corelight

White Paper

Advanced file inspection with YARA on Corelight Sensors

WHAT IS YARA?

Malware detection using hashes is a cat-and-mouse game, and malware authors regularly make minor changes to their malware in order to change the hashes and avoid detection. YARA is an open-source file-analysis framework that allows rule authors to write rules that examine file characteristics and create alerts when files match those characteristics. Because YARA rules inspect the contents of files instead of just hashes, they are more resilient and provide durable, longer-term detection capabilities. YARA is popular with threat hunters and incident responders for its flexibility, which makes it easy to adapt detection to intrinsic characteristics in the contents of files and executables. With YARA, defenders can expand their reach instead of only relying on static file indicators like filename or cryptographic hash, making it harder for attackers to avoid detection.

WHY USE YARA WITH NETWORK DETECTION AND RESPONSE (NDR)?

Files are frequently and organically present in network traffic. By extracting files from network traffic and analyzing them with YARA rules, defenders can take advantage of the centralized vantage point that the network offers and inspect traffic from managed and unmanaged devices alike. Since endpoint detection is restricted to managed devices with endpoint agents installed, there are gaps in the environment anywhere endpoint agents aren't installed. File inspection with YARA and NDR therefore complements file inspection using endpoint agents. YARA file analysis alerts provided by Corelight are linked to the metadata about the file and about the network protocol and session used to transmit the file, thus providing analysts with all the information they need to quickly investigate file analysis alerts without needing to pivot to other systems for additional information.

File inspection overlaid on an intrusion detection system (IDS) adds a layer of analysis that provides an additional signal for analysts looking at alerts. If there are network detections related to a particular strain of malware and there are also file analysis alerts for files downloaded by the same device, these alerts provide an additional confirmation of the severity of the situation. With Corelight, security engineers can consolidate IDS, file analysis, and packet capture into one appliance, saving rack space, power, and management overhead.

YARA FOR DETECTION ENGINEERING

Detection engineers are always looking for new opportunities to detect techniques and practices of threat actors and malware authors, and to adapt security controls to enterprise security policy. YARA, with its flexibility, makes for an excellent mechanism to create custom rules that detect files matching certain characteristics, especially those that wouldn't be considered "malicious" by an endpoint detection and response (EDR) agent, like:

- RDP configuration files
- Files containing sensitive or private information
- Files containing company proprietary information
- Executables that are engineered to be fully undetectable by malware analytics but contain some special characteristics that reverse engineers can extract and use for detection

THREAT HUNTING WITH YARA

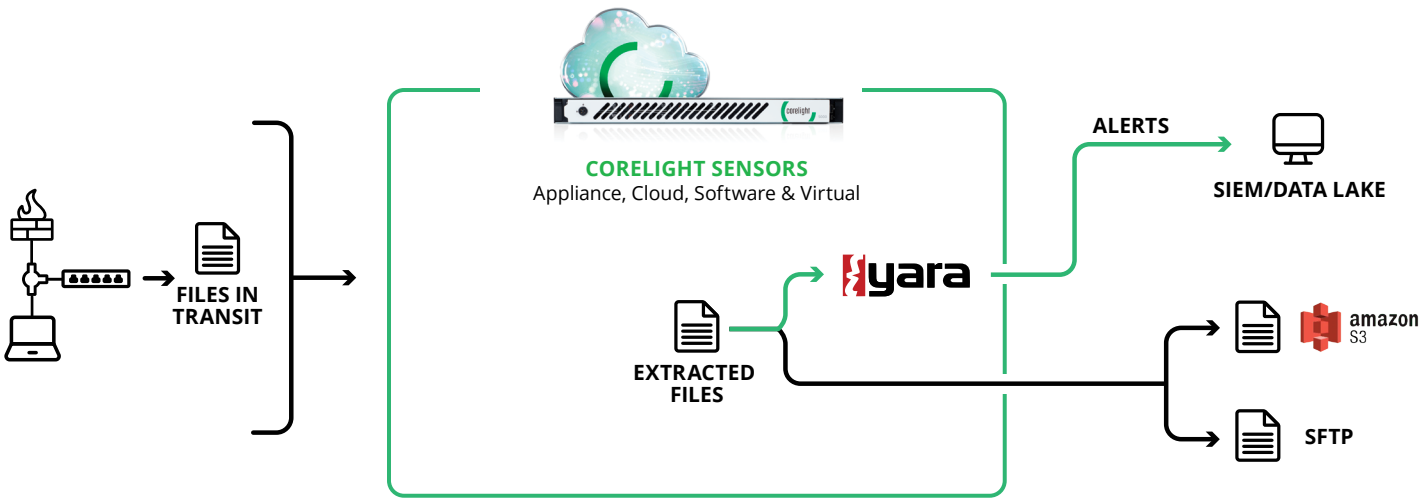
Threat hunters use YARA to look for files with specific characteristics that more generally may be associated with techniques that threat actors use, but which don't always completely translate to actionable detections. Each hit from these YARA rules is a file that becomes a candidate for additional analysis, such as dynamic analysis or reverse engineering. With Corelight, these rules can be leveraged to automatically extract candidate files from network traffic and have them waiting on disk for hunters and reverse engineers to inspect.

