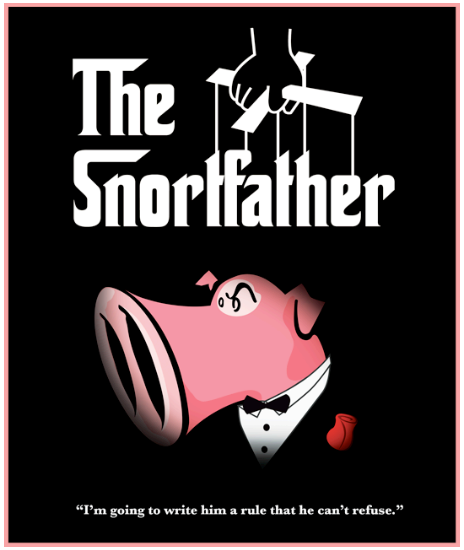
The Power of SNORT

SNORT Update

Jean-Paul Kerouanton
11th May 2010

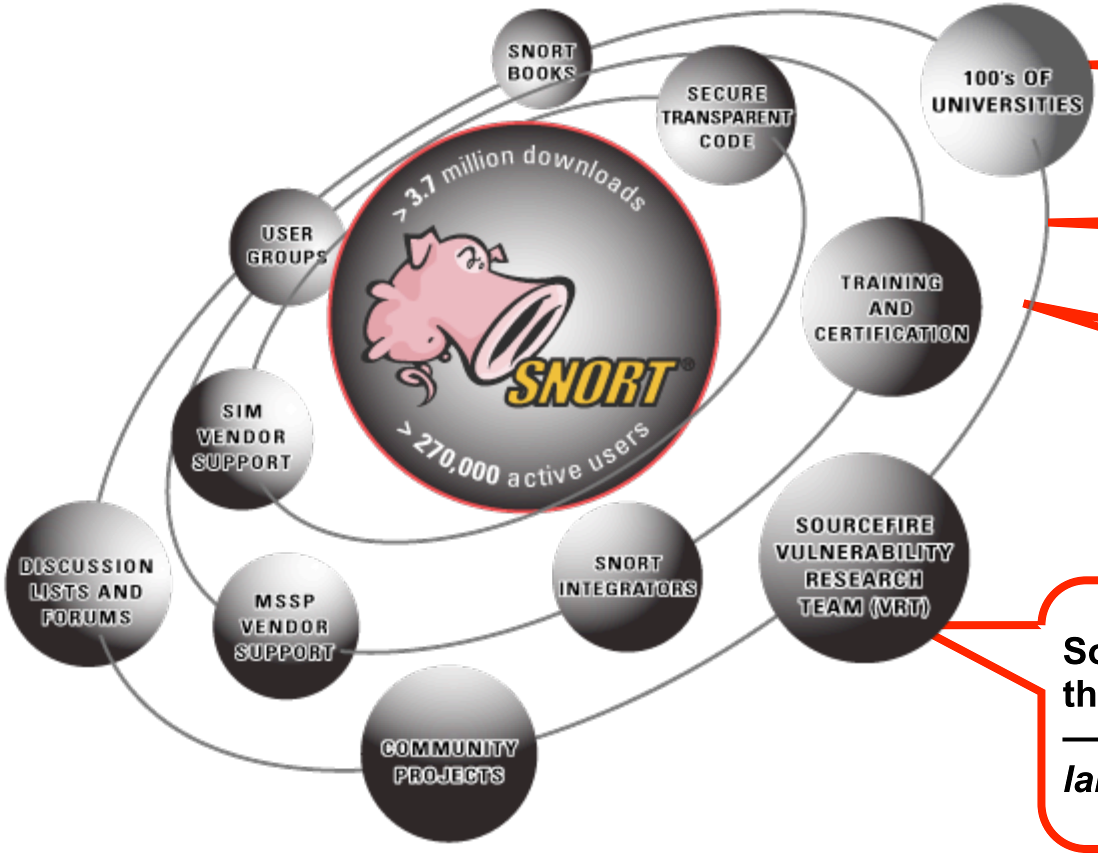
Leveraging the Snort Brand



SOURCEfire
©2008 Sourcefire, Inc. Imagery property of Sourcefire. All rights reserved.

