INTRUSION DETECTION SYSTEM (IDS) LOG ANALYSIS WITH SURICATA

This course is designed for new or experienced Network Analysts to automate some of the detections of malicious network traffic. It begins with the basics of network ingestion and Suricata configuration to ingest data into the Elastic Stack. Next, you will learn the various components of a Suricata rule. Finally, we learn how to use Regular expressions to write more effective rules.

This course is part of the Elastic Network Security Analyst Learning Plan. Please review the pre-reqs section for additional information.

LESSONS

All lessons include a hands-on lab.

Getting traffic to Suricata via common traffic capture methods
Learn about common traffic capture methods used to feed data to Suricata. Understand which configuration, a TAP or SPAN, is useful for the type of environment you will be using.

Suricata overview
Learn about how Suricata uses a rule-set to compare against incoming traffic to assist in analysis of traffic coming across the network. At the end of the lesson you will be able to identify the difference between Suricata's Intrusion Detection and Intrusion Prevention Modes. Lastly, we will cover where Suricata may be found in the overall security architecture in your environment.

Continued on the next page

COURSE INFORMATION

Audience
Network Analysts
Security Engineers

Duration
8 hours

Language
English

Prerequisites
- Linux Fundamentals
- Network Protocol Analysis
- Packet Analysis
- Intrusion Detection System (IDS) log analysis with Suricata
- Network Metadata log analysis with Zeek
- Kibana Security Analyst

Requirements
- Stable internet connection
- Mac, Linux, or Windows
- Latest version of Chrome or Firefox (other browsers not supported)
- Disable any ad blockers and restart your browser before class

elastic

INTRUSION DETECTION SYSTEM (IDS) LOG ANALYSIS WITH SURICATA

LESSONS

All lessons include a hands-on lab.

Configuration and setup of Suricata

Learn the basic installation requirements and procedures for Suricata. Learn how the configuration file can help define how Suricata will identify key attributes of your network architecture and provide different output formats to the user.

Suricata rule structure and options

Learn and identify the key components of a Suricata rule. Understand how they fit together to improve detections and relieve some of the burden from your network analysts.

Suricata rule writing using common protocols

Learn how to apply the rule structures we learned against a well known protocol. Instructor will walk through each step of the process to create a rule to match against HTTP and DNS.

Using Regular Expressions (REGEX) and Perl Compatible Regular Expressions in Suricata

Learn how different Regular Expressions can improve your detection results in Suricata. Learn how to distinguish between a simple string to complex expressions that leverage collections, anchors, quantifiers, and Wildcards.