Mandiant Advantage Threat Intelligence 情資授權產品說明-中文

Mandiant Advantage 威脅情報授權套件為組織提供各種規模的最新相關網路威脅情報，以便您可以立即關注對您的業務至關重要的威脅並採取行動。現代威脅行為者的堅韌和機智需要安全所有成員的關注和增加的知識團隊。 基於本土漏洞、機器、由 300 多人培養的作戰和對抗情報專家，遍布 23 個國家/地區，涵蓋 30 多種語言，Mandiant 提供 5 個基於用例的訂閱，為組織提供最新更新的威脅情報以執行其安全性更快、更準確地完成任務。

MANDIANT
ADVANTAGE

THREAT INTELLIGENCE SUITE

DATA SHEET

MANDIANT ADVANTAGE

Mandiant Advantage Threat Intelligence Suite provides organizations of all sizes with to-the-minute, relevant cyber threat intelligence so you can focus on the threats that matter to your business now and take action.

The tenacity and resourcefulness of modern threat actors requires attention and increased knowledge from all members of the security teams. Based on a combination of home-grown **breach, machine, operational and adversarial intelligence**, cultivated by more than 300 experts, across 23 countries and covering +30 languages, Mandiant offers 5 use-case based subscriptions providing organisations with **up-to-the-minute updated threat intelligence** to perform their security tasks faster and with more accuracy.

MANDIANT ADVANTAGE

Mandiant Advantage Free

PUBLIC KNOWN THREATS AND VULNERABILITIES CENTRALLY MANAGED

Highlights for Security Professionals overloaded with managing threat intelligence

- **Situational awareness on threat actors and malware on the rise**
- **Centralized repository for public known vulnerability descriptions with CVSS severity scoring**
- **Lookup public known threat Indicators and embed Mandiant's unique threat score directly into any web page with Browser-Plugin**

Centralizing and managing threat intelligence is often rated as one of the most time-consuming tasks for security analysts. Mandiant Advantage Free offers organizations of all sizes, free access to publicly known actors, malware, vulnerabilities. Additionally, Mandiant Advantage Free provides visibility into threats indicators enriched with Mandiant's unique maliciousness score as well as public known vulnerability descriptions with Common Vulnerability Scoring System (CVSS) severity metrics. This all to enable security practitioners to make more informed decisions without spending capital or operational expenditures.

WHAT'S INCLUDED:

- Global dashboards providing actor, malware, vulnerabilities activity trends
- Access to Open Source Indicators with Mandiant maliciousness score
- OSINT based vulnerability views and scoring
- News analysis with Mandiant expert judgements and commentary
- Threat intelligence accessible via portal and browser plugin

MANDIANT ADVANTAGE

Mandiant Advantage Security Operations

INCREASE SOC EFFICIENCY & EFFECTIVENESS

Benefits for Security Analysts, Incident Responders, Security Operations Managers and Intelligence Analysts

- **Alert Prioritization and Triage:** Use up to the minute updated threat intelligence to prioritize and contextualize security event information, reducing alert fatigue and improving overall SOC efficiency
- **Detect Hidden Threats:** Download indicators and expand your detection tools to uncover threat actors or malware activities that could be lingering unseen in your environment
- **Accelerate Response:** Empower security analyst teams with a MITRE ATT&CK based actor behavior insights to understand potential attack progress and help formulate the right response

Security Operations Center (SOC) personnel are under continuous barrage of security events requiring continuous attention and manual, laborious investigations. Mandiant Advantage Threat Intelligence security operations subscription offers security analysts and incident responders with up-to-the-minute actor, malware and vulnerability tracking to help them prioritize alerts and understand the attacker, capabilities and motivations behind their threat events. By correlating SOC generated alerts with Mandiant a well as with open source (OSINT) indicators, security teams get direct guidance during triage, investigation and response improving both speed and security effectiveness while reducing overall alert fatigue. Additionally, Security Operations subscription assists security teams with historical detection of emerging cyber threats by providing detailed actor or malware indicators data, made available via the Mandiant Advantage portal as well as the API.

