ThreatBook

ATI

From Advanced Intelligence to Fortified Defense

Executive Summary

In today's evolving digital landscape, Security Operations Centers (SOCs) are overwhelmed by an excessive volume of alerts and challenged by the increasing sophistication of cyber threats. To effectively counter these threats, security teams require more than just raw data; they need advanced, actionable intelligence that can be seamlessly integrated into their defensive workflows.

ThreatBook Advanced Threat Intelligence (ATI) is a comprehensive threat intelligence platform designed to empower your SOC. By transforming high-fidelity global threat data into actionable operational insights, ATI enables security teams to accelerate analysis, prioritize critical threats, and move from a reactive to a proactive security posture. This document outlines the core capabilities, architecture, and practical use cases of the ThreatBook ATI platform, demonstrating how it helps organizations fortify their defenses against modern cyber adversaries.

Key Challenges in Modern Threat Intelligence Operations

Modern Threat Intelligence operations are hampered by several critical pain points that prevent organizations from fully leveraging intelligence for proactive defense. These challenges span the entire intelligence lifecycle, from collection to action.

Inefficient Analysis due to Data Overload

Threat intelligence teams are often overwhelmed by vast amounts of data from open-source and security vendors. The signal-to-noise ratio is extremely low, forcing analysts to spend time sorting through it to find threats that are actually relevant to their own organization. This turns threat hunting into a time-consuming task of just filtering data.

Inaccurate Indicators and Wasted Time on False Positives

Indicators of Compromise (IoCs) can vary in data quality; some may be inaccurate, outdated, or presented without sufficient context. When these low-accuracy indicators are ingested by security tools, they correlate with a higher number of false positives, which impacts resource allocation and leads to analyst alert fatigue.

Lack of Technical Detail for Guiding Defense

A significant portion of threat intelligence reporting is too high-level, focusing on strategic descriptions of threat actors rather than providing a deep, technical breakdown. It often lacks the granular, actionable content—such as specific TTPs (Tactics, Techniques, and Procedures), malware behaviors, or ready-to-use detection rules—that is necessary to directly guide detection engineering and implement effective defensive measures.

Poor Integration and Disjointed Collaboration

A major operational bottleneck is the clunky and often manual workflow for integrating intelligence into security controls. The lack of smooth, automated processes for pushing validated intelligence to tools like SIEMs, SOARs, and firewalls creates a disconnect between the TI team and the SOC team. This friction prevents timely action and hinders effective collaboration.

ThreatBook ATI: A New Paradigm in Threat Intelligence

INTELLIGENCE

- **Accurate** machine-readable indicators
- **Advanced** & proprietary threat reports
- **APAC** perspective with global coverage

OPERATION

- **Accelerate** intelligence Analysis
- **Actionable** insights for detection & response
- **AI** empowered threat investigation

ThreatBook ATI is an Advanced CTI Portal built to bridge the gap between intelligence and operation. It is engineered around six core principles:

Advanced

Delivers exclusive and proprietary intelligence reports from elite threat experts, providing deep-dive analysis on the most sophisticated threats and campaigns.

AI-Empowered

Employs a powerful AI engine to automatically distill insights from massive threat data and to accelerate complex investigations for a faster response.

APAC Perspective

Offers specialized insights with an Asia-Pacific focus while maintaining comprehensive global coverage.

Accurate

Provides high-fidelity, machine-readable indicators with a proven 99.9% accuracy rate.

