CATO
NETWORKS

Real-Time Threat Intelligence with ML Feedback Loops

Tomer Doitshman, Security Research Team Lead
Cato Networks

Outline

- Introduction to Threat Intelligence
- Key Challenges in IOC Management
- Architecture of the ML Feedback Loop
- Technical Walkthrough: Key Components (ML model, Cloud-native stack, etc.)
- Feedback Loops in Action
- Real-World Applications and Case Studies
- Future Directions & Closing Remarks

Introduction to Threat Intelligence

Definition:

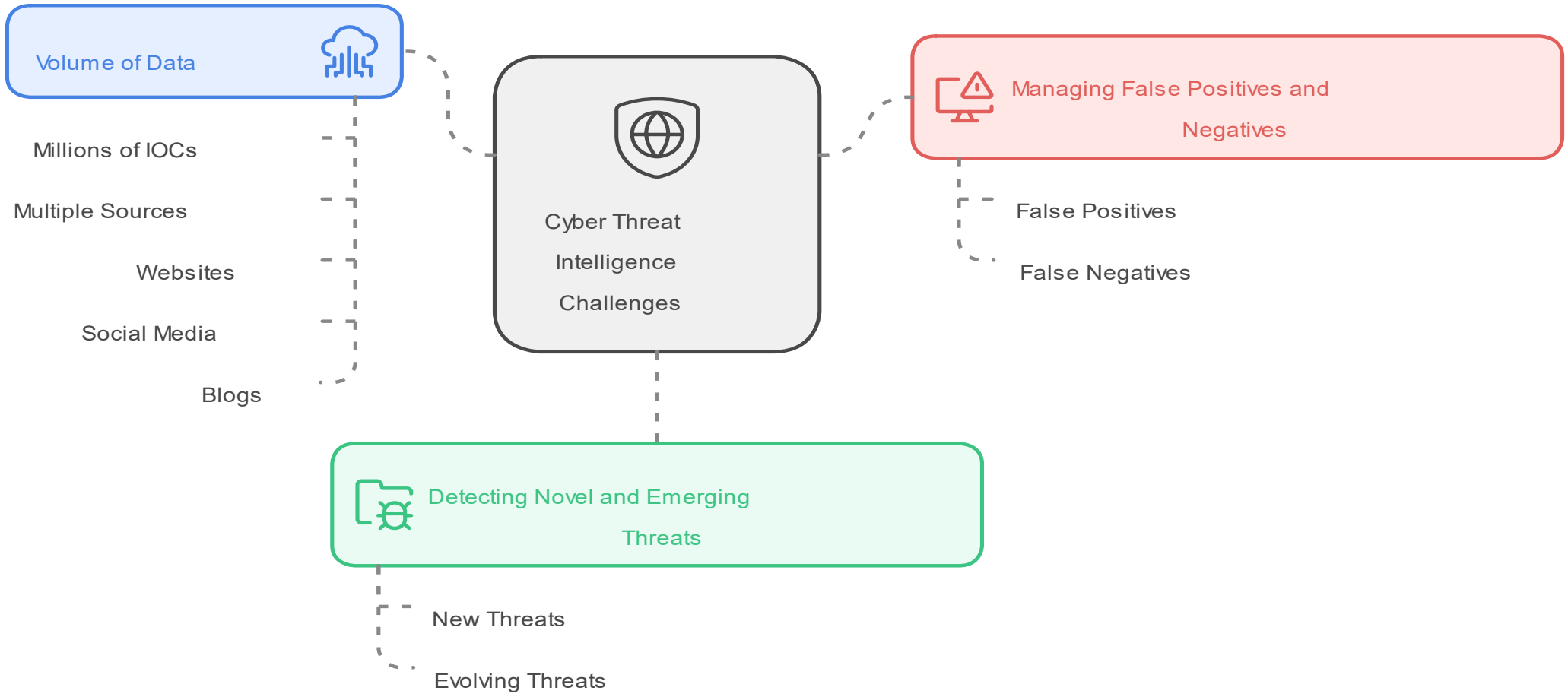
Threat intelligence is the collection, analysis, and action on data related to potential or existing cyber threats, helping organizations stay ahead of attacks.