The Power SNORT = The Power of Open Source

The SNORT- Universe

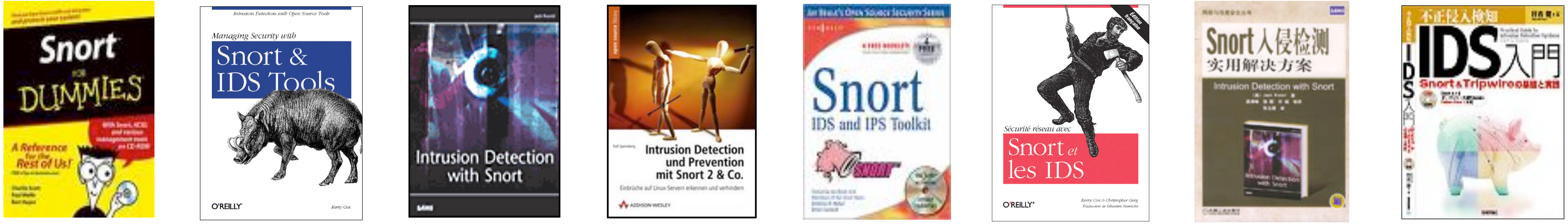


AMAZON - +100 items

GOOGLE – +3.700.000 hits

Global base of skilled security professionals – well trained

Sourcefire VRT is augmented by the resources of the community — *giving customers the world's largest threat response team.*



Snort FOR DUMMIES
Managing Security with Snort & IDS Tools
O'REILLY
Intrusion Detection with Snort
Intrusion Detection und Prevention mit Snort 2 & Co.
Snort IDS and IPS Toolkit
Sécurité réseau avec Snort et les IDS
Snort入侵检测 实用解决方案
Intrusion Detection with Snort
IDS入門

Snort and more …. Open Source

- SNORT
- CLAMAV
- OfficeCat
- Deamonlogger

A very nice pig …..

