

Open Source Community Webinar

Joel Esler, Open Source Manager

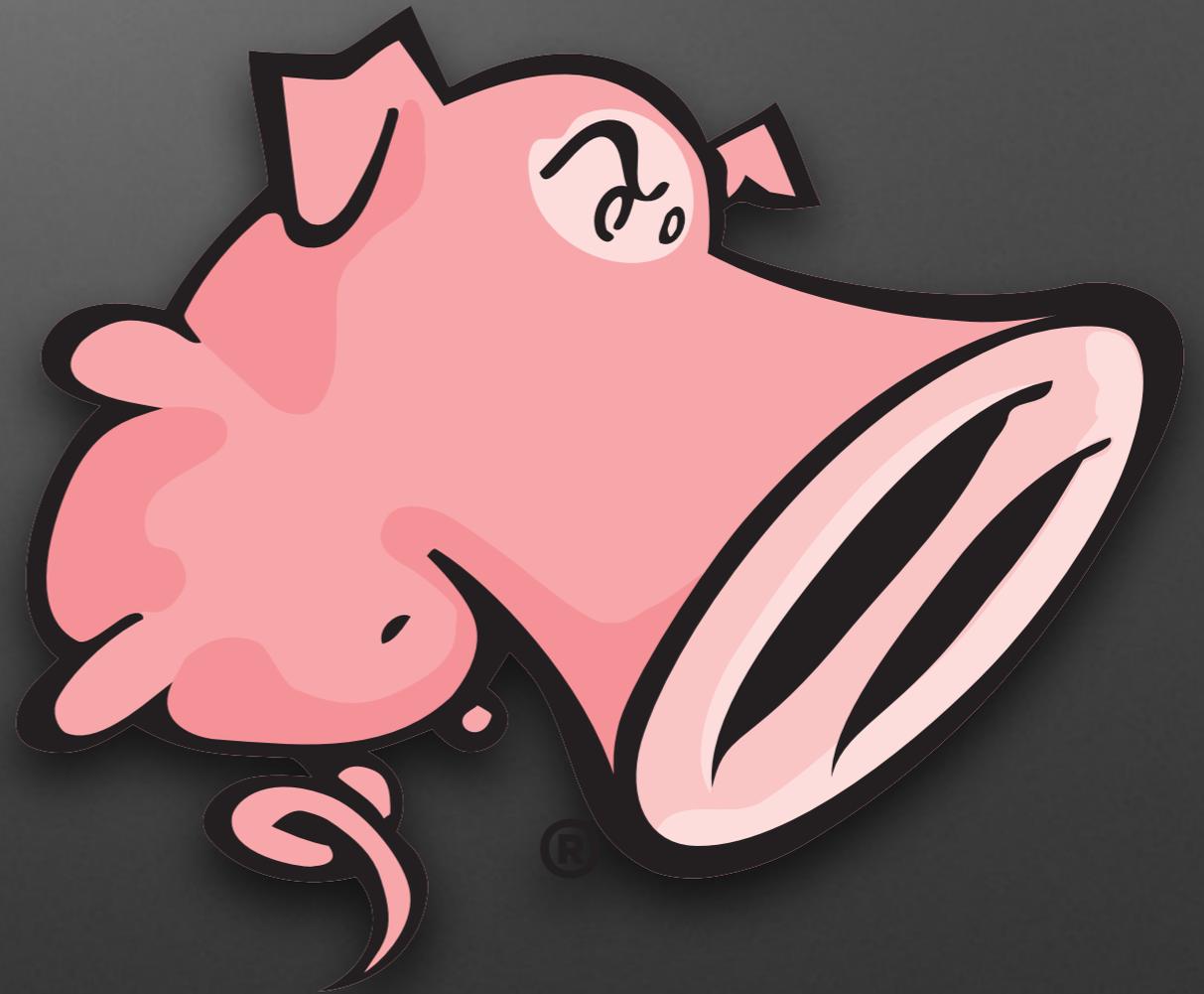
Agenda

- Snort Roadmap
- snort.org Roadmap
- ClamAV Roadmap
- Detection Roadmap
- Community Announcements
- Q&A

