Solution brief

Static file analysis powered by YARA and the Corelight Open NDR Platform

Improve malware detection by 35%—quickly analyze large volumes of files with pattern-based detection

YARA rules are a standard in the malware analysis community. Integrating YARA into security workflows allows for customizable pattern matching and can increase detection of malware by 35%. Additionally, with YARA rules, security teams can leverage shared intelligence from the malware analysis community to proactively detect variants of known malware within their organization and escalate for incident response.

THE CHALLENGE

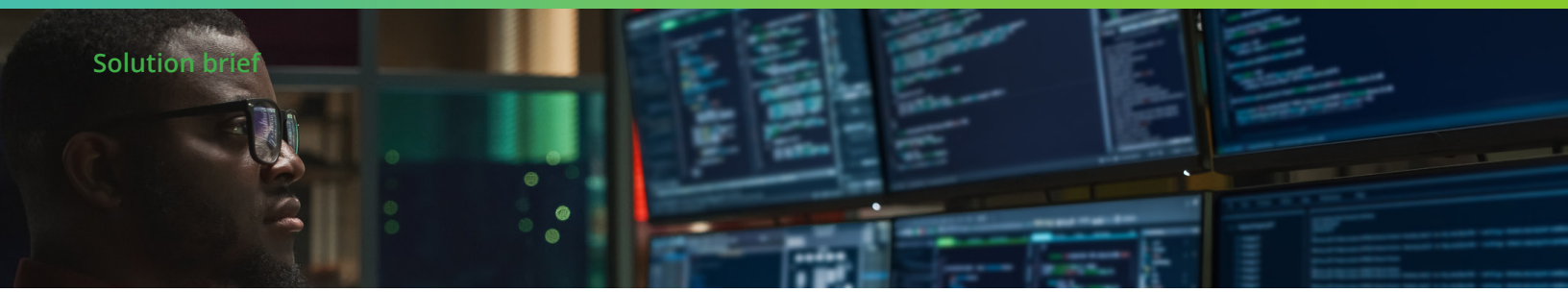
Large volumes of files are sent across enterprise networks every minute, giving attackers an opportunity to infect and spread malware across an organization—maliciously including code into files or disguising malware as helpful software. To detect and respond to these threats today, security teams resort to analyzing files either on the endpoint or using a dedicated file analysis solution. However, file analysis on endpoints has limitations:

- **Increased false positives**
  EDR tools can generate a large number of alerts with significant false positives, requiring analysts to sift through to find potential threats.
- **Lack of necessary context**
  Advanced attacks like modular RATs download a limited set of features. Lack of network context makes these difficult to detect.
- **Malware detection failures**
  An unsigned DLL with suspicious filenames is a common alert. If the hash value of the DLL does not match the EDR database, it can be easily missed.
- **EDR bypass**
  Malware can be delivered with EDR bypass techniques such as DLL sideloading, obfuscating a command line, or using code-signed malware.

Further, using a dedicated solution for file extraction and analysis adds yet another tool to a growing list of tools in the SOC. The management and maintenance of a DIY or custom solution can be cumbersome and resource intensive in the long term.

THE SOLUTION

Corelight delivers static file analysis powered by YARA in a single-sensor solution that enables security teams to create specific YARA rules for pattern-based detection that can quickly analyze large volumes of files and get the benefits of Corelight's Open NDR Platform. Users can streamline operations with a fully integrated solution that includes static file analysis, a complete suite of detection capabilities including AI/ML, network security monitoring, and packet capture in a single platform that is powered by both proprietary and open-source technologies including Zeek®, Suricata®, and now YARA.



Improve visibility: inspection at the network layer

- Inspect volumes of files transferred throughout the infrastructure
- Analyze large amounts of files for pattern matches
- See data exfil attempts where attackers use encoding techniques
- Detect compromised files

Detect threats faster: pattern matching at scale

- Discover unique strings, binary patterns, and behavior patterns in files beyond file hash matching
- Create custom detections
- Trigger alerts and surface files that pose threats
- Prioritize known threats and suspicious patterns

Accelerate SOC efficiency: consolidate for results

- Consolidate legacy IDS, PCAP, and other tool sets into a single-sensor solution
- Streamline management for network-based static file analysis with embedded YARA rules
- Build, configure, and deploy YARA rules through an easy-to-use, intuitive user interface
- Seamlessly integrate into existing solutions for response

THE SOLUTION IN ACTION

An Outlook calendar invite was shared to a department calendar at a Fortune 2000 Corelight customer. A file attached to the calendar invite matched a known Outlook vulnerability. Corelight, through YARA rules, was able to detect the malicious file and create an alert for the security team to review and remediate.

Evasive malware detected. Case closed.

HOW IT WORKS

1. Configure and manage YARA rules from Corelight Fleet Manager for easy deployment across sensor infrastructure. Upload an existing rule or draft a new one using a text editor.

2. The Corelight Sensor will search in extracted files for the unique strings, binary patterns, or behavior patterns outlined in the YARA rules.

3. When a YARA rule is triggered, Corelight generates a notice, alerting security teams to review it. These alerts indicate a potentially malicious file and can be forwarded to Investigator, SIEMs, or EDR/XDR platforms for investigation and response.

The solution architecture

1 Configure rules

2 Search for unique strings, binary patterns, or behaviors

3 Generate an alert