UNIVERSITY OF Southampton

comp6224 (2016)
week 8: Cyber Essentials

Vladimiro Sassone

Cyber Security Centre
University of Southampton

CyberSecuritySoton.org [w]

@CybSecSoton [fb & tw]

Project objectives: an academic study of

- typical SME networks
- common threats and vulnerabilities
- effectiveness of Cyber Essentials
- alternatives or extensions to Cyber Essentials

Project approach:

- develop models of typical SME networks
- use automatic analysis to determine number and status of threats in these networks

The scheme was developed by the UK Government and industry as a statement of basic controls that all organisations should implement to mitigate the risk from common cyber threats.

Focuses on SME, where there is no specialised security expert being hired.

Certification is awarded on the basis of a verified self-assessment.

Self assessment questionnaire of the organisation's implementation of the Cyber Essentials control and is approved by a senior executive such as the CEO.

This questionnaire is then verified by an independent Certification Body to assess whether an appropriate standard has been achieved, and certification can be awarded.

This option offers a basic level of assurance and can be achieved at low cost.

The assessment process is a ‘snap shot’ in time

New vulnerabilities are continually being identified.

It is recommended that organisations maintain the principles of the Scheme on an on-going basis and not just prepare for assessment.

As a minimum, to retain the badge organisations must recertify at least once a year.

Cyber Essentials defines a set of controls which, when properly implemented, will provide organisations with basic protection from the most prevalent forms of threats coming from the Internet.

In particular, it focuses on threats which require low levels of attacker skill, and which are widely available online.

the five key cse controls

UNIVERSITY OF Southampton

1. Boundary firewalls and internet gateways

these are devices designed to prevent unauthorised access to or from private networks, but good setup of these devices either in hardware or software form is important for them to be fully effective.

2. Secure configuration

ensuring that systems are configured in the most secure way for the needs of the organisation

3. Access control

Ensuring only those who should have access to systems to have access and at the appropriate level.

4. Malware protection

ensuring that virus and malware protection is installed and is it up to date

5. Patch management

ensuring the latest supported version of applications is used and all the necessary patches supplied by the vendor been applied.

Why do we need these 5 controls

SME's network model relatively simple.

82% of SMEs have up to 9 employees (1)

15% of them have between 10 - 49 employees (1)

88% of SMEs operate from a single site (1)

13% of SMEs have any provision for CS at managerial level (1)

(1)BIS Research Paper Mar 2015

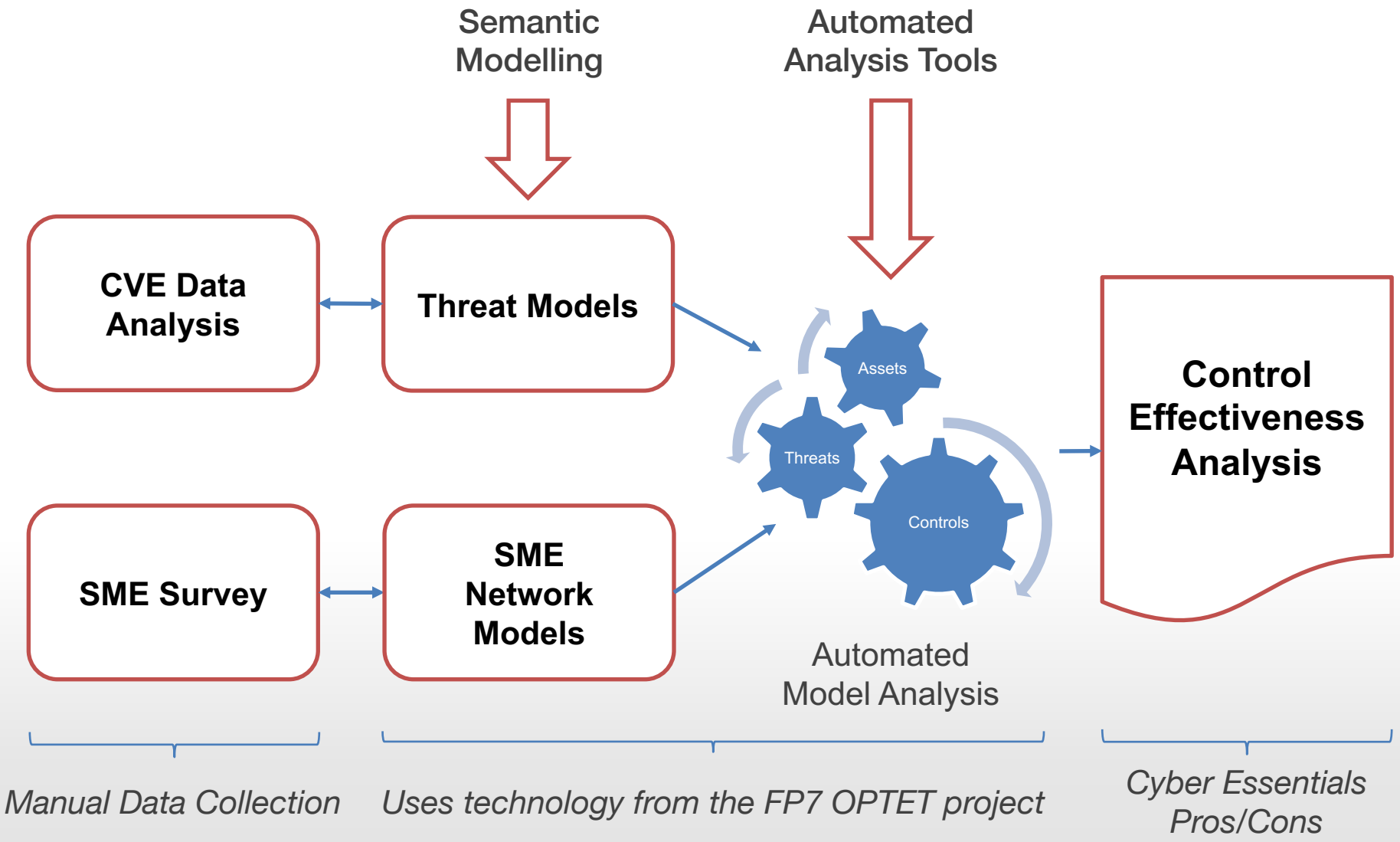
Why do we need these 5 controls

Survey curried in 2015, to find the most common network model used by SMEs.

Select three commonly network models used by SMEs.

