Mandiant

MANDIANT ADVANTAGE THREAT INTELLIGENCE BROWSER PLUG-IN

The Mandiant Advantage Threat Intelligence (MATI) Browser Plugin streamlines threat research and investigation efforts by integrating Mandiant Threat Intelligence directly into your browser. The plugin automatically scans the web page that you're browsing and tags any mention of known Threat Intel entities, including the following:

- Indicators
  - IPv4 addresses
  - Domains
  - URLs
  - File Hashes
- Actors
- Campaigns
- Malware
- Vulnerabilities (Common Vulnerabilities and Exposures, or CVEs)

The MATI Browser Plugin includes features and capabilities specific to each supported browser.

Chrome

- Tap into instant ratings for millions of indicators from open source feeds, using over 225,000 hours per year of Mandiant Incident Response engagements.
- Quickly and easily overlay Threat Intelligence to prioritize the investigation of suspicious indicators in your logs, tools, and systems.
- Pivot directly into Mandiant Advantage from the browser plugin to gather more contextual information on attributed actors and malware families.
- Integrate and share threat insights with your teams and workflows for collaboration, investigation, and remediation.
- Highlights web page elements that may be associated with vulnerability data, such as matching Common Vulnerabilities and Exposures (CVEs) or designated keywords.
- Overlay threat information directly with **Google Security Operations** **(https://cloud.google.com/solutions/security-information-event-management)**.
- Authenticate less frequently, including support for Federated Authentication.
  - All Mandiant Advantage subscribers have access to the MATI Browser Plugin using the same credentials as those used for the Mandiant Advantage platform.

    The server *auth.mandiant.com* must be added to any firewall or proxy allowlists to enable authentication.

  - Mandiant Advantage subscribers that use federated authentication can access the MATI Browser Plugin using their federated credentials. For more information, see **Federated Access** **(https://docs.mandiant.com/home/ma-federated-access)**.

    Federated Authentication is currently in Public Preview and is not supported in previous versions of the MATI Browser Plugin. You must upgrade to the latest version to use federated authentication with the Chrome browser extension.

Edge

- Tap into instant ratings for millions of indicators from open source feeds, using over 225,000 hours per year of Mandiant Incident Response engagements.
- Quickly and easily overlay Threat Intelligence to prioritize the investigation of suspicious indicators in your logs,

tools, and systems.

- Pivot directly into Mandiant Advantage from the browser plugin to gather more contextual information on attributed actors and malware families.
- Integrate and share threat insights with your teams and workflows for collaboration, investigation, and remediation.
- View highlighted web page elements that may be associated with vulnerability data, such as matching Common Vulnerabilities and Exposures (CVEs) or designated keywords.
- Overlay threat information directly with **Google Security Operations** (https://cloud.google.com/solutions/security-information-event-management).
- Authenticate less frequently, including support for Federated Authentication.
    - All Mandiant Advantage subscribers have access to the MATI Browser Plugin using the same credentials as those used for the Mandiant Advantage platform.

      The server *auth.mandiant.com* must be added to any firewall or proxy allowlists to enable authentication.

    - Mandiant Advantage subscribers that use federated authentication can access the MATI Browser Plugin using their federated credentials. For more information, see **Federated Access** (https://docs.mandiant.com/home/ma-federated-access).

      Federated Authentication is currently in Public Preview and is not supported in previous versions of the MATI Browser Plugin. You must upgrade to the latest version to use federated authentication with the Chrome browser extension.

Firefox

- Tap into instant ratings for millions of indicators from open source feeds, using over 225,000 hours per year of Mandiant Incident Response engagements.
- Quickly and easily overlay Threat Intelligence to prioritize the investigation of suspicious indicators in your logs, tools, and systems.
- Pivot directly into Mandiant Advantage from the browser plugin to gather more contextual information on attributed actors and malware families.
- Integrate and share threat insights with your teams and workflows for collaboration, investigation, and remediation.
- View highlighted web page elements that may be associated with vulnerability data, such as matching Common Vulnerabilities and Exposures (CVEs) or designated keywords.
- Overlay threat information directly with **Google Security Operations** (https://cloud.google.com/solutions/security-information-event-management).
- Authenticate less frequently, including support for Federated Authentication.
    - All Mandiant Advantage subscribers have access to the MATI Browser Plugin using the same credentials as those used for the Mandiant Advantage platform.

      The server *auth.mandiant.com* must be added to any firewall or proxy allowlists to enable authentication.