Actionable

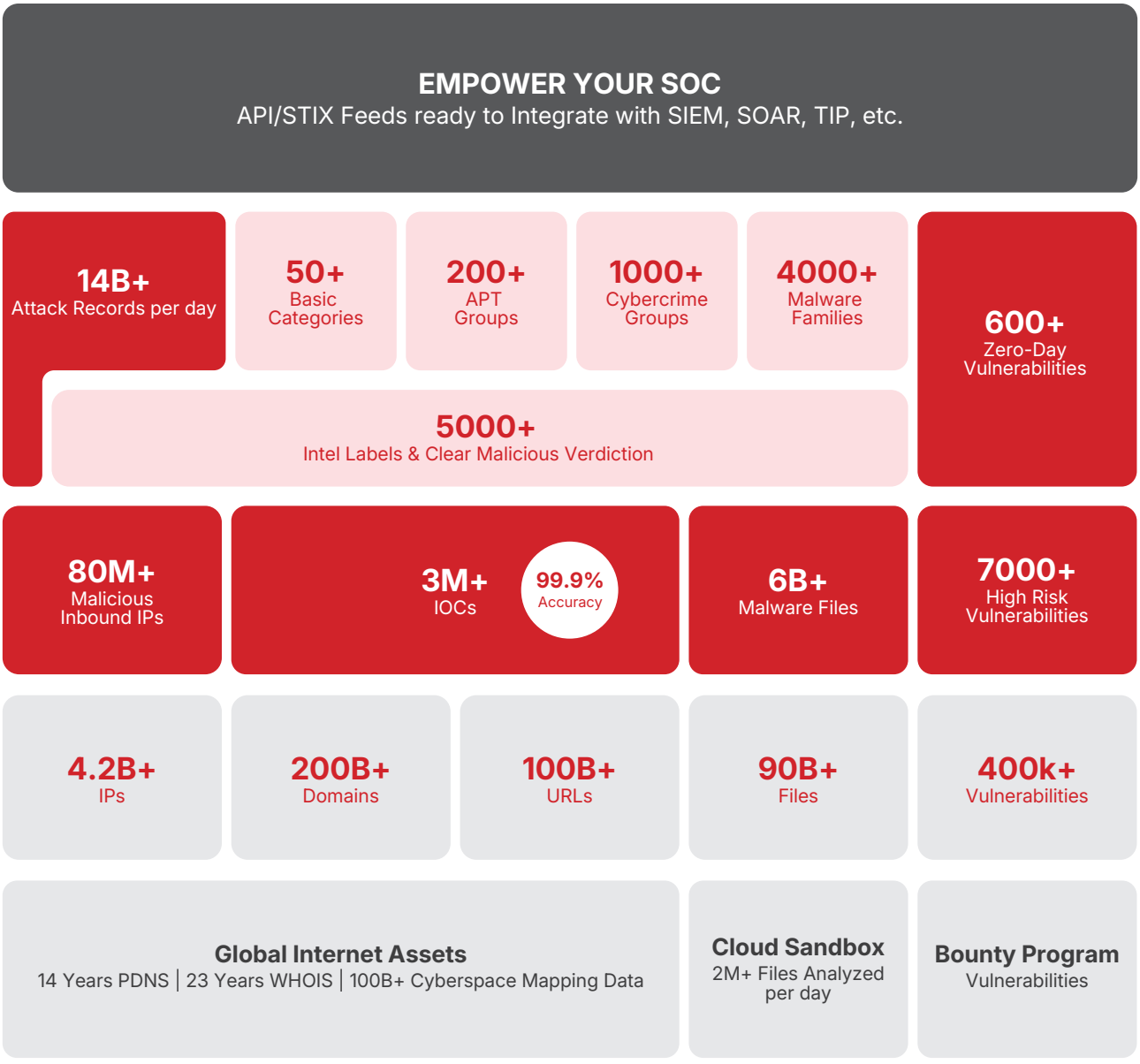
Delivers clear insights and curated detection rules to guide detection and response efforts.

Accelerate

Speeds up the entire intelligence analysis lifecycle, from data collection to operational response.

Comprehensive Data and Intelligence Architecture

ATI's power is derived from its vast and diverse data sources, which are processed into a rich set of intelligence entities.



Data Sources

Global Internet Assets
Including 4.2B+ IPs and 200B+ Domains

Files
90B+ in total , 2M+ analyzed per day

Internet Assets Data
100B+ Entries

Honeypot Collections and Exploit Logs
14B+ adversary behaviours per day

OSINTs
OpenWeb and Darkweb
3000+ Sources

DFIR Cases
First-hand Threat Information

Intelligence Entities

1

Threat Actors
- Profiles of over 200 Advanced Persistent Threat (APT) groups
- Information on more than 1,000 cybercrime groups

2

Indicators of Compromise (IOCs)
- 3M+ Active IOCs of 99.9% Accuracy
- 80M+ Malicious Inbound IPs

3

Malware
- 6B+ Malwares with Yara Rules

4

Vulnerabilities
- Tracking and details for over 400,000 known vulnerabilities
- Identification 7k+ high risk vulnerabilites by proprietary prioritization technology and in-wild exploit intelligence

5

TTPs (Tactics, Techniques, and Procedures)
- Mapping reports to MITRE ATT&CK frameworks
- Enpoint IOA and network rules
- Attack Tools inventory

Platform Features

ATI provides a comprehensive suite of features designed to bridge the gap from raw intelligence to decisive action, accessible via a web portal, mobile app, robust APIs, and integrated data feeds:

Customizable Threat Landscape

Create personalized dashboards and visualizations to monitor the specific threat actors, vulnerabilities, and TTPs most relevant to your organization, industry, or region.