WHAT'S INCLUDED:

- Mandiant Advantage Free capabilities
- Dynamic actor and malware pivot views with MITRE ATT&CK map, object explorer and indicator downloads
- Access to Mandiant known indicators (IP, Domain, File Hash, URL) with maliciousness scoring metrics
- News analysis with Mandiant expert judgements and commentary
- Quarterly Threat Briefings and basic support (provisioning plus onboarding)
- Threat intelligence accessible via portal, browser plugin and API

MANDIANT ADVANTAGE

Mandiant Advantage Fusion

COMPREHENSIVE THREAT INTELLIGENCE FOR THE ENTIRE SECURITY ORGANIZATION

Benefits

- **Uncover Unknown Risks:** Customizable, scalable access to frontline finished intelligence. Identify global threats, outside of your organization's perimeter, powered by Mandiant's breach intelligence
- **Informed Cyber Defense:** Improve security strategy with a holistic situational awareness of vulnerabilities, threat actors, their activity and potential impact to your business
- **Understand Priorities:** Alleviate alert fatigue with instant access to the specific threats that matter to your organization as and when they occur to help prioritize security activities and effectively prevent attacks
- **Reduce Threat Risks:** Enhance security controls and emulate actor specific tactics during red team exercises

In a bid to continuously understand more about their adversaries, security teams are often looking at mountains of public, often vendor influenced, threat info leading to data overload and reconciling unknown trusted data with internally discovered threat profiles. The Fusion subscription from Mandiant Advantage is the only source of threat intelligence your security team needs, providing full, unlimited access to Mandiant Threat Intelligence, including ongoing, past and predictive threat activity. Fusion gives security teams an unrivalled, strategic view of the threat landscape, one that combines multiple threat facets such as cyber-crime, cyber espionage, strategic intelligence, cyber physical intelligence and intelligence related to adversary operations. Access thousands of FINISHED INTELLIGENCE (FINTEL) reports based on strategic analysis from Mandiant experts, FireEye global telemetry, Mandiant incident response and technical research findings all from one searchable view.

WHAT'S INCLUDED:

- **Mandiant Advantage Free, Security Operations, Vulnerability and Digital Threat Monitoring capabilities**
- **Filter by report types, region, industry, actor or malware name**
- **Finished intelligence reports with full narrative covering strategic to tactical analysis research and context**

MANDIANT ADVANTAGE

Mandiant Advantage Vulnerability (Additional Module)

MAXIMIZE THREAT SURFACE REDUCTION EFFORTS

Benefits for Vulnerability Analysts, IT/System or Data Owners, Risk Managers and Intelligence Analysts

- **Visibility:** Review vulnerability data by technology, actors and exploit source
- **Prioritize:** Analyze data by risk and exploit rating to focus on the vulnerabilities that matter now
- **Notifications:** Get notified of 0-day vulnerabilities
- **Quick Installation:** Integrates with your vulnerability scanners via Browser Plugin or API

Faced with continuous expanding IT infrastructures, new applications and disparate geographical locations, Vulnerability Risk Analysts can feel overwhelmed by the number of vulnerabilities to be addressed in their environment. Analyzing vulnerability information can be a labor-intensive process and even when armed with a simplified vulnerability rating system, it can be hard to know where to start. The Threat Intelligence Vulnerability subscription from Mandiant Advantage allows security risk teams to assess, prioritize and remediate discovered vulnerabilities at enterprise scale by unique scoring mechanism based on ease of exploitation, likelihood of the exploit and perceived threat or impact.

