DataBee® BLUVECTOR

PRODUCT TECH BRIEF

Technical Overview: DataBee Detection Hub

Purpose: The DataBee Detection Hub enables scalable, long-term retention and investigation of network telemetry from BluVector, Zeek, Suricata and other sources. It supports advanced detection, correlation and forensic workflows without relying on traditional infrastructures.

Key capabilities

Deliver clarity, speed and scale.

The DataBee Detection Hub is built to meet the demands of modern security teams by combining scalable telemetry ingestion, intelligent correlation and intuitive investigation tools.

- **Unified Network Visibility**
  Aggregates telemetry across IT, IoT and OT environments for a holistic view.
- **Real-Time Detection**
  Supports machine-speed identification of high-risk behaviors including ransomware, zero-days and fileless activity.
- **Investigation Efficiency**
  Enables fast filtering, correlation and deep forensic analysis with intuitive dashboards.
- **Scalable Retention**
  Supports long-term storage of Zeek and Suricata logs for historical search and hunting.
- **Cost-Conscious Architecture**
  Designed to avoid traditional cost structures while maintaining high performance and fidelity.

Deployment Notes

Gain flexible integration and customization.

The DataBee Detection Hub is designed to integrated seamlessly into existing environments, supporting rapid deployment and customization based on team workflows and telemetry sources.

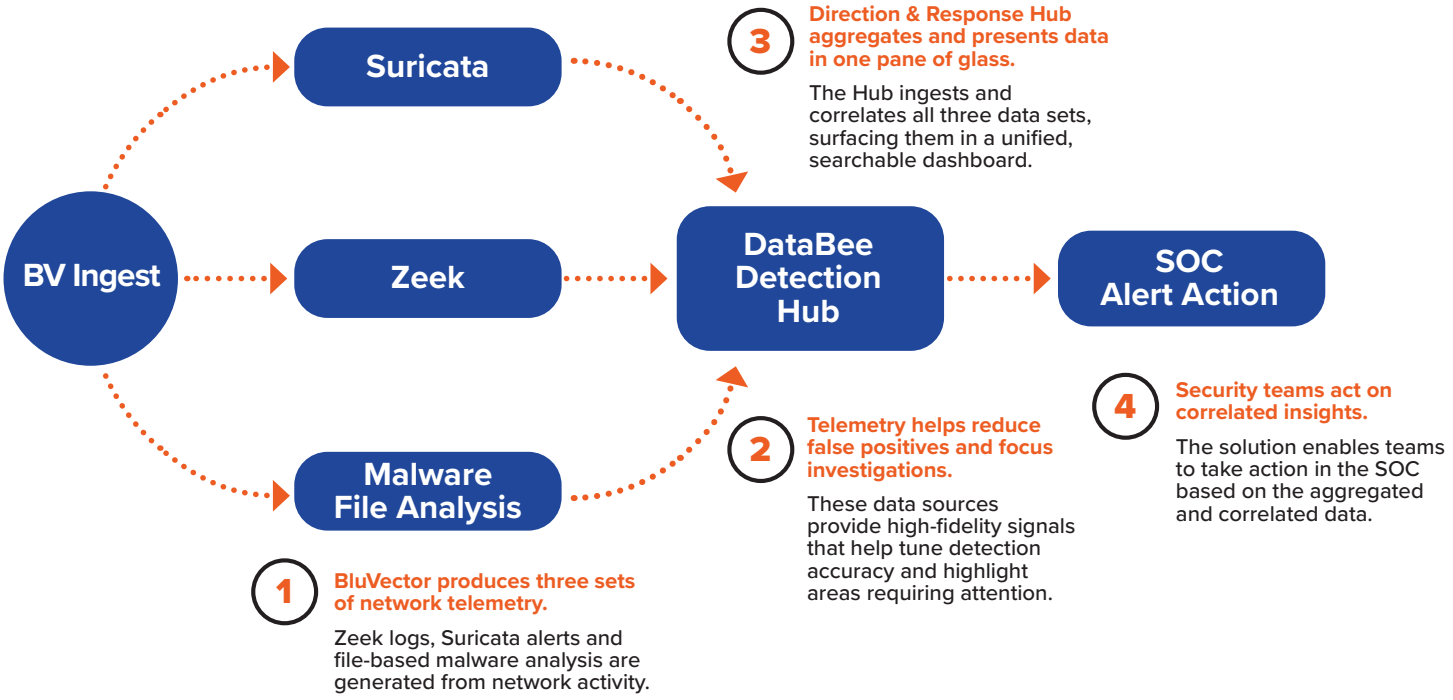
- Compatible with existing BluVector deployments
- Supports integration with Zeek and Suricata sensors
- Can be extended to additional telemetry sources as needed
- Dashboards are customizable based on team workflows and investigation priorities

USE CASES

Real-world applications drive clarity and action.

The DataBee Detection Hub supports a wide range of network monitoring and investigation scenarios. These use cases demonstrate how teams can leverage correlated telemetry to uncover hidden risks, enforce policy and accelerate response.

- **Detecting Command & Control (C2) Infrastructure**
  Identify malware using uncommon ports for communication.
- **Discovering Shadow IT**
  Locate unauthorized services running within the network.
- **Identifying Policy Violations**
  Detect applications bypassing standard ports to evade security controls.
- **Threat Hunting**
  Investigate unusual network behavior patterns on rare ports.
- **Incident Response**
  Rapidly assess the scope of potentially malicious communications.
- **Security Baseline Development**
  Establish normal port usage patterns specific to the environment.



Ready to see the signals, understand the impact and act with confidence?

Request a demo

Request a demo to see how the DataBee Detection Hub helps your team surface meaningful signals, understand the impact and take decisive action without traditional complexity or overhead.

databee.ai