Snort Roadmap

Snort Roadmap

- OpenAppId
- Flash / PDF Decompression
- SMTP / POP / IMAP PAF Support
- File Type ID
- File Extraction
- Unicode File Name Support



OpenAppID – First OSS Application and Control

- Open App ID Language Documentation
 - Accelerate the identification and protection for new cloud-delivered applications
- Special Snort engine with OpenAppID preprocessor
 - Detect apps on network
 - Report usage stats
 - Block apps by policy
 - Snort rule language extensions to enable app specification
 - Append 'App Name' to IPS events
- Library of Open App ID Detectors
 - Over 1000 new detectors to use with Snort preprocessor
 - Extendable sample detectors



Available now at Snort.org

Auto-Detection of Services

- Find any protocol, on any port
- Find any application, on any port
- alert tcp \$HOME_NET any -> \$EXTERNAL_NET any
(msg:"Look for malware"; content:"malware"; nocase;
metadata:service http; sid:1;)

Flash / PDF Decompression

- The ability to expand a Compressed Flash File on the wire and inspect the contents
- The ability to decompress a “FlateDecode” compressed section of a PDF and inspect the contents

File Type Support

- The ability to inspect files by type.
- Released as experimental in 2.9.6.0
- Allows the ability to write rules to the type of file, instead of using flowbits to identify file type.

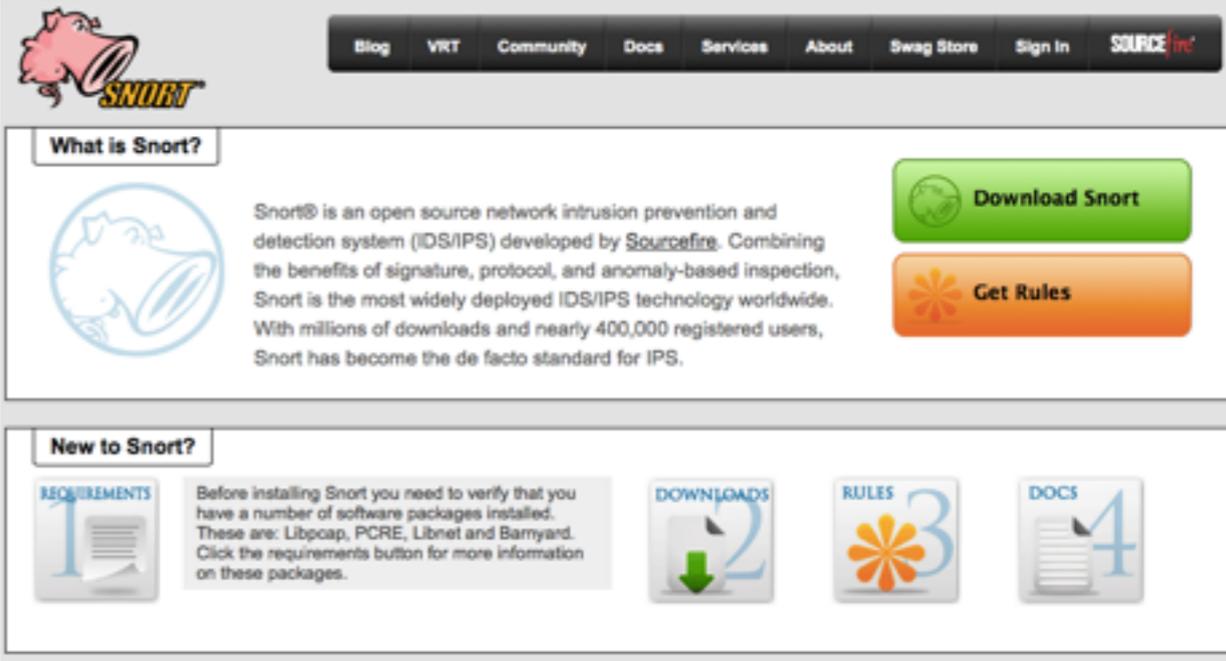
File Extraction

- The ability to extract files from network traffic and save them to disk.
- Supports SHA256 (will support md5 in future release)
- Ability to send files to another host for analyzation

