Snort Plugins

Joe Abraham
Cybersecurity Consultant

@joeabrah www.defendthenet.com

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

How to Write Plugins

C++ or LuaJIT

Create custom plugins with these languages

Snort++ Extras

Example plugins to assist with custom plugin development

Output plugin:

alert_fast

alert_fast

alert_smb

alert_unixsock

log_tcpdump

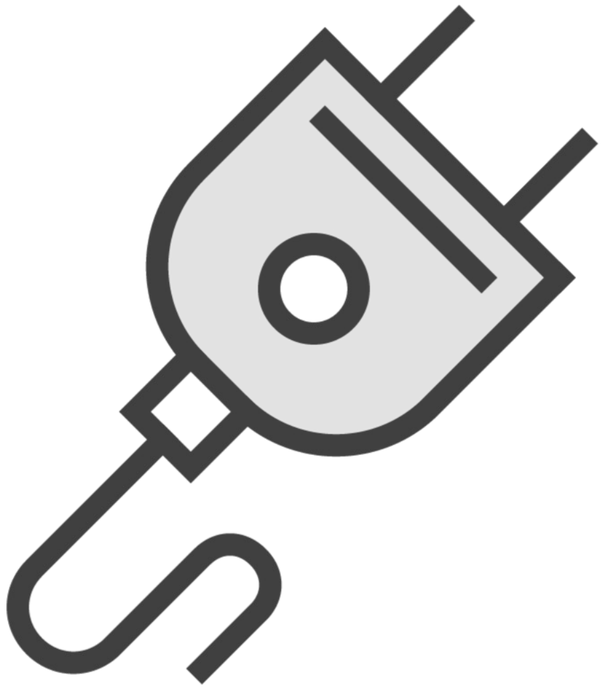
csv

xml

alert_syslog

What Plugins Do?

Snort 3 Plugins



- **Codec**
- **Data**
- **Inspector (Pre-processor)**
- **IPS Option**
- **IPS Action**
- **Search Engine**
- **Logger**
- **SO Rules**

Plugins with Snort++ Extras

AppID Listener

Snort.lua

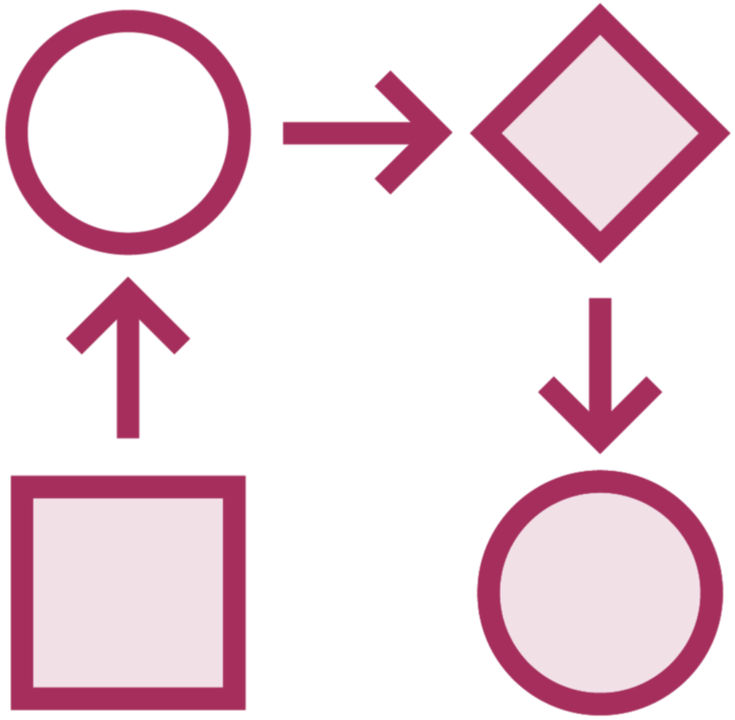
```
appid =
{
    -- appid requires this to use appids in rules
    app_detector_dir = '/usr/local/lib'
}

appid_listener =
{
    json_logging = true,
    file = 'var/log/snort/appid_stats.log',
}
```

LuaJIT

Lua “Just-in-Time” Compiler

https://luajit.org/luajit.html



codec::raw v0 static

codec::tcp v0 static

codec:udp v0 static

inspector::file_id v0 static

inspector::ftp_data v0 static

ips_option::sha512 v0 static

ips_option::sip_header v0 static

ips_option::tos v0 static

logger::alert_csv v0 static

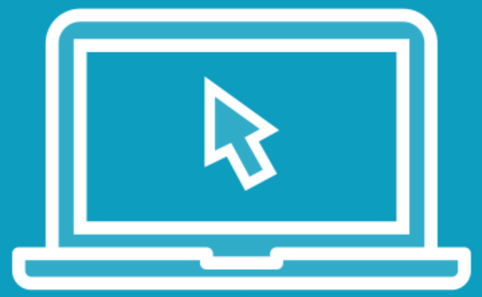
logger::alert_json v0 static

https://github.com/snort3/snort3_extra

Demo

Install Snort 3 Extras

Demo



Configure and use Snort 3 Extras plugin

AppID Example Review

```
globolab@globopcap: ~/snort_src
stream_udp
                  sessions: 4
                       max: 4
                   created: 4
                  released: 4
              total_bytes: 1380
-------------------------------------------------
wizard
                 tcp_scans: 58
                  tcp_hits: 3
                tcp_misses: 2
                 udp_scans: 1
                udp_misses: 1
-------------------------------------------------
Appid Statistics
-------------------------------------------------
detected apps and services
               Application: Services   Clients    Users      Payloads   Misc       Referred
                       dns: 3          3          0          0          0          0
                       ssl: 1          0          0          0          0          0
                     https: 2          0          0          0          0          0
                ssl_client: 0          2          0          0          0          0
                 microsoft: 0          0          0          1          0          0
                    splunk: 0          0          0          1          0          0
wap_connectionless_sessio: 1          0          0          0          0          0
                   unknown: 4          0          0          1          0          0
-------------------------------------------------
Summary Statistics
-------------------------------------------------
process
                  signals: 1
-------------------------------------------------
timing
                  runtime: 00:00:16
                  seconds: 16.978829
                 pkts/sec: 144
```

Up Next:
Manage Snort Rulesets