

Models will not solve
all of your problems

But they can help you understand...

Avi Shaked, PhD
Senior Research Associate



Why do we need model driven engineering?

- “To generate usable work products”
- “To organise, find, filter, retrieve, examine, and edit information about large systems”

But also:

- “To capture and precisely state requirements and domain knowledge so that all stakeholders may understand and agree on them”
- “To think about the design of a system”



Does modelling really support the objectives?

- UML Ref Manual:
 - “Semantics and presentation”
 - Semantics (“often called *the model*”) – capture “the meaning of an application as a network of logical constructs”
 - Presentation – “shows semantic information in a form the can be seen, browsed and edited by humans”. “Presentation elements carry the visual presentation of the model – that is, they show it in a form directly apprehensible by humans.”

Let's examine this in a real life application



A model driven approach to systems security engineering

Trying to design security aspects of systems and assess security posture and risks



A model driven approach to systems security engineering: Semantics (capture “the meaning of an application as a network of logical constructs”)

□ UML

□ Actor:

“characterizes and abstracts an outside user or related set of users that interact with a system of classifier”

□ Class:

“the named description of both the data structure and the behavior of a set of objects”

□ Real life:

□ System

□ Components

□ Threats, Risks

□ Security Controls

□ Mitigation



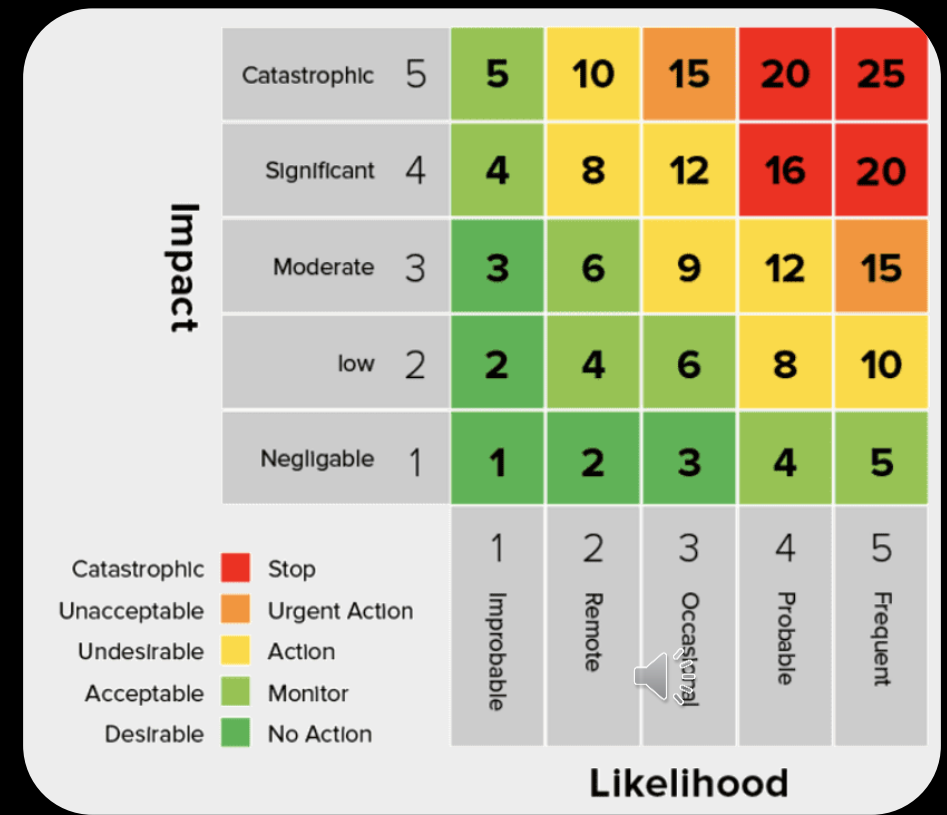
A model driven approach to systems security engineering: Presentation (show the model in a form directly apprehensible by humans)

So, what should we do?