Best of Both Worlds

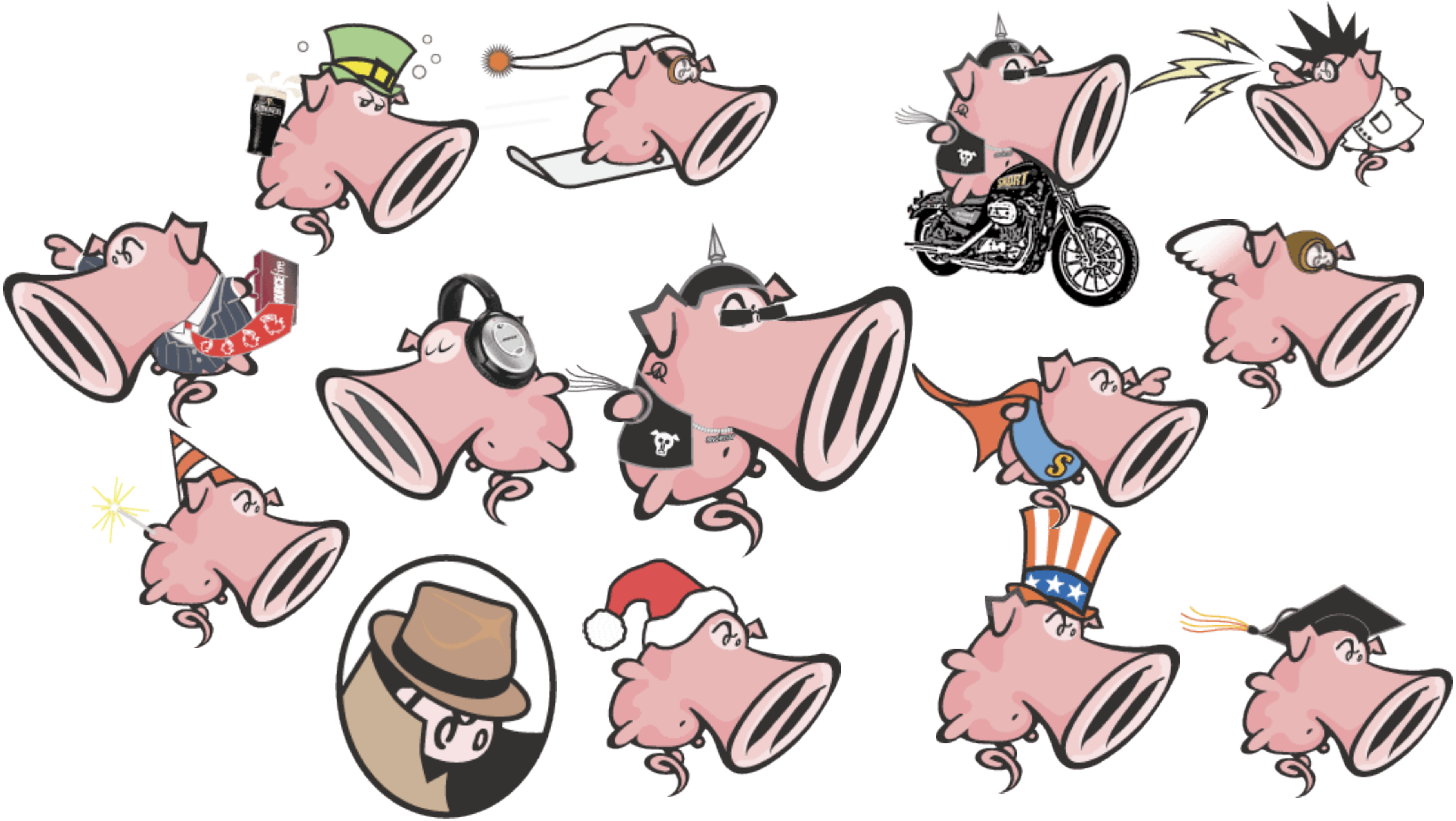
Open Source Community

+

Sourcefire Development

In different suites ….

In different suites ….



How it all started ….

How it all started ….

How it all started ….

- Marty invented SNORT….Back in Dec 1998
- Originally as a kind of better “Sniffer”
- Got quick huge recognition as IDS
- Participated successful in tests/challenges with commercial products
- Customer demand for commercial solution increased
- Sourcefire was founded 2001
- Martin Roesch – ranks amongst top 100 IT influencers

SNORT.ORG

- Free access to SNORT Engine and Rules
- +3.000.000 downloads
- +300.000 REGISTERED user
- Subscribe or not to subscribe, that is the questions …..
- Subscription is –virtually- cheap
  (personal: 29,99 USD/year; internal use, +6 sensors: 399,99 USD per year)
- Regular updates, much faster
- With no subscriptions – updates delayed (30 days)
- Able to contribute
- Rich information exchange
- Maintained by a special group @Sourcefire (around VRT)

SNORT and Sourcefire

SNORT and Sourcefire

- Snort and Sourcefire: 2010 in its 10th “wedding anniversary”
- BTW: 29% of spouses in US getting divorced prior 7 years being married …… ;-)
- SnortSP (Snort Security Platform) will help Snort to maintain its dominance for the next 10 years!
- Sourcefire owns 100% of the SnortSP code
- Provides a common infrastructure for processing and decoding traffic among multiple 3D applications (“engines”)
- Significant benefits for 3D customers, open source users
- SnortSP was the first major milestone toward Snort 3.0 and our 3D System architecture

SNORT rules are open …. Does this hurt ?

SNORT rules are open …. Does this hurt ?

