Summer 2012

OSSEC Symposium

Presented by the members of the OSSEC Team

Vic Hargrave, JB Cheng, Michael Starks

July 12 – 13, 2012

OSSEC Symposium Agenda – Day 1

11:00 am ~ 1:00 pm	*Registration and Lunch*
1:00 pm ~ 1:15 pm *	**Trend Micro – Welcome to the OSSEC Community** Joe Lin, Daniel Cid
1:15 pm ~ 2:00 pm *	**OSSEC Vision, Strategy & Community** Vic Hargrave & JB Cheng, OSSEC Dev Team
2:00 pm ~ 3:00 pm	**Attendee Introductions and General Questions** All Participants **License Considerations with OSSEC Contributions** John Chen, Trend Micro Legal Counsel
3:00 pm ~ 3:15 pm	*Break (choose Friday lunch)*
3:15 pm ~ 4:00 pm *	**Keynote I – Experiences Applying OSSEC** Michael Starks, OSSEC Dev Team
4:00 pm ~ 4:45 pm	**Open Discussion – Pain Points Using OSSEC** All Participants

Welcome to the OSSEC Community

Joe Lin

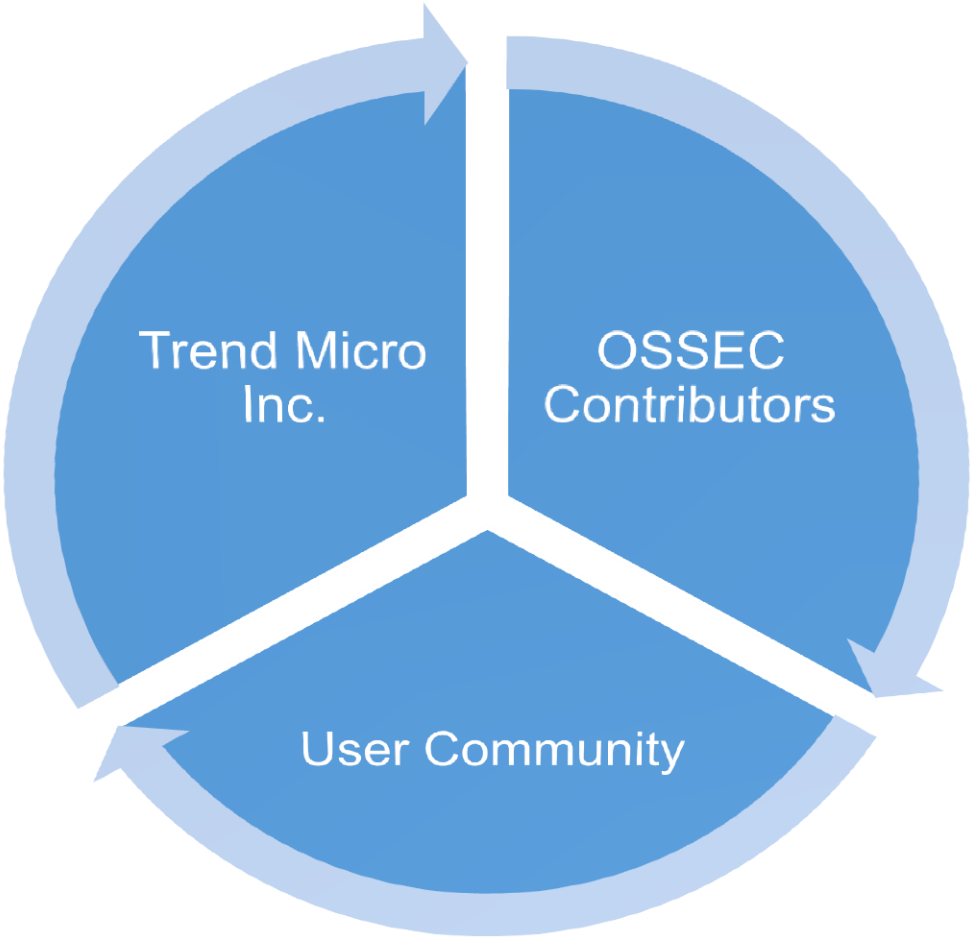
Welcome

- 2002-2007: Founder (Daniel)
- 2008: Third Brigade (Bill)
- 2009: Trend Micro (Joe)
- 2012: Community (You and me)

