White Paper

Maneuver: the cybersecurity strategy needed for the next ten years

Knowledge-driven security with Corelight & Splunk®

Introduction

Advanced adversaries outflank defenders by weaponizing time and knowledge against their target, eviscerating millions of dollars in cybersecurity investments by taking the time to understand the target environment better than the victim. Unfortunately, organizations who respond tactically to this challenge with incremental technology investments continue to lose these battles.

Instead, organizations need a seismic shift in cybersecurity strategy to refocus their mission to build a knowledge advantage against adversaries via superior operational awareness. Knowledge advantage is not a better machine learning algorithm. Knowledge advantage means having operational awareness of your digital environment and the ability to act on that awareness.

This strategy is called "Maneuver" and it involves instrumenting and operationalizing unified telemetry across your environment to leverage turnkey and create bespoke workflows that drive effective security response at scale - creating coverage zones that adversaries cannot avoid. Maneuver drives operational awareness by filling the dark crevices of your digital environment with unified data and analytics that adversaries can't avoid, thereby leaving evidence of their techniques, tactics and procedures (TTPs).

To successfully employ the Maneuver Strategy organizations must know their networks. Advanced adversaries fear environments with comprehensive network security monitoring in place because they know they cannot avoid the coverage zones. Even America's own elite cyberwarfare unit has acknowledged this fact:

> ***"One of our worst nightmares is that out-of-band network tap that really is capturing all the data, understanding anomalous behavior that's going on, and someone's paying attention to it. You've gotta know your network. Understand your network, because we're going to."***
>
> - *Rob Joyce, Former Chief of Tailored Access Operations, NSA*

Corelight provides security teams unsurpassed network knowledge and organizations that operationalize this knowledge with Splunk solutions eliminate dark crevices adversaries use to hide. Your decision to invest in Splunk was a strategic one, and adding Corelight leverages the value of that investment by creating a strategic network data reserve your defenders can use to outmaneuver adversaries for the next ten years.

Maneuver with Corelight and Splunk

Corelight integrates deeply across the Splunk portfolio and this joint solution can dramatically improve incident response times and threat hunting capabilities, as well as automate response and remediation, while unlocking powerful bespoke threat detection capabilities. Nearly all attacks cross the network; Corelight shines a light on them, where legacy sources of network knowledge (i.e. Netflow) leave you in the dark.

Without Corelight data in Splunk, adversaries roam freely across your unmonitored network space:

WITHOUT CORELIGHT
Adversaries roam freely across the entire space
Defenders operate in a much smaller subsection of this space

Corelight captures detailed, context rich network telemetry while Splunk provides the tools to operationalize it. Together, Corelight and Splunk illuminate the dark corners of your network, leaving adversaries with nowhere to hide:

Corelight and Splunk are foundational tools for implementing the Maneuver Strategy, which supports security initiatives ranging from machine learning to Zero Trust architectures. The following sections discuss the benefits of this joint solution to your organization.

Accelerate data onboarding

Legacy sources of network knowledge create serious data onboarding challenges in Splunk, forcing defenders to create data pipelines from a wide variety of sources, to normalize variable data formats, and hope that they bring sufficient detail to answer security questions. This data ingest morass slows SIEM implementation and prevents your team from taking advantage of turnkey Splunk analytics in tools like Enterprise Security, Security Essentials, and SOAR. Corelight provides a single, unified source of network truth that overcomes these challenges.

Corelight delivers the industry gold standard for network knowledge - open source Zeek - and has invested heavily to ensure Corelight data integrates seamlessly within the Splunk ecosystem. We have hundreds of customers around the world, including many nation state entities in the defense and intelligence space. The majority have implemented Corelight with Splunk.

Corelight provides comprehensive coverage of all relevant network connections - both north/south and east/west. The result is a context-rich summary of network connection data that is mapped to Splunk's Common Information Model (CIM), without any additional administrator effort. Instead of spending months or even years data onboarding into Splunk, Corelight customers can send a unified stream of data to their Splunk instance in a matter of minutes.

Force multiply your security teams

Ever-increasing alert volumes and chronically underfilled talent pools stretch SOCs thin and create an environment where breach detection is exceedingly difficult. Corelight and Splunk SOAR can reduce alert noise, eliminating wide swaths of alerts before they hit the human chain, providing precious time to develop your analysts so they can address bigger challenges. Corelight data is comprehensive, interlinked, and enriched with unique security insights so analysts can automate investigative tasks in SOAR with lighting speed and efficiency. For example:

- Filtering out false positives from an IDS
- Evaluating the scope of an incident
- Identifying mismatches between file content and file extensions
- Performing initial analysis of possible malware
- Enabling in-depth file analysis through high-speed file extraction

What can be automated can be accelerated. Corelight and Splunk have been shown to reduce average incident response time by 95%,[1] force multiplying security analysts by making them dramatically more efficient. With Corelight your team can field the same Splunk tools, interfaces, and query languages on which they've already trained to hit the ground running, achieving higher throughput with less people.

