System Security Modeller

What it does. How it works.

June 2022

Stephen C Phillips, Steve Taylor, J Brian Pickering,
Stefano Modafferi, Michael Boniface, Mike Surridge

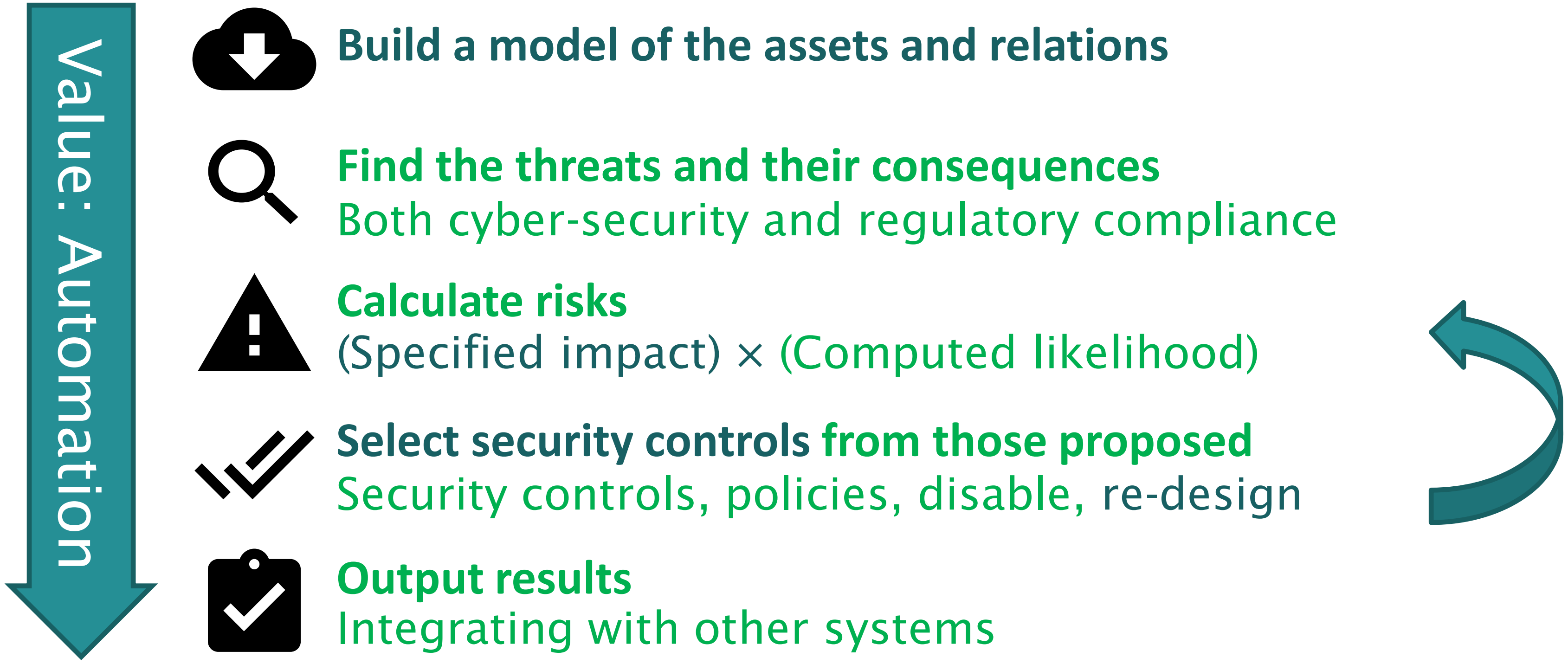
Contact: S.C.Phillips@soton.ac.uk

Complex systems have a web of attack paths.
Manual analysis is **hard**. Let’s automate!
Find the risks, communicate and deal with them.

The SSM automates much of a cyber-security risk assessment.

As well as looking for cyber threats it will also check for compliance (e.g. GDPR).

It follows the process of **ISO 27005** and thereby supports **ISO 27001** compliance.



Build a model of the assets and relations

Find the threats and their consequences
Both cyber-security and regulatory compliance

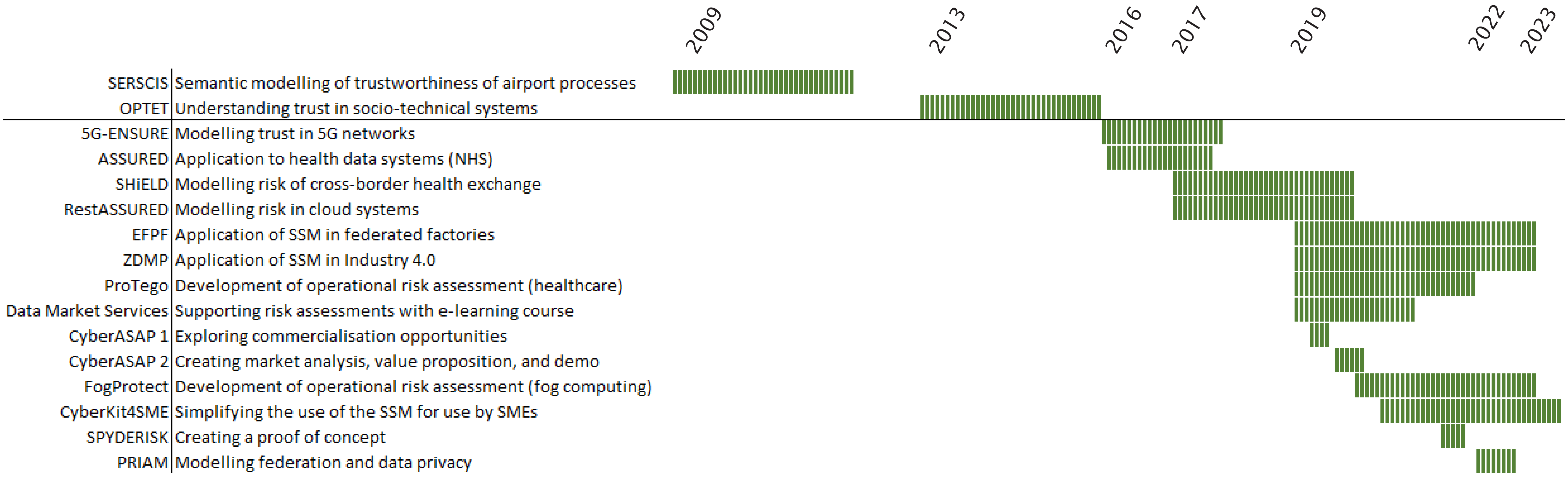
Calculate risks
(Specified impact) × (Computed likelihood)

Select security controls from those proposed
Security controls, policies, disable, re-design

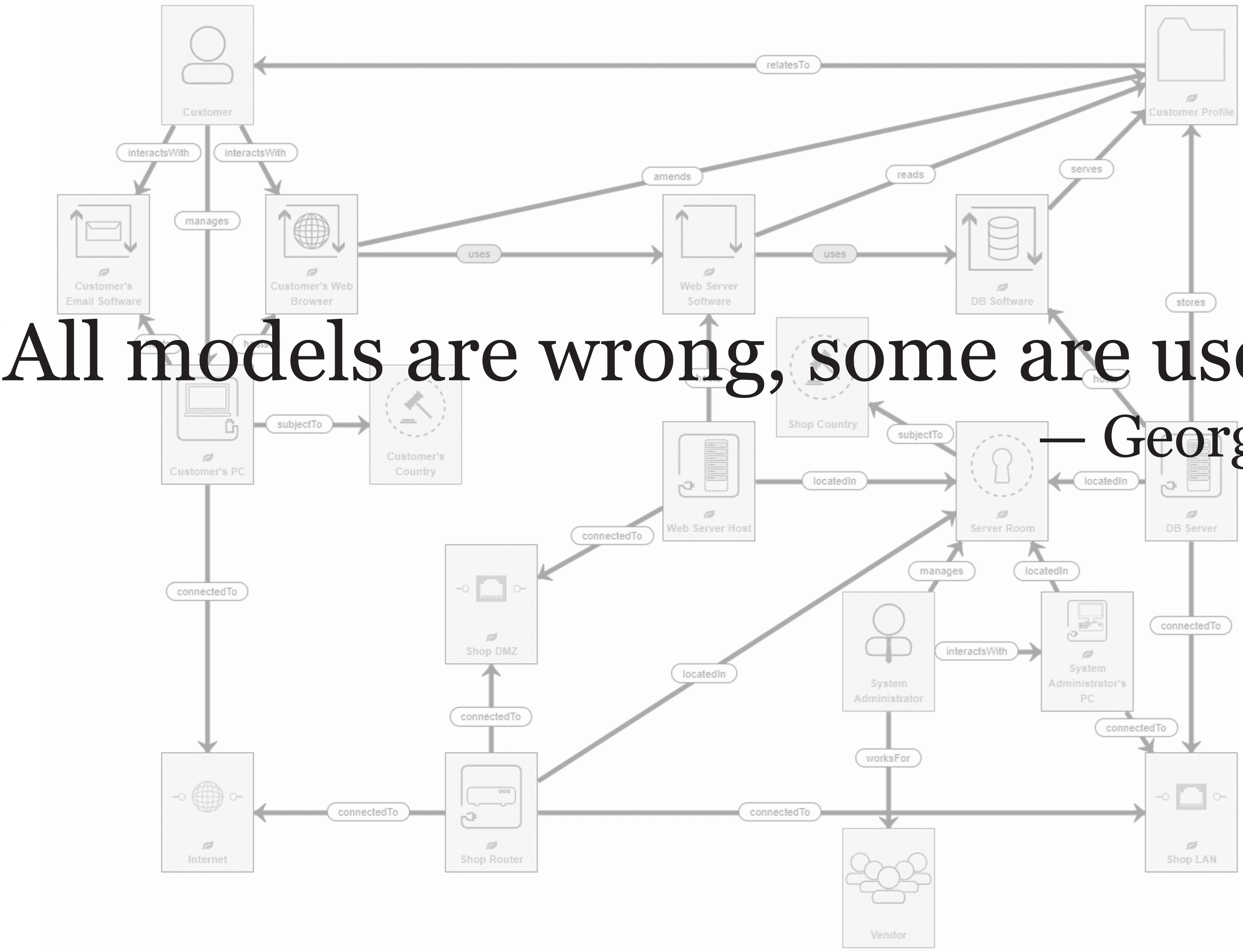
Output results
Integrating with other systems

History

The current tool builds on software initially created in 2016 but builds on research dating back to 2008.