- No security by obscurity
- Everybody can write its own
- Users will see what he gets
- Business proven
- Robust
- Security is proven by millions of people

SNORT and VRT – the lead in Cybersecurity

- Deep Snort knowledge
- Responsibilities include:
  - Publishing new Snort rules, SEU's & VDB's
  - Publishing new ClamAV signatures
  - Development of the ClamAV Engine
  - Threat Research
- 100 Percent MS Coverage
- Coverage for All Adobe 0-Days
- Covered 10 Critical Rated Adobe Bugs
  - No one else has coverage for these.
- ICSA Certified
- Best Overall Detection at NSS
- 900 Vulnerabilities covered with 890 rules in 2009

"My concern right now isn't what I'm being attacked with, its finding what I need to defend"

Sourcefire customer

But what are we protecting?

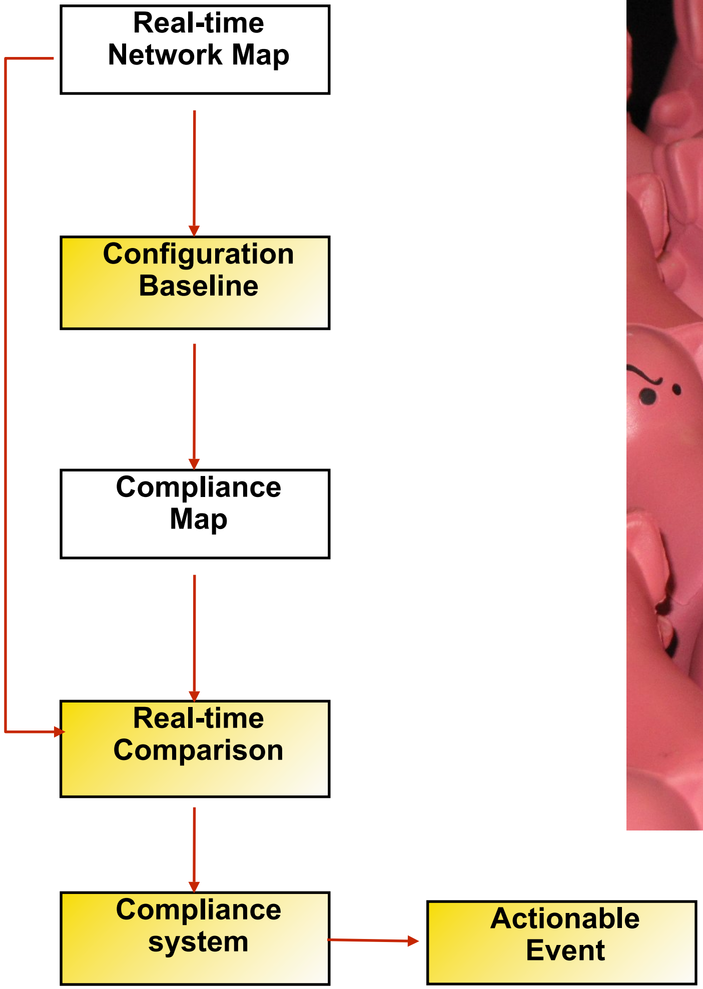
"My concern right now isn't what I'm being attacked with, its finding what I need to defend"

Sourcefire customer

Passive Discovery

- Network fingerprinting
- Real-time, not periodic
- Zero impact
- Impossible to evade

Enforcing network configurations



What’s New in Snort 2.8.5

Multiple Configurations

- Allows for multiple snort.confs to be used by one Snort Process
- Configuration selected by VLAN or IP Address
  - Prioritized by VLAN, Destination IP, Source IP
- Allows single Snort instance to monitor different networks with rules specific to each network

Multiple Configurations (cont.)

- Configuration Binding
  - Main snort.conf is default configuration
  - Specific path to network specific snort.conf and VLAN or subnet via “config binding” option in main snort.conf
- Can use different rule variables across configurations
  - Rule option (content, byte_test, pcre, etc) must be the same for each rule sid
  - Rule src/dst IP address & port can differ
  - Rule action (alert, drop, etc) can differ

Multiple Configurations (cont.)

