Deep Network Traffic Visibility with Fast, Flexible Log Management

A joint solution from Corelight and Humio

Managing a Sea of Security Alerts and IT Logs

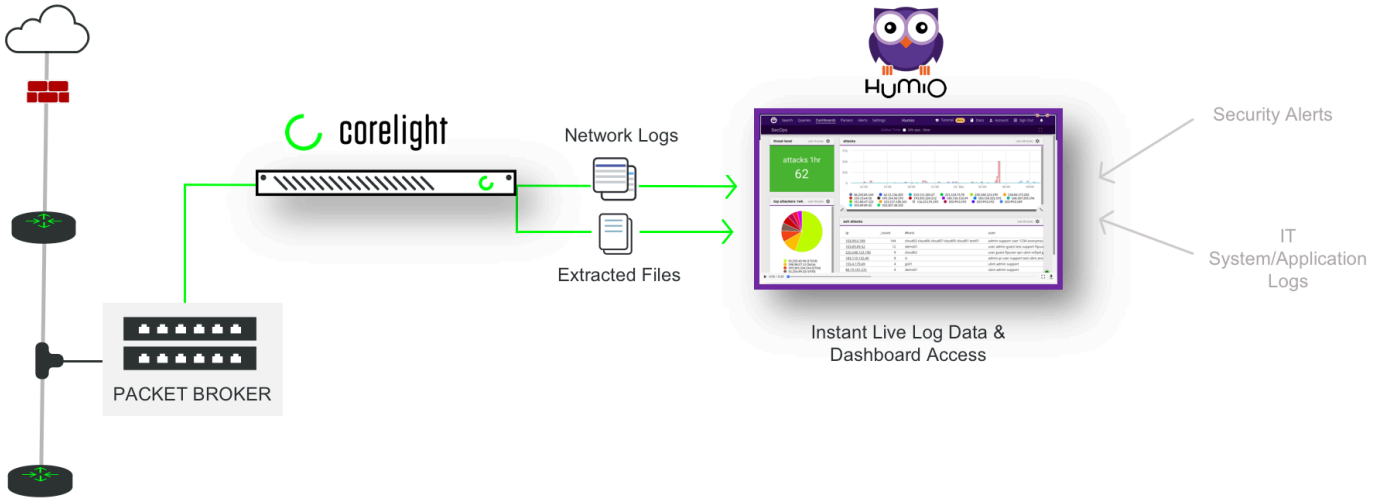
Triaging today's deluge of security alerts can overwhelm even the most well-staffed security teams. Similarly, modern IT tools and appliances generate huge log volumes that present thorny storage and search challenges for IT management.

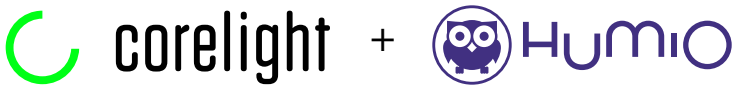
Incident responders rely on network data as a foundational source of truth to resolve security alerts, but common network data sources either fail to provide the full picture (e.g. NetFlow) or make storing and searching the full picture (i.e. PCAP) too difficult and cost-prohibitive to scale. Without comprehensive and readily-actionable network data it can take incident responders hours or even days to diagnose and resolve a single security alert.

In much the same way, the modern proliferation of IT tools and appliances has created an ocean of disconnected operational logs that can make the task of answering simple questions such as "Is a new deployment causing errors?" or "Are my systems up?" a maddening mystery. While common log management solutions make centralizing and searching logs easier they can also come with prohibitively high costs and can introduce complex query languages and undesirable latencies in query responses.

So how do you achieve both comprehensive, actionable network visibility and fast, affordable log management?

The Corelight and Humio Solution





The Corelight and Humio Solution --- Continued

This powerful solution pairs deep network traffic analysis and logging from Corelight with expedient and affordable log management from Humio that allows organizations to get fast, precise answers to critical security and IT questions about their environment.

The Corelight Sensor operates out-of-band and uses high performance hardware and a specialized version of the open-source Bro network security monitor to ingest network traffic, transform it into rich network logs and extracted files, and export this data directly to Humio. Corelight's sensor summarizes every network event across more than 35 different protocols and creates logs comprised of hundreds of fields, but with storage costs that are just a small fraction of the equivalent cost of storing full network traffic. In short, with Corelight you get nearly the fidelity of the full network packet capture at a fraction of its cost. The rich nature of Bro logs enables faster incident response times and more powerful threat hunting capabilities through better network evidence.

Key features of Corelight's sensor include:

- High performance 10+Gbps peak analysis throughput
- Simple, 15-minute sensor configuration and deployment
- Optimized network file extraction and reassembly
- A custom operating system designed for secure sensor operation
- Automatic sensor updates, feature enhancements, and monitoring
- World-class support from the definitive Bro experts

Use Humio to get full visibility from ALL Your Corelight Data

Humio is a time series log management solution that provides a fast (streaming) way to use and access Corelight log data. Answer critical security questions by sending ALL Corelight logs and other relevant data sources to a single place. Humio lets you instantly turn your data into usable information to answer your questions in the context of other data in your environment within a specific timeframe. From there, you can save and share what you found, and view all of your network data chronologically.

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 the data in Humio dashboards, supporting both on-premise and cloud-based requirements.

Unique capabilities of Humio include:

- Flexible, live dashboards for Bro 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 query language
- Available on-premise 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.

Customer Outcomes

Through integrated deployments of Corelight and Humio organizations have achieved substantial improvements in incident response, threat hunting, and IT analytics workflows, including:

- Dramatically reducing average incident response time
- Dramatically reducing log management costs
- Unlocking new threat hunting capabilities with deeper traffic visibility
- Unlocking visibility into new IT systems previously limited by log management costs
- Reducing average log query times and enabling real-time log querying and monitoring
- Reducing false positive security alerts through accurate, network-derived logs

About Corelight

Corelight delivers the most powerful network visibility solutions for information security professionals, helping them understand network traffic to detect, stop and remediate cyber attacks. Corelight built its first solution incorporating Bro, the powerful and widely-used open source framework that provides a comprehensive, real-time understanding of the traffic on the network. Corelight is based in San Francisco, CA. For more information, visit https://www.corelight.com or follow @corelight_inc.

About Humio

Humio is a solution for aggregating, exploring, reporting and analyzing log 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 has offices in London, UK, San Francisco, CA and Aarhus, DK. For more information visit https://www.humio.com/ or follow @MeetHumio.

Corelight Sensor

Transform network traffic into high-fidelity data for your security teams. Designed by the creators of open source Bro, the Corelight Sensor is a turn-key solution tuned for performance at enterprise scale. Configure in minutes, and gain exceptional visibility into your network activity.

info@corelight.com

510-281-0760

corelight.com

bro.org

Evaluate a unit for 30 days. Call us.