

## White Paper

# Alerts, meet evidence

Find and address threats that matter with Suricata IDS + Corelight network evidence

Corelight allows your organization to evolve beyond a standalone intrusion detection system. Get an IDS with rich network context that lowers mean time to respond (MTTR) by revealing incident scope and impact. Corelight fuses signature-based alerts with corresponding network telemetry, delivering ready-to-investigate packages to Corelight Investigator or your SIEM/XDR.

## Zero in on true positives



Analysts receive Suricata alerts and Zeek logs packaged at the SIEM, ready for investigation. Alerts linked to network evidence let them follow the trail of an attack, making it far faster to know which alerts to escalate and which to close.

## White Paper: Alerts, meet evidence

### Resolve critical cases with speed and accuracy

By integrating alerts and evidence, you can speed up critical workflows: before, during, and after attacks:

#### Triage


SOC teams bottleneck when triaging noisy IDS alerts because validation requires more context than what's included with the alert. Analysts need more time or significantly more context. Otherwise, they risk escalating false positives or ignoring alerts that aren't as benign as they thought. Corelight provides the SOC with pre-correlated network evidence that's linked to every Suricata IDS alert, enabling SOCs to triage each alert confidently and efficiently.

#### Investigate

When a zero-day threat is announced, most IDS systems are blind to the threat until the signature is tested, published, and enabled, leaving organizations vulnerable while they wait. Using Corelight network evidence integrated with Suricata IDS, SOCs can immediately use it as a hunting ground for signs of the zero-day, gaining an early start in protecting operations ahead of the signature release.

#### Remediate

When a threat is detected, incident responders need to react quickly to contain, eradicate, and remediate to disrupt or limit the impact of an attack. But when all you have is an IDS alert with some limited telemetry to start with, containment activities are stalled until response teams can complete an extended investigation to assess the scope of the threat. Corelight NDR significantly reduces the time to assess the scope of the attack, identify what was impacted, and validate confidently that eradication and remediation were successful.



### Help defenders level up their skills

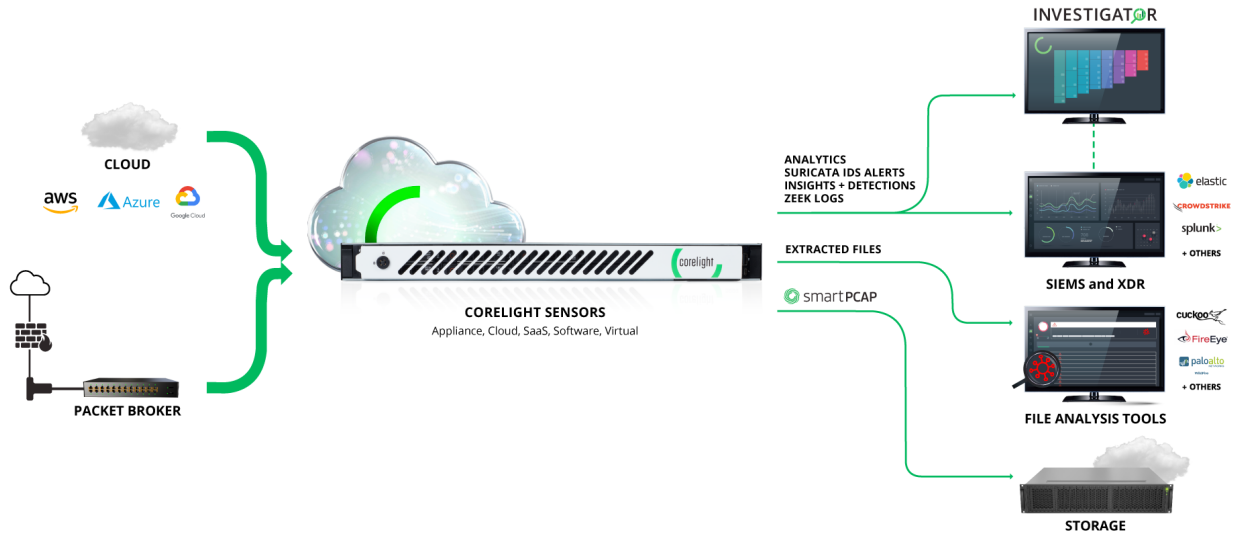
Are you helping your team keep learning and stay engaged beyond investigation and remediation? Corelight network context provides knowledge that builds critical expertise, increasing employee satisfaction and retention.

### How it works

Corelight integrates the best of open-source technologies: Suricata's signature-based alerting capabilities and the global standard for network telemetry, Zeek®. When an IDS alert is triggered, Corelight packages the alert with its full network context and delivers it to your SIEM or XDR. This package includes a unique link that makes it easy to find related data. Corelight also enables Zeek logs to be linked with other data sources like firewalls or EDR. For organizations that require packets, Smart PCAP is an option that fits seamlessly into our Open NDR platform.

**Instrumentation**

Corelight Sensors sit out-of-band, generating alerts and capturing evidence across a wide set of protocols to provide information often missing from SOC datasets, such as DNS activity. This correlated evidence reveals user behavior, websites visited, files downloaded, the spread of information, and more—succinctly organized for each unique connection.



To see Corelight’s Suricata IDS solution in action, request a demo with one of our experts today: <https://go.corelight.com/demo-corelight-suricata-ids>



Corelight provides security teams with network evidence so they can protect the world’s most critical organizations and companies. On-prem and in the cloud, our open Network Detection and Response platform enhances visibility and analytics, leading to faster investigations and expanded threat hunting. Corelight’s global customers include Fortune 500 companies, major government agencies, and large research universities. Based in San Francisco, Corelight is an open-core security company founded by the creators of Zeek®, the widely-used network security technology.

**info@corelight.com | 888-547-9497**

*The Z and Design mark and the ZEEK mark are trademarks and/or registered trademarks of the International Computer Science Institute in the United States and certain other countries. The Licensed Marks are being used pursuant to a license agreement with the Institute.*