    - Mandiant Advantage subscribers that use federated authentication can access the MATI Browser Plugin using their federated credentials. For more information, see **Federated Access** (https://docs.mandiant.com/home/ma-federated-access).

      Federated Authentication is currently in Public Preview and is not supported in previous versions of the MATI Browser Plugin. You must upgrade to the latest version to use federated authentication with the Chrome browser extension.

Videos

There are two additional Browser Plugin videos:

- **MATI Browser Plugin Onboarding** (https://docs.mandiant.com/home/onboarding-mati-browser-plugin-overview)
- **Using the Browser Plugin with Splunk** (https://docs.mandiant.com/home/how-to-use-mandiant-advantage-browser-plugin-with-splunk)
  This video is for version 1.0 of the plugin so is not 100% up-to-date

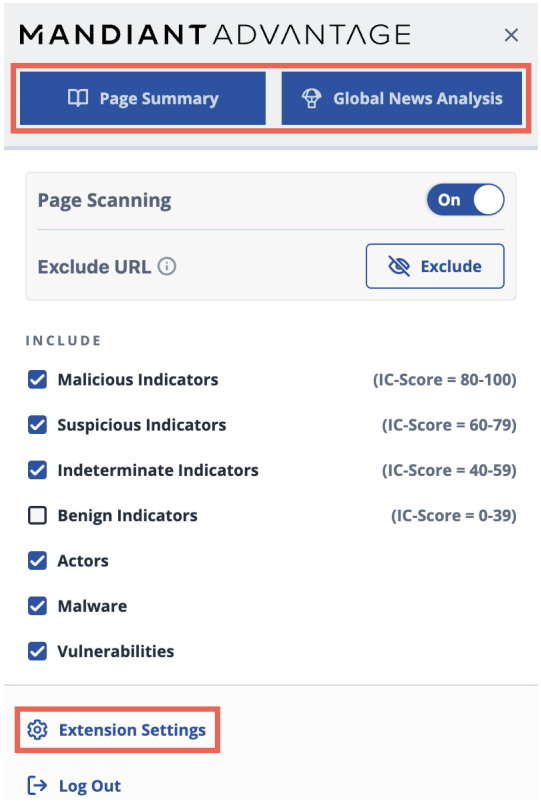
Download and install

Download and add the latest MATI Extension to your browser. If the available features don't match what you are seeing, go to the Browser's plugin page & verify you have the latest version.

- **Chrome** (https://chrome.google.com/webstore/detail/mandiant-advantage-threat/aghmgfkjfbkcockededacdhemkpgdcko)
- **Firefox** (https://addons.mozilla.org/en-US/firefox/addon/mandiant-advantage/)
- **Edge** (https://microsoftedge.microsoft.com/addons/detail/mandiant-advantage-thre/bbbhekpifeagoagebiifoieodkckkfcl)

Configure the plugin

1. Once installed, click the Threat Intelligence extension to authenticate with your Mandiant Advantage platform credentials.
2. Select the Threat Intelligence extension again to configure what Threat Intelligence artifacts you want to highlight on your web browser page.
3. (Optional) Click **Page Summary** to display the ongoing results of the scan as you scroll.
4. (Optional) Click **Global News Analysis** to view our latest article analysis.
5. (Optional) Click **Extension Settings** to configure webhooks to share content directly in your organization's chat client (Teams, Slack, or Google Chat).