WHAT'S INCLUDED:

- Mandiant Advantage Free capabilities
- Mandiant vulnerability views and scoring including exploit ratings, risk ratings, zero-day assessment and activity observed from our frontline experts
- Comprehensive vulnerability reports including CVE ID's, vulnerable technologies, exploit vectors and relevant reports
- Quarterly Threat Briefings and basic support (provisioning plus onboarding)

MANDIANT ADVANTAGE

Mandiant Advantage Digital Threat Monitoring (Additional Module)

EARLY WARNING ON EXTERNAL THREAT EXPOSURES

Benefits for Intelligence Analysts, Legal Counsel, Public Relations/ Corporate Communications, Executives & Senior Leadership

- **External Threat Visibility:** Identify threats to assets outside of your organization's perimeter, including the Dark Web
- **Simple Setup:** With your search parameters defined, Advantage will continuously monitor multiple forums, social media, paste sites and actor related posts
- **Reliable:** Reduce false positives or negatives with an industry trusted and protected portal
- **Accelerate response:** Prepare response to limit further damage and defend enterprise assets or information

Traditional cyber defenses typically focus on assets or events that exist within your network. But in today's highly connected world, you also need to protect assets that extend beyond your perimeter—such as your organization's brand, identities and partner community. The Digital Threat Monitoring subscription within Mandiant Advantage Threat Intelligence provides early visibility into external threat exposures your assets face with dark web peace of mind monitoring or eliminating impractical high manual effort. Defend against the risks that threaten your brand, infrastructure and high-value partnerships. Identify breaches, exposures and digital threats across the open, deep and dark web using customized keyword search terms. Automate, analyze and generate threat alerts on potentially significant matches.

WHAT'S INCLUDED:

- Mandiant Advantage Free capabilities
- Customized keyword-driven research tools for tailored, scalable reconnaissance and dark web monitoring
- Access to Mandiant Analyst for investigation support and expertise
- Threat alerts via the Alerts Dashboard including the status, source, severity attributes and insights to help manage your monitored assets.
- Quarterly Threat Briefings and basic support (provisioning plus onboarding)

THE MANDIANT ADVANTAGE THREAT INTELLIGENCE PORTFOLIO

	FREE	SECURITY OPERATIONS	FUSION
ACCESS TYPES			
Mandiant Advantage Platform and Browser Plug-in	●	●	●
API		●	●
DATA ACCESS			
Indicators - Open Source - with Mandiant Scoring	●	●	●
Threat Actors - Open Source and Publicly Known	●	●	●
Malware and Malware Families - Open Source	●	●	●
Real Time Dashboards - Actor, Malware, and Vulnerability	●	●	●
Indicators - Mandiant Proprietary - with Scoring and Context		●	●
Threat Actors - Mandiant Proprietary - UNC, Temp, APT, FIN		●	●
Malware and Malware Families - Mandiant Proprietary		●	●
Live Actor & Malware Pivot Views - MITRE ATT&CK and Graph		●	●
VULNERABILITY			
Public / Known Vulnerability Descriptions	●	●	●
Mandiant Risk and Exploit Rating	+ VULNERABILITY MODULE		●
Mandiant Vulnerability Analysis	+ VULNERABILITY MODULE		●
DIGITAL THREAT MONITORING (DTM)			
Dark Web Monitoring	+ DIGITAL THREAT MONITORING		●
Research Tools and Alerting	+ DIGITAL THREAT MONITORING		●
ANALYSIS & ADVERSARY INTELLIGENCE			
News Analysis	●	●	●
Quarterly Intelligence Threat Briefing		●	●
Strategic Reporting - Region, Industry, Trends			●
Adversary Motivations, Methods, Tools, and Behaviors Reporting			●
Threat Activity Alerts, Emerging Threats, and Trend Reporting			●
Mandiant Research Reporting			●

Vulnerability and Digital Threat Monitoring can be purchased independently.

Learn how Mandiant Advantage delivers the most comprehensive cyber threat intelligence on the market, visit **www.fireeye.com/advantage**

MANDIANT ADVANTAGE

The cyber landscape continues to grow in complexity as adversaries become increasingly more sophisticated and rapidly morph their tactics. To proactively reduce business risk from motivated attackers, organizations need continuous validation technology powered by timely and relevant intelligence. Mandiant, a part of FireEye, brings together the world's leading Threat Intelligence and front-line incident response data with its continuous security validation platform to arm organizations with the tools needed to increase security effectiveness and reduce organizational risk, regardless of the technology deployed.

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6500/877.FIREEYE (347.3393)
info@FireEye.com

M-EXT-DS-US-EN-000350-01