Vision, Strategy & Community

Vic Hargrave
JB Cheng
OSSEC Dev Team

OSSEC Vision 2012 – Three in One



OSSEC Strategy

- Trend Micro Inc.
  - Promote Trend Micro brand through OSSEC Project sponsorship
  - Engage in Open Source development and learn from the community
  - Ensure timely technical support for Trend Micro's paid support customers

OSSEC Community

- Contributors/Users Community Goals
  1. Provide the OSSEC user community with regular bug fixes and new features.
  2. Provide timely announcements of OSSEC rule and platform enhancements thru new OSSEC website and social media
  3. Promote OSSEC and Trend Micro brand and development through regular community meetings
  4. Increase adoption of the OSSEC HIDS platform.

OSSEC Expectations - 1

- High level demo of current features
- To have a better understanding of OSSEC and its offerings.
- Learn and understand how to set up, manage, deploy, monitor, maintain OSSEC in an enterprise env with 3000+ servers
- To learn, educate and befriend other OSSEC users.
- To spark innovation and excitement within the OSSEC community.
- To share attack data, success stories, and pain points.

OSSEC Expectations - 2

- It is a great tool - and wondering about the future direction.
- More information on new or upcoming features
- I would like to understand the future of OSSEC including expected enhancements.
- Want to know the future of the product what to expect and also networking with fellow OSSEC users.
- Find out what the future holds for OSSEC, comment some things, request some changes
- To have fun!