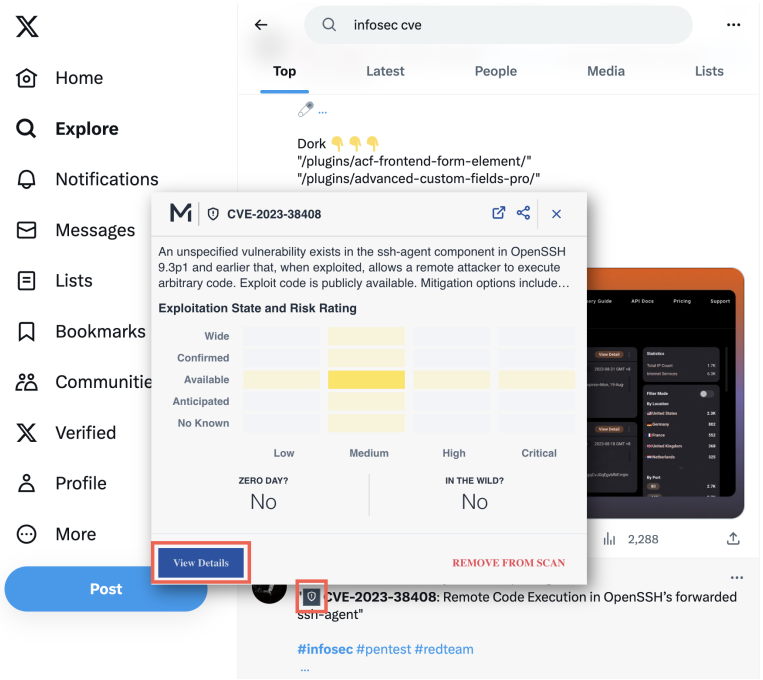


Use Case Scenarios

The following use cases provide exemplary persona-based workflows for using the MATI Browser Plugin.

Use Case Scenarios for a CTI Analyst

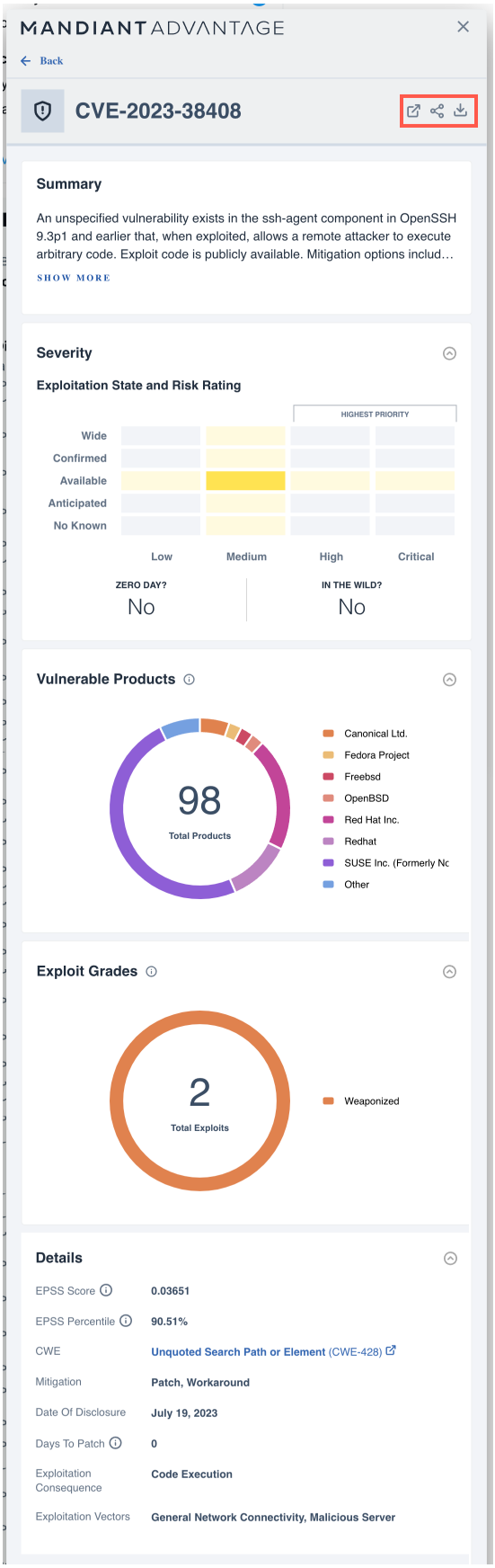
- **Review tweets**
  While browsing an InfoSec Twitter thread with Threat Intelligence extension configured to include **Vulnerabilities**, you can quickly get details of a Vulnerability (CVE).



