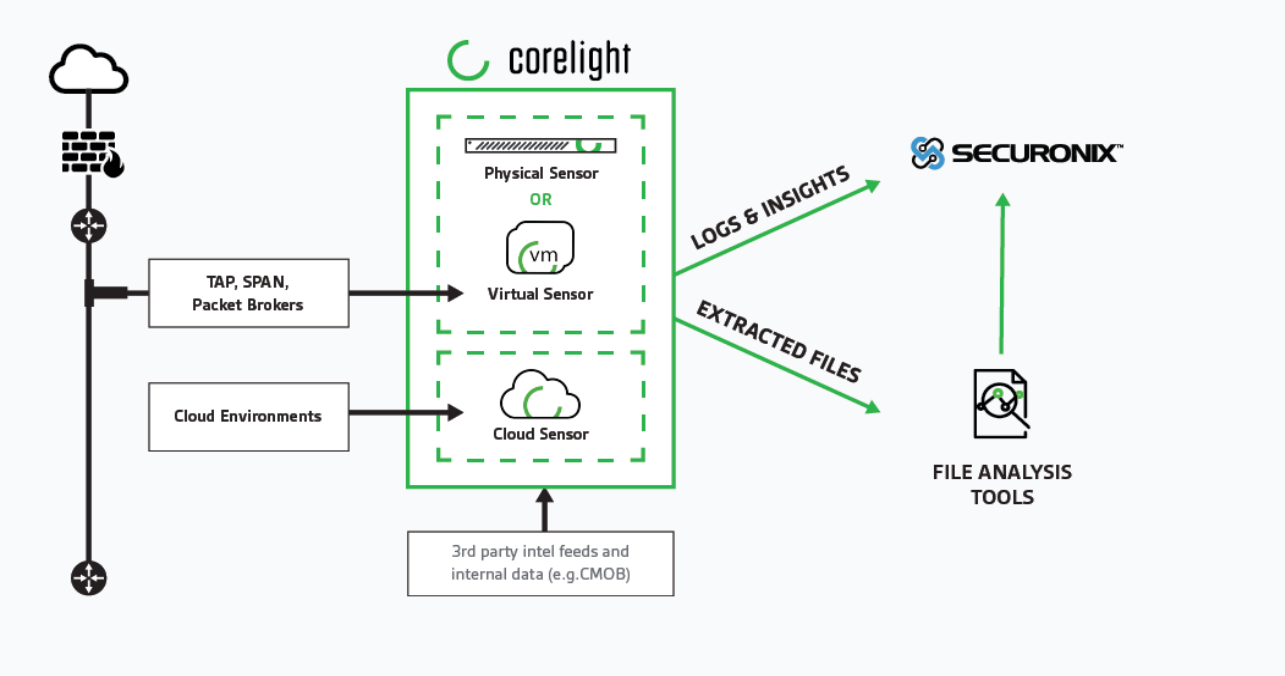
Joint Solution

One vantage point, continuous advantage: Corelight + Securonix NTA

Low and slow attacks are some of the most dangerous and hard to detect. Typically carried out by sophisticated adversaries with specific targets, these attacks take place over weeks or months. They're tough to spot because they can involve many disparate actions across different systems and tactics.

The Corelight / Securonix solution:



This powerful integration pairs deep network traffic analysis and logging from Corelight with Securonix's real-time enrichment and machine learning capabilities.

Joint Solution: **Corelight and Securonix**

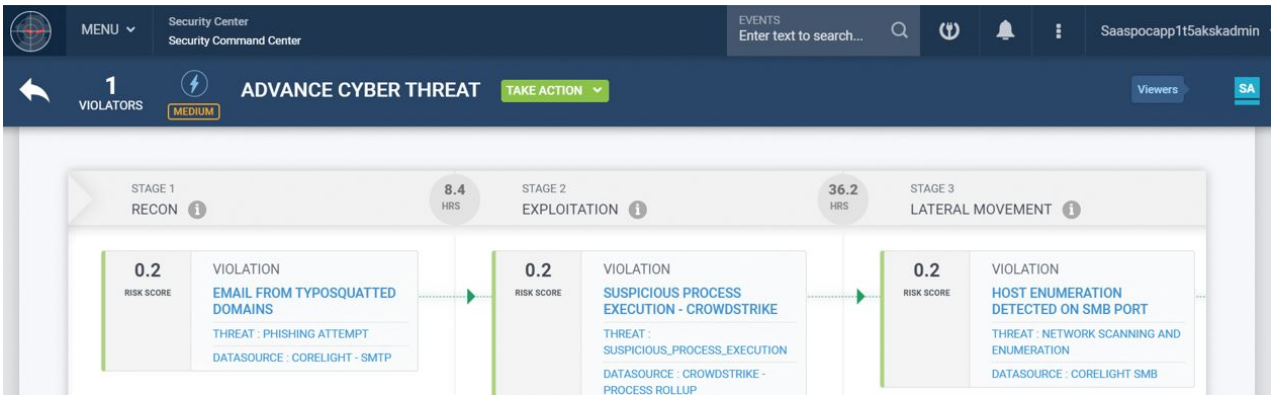
While stand-alone tools can monitor traffic and detect network traffic anomalies, without user and system context they can add to the noise. Traditional SIEM solutions have the same problem unless they ingest network traffic metadata.