snort.org roadmap

Current snort.org

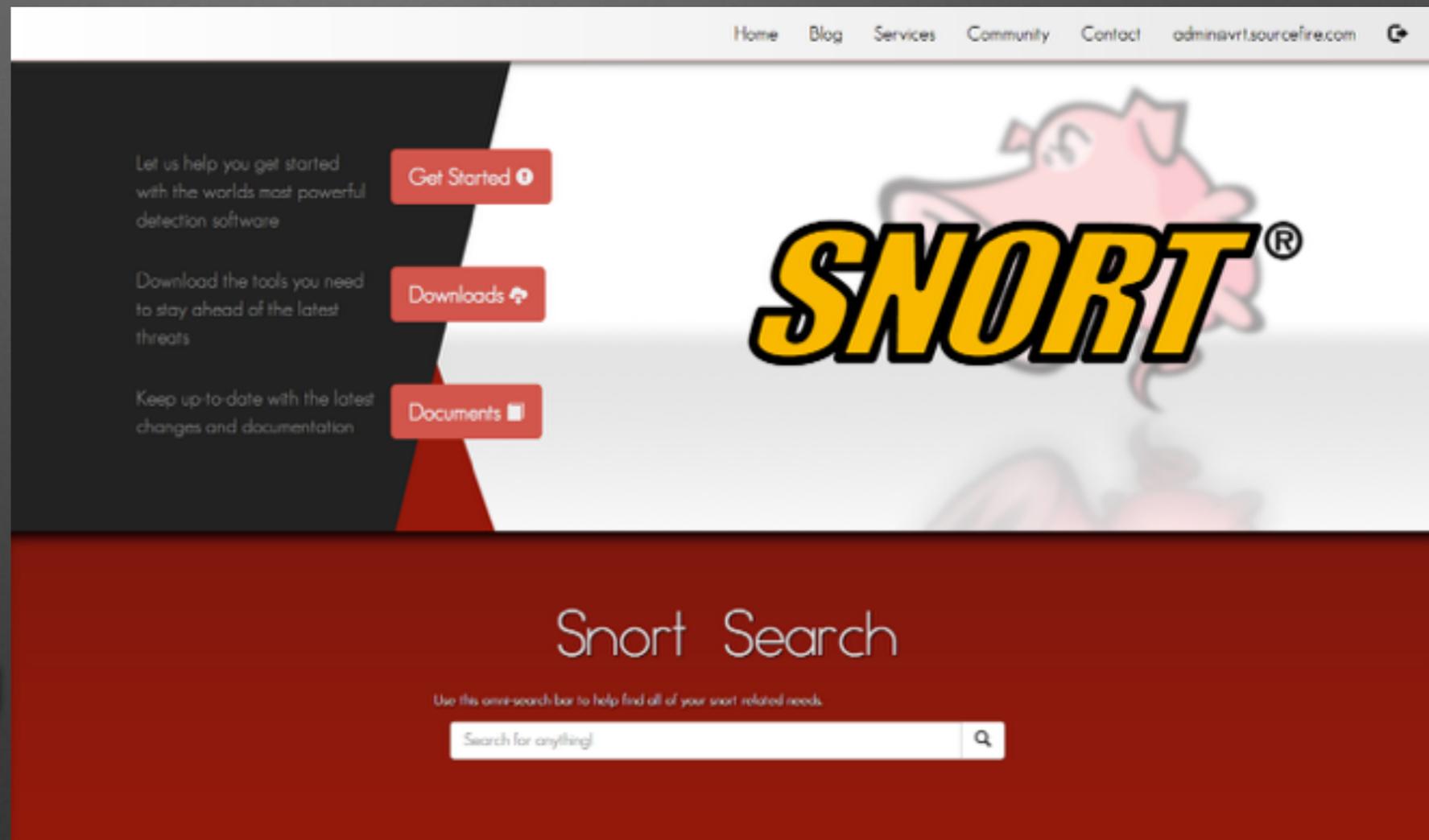
- Handles ~400,000 users
- ~100 new user accounts a day
- Hundreds of thousands of downloads a week
- On 2005 framework



