Technical Review Report of Pulsedive  
: A free threat intel platform

# Abstract The Technical Review Report of Pulsedive, a free threat intelligence platform, offers a comprehensive evaluation of its capabilities for SMEs and developing economies. The report assesses key aspects such as installation, functionality, usability, integration, and community support. Pulsedive's user-friendly interface, comprehensive threat intelligence feed, risk scoring, and customizable alerts make it a valuable tool for organizations with varying technical expertise. Recommendations for the development of a new platform focus on affordability, simplicity, localization, integration, and interoperability. Overall, Pulsedive emerges as a highly suitable solution for enhancing cybersecurity posture and proactive defense against cyber threats in diverse organizational settings.

[Abstract 1](#_Toc164858546)

[Tool Overview 4](#_Toc164858547)

[● **Tool Description:** 4](#_Toc164858548)

[● **Key Features:** 4](#_Toc164858549)

[Installation and Setup 5](#_Toc164858550)

[● **System Requirements:** 5](#_Toc164858551)

[● **Installation Process:** 6](#_Toc164858552)

[● **Configuration Needs:** 6](#_Toc164858553)

[Functional Capabilities 7](#_Toc164858554)

[● **Core Functionalities:** 7](#_Toc164858555)

[● **Performance Metrics:** 7](#_Toc164858556)

[● **Accuracy and Reliability:** 8](#_Toc164858557)

[Usability and Accessibility 8](#_Toc164858558)

[● **Ease of Use:** 8](#_Toc164858559)

[● **Interface Design:** 9](#_Toc164858560)

[● **Documentation and Support:** 9](#_Toc164858561)

[Integration, Compatibility, and Scalability 9](#_Toc164858562)

[● **Interoperability with Existing Tools:** 9](#_Toc164858563)

[● **APIs and Customization:** 9](#_Toc164858564)

[● **Scalability:** 10](#_Toc164858565)

[● **Flexibility:** 10](#_Toc164858566)

[Community Support and Sustainability 10](#_Toc164858567)

[● **Developer Community:** 10](#_Toc164858568)

[● **Updates and Maintenance:** 10](#_Toc164858569)

[● **Local and Global Support Networks:** 10](#_Toc164858570)

[Assessment of Gaps 11](#_Toc164858571)

[● **Identified Gaps:** 11](#_Toc164858572)

[● **Potential for Improvement:** 11](#_Toc164858573)

[Use Cases and Practical Applications 12](#_Toc164858574)

[● **Relevant Scenarios for SMEs/developing economies:** 12](#_Toc164858575)

[● **Examples of Successful Use:** 13](#_Toc164858576)

[Conclusion and Recommendations for Development 14](#_Toc164858577)

[● **Overall Suitability:** 14](#_Toc164858578)

[● **Recommendations for New Platform:** 14](#_Toc164858579)

[Reference 15](#_Toc164858580)

#### 

#### 

|  |  |
| --- | --- |
| **Tool Name :** | **PULSEDIVE** |
| **Evaluated Version:** | **6** |
| **Evaluation period:** | **14 April 2023 – 19 April 2023** |
| **Evaluator(s):** | **Gaurang Bansal, Ajitesh Arora** |
| **Purpose of Review:** | Assess capabilities for SMEs/developing economies and identify gaps and features for a new threat intel platform. |

# 

# Tool Overview

## **Tool Description:**

* + *Pulsedive is a comprehensive threat intelligence web platform designed to empower organizations with insights into cyber threats. Its primary purpose revolves around aggregating, analyzing, and disseminating threat data to enhance cybersecurity posture. Pulsedive serves as a centralized hub for accessing actionable intelligence to proactively defend against cyber threats.*

