Industry Experience Using STIX, TAXII, and CybOX to Accelerate Threat Response

Thursday, 8 September

Session Presenters

Joep Gommers,
EclecticIQ

Mike Small
KuppingerCole

Frank Lange,
Anomali

Daniel Riedel,
New Context,
Inc.

Jason Keirstead,
IBM Security
Intelligence

Alex Valdivia,
ThreatConnect,
Inc.

INTRODUCTION
MIKE SMALL

Need for Cyber Threat Intelligence

Cyber-Crime already has no borders

Cyber Criminal Eco-System

Cyber-Crime Techniques Evolution

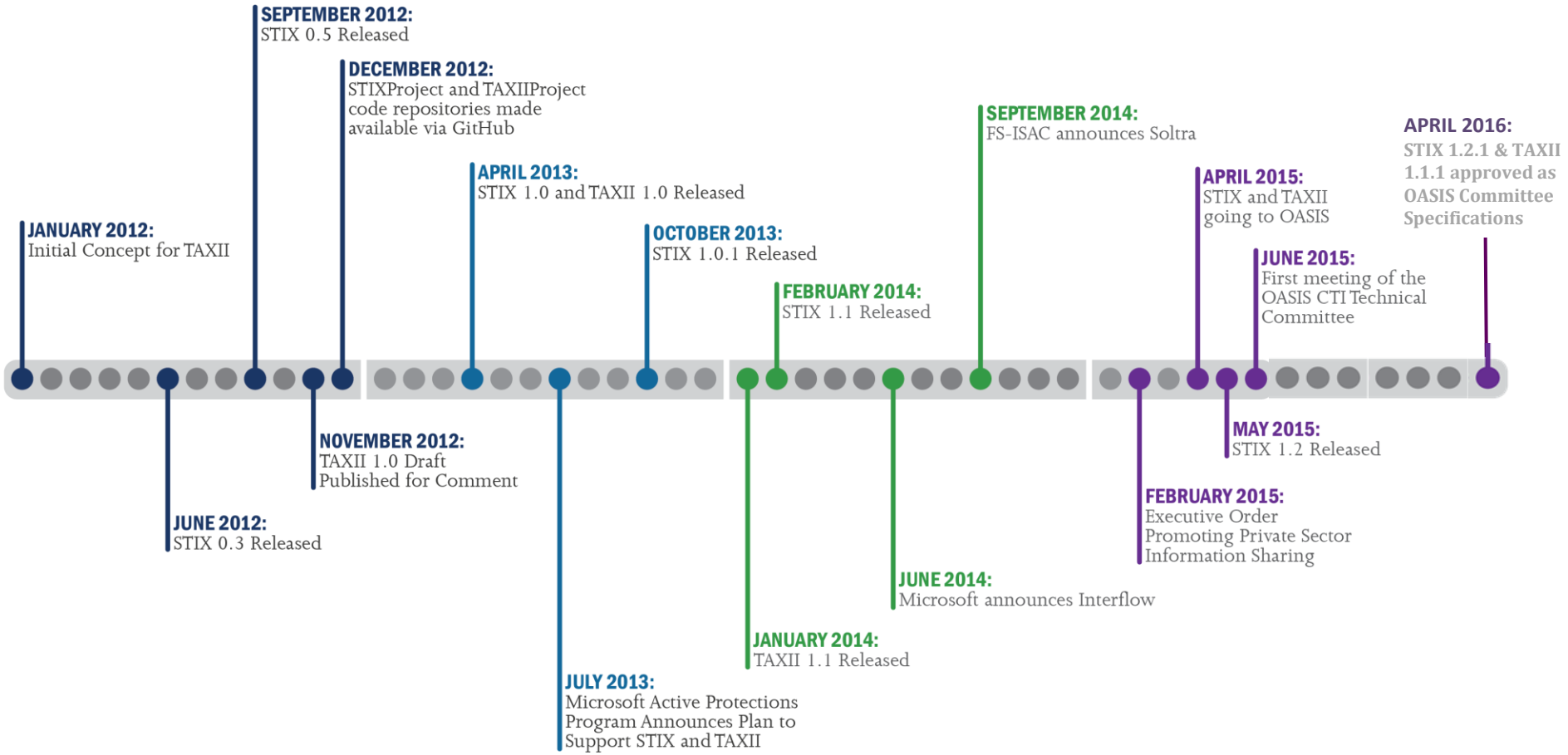
Good Guys MUST Cooperate

Cyber Threat Intelligence Objective…

To define a set of information representations & protocols to support automated information sharing for cybersecurity situational awareness, real-time network defense, and sophisticated threat analysis.

Cyber Threat Intelligence Standards

Cyber Threat Intelligence Timeline



Panel Discussion

Joep Gommers,
EclecticIQ

Mike Small
KuppingerCole

Frank Lange,
Anomali

Daniel Riedel,
New Context,
Inc.

Jason Keirstead,
IBM Security
Intelligence

Alex Valdivia,
ThreatConnect,
Inc.

Some Topics for Discussion

Real World Examples of CTI	Adoption of STIX, TAXII and CybOX	How to successfully implement CTI
Threat Data vs Threat Intelligence	Barriers to sharing Threat Intelligence	Reactive vs Proactive Threat Management
Does CTI really help with SIEM Overload	How does MLS and AI relate to CTI	Privacy Implications of CTI

- **For more information** on the OASIS Cyber Threat Intelligence work and technical committee, please go to www.oasis-open.org or ask a CTI member here at the conference.

  Look for the green CTI member ribbons.

- **Questions** regarding our the standards and how to become involved in the work, please contact an OASIS representative at info@oasis-open.org.