Pitch of the Project Proposal

Next Generation Cybersecurity Mesh-networks

Rob van Kranenburg, CIO, asvin.io
r.v.kranenburg@asvin.io

Teaser

The vast increase of public internet addresses enabled by IPV6 (to a theoretical maximum of 340 sextillions) requires a rethink of the cybersecurity paradigm. *Next Generation Cybersecurity Mesh-networks* is intended as a reliable yet cost-effective answer to this new threat environment

- **Mesh architectures** is **one promising answer** to the coming challenge of a vast expansion of sources of threat. GARTNER evaluates it as an *Innovation Trigger* in its *Emerging Tech Trends 2022*.
- This approach makes **two critical contributions** to this new cybersecurity paradigm
  1. Its information sharing through graph based models that provides added visibility to the relationships between the actors and endpoints, offering context and allowing for prioritization of risk.
  2. A heightened resilience through a peer-to-peer based information sharing between actors in a supply chain.

Overall Graph based analysis illuminates attack trajectories and offers better context information, picking up anomalies along more complete and relevant parameters, as well as allowing for a more reliable threat assessment .

Proposal Introduction

Most of these attacking entities exist only from a brief moment in time. What we want to investigate in this project is how disposable identities can lead to a temporary trustzone enabling us to identify anomalies and assess threats from minimal available characteristics, focusing on the relationships between them to produce the threat assessment.

Disposable Identities are designed for advanced decentralized privacy agreements, which can also be time, purpose and context bound through a secure digital contract; with verification functionalities based on tamper-proof technologies. (Twinds, 2021).

We thus talk about "event identities' that can help to build a repository of attack events.
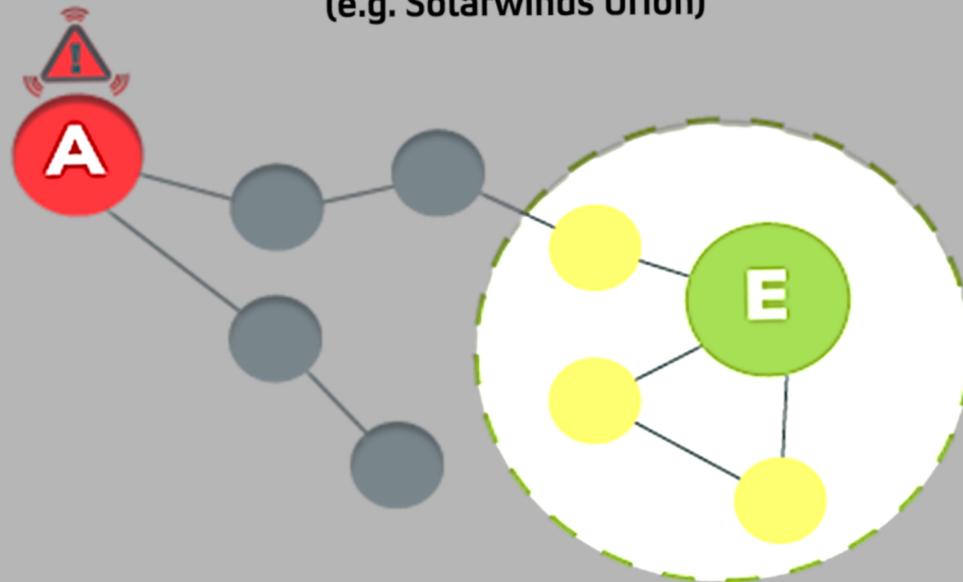
Proposal Introduction

What it means ... A schematic

Isolated View Today
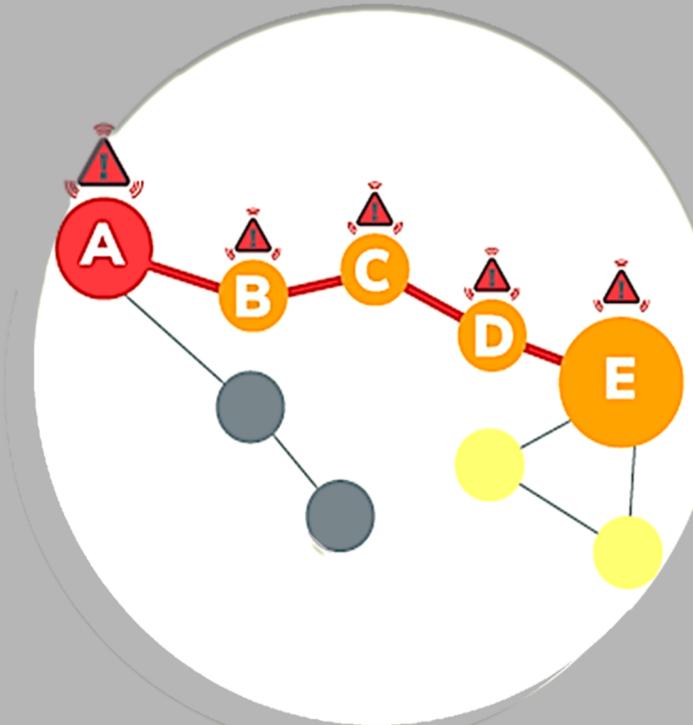
Supply Chain Attack Without Mesh Networks

(e.g. Solarwinds Orion)

