corelight

White Paper

Top 5 reasons why modern SOCs need multi-layered detections

INTRODUCTION

In today's complex cybersecurity attack landscape, perimeter and endpoint defenses are frequently breached. Sophisticated attacks are becoming increasingly difficult to detect with technologies like Security Information and Event Management (SIEM), Extended Detection and Response (XDR), and Endpoint Detection and Response (EDR) because these tools, particularly EDR, are working so effectively that attackers are compelled to shift their strategies to evade detection. As a result, breaches at firewalls/VPN gateways have surged from 3% to 22%, with attackers exploiting weaknesses in perimeter defenses (Source: Verizon DBIR). Likewise, in a recent report, it was determined that 79% of attacks are malware-free, bypassing EDR through techniques like credential theft and DLL hijacking (Source: CrowdStrike GTR). Along with this trend towards EDR evasion, Security Operations Centers (SOCs) are also seeing increased rapid attack speeds. The fastest breakouts occur in seconds, demanding real-time detection beyond EDR capabilities (Source: CrowdStrike GTR).

This is where Network Detection and Response (NDR) becomes crucial, offering a critical layer of defense by providing ground truth and a broad aperture for capturing network activity and activity that is typically invisible to EDR. NDR employs a multi-layered set of detections without the need to deploy agents, effectively identifying threats even when attackers utilize commonly available techniques like Living off the Land (LoTL). This adaptability and comprehensive coverage make NDR indispensable in defending against today's threats.

In addition to the growing number of attacks in an increasingly complex threat landscape, the modern SOC is also dealing with a larger attack surface with the proliferation of environments (including cloud), devices, Internet of Things (IoT), and Operational Technology (OT). Couple these two (increased threats, increasing attack surface) with the continued pressure to do more with less, and it is easy to understand how and why the modern Security Operations Center (SOC) needs multi-layered detections as part of its network security. When implemented correctly, the right multi-layered detection strategy can inspect threats from multiple perspectives to correlate and aggregate alerts to enable optimal outcomes.

Corelight's strategy with multi-layered detections fuses the best of each detection strategy to provide important benefits to the SOC. Next, let's examine the top 5 reasons SOCs need to ensure that multi-layered detections are part of their security solution.