USING YARA FOR INCIDENT RESPONSE

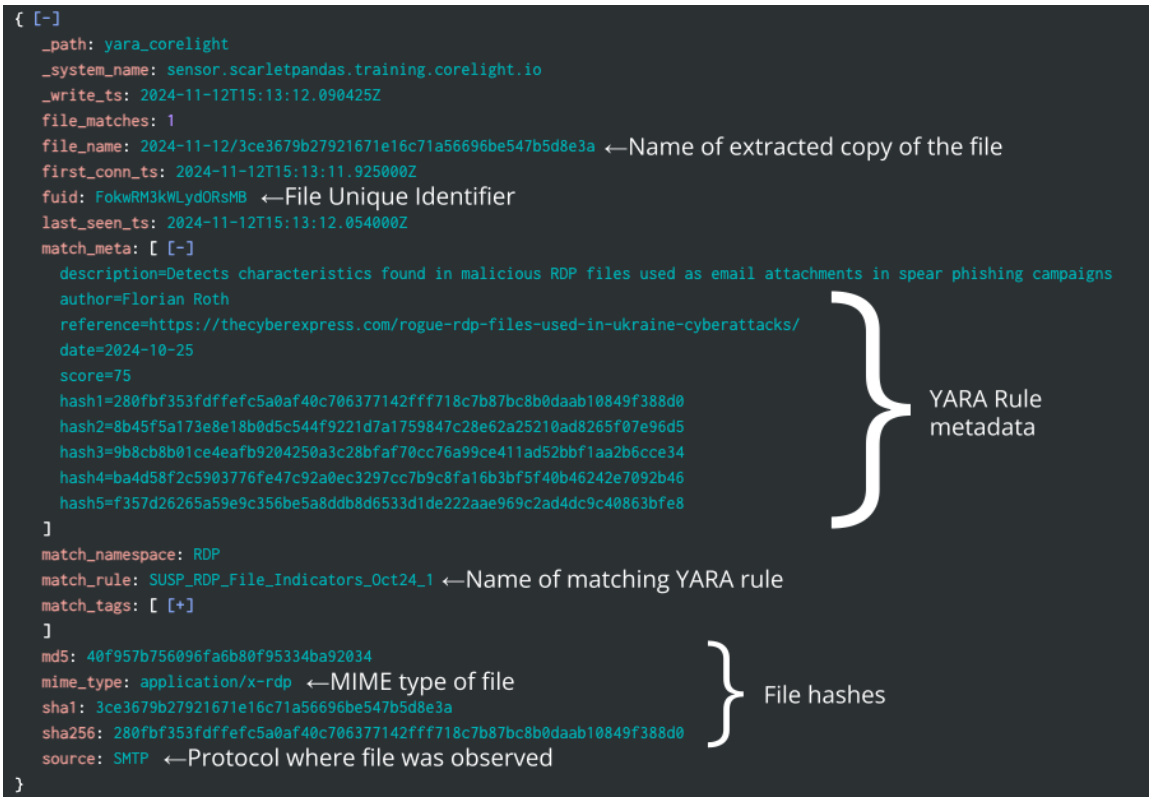
In the height of an incident, speed counts. Defenders need to understand who, what, when, where, and how, and they need to remain apprised of changes in the situation as quickly as possible. Corelight's Open NDR provides defenders with rich network evidence that they can search for signs of attacker behaviors in the network traffic. Defenders can leverage the integrated Suricata IDS to develop custom rules that apply incident knowledge to real-time network detection, and Smart PCAP can provide packet captures of network sessions based on the defender's preferences. YARA's flexibility and speed allow defenders to apply this detection customization to files observed in the network traffic as well, ensuring that they see from every angle.

HOW YARA IS INTEGRATED INTO CORELIGHT SENSORS

1. Corelight administrators upload one or more rule files to build a YARA rule set on a Corelight Sensor or in Corelight Fleet Manager.
2. Corelight administrators adjust the file extraction settings in the configuration policy to determine what file types to extract from the network traffic. Extraction is based on observed file (MIME) type, so administrators can scope extraction and YARA analysis to only the file types they deem a high risk or priority, and the file extension, if present, is not a factor in deciding what files to extract or analyze.
3. Corelight Sensors send all files destined for extraction through the YARA engine with the rule set applied. Alerts from the YARA engine are forwarded to Corelight Investigator and the customer's SIEM (if applicable), along with all other Corelight logs and telemetry, based on the customer's sensor configuration.
4. Extracted files are also forwarded to any configured file extraction destinations, such as object storage targets or an SFTP destination. Files are named by their cryptographic hash, so that analysts can easily retrieve them for further analysis based on information that is readily available in the logs.



EXAMPLE OF A CORELIGHT YARA LOG



WHY YARA AND CORELIGHT

Integrating YARA into Corelight Sensors significantly enhances your network defense strategy by enabling advanced, content-based file inspection at the network layer. This integration allows you to detect malicious files based on their intrinsic properties, offering superior resilience against evasion tactics employed by attackers. By bridging the visibility gaps left by unmanaged devices and augmenting your detection capabilities across detection engineering, threat hunting, and incident response, YARA and Corelight together provide a powerful toolset.

corelight

To learn more, request a demo at **https://corelight.com/contact**

info@corelight.com | 888-547-9497