Organization E sees no imminent security risk.
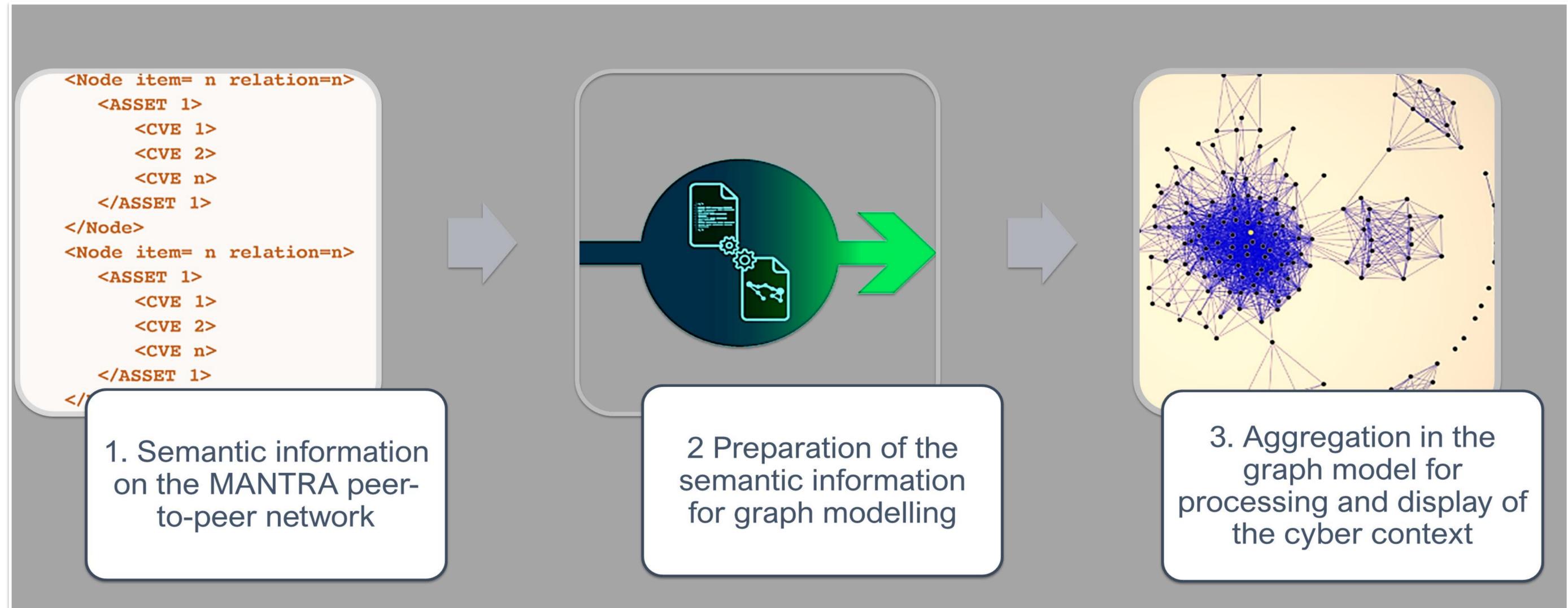Meanwhile, Attacker A, connecting through D,
remains unseen.

Expanded with Mesh Networks

Supply chain attack with Mesh Networks

Organization E recognizes
 through Graph Analysis
a connection to a security risk from A
(e.g. attack via B/C/D)

Nextgen Cybersecurity Mesh Networks, Rob van kranenburg, asvin.io, r.v.kranenbu@asvin.io

eureka
innovation beyond borders

Proposal
Introduction


```
<Node item= n relation=n>
    <ASSET 1>
        <CVE 1>
        <CVE 2>
        <CVE n>
    </ASSET 1>
</Node>
<Node item= n relation=n>
    <ASSET 1>
        <CVE 1>
        <CVE 2>
        <CVE n>
    </ASSET 1>
</
```

1. Semantic information on the MANTRA peer-to-peer network

2 Preparation of the semantic information for graph modelling

3. Aggregation in the graph model for processing and display of the cyber context

Organisation Profile

*At **asvin**, we have designed and developed*

- *a secure, resilient, scalable, and seamless platform*
- *equipped with advanced cryptographic algorithms*
- *Leveraging distributed ledger technology (DLT)*
- *powered by Hyperledger Fabric and peer-to-peer network storage using InterPlanetary File System protocol*

asvin BeeHive cybersecurity management system

provides a one-stop solution in a software as a service (SaaS) model for IoT vendors and manufacturers to facilitate the seamless delivery of IoT security patches and updates for IoT devices.

Proposal Introduction

Expected outcome

- *Demonstrate the feasibility of the implementation of the architecture with service providers.*

- *Measure and further enhance process results and generate evidence metrics for cost-effectiveness*

Timeline

M1-3 research → M 3-6 implementation → M6-9 testing

The process will be cycled 4 times with the latter two in real word setting.

Partners

Our multinational consortium brings a mix of technical expertise and the capacity to implement real-world user group testing: to be confirmed:

Asvin

Odins

Twinds

Eurocon

Crowdsec (tbc)

What we are looking for…

Partners providing a supply-chain environment for the real-life tests

eureka
innovation beyond borders

Contact Info

For more information and for interest to participate please contact:

Rob. van Kranenburg
CIO, asvin.io
asvin GmbH,
Schulze-Delitzsch-Str. 16
70565 Stuttgart
https://www.asvin.io
r.v.kranenburg@asvin.io

Presentation available via:

9th Sept. 11 CET

Join the follow-up Telco

Join meeting

Join by meeting number
Meeting number (access code):2740 389 9536
Meeting password: GaNPdk2ig57
Join by phone
+49-6196-7819736 Germany Toll

Can't join the meeting?