Years of OSSEC experience

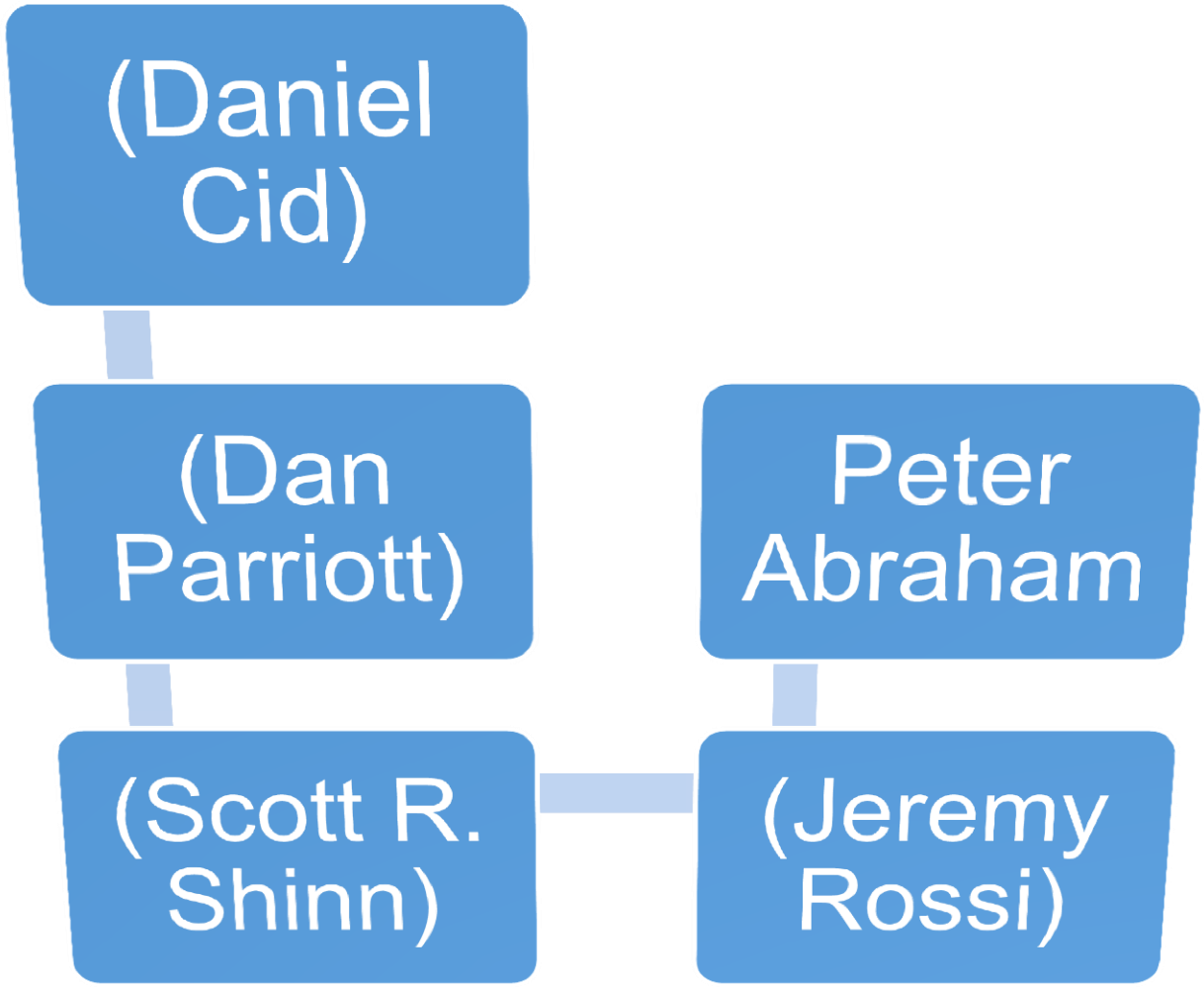
- 7
- 6
- 2
- 6
- 1
- 3
- 1
- 0
- 1

Attendees Introduction

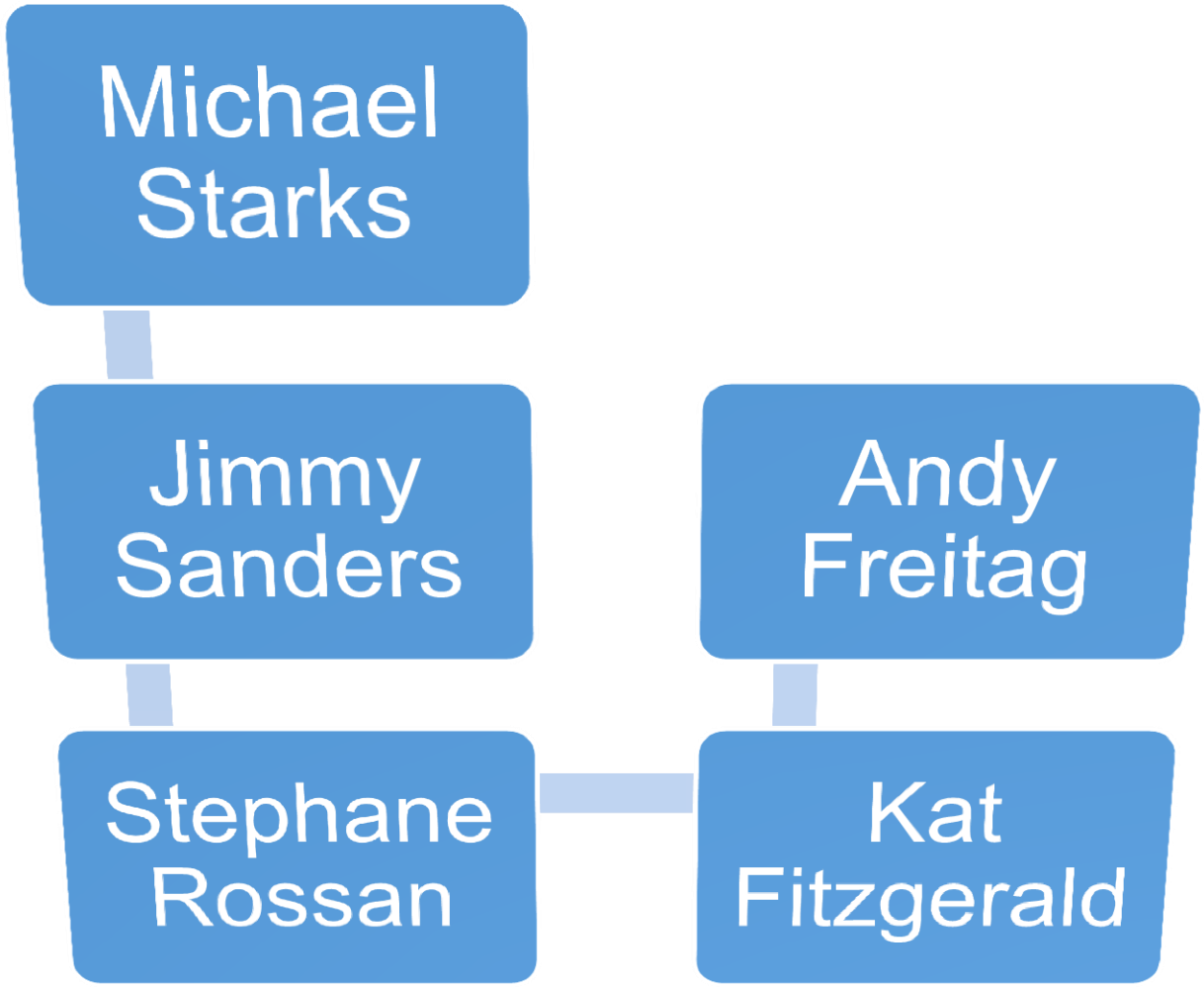
General Questions

All Participants

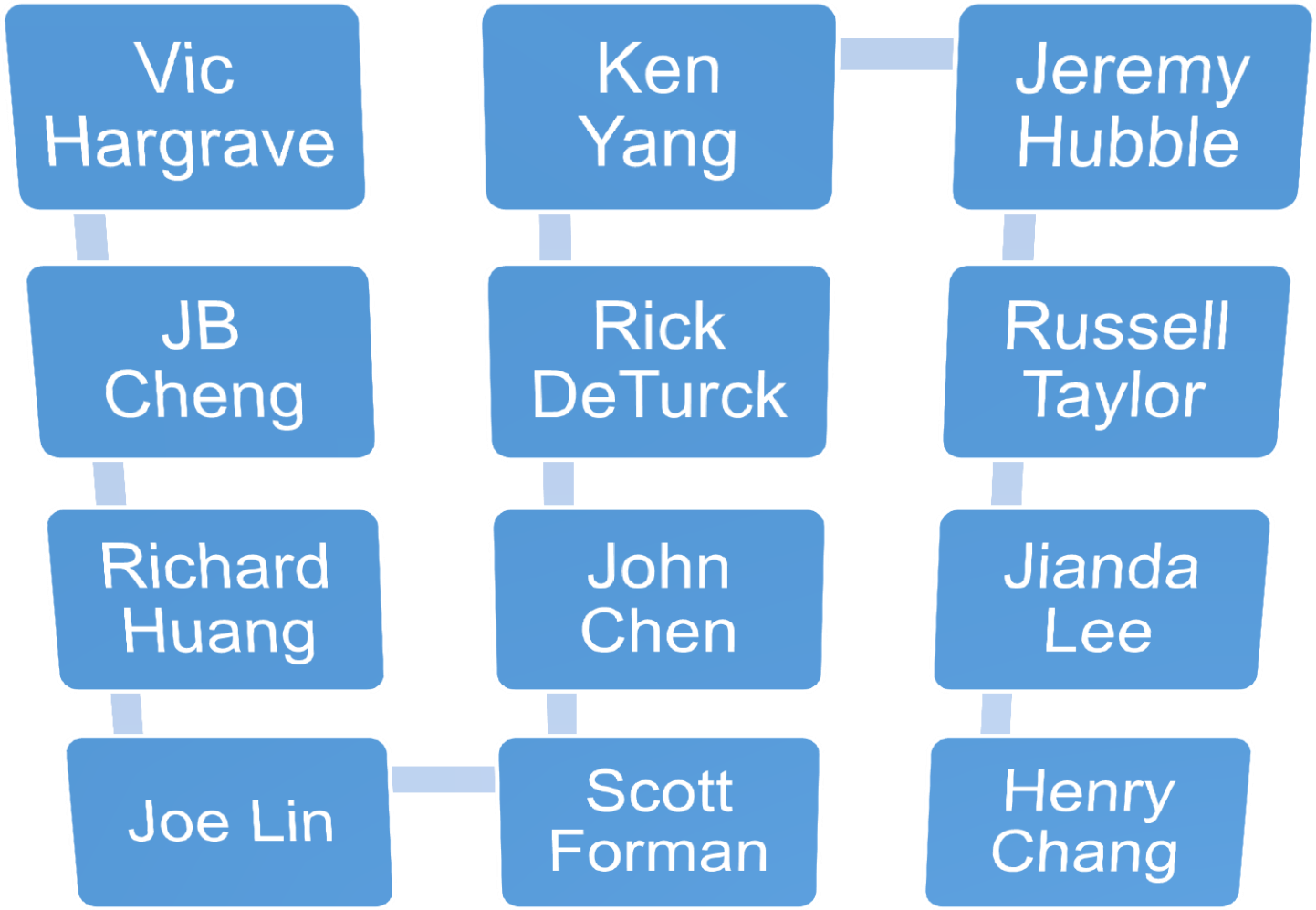
OSSEC Remote



Attendees -1


Michael Starks
Jimmy Sanders
Andy Freitag
Stephane Rossan
Kat Fitzgerald

OSSEC Attendees -2



License Considerations

OSSEC Contributions

John Chen
Trend Micro Legal Counsel

Break

15 minutes

Keynote I

Experience Applying OSSEC

Michael Starks, OmniAmerican Bank
OSSEC Dev Team

Open Discussion

Pain Points

All Participants

