corelight

Joint Solution Brief

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

Optimal visibility of all activity across IT, IoT, and ICS networks

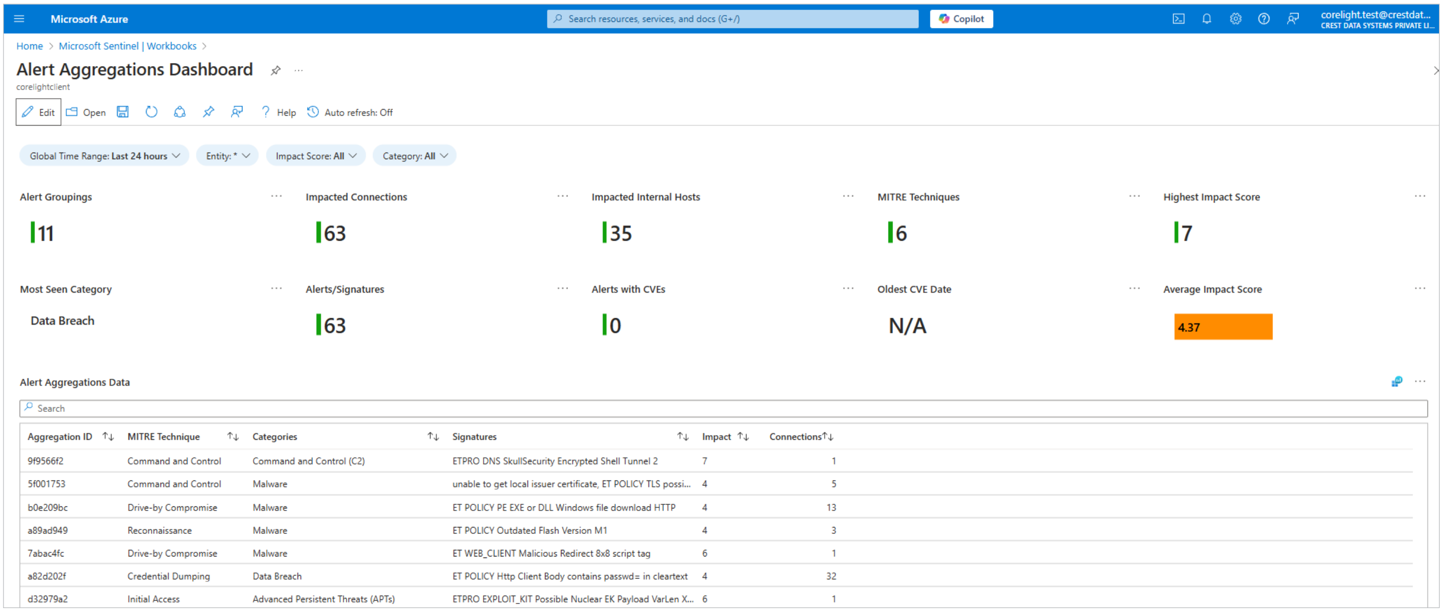
Overcome alert fatigue and accelerate investigations

Integrated data and dashboards simplify threat detections

Intuitive dashboards provide at-a-glance and detailed insights

Advanced network telemetry to support XDR and Zero Trust initiatives

Transforming network traffic into comprehensive, detailed evidence


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
corelight.test@crestdat...
CREST DATA SYSTEMS PRIVATE LI...
Home > Microsoft Sentinel | Workbooks >
Edit
Open
Help
Auto refresh: Off

Alert Aggregations Dashboard

corelightclient

Global Time Range: Last 24 hours | Entity: * | Impact Score: All | Category: All

Alert Groupings	Impacted Connections	Impacted Internal Hosts	MITRE Techniques	Highest Impact Score
11	63	35	6	7

Most Seen Category	Alerts/Signatures	Alerts with CVEs	Oldest CVE Date	Average Impact Score
Data Breach	63	0	N/A	4.37

Alert Aggregations Data

Search

Aggregation ID	MITRE Technique	Categories	Signatures	Impact	Connections
9f9566f2	Command and Control	Command and Control (C2)	ETPRO DNS SkullSecurity Encrypted Shell Tunnel 2	7	1
5f001753	Command and Control	Malware	unable to get local issuer certificate, ET POLICY TLS possi...	4	5
b0e209bc	Drive-by Compromise	Malware	ET POLICY PE EXE or DLL Windows file download HTTP	4	13
a89ad949	Reconnaissance	Malware	ET POLICY Outdated Flash Version M1	4	3
7abac4fc	Drive-by Compromise	Malware	ET WEB_CLIENT Malicious Redirect 8x8 script tag	6	1
a82d202f	Credential Dumping	Data Breach	ET POLICY Http Client Body contains passwd= in cleartext	4	32
d32979a2	Initial Access	Advanced Persistent Threats (APTs)	ETPRO EXPLOIT_KIT Possible Nuclear EK Payload VarLen X...	6	1

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.

