Mandiant

ASM MANDIANT ADVANTAGE THREAT INTELLIGENCE INTEGRATION

Mandiant Advantage Threat Intelligence (MATI) is directly applied to your attack surface. As a result, customers that have both Mandiant Advantage Attack Surface Management (MA-ASM) and MATI can identify the assets most likely to be exploited and the associated risk for faster remediation and improved prioritization.

Benefits

Based on your MATI subscription, you have access to different levels of integration with the MATI data:

- Intelligence gathered from the frontlines of incident response, managed services, and adversary research is used to create active checks featured in the Issue Library.
- All Paid and Freemium users receive Medium Severity Issues when an asset matches a Mandiant Indicator of Compromise (IOC), indicating potential suspicious activity.
- Threat Intelligence Fusion customers and Threat Intelligence Security Operations customers with the Vulnerability Module add-on can quickly assess the impact of CVEs directly from MA-ASM.
    - High Severity **Issues** (https://docs.mandiant.com/home/asm-issues) (suspicious activity detected on the **Entity** (https://docs.mandiant.com/home/asm-entities)): An asset in your attack surface matches an IOC monitored by Mandiant and has an IC-Score > 80.
    - Issues associated with CVEs include direct links to Vulnerability Reports.
    - Inferred CVEs include direct links to Vulnerability Reports.

The IC-Score, or Mandiant Indicator Confidence Score, is produced by machine learning algorithms to convey a confidence in an Indicator being benign or malicious. 0 is considered *high-confidence benign*, and 100 is *high-confidence malicious*. IC-Score is the Mandiant confidence rating. 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) for more information.

Visit the **Threat Intelligence Subscriptions** (https://docs.mandiant.com/home/mati-subscriptions) page for more information on what's included in each Mandiant Threat Intelligence subscription.

Pivot Points Available Based on Threat Intelligence Subscription

Intelligence Available within MA-ASM	MA-ASM & Threat Intelligence Freemium	Threat Intelligence Security Operations	Threat Intelligence Fusion
	Included with subscription		
Issue Creation from Entity IC-Score greater than 80	✔	✔	✔
Entities IC-Score (If Applicable)*	Available to customers with the **Vulnerability Module** add-on.		✔
Inferred CVEs Linked to Threat Intelligence			✔
Issues with CVEs Linked to Threat Intelligence			✔

* MA-ASM Freemium users see Entities with IC-Scores; however, no pivot points are available.

How MA-ASM defines Issue Severity for CVEs

MA-ASM provides severity-based scoring on Issues, aligned to NIST NVD, CISA's Known Exploited Vulnerability catalog and

Mandiant Vulnerability Intelligence. Additionally, Issue details include vulnerability and asset risk scores taken from Mandiant Threat Intelligence. Some example factors associated with Issue severity include:

- Mandiant Vulnerability Risk Rating
- Common Vulnerability Severity Score (CVSS) v3
- Exploit Prediction Scoring System (EPSS) Score
- Exploitation Status
- Existence of an exploit proof of concept (POC)

On the **<> Raw (JSON)** tab for any given Issue, use your web browser search feature to search for `mandiant_intel_details`. This search brings you to MATI related data associated with the Issue.

```
"mandiant_intel_details": {
    "id": "vulnerability--ab4165e8-b386-5413-8eaf-0d3edced7974",
    "epss": {
        "score": 0.97534,
        "percentile": 0.99982
    },
    "cve_id": "CVE-2019-9670",
    "risk_rating": "MEDIUM",
    "exploitation_state": "Confirmed",
    "cisa_known_exploited": {
        "due_date": "2022-07-10T00:00:00.000Z",
        "added_date": "2022-01-10T00:00:00.000Z"
    },
```

Create Issues from Inferred CVEs

MA-ASM pulls in CVE details from Vulnerability Intelligence and can be configured to create Issues from Inferred CVEs. To create Issues from Inferred CVEs, follow these steps:

1. In MA-ASM, navigate to **Collections >** ⚙ **Settings**.
2. Click ⚙ **Settings** associated with a Collection. The **Issue Settings** tab opens.
3. Click the **Inferred CVEs** toggle to the on position.

   If the **Inferred CVEs as Issues** option is not enabled, Inferred CVEs are only on the Entity.