END of Day 1

OSSEC Symposium Agenda – Day 2

9:00 am ~ 9:45am 9:45 am ~ 10:00 am	*Continental Breakfast* **Trend Micro product strategy and OSSEC** Bill McGee
10:00 am ~ 10:45 am	**Customer Insight – Experiences with High Volume OSSEC Deployment** Kat Fitzgerald, JB Cheng (Facilitator)
10:45 pm ~ 11:00 am	*Break*
11:00 am ~ 11:45 am	**3rd Party Add-on Tools – ELSA, Splunk, ArcSight, OSSIM, LogLogic…** Michael Starks (Round Table Facilitator)
11:45 am to 1:00 pm	*Lunch (*Open Discussion on other 3rd Party Add-on Tools)
1:00 pm ~ 1:45 pm *	**Keynote II – OSSEC Feature Wish List** Michael Starks, OSSEC Dev Team
1:45 pm ~ 2:45 pm	**Open Discussion – What's should be in next release of Rules, Core Engine, Web UI & Documentation?** All Participants
2:45 pm ~ 3:00 pm	*Break*
3:00 pm ~ 3:30 pm	**Small Groups and Logistics** (JB Cheng, Facilitator)
3:30 pm ~ 4:45 pm	**Open Discussion – Release Scheduling of Rules, Core Engine, Web UI & Documentation**

Breakfast

Trend Micro Product Strategy and OSSEC

Bill McGee

Customer Insight Volume Deployment

Kat Fitzgerald
JB Cheng (Facilitator)

Break

15 minutes

3rd Party Add-on Tools

ELSA, Splunk, ArcSight, OSSIM, LogLogic

Michael Starks (facilitator)

