White Paper

5 ways Corelight data helps investigators win

How Corelight data puts your SOC on top

Corelight's Network Detection and Response (NDR) solution—built on Zeek—helps your analysts do their jobs better by transforming network traffic into data that's faster, more useful, more powerful than anything else out there. Here's why:

1. Corelight data gives analysts everything they need—it covers all the network protocols investigators need in granular, actionable detail

2. Corelight data makes search fast & simple—it's formatted, organized, and interlinked so analysts find what they need, fast

3. Coreight gives your team access to extracted files—it can scalably extract every file that crosses the network

4. Corelight sees through protocol deception—it provides Dynamic Protocol Detection for deception and errors

5. Corelight gives analysts amazing flexibility—built-in scripting language offers customization, automation and analysis

In contrast to too much data (PCAP) and too little (NetFlow), Zeek offers just the right amount of data, without sacrificing context or usability.

Here's how Chris Sanders, security researcher, SOC trainer, and author of the best-selling Practical Packet Analysis, sees it:

> The only place Zeek data doesn't get a perfect score is in Acquisition, where Sanders notes that it's "difficult to customize" and requires a lot of horsepower to collect and process. But this is based on open-source Zeek, and Corelight delivers enterprise-grade Zeek on plug-and-play sensors

Corelight data gives analysts everything they need

Rather than using a patchwork of various appliances and security tools such as DNS and firewall logs, that's limited in scope, difficult to cross-analyze, Corelight gives you a comprehensive, security specific picture of what's happening on your network. Our Zeek logs cover 35+ different network protocols, and support for analysis of new protocols can be added as desired.

Example Zeek log detail for DNS request

1. Timestamp (308930716.700706)—this timestamp is precise to the microsecond, and derived from the network itself via NIC hardware. Incident response is all about reconstructing a narrative, so accurate event timestamps are key.

2. Connection unique identifier (CUID)
(CNFhPo1bq5dJD3wzJ6)—this UID specific to the connection and allows an investigator to easily 'pivot,' exposing all associated logs and understanding what came before and after— far more efficient than manually matching timestamps.

3. A more complete call detail record (172.16.238.131 54304 172.16.238.2 53 udp)—this makes up the 5-tuple: the source IP & port (172.16.238.131 54304), the destination IP and port (172.16.238.2 53) and the protocol used (udp)—details omitted by DNS server logs.

4. Round trip time (0.004850)—measured in seconds, this value could potentially reveal a man-in-the-middle attack, network misconfigurations, and/or significant network performance problems.

5. The content of the response (74.125.225.81,74.125.225.82, etc.) The victim gets a malicious IP address back, and it disappears from the cache after only a few seconds. But this data reveals exactly what the client saw.

Corelight data makes search fast & simple

With highly interlinked, structured, searchable data, your security team can be vastly more productive, limiting business risk by identifying and remediating issues before they spread. What makes Corelight's Zeek logs better for search? First, they're in a single, accessible log format, which can be exported to any

SIEM or data pipeline, and second, they're specifically formatted and linked. There's no need to ingest and cross-analyze network data from different sources.

Corelight's logs give you connection and application-layer data—content that matters most. Hundreds or thousands of packets could be transmitted in the download of a single, potentially-malicious PDF. Zeek assimilates and analyzes all those packets, compactly logging key elements of the file transfer. This data is hard to extract from PCAP, and impossible to extract from NetFlow.

The advantages of Corelight data

1. All signal, no noise: The relevant, human-readable data summarizing the connection, file event, and HTTP stream is recorded, not raw PCAP.

2. Connection UID and File UID: Only Zeek gives you these unique IDs, labelling the file so you can pivot quickly to other connections, enabling search across all logs related to that connection (DNS, HTTP, file, etc.).

3. File hashes: Zeek generates the MD5, SHA-1, and SHA-256 hashes for all files, so responders can check them against malware repositories, blacklists, and other Zeek logs.

Coreight gives your team access to extracted files

High-performance file extraction and reassembly is difficult for many reasons, including identifying the protocol, identifying and reassembling the packet stream, extracting the file embedded in the application dialog, and scaling the extraction under heavy load. Turning on file extraction in other vendors' products will often negatively impact performance.

Corelight, however, excels at file extraction at scale by attempting to fully parse the protocol, and robustly identifying it. Corelight's optimized export pipeline will not re-extract duplicate files traversing a network, allowing the sensor to scale in high-throughput environments without significant drops or negative impacts to other sensor analysis capabilities.

Corelight can't be fooled by protocol deception

Most network protocols use well-known ports, but attackers can send traffic over any port and often do, by hiding on non-standard ports (e.g., sending their HTTP traffic over the SSH port). Instead of relying on ports or simple signatures to identify protocols, Zeek uses parsing validation to analyze the content of the connection and verify the protocol in use. This can uncover situations such as the following example. where an attacker hid their C&C communications inside of what appears to be an SSL connection.

{"_path":"dpd","_write_ts":"2018-01- 15T17:11:57.552839Z","ts":"2018-01-15T17:11:5 7.552839Z","uid":"CpPNAD4SAqvPZf0h5b","id. orig_h":"1.2.3.4","id.orig_p":3908,"id.resp_h":"5.6.7.8","id. resp_p":443,"proto":"tcp","analyzer":"SSL","failure_ reason":"Invalid version late in TLS connection. Packet reported version: 4753"}

A Zeek DPD log for an alleged SSL connection

In the Zeek log shown above, we can see the host (1.2.3.4) and server (5.6.7.8) SSL handshake and each hello parses correctly as SSL. The next packet should also parse as an SSL data packet, yet it fails, showing that this connection is not, in fact, SSL. It's an attacker attempting to hide a backdoor by disguising their communications. Corelight automatically detects this kind of protocol evasion at scale.

Corelight gives analysts amazing flexibility

Zeek opens up a huge range of possibilities for analysts because it includes a built-in scripting language, scripts can be created that deal with logs after they're written or before the data is generated. Any Zeek log can be customized to include new details, and entirely new Zeek logs can be generated. This capability also allows teams to automate analysis like threat detection and network performance monitoring.

The Zeek Intelligence Framework is one of the most widely used script frameworks in the Zeek community. If you specify a DNS name to monitor, for example, the script will look across all protocols and alert whenever that DNS name appears.

This makes Zeek a more flexible and extensible option, allowing you to decide exactly what data you want and how to analyze it. This stands in stark contrast to most products today, where the analysis logic remains opaque and customers must rely on the vendor to update coverage for the latest threats. Additionally, the 20+ year history of Zeek's open-source community means that Corelight customers can leverage existing community scripts.

[1] Saldich, Alan. Corelight, Inc. *Bro is an IDS. Not, It's Not.* 2018. http://www3.corelight.com/bro-is-an-ids-no-its-not
[2] Grading criteria and grades developed by Chris Sanders, Founder at Applied Network Defense. www.investigationtheory.com
[3] Kreibich, Christian. Corelight, Inc. *Extensibility as a Guiding Principle*. 2017. https://corelight.blog/2017/12/06/extensibility-as-a-guiding-principle/
[4] Mens, Jan-Piet. *BIND querylog: know your flags*. 2011. https://jpmens.net/2011/02/22/bind-querylog-know-your-flags/
[5] Image licensed for Corelight commercial use from: www.istockphoto.com. The image download event cited in the paper came from: http://blogs.teradata.com/data-points/wp-content/uploads/2014/02/Open-Your-Mind-to- All-The-Data3-983x1024.jpg
[6] Script source: https://github.com/salesforce/ja3

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