- Can use different filter settings across configurations
  - Suppression, Event Filters, Rate Filters
- Can use different preprocessor settings across configurations
  - Preprocessor configurations can differ
  - Memory settings (memcaps, tcp limits, etc) used from the default configuration
- Output plugins (unified2, etc) are global and specified in default configuration

Rate Based Attack Prevention

- New/Updated Filters
  - Rate Filters
    - Limit connections & connection attempts per host
    - Change rule action when a rate is reached
    - Example: SYN Floods
  - Detection Filters
    - Use to detect attacks where a limit/rate is required
    - Drop rule will not drop traffic until rate is met
    - Example: DNS Spoofing attacks
  - Output/Event Filters
    - Limit the number of alerts Snort generates

Rate Based Attack Prevention (cont.)

Rate Filters

- New keyword “rate_filter”
- Change rule action when a rate is reached
  - Pass to Alert
  - Alert to Drop
- Based on rule’s GID & SID, use special ones for
  - 135:1 – Connection Attempts (SYN Attacks)
  - 135:2 – Simultaneous open connections
- Can specify multiple rate_filters per GID & SID pair
  - Use track by_src or by_dst options to control specific sides of the connection
  - Use apply_to to control specific hosts/networks

Rate Based Attack Prevention (cont.)

Detection Filters

- New rule option “detection_filter”
  - Replaces in-rule thresholds and restricts the number of times a rule actually alerts
  - Considered part of the rule, just the same as content, byte_test, etc.
- Used to detect attacks where a rule must match multiple times in a time period before alerting

Rate Based Attack Prevention (cont.)

Output Filters

- New keyword “event_filter”
  - Equivalent to the old “threshold” keyword
  - Same syntax
  - Changed to eliminate confusion between the filter and its type (threshold, limit, both)
    - Example: event_filter type threshold
  - “threshold” keyword still supported for backwards compatibility, will be removed in a future release
- Reduces the number of alerts Snort generates

No changes to “suppression” keyword

SSH Preprocessor

- No Longer experimental
- What does this preprocessor do?
  - Decode SSH connections
  - Identifies certin classes of attacks on SSH servers
    - SecureCRT SSH Client Buffer Overflow attack
    - Catalyst Exploit
    - Challenge Response Overflow
    - SSHv1 CRC32
  - Identifies encrypted sessions for Snort to ignore
    - Makes snort more efficient

Configuration Update/SigHUP

- Allows for full update to configuration without termination of Snort
- Continued inspection while new configuration is being loaded
- Improved startup/shutdown speed to allow continued flow of network traffic when Snort is deployed inline

Performance Improvements

- Leverages knowledge gained from SnortSP
  - Recognized internal packet structure
    - Makes packet decoding faster
    - Results in improved throughput, reduced CPU usage
  - Faster loading and use of shared libraries
    - Side-effect, cannot use Snort 2.8.5 with 2.8.4 shared rules or preprocessors (.so/DLL)
- Improvements of performance of some .so rules

What's New in Snort 2.8.6

Generally

- Improvements to Pattern Matching efficiency
- Improved HTTP response processing
- Improved detection of file-based attacks against client applications
  - Web Browser
  - MS Office
  - Others
- Better ways to detect credit card numbers, social security numbers, and other personal information

Improved Fast Pattern Matcher

- Improved memory usage of Snort Engine.
- Fast pattern matcher automatically measures memory and more efficiently identifies rules likely to match packets.
- Increase around 10 % the performance.
-