The screenshot shows the snort.org website interface. At the top, there is a navigation bar with links for Blog, VRT, Community, Docs, Services, About, Swag Store, Sign In, and SOURCEfire. The main content area is divided into two sections. The first section, titled 'What is Snort?', features a blue circular logo of a pig's snout and a text block describing Snort as an open source network intrusion prevention and detection system (IDS/IPS) developed by Sourcefire. To the right of the text are two buttons: a green 'Download Snort' button and an orange 'Get Rules' button. The second section, titled 'New to Snort?', contains a list of four numbered steps: 1. REQUIREMENTS (with a document icon), 2. DOWNLOADS (with a download icon), 3. RULES (with a flower icon), and 4. DOCS (with a document icon). The text in the 'New to Snort?' section explains that before installing Snort, users need to verify that certain software packages (Libpcap, PCRE, Libnet, and Barryard) are installed and provides a link to the requirements page for more information.

snort.org

- Complete rewrite underway
- Faster
- Easier to navigate
- Simpler purchasing process



ClamAV Roadmap

ClamAV Roadmap

- OSX DMG Support (Just released)
- Telemetry Support
- OpenSSL
- IPv6 Support
- Bytecode enhancement
- OpenIOC
- Yara
- Json Output
- Memory and Registry Scanning



Telemetry

- Allows us to see the efficacy of the ruleset
- Detection Rates, Infection Rates, etc

OpenSSL

- Introducing OpenSSL as a dependency
- Faster calculation of hashes
- Overall performance improvement of about 30%

OpenIOC

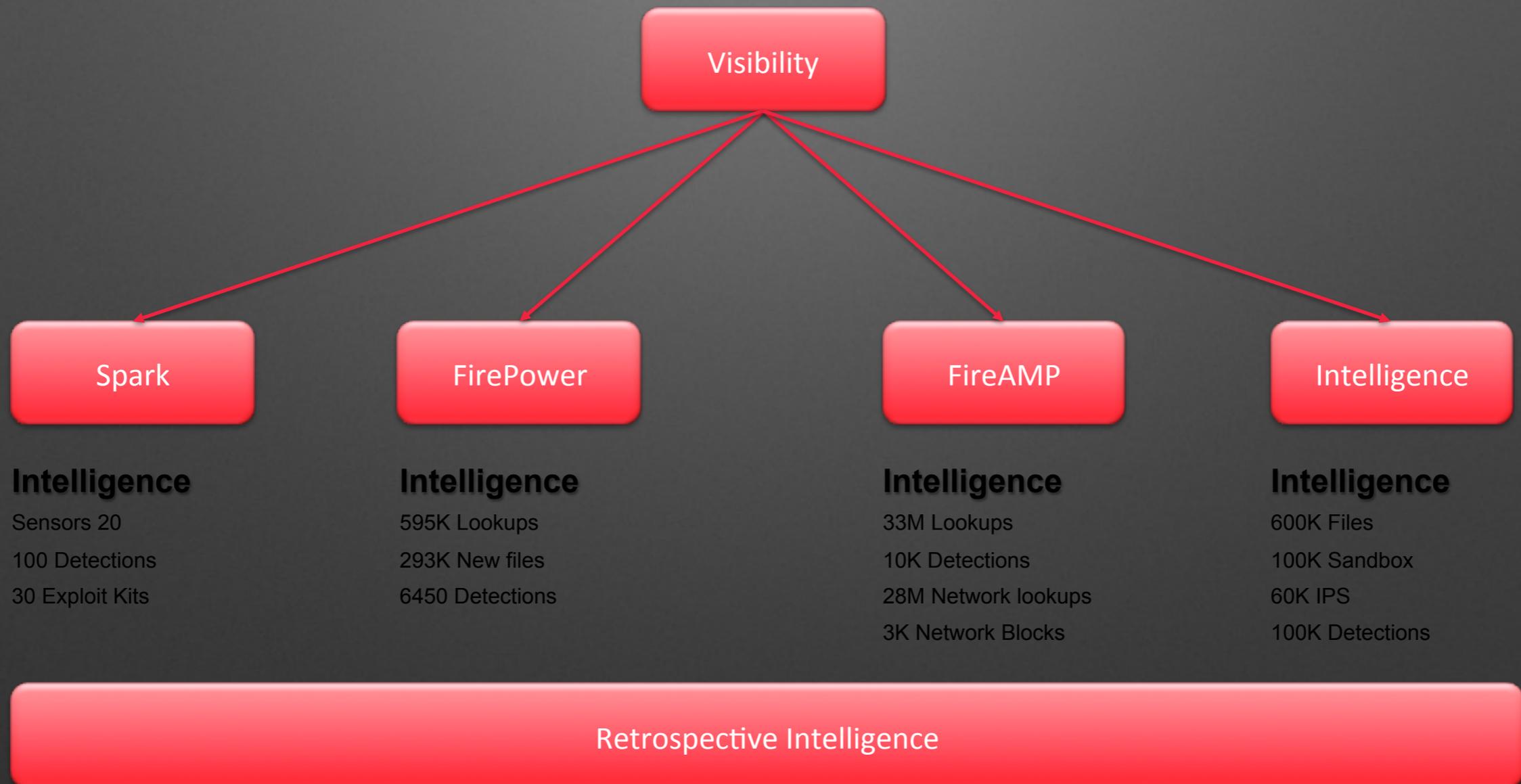
- Supporting the OpenIOC format for detection