Securonix NTA, fed by Corelight, gives you a single platform that monitors and correlates network data, security events, and user activities (with built-in UEBA) to detect the most advanced threats. Incident responders can use the solution, together with the MITRE ATT&CKTM framework, to help organize the indicators of compromise from NTA, SIEM, and UEBA. By unifying all this information, defenders can surface high-risk threats and break or interrupt the adversary kill chain.

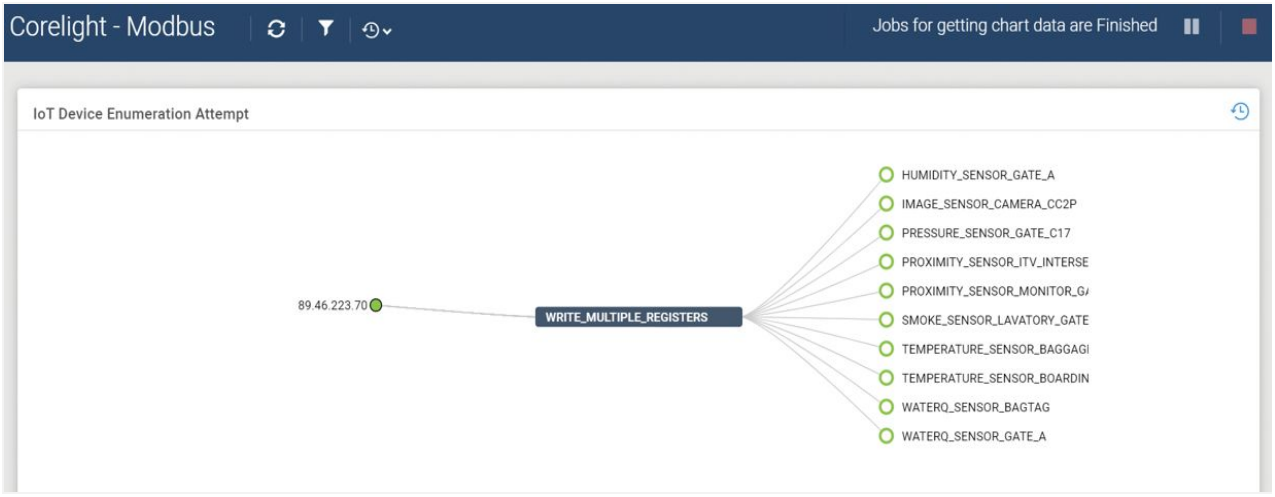
Close network visibility gaps and accelerate incident response

Corelight, powered by open-source Zeek (formerly Bro), details network activity across dozens of protocols, reassembles and extracts hundreds of file types and enables custom security insights to preserve this key source of truth. Securonix NTA combines data from Corelight Sensors which provide real-time insight by extracting more than 400 data elements from network traffic in real-time across dozens of protocols and data types. Securonix ingests this data using built-in connectors and enriches it with relevant user, entity, behavioral, and threat intelligence context. The integrated network analysis and threat model content triggers alerts and combines it with other indicators of compromise using the MITRE ATT&CK framework as a construct. Securonix then surfaces the actionable threats so analysts can quickly investigate and remediate in real-time.

Corelight automatically streams rich network data to Securonix, providing security teams faster, deeper, and more actionable insights that can reduce incident response time by up to 20x. This data serves as a centralized source of truth to investigate and rapidly respond to security incidents, replacing Netflow and augmenting low-level server logs spread across different business units outside the security team.



Interdict attacker behavior at multiple points in the kill chain by combining network data with user behavior.



Perform link analysis to visualize the attack pattern and interconnections between attacker, victims and data.

Zeek: The gold standard for network security.

Corelight runs on Zeek, the powerful, open-source network analysis tool that has become a global standard. Thousands of the world's most critical organizations use Zeek to generate actionable, real-time data to help defend their networks.

Zeek extracts over 400 fields of data in real-time, directly from network traffic. It covers dozens of data types and protocols from Layer 3 to 7, including TCP connections, SSL certificates, HTTP traffic, emails, DHCP, and more. Zeek logs are structured and interconnected to support threat hunters and incident responders.

Corelight Sensors—available in physical, cloud and virtual formats —vastly simplify the challenges deploying open-source Zeek. They offer excellent performance, combine the capabilities large organizations need with high-end, out-of-band hardware and a specialized version of the open-source Zeek network security monitor.

Corelight Sensor capabilities include:

- Up to 25 Gbps+ of monitored traffic per sensor
- Hardware, cloud or virtual appliance models
- A web-based sensor management GUI
- Fleet Manager to manage up to 250 Corelight Sensors
- Pre-installed collections of Zeek packages
- A comprehensive API
- On-box performance and health monitoring

Joint Solution: Corelight and Securonix

- Dynamic file extraction
- Flexible export options, including popular data formats, filtering, and forking
- Shunting to handle elephant flows over 25 Gbps (AP 3000 only)
- Support from the creators and builders of Zeek

Securonix is redefining the next generation of security monitoring using the power of machine learning and big data. The Securonix solution provides unlimited scalability and log management, behavior analytics-based advanced threat detection, and intelligent incident response on a single platform. Globally, customers use Securonix to address their insider threat, cyber threat, cloud security, fraud, and application security monitoring requirements. Contact Securonix at www.securonix.com.

info@securonix.com | 310-641-1000

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