OASIS

STIX™ TAXII™

Overview, History & Roadmap

June 2018

What is Cyber Threat Intelligence (CTI)?

"(Cyber) Threat Intelligence is evidence-based knowledge (e.g. context, mechanisms, indicators, implications and action-oriented advice) about existing or emerging menaces or hazards to assets".

Gartner Group (2016)

OASIS

Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

Why standardize the exchange of CTI?

- Enable interoperable sharing of CTI across:
  - Organizational boundaries
  - Technology boundaries
  - Geographic boundaries
- Enable efficient and effective automated processing of CTI
  - Allow automated ingestion, triage and correlation
  - Support automated analysis
  - Enrich CTI streams used by threat analysts

OASIS

Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

Historical Timeline

Inception

US Department of Homeland Security begins initiative to develop a standard for cyber threat intelligence exchange

Initial Operational Use

Financial sector begins pilot program to exchange indicators via STIX/TAXII

Development of STIX/TAXII 2.0

CTI TC begins development of the next generation of STIX/TAXII

2012 2013 2014 2015 2016 2017

STIX/TAXII 1.0 Released

First major release of STIX and TAXII

Transition to OASIS

DHS transitions governance of STIX/TAXII to OASIS, an international standards development organization - CTI TC formed

STIX / TAXII 2.0 Published

CTI TC approves “Committee Specifications” for STIX 2.0 and TAXII 2.0. Work begins on STIX 2.1 and TAXII 2.1

Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

Structured Threat Information Expression

A language for sharing cyber threat intelligence.

- JSON language to describe Cyber Threat Intelligence
- Designed to facilitate sharing
- Active community of developers and analysts
- International standard in OASIS
- Current version - STIX 2.0

Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

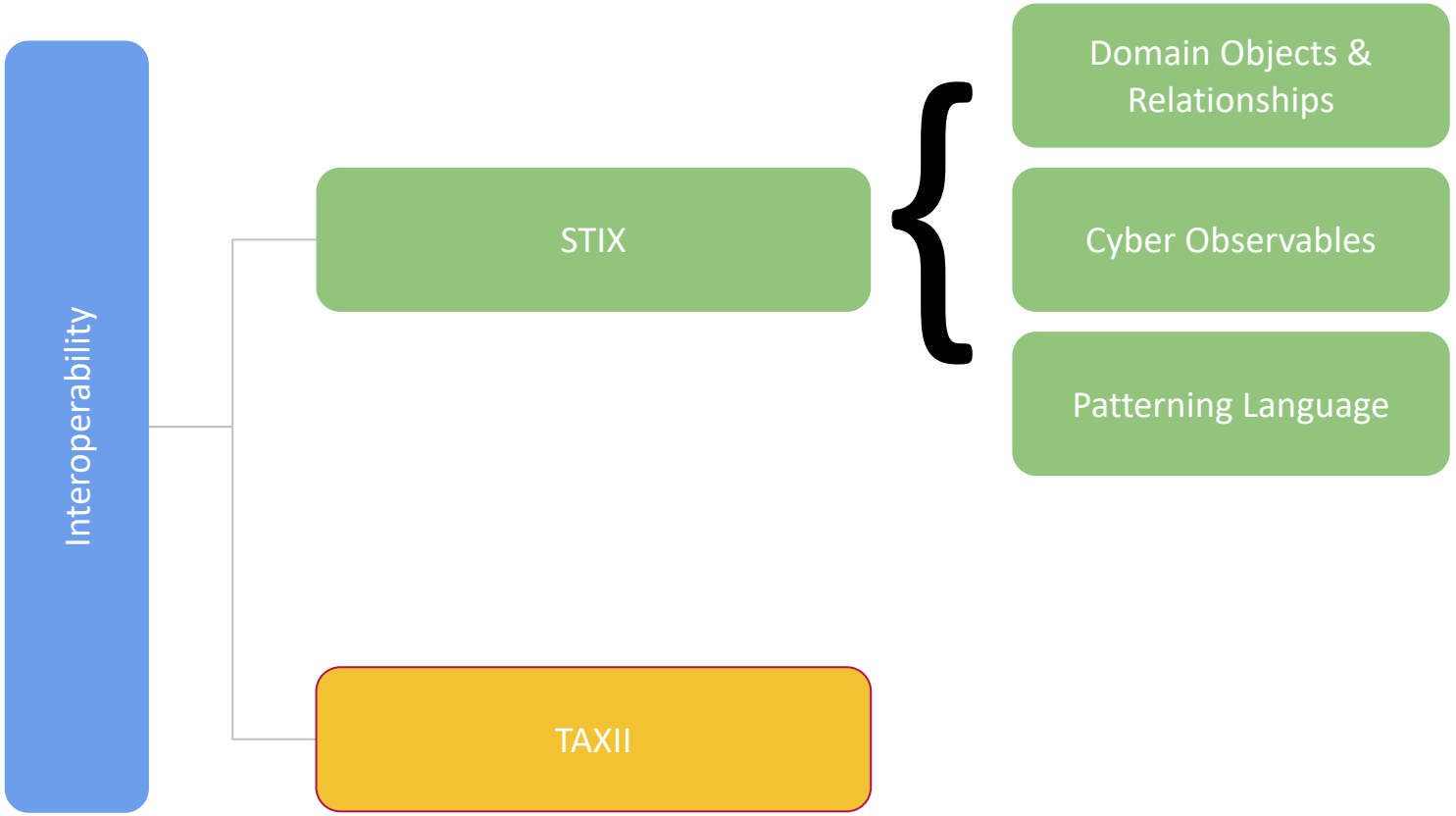
Trusted Automated eXchange of Intelligence Information

