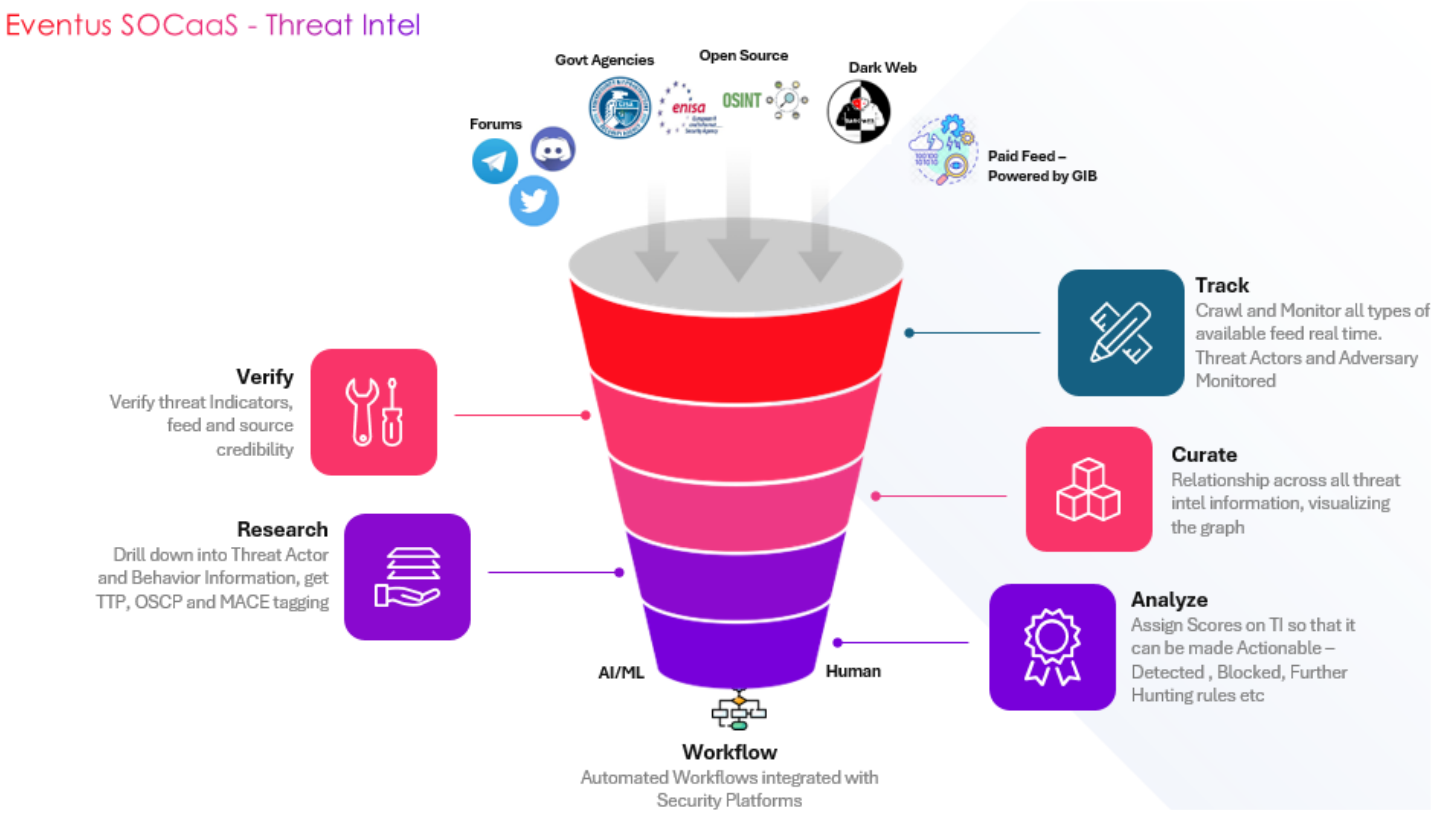
THREAT INTELLIGENCE PLATFORM

In today's rapidly evolving threat landscape, organizations face an unprecedented challenge: transforming overwhelming volumes of threat data into actionable intelligence that prevents attacks before they succeed. Traditional threat intelligence solutions collect data but fail to provide the contextual analysis and automated response capabilities needed for modern cybersecurity.

The Eventus Threat Intelligence Platform redefines cyber defense by transforming raw threat data into contextual, actionable intelligence. Built with a hybrid AI engine combining multi-stage LLM analysis and specialized machine learning models, the platform empowers security teams to move from reactive incident response to proactive threat prevention through intelligent automation and real-time correlation.