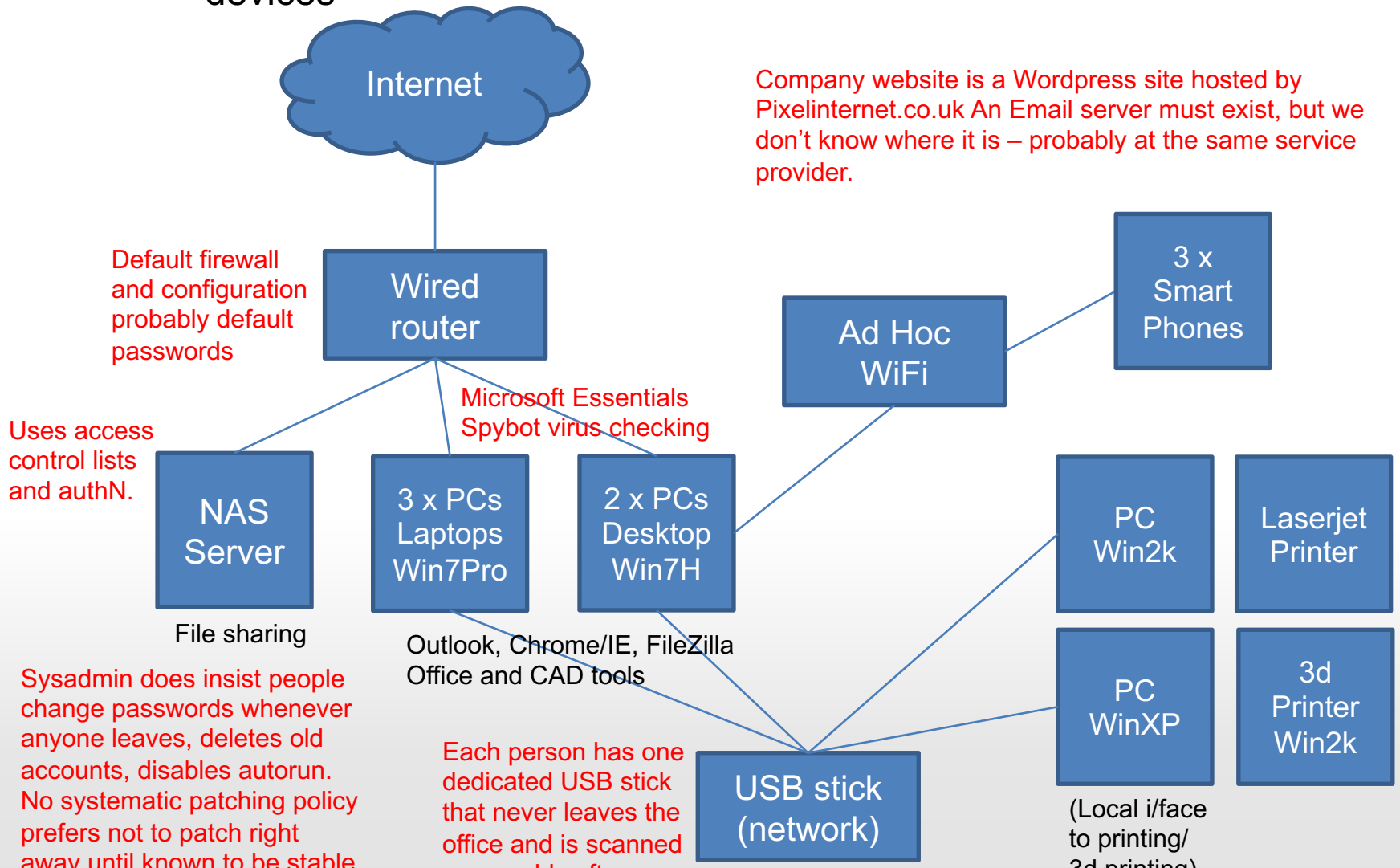
Common Vulnerabilities and Exposures database and in-house developed simulation tools used to evaluate the effectiveness of the five controls.

Approach


Semantic Modelling
Automated Analysis Tools
CVE Data Analysis
Threat Models
SME Survey
SME Network Models
Assets
Threats
Controls
Automated Model Analysis
Control Effectiveness Analysis
Manual Data Collection
Uses technology from the FP7 OPTET project
Cyber Essentials Pros/Cons

typical outcome from SME interviews

A Business: CAD and 3D Printing for medical devices

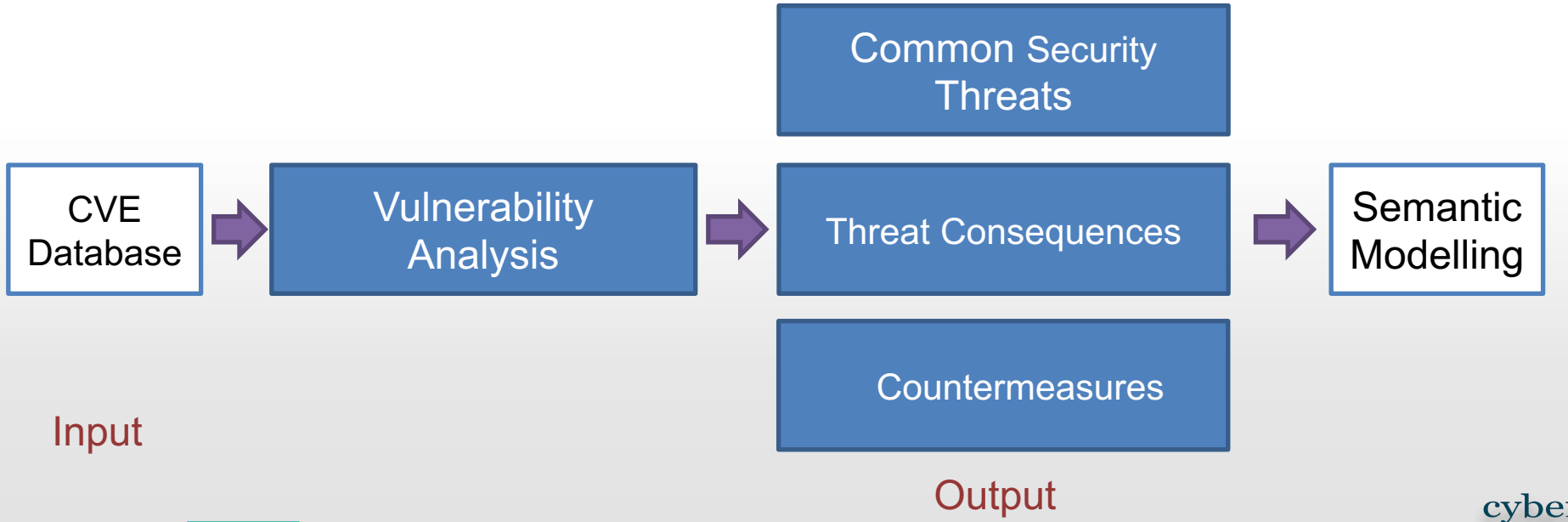


Used the Common Vulnerability Entries (**CVE**) database as a basis

captures ‘common’ threats that Cyber Essentials is supposed to counteract (zero day attacks were not considered for this work)