PIRS Monitoring

Define and implement Priority Intelligence Requirements (PIRs) to receive real-time, custom alerts on the specific threats and topics that matter most to you.

Structured Threat Reports

Access structured threat reports with over 50 standard attributions and automatic mapping to the MITRE ATT&CK® framework, providing consistent and easy-to-digest intelligence.

Detailed Threat Actor Profiling

Dive deep into comprehensive profiles of threat actors, detailing their motivations, historical activities, common TTPs, and associated malware and infrastructure.

IOC Analysis

Instantly analyze any IOC (IP, domain, hash, etc.) to get a clear verdict, rich contextual data, and attribution evidence linking it to known threat actors or campaigns.

Technical Details for Detection Engineering

Empower your defense teams with actionable technical details, including curated detection rules (YARA, Sigma, Suricata), network scripts (Zeek), query languages (KQL), and malicious code snippets.

AI-Powered Investigation

Leverage an AI assistant to uncover hidden connections, rapidly analyze massive datasets, and automatically generate tailored investigation reports.

API & Feeds Integration

Seamlessly integrate high-fidelity intelligence into your existing security ecosystem (SIEM, SOAR, TIPs) through robust APIs and customizable data feeds.

Practical Use Cases for the Modern SOC

Use Case 1: SIEM Alert Triage and Noise Reduction

Challenge: SOC teams are inundated with thousands of alerts daily and struggle to prioritize them effectively.
Solution: By integrating ATI's IP Intelligence API, SIEM alerts are automatically enriched with critical context. Analysts can instantly see if an IP is malicious, its threat type, and any links to known threat actors. This allows the team to cross-validate alerts and focus immediately on the most severe threats.

Use Case 2: Automated and Intelligent Response

Challenge: Blocking malicious IPs is essential, but aggressive blocking can inadvertently affect legitimate users, especially when dealing with dynamic IPs from mobile gateways or educational networks.
Solution: Before blocking, ATI's IP intelligence is used to check key attributes. If an IP is identified as dynamic, a mobile base station, a CDN, or a gateway, a more granular blocking policy can be applied—for instance, a temporary block of 10 minutes. This prevents long-term disruption for legitimate users while still mitigating the immediate threat.

Use Case 3: Proactive Compromise Detection

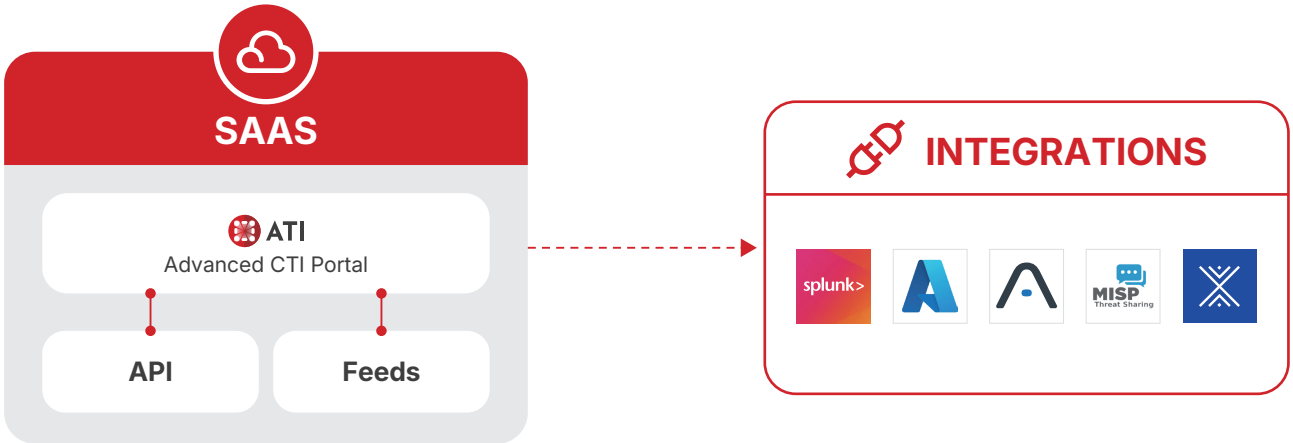
Challenge: A compromised internal host serves as a foothold for attackers to move laterally, escalating a minor incident into a major data breach.
Solution: By feeding DNS logs into the ThreatBook Compromise Detection API, organizations can proactively identify internal hosts communicating with malicious infrastructure. The API detects threats like APT C2 communication, ransomware, and botnet infections, providing actionable intelligence on the associated threat actors and malware families for rapid remediation.

