Security Data Engineering

The SOC Problem

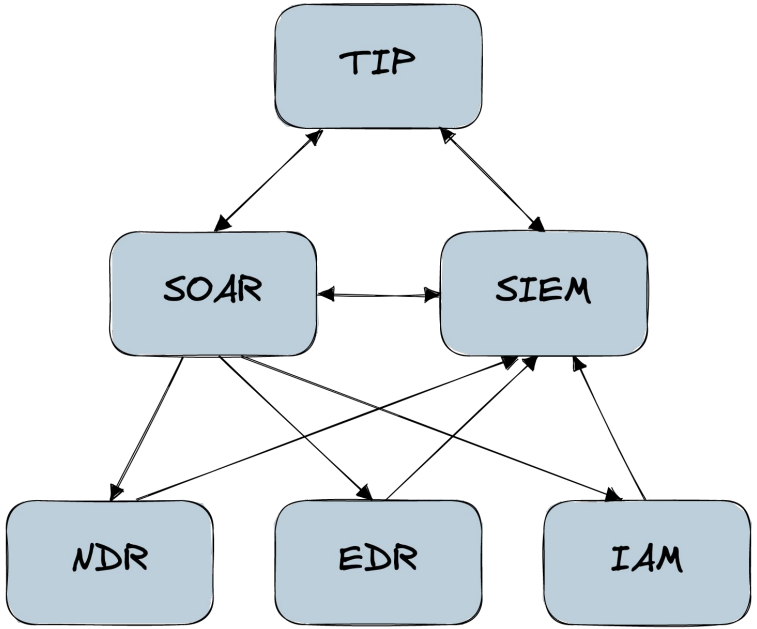
Defenders struggle with complexity

⚠️ **Point-to-point integration**

- → Unsustainable SOC architecture
- → Unmaintainable expert systems
- → Pre-defined use cases

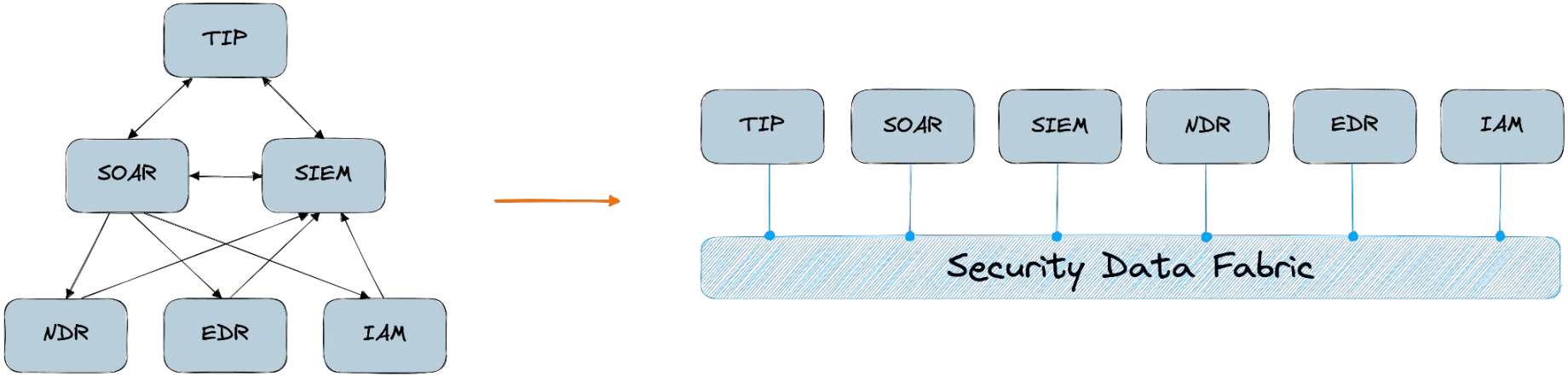
⚠️ **Proprietary data behind APIs**

- → Vendor lock-in
- → Partial analytics capabilities
- → Insufficient data residency controls