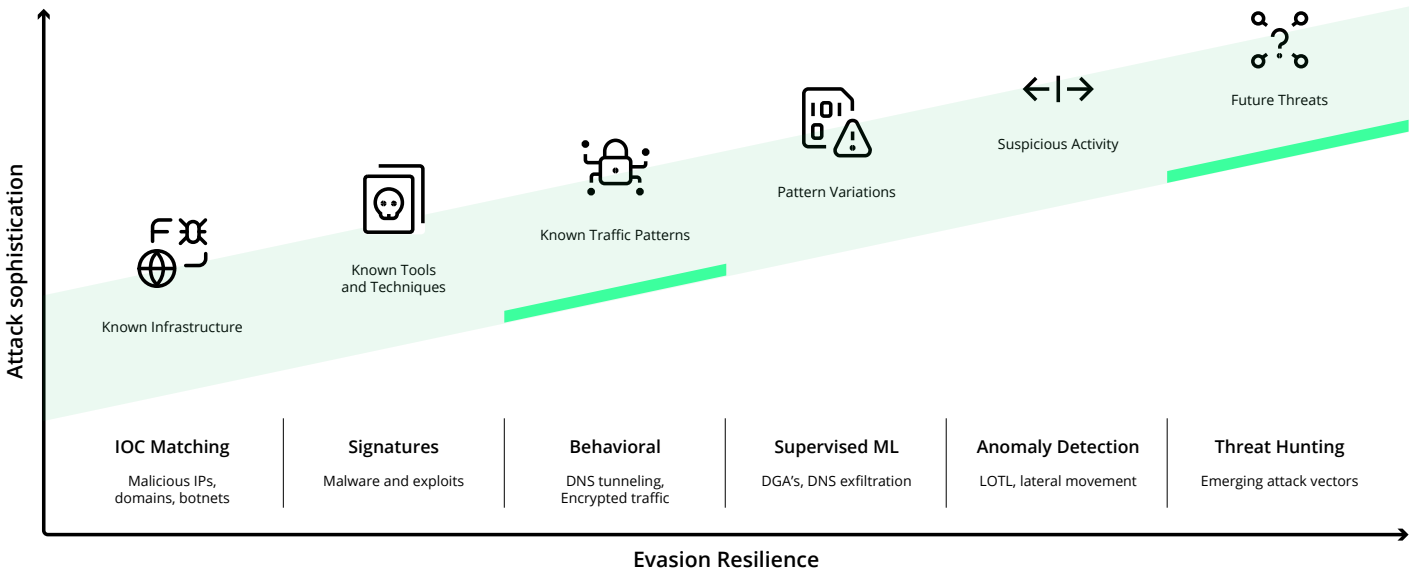
The top 5 reasons

1. FASTER DETECTION OF THREATS

One of the top priorities of the SOC should always be to detect threats as quickly as possible to mitigate the amount of damage that the threat might cause. Using a multi-layered detection architecture allows threat detection resources to be deployed optimally to achieve the quickest detection of threats. This is done by using low-impact detection engines to find common and known threats quickly, while allowing the higher resource-intensive detection engines to work on more evasive and unknown threats.

Corelight combines the industry's best data with advanced ML

Minimizing FP rates with community powered behavioral detections



To understand the advantages of a multi-layered threat detection architecture, we need to take a deeper look at the detection engines and how these detection engines and their specific and unique technologies are used together to provide the quickest detection of threats for the SOC. Corelight Open NDR utilizes an array of multi-layered engines that analyze network data and logs. Each detection engine is deployed to detect different known and unknown threats, all providing unique benefits, and implemented to improve detection accuracy and speed.

THE CORELIGHT OPEN NDR DETECTION ENGINES

- **Signatures**—Signature detection is generally one of the first tools used for network detection due to its accessibility, availability, and light-weight nature, enabling quicker threat detection than the heavier-weight tools that come later in the detection chain. Open NDR uses Corelight's signatures along with the industry-leading Proofpoint ET Pro signatures running on the integrated open-source Suricata detection engine.
- **YARA**—YARA rules, a standard for static file analysis in the malware analysis community, allows for customizable pattern matching. These rules search for unique strings, binary patterns, or behavior patterns in malicious files to identify malware families—malware that shares common code but is not identical. Corelight Open NDR supports an integrated YARA rules-based detection engine, combined with the platform's powerful file extraction and metadata capabilities.
- **Threat Intelligence**—Often composed of Indicators of Compromise (IOCs), it looks for known network entities (e.g., IP addresses, domain names, hashes) observed in actual attacks. As with signatures, IOCs are easy to share, light-weight and quick to deploy, offering quicker detection. Open NDR supports threat intel from various vendors, including native integration with Crowdstrike Threat Intel. Customers can also bring their own threat feeds and custom intel through STIX/TAXI and Zeek® input framework support. Millions of indicators are supported, matching across all network protocols for comprehensive and rapid alerting.
- **Behavioral detection**—Used to Identify types of activity that are associated with specific, generally dangerous behaviors observed in network traffic. Examples of activities that fall within this type of detection include domain generation algorithms (DGAs), command and control (C2), crypto mining, and transferring large amounts of traffic over control protocols like DNS and ICMP. Behavior detection is one of the key detection technologies for identifying unknown and evasive attacks and threats, in addition to known threats. The power of behavioral detection is that it remains effective even when attackers change their IOCs, or even components of the attack, since the underlying behaviors have not changed, enabling quicker detection of unknown threats. Open NDR also supports custom scripting capabilities, allowing customers to bring behavioral detections from the Zeek community and/or write and create their own.
- **Machine Learning (ML)**—ML is useful in detecting known, unknown and previously unseen attacks. Corelight Open NDR uses both supervised and unsupervised ML for detections.

Supervised ML: Open NDR uses supervised ML models on both sensor-only and SaaS-based deployments to identify specific types of known attacks on which the models have been pre-trained. Some of these include the discovery of DNS reconnaissance, Tor usage, malware using domain generation algorithms (DGAs), and exfiltration over DNS, to name a few. The targeted application of ML in these cases results in low false positives while still identifying unique differences in how attackers use these techniques.