Goal: identify distinct threats and possible security controls

Output: used to construct a semantic threat classification



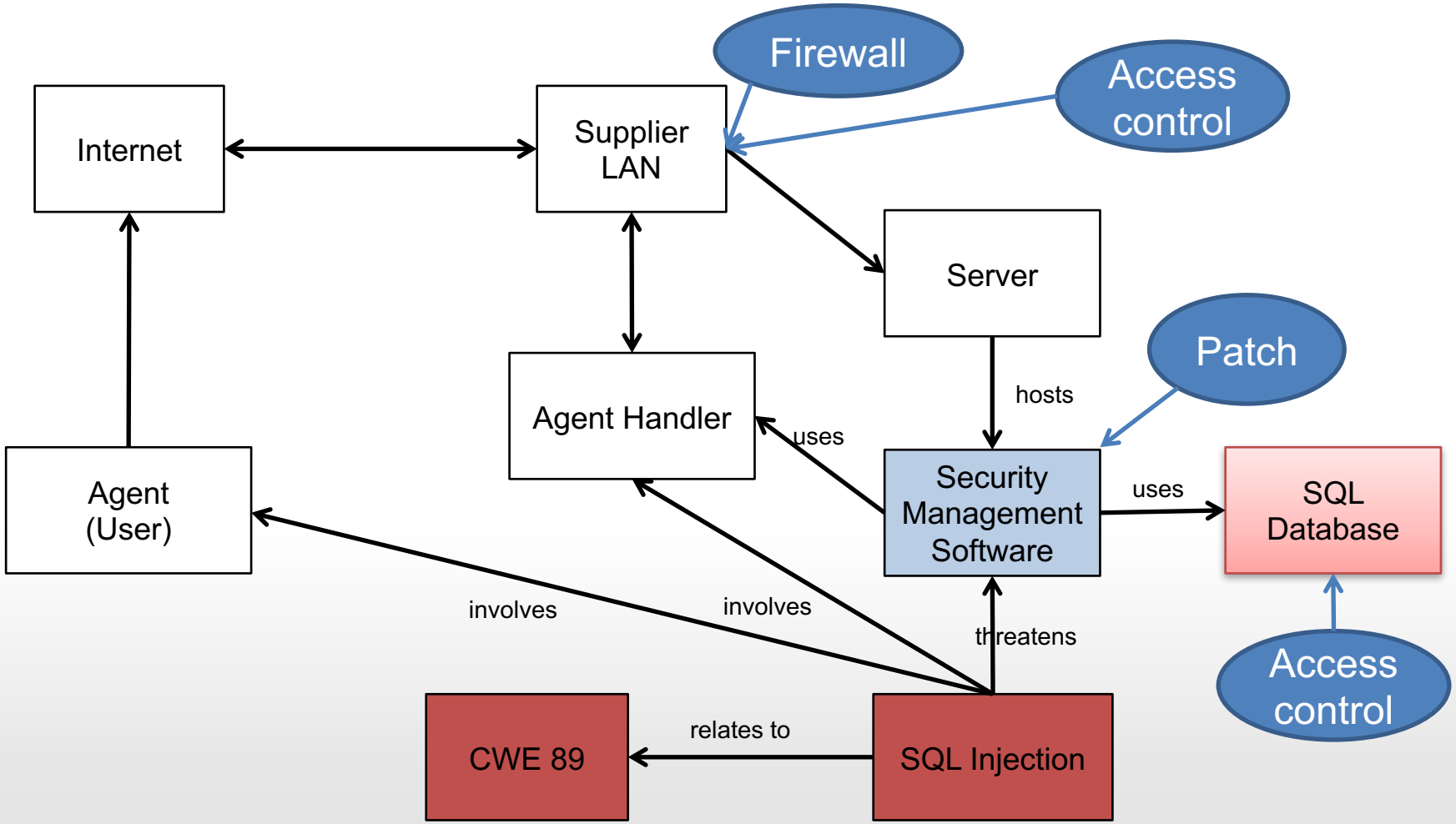
CVE entries (eg: SQL injection attack)

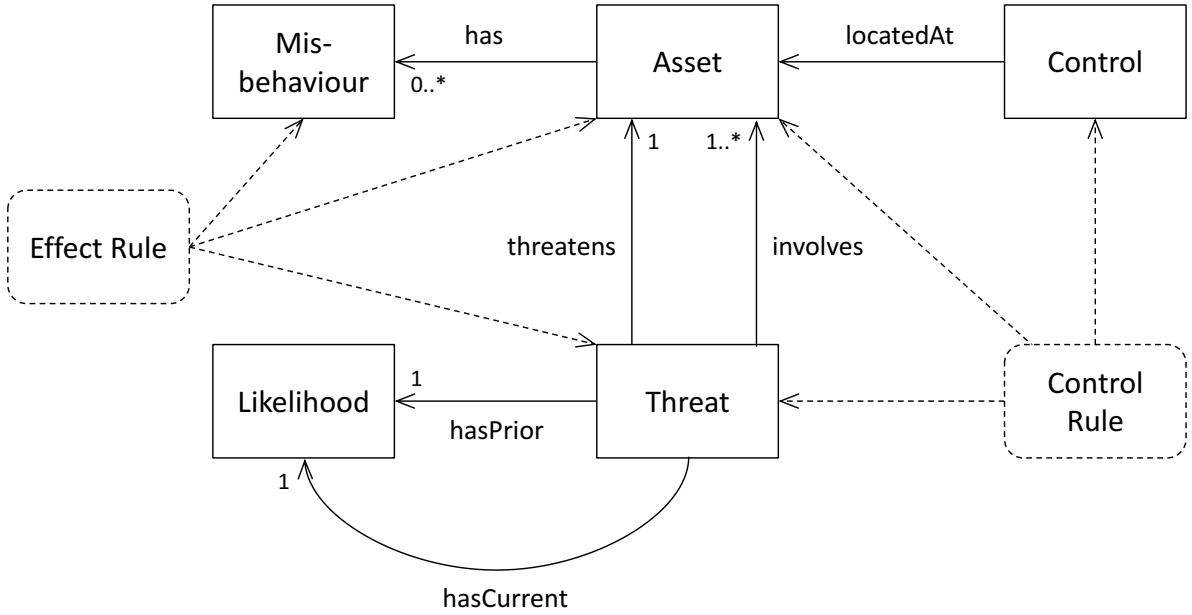
CVE	Description	CVSS = 7.9	CWE
CVE-2013-0140	SQL injection vulnerability in the Agent-Handler component in McAfee ePolicy Orchestrator (ePO) before 4.5.7 and 4.6.x before 4.6.6 allows remote attackers to execute arbitrary SQL commands via a crafted request over the Agent-Server communication channel.	Confidentiality Impact = Complete Integrity Impact = Complete Availability Impact = Complete Access Complexity = Medium Authentication = not required Gained Access = None	89

