CASE STUDY

# Carrefour, a top ten global retailer, uses Corelight to expand visibility & detect attacks at the earliest stages

## BACKGROUND

Carrefour, headquartered in France, is the seventh-largest retailer in the world by revenue, operating tens of thousands of department stores, supermarkets and convenience stores in over thirty countries.

Carrefour's SOC/CSIRT Manager, David Charpagne, sought to expand his organization's network visibility and improve detection coverage to address threats like lateral movement and ransomware and to defend endpoints unsupported by EDR, including internet-connected equipment in their retail locations. Charpagne knew that a Network Detection & Response (NDR) platform could help his team address these threats and his organization achieve the SOC visibility triad via integration with their existing SIEM and EDR solution.

**CHALLENGES**
*Ransomware, lateral movement, network & EDR visibility gaps*

**SOLUTION**
*Corelight Open NDR Platform*

**RESULTS**
*Expanded visibility & detection capabilities at earliest attack stages*

## CHALLENGES

As a global multinational Carrefour's network traffic is complex, voluminous, and highly distributed, spanning on premise and cloud networks across corporate headquarters, data centers, satellite offices, partner networks and retail locations.

Their default sources of network telemetry (e.g. firewall logs) did not deliver sufficient visibility to identify early stages of an attack nor illuminate dark corners of their organization such as those where EDR agents could not be deployed.

It was key as well not to add another tool that would require another interface but to have a seamless integration with their existing EDR and SIEM.

***"Due to the scale of the internal Carrefour network and the number of sites and partners with permanent or non-permanent interconnections, initial access is not very difficult to obtain. The main risk is an attacker who manages to extend control over our IT sufficiently to paralyze it and demand a ransom."***

David Carpagne,
Carrefour SOC Manager

## SOLUTION

To overcome these challenges the Carrefour team needed an NDR platform that could reliably scale to high throughput traffic, seamlessly integrate with their SIEM, and deploy flexibly and quickly across a range of networked environments to deliver comprehensive visibility and high fidelity threat detections with minimal alert noise.

The team evaluated a number of commercial NDR vendors and chose Corelight's Open NDR Platform based on its ability to satisfy their requirements and due to its competitive advantages, which included
deployment simplicity, support quality, and an open platform design that maximizes customer control and ability to drive high fidelity detections.

"Most NDR solutions on the market have opaque detection based on machine Learning or AI. These solutions are "black boxes" and it is very difficult in a network as extensive and complex as Carrefour to have a sufficiently clean detection baseline so as not to be overwhelmed by alerts," said Charpagne. "Corelight allows us to be masters of our detection, to deploy our use cases by iteration and to control them using the capabilities of our SIEM for detection. Costs are controlled and we make the most of our security tools."

Charpagne and his team were especially pleased with Corelight's ease of integration with their SIEM and telemetry quality, which is based on Zeek, Suricata and Machine Learning, creating an industry gold standard for network security monitoring.

"The community around this security product is one of the most dynamic and innovative that we have seen," said Charpagne.

## RESULTS

The Carrefour security team successfully deployed Corelight and integrated it with their SIEM, thereby achieving comprehensive network visibility and expanded threat detection coverage via Corelight's security analytics powered by machine learning, behavioral analysis, signatures, and threat intelligence. Corelight's Open NDR platform ultimately helped Carrefour illuminate and defend critical areas of their business and supported key security team use cases such as:

***"Corelight allows us to be masters of our detection, to deploy our use cases by iteration and to control them using the capabilities of our SIEM for detection. Costs are controlled and we make the most of our security tools."***

David Carpagne,
Carrefour SOC Manager

- Developing custom detections via Corelight telemetry, e.g. detecting large LDAP exports
- Managing false positives
- Accelerating investigations via Corelight telemetry for initial access & lateral movement
- Conducting "white zone" monitoring where EDR agents could not be deployed
- Analyzing encrypted traffic effectively to detect hidden threats

"With Corelight we gain visibility into the attack chain in the discovery, lateral movement and remote code execution phases and this at strategic locations in our network (partner interconnections). This costs us much less and is much more relevant than collecting Firewall logs indiscriminately," said Charpagne. "This deployment allows us to detect a malicious intruder in the very early phases of its attack before it attacks the endpoint, basically our SOC analysts shifted from a reactive mode thanks to Corelight to being proactive and having more time to do Threat Hunting."

Request a demo of the Open NDR Platform at **https://corelight.com/contact**

corelight

Corelight provides security teams with network evidence so they can protect the world's most critical organizations and companies. 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.*

*All rights reserved. © Copyright 2024 Corelight, Inc.*