- UML
 - Class diagram?
 - Use case diagram?
- Real life

	«Block» Radio	«ConstraintBlock» Joule Effect	«Block» AlarmRadio	«Block» Alarm
«Requirement» 004 : Save				
«Requirement» 007 : Radio frequencies				
«Requirement» 008 : Dissipation				
«Requirement» 003 : Clock control				
«Requirement» 001 : Alarm				
«Requirement» 005 : Radio station control	s			
«Requirement» 002 : Radio control	s			
«Requirement» 006 : Volume radio control				

Source: <http://www.uml designer.org/ref-doc/define-the-system.html>



Source: <https://www.balbix.com/insights/cyber-risk-heat-map/>

Why do we need model driven engineering?

- o "To generate usable work products"
- o "To organise, find, filter, retrieve, examine, and edit information about large systems"

But also:

- o "To capture and precisely state requirements and domain knowledge so that all stakeholders may understand and agree on them"
- o "To think about the design of a system"

A domain-specific, model driven approach to systems security engineering

The screenshot displays the TRADES Tool interface. At the top, a 'ShipSystem Risk Management Summary' table shows risk levels from 1 (Minor) to 7 (Frequent). A specific risk entry is highlighted: 'Combination of social engineering with malware installation on Shore Control Centre, Getting access to the shore' with a severity of 4. Below this, a 'Controls allocation to components' table lists various security controls like 'Data filtering between zones (Firewall)' and 'Redundant links (different technologies)'. The bottom half of the screenshot shows a 'System Scope' diagram with components such as 'Shore Control Centre', 'Ship control station', 'Engine automation system', 'Autonomous ship controller', 'Connectivity manager', 'Autonomous navigation system', and 'Route planning system'. Threats like 'Malware installation' and 'Physical attack' are linked to these components.

OK, but what properties of that link?

"... but some of our assessment is based on the link that conveys the data flow!"

Synchronised risk matrix

Function allocations

Formalised security assessment



Revised TRADES Tool

The screenshot displays the TRADES Tool interface with two main views. The top view, titled "System Scope", shows a network diagram with components like "Internet", "Shore Control Centre", and "Ship Systems". A blue starburst highlights the text "Formalised system design". The bottom view, titled "TRADES diagram", shows a similar diagram with a red starburst highlighting "New semantics".

On the right side, a "ShipSystem Risk Management Summary" table is visible:

	1...	2 [2]	3	4 [4]
Minor [1]	0	0	0	0
Significant [2]	0	0	0	0
Severe [3]	0	0	0	[Malware installation]
Catastrophic [4]	0	0	[Combination of social e]	0

At the bottom, a "Link 4G ship-shore" table shows properties:

Link	Property	Value
Semantic	Components	Communication Network, Ship Systems, Shore Control Centre
Style	Conveying Link	
Appearance	Link Conveyed	
	Link Type	Link Type 4G/5G
	Name	4G ship-shore