Yara

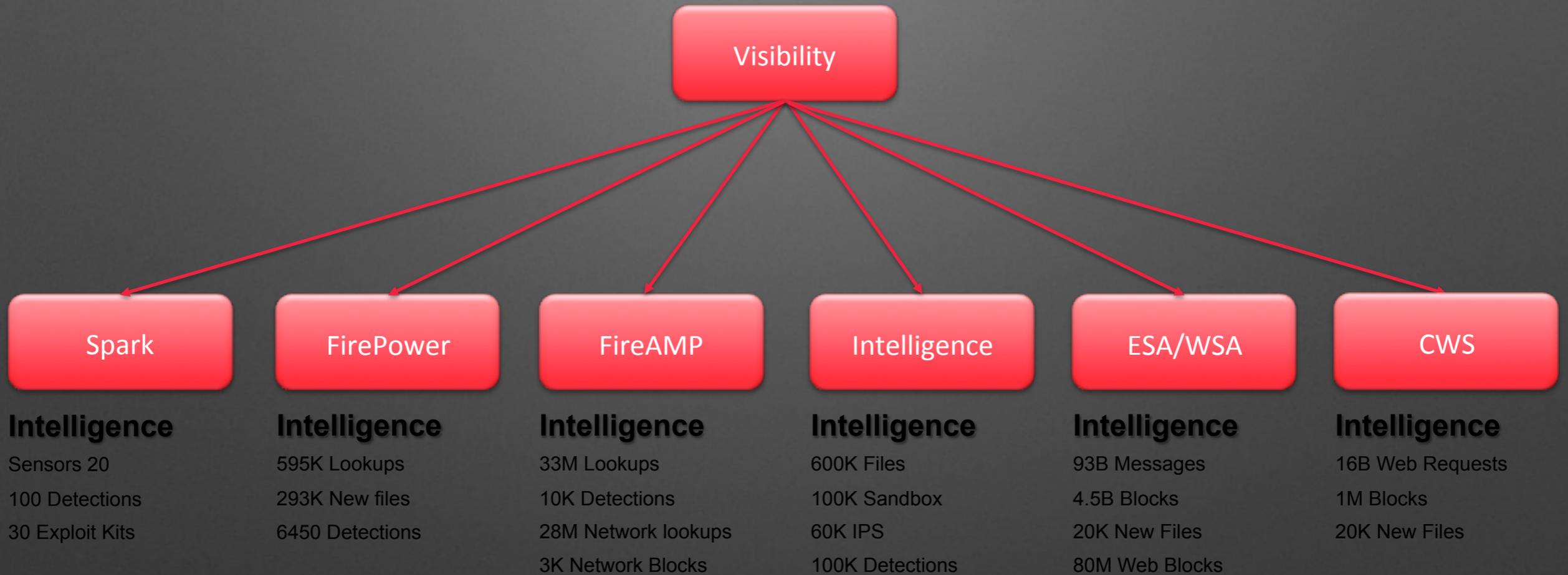
- Supporting the Yara format for the detection of malware.

