MANDIANT ADVANTAGE

DHS SHARED CYBERSECURITY SERVICES

DATA SHEET

U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency (CISA), extended a subscription to Mandiant Threat Intelligence (Mandiant). The initial subscription began in 2010.

- Subscription base period, 15 November 2020 - 14 May 2021
- Option Period 1, 15 May 2021 - 14 August 2021
- Option Period 2, 15 August 2021 - 14 November

All Federal Civilian Agencies (FCAs), State Fusion Centers, and the Multi-State-Information Sharing Analysis Center (MS-ISAC) are licensed to receive a Fusion subscription under this contract.

MANDIANT INTELLIGENCE OVERVIEW

Mandiant delivers comprehensive, non-classified, actionable intelligence to help organizations proactively defend against new and emerging cyber threats and align an organization's security program with its risk management goals. Mandiant is tailored to an organization's security mission and staff and provides both mature and growing security teams critical context on attacker intent and activity.

Mandiant is unique in the industry. More than 230 experts, across 23 countries and covering +30 languages, apply our rigorous intelligence standards to collect, process, analyze and disseminate forward-looking, adversary-focused intelligence.

Mandiant has an unmatched view into adversaries, victims, and global networks and delivers visibility across the extended cyberattack lifecycle to all levels of an organization's business.

Madiant Advantage Fusion

COMPREHENSIVE THREAT INTELLIGENCE FOR THE ENTIRE SECURITY ORGANIZATION

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
- **Lookup public known threat Indicators** and embed Mandiant's unique threat score directly into any web page with Browser-Plugin
- **Finished intelligence reports** with full narrative covering strategic to tactical analysis.

Centralizing and managing threat intelligence is often rated as one of the most time-consuming tasks for security analysts. The DHS Mandiant Advantage 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 and open source (OSINT) indicators ingested by API, security teams get direct guidance during triage, investigation, and response improving both speed and security effectiveness while reducing overall alert fatigue.

The Fusion subscription from Mandiant Advantage provides full, unlimited access to Mandiant Threat Intelligence, including ongoing, past, and predictive threat activity. 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 on the Mandiant Advantage portal.

WHAT'S INCLUDED:

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

MANDIANT ADVANTAGE

Madiant Advantage Vulnerability

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 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

MANDIANT ADVANTAGE

Madiant Advantage Digital Threat Monitoring

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:

- 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.

FAQ

Q: Who can I contact to request enablement training for my staff/organization?

A: Please send the request to fedinfo@fireeye.com or directly contact Aaron.Abramowitz@mandiant.com and Aviv.Benor@mandiant.com

Q: Who can I contact if I have a technical or analytical intelligence question and/or would like further information on a Mandiant report?

A: This is considered an Analyst Access request and should be sent to analystaccess@fireeye.com.

Q: How can I submit IPs, domains and/or malware for analysis?

A: Query IPs and domains directly within Mandiant Advantage. Submit malware within the "Tools" tab of the legacy FireEye Intelligence Portal (available via the top right hand app switcher) or for additional analysis, open an Analyst Access request via analystaccess@fireeye.com.

Q: To which FireEye subscription(s) does each organization have entitlement?

A: FCAs, State Fusion Centers, and MS-ISAC have access to Mandiant Fusion subscription.

Q: What is the scope of the Mandiant license within the FCAs?

A: The license provides Mandiant access to employees and contractors serving at Federal Legislative, Judicial and Executive organizations, including the Independent Agencies under the Executive branch, as well as State Fusion Centers, and MS-ISAC; however, the license does not include access to employees of the U.S. Department of Defense nor the Intelligence Community.

Q: With whom can I share FireEye Intelligence?

A: Any authorized FCA user may access and share Mandiant information within their organization and with other FCA covered under the same subscription. The license does not include re-distribution rights, in any form, outside of the licensed organization. Standard limitations are further described at https://www.fireeye.com/company/legal.

Q: Where can I provide feedback to DHS CISA.

A: Feedback on this program can be directed to cisa.ctis.scs_info@cisa.dhs.gov.

THE MANDIANT ADVANTAGE THREAT INTELLIGENCE PORTFOLIO

	DHS Subscription
	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	●
Mandiant Vulnerability Analysis	●
DIGITAL THREAT MONITORING (DTM)	
Dark Web Monitoring	●
Research Tools and Alerting	●
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	●

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