## **Key Features:**

* + *Unified Threat Intelligence Feed: Pulsedive offers a consolidated feed of threat intelligence data sourced from various repositories, including malware databases, threat feeds, and open-source intelligence (OSINT). This feature provides SMEs and developing economies with access to a broad spectrum of threat information without the need for extensive resources.*
  + *Risk Scoring and Prioritization: Pulsedive employs advanced algorithms to assess the severity and relevance of threats, assigning risk scores to prioritize mitigation efforts. This capability is particularly beneficial for SMEs and organizations with limited resources, enabling them to focus on addressing the most critical vulnerabilities and threats first.*
  + *Customizable Alerts and Notifications: Users can configure tailored alerts and notifications based on specific threat parameters, such as threat actor activity, indicators of compromise (IOCs), or emerging cyber threats. This functionality empowers SMEs to stay informed about potential security incidents and take timely remediation actions.*
  + *User-Friendly Interface and Documentation: Pulsedive offers an intuitive user interface coupled with comprehensive documentation and tutorials, making it accessible to users with varying levels of cybersecurity expertise. This aspect is particularly advantageous for SMEs and organizations in developing economies that may lack dedicated cybersecurity personnel.*

# Installation and Setup

## **System Requirements:**

*Minimal Requirements:*

* + *Internet Connection: Pulsedive is a cloud-based platform, requiring a stable internet connection for access.*
  + *Web Browser: Compatible web browsers include Google Chrome, Mozilla Firefox, Microsoft Edge, or Safari.*
  + *Device: Accessible on desktops, laptops, tablets, and mobile devices.*

*Recommended Requirements:*

* + *Operating System: Windows 10, macOS, Linux, or any other modern operating system.*
  + *Browser Version: Latest stable version of compatible web browsers for optimal performance.*
  + *Screen Resolution: Recommended screen resolution of 1280x720 pixels or higher for better viewing experience.*

## **Installation Process:**

*Simplicity for SMEs:*

* + *Pulsedive requires no installation process in the traditional sense since it is a web-based platform.*
  + *Users simply need to navigate to the Pulsedive website (https://pulsedive.com/) using a compatible web browser.*
  + *Registration or sign-up may be required to access certain features, but there's no software to download or install.*
  + *This simplicity makes Pulsedive ideal for SMEs with limited resources, as it eliminates the need for dedicated hardware or IT support.*

## **Configuration Needs:**

*Ease of Configuration:*

* + *Pulsedive is designed for immediate use with minimal configuration requirements.*
  + *Upon registration, users can customize their account settings, including notification preferences and threat feed subscriptions, through an intuitive user interface.*
  + *Advanced configurations, such as API integrations or custom threat intelligence feeds, are available for users with specific requirements but are not necessary for basic functionality.*
  + *The platform's user-friendly design and straightforward configuration options ensure that SMEs can quickly deploy and start using Pulsedive without extensive setup procedures.*

# Functional Capabilities

## **Core Functionalities:**

* + *Threat Intelligence Aggregation: Pulsedive aggregates threat intelligence data from various sources, providing SMEs in developing economies with access to a wide range of threat information without the need for costly subscriptions to multiple threat feeds. This fills the gap of cyber threat visibility by consolidating relevant data in one platform, simplifying analysis and decision-making processes.*
  + *Risk Prioritization: Pulsedive employs risk scoring algorithms to prioritize threats based on severity, enabling SMEs to focus their limited resources on addressing the most critical vulnerabilities first. This helps SMEs effectively allocate resources and mitigate risks, reducing the likelihood of costly security incidents.*
  + *Customizable Alerts: Pulsedive allows users to configure customized alerts and notifications based on specific threat parameters, ensuring that SMEs can stay informed about potential security incidents in real-time. This proactive approach to threat detection enables SMEs to respond swiftly to emerging threats, even with minimal technical capabilities.*
  + *Collaborative Intelligence Sharing: Pulsedive facilitates collaboration among security professionals and organizations by enabling the sharing of threat intelligence insights and analysis. This feature allows SMEs to leverage the collective knowledge and expertise of the cybersecurity community, enhancing their cyber threat visibility and response capabilities without significant financial investments.capabilities .*

## **Performance Metrics:**

* + *Resource-Constrained Environments: Pulsedive is designed to perform efficiently in resource-constrained environments, requiring only a stable internet connection and compatible web browser for access. The platform's cloud-based infrastructure ensures scalability and reliability, even for SMEs with limited IT resources. Performance metrics such as uptime, response time, and data processing speed are consistently monitored to ensure optimal performance.*