TRADES Tool

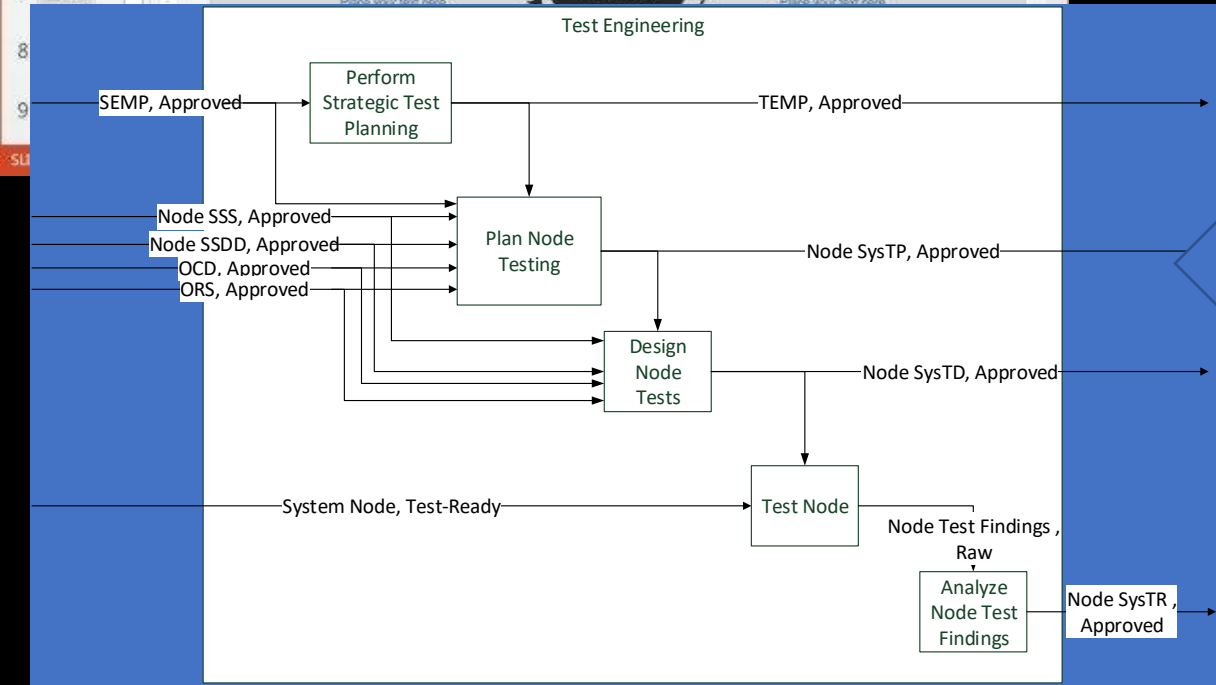
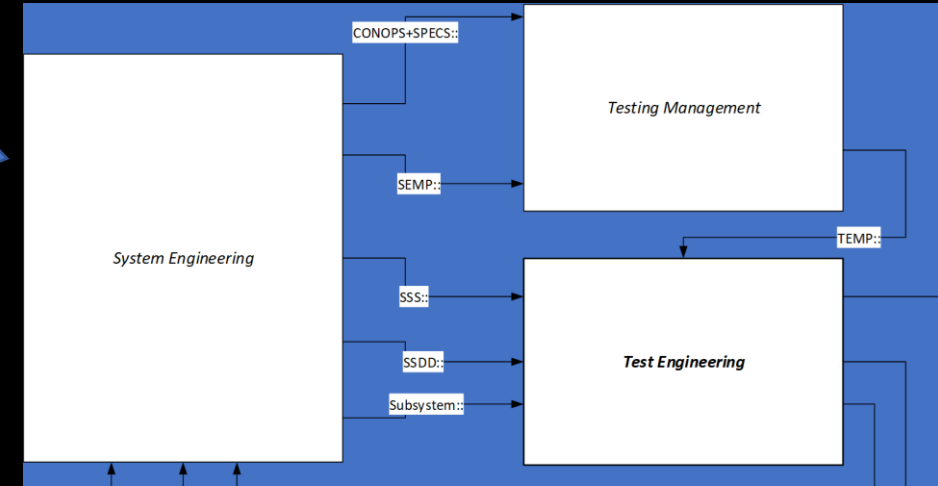
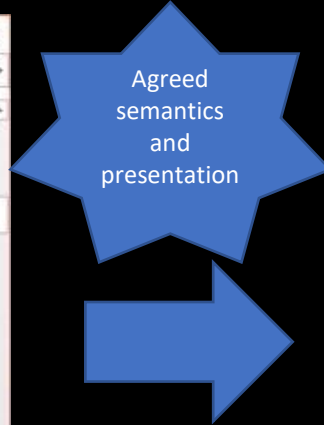
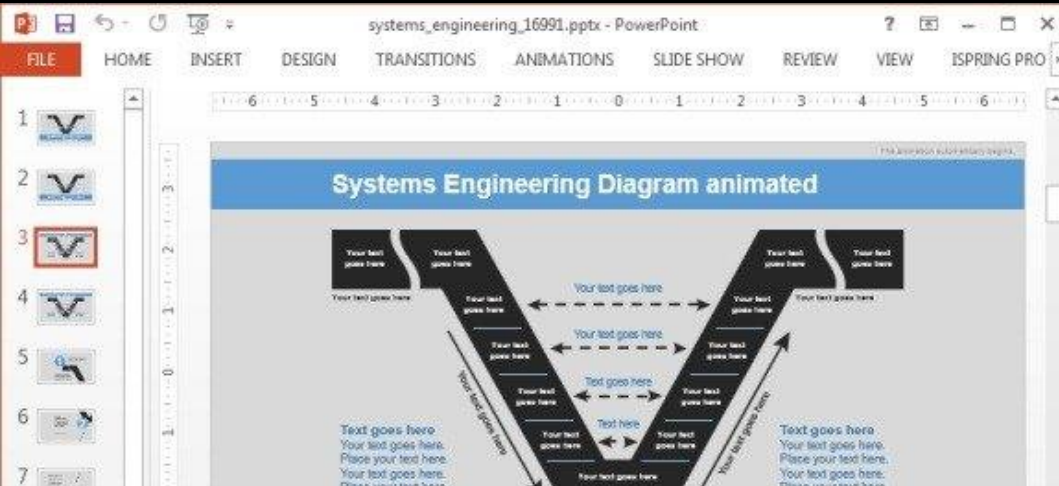