IOC

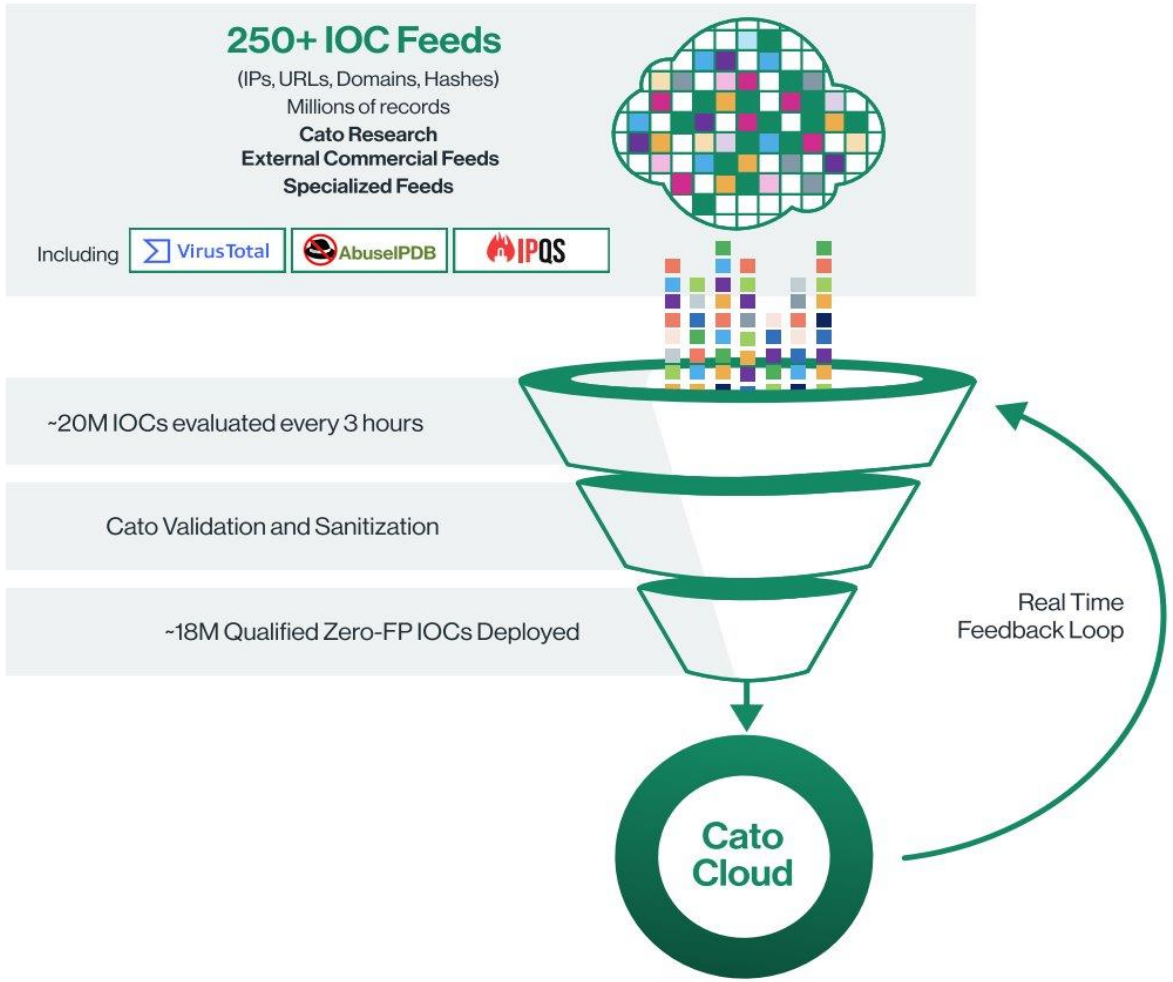
TI Feed

TIP

Key Challenges in IOC Management

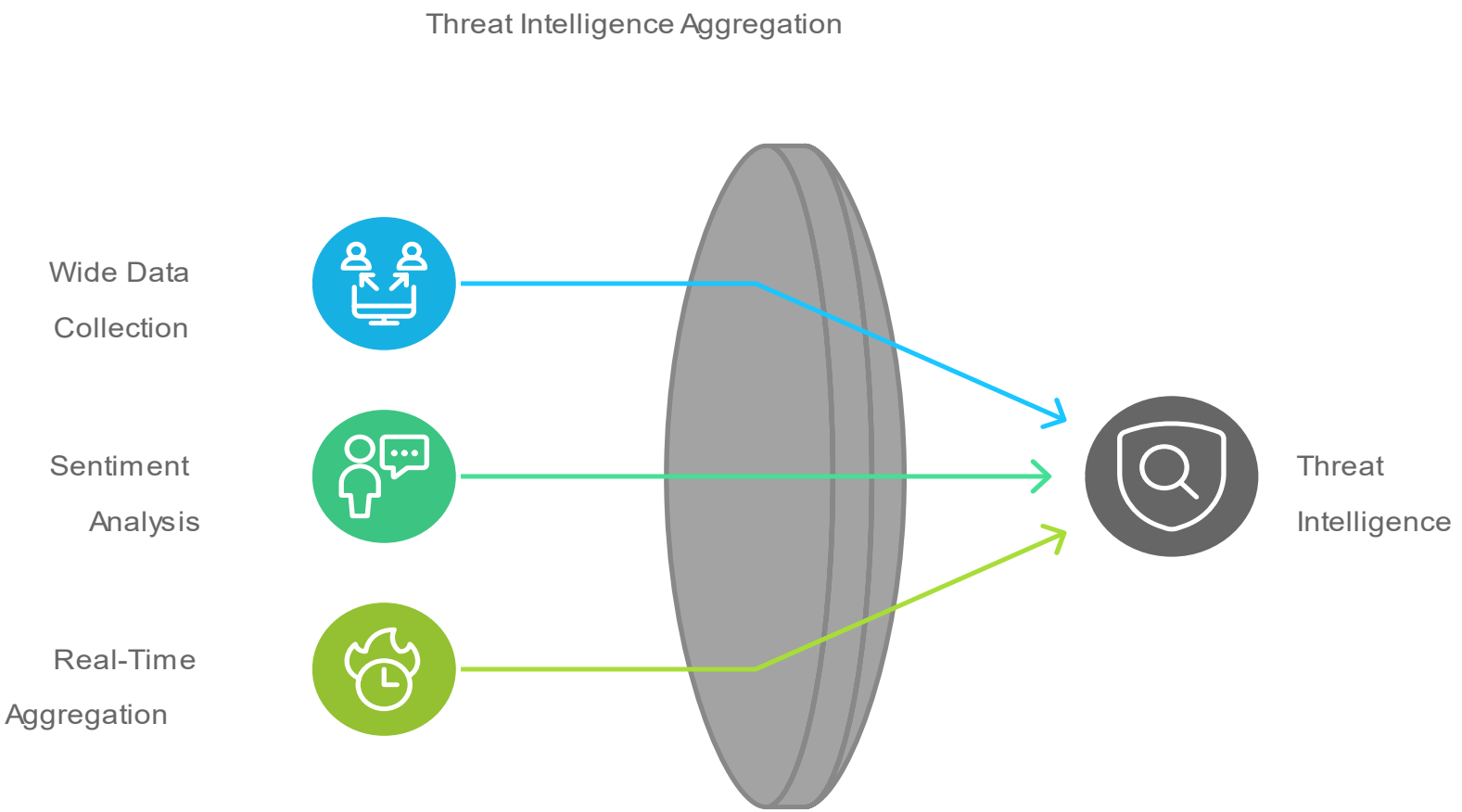


High-Level Architecture of a TIP

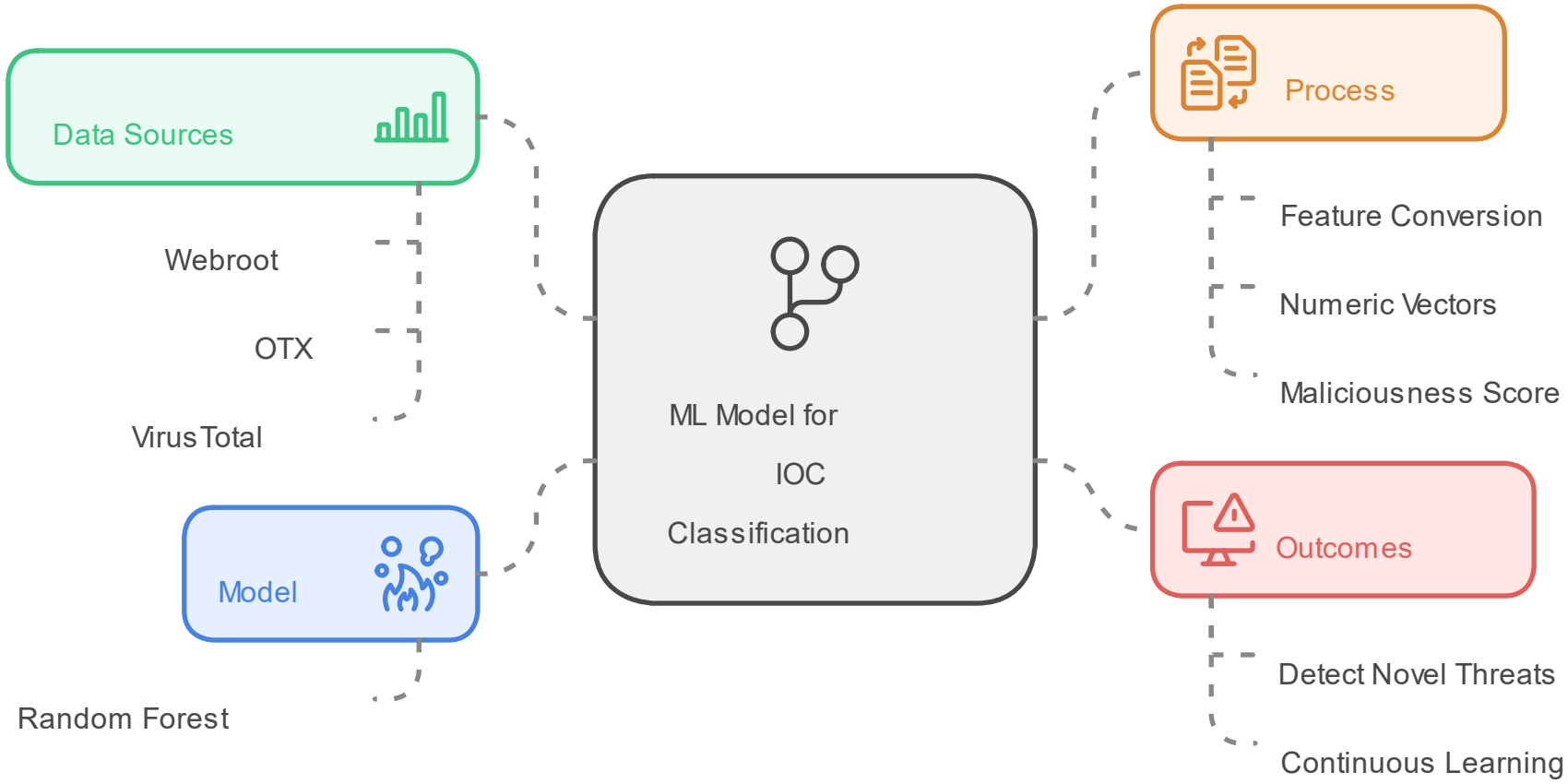


*Disclaimer: All vendor and company names mentioned in this presentation, such as VirusTotal, AbuseIPDB, and IPQS, are used for illustrative purposes only and do not imply any affiliation, endorsement, or partnership.

