

WELCOME!

Network Security Monitoring with Suricata



Provide you with all the basic knowledge, instructions, information, and skills needed to get started with Suricata.

Our hope is this course sparks your curiosity to join us for one of our live 2-day classes

<https://suricata.io/learn/>

What to Expect

- Self-Guided sections
- Section length -> 45 - 90 minute
- Lots of hands-on, real-world exercises and demonstrations
- Labs and comprehensive lab guides
- Quizzes to test what you've learned (don't stress, they are fun!)

Need Help?

Use the discussion feature in the learning software!

Contact our Training Team: training@oisf.net

Contact our Dev Team via the Suricata
Community Forum:
<https://forum.suricata.io/>

Section 1 - Course Introduction

1.1 - Welcome

1.2 - OISF and Suricata

1.3 - Intrusion Detection and Prevention - The Basics

1.4 - Lab: The Training VM

1.5 - Demo: Getting Started with the Training VM

Section 2 - Suricata Basics

2.1 - Introduction to Network Security Monitoring

2.2 - Demo: Introducing the Training VM

2.3 - Suricata Common Operations

2.4 - Demo: Working with Suricata

2.5 - Updating Rules

2.6 - Demo: Working with Suricata-Update

Section 3 - Suricata Core Functions

3.1 - Alert Generation

3.2 - Demo: Generating Alerts and Querying EVE.JSON

3.3 - Basic Rule Comprehension

3.4 - Demo: Working with Rules

3.5 - Tuning out the Noise

3.6 - Demo: Working with Suricata's Configuration File

3.7 - Suricata's Investigative Data Outputs

3.8 - Demo: Extended Logging

Section 4 - Enterprise Suricata Deployments

- 4.1 - Deployment Modes
- 4.2 - Network Placement and Capture Methods
- 4.3 - Modifying Rules with Suricata-Update
- 4.4 - Demo: Working with modify.conf
- 4.5 - Integrating Suricata into Your Security Stack
- 4.6 - Demo: Shipping Suricata Logs with Filebeat
- 4.7 - Working with Files on the Wire
- 4.8 - Demo: Extracting Portable Executable (PE) Files

Section 5 - Now You're Ready!

5.1 - Let's Recap

5.2 - Test Your Suricata Skills

5.3 - Ready to Level Up? We can help...

5.4 - Getting Involved

More Resources

- Read the Docs: <https://readthedocs.org/projects/suricata/>
- More Suricata trainings/webinars: <https://suricata.io/learn/>
- Learn about OISF: <https://oisf.net/>
- SELKS 6: <https://www.stamus-networks.com/selks-6>
- EveBox: <https://evebox.org/>
- ELK 7 ready to use Dashboards/Vizs 450+
<https://github.com/StamusNetworks/KTS7>
- Grafana 7+ Dashboards/Vizs
https://github.com/b4b857f6ee/selks_grafana_dashboard



OISF



SURICATA

Open Information Security Foundation (OISF)

US 501(c)3 non-profit organization that ensures Suricata remains world-class.

Dedicated to preserving the integrity of open source security technologies and the communities that keep them thriving. Our team and our community includes world-class security and non-profit experts, programmers, and industry leaders dedicated to open source security technologies.

Funding for Suricata comes from donations from world-class security organizations committed to our mission. A list of these organizations is available on our [Consortium Members](#) page.

About Suricata

- First lines of code written in 2009 by Victor Julien
- Powered by Open Source GPLv2 (source on GitHub)
- Worked on/Developed with a global open source community in over 23 different countries

“Swiss Army Knife” of Network Monitoring

- Intrusion Detection (IDS) - passive
- Intrusion Prevention (IPS) - active
- IDPS - hybrid
- Security logging - totally passive
- PCAP digest - read PCAP or folders of PCAPs

Open Source ≠ Free to Develop

- OISF is a nonprofit organization, therefore any funding or support we get goes directly to Suricata's roadmap.
- Development is funded through contributions from world-class security organizations -> [Consortium Members](#), SuriCon Sponsors, and more.
- Support OISF and Suricata - visit <https://oisf.net/> or contact us at info@oisf.net

Community Forum

<https://forum.suricata.io/>

Connect with the OISF's development team and world-wide community using Suricata every day - bring your questions, challenges, ideas, breakthroughs, research ideas, or simply come to ask for help.

Meet the Community



<https://suricon.net/>

NEXT

Module 1.3 Intrusion Detection and Prevention -> The Basics



Get Involved

Supporting Suricata



Intrusion Detection and Prevention The Basics



Suricata

- Suricata is a high-performance network security monitoring engine with IDS, IPS capabilities.
- Open-source software - find it on Github. (<https://suricata.io/download/>)
- Produces a high-level of situational awareness and detailed application layer transaction records from network traffic.
- Most robust and effective threat hunting technology available today - and open source!

Network Security Monitoring

Network security monitoring (NSM) is network data collection & analysis.

- Entire ecosystem of bundled tools/software:
 - Stand alone
 - Distributed (multiple servers/systems)
- Suricata plays a central role in generating valuable data:
 - Logs
 - Events
 - Metadata and protocols
 - Alerts

Suricata Capabilities

- Standards based formats (YAML, JSON) ease integrations with SIEM or other analysis tools
- Multithreaded, hardware acceleration available
- Native IPv6
- Auto protocol detection
- Advanced HTTP/HTTP2, DNS, SMTP and TLS support
- File extraction - FTP/SMTP/HTTP/HTTP2/NFS/SMBv1/2/3
- File MD5, SHA1 and SHA256 checksum support
- Netflow output available

Suricata Capabilities Con't

- Lua scripting
- IP lists, IP reputation and GeoIP
- Bypass (deals with Elephant flows)
- Community ID
- JA3/JA3S
- SCADA protocols - DNP3, ENIP, CIP and Modbus
- Full Packet Capture (FPC)

IDS vs IPS

- Intrusion Detection System
 - **Passive** system used to identify specific or anomalous traffic on a network
 - Generally implemented in an “out-of-band” architecture
 - Acts as a “network **monitor**”
- Intrusion Prevention System
 - **Active** system used to identify specific or anomalous traffic on a network
 - Generally implemented inline with the network flows
 - Acts as a “network **control** system”

Type -> Signature Based

- Relies on a set of pre-configured list of rules for known behaviors
- These behaviors will trigger when matched
- These signatures, or rules, can include:
 - Specific IP address(es), port(s), protocol combinations
 - Patterns in popular protocols, such as HTTP
 - Specific user activity, such as downloading executable files