CTI-TC Monthly Meeting:
Session #2

Meeting Date: January 20, 2022
Purpose: Monthly CTI TC Meeting

Attendees:

<table>
<thead>
<tr>
<th>Name</th>
<th>Company</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Coderre, Robert</td>
<td>Accenture</td>
<td>Chair</td>
</tr>
<tr>
<td>Keith, Robert</td>
<td>Accenture</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Kostrosky, Curtis</td>
<td>Accenture</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Thompson, Dean</td>
<td>Australia and New Zealand Banking Group</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Gurney, John-Mark</td>
<td>Copado</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Hunt, Christian</td>
<td>Copado</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Ginn, Jane</td>
<td>Cyber Threat Intelligence Network, Inc.</td>
<td>Secretary</td>
</tr>
<tr>
<td>Ricard, Chris</td>
<td>FS-ISAC</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Masuoka, Ryusuke</td>
<td>Fujitsu Limited</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Satomi, Toshitaka</td>
<td>Fujitsu Limited</td>
<td>Voting Member</td>
</tr>
<tr>
<td>MacDonald, Terry</td>
<td>Individual</td>
<td>Member</td>
</tr>
<tr>
<td>Piazza, Rich</td>
<td>MITRE</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Relitz, Stephan</td>
<td>Peraton</td>
<td>Member</td>
</tr>
</tbody>
</table>

Agenda:
- TC Updates
- STIX SC Update
- STIX Co-Chair update; Welcome to Christian Studer
- Extensions WG
- Incident WG
- Interop SC Updates
- Community Development Corner

Meeting Notes:

Rob Coderre
Welcome to all – thank for you recording your attendance
This meeting will be recorded

Trey Darley
STIX and TAXII 2.1 won the OASIS Open Cup for Outstanding Approved Standard
This award is not given out every year so when it does, it is meaningful

Rob Coderre
This represents your work. This is a group recognition and we should be very proud. Thank you all!
Call for nominations
We still need TC members to fill the following roles:

- Interop SC co-chair
- TAXII SC chair/co-chairs
- One or more people willing to serve as a specification editor
- One or more maintainers for STIX Open Repository tools
  - Contact Chris Lenk (clenk@mitre.org) directly
- If you are interested in any one of these roles, please send a note to the co-chairs or listserv

Meeting Updates
The TC will continue to meet monthly for Q1 2022. Meeting times may be adjusted. Stay tuned for more information

STIX SC Update
Emily Ratliff
Welcome Christian Studer, our new STIX co-chair!
Focus on Extension Policy definition led by Rich Piazza
Please read the doc and provide follow up:
https://docs.google.com/document/d/1bjcYUWb9uF0qYrdSP-bqtmxVyxONB-RF7SLVR9dZC8/edit
Next week: JSON Signing
  JMG and cvoid taking lead on this. Please join the kick off convo next week.

Rich Piazza
Extensions Update

Contents of an Extension Definition
- JSON schema
- Extension Definition object
- Documentation in the style of the STIX Specification
- Examples
Jeff Mates
Incident WG Update

What it supports:
- Timeline and lifecycle information for incidents
- IoCs and TTPs for an incident
- Recording and sharing severity and impacts in a structured manner
- Automated alerting options with varying levels of trust / fidelity
- Related incidents and follow-ons
• Recording and sharing high level plans via Courses of Actions

What it doesn’t do:
• Provide a way to record time to tickets
• Provide a way to handle actions... this will be a future object

How We Got Here
▪ STIX 2.1 is a powerful open standard for sharing CTI
  • Unfortunately, the Incident object is still a placeholder
▪ May 12, 2021, an Executive Order was issued that among other things sought to improve cyber threat and incident information sharing
▪ DC3 and CISA began collaboration on the STIX Incident in June 2021
▪ STIX Incident Working Group kicked off October 1, 2021
▪ Work is finalizing lets get it done and out there

Current Incident Object
▪ ID (required)
▪ Name (required)
▪ Versioning (required)
  • Several different fields, but these all serve the general purpose of versioning
▪ Description
▪ Labels
▪ Data Markings
▪ Standard STIX relationship options

Life Cycle
▪ Investigation Status (required) – Open Vocab (new, open, closed)
▪ Determination (required) – suspected, low-value, false-positive, blocked, failed-attempt, successful-attempt
▪ Attacker Activities: List of Objects
▪ Defender Activities: List of Objects
▪ Detection Methods: List of Strings

