Lumu Maltiverse

Threat Intelligence for Decisive Defense

Overcome Threat Intelligence Challenges

Data Overload

Managing exponentially growing volume of diverse, often irrelevant, and inconsistently formatted threat intelligence data overwhelms human analysts.

Cost & Effort

Effectively using threat intelligence requires significant investment in human oversight, maintenance, data sources, and platforms.

False Positives

Inaccurate alerts stemming from unreliable sources and outdated indicators waste valuable analyst time and disrupt legitimate operations.

Integration Difficulties

Threat intelligence integration with existing security tools must be frictionless; bad deployments result in wasted data and delayed action.

Threat Intelligence as a Service

Subscribe to and integrate high-fidelity threat intelligence feeds or customize feeds according to your needs with Maltiverse.

Includes 100+ Intelligence Sources

Aggregates data from more than 100 different threat intelligence sources. Public, private, and community feeds are merged to provide a powerful aggregation.

Real-Time Classification

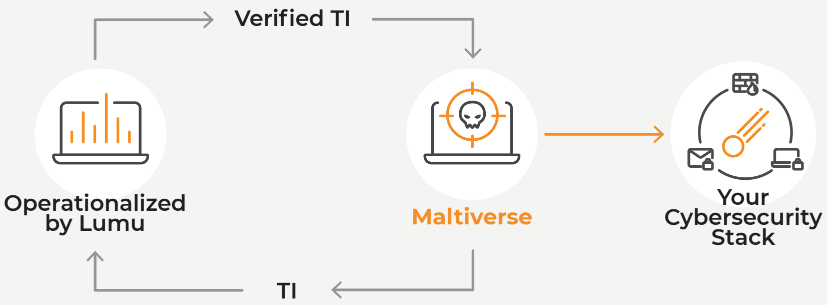
Analyzes hundreds of conditions to deliver accurate, human-readable classifications that update in real time.

Delivers to Your SIEM/SOAR/FW

Integrates with leading security tools, enabling a seamless setup with your security stack in minutes.

Real-Time Compromise Feedback

Lumu's broad visibility across networks, geographies, and industries ensures Maltiverse intelligence remains accurate, effective, and relevant.



Seamless Integrations

Supercharge your existing cybersecurity investments with 180+ pre-built integrations.

paloalto NETWORKS · FORTINET · CROWDSTRIKE · SentinelOne · CORTEX · D3 SECURITY · DEVO · OPENCTI

CHECK POINT · splunk> · TREND MICRO · TheHive · elastic · MISP Threat Sharing · THREAT CONNECT

Key Use Cases

Threat Analysis

Instantly transform raw text from any threat report, article, or log file into actionable intelligence. Maltiverse automatically extracts every IoC and gives the critical context needed to understand the risk.

Incident Triage

Assess an IoC (e.g. from a SIEM) for malicious activity using the blacklist timeline feature, tags that predict behaviors like C2 activity and provide context from MITRE. This focused, reactive evaluation of an indicator cuts triage time by 40-50%.

Threat Feeds

Create your own precise feeds by saving a Maltiverse Query Language (MQL) search or access curated pre-built feeds from over 100 sources. This enables proactive prevention for known threats and is scalable through more than 27 integrations with 3rd party cybersecurity tools.

Threat Hunting

Build hypotheses for attacks (for example a supply chain incident that might affect the organization) and test them using IoCs related to the incident or by building custom feeds to start hunting for that threat within your network.

Private IoCs

Upload your IoCs to the Maltiverse Platform to apply them to your threat intelligence cycle, including analysis, enhanced context, and dissemination. Your threat intelligence will remain private and not shared with other organizations or exposed publicly.

IoC Dissemination

Threat intelligence means little unless it's operationalized by controls. The Maltiverse Platform ensures that relevant, non-expired intelligence is delivered to all your cybersecurity tools.

Maltiverse Plans

Intelligence Plan

Gain full access to the entire range of Maltiverse threat intelligence feeds, connectors, and TAXII servers. Empower your team to customize threat intelligence feeds and bring high-fidelity Maltiverse data directly into your existing SIEM, SOAR, XDR, EDR, email, and Firewall solutions to enhance incident detection and response workflows.

Key Features

1. Threat Intelligence Feeds: Full access to Maltiverse threat feeds.
2. TAXII Server: Full support for structured feed integration.
3. Connectors: Direct integration with security solutions (e.g., Checkpoint, Fortinet, CrowdStrike, Elastic).
4. Custom Feeds: Build and manage your own feeds, tailored to your organization's needs.

Platform Plan

Go beyond consuming global feeds and fully operationalize unique, internally generated intelligence. Enable security teams to seamlessly move from raw data to actionable intelligence. Upload of your own private IoCs for processing and validation through advanced classification and scoring algorithms. By leveraging Enrichment Modules, IoCs are transformed into rich intelligence objects, giving analysts the context needed for fast, confident decisions.

Key Features

1. Unlimited threat feeds updated in real time.
2. Private IoC upload with secure cloud storage for secure, compliant management of your intelligence.
3. Advanced enrichment modules (MITRE ATT&CK, WHOIS, AbuseIPDB, Barracuda, Geolocation, etc.) to add actionable context.
4. Custom feed creation to tailor intelligence dissemination to your environment.
5. Connectors and integrations with SIEM, SOAR, XDR, email, firewalls, and EDRs.
6. TAXII server support for large-scale intelligence sharing.

Request Your 14-Day Trial at
www.maltiverse.com/trial