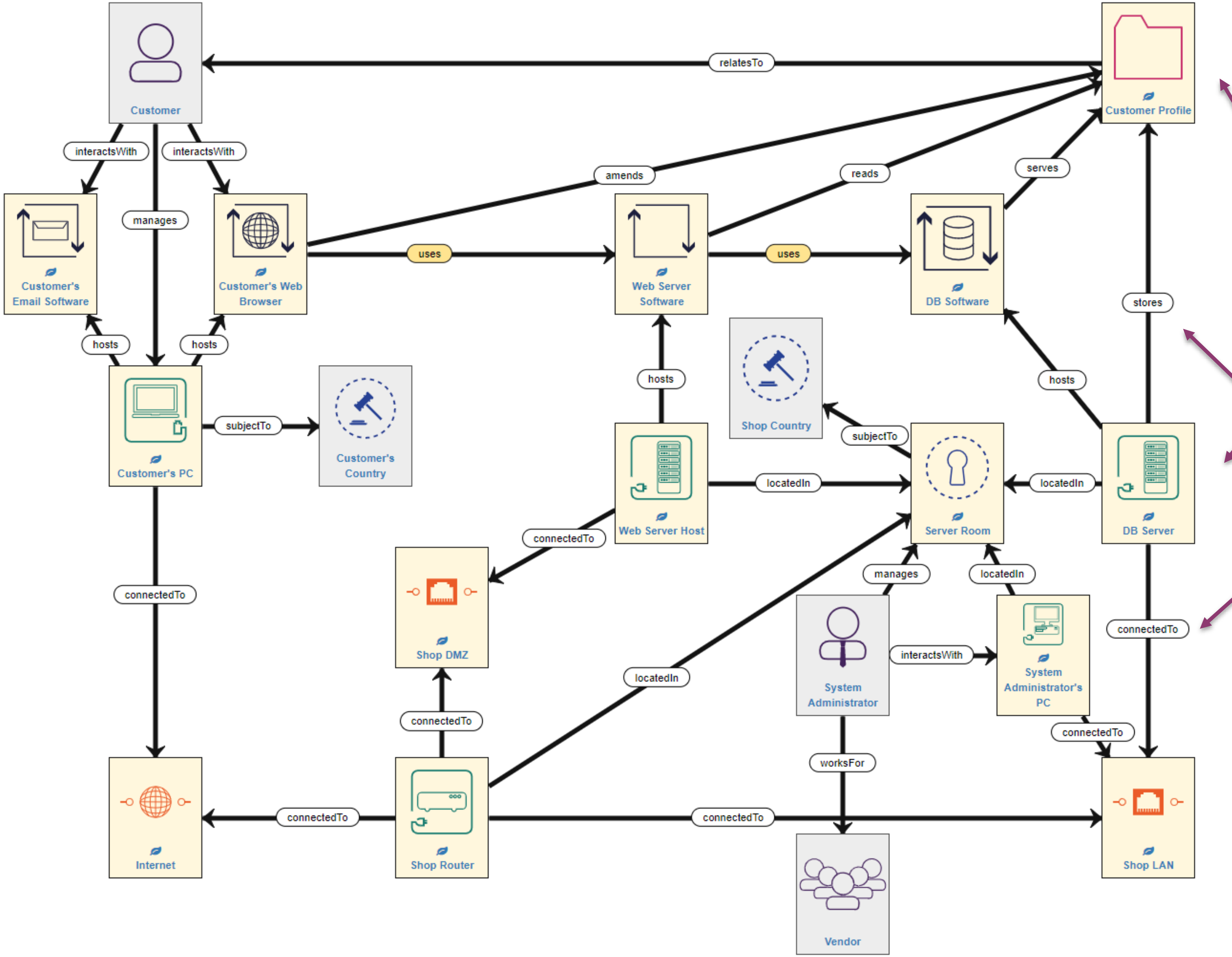


SERSCIS	Semantic modelling of trustworthiness of airport processes
OPTET	Understanding trust in socio-technical systems
5G-ENSURE	Modelling trust in 5G networks
ASSURED	Application to health data systems (NHS)
SHiELD	Modelling risk of cross-border health exchange
RestASSURED	Modelling risk in cloud systems
EFPF	Application of SSM in federated factories
ZDMP	Application of SSM in Industry 4.0
ProTego	Development of operational risk assessment (healthcare)
Data Market Services	Supporting risk assessments with e-learning course
CyberASAP 1	Exploring commercialisation opportunities
CyberASAP 2	Creating market analysis, value proposition, and demo
FogProtect	Development of operational risk assessment (fog computing)
CyberKit4SME	Simplifying the use of the SSM for use by SMEs
SPYDERISK	Creating a proof of concept
PRIAM	Modelling federation and data privacy



“All models are wrong, some are useful”

— George Box



Assets

Relations

The SSM models socio-technical systems using many assets types along with detailed relationships. A detailed model gives a precise risk analysis.

Humans and their interactions with information systems must be modelled as they are both a source of threats and are impacted by security controls and system failures.

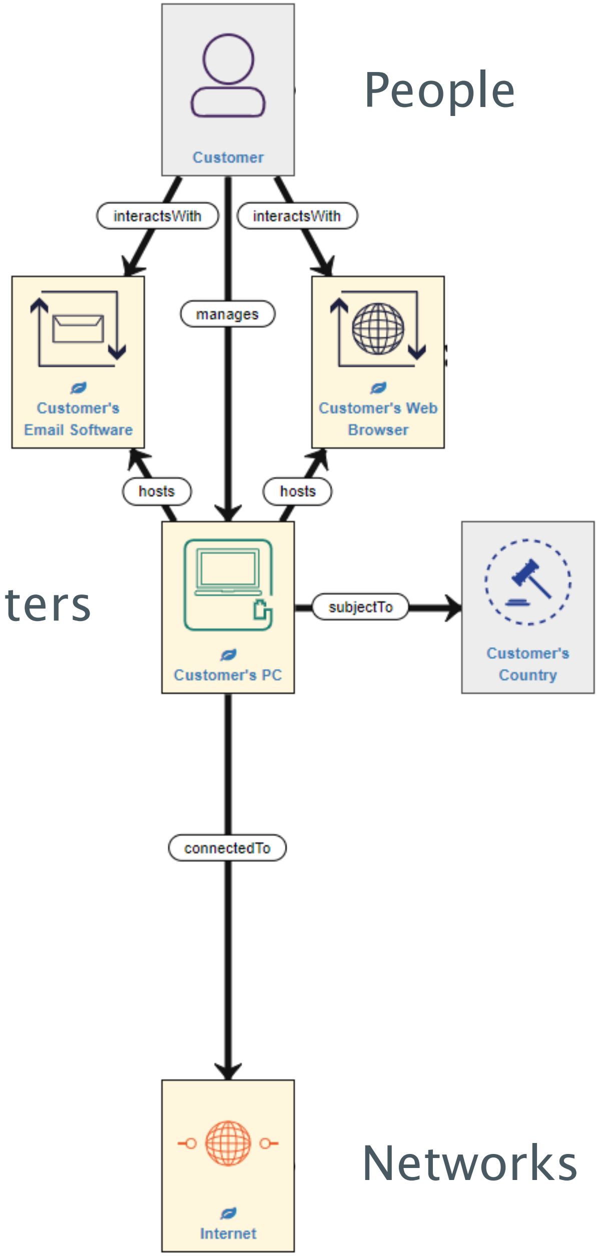
People

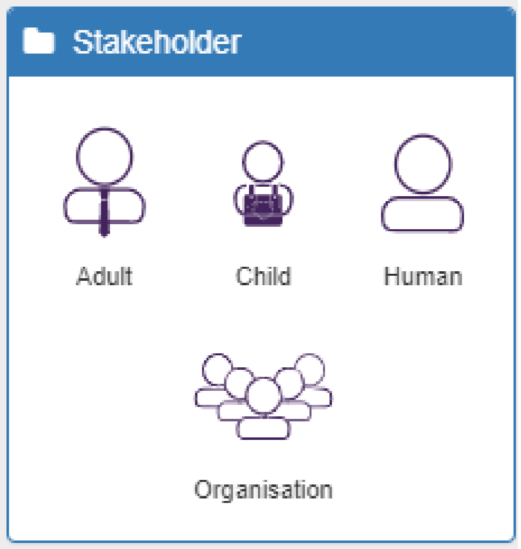
Software processes, sometimes specialised

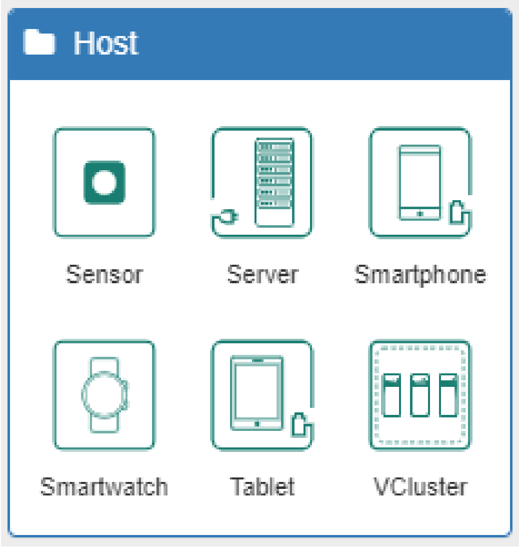
Computers

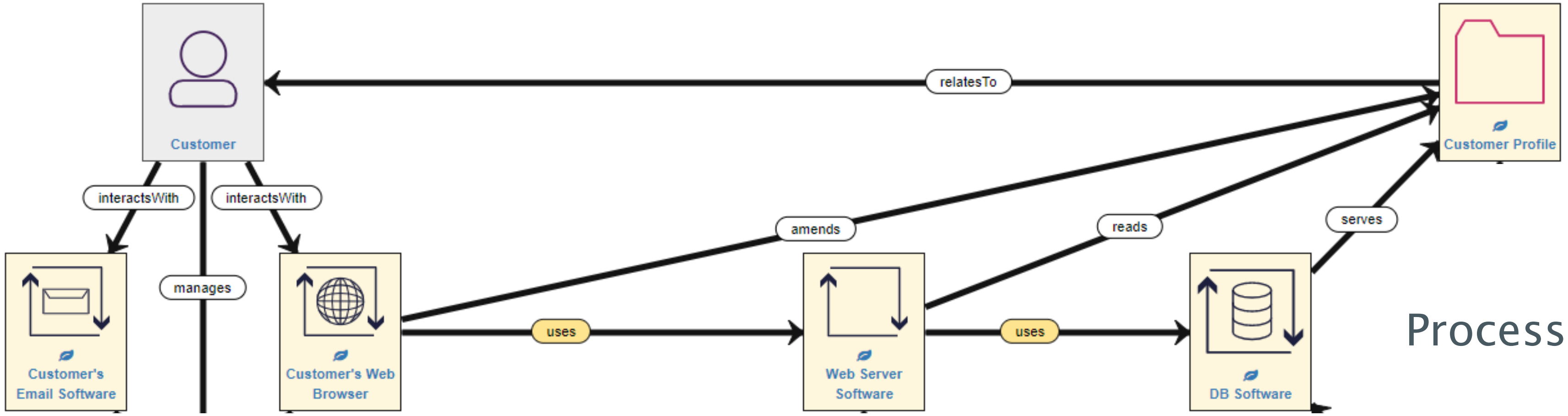
Legal jurisdictions

Networks









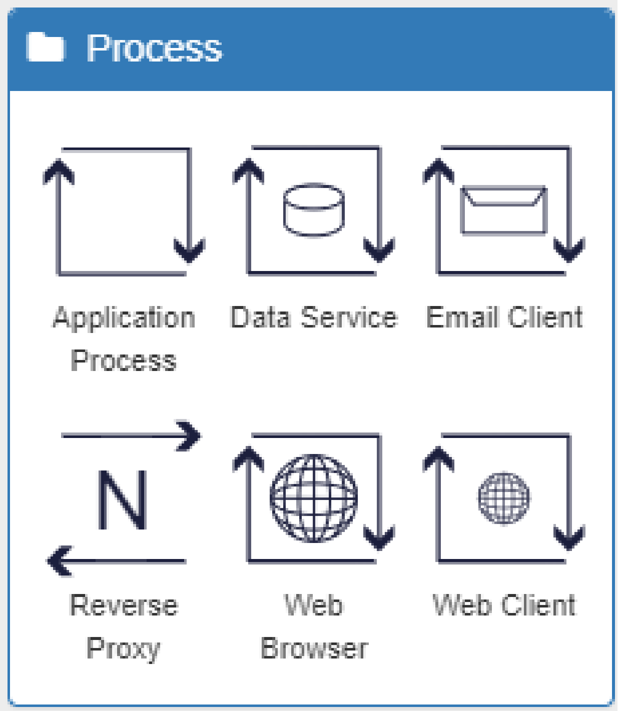
Data “relating to” a human makes it personal data