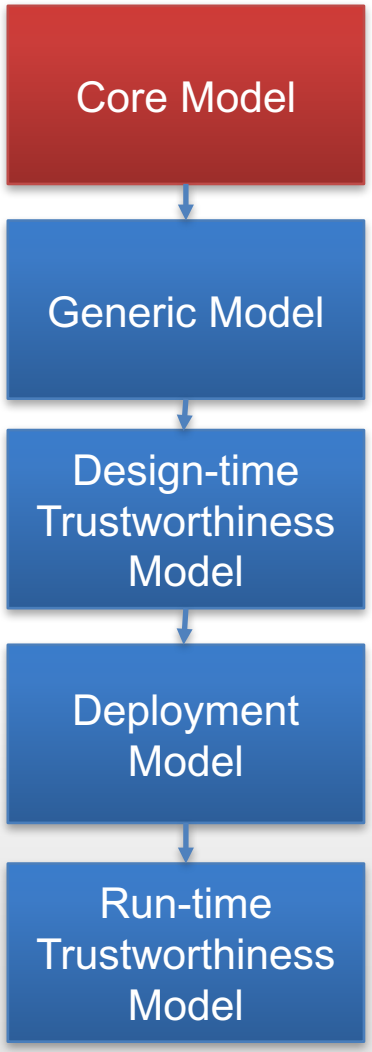
common vulnerabilities scoring system

common weakness enumeration

modelling assets, threats & vulnerabilities







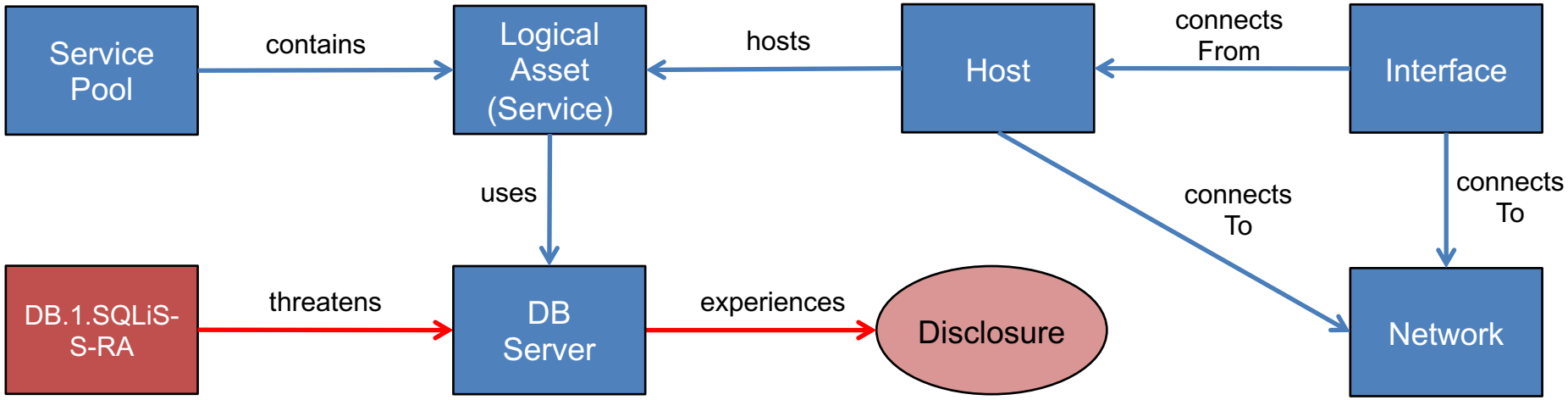
Assets: things of value in the modelled system

Threats: actions/events involving assets that may compromise an asset's value

Misbehaviour: adverse consequences of threats that signify compromised asset value

Controls: security mechanisms associated with assets to block/mitigate threats involving them

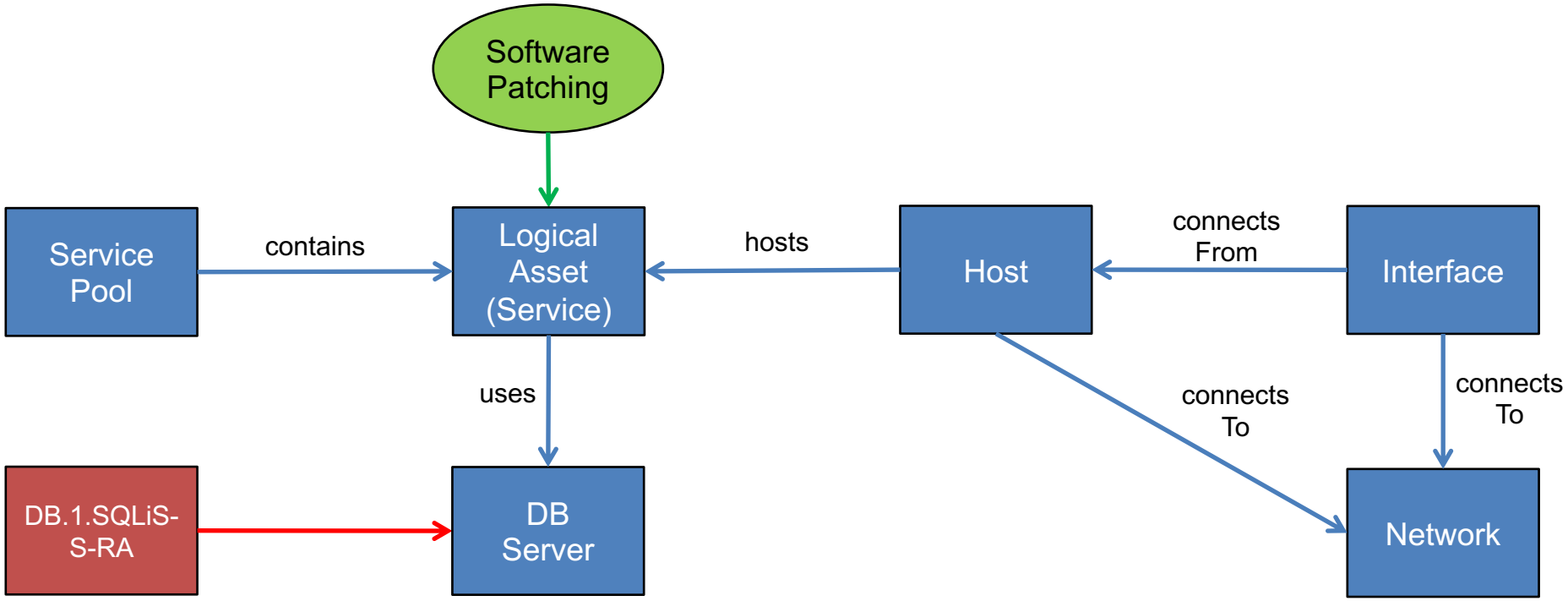
modelling threats (eg SQL injection)



A problem with a Service can be exploited by an anonymous remote user to send inappropriate queries to a back-end DBServer.