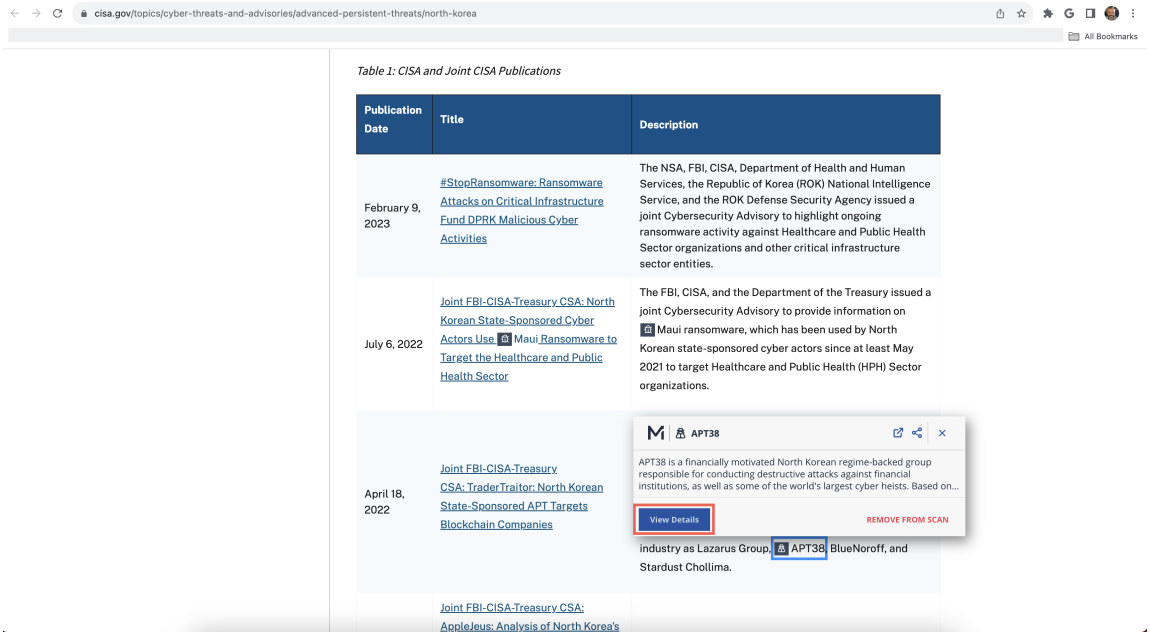
  - Click **View Details** to display observed threat intelligence related to the Vulnerability.

    > The widgets displayed are dynamically populated based on live data in the Mandiant Advantage platform. If no supporting data is available, the associated widget will be hidden from the View Details modal.

  - Click the respective icons to perform the following actions:
    - **View in Mandiant Advantage**: Pivot directly to the Mandiant Advantage platform to interact directly with the complete Vulnerability profile.
    - **Share**: Pivot directly to your organization's chat client to place a link to the Mandiant Advantage platform for the Vulnerability.
    - **Download CSV**: Download a CSV containing the details of the Vulnerability, including the following headers:
      - Name
      - Summary
      - Exploitation State
      - Risk Rating
      - Exploited in the Wild
      - Exploited as Zero-Day
      - Actors Associations
      - Malware Associations
      - CVSS Ratings
      - Relevant Reporting



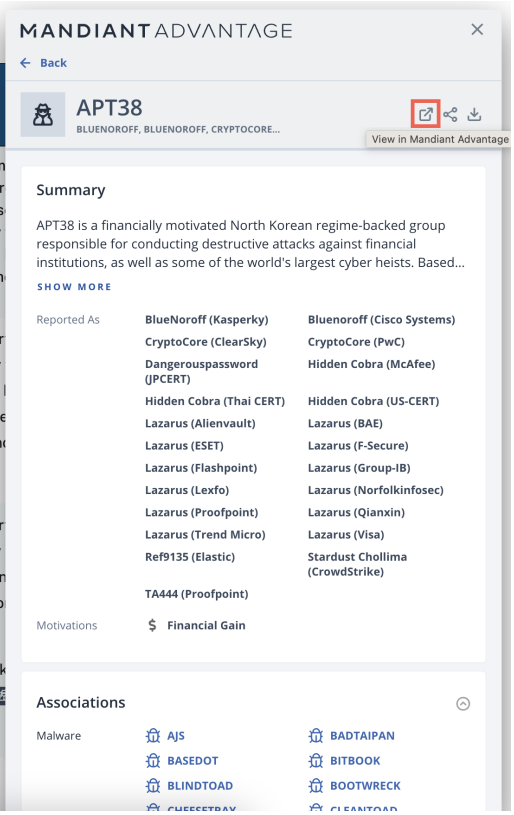
- **Explore Threat Actor details from a threat report**
  - While browsing a threat report, you can quickly get details of a Threat Actor and pivot directly into Mandiant Advantage.