Data Sources and Aggregation

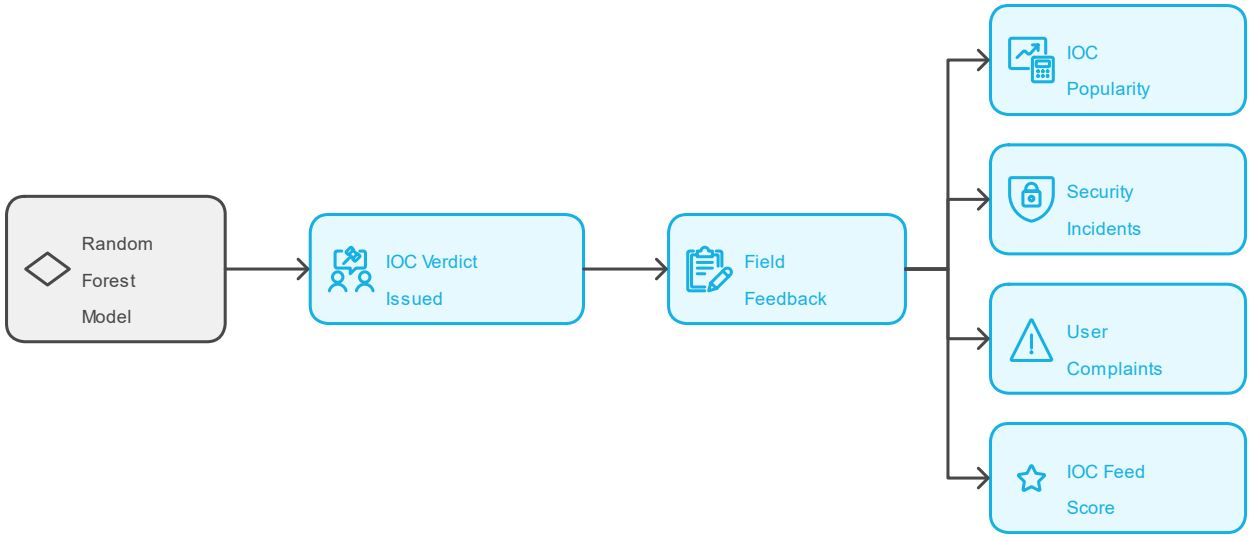


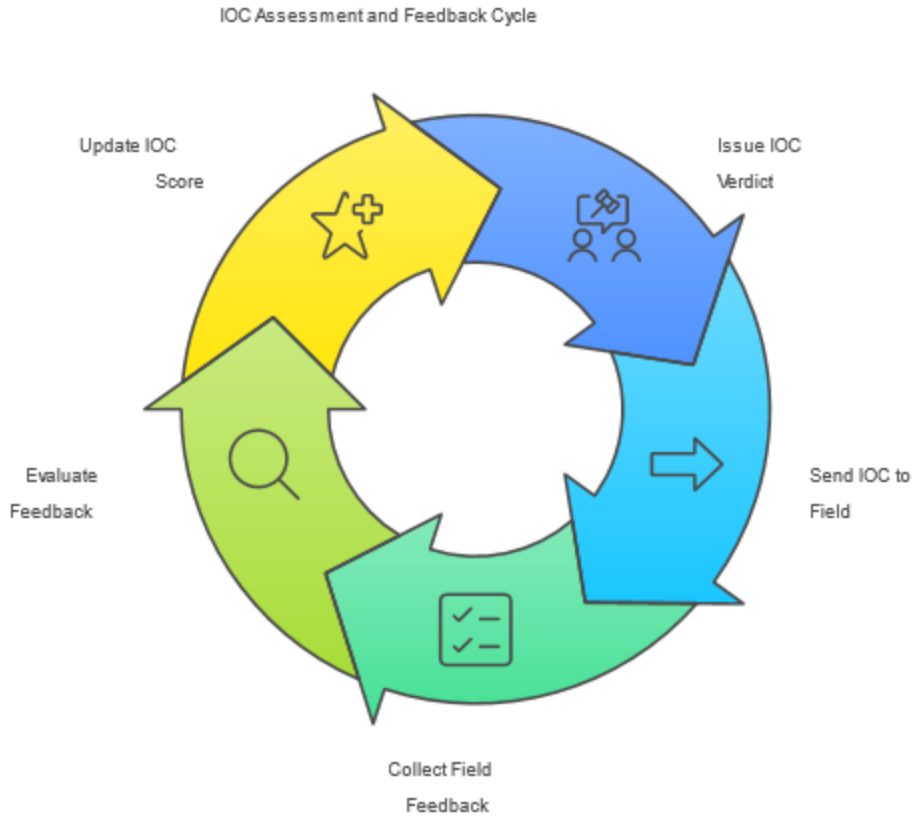
ML Model for IOC Classification



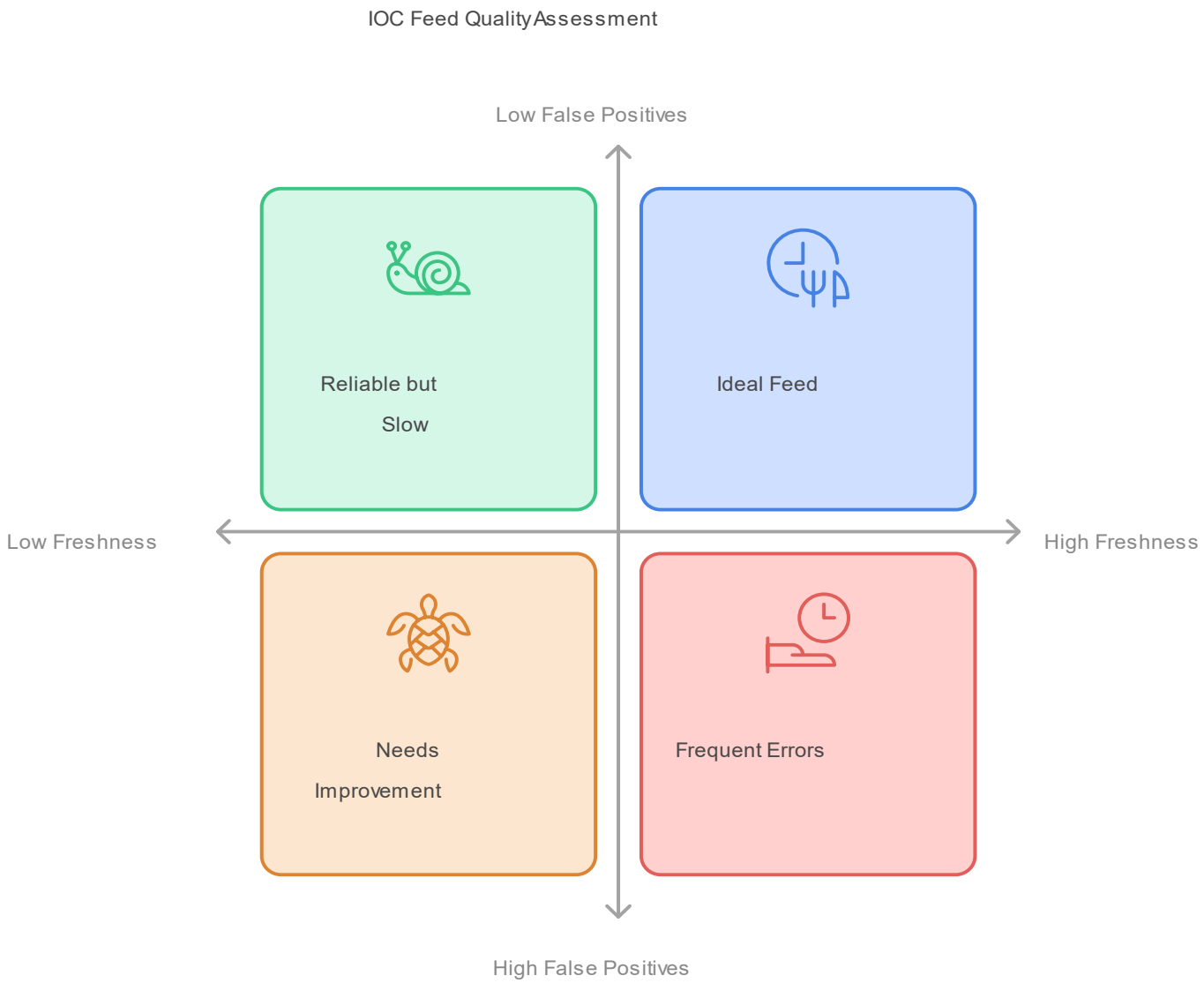
CATO NETWORKS

Continuous Feedback Loop Overview

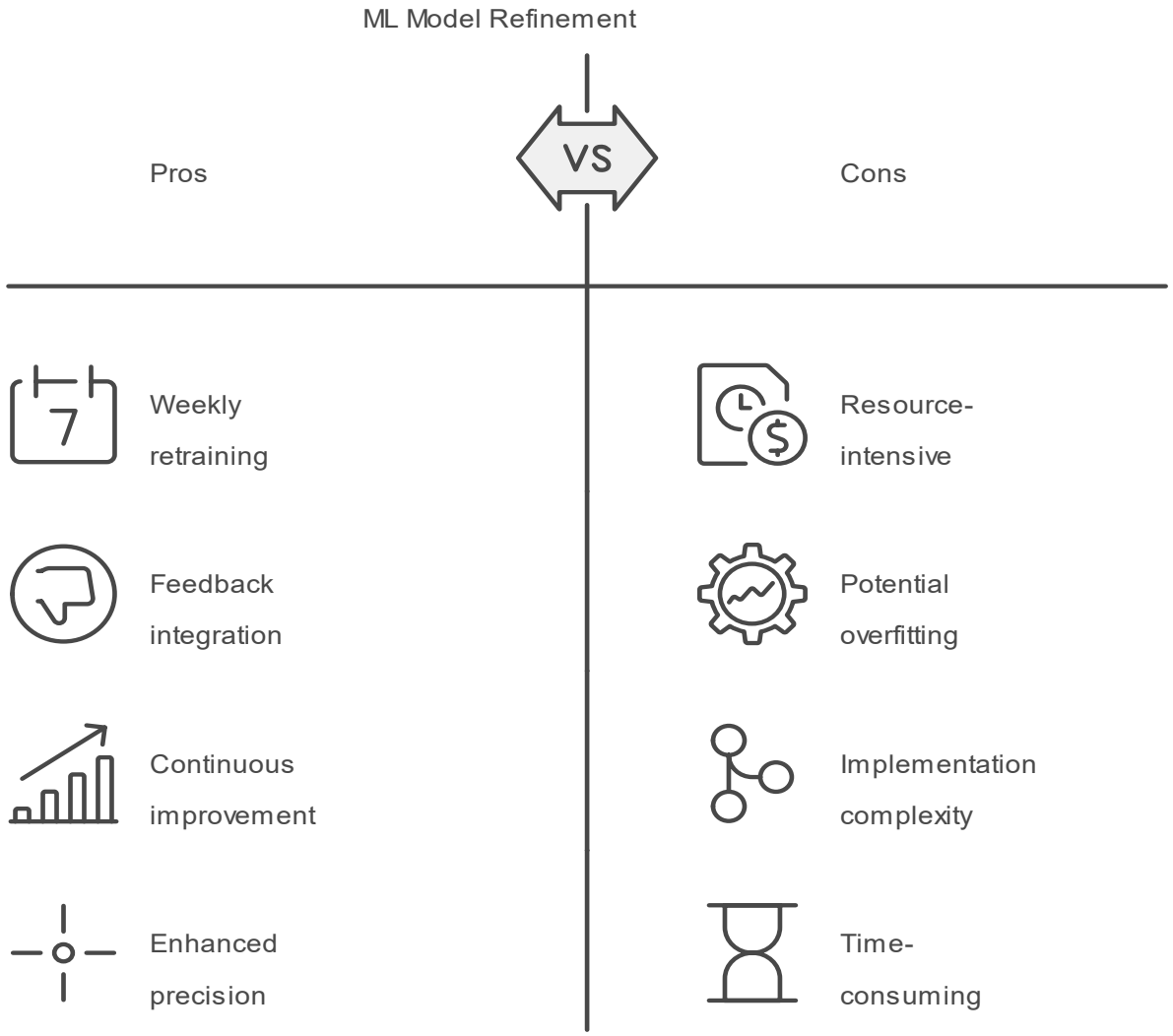




Evaluating IOC Feed Quality: Metrics and Scoring