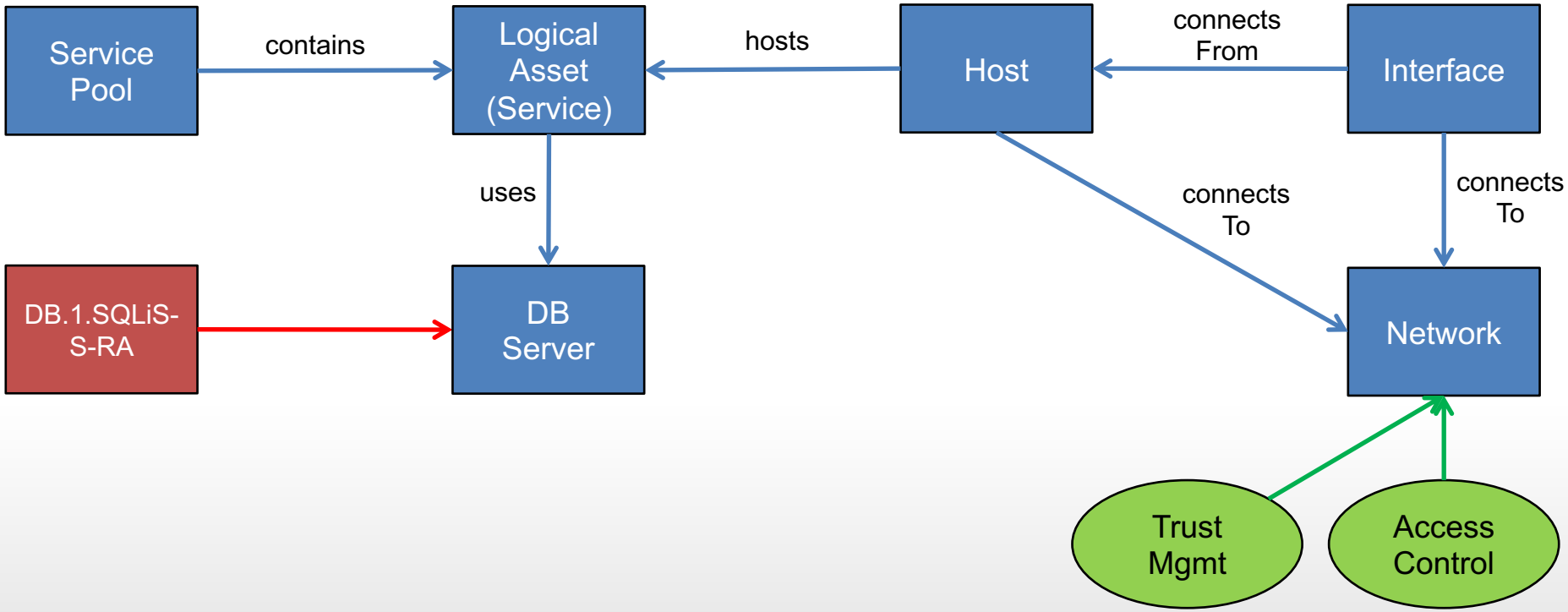
Threatened asset is ‘DB’, threat consequence is ‘1’ = ‘disclosure’. Pattern SQLiS refers to the arrangement of involved assets. The vulnerable asset is the service ‘S’, and the attacker is remote and anonymous ‘RA’.

applying mitigations: (eg. SQL injection)



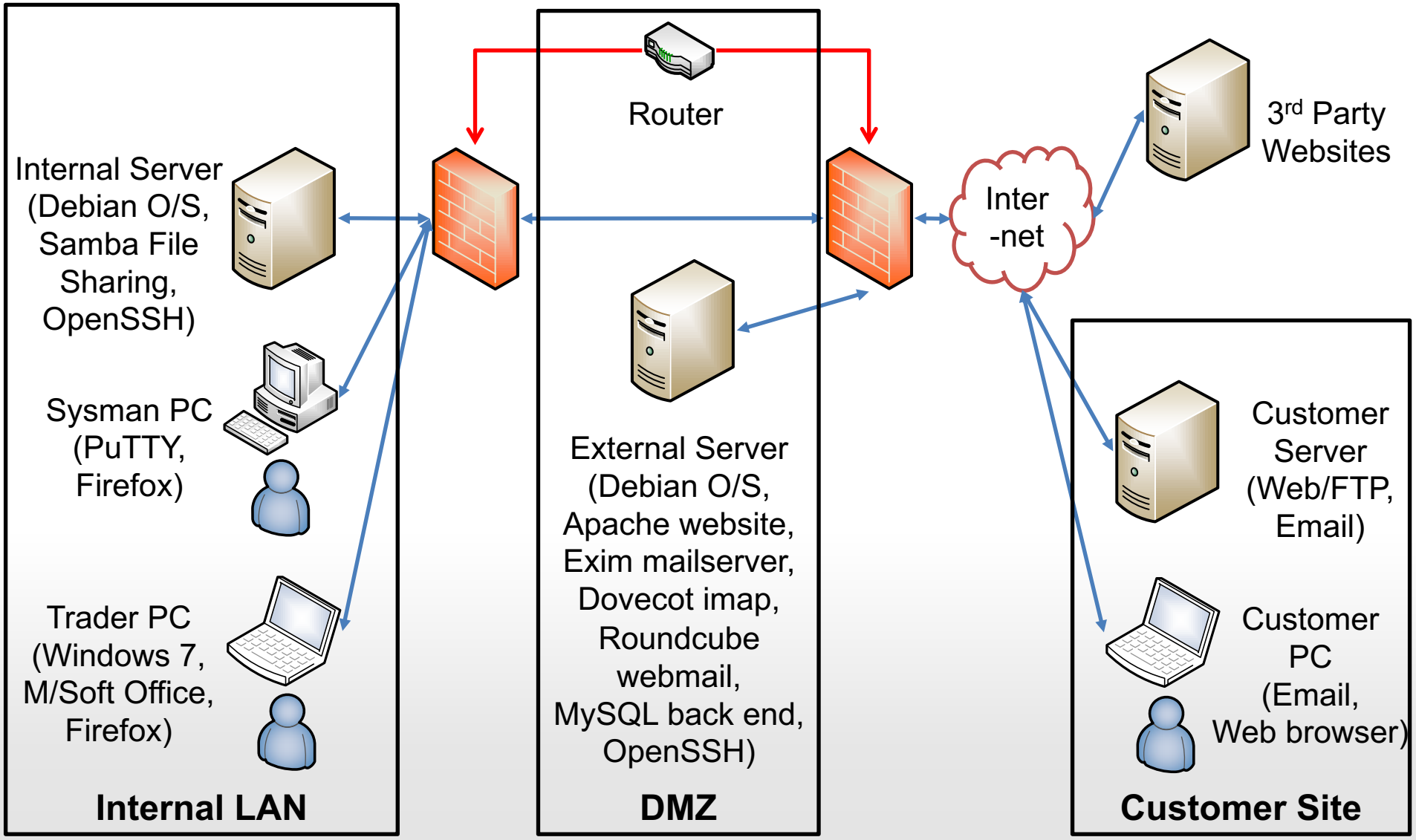
Control option 1: patch the vulnerable software.

applying mitigations: (eg. SQL injection)