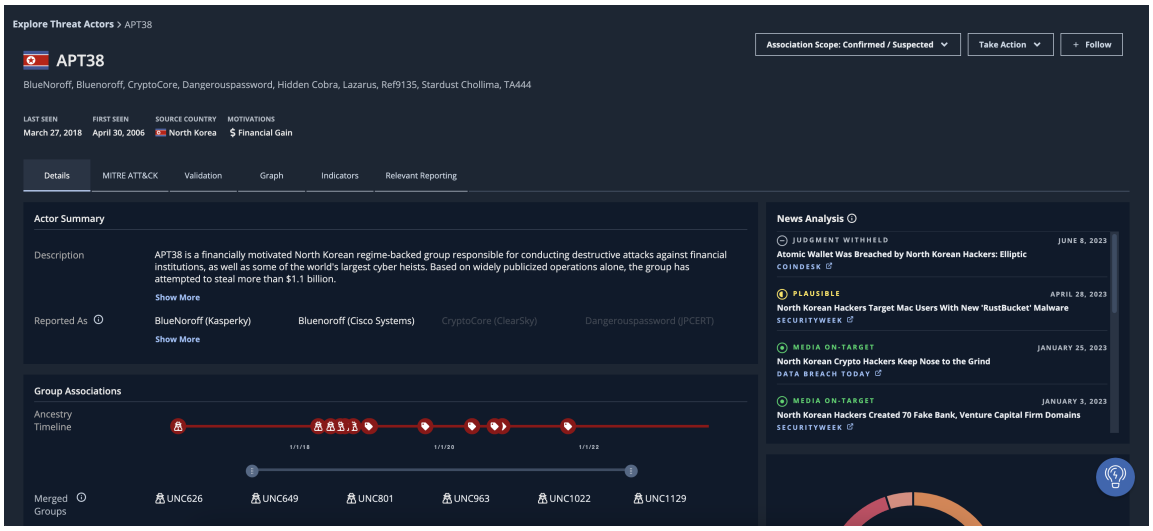
  - Click **View Details** to display observed threat intelligence related to the Threat Actor.

Table 1: CISA and Joint CISA Publications

Publication Date	Title	Description
February 9, 2023	#StopRansomware: Ransomware Attacks on Critical Infrastructure Fund DPRK Malicious Cyber Activities	The NSA, FBI, CISA, Departm Services, the Republic of Kor Service, and the ROK Defens joint Cybersecurity Advisory ransomware activity against Sector organizations and oth sector entities.
July 6, 2022	Joint FBI-CISA-Treasury CSA: North Korean State-Sponsored Cyber Actors Use Maui Ransomware to Target the Healthcare and Public Health Sector	The FBI, CISA, and the Depar joint Cybersecurity Advisory Maui ransomware, which Korean state-sponsored cybe 2021 to target Healthcare an organizations.
April 18, 2022	Joint FBI-CISA-Treasury CSA: TraderTraitor: North Korean State-Sponsored APT Targets Blockchain Companies	The FBI, CISA, and the Depar joint Cybersecurity Advisory associated with cryptocurren a North Korean state-sponso threat. This group is commonly track industry as Lazarus Group, Stardust Chollima.
	Joint FBI-CISA-Treasury CSA: AppleJeus: Analysis of North Korea's	