ML Model Refinement: Reducing False Positives

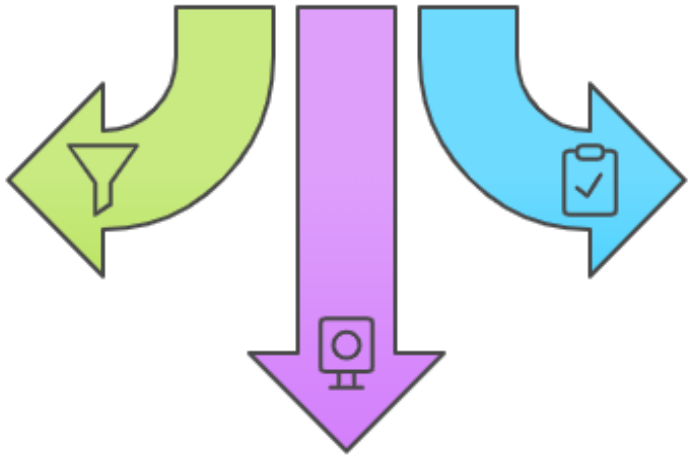


Filtering Accuracy and Monitoring

How to improve the accuracy of false positive filtering?

Continue with automatic filtering

Nearly 99% of false positives are filtered automatically using popularity and feed score calculations.



