Manage Snort Rulesets

Joe Abraham
Cybersecurity Consultant

@joeabrah www.defendthenet.com

Default Rulesets

Connectivity over Security

Favors performance over security controls

Balanced

Default recommended policy for initial deployment

Security over Connectivity

For protected networks and high security requirements

Maximum Detection

Combines rules in other three rulesets

Updating rules and rulesets helps detect new and emerging threats

Rule Management Automation

GUI-based tools

Cron jobs

Automation scripts

Managed platforms

Manual downloads and updates

New and Emerging Threats

Can be detected and blocked via new and updated rules

IP blocklist updates also assist with detection and mitigation

Introducing Pulled Pork 3

How it's Cooked

Originally built in Perl for Snort 2

Snort 3 version written in Python 3

Installs with mostly standard Python libraries

Installs on Windows, Linux, and other Unix-based systems

pulledpork.conf file is configuration file

Pulled Pork Configuration

Pulledpork.conf

```
# Which Snort/Talos rulesets do you want to download
community_ruleset = true
registered_ruleset = false
LightSPD_ruleset = false

# which blocklists to download
snort_blocklist = false
et_blocklist = true

# additional blocklists to download from a
URLblocklist_urls = http://a.b.com/list.list

# Where to write the blocklist
blocklist_path = /usr/local/etc/lists/default.blocklist

ips_policy = balanced

rule_path = /usr/local/etc/rules/pulledpork.rules
```

Demo

https://github.com/shirkdog/pulledpork3

Install and validate Pulled Pork 3

Demo

Use Pulled Pork 3 to modify rulesets and blocklists in real time

Reviewing Snort's Additional Capabilities

Expanding Snort's Capabilities

Cisco tools

3rd party tools

Firewall integrations

SIEM integrations

Optimizing Snort Data

Snort output plugins

Elastic stack visualizations

Cisco Secure Firewall

HTTP Inspect

sfPortscan

AppID

Additional Important Pre-processors

Information About Plugins

Introduced in Snort 1.5

Started as detection plugins or pre-processors

Detection plugins look for specific aspects of packets

Snort 3 has full plugin system

Snort 2 only provides pre-processor and output plugins

Additional Snort Resources

https://www.snort.org/documents#OfficialDocumentation

Pluralsight Skill Path: Network Monitoring with Snort

https://blog.snort.org

https://www.snort.org/integrators

Demo Placeholder

Thank You!