(c) 2020 ELTA - All rights reserved IAI ELTA

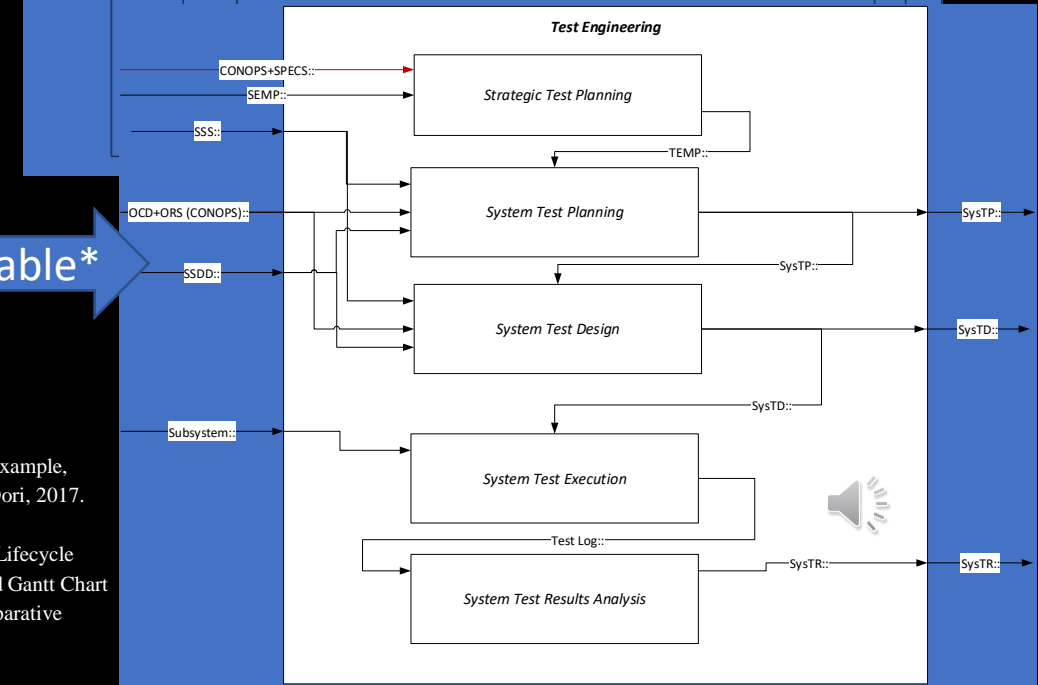
Restructuring the development process definitions