Increase manual reviews

User complaints and manual analysis are always 100% accurate in identifying true positives.

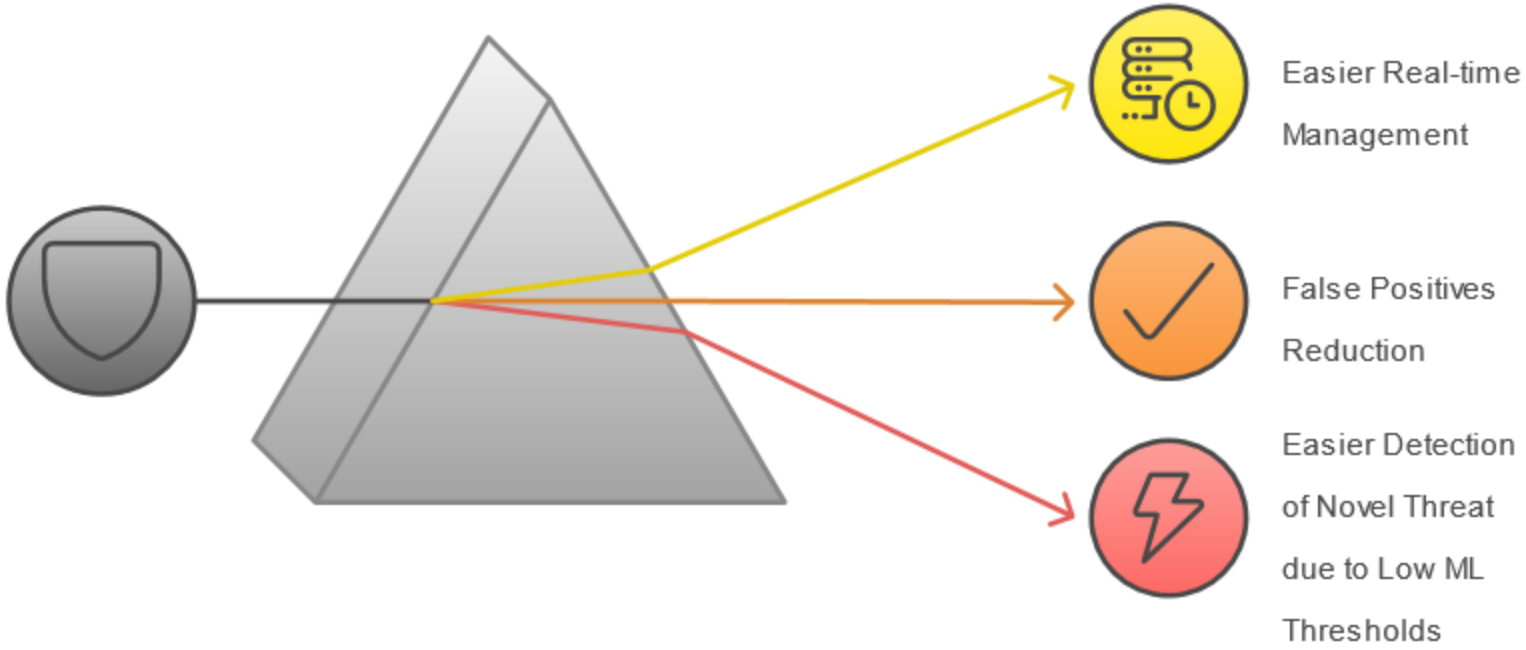
Enhance continuous monitoring

Since automatic filtering is statistical, we constantly monitor metrics to ensure no false negatives slip through.