- **Anomaly Detection**—Corelight Open NDR uses unsupervised ML in its anomaly detection engine to generate alerts for irregular and anomalous behavior, and includes specific context, enabling faster interpretation and assisting in quicker incident resolution.

Unsupervised ML: By combining the ability to learn from a baseline of traffic, an advanced framework for identifying deviations from such a baseline, and an intense focus on the explainability of the detections, Open NDR's anomaly detection engine applies unsupervised ML to a variety of network use cases. Live predictions generate alerts when anomalous activity is observed and include context to explain why the alert was generated with additional information to assist in faster triage. Types of anomalous behavior this engine can identify include the use of unexpected new network services, anomalous client software, unusual login behavior, and potentially malicious management traffic, just some examples of potential risks Corelight customers face on their networks. Anomaly detection also enables proactive threat hunting, giving organizations the ability to uncover elusive threats that would otherwise be hiding amongst normal activity by actively seeking out anomalies and reducing attacker dwell time.

50%

reduction in **incident response time** by using Artificial Intelligence (AI) to assist in providing guided triage, along with the ability to automate workflows.

(Source: CrowdStrike GTR)

- **Search-based**—For some types of rapid response, there is simply no faster way to generate an alert than to query the existing log data. Corelight-defined log search queries generate search-based alerts and detections. The Corelight Labs team creates these alerts using LogScale searches, correlating indicators and attack activity from the logs directly. Some examples of searches include initial access via Adobe ColdFusion arbitrary file read, Cisco IOS XE command execution attempt,C2 via Async RAT Trojan, Kolobko, and credential access via confluence hardcoded password usage.

Many organizations may find it also makes sense to use an NDR like Corelight as an additional detection filter layer to their security architecture by placing Corelight as a detection engine in front of a SIEM. With the high cost of SIEMs, another layer to pre-filter threats can also more quickly identify threats and reduce overall SIEM costs. With Corelight Open NDR, SOCs can benefit from faster detections, generated by the comprehensive array of available threat detection engines.

2. FASTER INCIDENT RESPONSE

Another equally important goal for SOCs is faster incident response, likewise to reduce the amount of damage an attack can cause. The use of multi-layered detection engines provides not only quicker detection of threats, but also facilitates faster incident response, including quicker triage and resolution (and additionally leads to increased ROI). Multi-layered detections make this possible when multiple detection engines can provide additional context and understanding around a given threat, to enable quicker resolution to the incident.

Corelight Open NDR further reduces incident response time by adding the use of Artificial Intelligence (AI) to assist by providing guided triage, along with the ability to automate workflows resulting in an over 50% reduction in incident response time. Each alert (generated by any of the multi-layered detection engines) is associated with a network entity—a host, domain, or IP address—that Corelight Open NDR identifies as associated with a potential threat. Alerts from different sources and entities are correlated with a unique ID for each entity making it easy to pivot to related alerts referencing the same unique ID for quicker understanding and resolution of any incident. Alerts are also assigned a normalized severity score based on the likelihood that they represent a real security threat. The score ranges from 1 to 10, with higher scores indicating more severe and critical threats, and these scores can be easily customized to best reflect local organizational knowledge.

In addition to severity scoring, detections from the same category and entity combination (which can include a combination of detection types) are aggregated for display and response, which can aid in determining the extent of the threat, reducing alert volume, and provide additional detail for quicker overall incident response time.

Corelight Open NDR also leverages Zeek data and explainable machine learning model output to provide context and helpful information to assist the analyst in their understanding of the threat and their planned response. In addition, detections are mapped to the MITRE ATT&CK framework and include links to the relevant MITRE ATT&CK techniques (more on this in the section on Comprehensive Coverage and Visibility). Corelight Open NDR's expanded detection includes coverage across more than 90% of network-centric adversary Tactics, Techniques and Procedures (TTPs)—where EDR coverage is sparse.