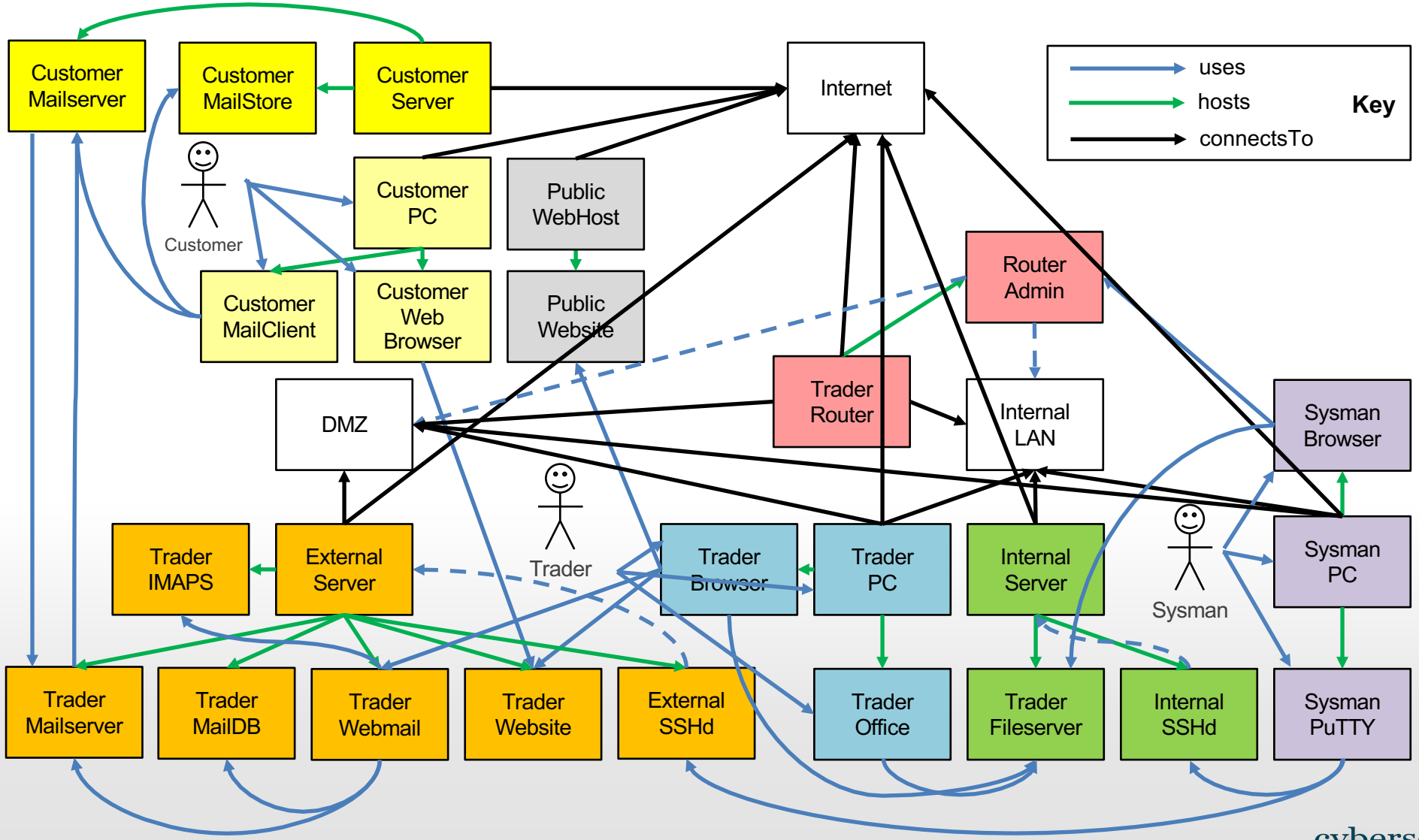


Control option 2: restrict access to the network to fully trusted users. Note that we can't do this at the service because the attack is anonymous. The equivalent attack by an authenticated user could be handled by restricting access to the service.