<https://github.com/TAU-SERI/PROVE>

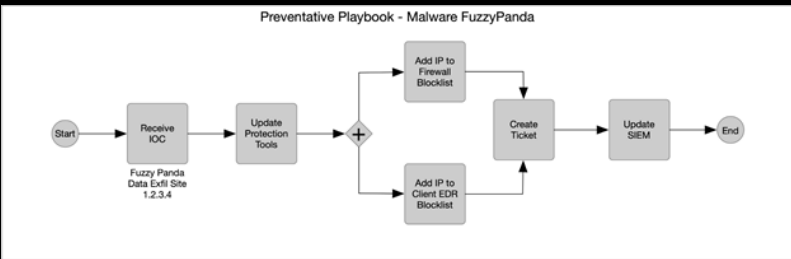


Comparable*



* Compare, for example, with Sharon & Dori, 2017. Model-Based Project-Product Lifecycle Management and Gantt Chart Models: A Comparative Study.

Designing Cyber Security Incident Response: Restructuring the process playbook

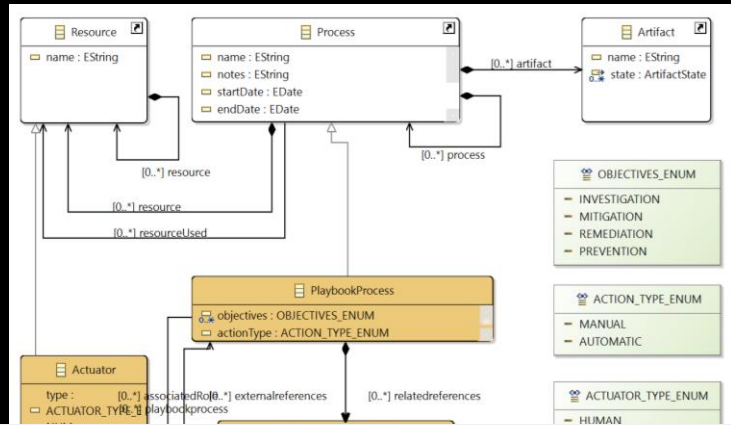


Source: <https://docs.oasis-open.org/cacao/security-playbooks/v1.0/security-playbooks-v1.0.html>