Lunch Break

Open Discussion

75 minutes

Keynote II

OSSEC Feature Wish List

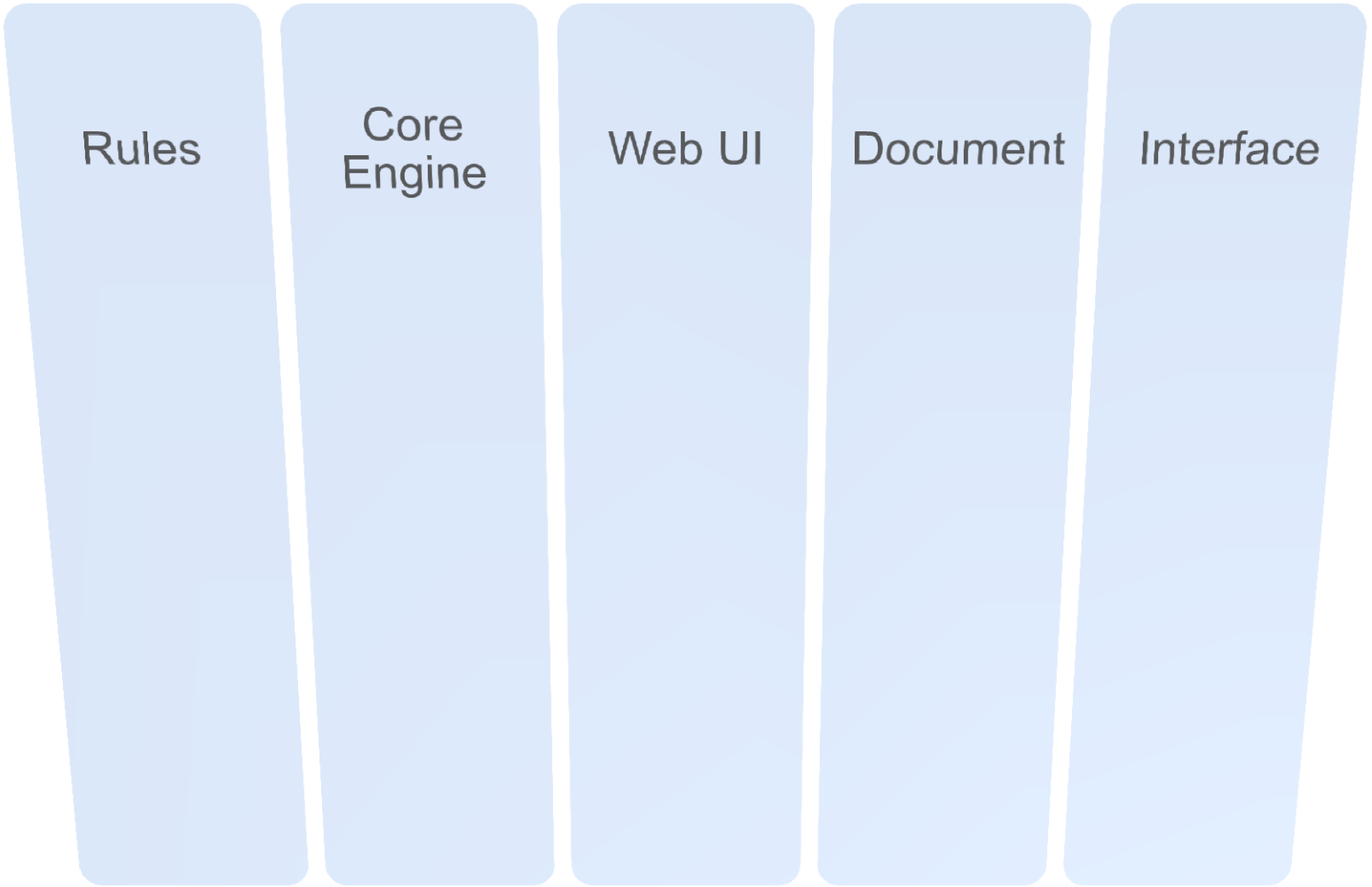
Michael Starks, OmniAmerican Bank
OSSEC Dev Team

Open Discussion

What's in the Next Release?