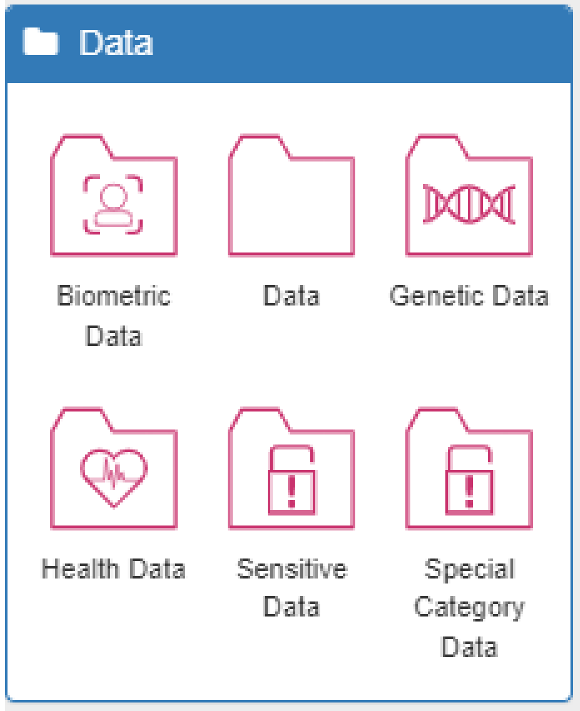
Process flows

The model of data and software process is detailed.

From this the SSM can work out what processes data can access data in a system and therefore where it may be vulnerable.

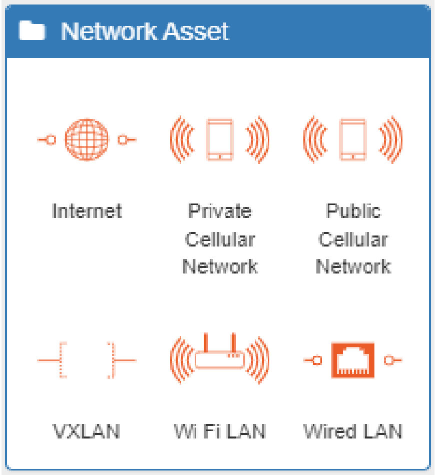
There are several specialised data types to take into account the sensitivity of the data and understand regulatory compliance.

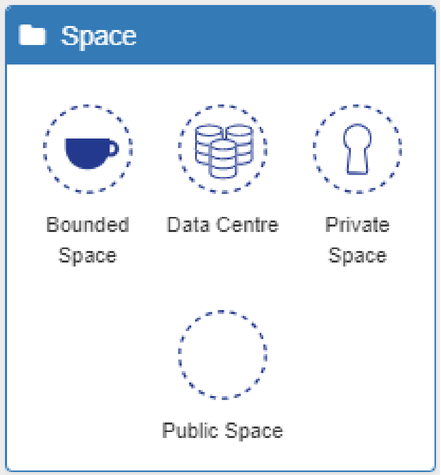


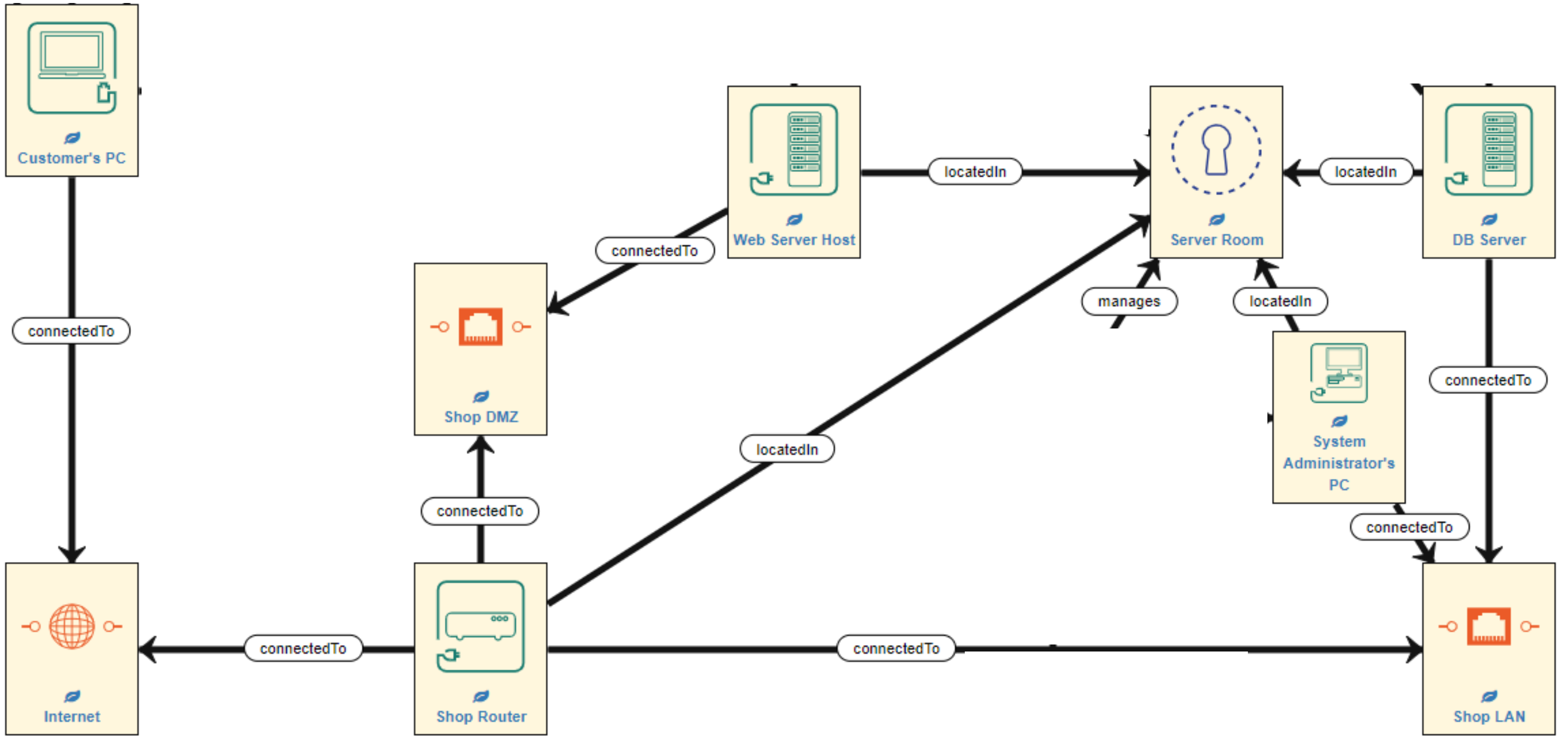


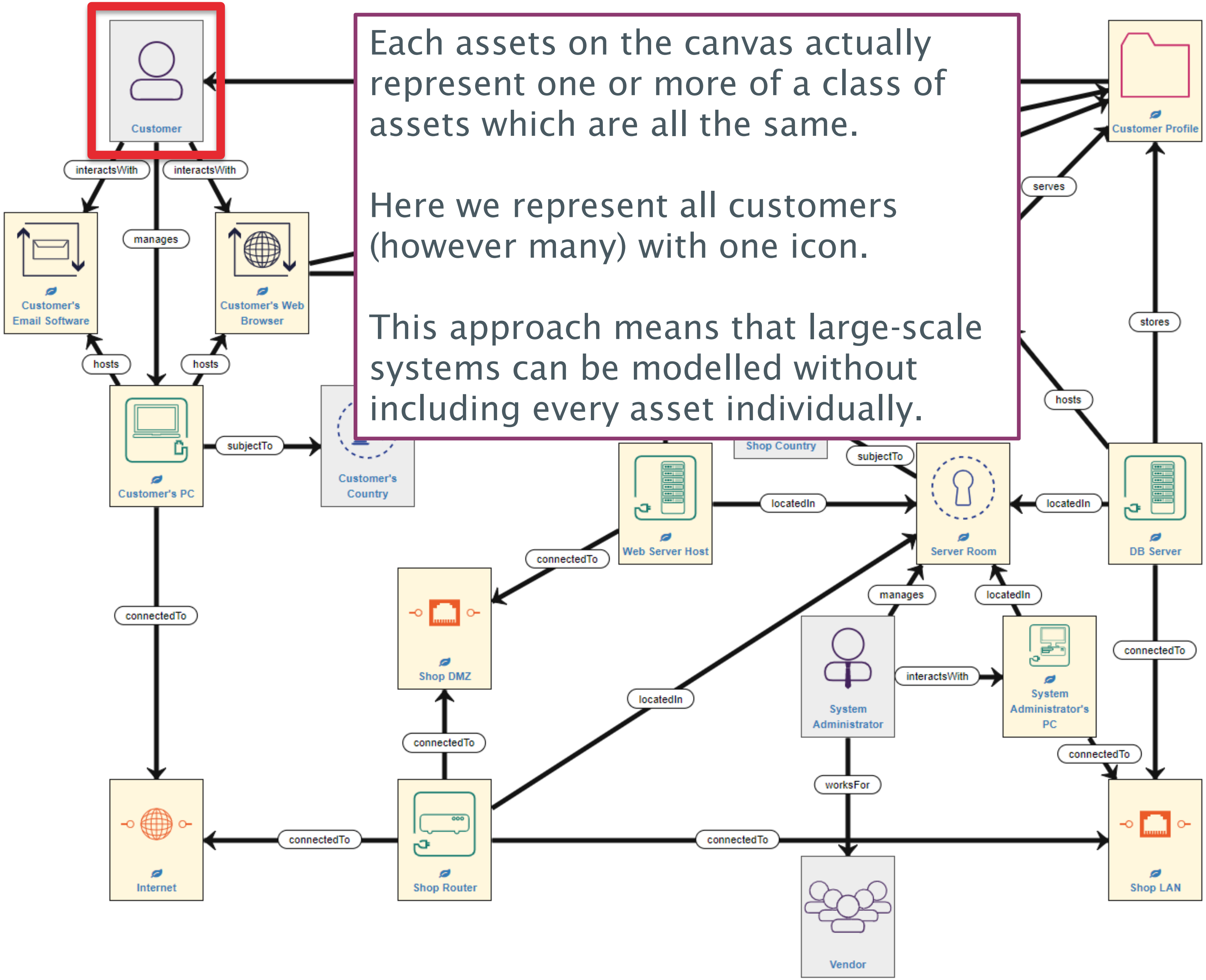
The network layer of the model shows the hosts and network connectivity. Virtual hosts and networks are also modelled.

Physical locations of assets are also modelled. A computer placed in a public café will be more at risk than one in a locked server room.