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.

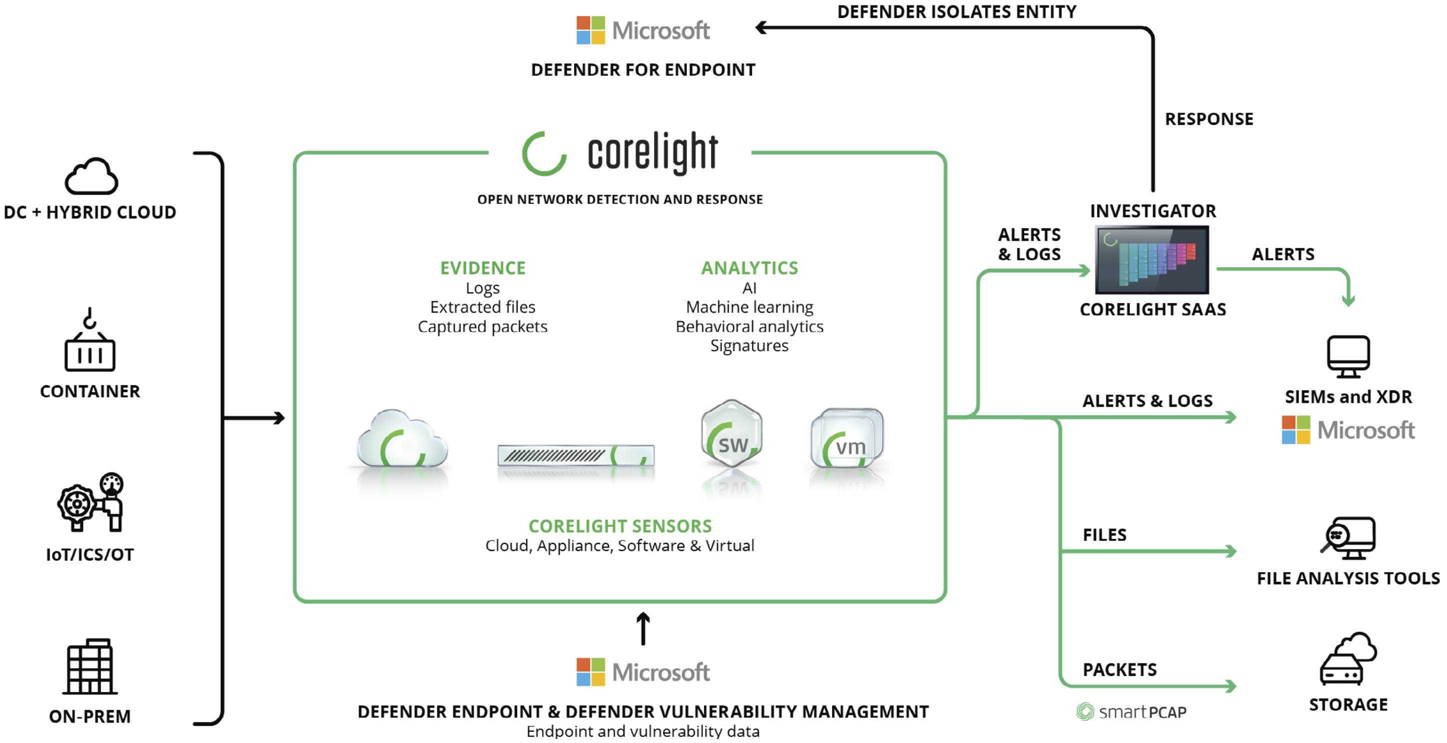
Intuitive dashboards provide at-a-glance views of an organization’s security posture and visual insights into potential threats using real-time network telemetry. With summary charts, counters, and maps, SOC analysts can quickly discern trouble spots and drill down into details to validate threats. This clarity and guidance provides focus where it’s most needed to accelerate investigations and response times while streamlining workflows.

Member of
Microsoft Intelligent Security Association
Microsoft

ESSENTIAL COMPONENT FOR XDR AND ZERO TRUST SOLUTIONS

Along with native data integration and intuitive dashboards, the Corelight App for Microsoft Sentinel also includes pre-defined workbooks, 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.

Corelight Open NDR and Microsoft Sentinel



Simplify investigations and prioritize alerts according to actual risk to the enterprise with integrated network, endpoint, and vulnerability data.

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. Intuitive dashboards provide at-a-glance and detailed insights.

EXPERT HUNTING

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

corelight

To learn more about the Microsoft Sentinel integration, request a demo at

https://corelight.com/contact

info@corelight.com | 888-547-9497