## **Accuracy and Reliability:**

* + *Data Collection and Processing: Pulsedive utilizes advanced data collection and processing techniques to ensure the accuracy and reliability of threat intelligence. Data is collected from reputable sources and subjected to rigorous analysis to identify and eliminate false positives. Users have control and visibility over the data being collected and processed, with transparency into the sources and methodologies used.*
  + *Effectiveness in SME Scenarios: Pulsedive's effectiveness in various scenarios typical for SMEs is validated through its user-friendly interface, actionable intelligence, and reliable threat data. The platform's intuitive design and customizable features cater to the specific needs and constraints of SMEs in developing economies, empowering them to enhance their cyber threat visibility and response capabilities effectively.*As a user of Pulsedive, you'll find its functionalities to be invaluable for enhancing your organization's cyber threat visibility. From aggregating threat intelligence to prioritizing risks and enabling proactive threat detection, Pulsedive equips you with the tools you need to stay ahead of potential security incidents. Its user-friendly interface and customizable features make it accessible and effective, even for users with minimal technical expertise. With Pulsedive, you can trust that you have control and visibility over the threat landscape, empowering you to make informed decisions and bolster your cybersecurity defenses.

# Usability and Accessibility

## **Ease of Use:**

* + *Pulsedive excels in usability, catering to the skill levels commonly found in SMEs and developing economies. Its intuitive design ensures that users, regardless of technical proficiency, can easily navigate the platform to derive actionable intelligence. The straightforward interface and simplified workflows enable users to quickly access and interpret threat data, empowering them to make informed decisions to mitigate risks effectively.*

## **Interface Design:**

* + *The interface design of Pulsedive is tailored to accommodate non-technical users, making it accessible to a wide range of individuals within SMEs and developing economies. The platform's clean layout and intuitive navigation minimize complexity, allowing users to focus on extracting meaningful insights from the wealth of threat intelligence available. Clear labeling and visual cues enhance usability, ensuring that users can effortlessly locate and utilize key features without requiring extensive technical knowledge.*

## **Documentation and Support:**

* + Pulsedive provides comprehensive documentation and support resources to assist users, particularly those with limited technical expertise. The documentation is written in clear and concise language, making it easy for users to understand and follow. It covers a wide range of topics, from basic platform functionalities to advanced configuration options, ensuring that users have access to the information they need to maximize the value of Pulsedive. Additionally, responsive customer support is available to address any questions or issues that may arise, further enhancing the accessibility of the platform for users with varying levels of technical proficiency.

# Integration, Compatibility, and Scalability

## **Interoperability with Existing Tools:**

* + *Pulsedive offers seamless interoperability with existing tools commonly used by SMEs, ensuring compatibility with their current infrastructure. Through its flexible APIs and integration capabilities, Pulsedive can easily integrate with a variety of security tools, SIEMs, and other platforms, allowing SMEs to leverage their existing investments while enhancing their cyber threat intelligence capabilities.*

## **APIs and Customization:**

* + *Pulsedive provides robust APIs and customization options, enabling SMEs to tailor the platform to their specific needs and workflows. The APIs allow for seamless integration with internal systems and third-party applications, facilitating automated data exchange and workflow orchestration. Additionally, Pulsedive offers customization features that enable users to configure alerts, notifications, and dashboards according to their preferences, ensuring a personalized experience that aligns with their unique requirements.*

## **Scalability:**

* + *Pulsedive is highly scalable, capable of accommodating the growing needs of SMEs as their operations expand. The platform's cloud-based architecture allows for elastic scaling, ensuring that resources are dynamically allocated based on demand. Whether an SME is just starting or experiencing rapid growth, Pulsedive can scale seamlessly to support their evolving requirements without compromising performance or reliability.*

## **Flexibility:**

* + Pulsedive offers unparalleled flexibility, empowering SMEs to adapt to changing threat landscapes and business environments. The platform's modular design and customizable features enable users to tailor their cyber threat intelligence strategies to meet their specific objectives and constraints. Whether it's adjusting risk scoring criteria, configuring alert thresholds, or integrating new data sources, Pulsedive provides the flexibility needed for SMEs to stay agile and resilient in the face of emerging cyber threats.

