OISF
OPEN INFORMATION SECURITY FOUNDATION

Homeland Security

Brainstorming Session Agenda

RAID 2011, Menlo Park, San Francisco CA
Monday September 19, 2011

The Open Information Security Foundation (OISF) is a non-profit foundation organized to build a next generation IDS/IPS engine, Suricata.

The primary goal of this our fourth Brainstorming Session is to review and adjust the Development Roadmap. To do this we will outline the current complete features and development status, proposed features from public and private sources, and seek input on these items.

Any new idea, any new feature, any new relationship is welcome. This is an open discussion session. Let us know what you'd like your IDS/IPS to do!

Free Lunch will be available on a first come first served basis.

Not all topics will be covered in detail unless there are questions to keep the meeting moving along.

Project Funding Status

Release Schedule

Current Stable Features

Phase 3 Dev Roadmap

Technical Topics/Proposed Features

Byte_Extract

IP and DNS Reputation

File Extraction and Inspection

Unix Socket Output

Http_Host:

Regex Optimization

Rotating Pcap Support

Additional Protocol Recognition / Open DPI Integration

IP Only Match Payload Capture

HTTP Header Anomaly Preproc

Snortsam Output Plugin

SCADA Preprocessors

Replace Keyword

GeoIP Keyword

Performance Stats Addition

DNS Name Var Support

Host/App/OS Table Import

DNS Fast Flux/Anomaly Preprocessor

IP and DNS Reputation Distribution Spec

Alienvault’s Proposed Classification Schema

Time-based Counters

Passive Fingerprinting

Host Attribute Scrubbing

Mysql/Postgres/Sguil Output

SSL Cert Analysis

FTP-Data Stream Prediction / Exclusion

Live Ruleset Swap

Built-in Rule Testing

Digital Bond SCADA Preprocessors

Max Inspection Time Cutoff

Stateful Pattern Matching

Global Shared Flowvars

Snort Syntax Support Status

Homeland Open Security Technology Program