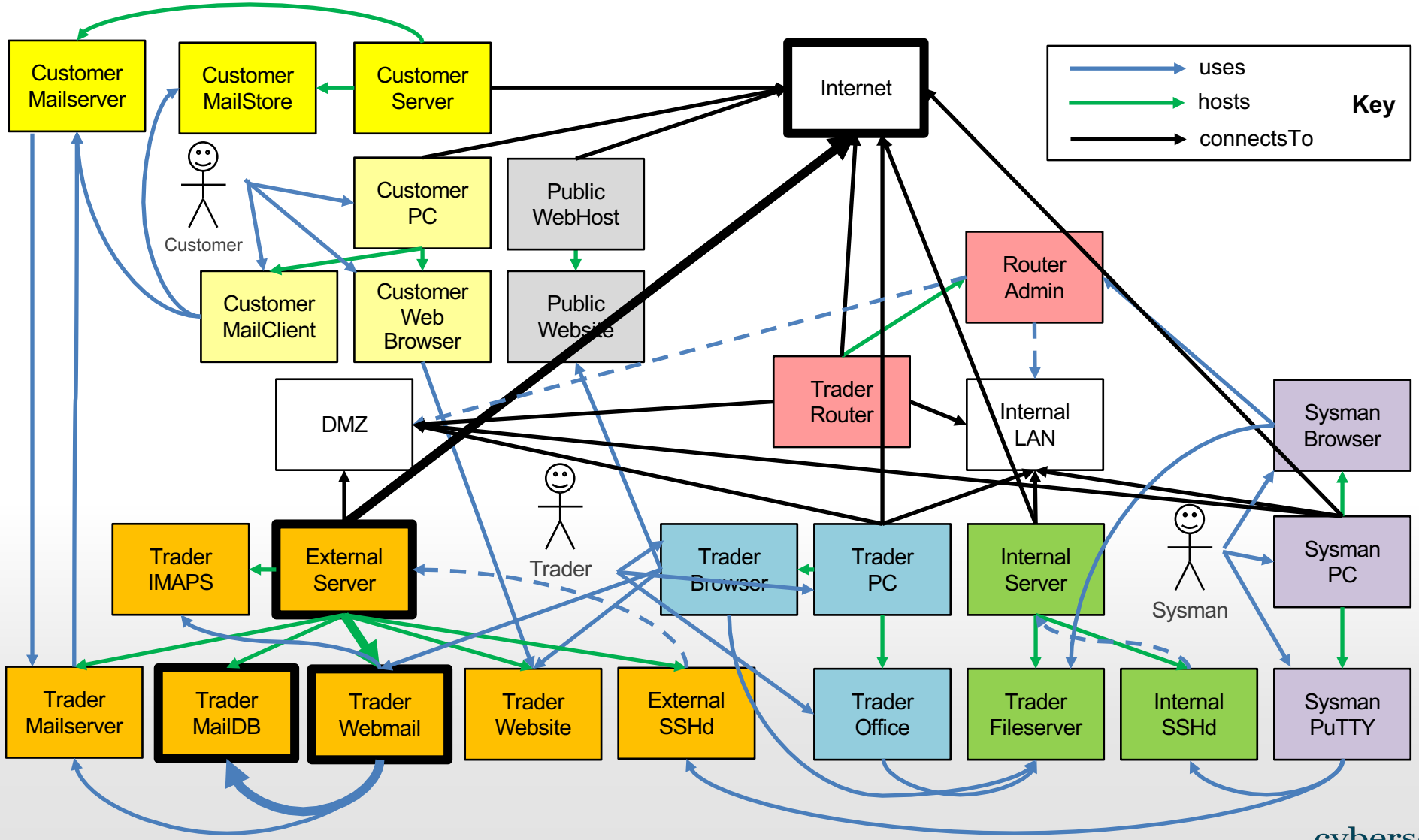
in-house SME network



SME network modelling



SME network threat analysis



in-house SME network

Cyber Essentials Chapter(s)	#Relevent Threat Classes	#Addressed Threat Classes	%Effectiveness
None	493	0	0%
Boundary Firewalls	493	65	13%
Plus Secure Configuration	493	75	15%
Plus User Access Control	493	177	36%
Plus Malware Protection	493	262	53%
Plus Software Patch Management	493	390	**79%**

Cyber Essentials claims to address 80% of common threats

our analysis shows it does for this type of network

cloud-based SME network

Cyber Essentials Chapter(s)	#Relevent Threat Classes	#Addressed Threat Classes	%Effectiveness
None	300	0	0%
Cloud Service Provider Security	300	91	30%
Boundary Firewalls	300	128	43%
Plus Secure Configuration	300	137	46%
Plus User Access Control	300	143	48%
Plus Malware Protection	300	160	53%
Plus Software Patch Management	300	217	72%

Cloud security helps, but leaves unresolved threats

e.g. phishing or snooping for Cloud service passwords

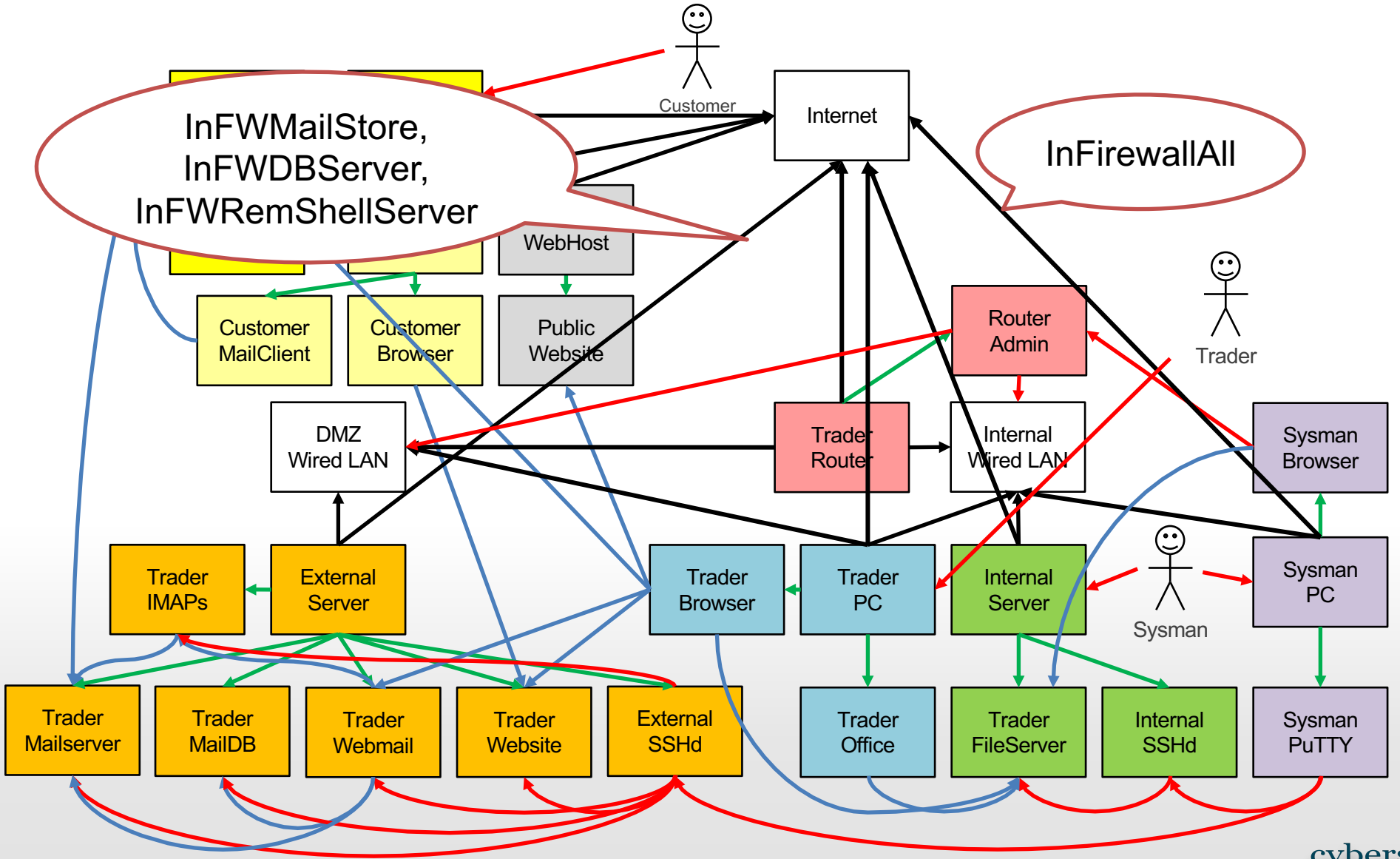
SME network with mobile staff

Cyber Essentials Chapter(s)	#Relevent Threat Classes	#Addressed Threat Classes	%Effectiveness
None	307	0	0%
Cloud Service Provider Security	307	130	42%
Boundary Firewalls	307	150	49%
Plus Secure Configuration	307	158	51%
Plus User Access Control	307	164	53%
Plus Malware Protection	307	189	62%
Plus Software Patch Management	307	213	69%