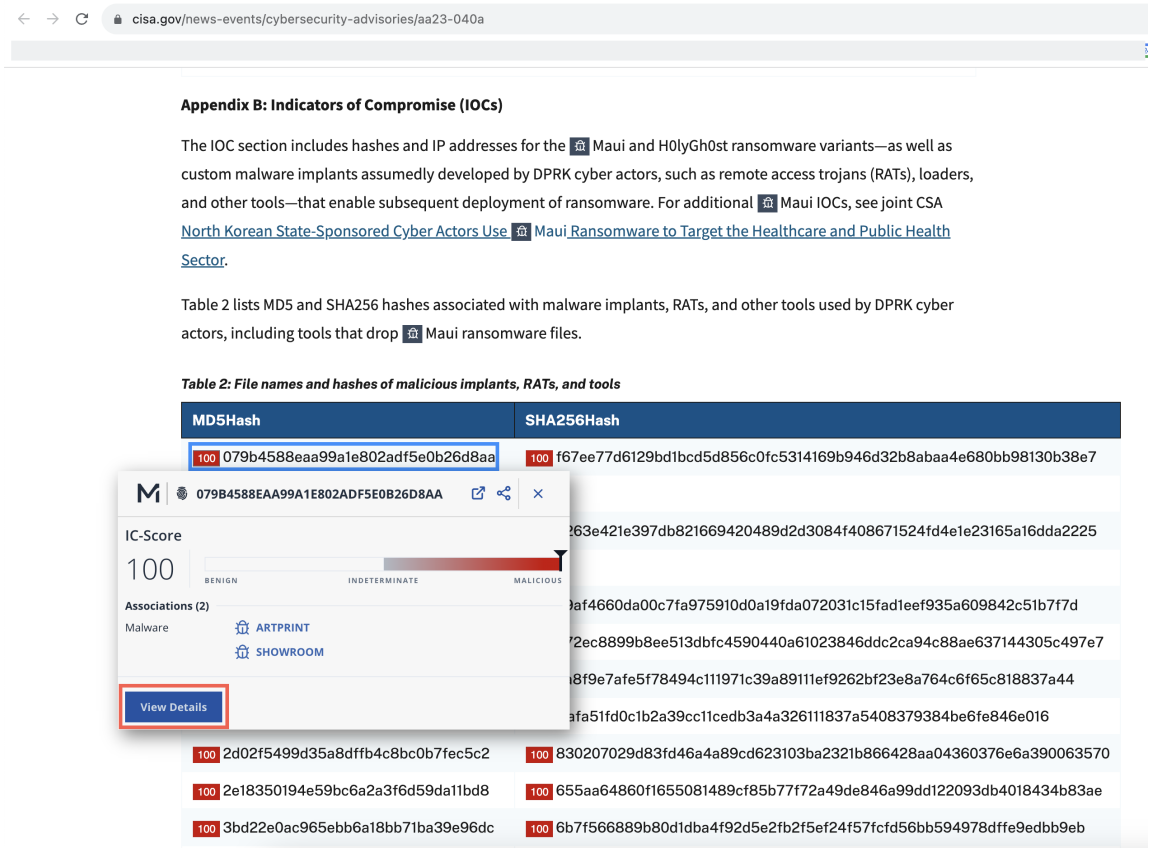


- Click the **View in Mandiant Advantage** icon to pivot directly to the Threat Actor profile in the Mandiant Advantage platform.

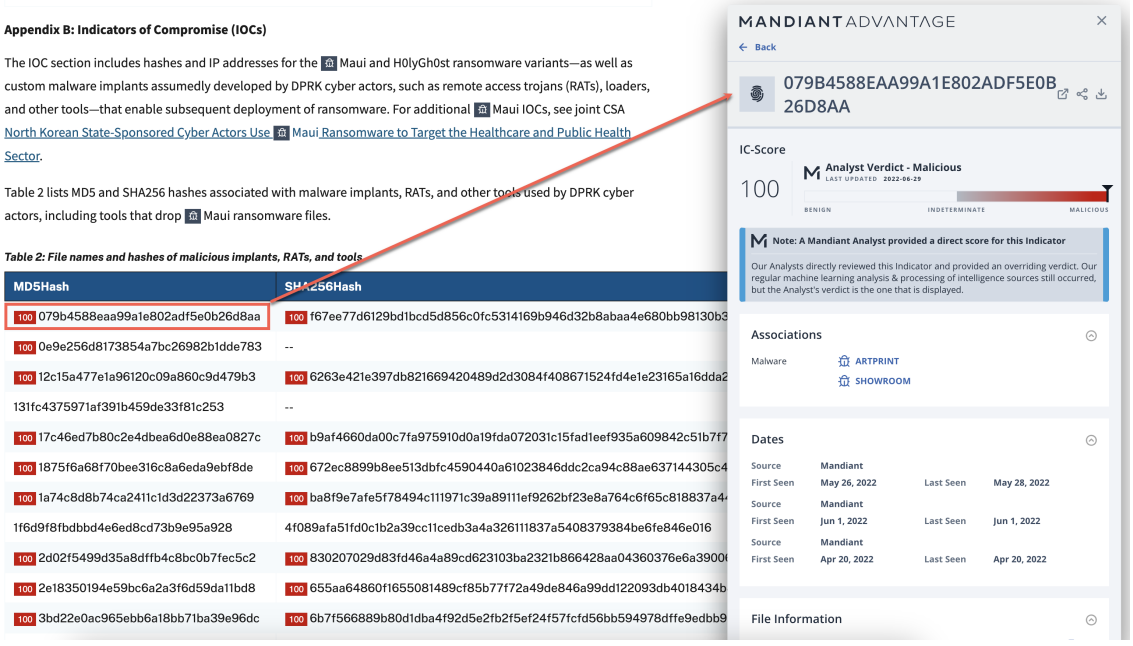


- **Get details of a file hash Indicator from a security advisory**
  - While browsing a threat report, you can quickly get details of an Indicator such as a file hash.

