STRENGTHS & WEAKNESSES OF LEGACY SOLUTIONS

MixMode

The evolving threat landscape and the proliferation of modern advanced threats have exposed the capability gaps of legacy security tools, necessitating a paradigm shift in the approach to threat detection and response.

The importance of adaptable and automated detection approaches cannot be overstated, as organizations seek to fortify their defenses against sophisticated cyber threats that evade traditional security measures.

Each of these tools has its strengths in specific areas of security, but they also have limitations.

NETWORK DETECTION AND RESPONSE (NDR)

Strengths: Provides deep visibility into network traffic, making it effective against network-based novel attacks and lateral movement of threats. It can also detect and respond to data exfiltration.

Weaknesses: Limited visibility into endpoint activities will cause difficulty detecting novel and AI-generated attacks that do not involve network traffic.

SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

Strengths: Centralized logging and correlation of security events for threat detection and compliance. Effective for identifying patterns of compromise and compliance-related issues.

Weaknesses: Often relies on rule-based detection, making it less effective against novel and AI-generated attacks that may not leave traditional traces.

ENDPOINT DETECTION AND RESPONSE (EDR)

Strengths: Provides visibility into endpoint activities and rapid response to threats originating from endpoints. Effective against ransomware and file-less attacks that target endpoints.

Weaknesses: Limited in defending against network-based attacks and will struggle with detecting novel and AI-generated attacks that do not involve endpoints.

EXTENDED DETECTION AND RESPONSE (XDR)

Strengths: Offers integrated visibility across multiple security layers, including network, endpoint, and cloud. Effective for correlating and responding to threats across different vectors.

Weaknesses: Will struggle with detecting AI-generated attacks that involve sophisticated evasion techniques and novel attack vectors.

USER AND ENTITY BEHAVIOR ANALYTICS (UEBA)

Strengths: Effective in identifying abnormal user behavior and insider threats, particularly in AI-generated attacks targeting user accounts and credentials.

Weaknesses: Limited in defending against network-based attacks and will struggle with detecting novel attack techniques that do not involve user behavior.

Organizations often need a combination of these tools along with advanced AI-driven analytics to combat the evolving threat landscape effectively.

MixMode®

MixMode offers a transformative solution to enhance legacy security controls by integrating advanced AI-driven threat detection and response capabilities. By addressing the limitations of traditional tools and augmenting them with adaptive, AI-powered analytics, MixMode empowers organizations to proactively defend against a wide array of threats, including novel attacks, ransomware, zero-day attacks, AI-generated threats, and more helping organizations to:

STRENGTHEN DEFENSES

Precision real-time threat detection for novel & known attacks, for cloud, on-prem or hybrid environments.

INCREASE EFFICIENCY

Make informed decisions & save time by focusing on the threats that matter & avoiding false positives that don't.

REDUCE COSTS

Reduce storage costs and eliminate the need for multiple disparate toolsets while up-leveling existing investments.

DETECT AT SCALE

Easily monitor the world's largest data sets in real-time to quickly detect & remediate advanced threats.

mixmode.ai

+1 (858) 225-2352 | info@mixmode.ai