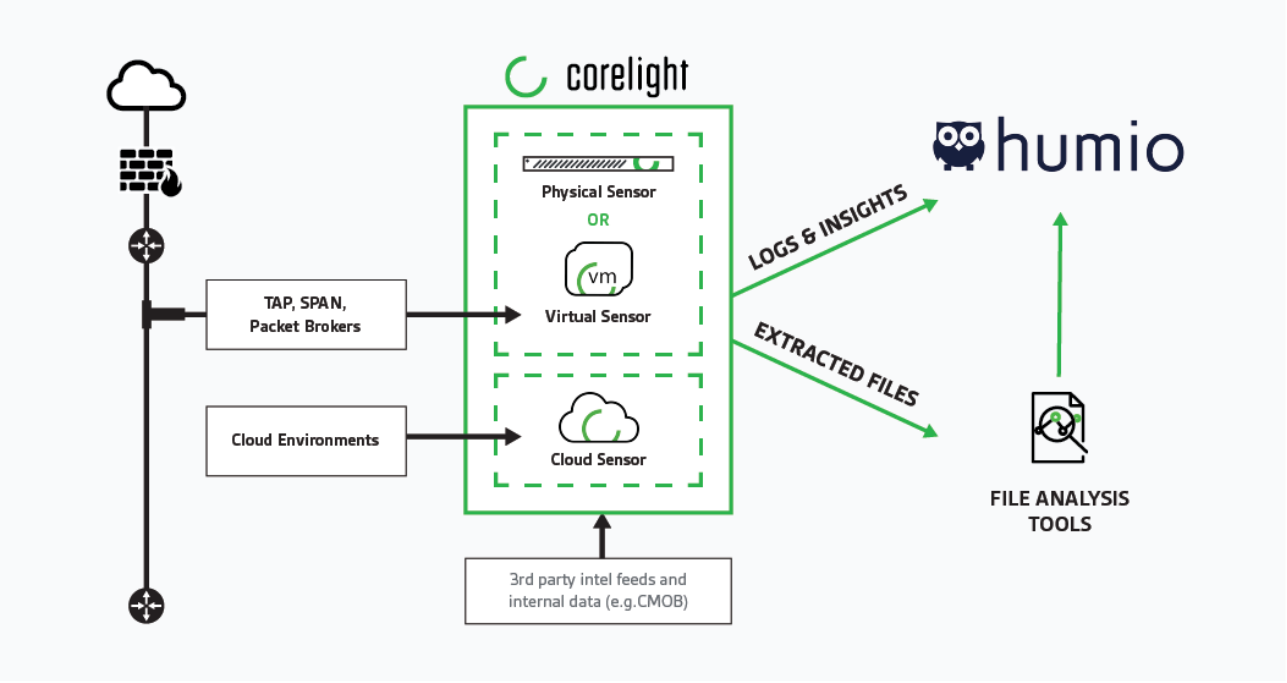
Joint Solution

Comprehensive network security monitoring with fast, scalable log management

Since nearly all attacks must cross the network, it's an essential source of truth, yet common logs like Netflow or DNS records provide few details and often leave security teams in the dark. Full packet capture, while comprehensive, is cost-prohibitive to store at scale and slow to search. Corelight transforms raw traffic into protocol-rich, connection-oriented logs that comprehensively summarize network traffic at less than 1% the size of full packet capture so incident responders and threat hunters can make lightning-fast sense of their network traffic and move at the speed of attack.

The Corelight/Humio solution:



Joint Solution: Corelight and Humio

When it comes to storing and analyzing rich logs like these, however, organizations can find themselves data-constrained by their SIEM's pricing model and encountering undesirable latencies in query responses at scale. Humio's innovative data storage and in-memory search/query technologies provide customers with a cost-competitive log management platform that enables real-time data observability, while requiring significantly less hardware and engineering resources than comparable tools.