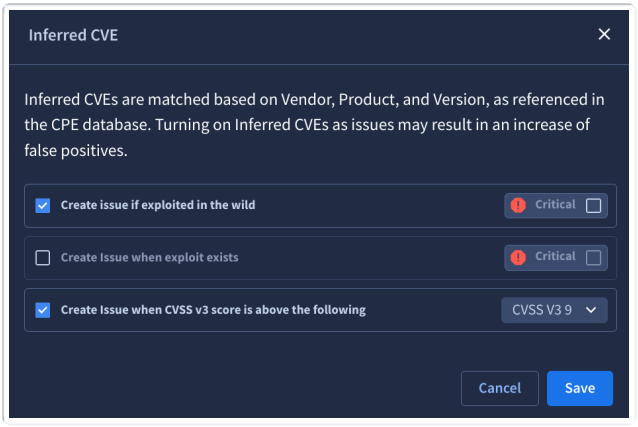
4. Click ⚙ **Settings** to configure the options that you want to use to create Issues:
   - **Create Issue if exploited in the wild**: Exploitation has been observed in the wild.
     - Optional: Assign **Critical** severity to these Issues
   - **Create Issue when exploit exists**: Exploit or POC code is publicly available or underground discussions, alleged selling, or alleged privately held code is observed.
     - Optional: Assign **Critical** severity to these Issues
   - **Create Issue when CVSS v3 score is above the following**: Choose a minimum score threshold at which to generate Issues.

Issue severity is based on the CVSS ranges from **NIST NVD** (https://nvd.nist.gov/vuln-metrics/cvss).

Issue Severity Based on CVSS v3 Score	
Severity	**Ranges**
Critical	9.0 - 10.0
High	7.0 - 8.9
Medium	4.0 - 6.9
Low	0.1 - 3.9
None (Informational)	0.0

For more detailed information, see **ASM Issue Severity Definitions and Examples** (https://docs.mandiant.com/home/asm-issue-severity-definitions-and-examples).

5. Click **Save**.

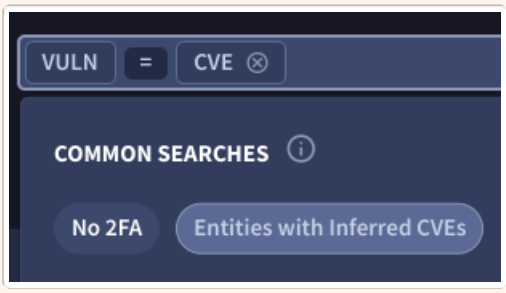


- Setting Inferred CVEs as Issues to off prevents new Inferred CVE Issues from being created. Existing Issues initially generated by Inferred CVEs continue to show up on the Issues page as Inactive Issues.
- When toggling this feature **Off**, you must then **Scan Collection** for these changes to take effect.

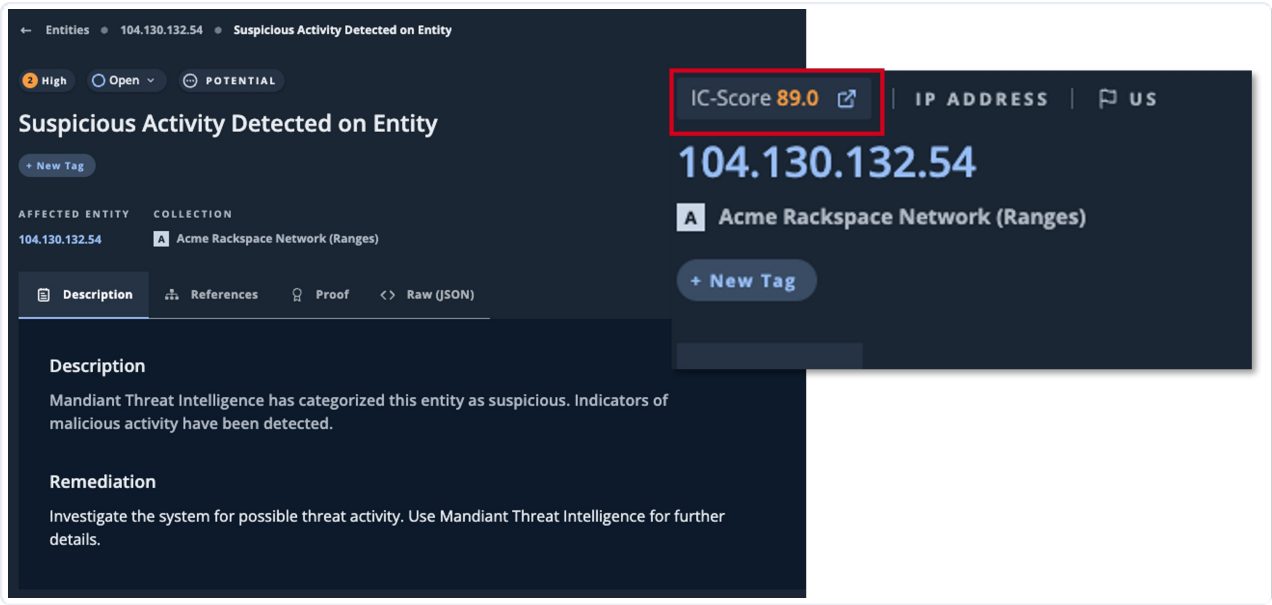
Examples of Issues created from Inferred CVEs

Issues created from Inferred CVEs include **Inferred CVE** in their name and a **Potential** Confidence assignment.