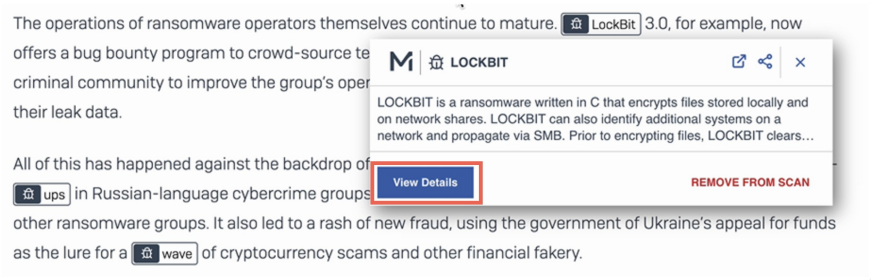
> The Indicator Confidence Score (IC-Score) is displayed for Indicators that have been reviewed by Mandiant. IC-Score is a measure of the degree of confidence that an Indicator is malicious, but not a measure of severity. For more information, see **Understanding IC-Score (https://docs.mandiant.com/home/understanding-ic-score)** and **Indicator Threat Score and Confidence Score Source Descriptions (https://docs.mandiant.com/home/mati-ic-score-source-descriptions)**.



- Click **View Details** to display observed threat intelligence related to the associated file.



- **Reading or Perusing a Blog Post**
  - While browsing a cybersecurity blog, you can quickly get details of a ransomware. Again, click **View Details** for more detailed information, including a link to the ransomware in Mandiant Advantage.