Corelight and Humio have partnered to combine comprehensive network security monitoring with fast and flexible log management so customers don't have to compromise and can capture, store, and quickly make sense of all of their network traffic. This integrated joint solution streams Corelight's network logs and insights to Humio's platform so security teams can observe their networks in real time, driving faster incident response times and unlocking powerful new threat hunting and detection capabilities.

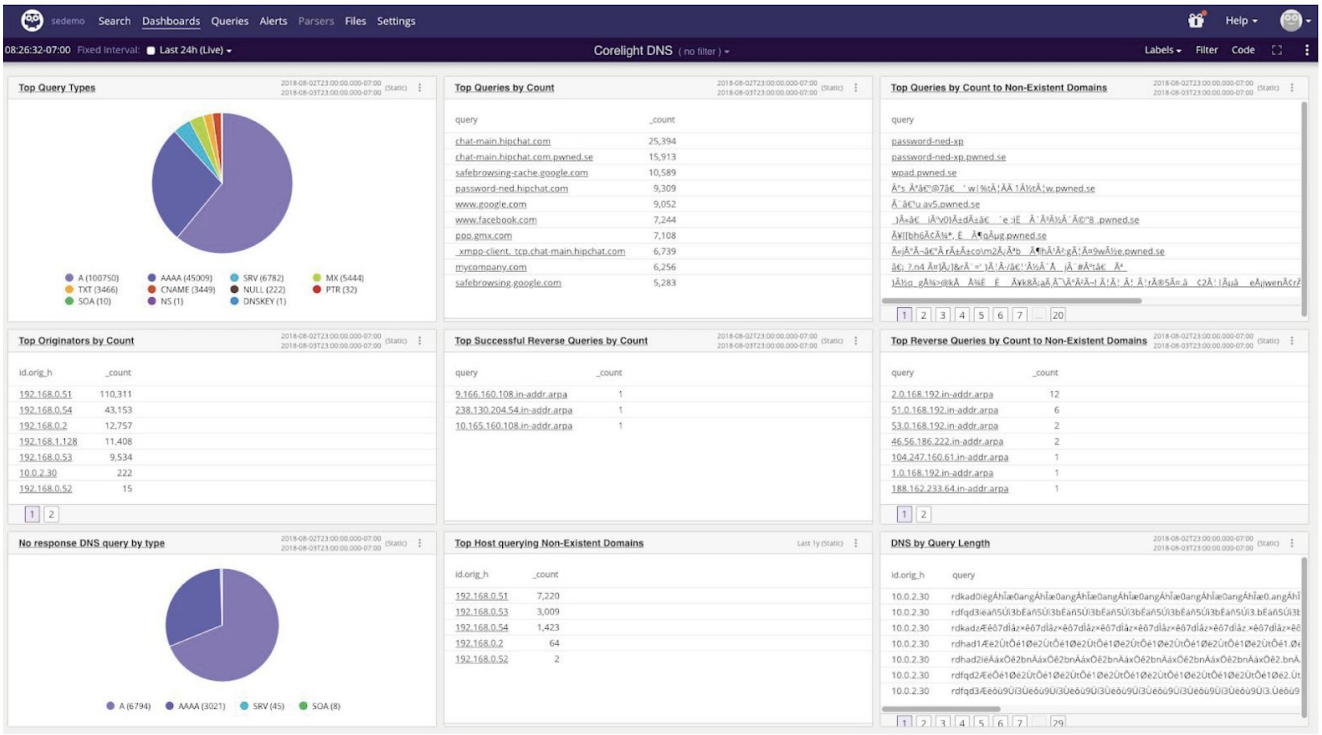
Corelight Sensors operate out-of-band and transform raw traffic into rich logs, extracted files, and security insights using a specialized version of the open-source Zeek (formerly 'Bro').Security teams can stream Corelight's logs and insights directly to the Humio platform for search and analysis. The Humio platform can run on-premise or in the cloud, via self-hosting, public cloud or Humio Cloud. Humio's platform enables 5-20x data compression datastore, sub-second ingest, and lightning-fast, full text search without indexing. Together, Corelight and Humio enable powerful incident response and threat hunting use cases such as:

- **Resolving phishing incidents faster** - take phishing alerts and pivot in Humio from the flagged domain directly into the corresponding Corelight http.log and files.log to see that a malware payload was downloaded when the link was clicked.
- **DNS-based threat discovery** - hunt through Corelight's dns.log in Humio to look for evidence of threats like DNS tunnelling by quickly filtering and identifying suspicious DNS queries extra long character counts that contain encoded strings.
- **Uncover hidden C2 communication** - spot c2 communications in Humio by reviewing Corelight's dpd.log that shows protocols on non-standard ports, such as attackers trying to disguise their C2 traffic in a purported SSL connection.
- **Blacklisting & Whitelisting SSL connections** - use Corelight to enable the JA3 Zeek package that fingerprints SSL connections and create SSL connection blacklists and whitelists to monitor in Humio.
- **And more**...

Corelight Dashboards in Humio

The Humio platform aggregates and visualizes data in true real-time, enabling live observability and insights into the data on top of which you can build and share rich dashboards monitoring key activities or metrics across the security team. Corelight has pre-built security-specific dashboards in the Humio platform that track leading indicators of security risk such as expired SSL certificates or DNS queries to non-existent domains. Use these dashboards as a launch point for investigations:

Joint Solution: Corelight and Humio



Use Corelight to transform traffic into security visibility and insight

Corelight Sensors run a specialized-version of open-source Zeek to deliver best-in-class network security monitoring so security teams can make fast sense of traffic and move at the speed of attack. Unique capabilities of Corelight include:

- Physical, virtual and cloud-based sensors
- Up to 25 Gbps of monitored traffic per sensor
- A fleet management GUI for multi-sensor deployments and hybrid environments
- Sensor performance and health monitoring
- Optimized file extraction capabilities supporting 10,000+ file extraction per minute
- Flexible export options, including data formats, filtering and forking
- Shunting to handle network traffic / elephant flows over 25 Gbps (AP 3000 only)
- Support from the creators and builders of Zeek

Use Humio to get full visibility from ALL Your Corelight Data

Humio is a purpose-built, time-series database that streams massive log volumes in real-time and scale. Sending all Corelight logs and other relevant data sources to Humio's aggregated platform allows you to quickly answer critical security questions.

Humio directly ingests and stores Corelight's network logs and extracted files via API and enables incident responders and threat hunters to instantly search and visualize both streaming and historical data in Humio dashboards for any infrastructure including on-premises and in the cloud.

Joint Solution: Corelight and Humio

Unique capabilities of Humio include:

- Flexible, live dashboards for Zeek data
- Scalable to handle multiple TB/day log volumes (handles 1 TB/day ingest on a single instance)
- Live and instant dashboard and search capabilities
- Real-time alerting
- Ad-hoc search capabilities using a simple unix pipe search language
- Available on-premises or in the cloud
- Low TCO - significantly lower license and resource cost vs. competitive solutions

Humio is a solution built specifically for aggregating, exploring, reporting, and analyzing data in real-time. It gathers log data from a range of sources and can be deployed in both cloud and on-premise environments. Humio's innovative data storage and in-memory search/query engine technologies provide a cost-competitive log management and analysis solution that requires significantly less hardware, engineering resources and licensing costs vs. competing solutions.

Humio's live observability platform enables data aggregation, exploration, reporting and analysis from a range of sources ingesting massive volumes of log data instantly and is deployable on any infrastructure including both in the Cloud and On-Premises. The purpose-built, innovative data storage and in-memory search/query engine technologies provide developers, security teams and operations managers a cost-competitive log management and analysis solution, all while requiring significantly less hardware and engineering resources. For more information visit https://www.humio.com/ or follow @MeetHumio.

Defenders have always sought the high ground in order to see farther and turn back attacks. Corelight delivers a commanding view of your network so you can outsmart and outlast adversaries. We capture, interpret, and connect the data that means everything to defenders.

info@corelight.com | 888-547-9497