CIA Impacts
▪ Confidentiality Impacts: List
  • Description: String
  • Information Type (required*): Open Vocabulary
    • Examples: classified-material, credentials-admin, phi, pii, proprietary
  • Loss Type (required): none, contained, suspected-loss, suspected-major-loss, some-loss, major-loss, exploited-loss, exploited-major-loss
  • Record Count: Whole Number
  • Record Size: Whole Number
▪ Integrity Impacts: List
  • Alteration (required): none, potential-destruction, potential-modification, partial-destruction, partial-modification, full-destruction, full-modification
  • Description: String
• Information Type (required*): Open Vocabulary
• Record Count: Whole Number
• Record Size: Whole Number
• Recoverability: not-applicable, regular, supplemented, extended, not-recoverable
  ▪ Availability Impact – 0 to 100

Non CIA Impacts
▪ Recoverability: not-applicable, regular, supplemented, extended, not-recoverable
▪ External Impacts: List of open vocabulary items
  ▪ Examples: civil-liberties, economic, national-security, public-health
▪ Traceability Impact: accountability-lost, partial-accountability, provable-accountability
▪ Impacted Entity Counts: Dictionary of type: count

Scoring for Automation
▪ Criticality – 0 to 100
▪ Incident Types: List of open vocabulary items
  ▪ Examples: compromised-system, supply-chain-customer, unauthorized-release
▪ Scores: List
  ▪ Name (required): String
  ▪ Value (required): Number
  ▪ Description: String

Attacker Activity
▪ Required Fields (only one is required, but both can be present)
  ▪ Activity Type: String
  ▪ Pattern Reference: Reference to Attack Pattern (ATT&CK)
▪ Optional Fields
  ▪ Description: String
  ▪ Start / End Time (separate fields): Timestamp
  ▪ Start / End Sequence (separate fields): Number
  ▪ Object References: List of References to Indicators, Observables, Sightings and SCOs

Defender Activity
▪ Used to generate a list of activity performed by defenders
▪ Timestamps are required, but every action is considered atomic. So, recovery-started and recovery-completed are recorded separately.
▪ Fields
  ▪ Timestamp (required): Timestamp
  ▪ Activity Type (required): Open Vocab
    ▪ Examples: detected, escalated, recovery-started, recovery-completed, reported
  ▪ Description: String
  ▪ is_projection: Boolean
    ▪ Indicates that this is a future projection instead of a record time.
    ▪ Example: The projected time recovery will be completed
  ▪ Object Reference: Reference to a Course of Action / Playbook
So What?

- Allows incident / case management systems to generate, track and share STIX content
- Results can be merged with SIEM, incident detection and response tools and workflows
- Results can be passed along through mandatory and voluntary reports while removing elements that are deemed sensitive for internal purposes
- Having a codified set of fields means that this becomes more vendor agnostic lowering costs and barriers to entry

Marlon Taylor
Interop TAXII Working Calls
   TUESDAYS @ 2PM EST
Plugfest Update
   2 planning meetings have occurred
   12 orgs on the roster
STIX Personas identified so far (MAS, SIEM, SXP*, SXC*, TIP) all at Level 2
   18+ Interop use-cases TDB (out of 21 use-cases)
TAXII Personas identified (TXS, TXC)
   Tentative Dates March/June 2022 (2nd/3rd week)
   Virtual with possible In-person sponsorship

Remaining Personas
   Software or system, that consumes and produces STIX content, that is used to map out adversarial networks

Local Infrastructure Mapping (LIM)
   Software that scans local networks and provides STIX representations of these finds.

Threat Detection System (TDS)
   Software instance of any network product that monitors, detects and alerts such as Intrusion Detection Software (IDS), Endpoint Detection and Response (EDR) software, web proxy, etc. This is applicable for both Producers and Consumers.

Threat Mitigation System (TMS)
   Software instance that acts on Course of Action and data from other threat mitigations such as a firewall, IPS, Endpoint Detection and Response (EDR) software, etc. This is applicable for both Producers and Consumers.

Recap
   TAXII 2.1 Interoperability Test Document
      TAXII Requirement Checklist (Conformance)
      Use Cases
      Interop / Checklist
PlugFest
   Next Session (Jan 27 @ 9PM EST)
OASIS CTI-TC Monthly TC Call

STIX Preferred Website
Update Website & Develop Workflows

Community Development Corner
Tomas Sabat & Brett Forbes
https://vaticle.com/discord
https://github.com/typedb-os/typedb-data-cti
https://github.com/typedb-os/typedb-data-cti

Recording of Demo

https://youtu.be/nQeot-WyplY

Meeting Terminated