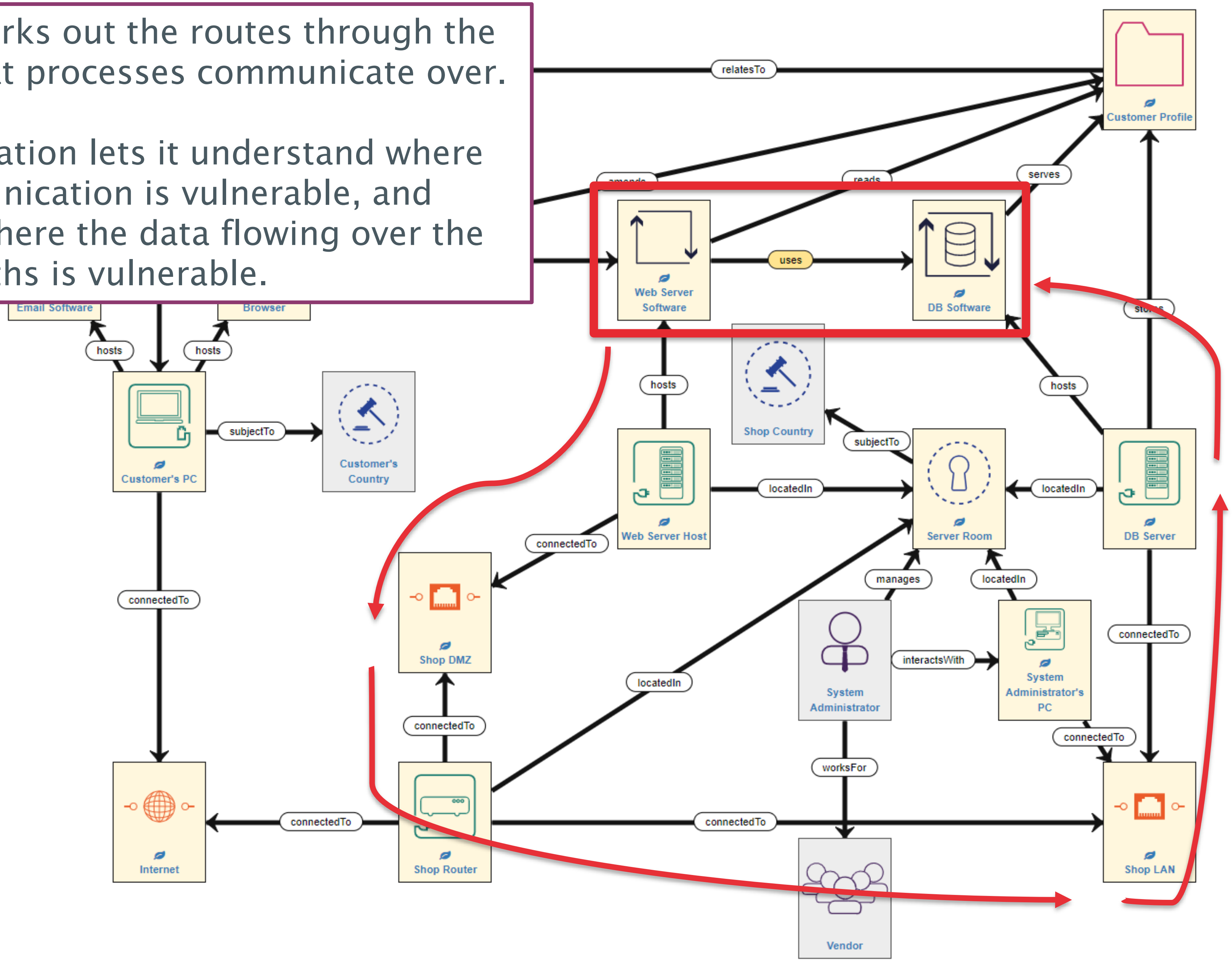
Each assets on the canvas actually represent one or more of a class of assets which are all the same.

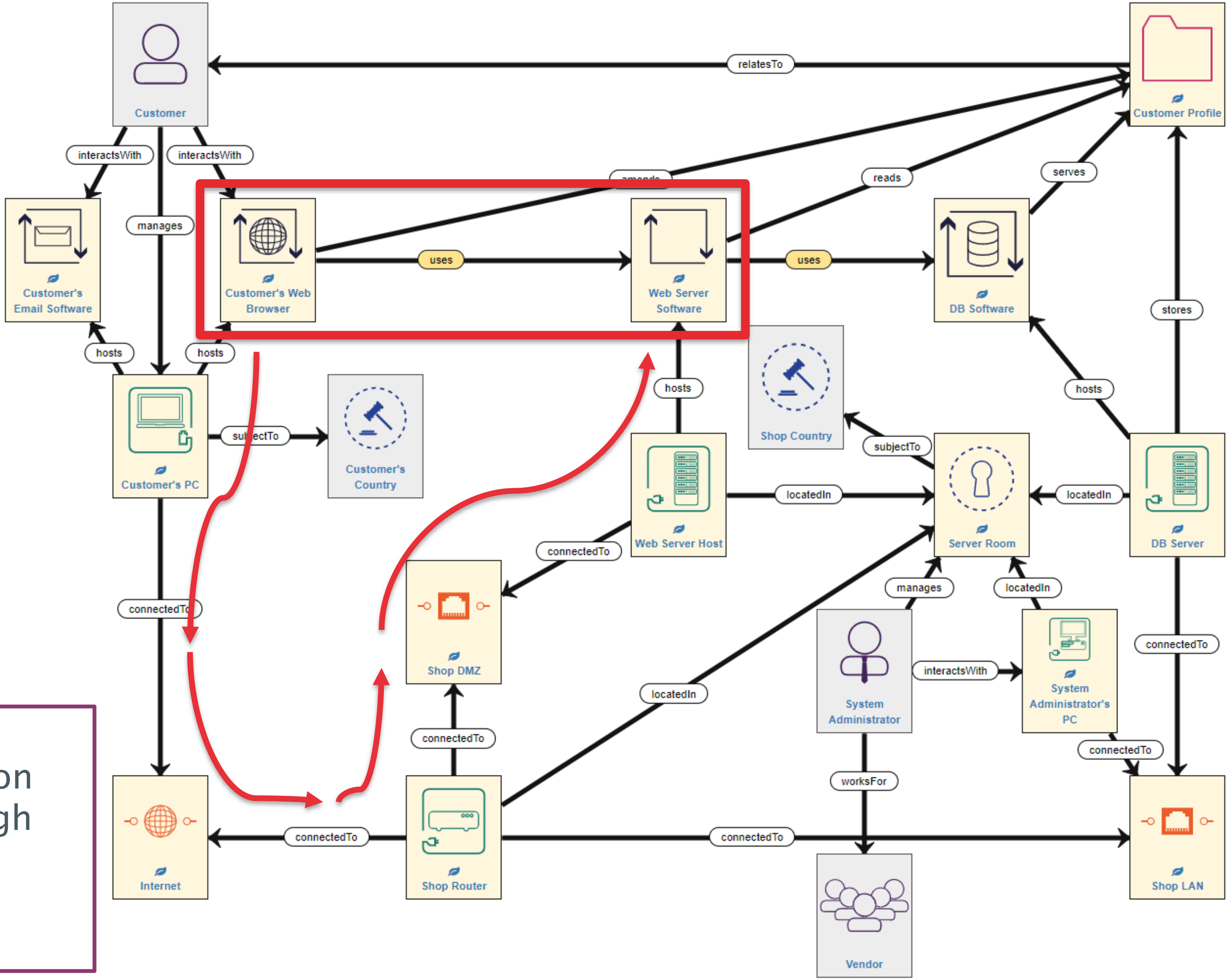
Here we represent all customers (however many) with one icon.

This approach means that large-scale systems can be modelled without including every asset individually.

The SSM works out the routes through the network that processes communicate over.

This information lets it understand where that communication is vulnerable, and therefore where the data flowing over the network paths is vulnerable.





This communication passes through the untrusted internet so is more at risk

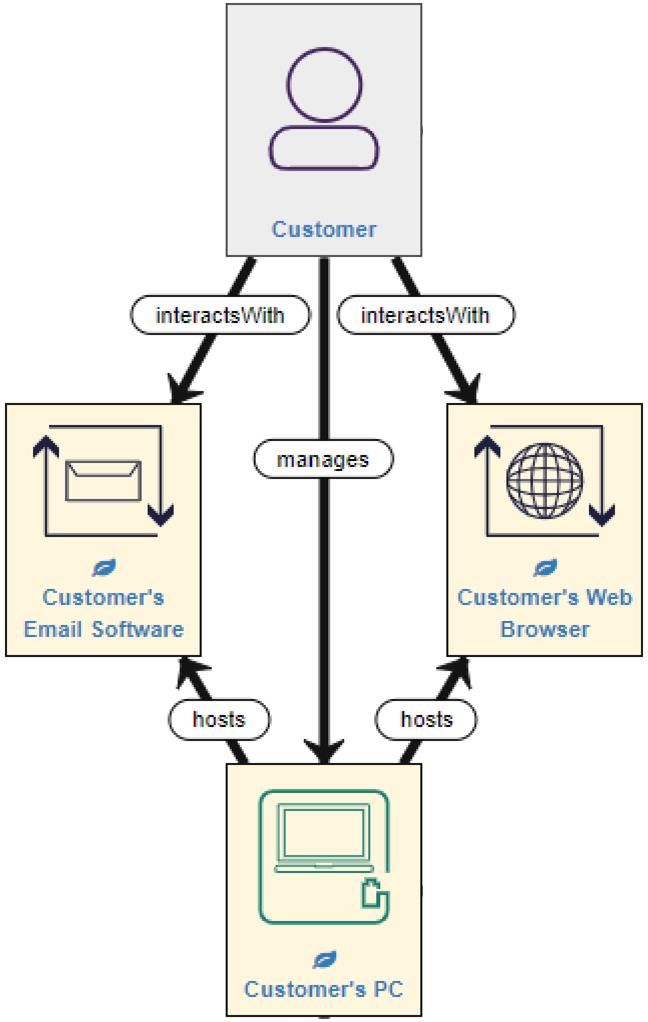
Threats to a System

> “A threat has the **potential** to cause harm to assets such as information, processes and systems and therefore organizations. Threats may be of **natural** or **human** origin, and could be **accidental** or **deliberate**.”
>
> — ISO 27005

- Natural, accidental threats include:
  - Hardware failures
  - Software bugs
- Human threats include:
  - Deliberate: malicious attackers
  - Accidental: people making mistakes
- We need to mitigate the high risk threats: those with risky consequences.
- The SSM has a knowledgebase of generic, fine-grained threats along with appropriate security controls that mitigate the threats.

Threat Discovery

- The SSM analyses the system model to find patterns of assets, relations and security controls that indicate the presence of threats.
- The threat patterns may include the data flows, network paths, etc, that it finds in the model.
- The threats are generic: regular updates are not required.
- All threats are considered at once: there is no need to define the attacker or attack point.
- E.g. the pattern shown here of a person using email and a web browser on the same PC indicates that a phishing threat exists.



Threat Coverage

Access and Control Privileges
Situations where an untrustworthy agent with certain privileges can gain access to further privileges, related to resource access and control

Exploiting Vulnerable Software
Situations where an attacker can cause execution of vulnerable code and thereby gain temporary use of privileges

Non-Malicious Threats
The effect of accidents and unintentional errors that could cause problems without provocation by malicious attackers

Insider Attacks
Situations where a legitimate user or organisational stakeholder performs malicious actions

Exploitation of Stolen Devices
Actions an attacker can take once physical theft has occurred

Other Malicious Attacks
Situations where a malicious attacker exploits a weakness other than a software vulnerability

Compliance Threats
Breaches of regulations, best practice guidelines, etc

Regulatory Compliance

- Non-compliance with regulation (e.g. GDPR) or best practice is modelled as a “threat”.
- These compliance threats are special in that they do not have a likelihood (or consequent risk): the system is compliant or not compliant.
- Personal data is indicated by data sets having the link “related to” to humans.
- Various specialised data types are modelled which link to different GDPR articles.
- Jurisdictions can be modelled which means cross-border data transfer can be inferred.
- Controls to bring a system into compliance include specifying policies such as gaining user consent or other lawful basis.