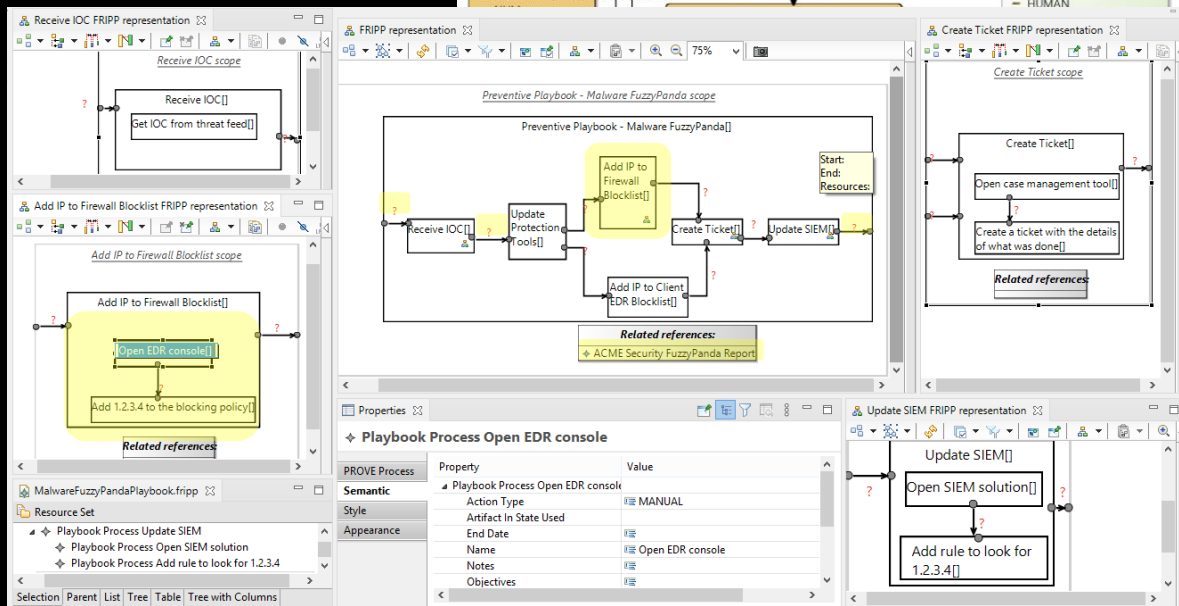
```

{
  "type": "playbook",
  "spec_version": "1.0",
  "id": "playbook--6b74199d-42a6-43a1-99cb-75d52207a778",
  "name": "Prevent FuzzyPanda Malware",
  "description": "This playbook will block traffic to the FuzzyPanda data exfil site",
  "playbook_types": [ "prevention" ],
  "external_references": [ { "name": "ACME Security FuzzyPanda_Report" } ],
  "features": { "parallel_processing": true, "data_markings": true },
  "markings": [ { "marking-statement": "16a48f6b-ab42-4f99-ba9b-8b21e1225836", "marking-tlp": "a099a2eb-1113-4368-9b17-d7ef75841239" }, { "marking-statement": "7269bda2-e651-44d3-9fe5-aa7e88484b93", "marking-tlp": "a099a2eb-1113-4368-9b17-d7ef75841239" } ],
  "workflow_start": { "start": "7269bda2-e651-44d3-9fe5-aa7e88484b93", "workFlow": { "start": "7269bda2-e651-44d3-9fe5-aa7e88484b93", "type": "start", "on_completion": "single--a13c8450-2bd1-4a2b-9241-cf477e9f48cb" }, "single--8c46cab0-46a3-48f4-b4bb-9643dcfa642": { "type": "single", "name": "Add IP to Firewall Blocklist", "description": "This step will add the IP address of the FuzzyPanda data exfil site to the firewall", "on_completion": "single--d5780323-5107-4cd0-bac4-6553c9d90c8e", "commands": [ { "type": "manual", "command": "Open firewall console and add 1.2.3.4 to the firewall blocking policy" } ], "single--3d930f88-e22c-4dd4-906f-61f2d022121c": { "type": "single", "name": "Add IP to Client EDR Blocklist", "description": "This step will add the IP address of the FuzzyPanda data exfil site to the client EDR solution", "on_completion": "single--d5780323-5107-4cd0-bac4-6553c9d90c8e", "commands": [ { "type": "manual", "command": "Open EDR console and add 1.2.3.4 to the blocking policy" } ] }, "single--d5780323-5107-4cd0-bac4-6553c9d90c8e": { "type": "single", "name": "Create ticket", "description": "This step will create a ticket for this issue", "on_completion": "single--33dc512c-263d-4f8a-a07d-cfe9fd6ed26", "commands": [ { "type": "manual", "command": "Open case management tool and create a ticket with the details of what was done" } ] } } } }

```



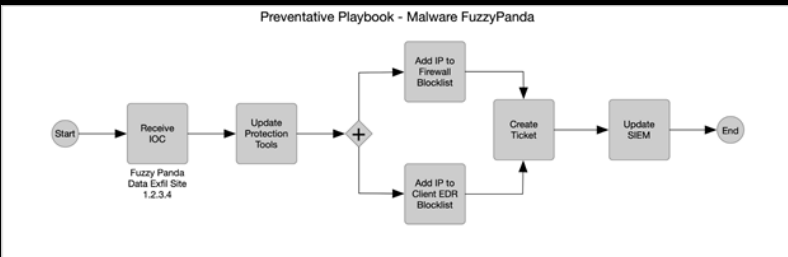
Formalised Incident Response Semantics



Formalised Incident Response Presentation

Source: Shaked, Cherdantseva, and Burnap, 2022. Model-Based Incident Response Playbooks. In Proceedings of the 17th International Conference on Availability, Reliability and Security.

Designing Cyber Security Incident Response: Restructuring the process playbook is insufficient!