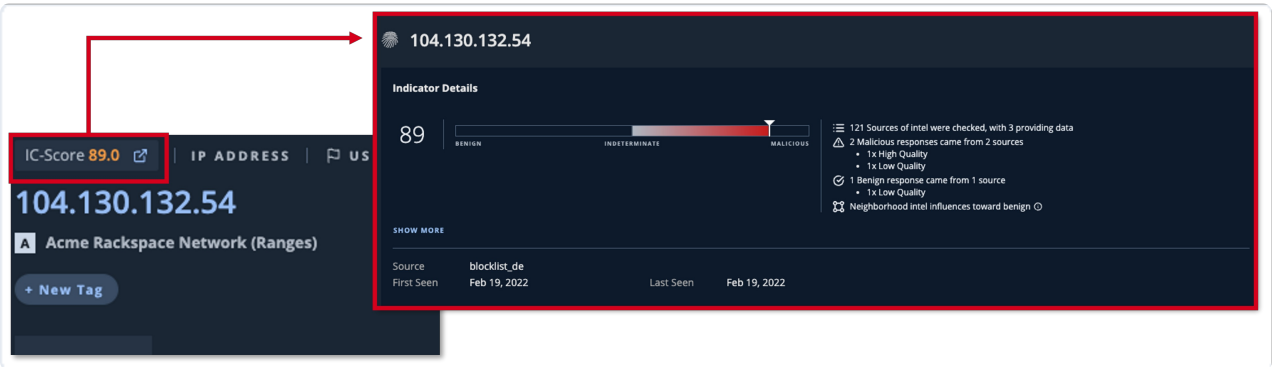
- To return all Issues created from Inferred CVEs, search **Issues** (http://asm.advantage.mandiant.com/issues) using the keyword `inferred`.
- To return all Entities with Inferred CVEs, search **Entities** (http://asm.advantage.mandiant.com/entities) using the `Entities with Inferred CVEs` search option.



Issues Created from Entity IC-Score

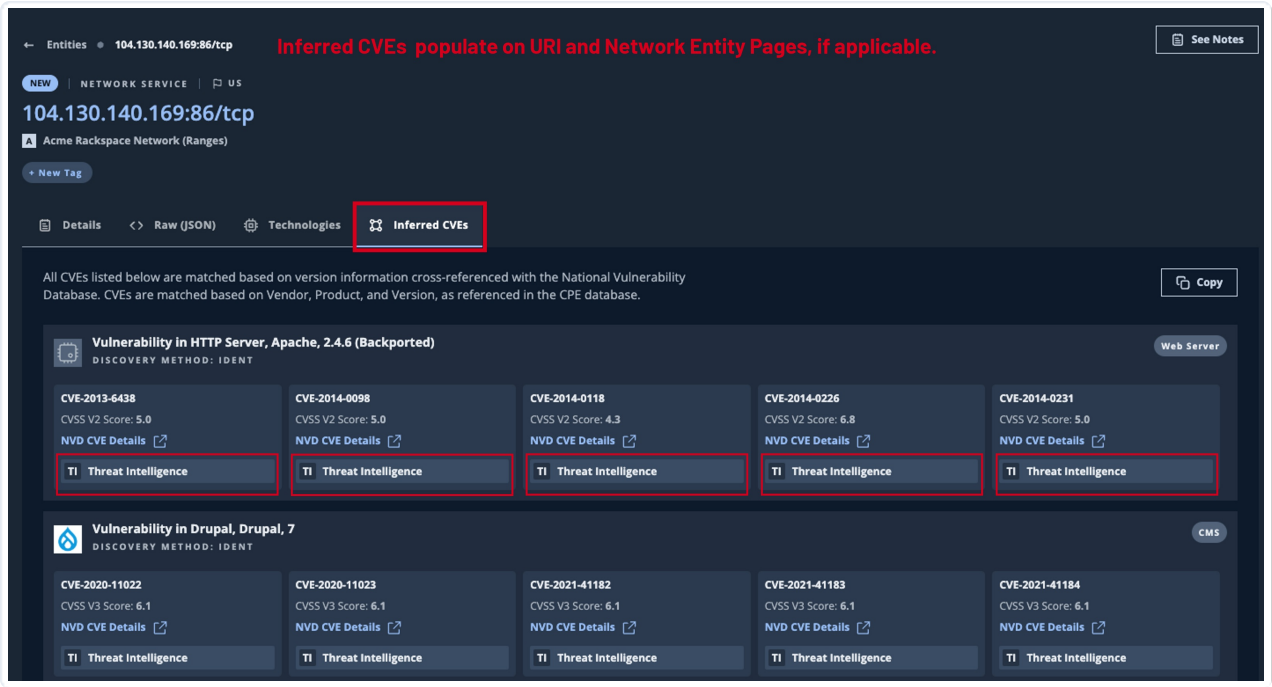


Entities with IC-Score



Inferred CVEs Linked to Threat Intelligence

When available, the Inferred CVEs populate on URI and Network Entity Pages.



Issues with CVEs Linked to Threat Intelligence