Feature Wish List
Aka: My Vision

Michael Starks, CISSP, CISA
OSSEC Symposium Summer 2012
July 13, 2012
Working towards a shared vision
Project Rainbow

A lesson in working towards a shared vision.
“Build me a rainbow, daddy. You can build anything!”
I Got This

1. 4x8 sheet of plywood
2. Draw rainbow pattern
3. Cut out with skill saw
4. Paint white and add rainbow lines
5. Assist daughter with painting rainbow
6. Hang onto bedroom wall
“It should be bigger than my room and have all of the rainbow colors*!”

*Except for blue, because that's a boyish color.
“Oh, and I want to ride it like a bike!”
Lack of a shared vision and realistic goals put this project on hold.
Interoperability Based on Standards

Some standards succeed while others fail. We don't need to change OSSEC. We can enhance OSSEC.
SSH Rule

<rulenumber id="5719" level="10" frequency="6" timeframe="120" ignore="60">
  <if_matched_sid>5718</if_matched_sid>
  <description>Multiple access attempts using a denied user.</description>
  <group>invalid_login</group>
</rule>

What's the Standard?

VSFTPD Rule

<rulenumber id="11452" level="10" frequency="10" timeframe="60">
  <if_matched_sid>11401</if_matched_sid>
  <same_source_ip />
  <description>Multiple FTP connection attempts from same source IP.</description>
  <group>recon</group>
</rule>
Working from common schemas and taxonomies increases understanding
Let's Be Friends :)

CVE

OVAL

OSSEC

syslog-ng
A collective attitude which encourages and supports contributions
The Wrong Way

“My mother could write better decoders!”
The Right Way

“Nice job on the decoder. I'd like to make a few changes and include it in the next release. Is that OK?”
The Right Way

Writing code is not necessary. Everyone has something to offer.

Can you submit a bug report?

Are you an artist?

Do you have an idea?
With a friendly and encouraging community, talent naturally emerges.
Laying the Foundation
Dealing with bugs

Prioritizing

Fixing

Accepting patches

Communicating
Reducing the noise level

Email alerts should be

- Meaningful and actionable
- Consistent
- Informative

The rest can be viewed in a GUI
Making Agent Deployment Easier

Agent key management is a barrier to entry

MSI for Group Policy

RPMs, Debs, etc

It should “just work”
Decoupling Rule and Decoder Updates

Faster response to current and emerging threats

Faster rule fixes
Taking OSSEC to the Next Level
The future of OSSEC is about sharing.

Sharing attack data

Sharing rules and decoders

Sharing creativity, features and bug fixes
Today

Attack data not widely shared

Everyone tunes their own rules

We share our failures, but not many successes
What Can Be

A collective infrastructure, automatically sharing data

*Suspects are innocent until proven guilty in a court of law (but it was the green hat that gave him away.).
An opt-in rule mechanism for sending tuned rules, resulting in better rules in future releases.
1. New file added
2. Is it a known good file?
3. Is it a known bad file?

1. URL accessed
2. Is the site malicious?
Guiding Principles

Make it easy
Make it automatic
Make it cool
Many Thanks for the Use of the Following Images

- Level: http://www.sxc.hu/photo/278476
- Stonehenge: http://www.sxc.hu/photo/806189
- Rainbow girl: Personal copyright
- Plywood: http://www.sxc.hu/photo/1155687
- Rainbow stars: http://www.sxc.hu/photo/1014098
- Pointed finger: http://www.sxc.hu/photo/642260
- Happy face: http://www.sxc.hu/photo/1108723
- Group: http://www.sxc.hu/photo/1254522
- Rainbow chairs: http://www.sxc.hu/photo/1379341
Many Thanks for the Use of the Following Images

- Island: http://www.sxc.hu/photo/1210282
- Orange juice: http://www.sxc.hu/photo/1032249
- Lady bug: http://www.sxc.hu/photo/1321755
- Ear protectors: http://www.sxc.hu/photo/1005134
- Padlock: http://www.sxc.hu/photo/1331533
- Butterfly: http://www.sxc.hu/photo/1081069
- Chain: http://www.sxc.hu/photo/1018190
- Book: http://www.sxc.hu/photo/810896
- CEE: http://cee.mitre.org/
This presentation is licensed under the Creative Commons Attribution-Noncommercial-Share Alike 3.0 license. The license does not extend to images, which hold their own copyrights attributed to various authors.

You are free:

to Share — to copy, distribute and transmit the work

to Remix — to adapt the work

Under the following conditions:

Attribution — You must attribute the work in the manner specified by the author or licensor (but not in any way that suggests that they endorse you or your use of the work).

Noncommercial — You may not use this work for commercial purposes.

Share Alike — If you alter, transform, or build upon this work, you may distribute the resulting work only under the same or similar license to this one.

With the understanding that:

Waiver — Any of the above conditions can be waived if you get permission from the copyright holder.

Other Rights — In no way are any of the following rights affected by the license:

Your fair dealing or fair use rights;

Apart from the remix rights granted under this license, the author's moral rights;

Rights other persons may have either in the work itself or in how the work is used, such as publicity or privacy rights.

Notice — For any reuse or distribution, you must make clear to others the license terms of this work.