Use Case 4: Advanced Detection Engineering

Challenge: Security teams need effective and up-to-date detection rules to identify new and evolving threats within their environment.
Solution: ATI provides curated, actionable detection rules in formats like Yara, Suricata, and Sigma. This intelligence is prioritized based on real-world threats and vulnerabilities actively being exploited, allowing teams to build a strategic defense plan based on the most relevant risks.

Flexible Integration

ATI provides high-fidelity API and STIX-compliant feeds ready for integration with leading SIEM, SOAR, and TIP solutions. ThreatBook is also available as a premium feed on the Anomali App Store.



ABOUT THREATBOOK

ThreatBook is a leading provider of cyber threat detection and response that driven by TI and AI. We pioneered new approaches to deliver high-fidelity, efficient and actionable security intelligence and integrated the ability with full life cycle threat detection system and incident response capabilities to empower the protection on cloud, network and endpoints, help enterprises achieve high efficiency of responding to threats, reduce complexity and improve security operations.

No.1
Market Share of Threat Intelligence in GCR

The Largest
CTI Community in Asia, Over 300,000 Members

Representative Vendor
Listed in ***Gartner's Market Guide for Security Threat Intelligence Products and Services*** for 4 Consecutive Times

Representative Vendor
Recognized in the ***2025 Gartner Magic Quadrant for Network Detection and Response*** (NDR)

Trusted by Industrial Customers

Banking	Securities & Insurance	Energy	Internet & Telecom	Intelligent Manufacturing	Multi National Companies
BEA	GUOTAI JUNAN SECURITIES	SPIC	airbnb	BMW	BlackRock.
BANK OF COMMUNICATIONS	HAITONG	STATE GRID CORPORATION OF CHINA	bilibili	HONDA The Power of Dreams	CARLYLE
CHINA MERCHANTS BANK	HUATAI SECURITIES	CHN ENERGY	JD.COM	Li Auto	KPMG
ICBC	SSE	China Datang Corporation Ltd.	KUAISHOU	GREE	wilmar
China Construction Bank	SHENZHEN STOCK EXCHANGE	cnooc	ANT GROUP	BOE	HERBALIFE NUTRITION
CHINA EXIM BANK	PING AN	CHINA SOUTHERN POWER GRID	Tencent	oppo	lululemon
AGRICULTURAL BANK OF CHINA	CHINA LIFE	SINOPEC	ByteDance	SAIC	watsons
THE PEOPLE'S BANK OF CHINA	CICC	CNPC	CHINA TELECOM	vivo	ESTĒE LAUDER
BANK OF CHINA	CITIC SECURITIES	ChinaCoal	China Mobile	NIO	Envision digital
					CITIC Group

☆ Awards and Recognitions

Gartner

Magic Quadrant for Network Detection and Response
(2025)

Gartner Peer Insights

A Strong Performer in the Voice of the Customer for Network Detection and Response
(2023, 2024, 2025)

FORRESTER®

The Network Analysis and Visibility Solutions Landscape
(2025)

Gartner

Hype Cycle for Security Operations: CTI Tech Representative Vendor
(2024)

FROST & SULLIVAN

The Growth Index Leader of the Frost Radar™: Threat Intelligence Platforms
(2024)

Gartner

Market Guide for Threat Intelligence Products and Services
(2017, 2019, 2020, 2021)

FORRESTER®

The External Threat Intelligence Service Providers Landscape
(2023)

Gartner

Market Guide for Managed Detection and Response Services, China
(2022, 2024)

FROST & SULLIVAN

No.1 in growth index in the leader quadrant of China Threat Intelligence Market Report
(2022)

"Black Unicorn" Awards
(2021-2023)

Red Herring Top 100 Asia Winner
(2019)

Cybersecurity 500
(2017-2019)

The designated cybersecurity vendor of China International Import Expo (CIIE)
(2018-2024)

The designated cybersecurity vendor of UN Biodiversity Conference COP15
(2020)

Awarded Outstanding Vendor in cybersecurity support of the Beijing Winter Olympics
(2022)

ThreatBook

www.threatbook.io
contactus@threatbook.io

SINGAPORE
12 Marina View #11-01,
Asia Square Tower 2,
Singapore
(018961)

HONG KONG
Units 309 & 311, Level 3,
IT Street, Cyberport 3,
100 Cyberport Road,
Pok Fu Lam, Hong Kong

BEIJING
10th Floor,
JD Technology Building,
No. 76 Zhichun Road,
Haidian District, Beijing

Follow Us on @ThreatBookLabs @Threatbook