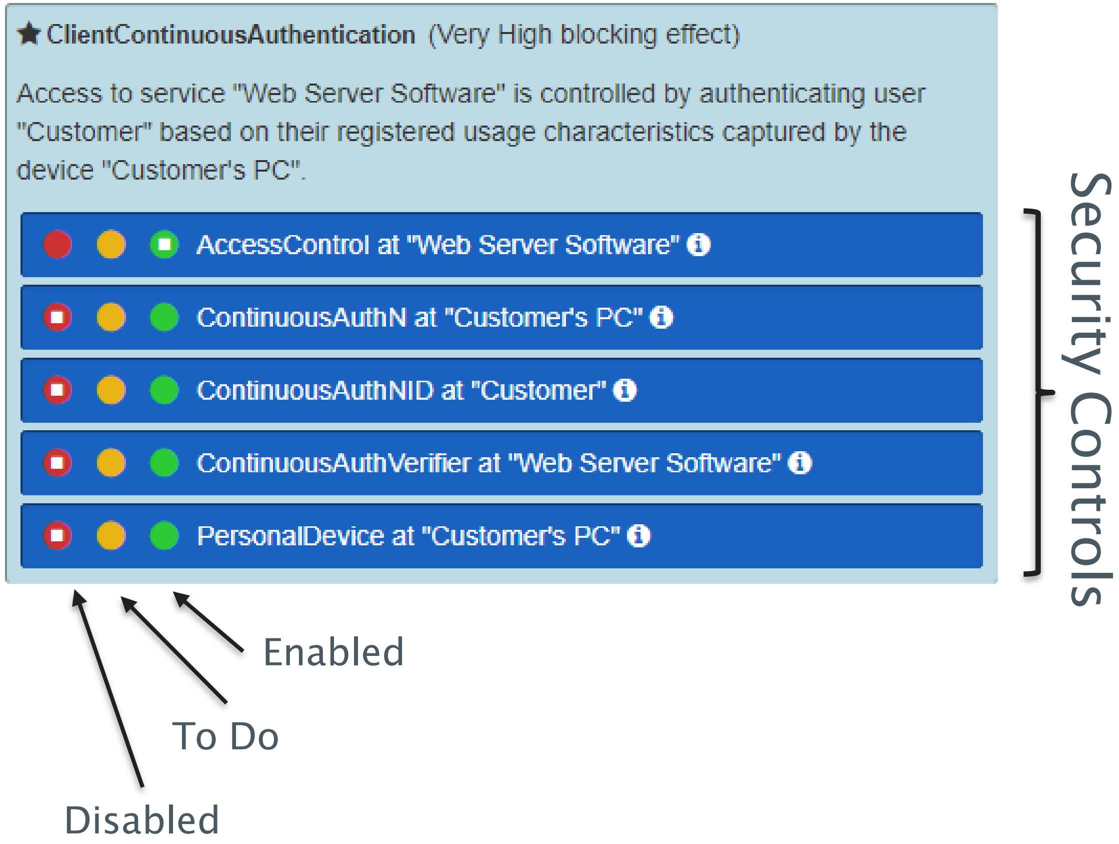
Threat Consequences

- The SSM models the risk of the standard “CIA” consequences for data:
  - Loss of **C**onfidentiality: access by an unauthorised party
  - Loss of **I**ntegrity: alteration (accidentally or deliberately) by an unauthorised or dysfunctional process
    - Loss of Authenticity: special case in which the alteration is malicious and designed to subvert a recipient (another asset) causing it to participate in malicious action.
  - Loss of **A**vailability: the data has been (accidentally or deliberately) deleted or otherwise rendered inaccessible (e.g. by encryption)
- Other asset types also have appropriate properties, for instance:
  - Software processes: loss of availability, malware infection, being overloaded
  - Spaces: physical intrusion
  - Hosts (e.g. servers): loss of availability, loss of control, theft

Threat Treatments or Mitigations

- The SSM knowledgebase includes ways of mitigating the threats.
  - For some threats there is no mitigation.
  - For others there are several options.
- Each threat treatment has an “effectiveness”: some are better than others.
- A threat treatment requires one or more security controls to be put in place.
  - E.g. Continuous client authentication requires controls at the website, the PC and involvement of the user themselves.

Example Threat Treatment



★ **ClientContinuousAuthentication** (Very High blocking effect)

Access to service "Web Server Software" is controlled by authenticating user "Customer" based on their registered usage characteristics captured by the device "Customer's PC".

- ● ● ● AccessControl at "Web Server Software" ℹ
- ● ● ● ContinuousAuthN at "Customer's PC" ℹ
- ● ● ● ContinuousAuthNID at "Customer" ℹ
- ● ● ● ContinuousAuthVerifier at "Web Server Software" ℹ
- ● ● ● PersonalDevice at "Customer's PC" ℹ

Threat Treatment Coverage

Organisational measures
Staff screening, training, policies

Physical Security
Physical locks & keys, chip & PIN, biometrics, ID checks

Service Security
TLS, AuthN, passwords, strong password, OTP, SMS codes, X.509, etc

Software Security
Software testing, pen testing, patching, device certification

Data Security
Encryption of data flows or stored copies; replicated storage

Network Security
Network access control (encryption, network AuthN) and routing restrictions

Client Security
Spam filtering, passwords

Device Security
Controlling direct access to devices; preventing alteration of software on devices

Resource Management
Elastic hosting, process prioritisation

User Intervention

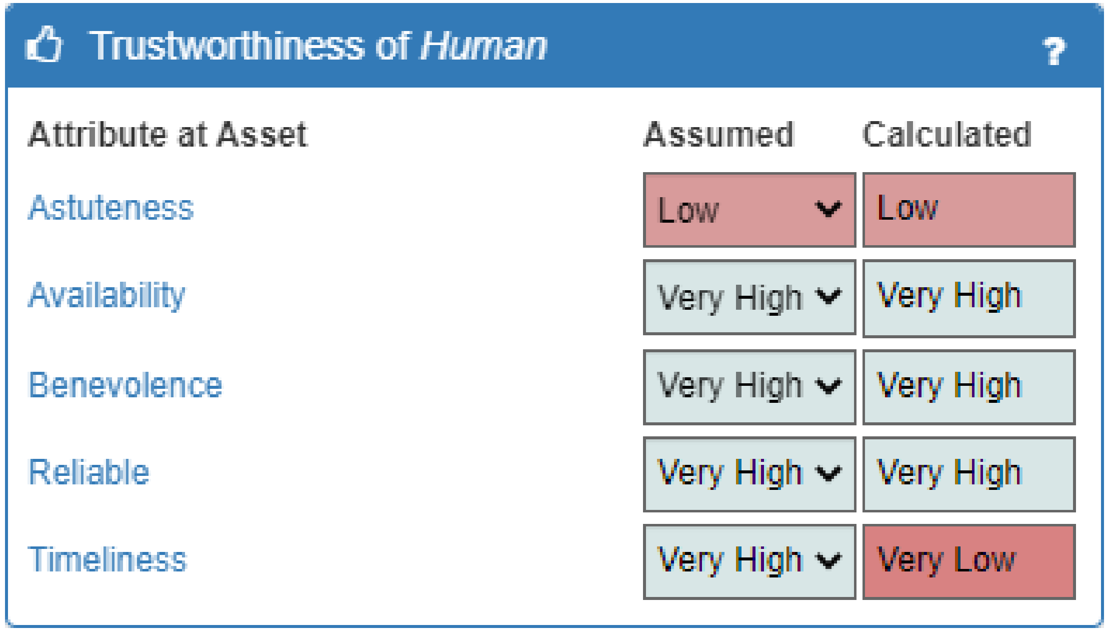
System Environment and State

- The system model describes how the system is intended to operate, with no attacker or problem explicitly present.
- All the assets have various “trustworthiness” parameters which configure their behaviour in a variety of ways.
- With these parameters the SSM models:
  - The external environment that the system exists in
  - The inherent likelihood of assets failing in different ways
  - How threats propagate through the inter-connected assets of the system making failures more likely

Trustworthiness of Assets

“How likely it is that an asset will avoid, or resist being involved in, a threat”

— not in any standard!



Trustworthiness of *Human*

Attribute at Asset	Assumed	Calculated
Astuteness	Low	Low
Availability	Very High	Very High
Benevolence	Very High	Very High
Reliable	Very High	Very High
Timeliness	Very High	Very Low

Ability to spot e.g. a phishing attack

How free they are from bad intentions
Low benevolence == “malicious”

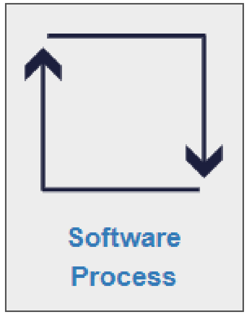
Has up to date inputs to perform
their role in the system

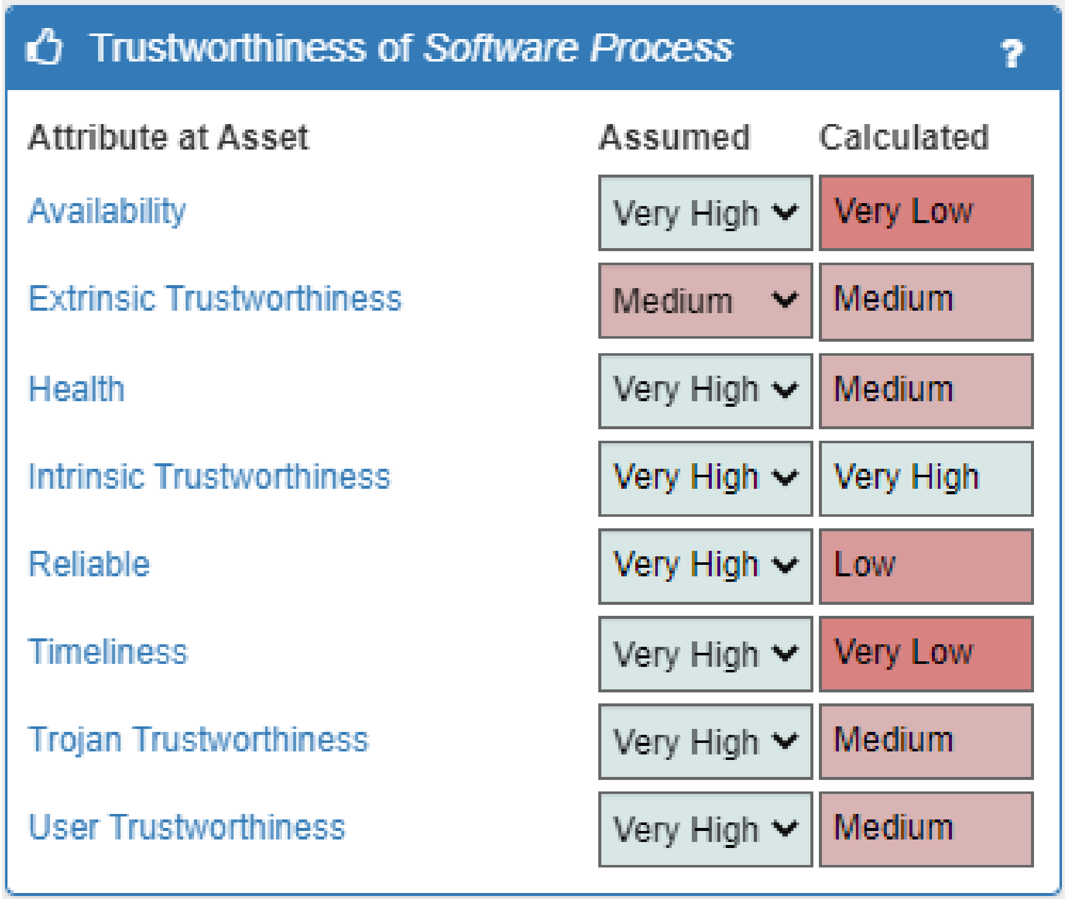
Trustworthiness of Assets

Free from software vulnerabilities that may be discovered by hackers

Free from bugs that would cause it to crash without provocation

Trustworthiness of users who have the rights of this process on the host




Trustworthiness of *Software Process*

Attribute at Asset	Assumed	Calculated
Availability	Very High	Very Low
Extrinsic Trustworthiness	Medium	Medium
Health	Very High	Medium
Intrinsic Trustworthiness	Very High	Very High
Reliable	Very High	Low
Timeliness	Very High	Very Low
Trojan Trustworthiness	Very High	Medium
User Trustworthiness	Very High	Medium

