

JOINT SOLUTION

Superior network detection & response natively integrated with Microsoft Sentinel

IT COMPLEXITY IS DECREASING VISIBILITY

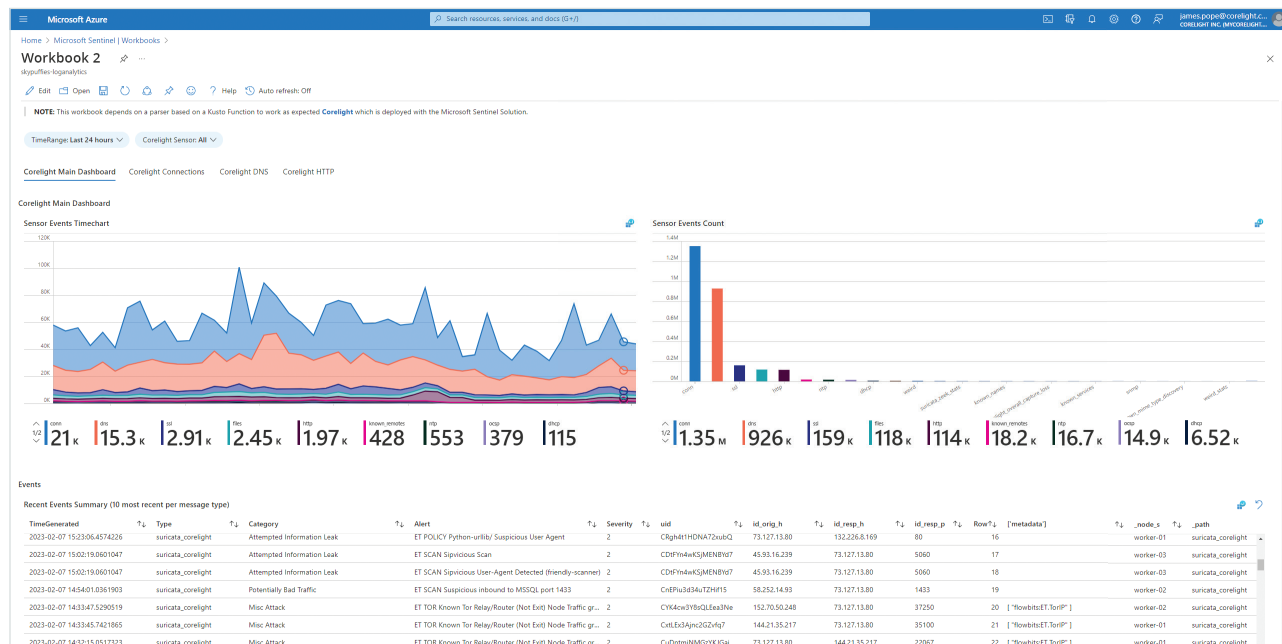
Today's threat landscape can be hard to navigate, especially when you lack full visibility and control over your IT and IoT environments. With the wide adoption of cloud, the proliferation of smart devices, and the growth of microservices development architectures, threats are getting more complicated and difficult for security teams to keep up with.

Corelight and Microsoft offer an integrated solution for overworked security teams to optimize visibility and threat investigations across their IT, IoT, and industrial control systems (ICS) networks. By transforming all network traffic into comprehensive, detailed evidence, Corelight gives security teams using Microsoft Sentinel the visibility to understand exactly what is happening across the enterprise.

INTEGRATION HIGHLIGHTS

- Best-in-class, NDR and cloud-native SIEM & SOAR platforms
- Optimal visibility of all activity across IT, IoT, and ICS networks
- Overcome alert fatigue and accelerate investigations
- Integrated data and dashboards simplify threat detections
- Advanced network telemetry to support XDR and Zero Trust initiatives

TRANSFORMING NETWORK TRAFFIC INTO COMPREHENSIVE, DETAILED EVIDENCE



Network telemetry from Corelight in Microsoft Sentinel shows log throughput along with the correlated Suricata alerts and Zeek logs that can be examined more deeply.

JOINT SOLUTION: CORELIGHT AND MICROSOFT SENTINEL

This network insight helps security operations center (SOC) teams tame the exponential growth of security alerts and incidents to ensure nothing falls through the cracks.