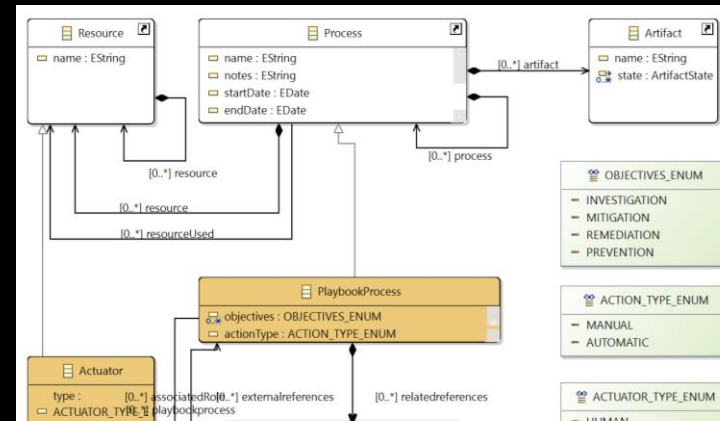


Source: <https://docs.oasis-open.org/cacao/security-playbooks/v1.0/security-playbooks-v1.0.html>

```

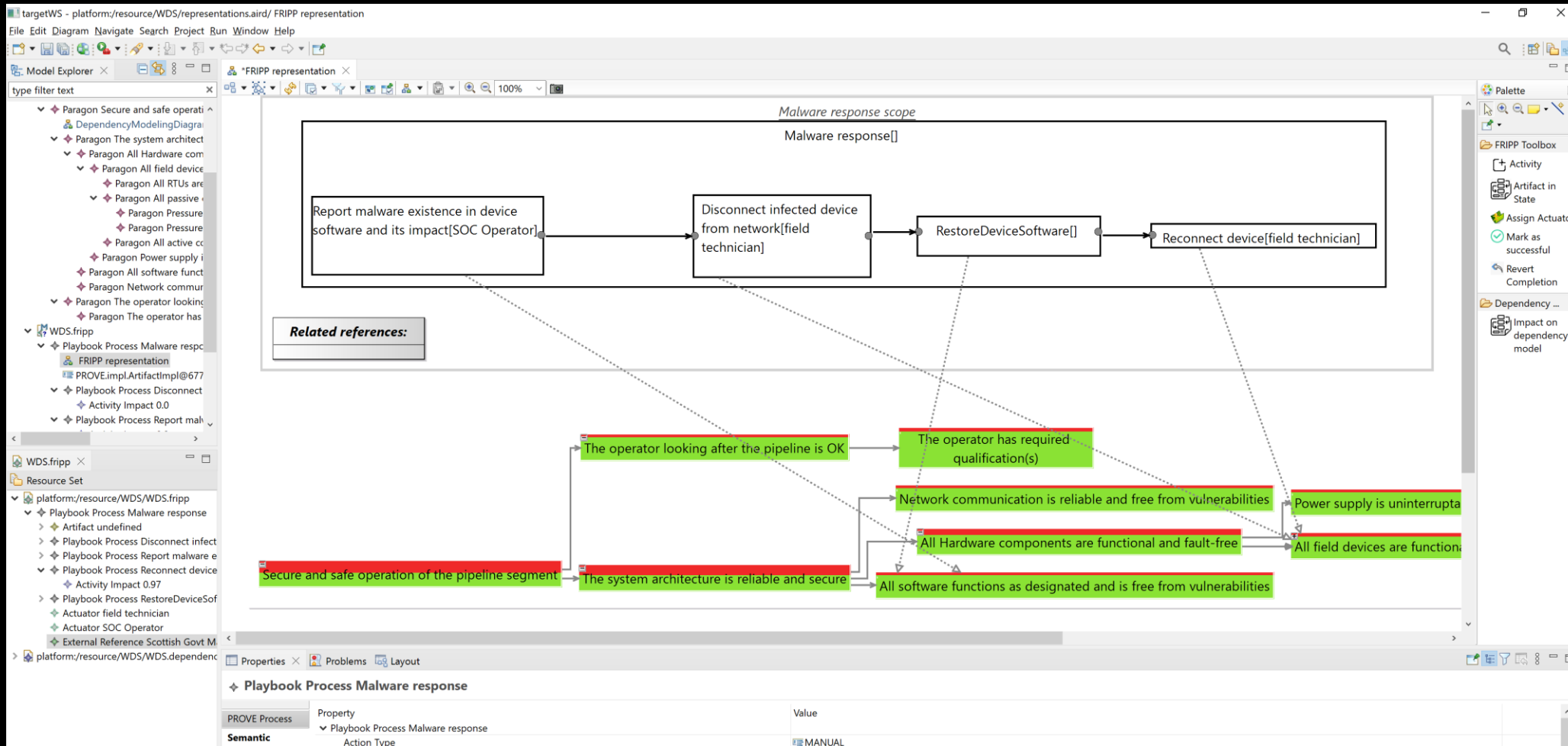
{
  "type": "playbook",
  "spec_version": "1.0",
  "id": "playbook--6b74199d-42a6-43a1-99cb-75d52207a778",
  "name": "Prevent FuzzyPanda Malware",
  "description": "This playbook will block traffic to the FuzzyPanda data exfil site",
  "playbook_types": [ "prevention" ],
  "external_references": [ { "name": "ACME Security FuzzyPanda_Report" } ],
  "features": { "parallel_processing": true, "data_markings": true },
  "markings": [ { "marking-statement": "16a48f6b-ab42-4f99-ba9b-8b21e1225836", "marking-tlp": "a099a2eb-1113-4368-9b17-d7ef75841239" }, { "workFlow_start": "start--7269bda2-e651-44d3-9fe5-aa7e88484b93", "workFlow": { "start--7269bda2-e651-44d3-9fe5-aa7e88484b93": { "type": "start", "on_completion": "single--a13c8450-2bd1-4a2b-9241-cf477e9f48cb" }, "single--8c46cab0-46a3-48f4-b4bb-9643dcfaf642": { "type": "single", "name": "Add IP to Firewall Blocklist", "description": "This step will add the IP address of the FuzzyPanda data exfil site to the firewall", "on_completion": "single--d5780323-5107-4cd0-bac4-6553c9d90c8e", "commands": [ { "type": "manual", "command": "Open firewall console and add 1.2.3.4 to the firewall blocking policy" } ] }, "single--3d930f08-e22c-4dd4-906f-61f2d022121c": { "type": "single", "name": "Add IP to Client EDR Blocklist", "description": "This step will add the IP address of the FuzzyPanda data exfil site to the client EDR