



ACTIONABLE THREAT INTELLIGENCE

Threat Intelligence That Turns Observables Into Context

Investigate domains, IPs and URLs with high-fidelity intelligence, infrastructure context and machine-readable outcomes

From Raw Observables to Actionable Intelligence

In today's rapidly evolving threat landscape, the battle against cyber adversaries requires constant vigilance and access to the latest threat data. To protect your organization, it's important to leverage an accurate and unambiguous threat feed to enable an accurate and efficient response.

Security analysts and incident responders are often confronted with observables for which they know little. Without context, it is difficult to understand an attack, assess impact or determine the next response action. Underscore's Threat Intelligence Aggregator (TIA) is a subscription-based service that provides high-fidelity, low-noise and actionable intelligence through API and web-based interaction.

TIA uses data from the deep, dark and surface web, combined with OSINT integration and heuristics, to help security teams investigate suspicious indicators and understand the infrastructure around them.

Benefits

- Improve the efficiency of security teams.
- Strengthen security posture with current threat intelligence.
- Make faster, better-informed threat and risk decisions.
- Reduce false positives and alert fatigue with higher-confidence intelligence.
- Detect and monitor threats targeting the organization and its industry.
- Accelerate incident response with contextual enrichment.
- Streamline collection and analysis through API-based access.

Core Capabilities

High-Fidelity Threat Intelligence

- Curated, context-rich intelligence designed to deliver relevant outcomes with minimal noise.

Observable Enrichment

- Investigate suspicious IP addresses, domains, URLs and other observables with security verdicts and supporting context.

Domain, IP & URL Analysis

- Go beyond reputation with infrastructure, DNS, hosting, technology, vulnerability and relationship analysis.

Domain Analysis: TIA analyzes submitted domains to determine their security verdict, associated applications and category. It examines accessible websites, mapped IP addresses and DNS records, discovers active and inactive subdomains, and identifies potentially deceptive or typosquatted domains.

IP Analysis: TIA analyzes submitted IP addresses to assess their security verdict, associated applications, category and ASN reputation. It identifies hosting and Anycast characteristics, analyzes accessible websites, exposed ports and services, and maps detected software and vulnerabilities to CVE, CPE and CWE classifications while examining associated hostnames.

URL Analysis: TIA analyzes submitted URLs for reputation, categorization and underlying infrastructure, including domains, IPs, ASNs, hosting and cloud services. It examines TLS certificates, network activity, technologies and web content, detects publicly exposed PII, and correlates URLs with related domains, IPs, certificates and infrastructure to provide broader context.

Machine-Readable Integration

- Consume intelligence through simple API request-response workflows and JSON output for security and protection tools.

Automated Blocking

- Feed vetted indicators to firewalls, proxies and EDR/NDR/XDR tools for automated threat blocking.

Incident Response

- Accelerate investigations with high-confidence threat data and contextual enrichment.

Compliance Support

- Support proactive threat mitigation and evidence for regulatory requirements and security programs.

Intelligence Sharing

- Share timely, actionable intelligence across teams and integrate it into existing security infrastructure

Key Advantages

Feature	Value Delivered
Observable Intelligence	Real-time, usable intelligence and contextual enrichment for suspicious observables.
Infrastructure Context	Maps domains, IPs, ASNs, certificates, services, technologies and relationships.
Incident Response	Rich context helps analysts investigate and triage suspicious activity faster.
Actionable Integration	Simple API request-response interaction with JSON output for protection and detection tools.
Threat Prevention	Helps prevent communication with unsafe IP addresses, domains and URLs.
Analyst Efficiency	High-confidence intelligence reduces manual collection, noise and alert fatigue.
Confidentiality	No logging of client requests, supporting confidential intelligence lookups.
Intelligence Coverage	OSINT integration and heuristics support relevant outcomes across a broad range of observables.

About Underscore:

Unlocking Cyber Resilience in the digital realm. Our robust platform combines proactive prediction, powerful forecasting, prioritizing risk, providing unparalleled real-time insights to keep you ahead of threats and assuring business continuity.

Contact Us:

info@underscorecs.com
Tel. +91-9811344253