JOINT SOLUTION BRIEF

Mira ETO and Suricata Solution to Give You Optimal Security and Visibility

The Business Problem

The use of encrypted SSL/TLS traffic has been on the rise for many years now. It has become the standard that most users and applications expect. Its ease of implementation has allowed organizations of all sizes to utilize it. However, this has also created a blind spot for IT administrators. While protecting data from prying eyes, it can also conceal malicious files from network security tools, allowing them to slip into the network unseen. It has become clear that organizations require visibility into encrypted SSL/TLS traffic in order to protect their employees, customers, and business. While providing visibility into traffic sounds great, it should not be at the expense of performance or security. The end user should not be impacted by the visibility which should be transparent, safe, and secure.

The Solution

Mira Security's Encrypted Traffic Orchestrator (ETO) decrypts that SSL/TLS traffic and gives visibility by delivering the traffic flows to Suricata, which is able to inspect this traffic and take action on it. They are able to detect files that are in SSL/TLS traffic flows that they wouldn't be able to detect normally. Despite decrypting SSL/TLS traffic, they still maintain security by keeping the plaintext traffic only between the ETO and Suricata.

Joint Solution Benefits

- **Visibility.** The ETO eliminates SSL/TLS blind-spots allowing Suricata to detect traffic that might otherwise be hidden by encryption. The ETO is capable of decrypting SSL v3, TLS 1.0, 1.1, 1.2, and 1.3, as well as SSHv2.
- **Scalable.** The ETO is available with 1G, 10G, 25G, and 40G interface speeds and allows for high throughput. Suricata uses multi-threaded signature detection which allows it to scale, and is able to inspect traffic at up to 40G.
- **Flexible.** Port-agnostic decryption allows the ETO to decrypt on more than just port 443. Port- agnostic protocol detection allows Suricata to detect suspicious traffic regardless of whether it's on the port that it would be expected to be on. Suricata can also be configured as either IDS, IPS, or NSM, allowing it to fill many functions.
- **Rules.** Use the ETO's Category Database to bypass certain categories of traffic and protect sensitive user data. Easily create custom rules for Suricata or automatically update the rules from subscription services.
- **Support for different Platforms.** The ETO is available as a physical appliance (hardware) or virtual appliance (that runs on KVM or VMware ESXi) to fit the needs of various networks.

The ETO is available as a physical appliance (hardware) or virtual appliance (that runs on KVM or VMware ESXi) to fit the needs of various networks.

KVM

vmware ESXi

Typical Deployment Topologies

Network Inline – Suricata IDS Passive

The ETO sits in the middle of the traffic flow between the client and the server. When the SSL/TLS handshake occurs, the ETO actively decrypts the traffic and passes the plaintext data over to Suricata to analyze it. Then it re-encrypts the data and sends it on to the destination, maintaining the end-to-end connection in an encrypted form.

Network Inline – Suricata IPS Inline

The ETO sits in the middle of the traffic flow. When the SSL/TLS handshake occurs, the ETO actively decrypts the traffic. It passes this plaintext data over to the Suricata platform which then analyzes it and removes any threats it detects before passing the traffic back to the ETO. ETO then re-encrypts the data and sends it on to the destination.

About Suricata

Suricata is a high-performance Network IDS, IPS and Network Security Monitoring engine. Open Source and owned by a community-run non-profit foundation, the Open Information Security Foundation (OISF). Suricata is developed by the OISF and its supporting vendors.

Visit https://suricata.io to learn more.

MiraSecurity.com

mira SECURITY

info@mirasecurity.com

Mira Security
3159 Unionville Road, Suite 100
Cranberry Township, PA 16066
Phone: +1 (412) 533-7830

Email: info@mirasecurity.com
mirasecurity.com

MIRA-SURICATA-11/22