Extensions, Frameworks, and Integrations Used with Snort

Expand Snort Capabilities

Joe Abraham
Cybersecurity Consultant

@joeabrah www.defendthenet.com


API

Information sharing is crucial to cyber operations!

Extensions, Frameworks, and Integrations Used with Snort

Expand Snort Capabilities

Joe Abraham
Cybersecurity Consultant

@joeabrah www.defendthenet.com

Meet the Team

Kali

Globomantics' Security Engineer

Tre

Globomantics' SOC Analyst

What You'll Learn Here

Expand Snort's Capabilities

Optimize Snort Data

Snort Pre-processors

Snort Plugins

Manage Snort Rulesets

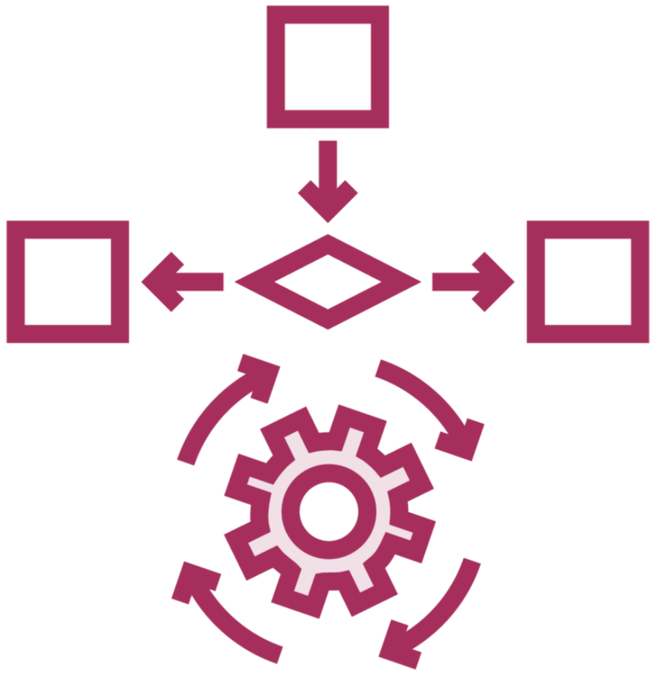
Network Security Monitoring with Snort

Getting Started with Snort 3

Writing Snort 3 Rules

Extensions, Frameworks, and Integrations Used with Snort

Snort's Expansion Capabilities



Expanding Snort with Cisco

- Cisco Secure Firewall
- Pulled Pork
- The PigDoktah
- Daemonlogger
- Razorback
- Snort-vim

Security Onion

Sguil

BASE

Snorby

PacketFence

OSSIM

Third Party Integrations

Snort Plugins

Plugins allow you to expand the tool even more

Over 200 by default with Snort++ Extras

- **Output plugin**

Detection plugins and preprocessors

OpenAppID plugin

https://snort.org/documents

Integrating and Using Snort with pfSense

Snort and pfSense

GUI Interface

Add Context to Alerts

Manage Rulesets

Demo

Explore pfSense/Snort integration

The Elastic Stack and Snort

Elastic Stack Tools

Elasticsearch is a distributed, RESTful search and analytics engine

Kibana is a free and open user interface that lets you visualize your Elasticsearch data and navigate the Elastic Stack

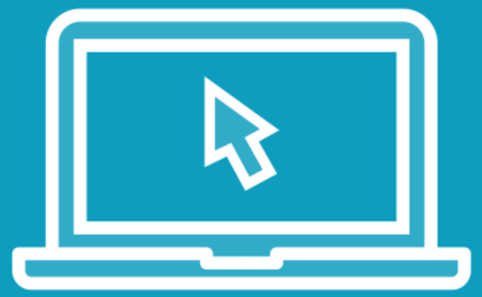
Logstash is a free and open server-side data processing pipeline that ingests data from a multitude of sources, transforms it, and then sends it to your favorite "stash."

Beats is a free and open platform for single-purpose data shippers


Security
Information and
Event
Management

https://www.elastic.co/guide/index.html

Demo



Explore Elastic Stack configurations for Snort

Module Summary

Discussed Snort's expansion capabilities

Snort + pfSense

Snort + SIEMs

Up Next:
Optimize Snort Data