# Community Support and Sustainability

## **Developer Community:**

* + *Pulsedive benefits from a vibrant developer community, offering robust support for SMEs lacking in-house expertise. The community provides forums, discussion boards, and knowledge-sharing platforms where users can seek assistance, exchange best practices, and collaborate on solutions to common challenges. Additionally, Pulsedive's developers actively engage with the community, addressing feedback, providing guidance, and continuously improving the platform to better meet the needs of users.*

## **Updates and Maintenance:**

* + *Pulsedive prioritizes updates and maintenance to ensure the platform's long-term sustainability. Updates are rolled out regularly to introduce new features, enhancements, and security patches, addressing emerging threats and evolving user requirements. The frequency and quality of updates demonstrate Pulsedive's commitment to maintaining a secure and reliable platform that remains relevant in an ever-changing threat landscape..*

## **Local and Global Support Networks:**

* + *Pulsedive*

# Assessment of Gaps

## **Identified Gaps:**

* + *Cost Barrier: Despite its effectiveness, Pulsedive may still pose a cost barrier for some SMEs and organizations in developing economies due to its subscription-based pricing model. While Pulsedive offers flexible pricing plans, further efforts could be made to provide discounted rates or special packages tailored to the financial constraints of these entities.*
  + *Complexity: While Pulsedive prides itself on usability, there may still be areas where the platform could be simplified to better cater to users with limited technical expertise. Enhancing the onboarding process with guided setup wizards and providing more extensive documentation and tutorials could further reduce the complexity of using Pulsedive for non-technical users.*
  + *Lack of Localization: Pulsedive primarily focuses on English-language support and may not fully address the localization needs of users in diverse regions. Expanding language support and incorporating region-specific threat intelligence feeds could improve the platform's relevance and effectiveness in addressing localized cyber threats and regulatory requirements.*
  + *Limited Integration: While Pulsedive offers APIs for integration with external systems, there may be room for improvement in terms of the breadth and depth of integration options available. Enhancing compatibility with a wider range of security tools and platforms would enable SMEs to seamlessly integrate Pulsedive into their existing security infrastructure, reducing data silos and improving overall visibility.*

## **Potential for Improvement:**

* + *Affordability: Pulsedive could explore additional pricing options or discounts for SMEs and organizations in developing economies to make the platform more accessible. This could include offering discounted rates for non-profit organizations, educational institutions, or startups, as well as introducing tiered pricing plans based on usage levels.*
  + *Simplicity: Pulsedive could continue to prioritize simplicity and ease of use by further refining its user interface and streamlining key workflows. Providing more extensive documentation, interactive tutorials, and in-platform guidance features would empower users with varying levels of technical expertise to derive maximum value from Pulsedive.*
  + *Localization: Pulsedive could invest in expanding language support and incorporating region-specific threat intelligence feeds to better address the needs of users in diverse regions. Collaborating with local cybersecurity communities and organizations could help identify and prioritize localization efforts to ensure the platform remains relevant and effective on a global scale.*
  + *Enhanced Integration: Pulsedive could focus on enhancing its integration capabilities by developing pre-built connectors and expanding support for industry-standard protocols and formats. This would enable seamless integration with a wider range of security tools, SIEMs, and threat intelligence platforms, empowering SMEs to build comprehensive security ecosystems that leverage the full potential of Pulsedive's threat intelligence capabilities.*

# Use Cases and Practical Applications

## **Relevant Scenarios for SMEs/developing economies:**

*Phishing Threat Detection:*

* + *Scenario: SMEs in developing economies often lack robust email security measures, making them vulnerable to phishing attacks that can result in data breaches or financial losses.*
  + *Solution: Pulsedive's threat intelligence feed can identify known phishing domains and indicators of compromise (IOCs), enabling SMEs to proactively block malicious emails and educate employees about phishing tactics to prevent successful attacks.*

*Malware Infection Prevention:*

* + *Scenario: SMEs with limited cybersecurity resources may struggle to detect and mitigate malware infections, which can disrupt operations and compromise sensitive information.*
  + *Solution: Pulsedive provides real-time threat intelligence on malware campaigns and indicators of compromise, allowing SMEs to identify and block malicious files and URLs before they can infiltrate their networks or endpoints.*

*Supply Chain Risk Management:*

* + *Scenario: SMEs in developing economies often rely on interconnected supply chains, increasing their exposure to supply chain attacks and disruptions.*
  + *Solution: Pulsedive's collaborative intelligence sharing features enable SMEs to monitor and assess the security posture of their suppliers and partners, mitigating supply chain risks by identifying and addressing vulnerabilities before they can be exploited by adversaries.*