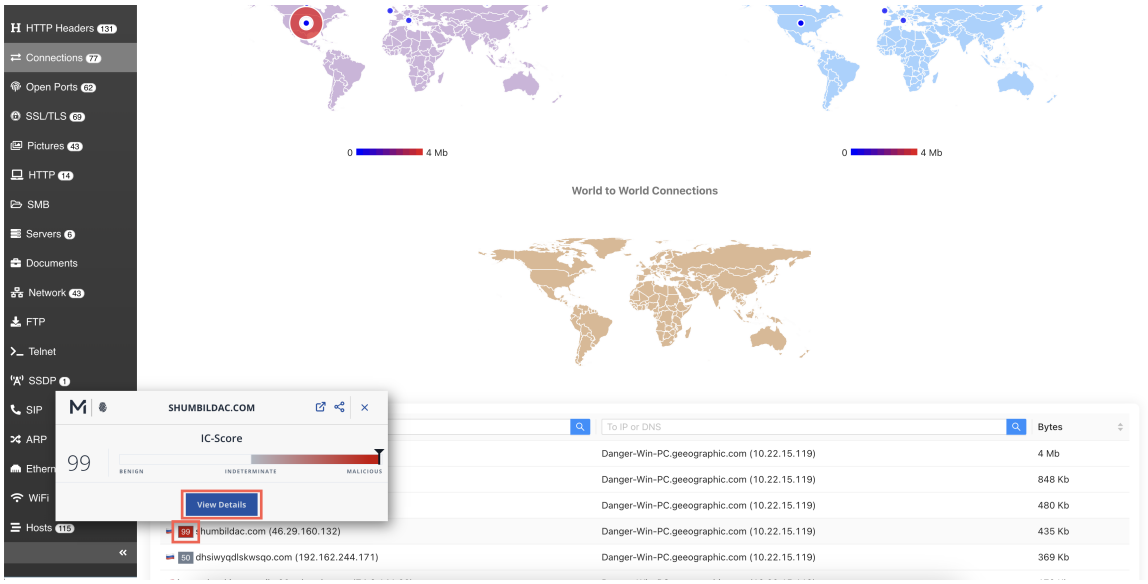


Use Case Scenarios for a SOC Analyst

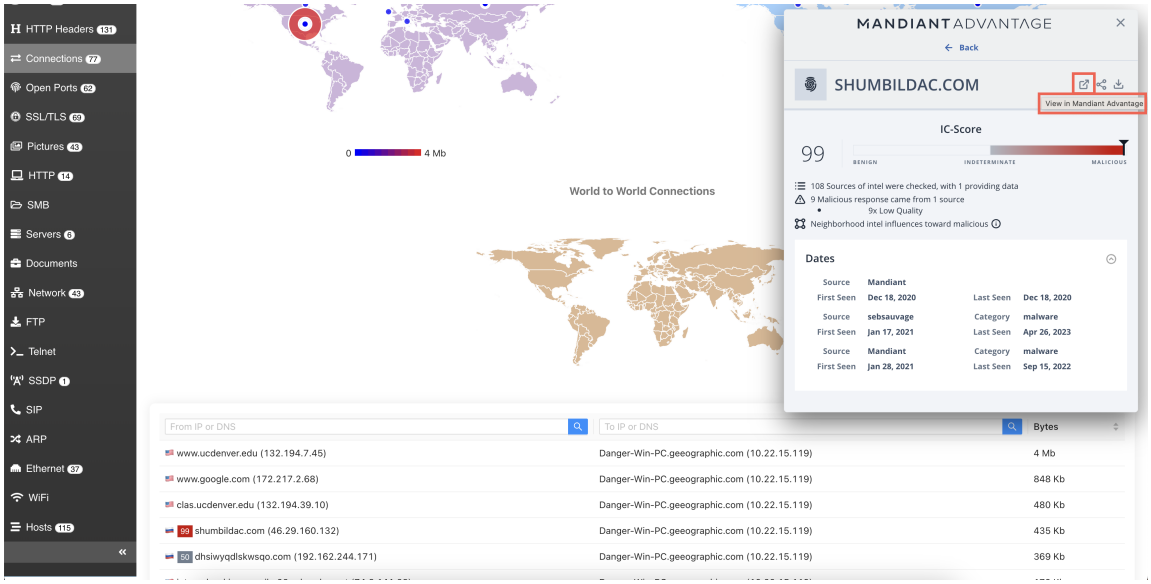
- **Triage and prioritize alerts in your SOC**
  Since many SIEMs and other security tools are browser-based, the MATI Browser Plugin can help you prioritize response efforts at a glance. Because the IC-Score is displayed for each highlighted Indicator in your view, you can focus on those Indicators that are known to be malicious.

  > For more information about how IC-Scores are generated, see **IC-Score Source Descriptions (https://docs.mandiant.com/home/mati-ic-score-source-descriptions)**.

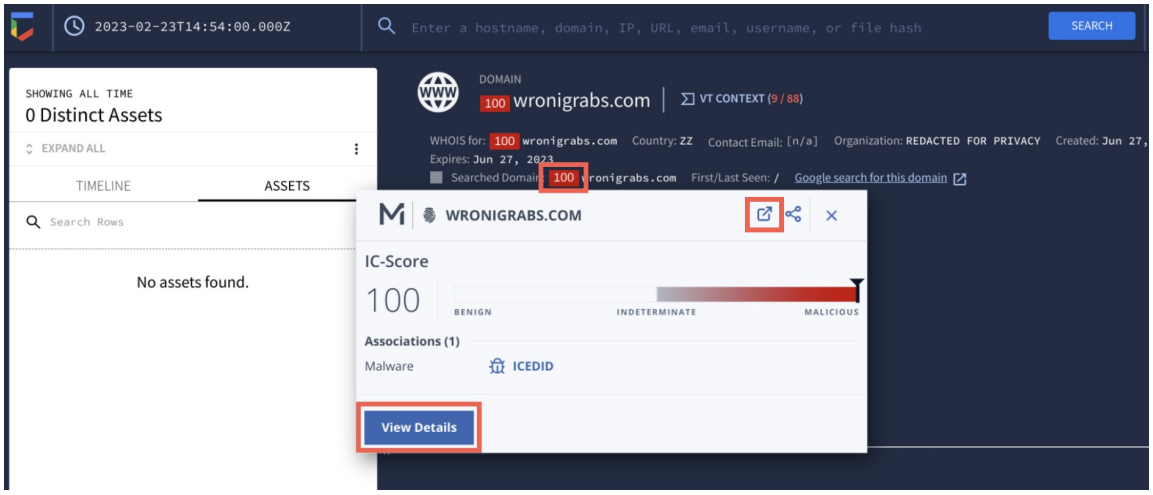
- **Investigate an uploaded PCAP file or firewall logs**
  The MATI Browser Plugin applies critical context to packet capture (PCAP) files or firewall logs viewed in a web-based application.
  - Click the highlighted IC-Score for more information about the associated Indicator. Click **View Details** to display observed threat intelligence related to the Indicator.



  - Pivot directly into Mandiant Advantage by clicking **View in Mandiant Advantage.**



- **Domain Search in Google SecOps**
  A search in Google Security Operations (SecOps) for suspicious domains provides the same pivot points to Mandiant Advantage.
  - Click the highlighted IC-Score for more information about the associated domain. Click **View Details** to display observed threat intelligence related to the domain.



  - Pivot directly into Mandiant Advantage by clicking **View in Mandiant Advantage.**