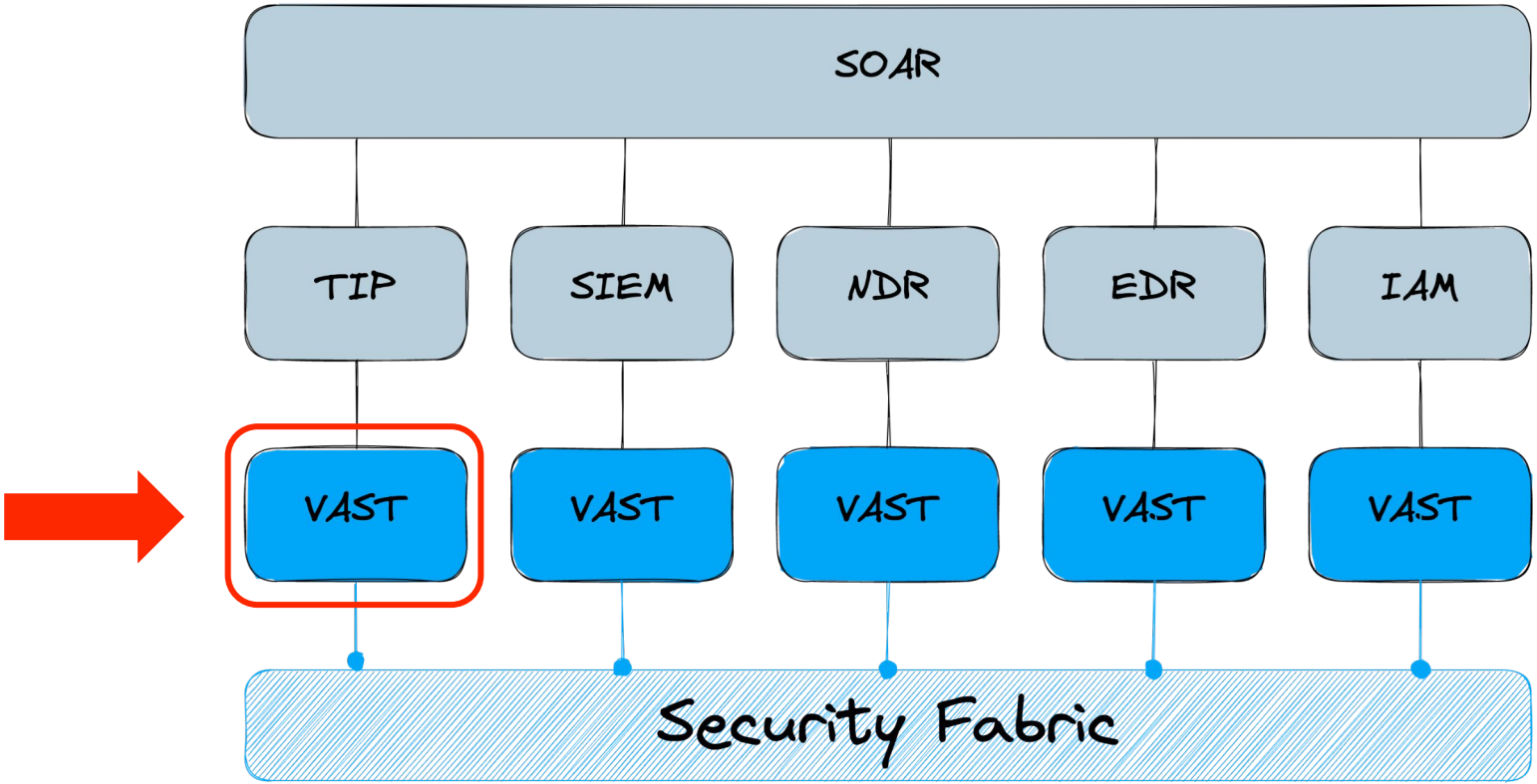


https://www.isc2.org/Research/Workforce-Study
https://www.mandiant.com/m-trends

Our Approach



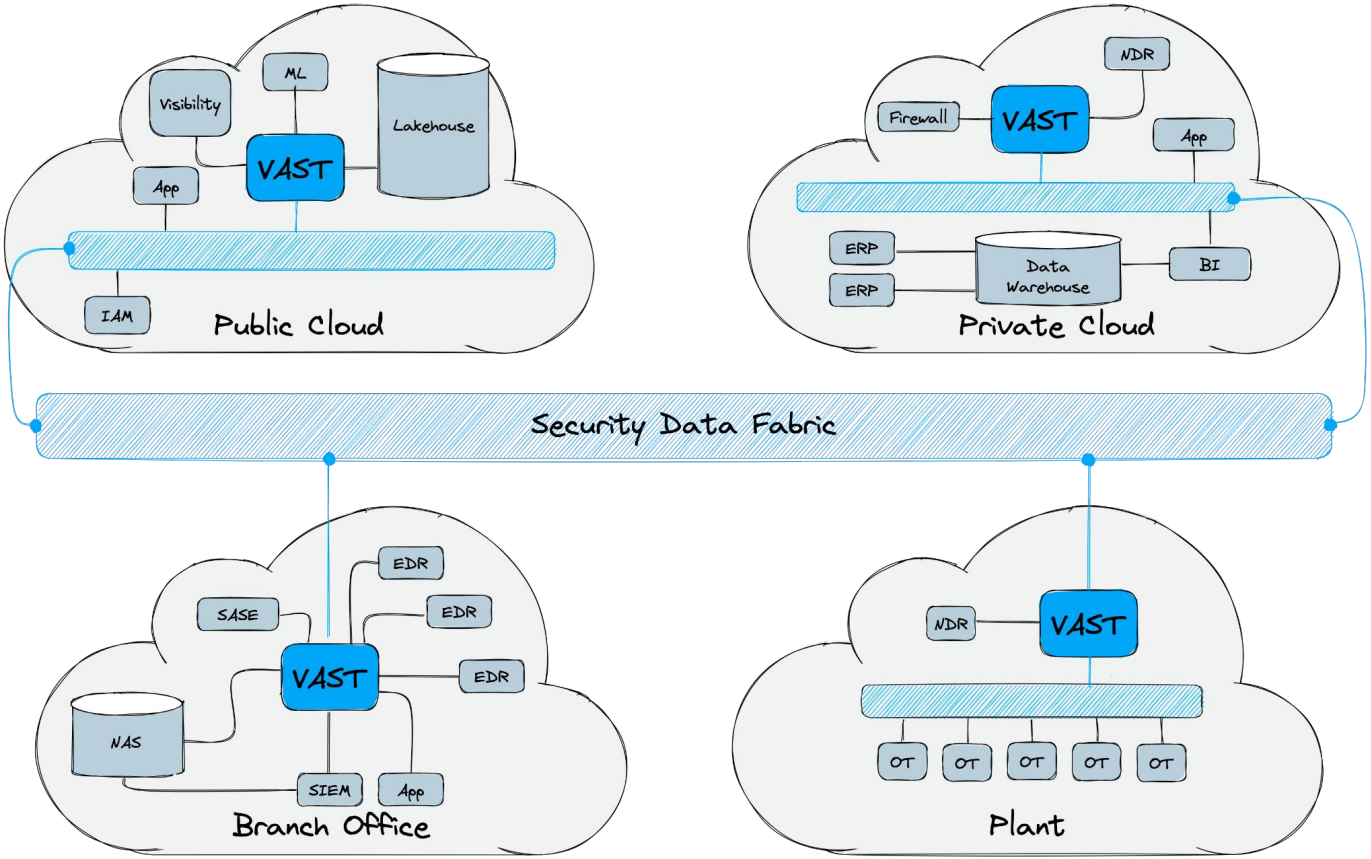
Our Solution: a Sidecar for the SOC



Benefits

- ✓ **Open & standardized security control and data plane**
  - → Implement tool-independent use cases
  - → Full access to data in a standardized representation
- ✓ **Sustainable SOC architecture**
  - → Optimal number of integrations (connect once, use everywhere)
  - → Easy on/off-boarding of tools enables best-of-breed approach
- ✓ **Federated deployment at the edge**
  - → Easily adhere to data residency requirements
  - → Reduce cost and and load in data-intensive tools (e.g., legacy SIEM)

Federated Deployment



Free and Open Software

https://vast.io

Join our Community Slack!

http://slack.tenzir.com

Summary

Our Vision: heterogeneous security solutions interact autonomously on top of a common open platform built on open-source principles.

Our Mission: To deliver an open data platform for building sustainable cybersecurity architecture.

Our Team: decades of industry experience coupled with outstanding academic and engineering capacity to solve the hardest problems in cybersecurity.

TENZIR

Join us on our mission!

Our Business Model: a simple subscription-based mechanism that include customer success services.

Our Opportunity: perfect timing to disrupt the highly fragmented, under-staffed security operations market.