ADVANCED NETWORK TELEMETRY FOR MICROSOFT SENTINEL

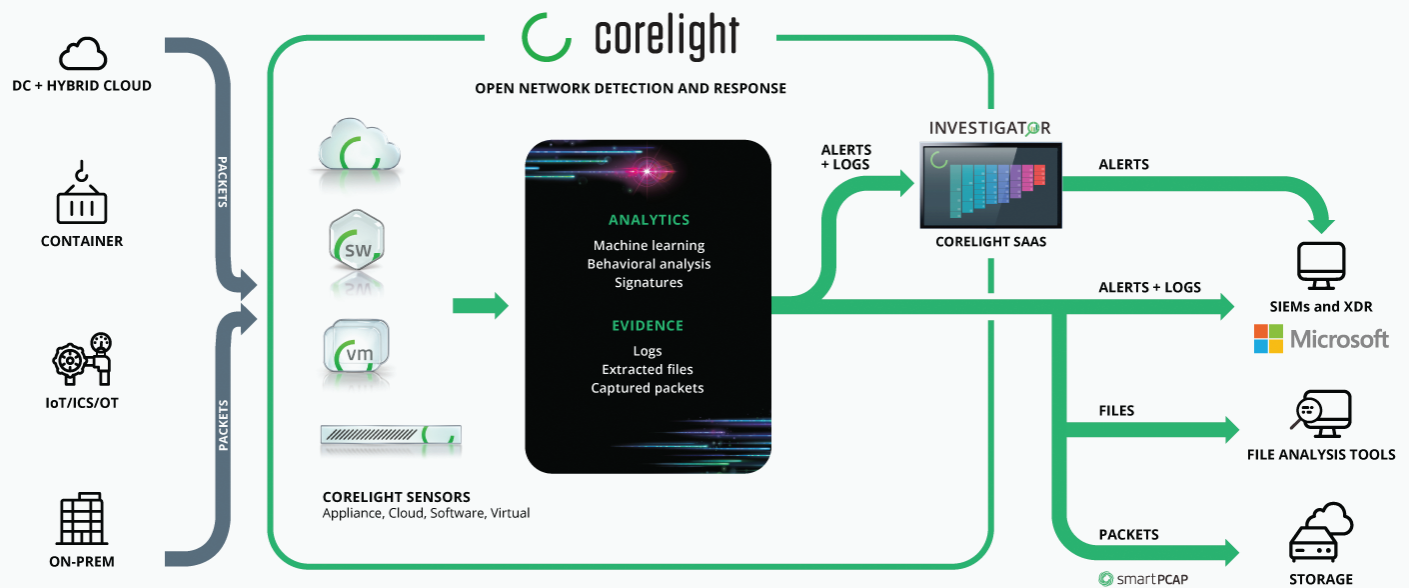
By providing correlated log data from over 50 protocols through passive network monitoring, Corelight provides SIEM analysts using Sentinel a clear picture of all the activity across their global networks.

Additionally, the Corelight App for Microsoft Sentinel helps resource-constrained SOC teams simplify deployment and alert triage by ingesting pre-formatted, correlated network evidence directly into Sentinel dashboards and data repositories. This helps provide a holistic view of the environment, including context for device inventory and the ability to respond quickly to alerts to mitigate advanced threats from a single pane of glass.

Member of
Microsoft Intelligent Security Association



CORELIGHT OPEN NDR AND MICROSOFT SENTINEL



ESSENTIAL COMPONENT FOR XDR AND ZERO TRUST SOLUTIONS

Along with native data integration, the Corelight App for Microsoft Sentinel also includes pre-defined workbooks, custom dashboards, sample queries, and analytics rules to help SOC teams accelerate investigations, incident response, and threat hunting. And with an open and flexible design based on the open-source Zeek and Suricata platforms, Corelight is an integral component of Microsoft's XDR and Zero Trust solutions.

SOLUTION BENEFITS



COMPLETE VISIBILITY

Corelight enables Sentinel users to accelerate threat detection and response with detailed evidence and analytics of all network traffic, including that for unmanaged devices and those lacking endpoint agents.



NEXT-LEVEL ANALYTICS

Corelight's high-fidelity, correlated telemetry powers Sentinel analytics, machine learning tools and SOAR playbooks so you can make better decisions faster.



FASTER INVESTIGATION

Correlate alerts, evidence, and packets for a baseline of network activity and the insightful context to power your Sentinel workflows.



EXPERT HUNTING

Quickly spot vulnerabilities, intruder artifacts, signs of compromise, and undetected attacks with correlated and contextual evidence.

To learn more about the Microsoft Sentinel integration, request a demo at <https://corelight.com/contact>



Microsoft enables digital transformation for the era of an intelligent cloud and an intelligent edge. Its mission is to empower every person and every organization on the planet to achieve more.



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