LiveAction®

ThreatEye

Solution Overview

ThreatEye

Table of Contents

Key Challenges

Sophisticated threat actors are continually advancing their tactics through phishing and credential theft, social engineering attacks, and exploiting known vulnerabilities to launch cyber-attacks on enterprises. Malware resident on an endpoint is no longer a requirement to breach an organization. With the shift away from signature-based malware used in attacks, strategies focused on leveraging Endpoint Detection and Response (EDR) solutions are increasingly less effective.

SOC Analysts and Network Security Teams need a superior approach to effectively combat cyber-threats. Depth-in-defense strategies will always prove useful, but traditional security staples are proving ineffective to rapidly evolving threat actor methods.

The increased adoption of encryption by enterprises to harden their security posture and protect data has almost killed off the future of Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS) solutions.

For organizations to make an immediate impact against adversaries and stay ahead of tomorrow's threats, a different security strategy is overdue.

Encrypted Traffic Visibility and Advanced Behavioral Analysis

A Fundamentally Different Approach to Threat Detection

ELIMINATE NETWORK BLIND SPOTS

Encryption on the rise has rendered legacy EDR, IPS and IDS solutions ineffective in combating cyber-attacks. Decryption as a strategy is a doomed approach. Decryption leads to massively degraded network performance in addition to being difficult to manage and is also expensive to operate. ThreatEye's approach to encryption applies machine learning to deep packet dynamics without having to decrypt traffic. This approach significantly reduces operational complexity and costs to eliminate encryption blindness by detecting threats without having to inspect packet content.

EMPOWER EFFICIENT, EFFECTIVE SECOPS

ThreatEye's AI-powered NDR enables simplified management of the threat investigation life cycle by combining and correlating sets of high-fidelity findings to track the state of an incident.

ThreatEye's workflow capabilities support SOC analyst workflows with integrated packet analysis insights. This allows analysts to collaborate across their teams with an interactive layer. ThreatEye's integrated approach to searching, collaborating, and alerting, all in one place

- enables easy pivots from incident findings to flows to packets
- delivers lower mean time to resolution (MTTR)
- reduced costs of investigation by categorizing and classifying findings into incident states, conditions, and techniques

Auto-Correlated findings and enriched metadata provides complete contextual and actionable information needed to resolve incidents. ThreatEye collects and correlates information from disparate data sources such as geography, passive DNS, MITRE ATT&CK techniques, threat intelligence, risk, and threat scores, and more to aid responders with the best course of action for any investigation.

With a full REST API, ThreatEye interconnects with existing security tools such as SIEMs, SOARs, and Threat Intel solutions seamlessly. This allows SecOps teams to use ThreatEye as a valuable and easy addition to their existing security defense without creating more disparate environments within their organization.

ENABLE RAPID SECURITY INCIDENT RESPONSE

Predictive Threat Intelligence gives you an edge against Attackers. Threat Intelligence today is reactive, relying on Indicators of Compromise (IOCs) from active campaigns to get discovered and shared. You've likely already been breached to see an alert where you matched with an IOC.

ThreatEye's threat intelligence feeds are curated by our team to provide up-to-date indicators for active threats in the wild. This feed includes predictive threat intelligence and campaign tracking, revealing IPs and domains associated with threat actors before they are activated.

Tailored and predictive threat intelligence sets off fire alarms when users connect to threat actor infrastructure before campaigns are known, and IOCs get shared across the community

Lowering the time to detection reduces the dwell time of threat actors operating in an environment, in turn reducing the impact of ransomware attacks on enterprises. ThreatEye's advanced behavioral analysis allows analysts to quickly identify anomalies as the solution applies advanced AI to fingerprint profiles to understand when assets are behaving differently.

How ThreatEye Works

Supporting the ThreatEye platform is-an AI-powered analysis pipeline, combining data collection, advanced behavioral analysis, predictive threat intelligence, and machine learning to detect threat actors and comply with security regulations. Unfazed by encryption, ThreatEye examines network traffic traits and characteristics with machine learning-based analysis. Unlike traffic analysis solutions built on DPI technologies, the ThreatEye platform leverages Deep Packet Dynamics (DPD) to analyze traffic flows without decryption. DPD provides high-fidelity flow records with over 150 features for each flow—all without payload inspection. Packet Dynamics, backed by machine learning, enables new insights into encrypted traffic.

AI-Powered Advanced Behavioral Analysis

ThreatEye's AI-powered fingerprinting learns how networks operate and how devices interact. ThreatEye discovers anomalies by tracking multiple vectors of information, like Producer-Consumer-Ratios (PCRs) and nth degree social networks, to know when an attacker is active in an environment. ThreatEye creates a historical inventory of traits and behaviors, fingerprinting, mapping, and profiling assets. This technique works equally well with encrypted and unencrypted traffic. Machine Learning models are applied to identify behavioral anomalies indicating threat actor presence.

Key Benefits

- Encrypted Traffic Analysis
- Real-Time Threat Detection
- Advanced Behavioral Analysis
- Predictive Threat Intelligence
- Effective when EDR/IDS/MFA is bypassed
- Decreased Time to Investigate and Respond
- Validate Encryption Policy Compliance
- Auto Correlated and Enriched Findings with Passive DNS
- 365 Days of Retention
- Asset Tracking and Risk / Threat Scoring
- Unified Sensor & Intelligent Packet Capture
- Deploys in Minutes

Learn More

For more information about ThreatEye, please visit: https://www.liveaction.com/threateye

About LiveAction

LiveAction provides end-to-end visibility for network security and performance. By relying on a single source of truth – the packets – LiveAction gives modern enterprises the confidence needed to ensure the network is securely meeting business objectives, providing full network visibility to better inform NetOps and SecOps, and reducing the overall cost of network and security operations. By unifying and simplifying the source of collection, inspection, presentation, and analysis of network traffic, LiveAction empowers network and security professionals to identify, troubleshoot, and resolve issues across increasingly large and complex networks proactively and quickly. To learn more about LiveAction, visit www.liveaction.com.

LiveAction® | ThreatEye

960 San Antonio Rd, Suite 200, Palo Alto, CA 94303 +1 (888) 881-1116