solution", "on_completion": "single--d5780323-5107-4cd0-bac4-6553c9d90c8e", "commands": [ { "type": "manual", "command": "Open EDR console and add 1.2.3.4 to the blocking policy" } ] }, "single--d5780323-5107-4cd0-bac4-6553c9d90c8e": { "type": "single", "name": "Create ticket", "description": "This step will create a ticket for this issue", "on_completion": "single--33dc512c-263d-4f8a-a07d-cfe9fd6ed26", "commands": [ { "type": "manual", "command": "Open case management tool and create a ticket with the details of what was done" } ] } } } ],
  "single--a13c8450-2bd1-4a2b-9241-cf477e9f48cb": { "type": "single", "name": "Update SIEM", "description": "Update SIEM", "on_completion": "end" } } ],
  "end": "end"
}

```



Source: Shaked, Cherdantseva, and Burnap, 2022. Model-Based Incident Response Playbooks. In Proceedings of the 17th International Conference on Availability, Reliability and Security.

Designing Cyber Security Incident Response: Restructuring the process playbook is insufficient!



Improved semantics and presentation



Conservation of enterprise energy applies to Model-Driven Engineering

- Modelling requires significant effort
 - Develop meaningful semantics and representations
- Efficiency
 - Distributed “semantics” vs. governed, formal semantics
 - Reimagined “usable work products” - *sustainably usable products*
 - Model-based presentations
 - Can evolve, while relying on a formal information model
 - Model-based tool infrastructure (baseline, coherent integration)



Model responsibly and continuously
to better understand your domain

Thank you

Feedback is welcome:
avi.shaked@cs.ox.ac.uk