3. REDUCTION IN FALSE POSITIVES

The use of multi-layered detection engines reduces the overall false positive rates by using additional detection engines to validate the results of any initial detection. When multiple detection engines flag the same threat, it is a good indication there should be a higher confidence in the alert. Alerts from multi-layered detections can be correlated to create higher quality detections, with lower false positives as the result, along with the ability to provide better context and understanding of the underlying threat. Some multi-layered detection engines also give practitioners the ability to tune specific engines in response to false positives, which should reduce the overall false positive rate over time.

In addition, Corelight Open NDR implements peer group modeling to validate anomalies and minimize unnecessary alerts and reduce false positives. Corelight Open NDR also uses thoughtful aggregation of signatures, testing on data-at-scale, and environment-specific tuning, all of which also lead to a lower false positive rate.

By using multi-layered detections, Corelight Open NDR provides higher quality detections which in turn ensures fewer false positives. Corelight uses detection engines where they are most efficient and logically enhance threat detection. As described earlier, signature-based detections are provided by multiple detection engines, including Suricata rules, while Zeek scripts also provide behavioral analysis to further analyze data. Utilizing a YARA rules engine also enables enhanced precision, and has been shown to reduce false positives by 25% ("Reducing False Positives with Advanced Threat Detection", Fireeye 2022).

25%

reduction in **false positives** by utilizing a YARA rules engine.

(Source: "Reducing False Positives with Advanced Threat Detection", Fireeye 2022)

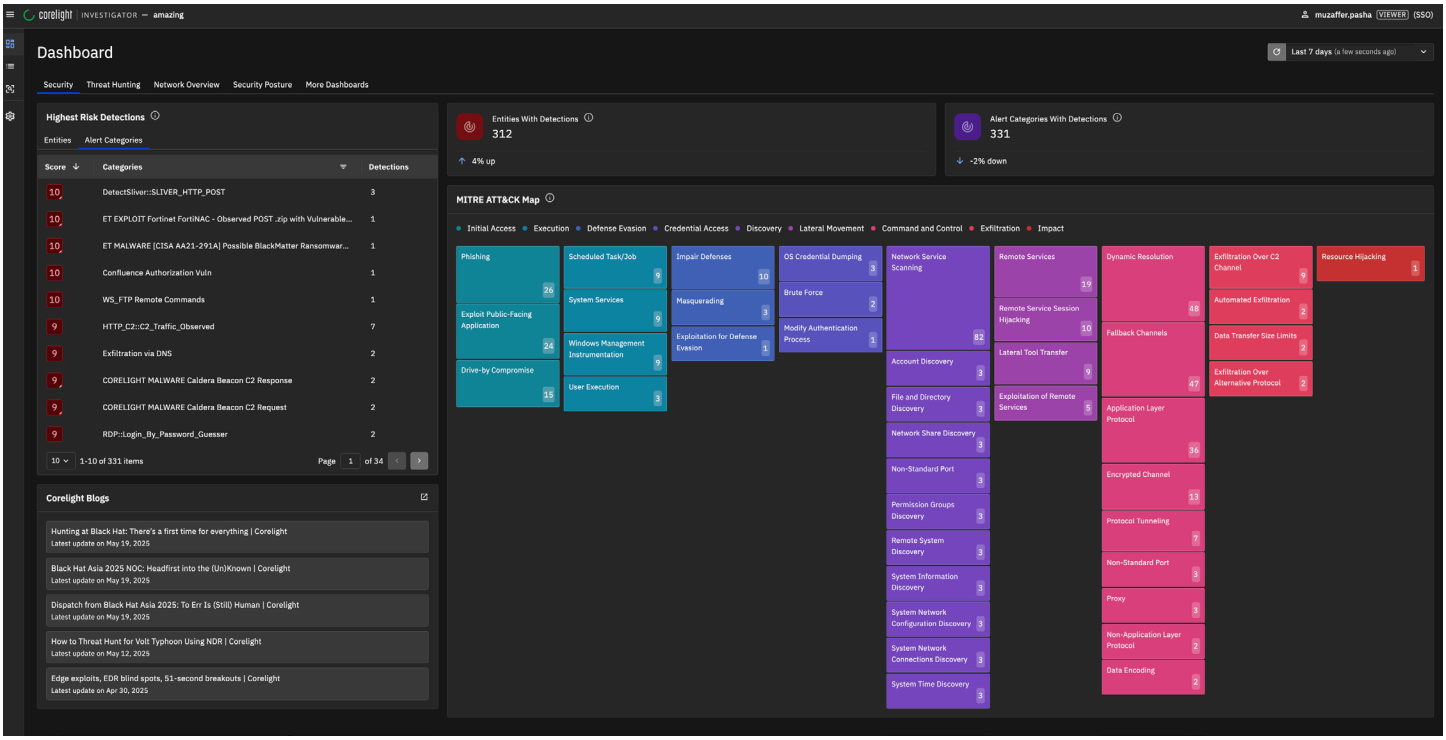
This multi-layered approach provides the coverage and correlation necessary between engines to further reduce false positives. It also allows the more advanced detection engines to focus on unknown and evasive attacks, as well as provide additional perspective to any threats already detected by other engines.