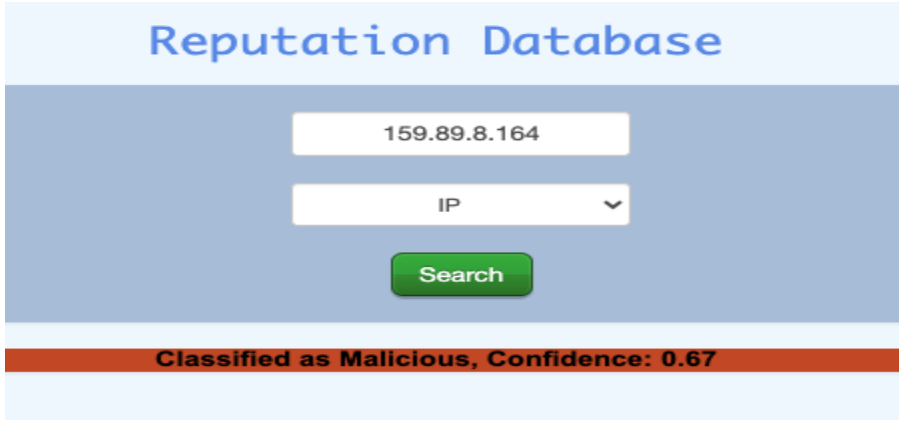
CATO NETWORKS

Impact on Detection Capabilities

TI Feedback Loop



TIP Service in Action



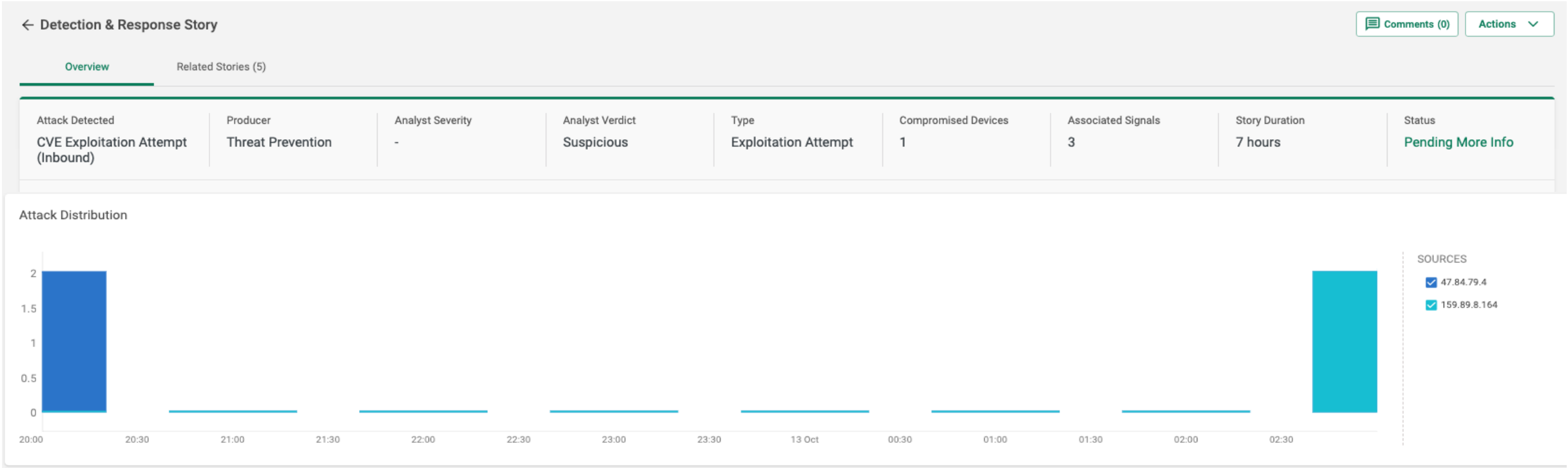
Popularity

Popularity Measure	Popularity Value
Cato Popularity Bin	4
Alexa Rank	-1
Umbrella Rank	-1

RPP

Measure	Value
Benign Score	0.6671474358974359
Malicious Score	0.3328525641025641
Last Update	10/13/2024, 10:02:27 PM

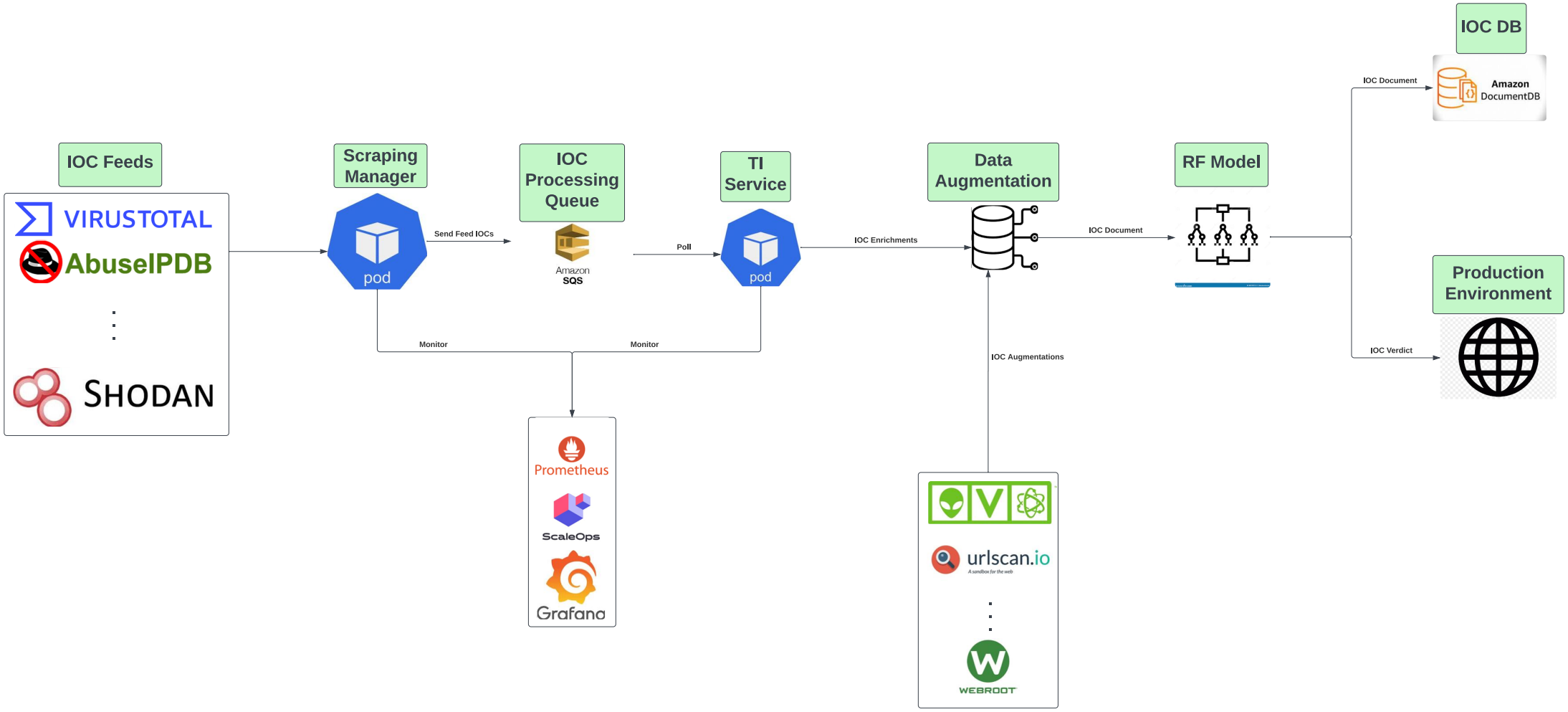
Integrating TIP Outputs into XDR Product



