

STRATEGIC INTELLIGENCE

The Global Risks of Systemic Reliance on Critical Mineral Imports



TLP:WHITE

Oct 08, 2024

The global supply chain for healthcare is in a strained state, with current medicine shortages outnumbering those during the height of the COVID-19 pandemic. It is imperative that systemic supply chain vulnerabilities be discovered and remediated. One of these systemic challenges is finding sustainable long-term suppliers of critical minerals. Many cutting-edge healthcare technologies are built using these minerals, yet many countries are essentially completely reliant on the exports of external, often adversarial, nations. This white paper seeks to discuss the current state of the global healthcare supply chain and shine a light on the unique characteristics of the critical mineral trade that both enables and hinders the sector as a whole.

Key Judgements

- There is an ongoing drug shortage that is highlighting some upstream issues with the global healthcare supply chain.
- Some metals critical to healthcare delivery are almost exclusively sourced from China.
- Trade obstacles created by geopolitical tensions have major ramifications on the procurement of certain metals, increasing the likelihood of shortages in the event of global conflicts.
- Dependence on imports of critical minerals is a systemic risk to the healthcare sector.

- Due to the unique risks posed by single-source minerals, preemptive risk mitigation strategies may better navigate the situation than reactionary measures.

To read the full report, click [here](#).

The full report is attached and has been posted to the White Papers folder in the Cyware Doc Library.

Folder Location: Doc Library > White Papers

The title of this report is: **The Global Risks of Systemic Reliance on Critical Mineral Imports**

If you have any ideas for collaborative efforts with Health-ISAC's Threat Operations Center, please reach out to toc@h-isac.org.

Report Source(s)

Health-ISAC

Release Date

Oct 08, 2024 (UTC)

Alert ID 377dfb17

This Alert has 1 attachment(s). To view or download the attachment(s), click "View Alert" to login to the web portal.

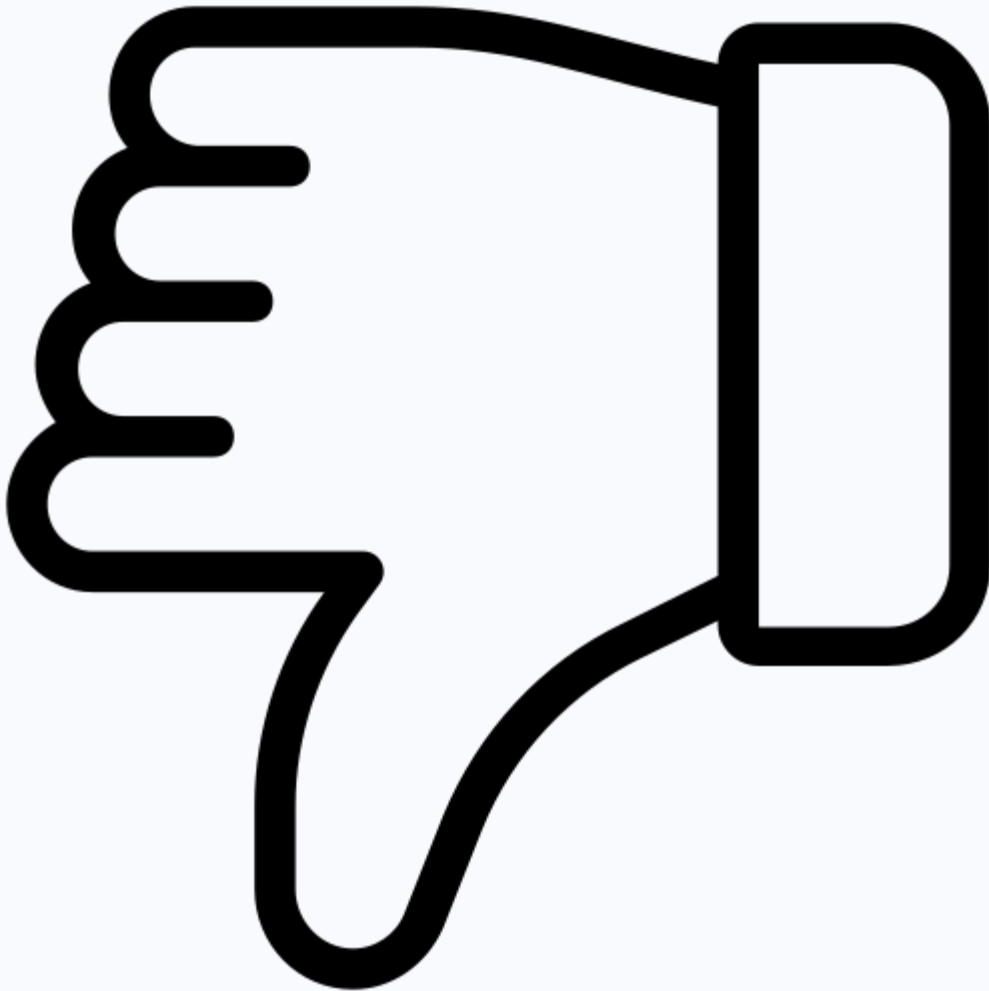
[View Alert](#)

Share Feedback

was this helpful?



|



Tags Critical Minerals, Strategic Intelligence, White Papers, business continuity, Risk Management, Supply Chain, Critical Infrastructure

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

HICP

The [Health Industry Cybersecurity Practices](#) (HICP) refer to a set of guidelines and recommendations developed by the U.S. Department of Health and Human Services (HHS) to help healthcare organizations improve their cybersecurity posture. The HICP was created in response to the increasing threat of cyberattacks and data breaches in the healthcare sector, which has been a target for cybercriminals due to the sensitive and valuable nature of healthcare data.

The HICP resources are aimed at helping healthcare organizations of all sizes, including small, medium, and large entities. It provides practical and actionable guidance for managing and mitigating cybersecurity risks in healthcare environments, with a focus on five key cybersecurity threats: ransomware, phishing, loss or theft of equipment or data, insider threats, and attacks against connected medical devices.

Conferences, Webinars, and Summits

<https://h-isac.org/events/>

Share Threat Intel

For guidance on sharing indicators with Health-ISAC via HTIP, please visit the Knowledge Base article "HTIP - Share Threat Intel" [here](#).

The "Share Threat Intel" feature allows for attributed or anonymous sharing across ISACs and other cybersecurity-related entities.

Access the Health-ISAC Threat Intelligence Portal

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Health-ISAC Threat Intelligence Portal (HTIP).

For Questions or Comments

Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.



For more updates and alerts, visit: <https://health-isac.cyware.com/webapp/>

If you are not supposed to receive this email,
please contact us at toc@h-isac.org.