A protocol for sharing cyber threat intelligence.

- Application protocol running on top of HTTPS
- Designed to facilitate sharing of CTI data - especially STIX
- Open-source implementations in multiple programming languages
- International standard in OASIS
- Current version - TAXII 2.0

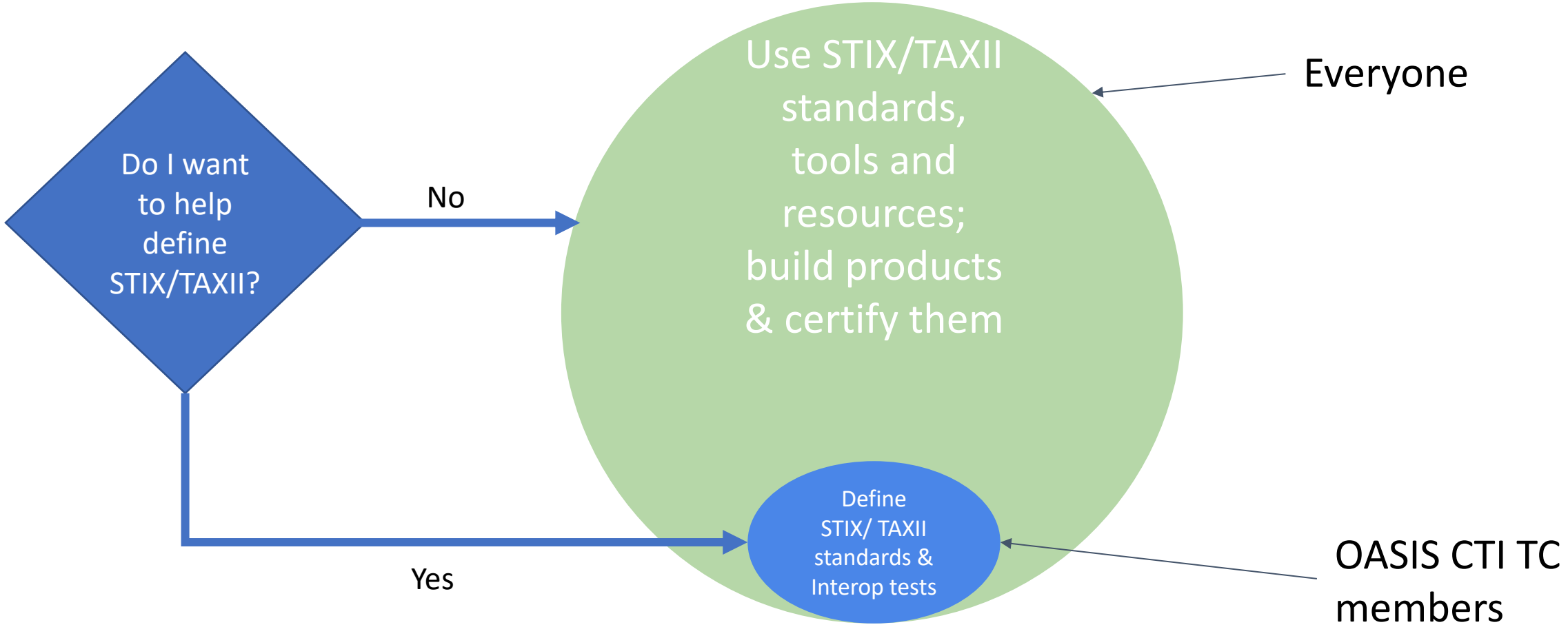
Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

The STIX/TAXII Standards Ecosystem



Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

Who does what with STIX/TAXII?



Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

OASIS Cyber Threat Intelligence TC

- Large: 299 Members (Largest OASIS TC in history)
- Broad: Multi-nationals, start-ups, universities, government agencies, consultants
- Representative: Financial services, healthcare, software, research, public sector
- International: Asia, Australia, Europe, North America

Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

OASIS CTI TC Members

accenture
aetna
AIRBUS
AIT Austrian Institute of Technology
ANOMALI
ANZ
Bank of America
BMO Bank of Montreal
BOEING
circl
CISCO
Center for Internet Security
Cyber Threat Intelligence Network
DELL
eclectic iq
EPRI
Financial Services ISAC
FireEye
FORNETIX
ForeScout
FORTINET
FUJITSU
G2
GENIVIA
Georgetown University
Google
Government Digital Service
HITACHI
Huntsman
IBM
iboss
情報セキュリティ大学院大学 Institute of Information Security
intel
APL Johns Hopkins Applied Physics Laboratory
JPMorganChase
Kaiser Permanente
Lookingglass
McAfee
MITRE
MTG
NFESB
NATO OTAN
NC4
NEC
New Context
NINEFX
NIST
Northrop Grumman
paloalto Networks
PERCH
Queralt
Seekintoo
Semper Fortis Solutions
SIEMENS
Southern California Edison
splunk>
Symantec
surevine
SYNOPSYS
TELUS
ThreatConnect
ThreatQuotient
Trend Micro
TruStar Technology
usbancorp
Department of Defense
Department of Homeland Security
National Security Agency
VERISIGN
ViaSat
XLAB
YAANA

Some OASIS terminology

"Committee Note" (CN)

- TC work product (not standards track)

"Committee Specification Draft" (CSD)

- Intermediate TC work product
- No public comment required

"Committee Specification" (CS)

- Final TC work product
- Requires public comment period and adjudication
- Once approved by the TC "locks in" IPR protections
- Many TCs stop here in the process

"OASIS Standard"

- Requires approval by OASIS membership writ large

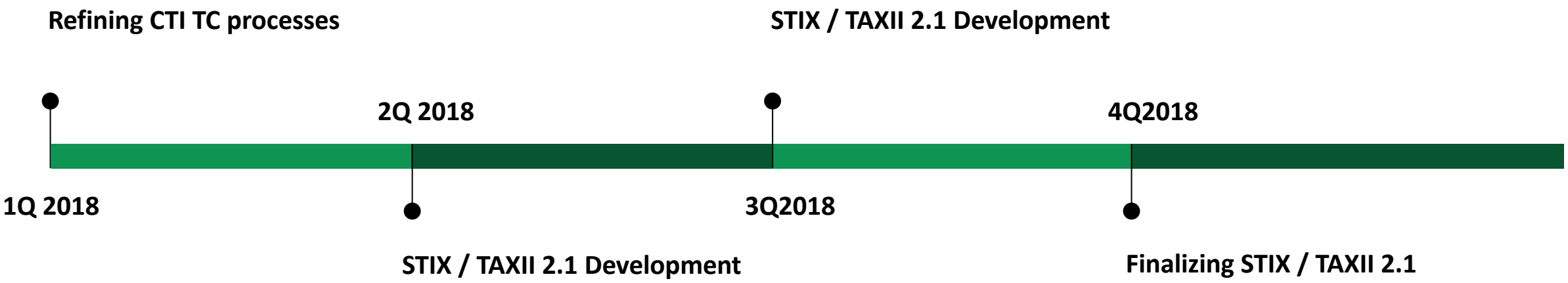
Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

If you want to…

- Get an overview and examples of STIX/TAXII:
  - https://oasis-open.github.io/cti-documentation/
- Read the actual specifications:
  - https://oasis-open.github.io/cti-documentation/resources#stix-20-specification
- Learn more about the CTI TC:
  - https://wiki.oasis-open.org/cti/
- Access STIX/TAXII APIs and tools:
  - https://github.com/oasis-open?q=cti-
- Join OASIS and the CTI TC:
  - https://www.oasis-open.org/join/ or email join@oasis-open.org

Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

Current Timeline



Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

Thank You