Sources

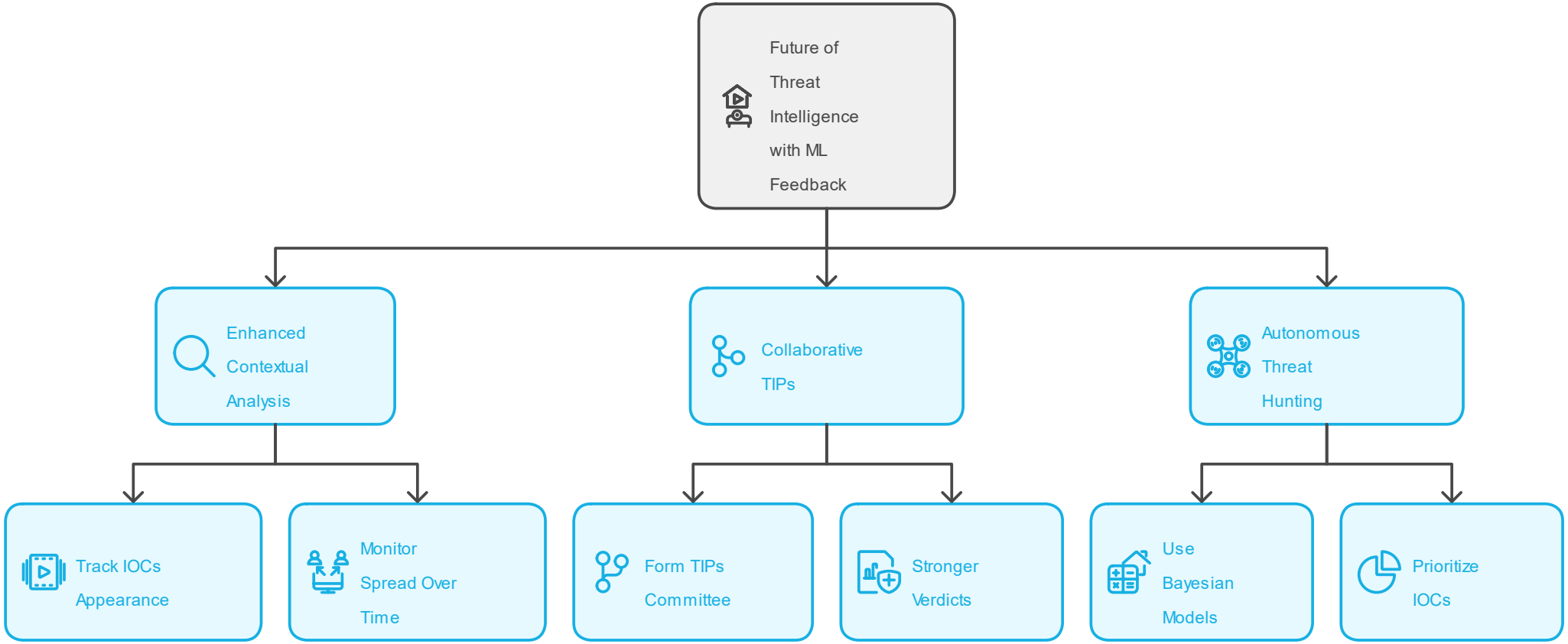
Source	Source Links	Malicious Score	Popularity ↓	Categories	Threat Feeds	Engines	Registrant country	Google Search Hits
47.84.79.4		0.33	MEDIUM	-	16	-	Singapore	-
159.89.8.164		0.33	LOW	-	11	6	Germany	-

TIP Implementation with Integrated Feedback Loop



*Disclaimer: All vendor and company names mentioned in this presentation, are used for illustrative purposes only and do not imply any affiliation, endorsement, or partnership.

Future of Threat Intelligence with ML Feedback



Conclusion & Takeaways

- **ML Feedback Loops:** Crucial for modern threat intelligence.
- **Continuous Improvement:** Ongoing refinement of IOC classification.
- **Real-World Impact:** Enhanced security operations.
- **Call to Action:** Explore ML-driven threat intelligence solutions.

CATO NETWORKS

Questions?

CATO
NETWORKS

Cato SASE. Ready for Whatever's Next.