The Eventus Threat Intelligence platform employs a comprehensive funnel-based approach that begins with multi-source intelligence collection from forums, government agencies, open-source feeds, and dark web monitoring. Raw threat data flows through systematic processing stages

including verification of threat indicators and source credibility, detailed research into threat actor behavior and campaign attribution, relationship curation across all threat intelligence to build comprehensive knowledge graphs, and AI-powered analysis that assigns actionable scores enabling automated detection, blocking, and threat hunting capabilities. This integrated workflow combines human expertise with AI/ML processing to transform overwhelming threat data streams into precise, contextual intelligence that directly enhances security platform effectiveness through automated workflows and real-time threat correlation.

AI-POWERED THREAT INTELLIGENCE

The Eventus Threat Intelligence Platform operates as a comprehensive intelligence-driven defense system that transforms raw threat data into actionable security intelligence through automated processes and AI-powered analysis.

The platform continuously collects and processes threat intelligence from multiple premium sources including dark web monitoring, government agencies, commercial feeds, and open-source intelligence, processing thousands of threat indicators daily through advanced AI models to extract actionable intelligence with exceptional accuracy and minimal false positives.

KEY HIGHLIGHTS

- **Real-Time IOC Detection**
- **Automated Retrospective Scanning**
- **AI-Powered Advisory Generation**
- **Contextual Vulnerability Prioritization**
- **Knowledge Graph Intelligence**
- **Multi-Source Intelligence Aggregation**
- **Customer-Specific Contextualization**
- **MITRE ATT&CK Mapping**
- **Automated IOC Distribution**
- **Threat Actor Attribution**
- **Campaign Correlation**
- **EDR/SIEM Integration**
- **API-Driven Intelligence**
- **Evidence Chain Management**
- **Cross-Vector Correlation**
- **Historical Compromise Discovery**
- **MBC Mapping**
- **Processor-based attack detection**
- **Automated Threat Hunting**

CORE FEATURES

Real-Time IOC Detection:

Sub-second scanning of every ingested log against millions of IOCs in the threat intelligence database, immediately detecting and alerting on active threats as malicious activity occurs in customer environments while preventing persistence establishment through instant detection and response workflows.

Automated Retrospective Scanning:

When new threat indicators emerge, the platform automatically scans months of customer historical data to identify previously undetected compromises, providing complete attack timeline reconstruction for incident response and enabling comprehensive threat hunting across archived security events.

AI-Powered Advisory Generation:

Multi-stage ML and LLM processing engine automatically analyzes incoming threats, performs attribution analysis, and generates customer-specific advisories within same-day timelines, including executive summaries, technical analysis, MITRE ATT&CK mapping, and machine-readable IOC packages.

Contextual Vulnerability Prioritization:

Real-time correlation between emerging threats and customer vulnerability scans identifies which specific vulnerabilities are under active exploitation, automatically prioritizing patches based on active threat intelligence rather than theoretical CVSS scores for strategic risk management.

Knowledge Graph Intelligence:

Advanced relationship mapping between threat actors, campaigns, infrastructure, and attack techniques provides comprehensive threat context and enables predictive analysis, allowing security teams to anticipate threat actor behavior and implement proactive defense strategies.

Multi-Source Intelligence Aggregation:

Continuous collection and processing from dark web monitoring, government agencies, commercial feeds, and OSINT sources, with specialized threat research team validation ensuring high-quality intelligence delivery through automated curation and expert human oversight.

Sector-Specific Contextualization:

Sector specific analysis considers customers industry, geography, and technology stack for relevant threat assessment, automatically delivering customized threat intelligence that eliminates information overload while maximizing operational relevance and actionable insights.

Automated IOC Distribution:

Seamless integration with customer security ecosystems through high-success-rate IOC integration with EDR platforms, SIEM threat feed delivery with exceptional uptime, and real-time API integration for programmatic threat intelligence consumption.

Threat Actor Attribution:

Comprehensive threat actor identification and campaign correlation with exceptional accuracy, enabling organizations to understand attack motivations, predict likely next steps, and implement targeted defensive measures based on specific threat group behaviors and methodologies.

TRANSFORM YOUR SECURITY

The Eventus Threat Intelligence Platform fundamentally transforms how organizations approach cyber defense, shifting from overwhelming data streams to strategic intelligence that drives proactive security decisions. Through comprehensive multi-source collection, AI-powered analysis, and automated contextualization, the platform ensures that every piece of threat intelligence serves a clear defensive purpose.

What sets Eventus apart is its ability to learn and adapt—the hybrid AI engine and knowledge graph capabilities create an intelligence ecosystem that becomes more effective over time, automatically refining threat detection and attribution accuracy based on emerging attack patterns. This self-improving architecture means organizations don't just receive threat intelligence; they gain an evolving defense capability that anticipates and counters sophisticated adversaries.

By delivering contextual, automated, and immediately actionable intelligence, Eventus empowers security teams to stay ahead of the threat landscape rather than constantly reacting to it, creating a sustainable competitive advantage in an increasingly complex cybersecurity environment.