*Regulatory Compliance:*

* + *Scenario: SMEs operating in developing economies face increasing regulatory scrutiny and compliance requirements, particularly in industries such as finance, healthcare, and e-commerce.*
  + *Solution: Pulsedive offers threat intelligence feeds tailored to specific regulatory frameworks and compliance standards, helping SMEs identify and address security gaps to maintain compliance and avoid costly penalties or legal consequences.*

*Incident Response and Recovery:*

* + *Scenario: Despite their best efforts, SMEs may still experience security incidents such as data breaches or ransomware attacks, requiring rapid incident response and recovery efforts.*
  + *Solution: Pulsedive provides actionable threat intelligence and real-time alerts to facilitate rapid incident detection and response. SMEs can leverage Pulsedive's risk scoring and prioritization features to triage incidents and allocate resources effectively, minimizing downtime and financial losses.*

## **Examples of Successful Use:**

*The case study details Realtime Register's proactive approach to combating DNS abuse through the development of threat intelligence-driven monitoring and mitigation strategies. Led by CTO Wiebren Braakman, the company collaborates with external vendors to collect and process data effectively. Key points include:*

*1. Realtime Register defines requirements for vendors to collect and process data sources, enrich new domains, and support an intuitive platform.*

*2. The company focuses on quality intelligence and contextual data related to domain abuse to take precise actions.*

*3. Collaboration with Pulsedive enables bidirectional data flow, maximizing value and enhancing intelligence sharing.*

*4. Realtime Register engages in security discussions and contributes to initiatives targeting online abuse within the ICANN community.*

*5. The company allows users to dive deeper into domain and URL information through Pulsedive's community feed, enabling comprehensive research.*

*Conclusion:*

*Realtime Register's strategic partnership with external vendors, particularly Pulsedive, empowers the company to address DNS abuse effectively. By leveraging multiple intelligence sources, automating data feeds, and engaging in industry discussions, Realtime Register demonstrates a commitment to combatting online abuse proactively. The integration of bidirectional data flow and user-friendly interfaces enhances the platform's usability and provides customers with valuable insights to take informed actions against domain abuse.* *(Pulsedive, n.d.)*

# Conclusion and Recommendations for Development

## **Overall Suitability:**

* + *In conclusion, Pulsedive presents a highly suitable solution for SMEs in developing economies seeking to enhance their cybersecurity posture. Its comprehensive threat intelligence capabilities, user-friendly interface, and scalability make it accessible and effective for organizations with varying levels of technical expertise and resources. By providing actionable insights into emerging cyber threats and facilitating collaborative intelligence sharing, Pulsedive empowers SMEs to proactively defend against cyber attacks and mitigate risks, thereby safeguarding their assets and operations.*

## **Recommendations for New Platform:**

*Affordability and Flexibility:*

* + *Introduce flexible pricing options tailored to the budget constraints of SMEs, such as pay-as-you-go models or discounted rates for non-profit organizations and startups.*

*Simplicity and Usability:*

* + *Design an intuitive user interface with guided setup wizards and interactive tutorials to streamline onboarding and maximize usability for users with limited technical expertise.*

*Localization and Regional Support:*

* + *Incorporate multilingual support and region-specific threat intelligence feeds to address the unique needs and regulatory requirements of SMEs in diverse regions.*

*Integration and Interoperability:*

* + *Enhance integration capabilities with pre-built connectors and APIs to facilitate seamless integration with existing infrastructure and third-party applications, reducing data silos and improving overall visibility.*

*Customization and Collaboration:*

* + *Provide customizable features for alerts, notifications, and dashboards to enable SMEs to tailor the platform to their specific requirements and workflows.*
  + *Foster a collaborative community by facilitating knowledge sharing and collaboration among users, enabling SMEs to leverage collective intelligence and best practices to enhance their cybersecurity defenses.*

# Reference

# 1- *Pulsedive (n.d.). Feed - Pulsedive. [online] pulsedive.com. Available at: https://pulsedive.com/about/feed.*

2- *Growing Demand to Address DNS Abuse. (n.d.). Available at: https://pulsedive.com/downloads/casestudy\_realtimeregister.pdf.*