Support Zero Trust implementation

Recent guidance from the National Security Agency on "Embracing a Zero Trust Security Model" recommends "Inspect[ing] and log[ging] all traffic before acting" among its four key guiding design principles for implementing Zero Trust.[2] Organizations cannot implement a Zero Trust architecture without a unified source of network truth to support it. This joint Corelight and Splunk solution represents a strategic investment in Zero Trust architecture - providing continuous verification of the efficacy of an organization's Zero Trust policies, by storing all network connection information, so it can be queried for reporting trends in violation frequency, source, and priority.

Telemetry that informs Zero Trust operations should resist compromise, as adversaries will attempt to muddle the operational picture by compromising telemetry, up to and including generating false information from hijacked sources such as compromised endpoints. Comprehensive network

[1] "Security team sees 95% reduction in average incident response time with Corelight's network visibility"
https://f.hubspotusercontent00.net/hubfs/8645105/Corelight_May2021/Pdf/cs_co_corelight_education_first.pdf

[2] "*Embracing a Zero Trust Security Model.*" National Security Agency. February 2021.
https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF

monitoring from Corelight is resistant to compromise because the network cannot lie: what was communicated, parsed, and recorded over the wire cannot be altered.

Unlock unique threat detection capabilities

The off-the-shelf integrations between Splunk's security algorithms and Corelight's data provide a turnkey experience, lighting up dashboards and enabling detections by default. Designed to give security teams a head start, these integrations are particularly effective against the commodity malware and automated attack tier that so frequently takes analyst time away from the subtle trails left by more advanced adversaries.

This higher level of attackers routinely acquires and reverse engineers commercial detection technology, but cannot reverse engineer a detection that they do not know exists. Thus, the most durable threat detection is one developed and deployed in-house, unique to a specific organization and/or adversary.

Corelight offers native detection engineering capabilities via Zeek scripting and Suricata signatures, and its data format also readily supports the development of custom analytics and threat detection in the Splunk platform. The solution provides turnkey, yet extensible detections for:

- Splunk Enterprise Security
- Splunk Security Essentials
- User entity behavior analytics (UEBA)
- Splunk Machine Learning Toolkit

Control data and costs

Corelight can replace a wide range of disparate network sources with a consolidated source of network telemetry, removing the costs of maintaining separate logging systems and Splunk integrations. Corelight also gives customers a range of capabilities to control the filtering and streaming of Corelight data itself to Splunk to manage downstream data processing costs, including:

- **Data reduction mode** which removes lower-value security fields in Corelight data to reduce the overall data export footprint by 30-50%.

- **Data fork & filter controls**, offering a range of opt-in filters to remove specific data types from export and/or split data to different destinations to send only a subset to Splunk and send 100% of the data to cold storage for backup.

What makes Corelight unique

Corelight's open Network Detection & Response (NDR) platform holds numerous advantages over competitive solutions in the market, which include:

- **Superior performance and scalability**
  No one in the open source community or vendor space can scale like Corelight. We have the unfair advantage of having the inventor and maintainers of the open source Zeek project as founders. They've leveraged their knowledge to deliver commercial appliances that offer 10x higher performance than what other vendors or the open source community has achieved, all with no packet loss.

- **Platform openness**
  Corelight is built on open source technology. It gives customers unfettered access to the underlying data and detection logic, and supports customer modification and extension of the platform. This stands in stark contrast to locked-down, black box competitor solutions that make tuning, export, and integration exceptionally difficult. Openness gives organizations choice and flexibility. To maximize the utility of Splunk's Machine Learning Toolkit, for example, teams need a data format that's extensible.

- **Greatest depth of Splunk integration**
  Other vendors in the space have their own panes of security glass that compete with Splunk for analyst time. Corelight is focused on reducing analyst console fatigue, and has designed its product around integrating into the broader ecosystem to improve the human experience. As a result, the reliability and depth of our Splunk integration is unmatched by any other network security vendor.

- **Unmatched enterprise support**
  Every Corelight subscription brings access to Corelight's customer success organization, which has a world class bench of security talent with unmatched expertise in foundational open source technologies and key security disciplines like threat hunting. We assign a post-sales technical account manager (TAM) to every customer who meets with your team regularly to ensure your deployment is successful, offering assistance on everything from system turning to the development of custom analytics.

Conclusion

When faced with advanced adversaries who continue to cut through security defenses, throwing incremental technology at the problem is a losing strategy. A seismic shift in strategy is needed that refocuses efforts not on better blocking or alerting technology, but on building an asymmetric knowledge advantage against adversaries via superior operational awareness. From this position of knowledge better detections and more efficient and effective security workflows naturally follow.

Organizations that have invested in Splunk have made a wise strategic decision to consolidate their operational awareness in a purpose-built SIEM platform. Investing in Corelight compounds this investment and the in-house Splunk expertise developed and makes it 100x more powerful by equipping teams with the right network data from Corelight. With a strategic data reserve from Corelight in Splunk your security team is well positioned to outmaneuver adversaries over the next ten years.

corelight

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