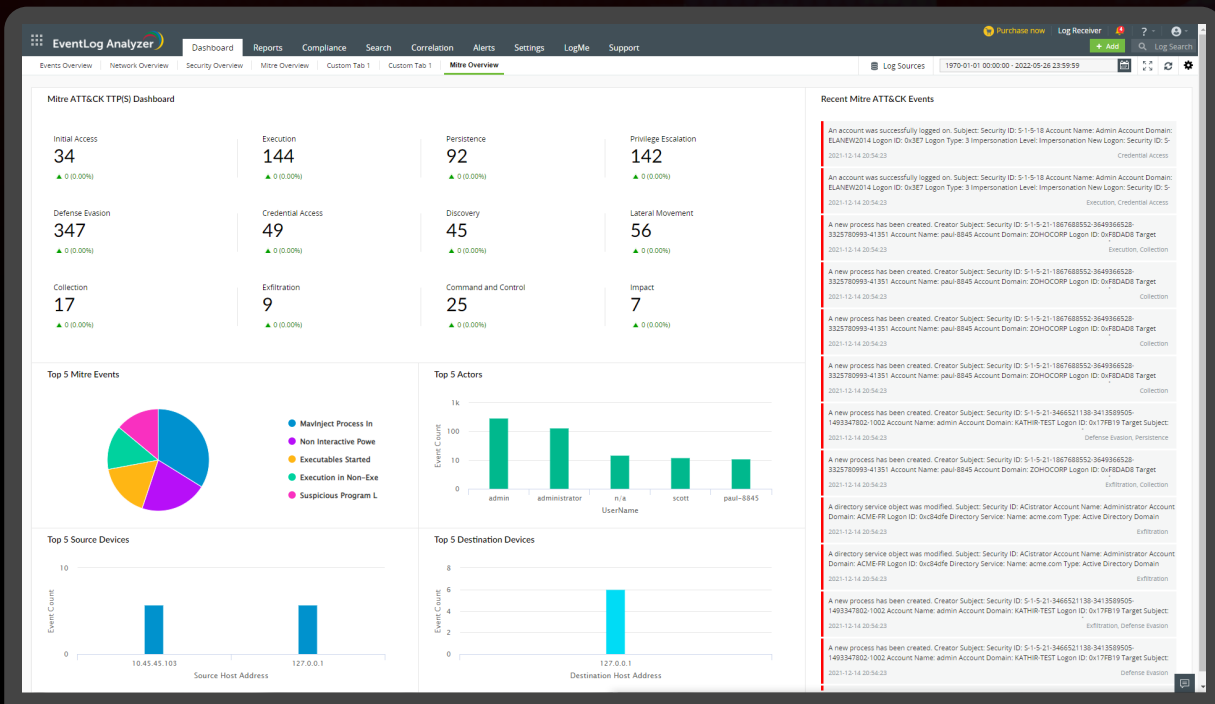


Extend your threat detection capabilities  
with Log360's adoption of

# MITRE ATT&CK



## Here's how Log360 can strengthen your threat detection and response capabilities with its MITRE ATT&CK dashboard:



### Expand threat detection capabilities

Broaden your threat detection capabilities by detecting and prioritizing security threats using the MITRE ATT&CK framework. Get a quick overview of recent and frequently used attack tactics and techniques, the most affected sources, and top actors to neutralize threats swiftly.



### Optimize your SOC metrics

Improve your mean time to detect and resolve an attack by gaining visibility into the most impactful threats with the ATT&CK dashboard. Investigate the recent red flags, mark them as incidents, and ensure accountability during threat resolution, all from a single console.



### Go beyond a single red flag

Trace the attacker's path, correlate different security threats mapped directly to MITRE ATT&CK techniques, and get insights into the complete plan of your attackers. This comprehensive approach enables you to devise strategies to prevent future incidents.



### Augment your threat detection accuracy

With more contextual data for each detected attack technique, improve your threat detection accuracy. Gain visibility into security loopholes, impacted hosts and destinations, and top actors to develop effective defensive and mitigation strategies.

## About Log360

Log360 is a unified SIEM solution with integrated DLP and CASB capabilities that detects, prioritizes, investigates and responds to security threats. Vigil IQ, the solution's TDIR module, combines threat intelligence, ML-based anomaly detection and rule-based attack detection techniques to detect sophisticated attacks, and it offers an incident management console for effectively remediating detected threats.

Scan this QR code for  
**Log360 Demo**



(or) logon to  
**zoho.to/log360demo**