Risk, Impact, Likelihood

		Calculated **Likelihood**				
		Very Low	Low	Medium	High	Very High
Specified **Impact**	Very Low	Very Low	Very Low	Very Low	Low	Low
	Low	Very Low	Very Low	Low	Low	Medium
	Medium	Very Low	Low	Medium	High	High
	High	Low	Medium	High	Very High	Very High
	Very High	Low	Medium	High	Very High	Very High

- Calculated risk = (specified business impact) × (calculated likelihood)
- The impact of an adverse effect varies according to the asset, but generally only needs to be set on the primary assets because the SSM works out any inter-dependencies:
  - Loss of confidentiality of customer profile data ⇒ high impact
  - Loss of confidentiality of data on a public website ⇒ very low impact
- Likelihoods are calculated from the configured asset trustworthiness, the adverse effects of threats, and the presence of security controls.
- Sometimes we say A “causes” B: we mean A is the reason B is as likely as it is.

Threat Propagation

This is a unique and crucial feature of the SSM.
It models how the consequence of one threat makes other threats more likely.

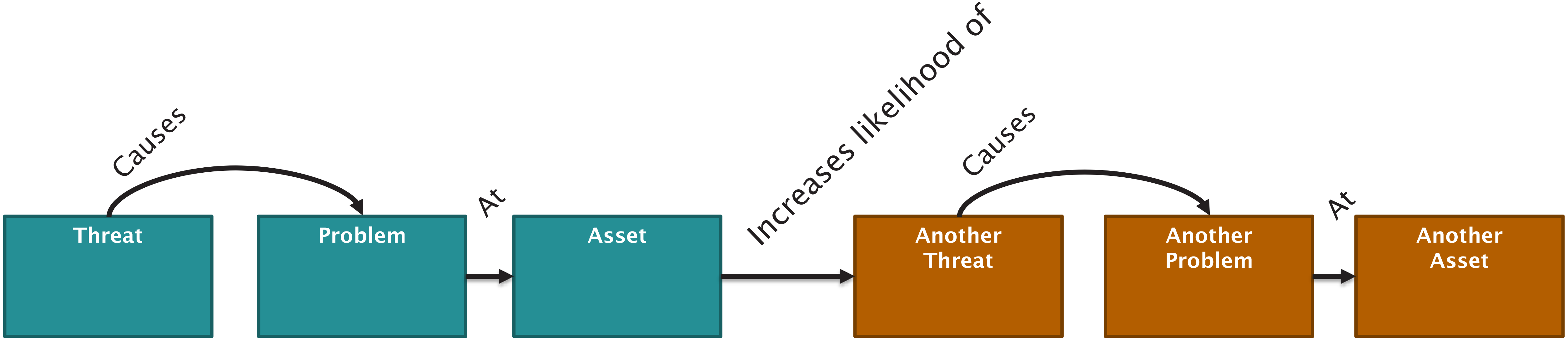
Attack Path

- It is rare that a malicious attack achieves its target in a single step.
- The SSM's model of threat propagation will find and simulate deliberate attack steps through a system.
  - E.g. lateral movement through a system.
  - E.g. escalation of privileges followed by reading data within one host.

Secondary Threat Cascade

- The threat propagation method means automatic "secondary threats" are considered
  - E.g. if a server is disrupted and ceases to function then the SSM knows that any hosted data will also lose availability.
- This means that the user only needs to consider the impact of threats on the primary assets (e.g. the data, not the server).