All Participants

OSSEC Next Release



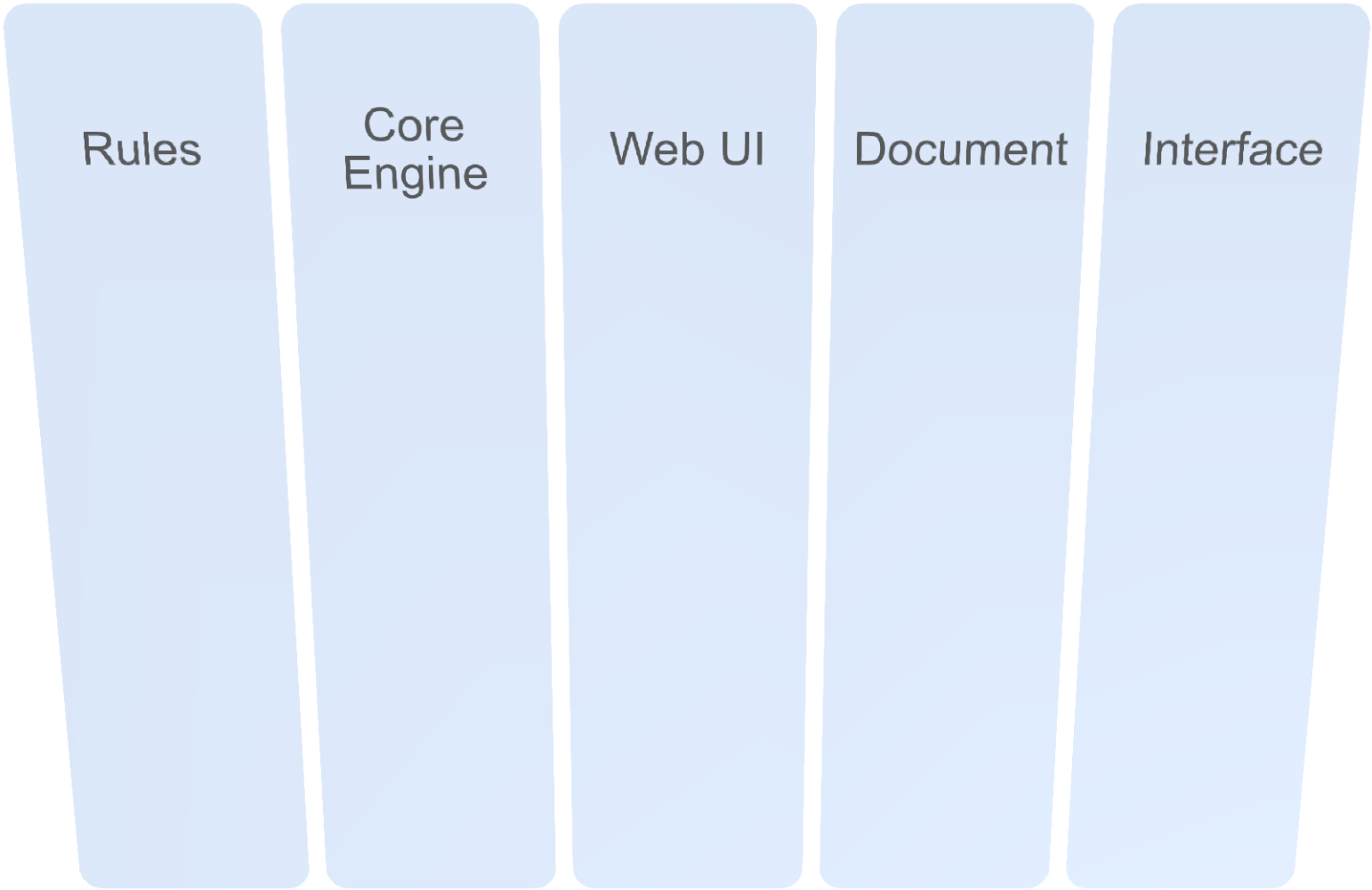
Break

15 minutes

Small Groups & Logistics

JB Cheng (facilitator)

Small Groups & Logistics



Open Discussion

Release Schedule

All Participants

OSSEC Symposium

TREND MICRO

Wrap Up