Detection Roadmap Update

Detection Roadmap

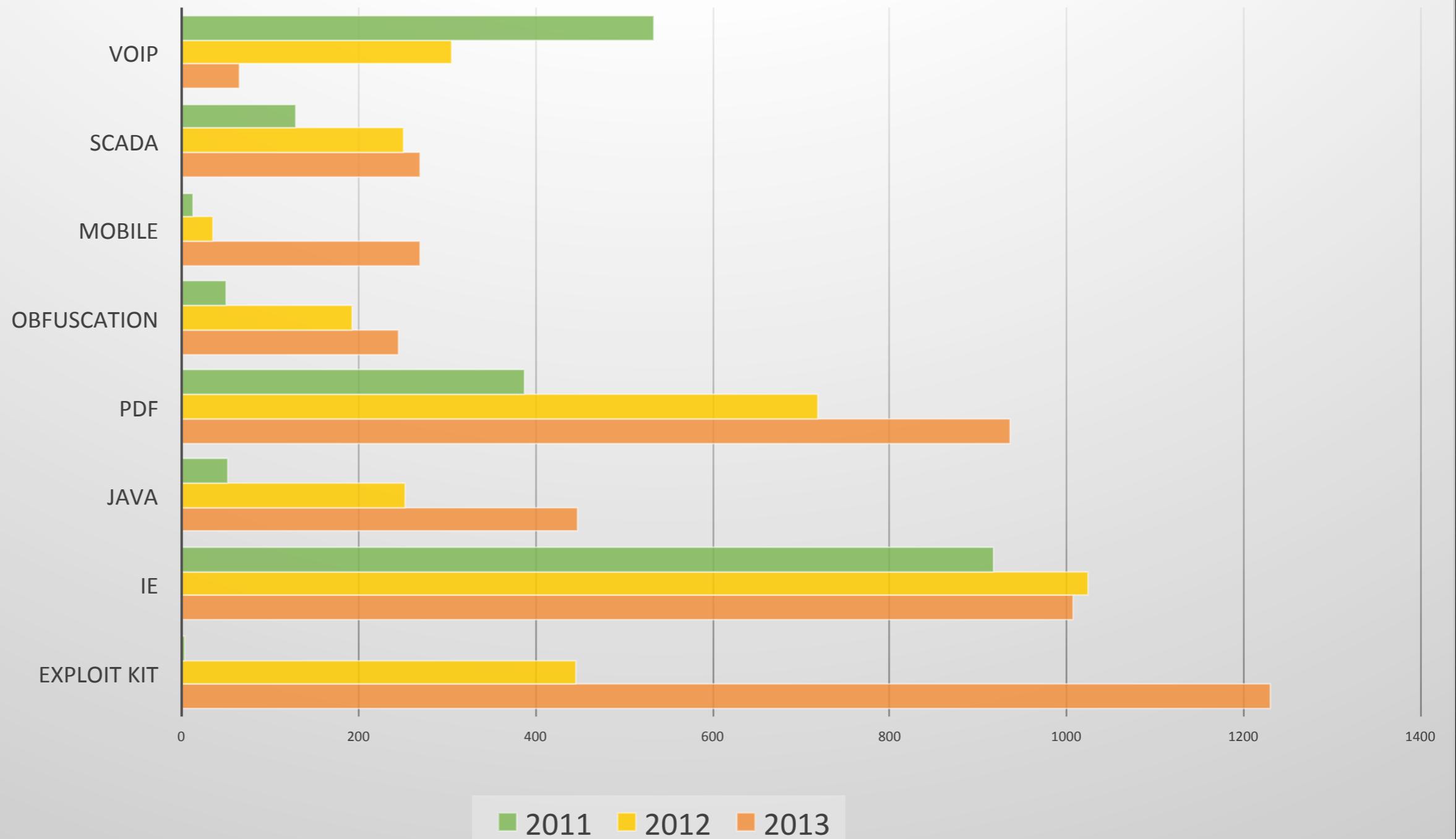


Detection Roadmap Now



Retrospective Intelligence

Detection Trends

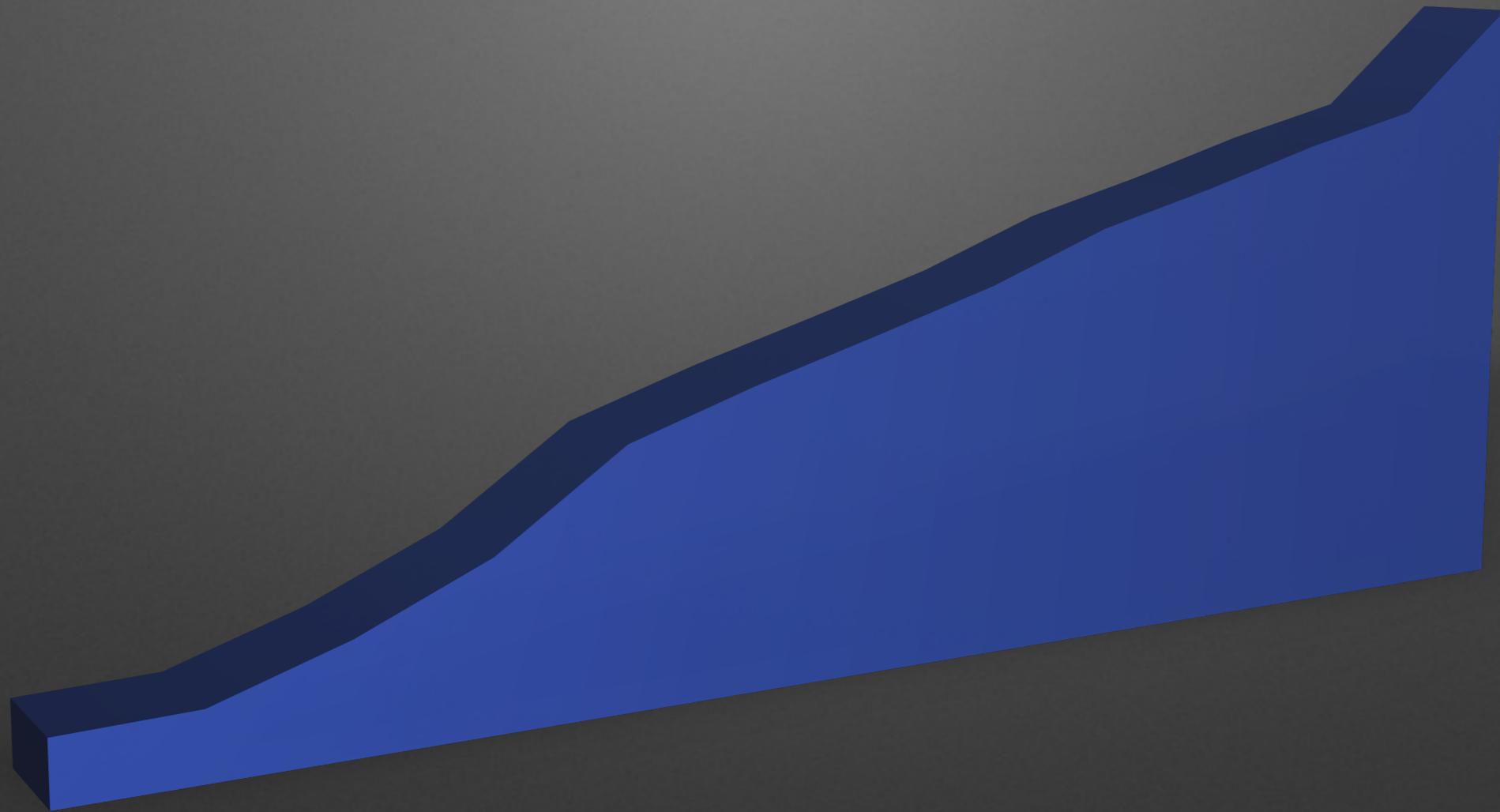


Community Announcements

Community Announcements

- Community Signatures
 - Snort
 - ClamAV

Snort Community Signatures



2,908 Community Rules

ClamAV Community Signatures

- Accepting Community Signatures from the ClamAV Community
- Community-sigs mailing list at [ClamAV.net](mailto:community-sigs@ClamAV.net)

Question and Answer Time