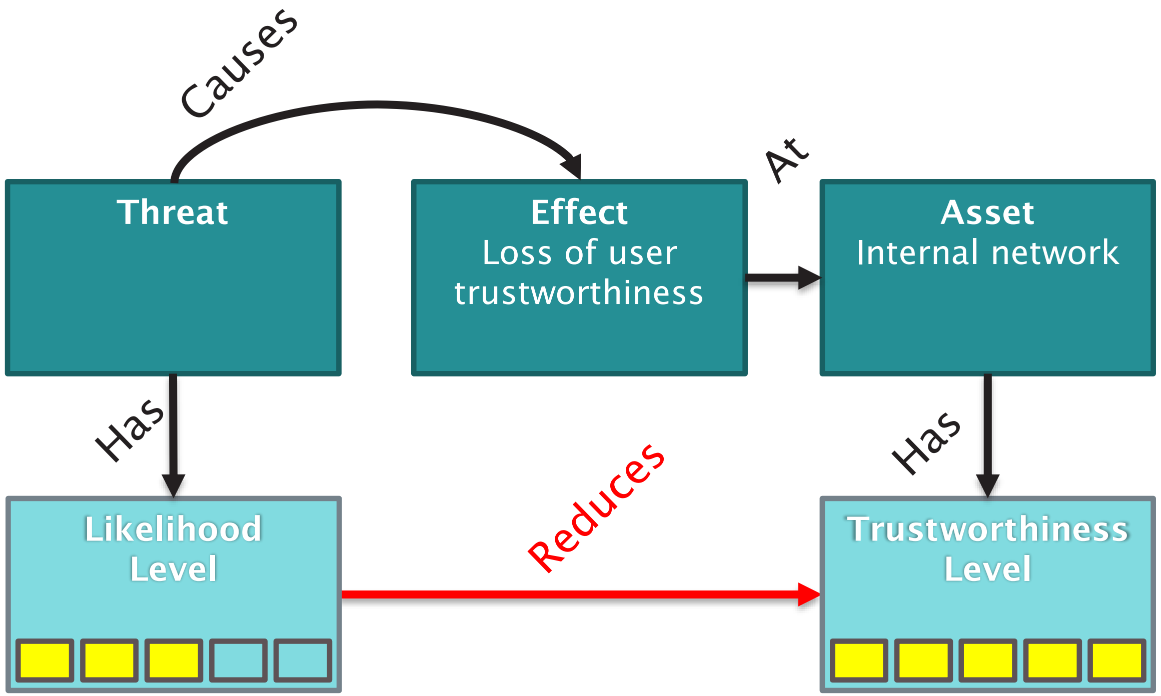
Threat Propagation



Threat Propagation

Threat
an attack on an external firewall

Reduction in trustworthiness in the users of an internal network



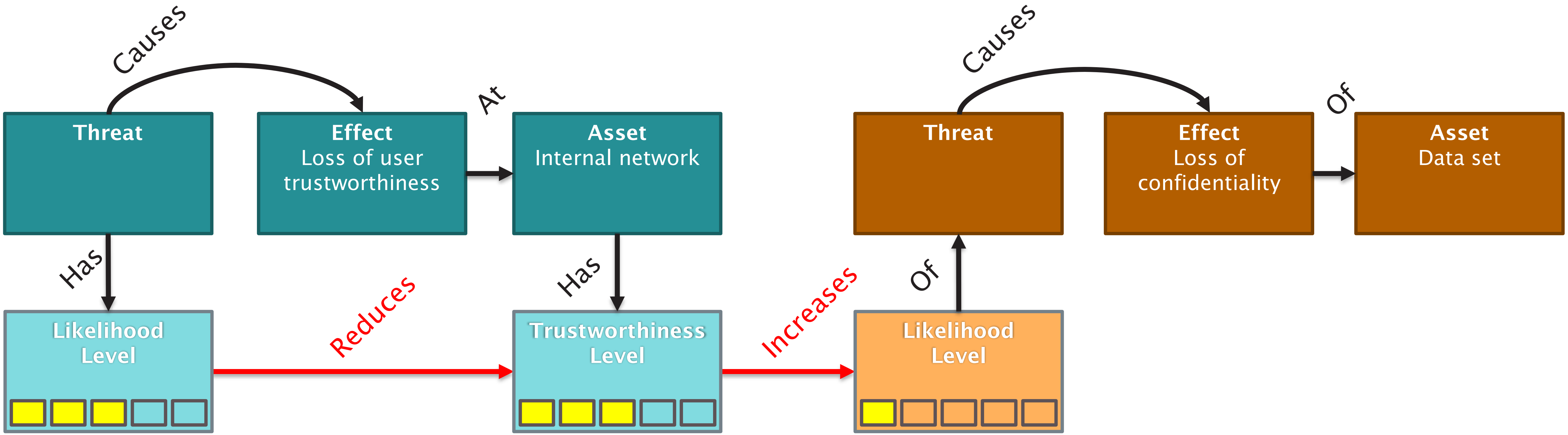
Threat Propagation

Threat
an attack on an external firewall

Reduction in trustworthiness in the users of an internal network

Threat
an internal data flow being read

Loss of confidentiality in a data set



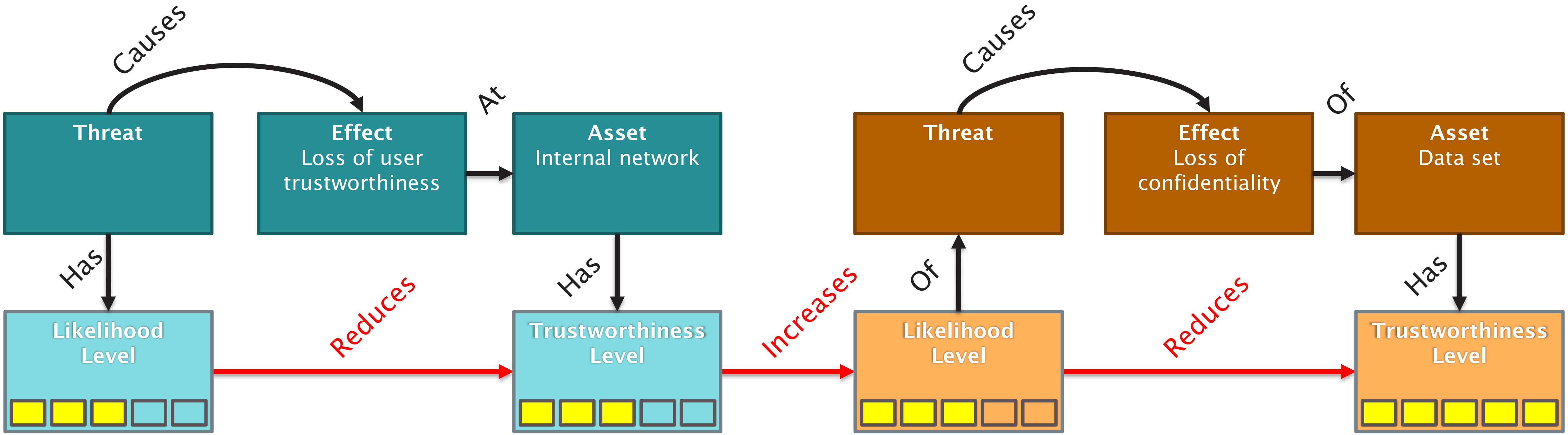
Threat Propagation

Threat
an attack on an external firewall

Reduction in trustworthiness in the users of an internal network

Threat
an internal data flow being read

Loss of confidentiality in a data set



Threat

Effect
Loss of user trustworthiness

Asset
Internal network

Likelihood Level

Trustworthiness Level

Threat

Effect
Loss of confidentiality

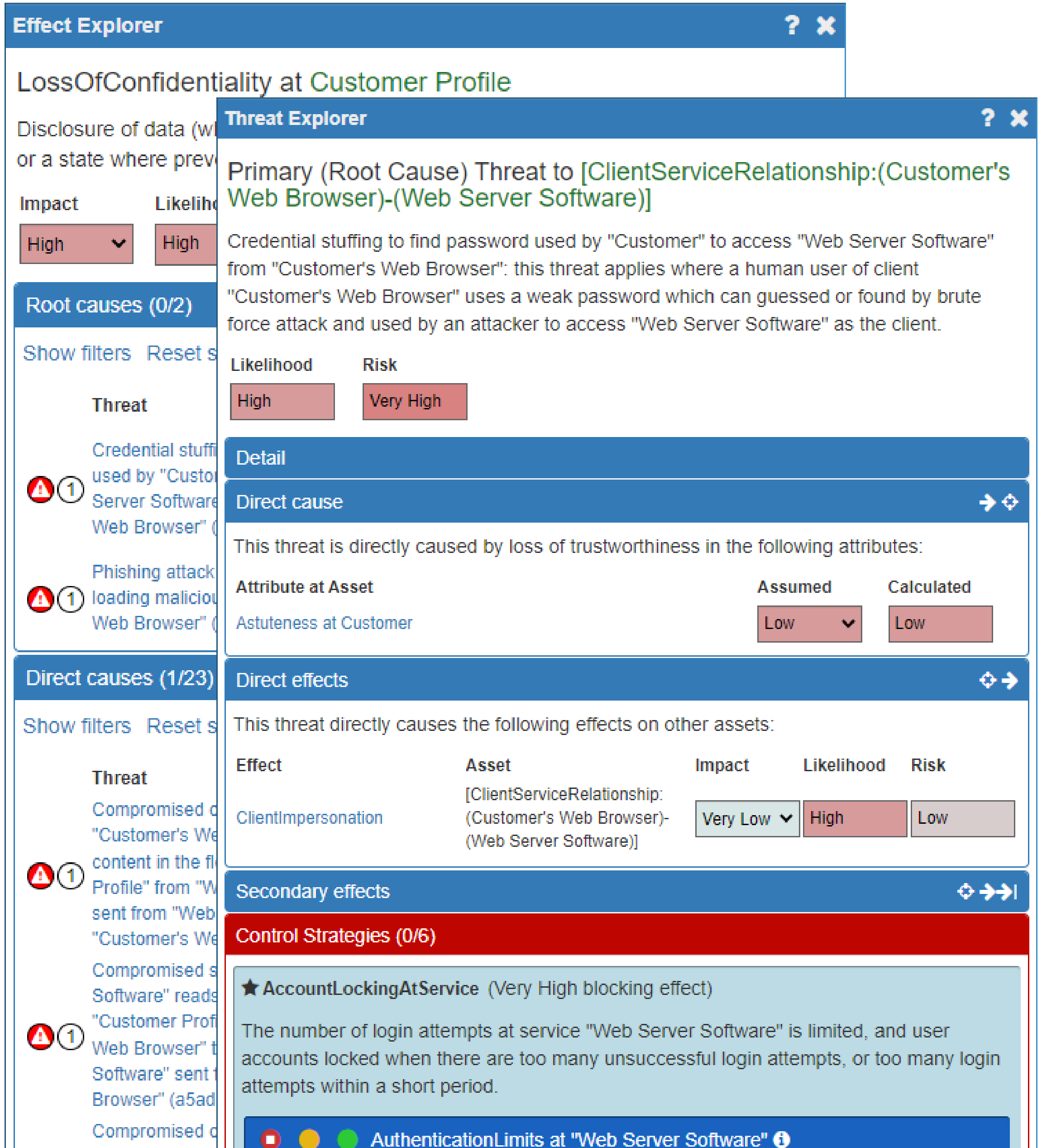
Asset
Data set

Likelihood Level

Trustworthiness Level

Threat Paths

- The threat propagation model does not create a simple linear path.
- Threats and their effects combine and branch:
  - Threats can need more than one cause to be present/likely
  - The effect of a threat can cause more than one other threat
- Determining where best to put the security controls is therefore not easy.
- The SSM includes exploration tools to navigate the paths.



LossOfConfidentiality at Customer Profile

Disclosure of data (wh
or a state where prev

Impact: High
Likelih: High

Threat

Credential stuffi
used by "Custor
Server Software
Web Browser" (

Phishing attack
loading maliciou
Web Browser" (

Threat

Compromised c
"Customer's We
content in the fi
Profile" from "W
sent from "Web
"Customer's We

Compromised s
Software" reads
"Customer Profi
Web Browser" t
Software" sent t
Browser" (a5ad

Compromised c

Primary (Root Cause) Threat to [ClientServiceRelationship:(Customer's Web Browser)-(Web Server Software)]

Credential stuffing to find password used by "Customer" to access "Web Server Software" from "Customer's Web Browser": this threat applies where a human user of client "Customer's Web Browser" uses a weak password which can guessed or found by brute force attack and used by an attacker to access "Web Server Software" as the client.

Likelihood	Risk
High	Very High

This threat is directly caused by loss of trustworthiness in the following attributes:

Attribute at Asset	Assumed	Calculated
Astuteness at Customer	Low	Low

This threat directly causes the following effects on other assets:

Effect	Asset	Impact	Likelihood	Risk
ClientImpersonation	[ClientServiceRelationship:(Customer's Web Browser)-(Web Server Software)]	Very Low	High	Low

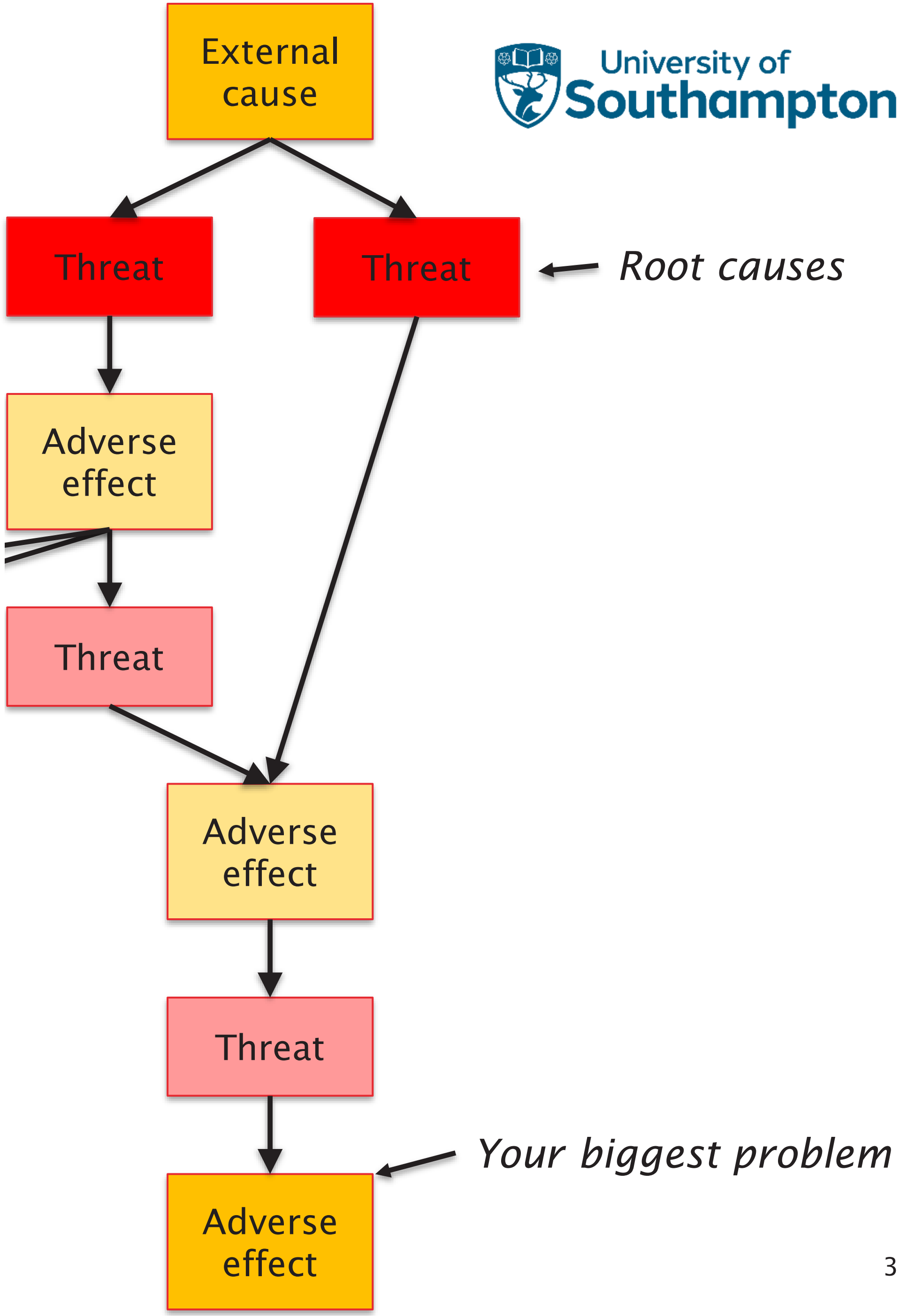
★ **AccountLockingAtService** (Very High blocking effect)

The number of login attempts at service "Web Server Software" is limited, and user accounts locked when there are too many unsuccessful login attempts, or too many login attempts within a short period.