With the correlation and ranking of detections by severity, Corelight Open NDR also provides a reduced volume of critical alerts, and enables SOC triage teams to concentrate on the highest priority detections. In addition to providing fewer false positives, Corelight Open NDR gives security teams the tools that help to expedite alert response and provide valuable evidence and context to identify false positives quickly, if they do appear.

4. COMPREHENSIVE COVERAGE AND VISIBILITY

Multi-layered detections greatly enhance the recognition of novel threats and emerging attack vectors, enabling comprehensive security coverage and visibility for the SOC. As discussed earlier in reason #1 "Faster Detection of Threats", each detection engine enables different detection capabilities, suitable for detecting known, unknown, evasive and zero day attacks. By using network based detection, these detection engines also have the visibility and ability to detect threats that typically evade EDR.

As mentioned earlier, Corelight makes it easy to track detections by using a unique identifier for entities across different sources and engines. This and the other features provided by multi-layered detections contribute to the comprehensive coverage and visibility provided by Corelight to the SOC, that is unavailable when only using an EDR or other endpoint based security system.



Corelight Investigator dashboard displaying alerts mapped to the MITRE ATT&CK map.

Open NDR's detection coverage also includes comprehensive approaches to uncovering over 100 TTPs, providing exceptional visibility into adversary methods used for Defense Evasion, Credential Access, Discovery, and Command and Control. As mentioned earlier, threat detection from the Corelight NDR is mapped to the MITRE ATT&CK framework, allowing SOC analysts to easily see the comprehensive nature of the detections and allows the MITRE ATT&CK mapping to be used to identify the type and nature of the threat to assist in incident response.

MITRE ATT&CK Mapping

Corelight drives broad coverage across the MITRE ATT&CK TTPs using an approach focused on visibility and explainable, evidence-based analytics. The foundation of this approach is Zeek network telemetry, data that captures activity across a broad set of network protocols and fuels advanced analytics. With these analytics, Corelight provides machine learning models, behavioral alerts, and Suricata-based IDS and SIEM rules to detect the relevant ATT&CK tactics, techniques, and procedures. The Open NDR dashboard summarizes data about detections on the network, including the number of detections over time, the distribution of detections across MITRE ATT&CK categories, and information about individual detections.

5. BROAD COMMUNITY CONTRIBUTIONS

A fifth reason for using multi-layered detection is the ability to benefit from community contributions. Many solutions using multi-layered detections already benefit to some degree from community contributions. Typically one or more of the detection engine layers will use threat intelligence that is provided by the various actors in the security community. Many security organizations already share their threat intelligence including signatures, as well as security findings, and usually take part in threat intelligence sharing bodies.

The Corelight Open NDR solution benefits from additional community contributions. We have already covered how a comprehensive multi-layered detection benefits SOCs by using machine learning, behavioral analysis, signatures, rules, and threat intelligence for in-depth high-fidelity detection. Corelight Open NDR does this while at the same time offering an open architecture. By being open, Corelight ensures data portability, so that organizations can take their data and use it in the tools that are most optimal for the SOC. In addition to the threat intelligence feeds that Corelight already uses, Open NDR can also ingest additional threat intelligence feeds as needed by the SOC. As mentioned earlier, Open NDR also supports custom scripting capabilities, allowing customers to bring behavioral detections and/or write and create their own, as well as utilizing YARA scripts for malware detection.

