Microsoft | corelight

Joint solution brief

Corelight Investigator integration with Microsoft Entra ID

Accelerate triage and response with unified network, host, and identity context

Security teams frequently struggle to sustain a proactive, resilient security posture because legacy detection tools often lack the ability to correlate host and user data with live network activity. This lack of unified visibility compels SOC analysts to jump between multiple consoles, investing valuable time manually connecting data points to identify genuine threats. Such fragmented workflows make it easier for sophisticated adversaries to slip through the cracks, ultimately delaying incident response and contributing to analyst alert fatigue.

The Corelight integration with Microsoft Entra ID eliminates this critical "network-identity blindness" by seamlessly ingesting real-time host and identity data from Microsoft into the Corelight Investigator interface. Building on Corelight's existing integration with Microsoft Defender for Endpoint, the new integration with Microsoft Entra ID enables analysts to quickly zero in on systems and users posing the highest risk and take immediate action. This includes forcing a user logout, resetting a password, or disabling a user account directly from the Corelight detections screen.

With this unified context at their fingertips, analysts can make decisive, high-confidence decisions on alerts, close cases faster, and measurably improve the organization's overall security posture by streamlining workflows and focusing attention where it's needed most.

SOLUTION HIGHLIGHTS

Unified visibility: Enrich Corelight's multi-layered detections with contextual, real-time host and identity data

Risk-based prioritization: Accelerate investigations by correlating network evidence with Entra ID risk context to focus on what matters most

Faster remediation: Improve mean time to respond by enabling analysts to take immediate action directly from Investigator

For example, rather than seeing an anonymous IP address attempting a Kerberoasting attack to impersonate an authenticated user, a Corelight Investigator analyst triaging the source IP can immediately see the specific user details, such as login ID, display name, login history, related alerts, and the user's overall risk score as defined by Entra ID. Directly integrating this real-time identity context into the Investigator detection view is essential for efficient alert prioritization and quick remediation, as it unmasks the user, eliminates the need to manually stitch data from various dashboards, and enables a response directly from the detections panel.

Ground-truth network evidence for Microsoft Entra ID

Corelight's Open NDR Platform converts raw network traffic into detailed, actionable evidence that empowers security teams to optimize threat investigations and detection workflows. By ingesting real-time identity data from Entra ID directly into the Corelight Investigator detections dashboard, analysts can not only focus on the endpoints and users that pose the highest risk to their environment, but also take immediate action from the Corelight detections screen to thwart an attack.

Extending Corelight integration across Microsoft Security with Entra ID equips analysts and threat hunters with the real-time context needed to effectively triage, prioritize, and contain identity-based threats before they escalate into a breach that can disrupt your business and cause enormous damage.

corelight

To learn more about Corelight for Microsoft Security, request a demo at

https://corelight.com/contact

info@corelight.com | 888-547-9497