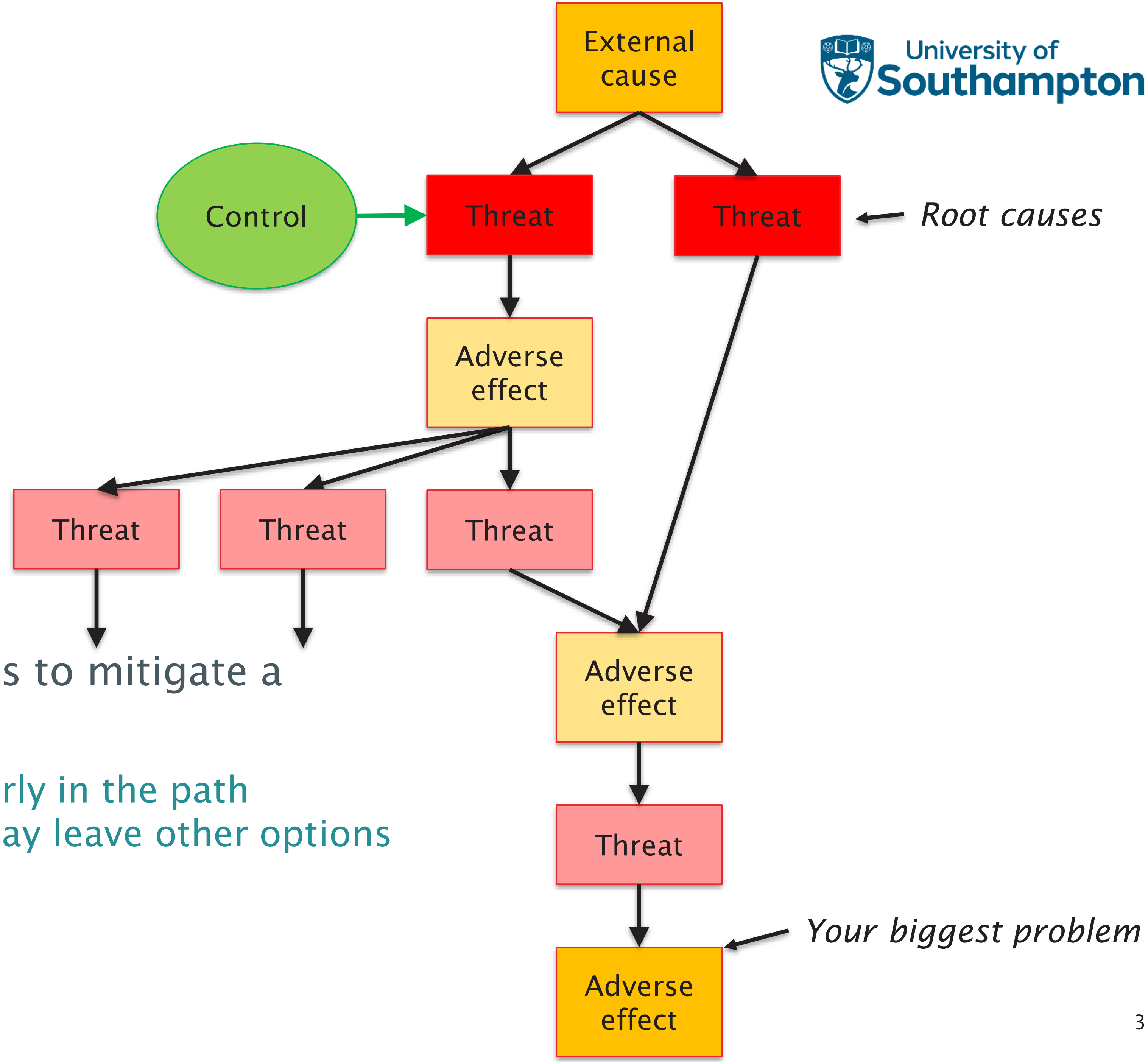
AuthenticationLimits at "Web Server Software"

Threat Paths

- The SSM's analysis shows the highest risk adverse effects: your biggest issues
  - E.g. loss of confidentiality in customer profile data
- As an analyst you want to know what has caused this risk (to be so likely) and therefore how to mitigate it
- There are often many options to mitigate a threat

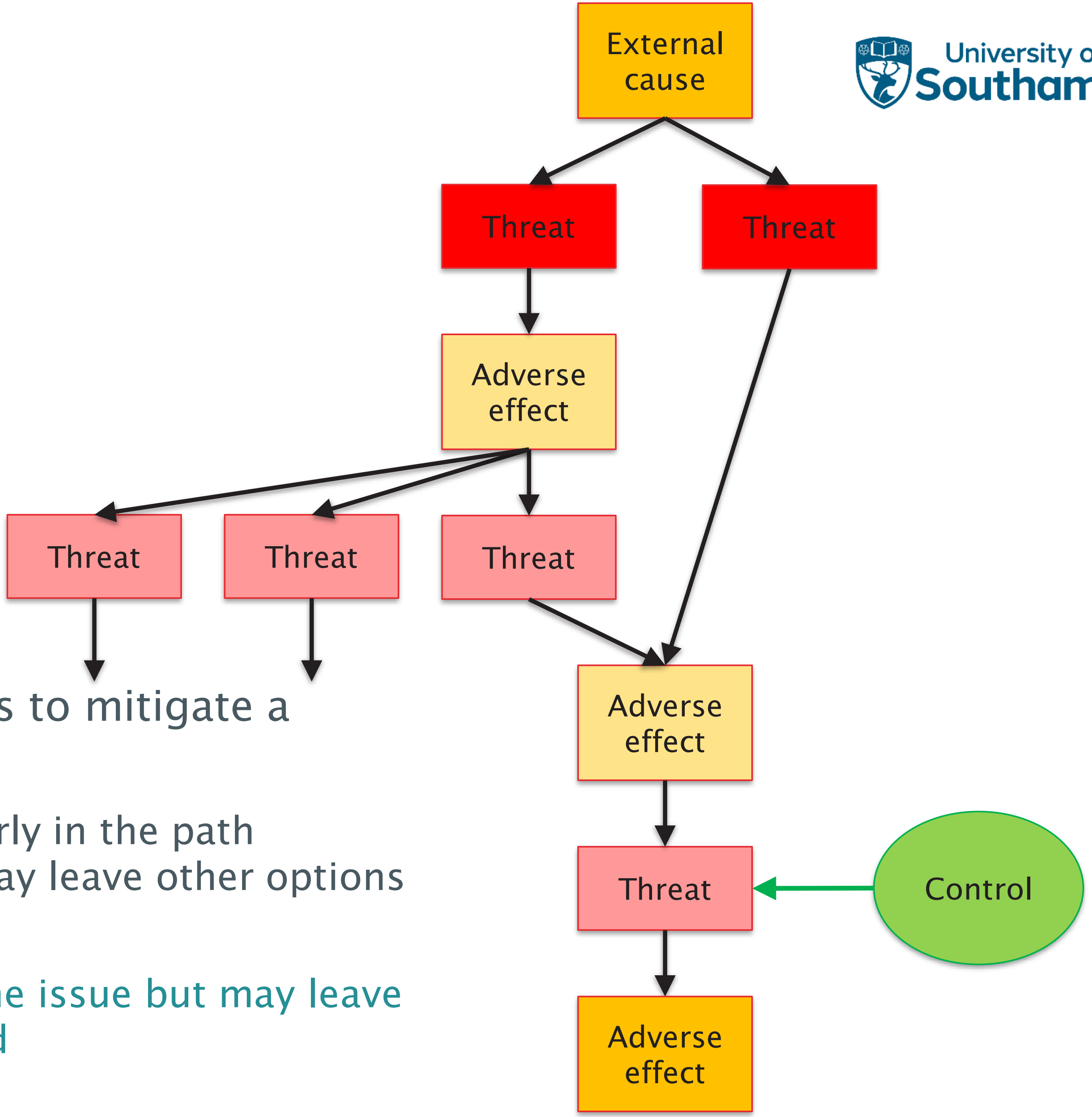


Threat Paths



- There are often many options to mitigate a threat
  - Putting a security control early in the path mitigates many paths but may leave other options for the attacker

Threat Paths



- There are often many options to mitigate a threat
  - Putting a security control early in the path mitigates many paths but may leave other options for the attacker
  - Putting it late will fix that one issue but may leave other problems unaddressed

Operating Modes

Security by Design

- Model the long term risk.
- Model a system before it is built and deployed.
- Model an existing system or proposed changes to it.
- Put in place recommended controls and procedures to secure it before problems arise.
- Do a “what if?” experiment.

Operational Risk Assessment

- Model the immediate risk.
- Based on knowledge of the current state of a live system.
- Configure the trustworthiness of software processes based on vulnerability scans, CVE database, etc.
- Receive recommendations suitable for immediate implementation.

Alternatives

	Whiteboard	securiCAD	ThreatModeler	IriusRisk	OWASP Threat Dragon	Microsoft Threat Modelling Tool	SSM
Semi-automated; Fast; Repeatable	×	✓	✓	✓	✓	✓	✓
Hosts	✓	✓	×	×	×	×	✓
Networks	✓	✓	×	×	×	×	✓
Software processes	✓	✓	✓	✓	✓	×	✓
Communication protocols	✓	✓	✓	✓	✓	✓	If necessary
Data	✓	✓	×	✓	×	×	✓
People	✓	✓	×	×	×	✓	✓
Physical spaces	✓	✓	×	×	×	×	✓
Legal jurisdictions	✓	×	×	×	×	×	✓
Software functions	×	×	×	✓	×	×	×
Business functions	✓	×	×	×	×	×	×
Trust boundaries	✓	×	×	✓	✓	✓	×
Data flow	✓	✓	×	✓	✓	✓	✓ (automatic)
Process flow	✓	×	✓	✓	×	×	✓
Asset relationships	✓	Basic	Basic	×	Basic	Basic	✓
Threat database	If expert	✓	✓	✓	×	✓	✓
Control database	If expert	✓	✓	✓	×	Comms only	✓
Calculated Risk	If expert	Fixed	Fixed	✓	×	×	✓ (ISO 27005)
Time to compromise	×	✓	×	×	×	×	×
Attacks considered	Some	Single	?	All	×	All	All
Attack path	If expert	✓	✓	×	×	×	✓
Report generation	Manual	Basic	✓	✓	×	Basic	Basic
Automated model building	×	AWS	×	Terraform	×	×	Research
Live status	×	×	×	×	×	×	Research
DevOps integration	×	×	✓	×	×	×	×

Current and Future Directions

- Operational risk assessment
  - Integration with vulnerability scanners etc along with support in the UI
  - Integration with Security Incident Event Management systems
- Attack path analysis
  - Development of visualisations to help users understand cause and effect
- Threat treatment recommendations
  - Using attack path analysis to recommend good mitigation options
- Model discovery
  - Using network scanner and cloud API data to semi-automate the model building
- GDPR compliance
  - Extending and updating the existing model
- General user interface and performance improvements
- Intelligence sharing along supply chains

Selected References

- (2021) Regulatory Compliance Modelling Using Risk Management Techniques https://doi.org/10.1109/AIIoT52608.2021.9454188
- (2021) Cybersecurity for SMEs: Introducing the Human Element into Socio-technical Cybersecurity Risk Assessment https://doi.org/10.5220/0010332902660274
- (2020) Systematic Risk Assessment of Cloud Computing Systems Using a Combined Model-based Approach https://doi.org/10.5220/0009342700530066
- (2019) Modelling compliance threats and security analysis of cross-border health data exchange https://doi.org/10.1007/978-3-030-32213-7_14
- (2018) Trust Modelling in 5G mobile networks https://doi.org/10.1145/3229616.3229621
- (2015) Trustworthy systems design using semantic risk modelling http://eprints.soton.ac.uk/id/eprint/383465
- (2013) A Novel Risk-based Approach for Online Community Management http://eprints.soton.ac.uk/id/eprint/354147
- (2013) Next generation community management: A proactive risk-based approach http://eprints.soton.ac.uk/id/eprint/354148

Summary

- The SSM automates much of an ISO 27005 risk assessment of socio-technical systems
  - People, places, networks, computers, data
  - Reliably, repeatedly, comprehensively
- The risk assessment takes into account the propagation of threats and their effects through the system
  - This technique is unique and crucial
- A wide range of threats are modelled, both cyber-security and compliance
- Physical, technical and policy-based security controls are recommended
- The software code will be open sourced in the near future
- Please contact us if you are interested in joining the community around this tool

The opinions expressed in this publication are those of the authors and do not necessarily reflect the views of the University of Southampton.

IT Innovation Centre, Building 32, Room 3001, Electronics and Computer Sciences, Faculty of Engineering and Physical Sciences, Highfield Campus, University of Southampton, SO17 1BJ