***Challenge***
An education organization sought to expand network visibility to accelerate incident response beyond the capabilities of their incumbent, black box NDR solution provider.

***Solution***
Corelight's Open Network Detection and Response (NDR) Platform allowed the organization to combine "the knowledge of today with the logs of yesterday" to gain new threat insights.

Case Study

# Corelight expands network visibility and detection coverage and accelerates incident response for Grand Canyon University

## Background

The security team at Grand Canyon Education (GCE), a shared services partner dedicated to serving colleges and universities, sought to replace its reliance on black box network security solutions with an open-core NDR platform that delivers comprehensive and actionable insights around threat activity.

## Challenges

Black box NDR solutions make it difficult for security analysts to gain access to the complete set of evidence behind every alert and network connection and notably fail to detect command and control activity on the network. These proprietary solutions are tightly controlled and, as the GCE security team found, opaque.

Typically, black box solutions run on the collective knowledge of the vendor security researchers behind them. So when real-life adversaries are scheming to get inside the network and detection proves critical to stopping them, it's sometimes unclear whether a black box product even knows about a specific threat activity or pattern. For example, if a new exploit such as Log4Shell or SUNBURST emerges, it can take the proprietary solution team many days to create and release a new detection capability.

Where detection capabilities do exist, they often lack transparency or don't provide enough evidence to investigate or validate an alert. When GCE received a ransomware alert and sought more information from one of its black box vendors, despite persistent inquiries, the GCE team was never able to obtain the full detection logic required for successful analysis. Ultimately, the ransomware alert turned out to be a false positive.

To grow beyond these limitations, the GCE team wanted to deploy an open-source platform that would give them more transparent, community-driven detection engineering and unfettered access to the underlying evidence behind every alert to expand visibility and accelerate incident response.

## Solution

GCE turned to Corelight's Open Network Detection and Response (NDR) Platform. Fueled by comprehensive network security analytics and rich, interconnected evidence, Corelight integrates with security information and event management (SIEM) and extended detection and response (XDR) platforms. Corelight's commercial platform is built around two gold standard open source security technologies: **Zeek**®, which analyzes traffic and transforms network traffic into compact, high-fidelity transaction logs, and **Suricata**®, an intrusion detection system (IDS).

Via proprietary machine learning, behavioral analysis and signatures, combined with community-developed detection engineering, Corelight ensures comprehensive coverage of MITRE ATT&CK®. This framework is a globally-accessible knowledge base of adversary tactics and techniques, based on real-world observations that support the development of threat models and methodologies for the private sector and government.

## Results

GCE team members can now investigate and respond to attacks more rapidly, with much higher confidence in the quality of the decisions that are reached by their team. They're using Corelight network evidence and asking the platform constant questions about internet protocol (IP) activity to arrive at a transparent, actionable level of detection logic that black box NDR solutions cannot provide. Notably, Corelight's Command-and-Control analytics collection was also able to detect the C2 activity missed by the black box vendor in a PoC test.

"We are combining the knowledge of today with the logs of yesterday to better understand what is going on in our network," says Christian Taillon, an IT security engineer at GCE. "That is very valuable to us." The platform also allows for greater flexibility when new threats emerge, since team members can take advantage of intelligence and detections from the open-source community that may take just hours to develop.

"If you have intelligence from the platform along with skilled people who know how to use it," says Mike Manrod, Chief Information Security Officer (CISO) at Grand Canyon Education, "you at least have a fighting chance against the evolving threat landscape."

corelight

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.*