Challenge
Close a distinct, long-standing gap in its current monitoring capability

Solution
Combination of Corelight AP 3000 and AP 1000 sensors across four datacenters

Integrations
Corelight integration with Splunk UBA

Case Study

Publicly-held energy company selects Corelight for better internal visibility & enhanced threat analysis

Background

A leading, publicly-held, energy company serving millions of customers throughout the southern United States, needed a network visibility solution capable of capturing and parsing DNS and DHCP network protocol traffic, as well as visibility into internal network connections with ability to enhance threat analysis at enterprise scale.

Challenges

The organization was already utilizing Splunk UBA for behavioral analytics and a network traffic analysis (NTA) solution from IronNet which it determined was not sufficient in providing the rich data offered with Zeek. The team identified a distinct, long-standing gap in its current monitoring capability. During testing against a competing solution, the team discovered that while there was heavy visibility overlap between the two platforms, the data generated by Corelight, was much more informative for security use cases, and much more easily correlated against other security data.

Solution

Ultimately, the security team decided to roll out the Corelight sensors to four of its data centers with a combination of Corelight AP 3000 and AP 1000 sensors and plans to continue exploring additional investment in sensors and the Corelight Fleet Manager.

Results

Corelight data supported unplanned use cases, such as validation of WPAD configurations across the organization to support audit response research. This data was also used to identify potentially impacted systems during an Incident Response investigation. Corelight was very successful as a platform in terms of collecting security-relevant network data at scale. The customer found that this data provided a good balance between limited flow data and comprehensive full content capture (PCAP). Further, the customer was pleased with the ”extreme dedication” and support from Corelight and determined that resources were knowledgeable and responsive to questions and concerns raised throughout the process.

888-547-9497 | info@corelight.com