Http Detection Enhancements

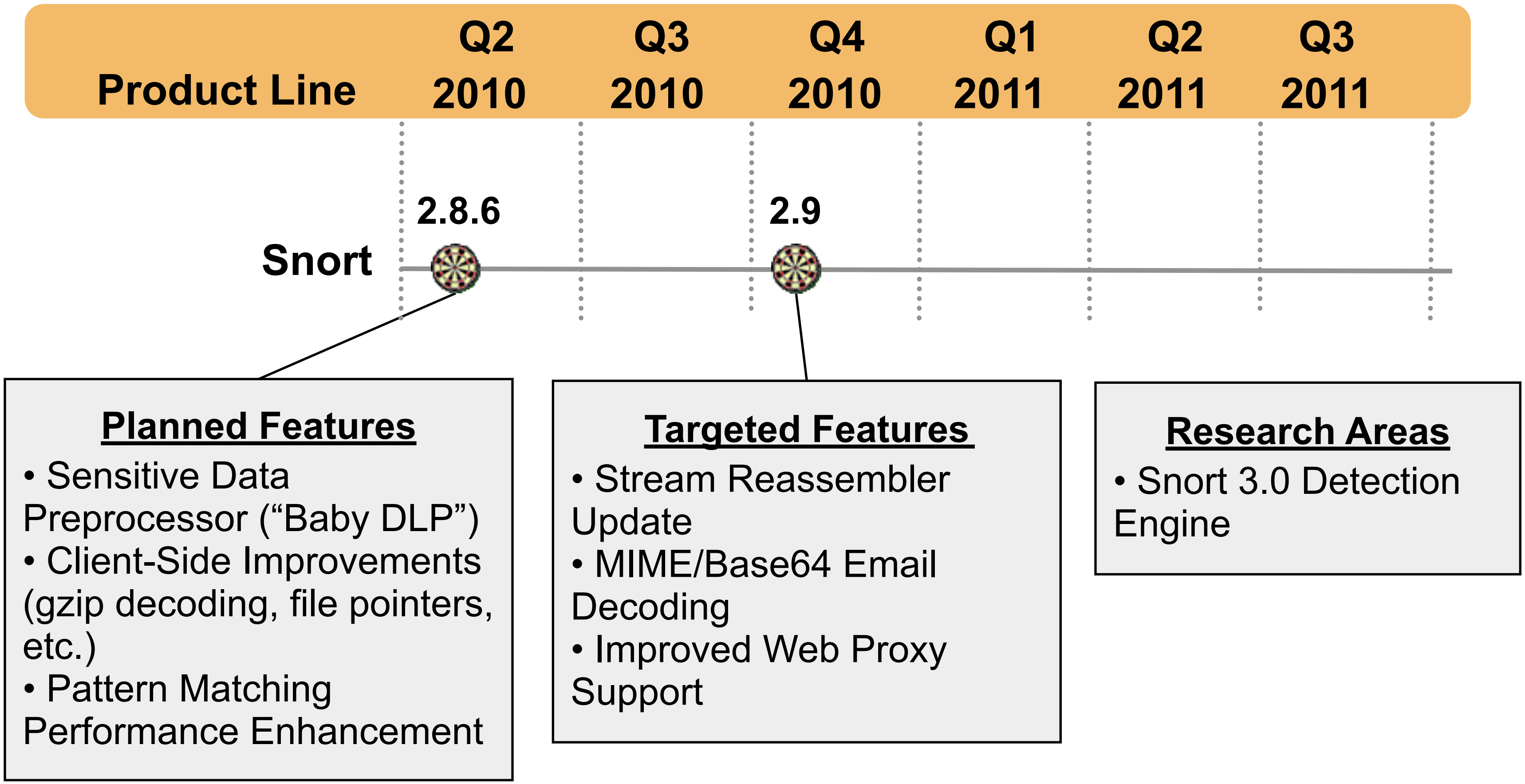
- Analyze more in depth http traffic
  - New Options for http pre-processor
    - Compressed gzip inspection
    - Cookies
  - New Keywords :
    - http_encode and file_data
  - New arguments for Content and pcre keywords

Sensitive Data Detection

- Detect and alert on sensitive data leaks
- Can detect data as Social Security numbers, Credit Card...
- Detection in ASCII text
- Known as “Baby-DLP”

Next ?

Snort Roadmap



Product Line	Q2 2010	Q3 2010	Q4 2010	Q1 2011	Q2 2011	Q3 2011
Snort	2.8.6		2.9			

Planned Features

- Sensitive Data Preprocessor (“Baby DLP”)
- Client-Side Improvements (gzip decoding, file pointers, etc.)
- Pattern Matching Performance Enhancement

Targeted Features

- Stream Reassembler Update
- MIME/Base64 Email Decoding
- Improved Web Proxy Support

Research Areas

- Snort 3.0 Detection Engine

S