Open NDR's behavioral detection engine utilizes publicly available detections developed and supported by the open source community's 25+ years of experience, providing organizations access to one of the most comprehensive collections of behavioral detections available. By leveraging community contributions, Corelight Open NDR enables the democratization of detections, something that's already happened with attack techniques, where it's already too easy for individuals with no background in hacking to acquire and use attack tools. Corelight's Open NDR Platform also allows the SOC to build its own detection content, as well as use the open source community contributions to Zeek and Suricata, such as MITRE's BZAR package.

CONCLUSION

Corelight collects and analyzes rich contextual data and applies a multi-layered detection strategy that fuses best-in-class technologies, including machine learning, behavioral analytics, curated signatures, and threat intelligence. By integrating a diverse array of detection engines—including signature-based, static file, threat intelligence, behavioral, and machine learning models—Open NDR provides an adaptable and robust framework for identifying and mitigating potential threats, creating significant benefits to the SOC. The most important of these include the ability to detect threats faster, decrease the time to resolution for incident response, while reducing false positives and offering comprehensive coverage and visibility in an open architecture. These are the top 5 reasons why modern SOCs need multi-layered detections as part of their security framework.

With the benefit of multi-layered detections, Open NDR offers visibility into adversary techniques, including those that evade EDR, facilitating a proactive and strategic approach to threat management with faster detection and faster incident response Corelight Open NDR aggregates alerts and provides context through guided workflows and integrated AI capabilities streamlining the triage process for SOC teams, reducing the burden of high alert volumes and enhancing decision-making, while offering comprehensive coverage and visibility.

By integrating community-driven along with proprietary analytics, Corelight Open NDR continuously evolves to address emerging threats and attack vectors. The platform's flexibility in deploying the right detection engine for specific scenarios allows organizations to maintain security fidelity without compromising scalability.

With new detections regularly added from Corelight Labs, third-party vendors, and open-source vendors enables access to a wide spectrum of continually advancing coverage. Corelight Open NDR is a robust and comprehensive solution for enhancing cybersecurity defenses in today's sophisticated threat landscape.

ABOUT CORELIGHT OPEN NDR

At the core of the Corelight Open NDR solution is a commitment to delivering rich, non-judgmental network data—super-deep context about every network connection. This foundational value empowers security teams with unmatched visibility and neutrality. By layering in sophisticated detection engines, Corelight is not replacing that depth of context but rather amplifying it—providing practitioners with even greater precision and speed in triaging and responding to events.

Appendix A: Glossary

Internet of Things (IoT)—IoT encompasses a wide range of equipment with embedded systems, from smart home devices like thermostats and appliances to wearable technology, industrial machinery, and vehicles.

Machine learning (supervised/ unsupervised)—Supervised ML uses labeled data to train models for making predictions or classifications, while unsupervised ML explores unlabeled data to discover patterns and insights without prior knowledge of outcomes. Supervised learning is used in tasks like weather forecasting, where the output is known for the training data. Unsupervised learning is better for tasks like identifying anomalies, where the goal is to uncover hidden structures in the data.

MITRE ATT&CK—MITRE ATT&CK is a guideline for classifying and describing cyberattacks and intrusions. It was created by the Mitre Corporation and released in 2013.

Notice—Notice is the name for alerts and logs generated by Zeek.

Operational Technology (OT)—OT describes the systems and devices that monitor, control, and automate physical processes and devices in various industries, like manufacturing, energy, and transportation.

Suricata—Suricata is an open-source based intrusion detection system (IDS) and intrusion prevention system (IPS

YARA—YARA is a tool primarily used in malware research and detection. YARA It provides a rule-based approach to create descriptions of malware families.

Zeek—Zeek is an open-source software network analysis framework. Zeek is a network security monitor (NSM) but can also be used as a network intrusion detection system (NIDS). Zeek was formerly known as Bro (a reference to Big Brother from the novel 1984).

corelight

To learn more about multi-layered detections, request a demo at

https://corelight.com/contact

info@corelight.com | 888-547-9497