INFOSECTRAIN

TOP 12

Open Source Tools for Threat Hunting

www.infosectrain.com

INFOSECTRAIN

Yara

Feature

Identifies and classifies malware through rule-based patterns for threat detection.

TheHive

Feature

Collaborative incident response platform manages and analyzes security events efficiently.

ELK (Elasticsearch, Logstash, Kibana) Stack

Feature

Centralizes, analyzes, and visualizes logs for real-time threat detection.

Sigma

Feature

Generic signature format converting logs into SIEM queries for threat detection.

INFOSECTRAIN

Snort

Feature

Real-time network traffic analysis and packet logging, detecting attacks and unusual behavior.

Suricata

Feature

Multi-threaded intrusion detection system provides network traffic analysis and threat alerts.

OSQuery

Feature

SQL-powered visibility tool querying operating system data for threat hunting.

Zeek

Feature

Network analysis framework offering detailed traffic insights for security monitoring.

INFOSECTRAIN

GRR Rapid Response

GRR RAPID RESPONSE

Feature

Identifies and classifies malware through rule-based patterns for threat detection.

Cuckoo Sandbox

Feature

Malware analysis tool executes and inspects suspicious files in virtualized environments.

MISP

MISP
Threat Sharing

Feature

Threat intelligence platform sharing Indicators of Compromise (IoCs) for collaborative defence.

Falco

Falco

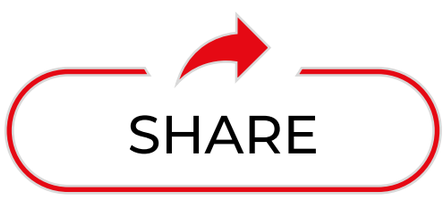
Feature

Runtime security tool, monitoring container activities and detecting abnormal behavior.

FOUND THIS USEFUL?

To Get More Insights Through Our FREE

Courses | Workshops | eBooks | Checklists | Mock Tests



INFOSECTRAIN