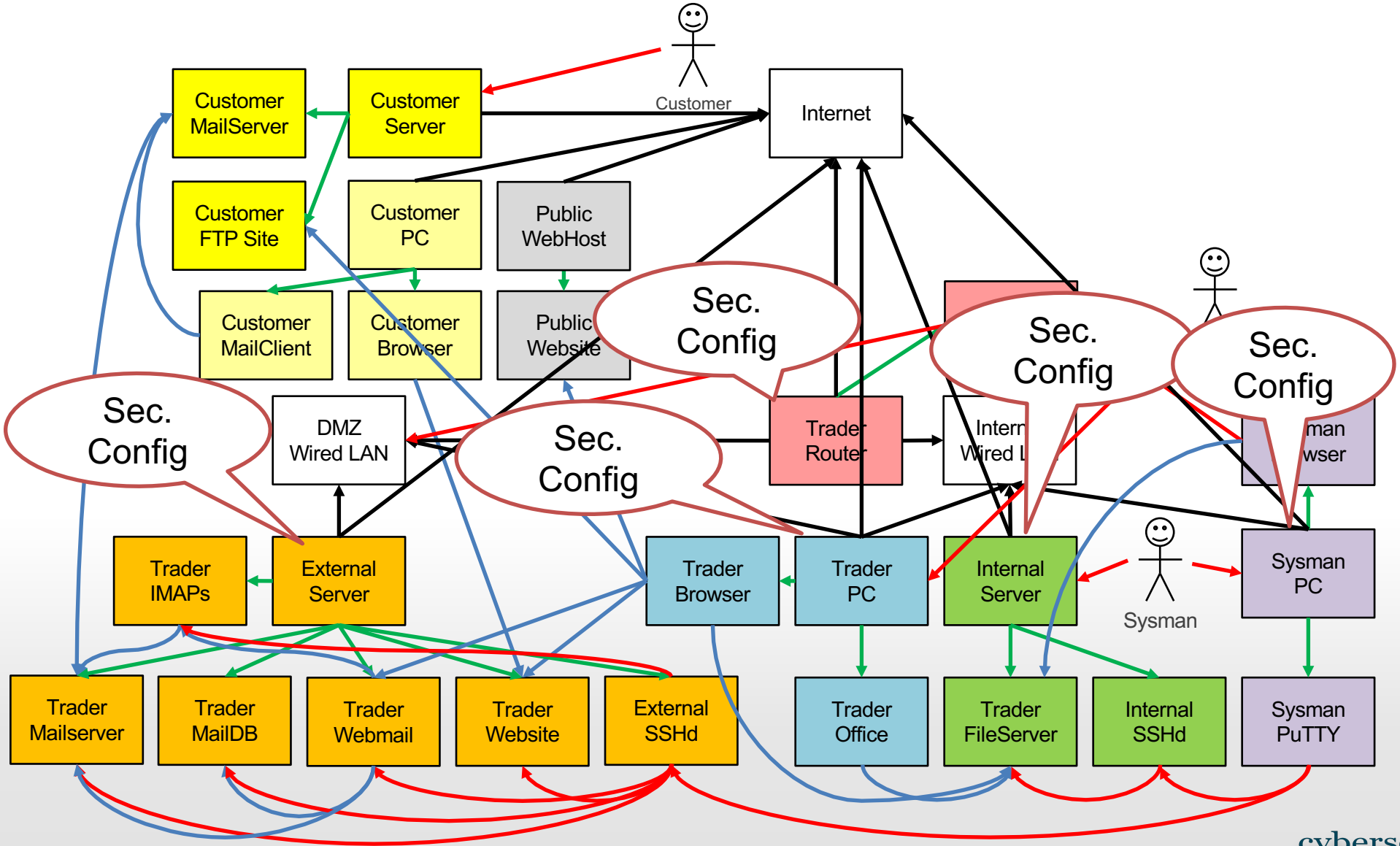
Extra threats beyond the reach of Cyber Essentials

now all services are accessed over public networks

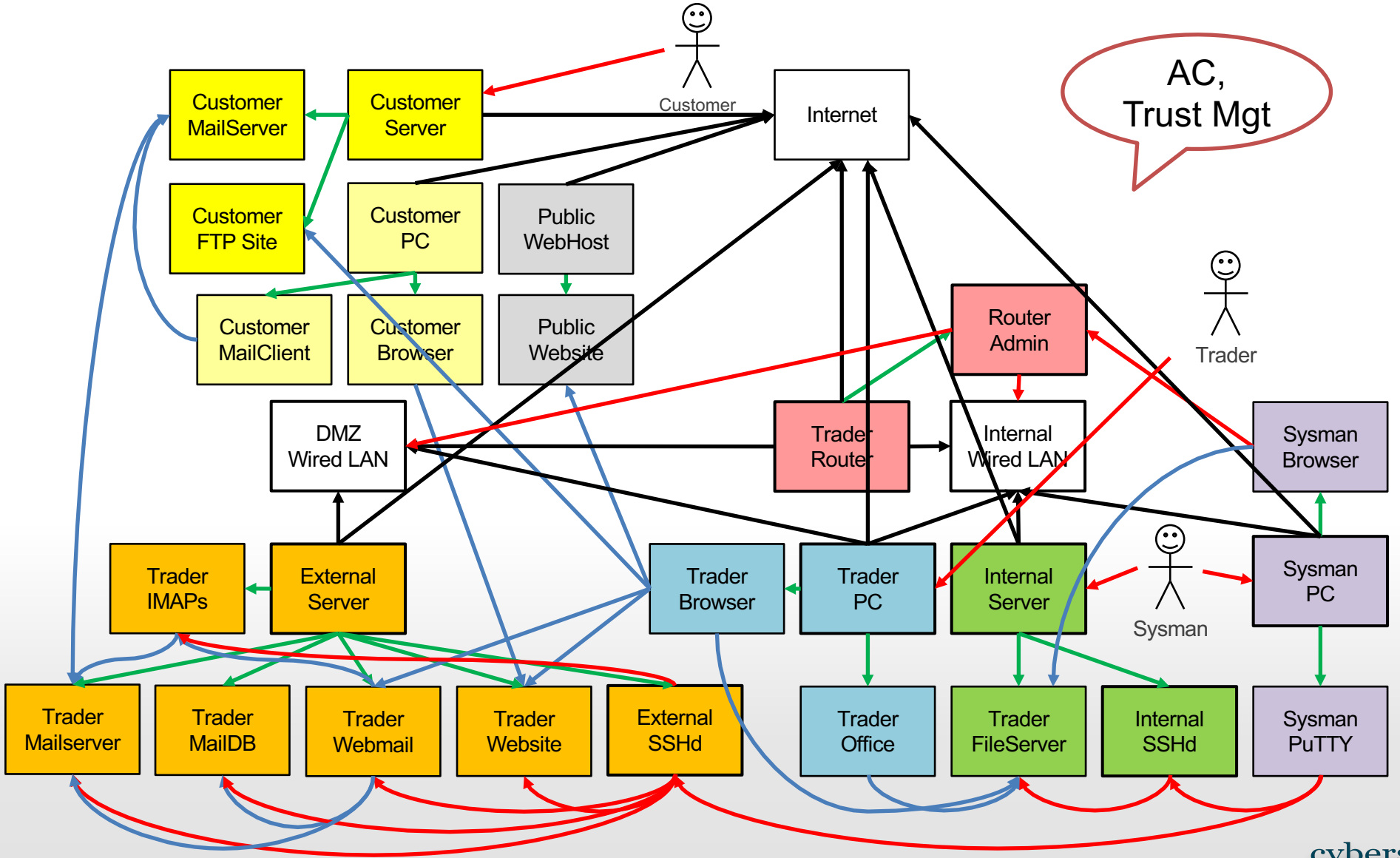
in-house SME network



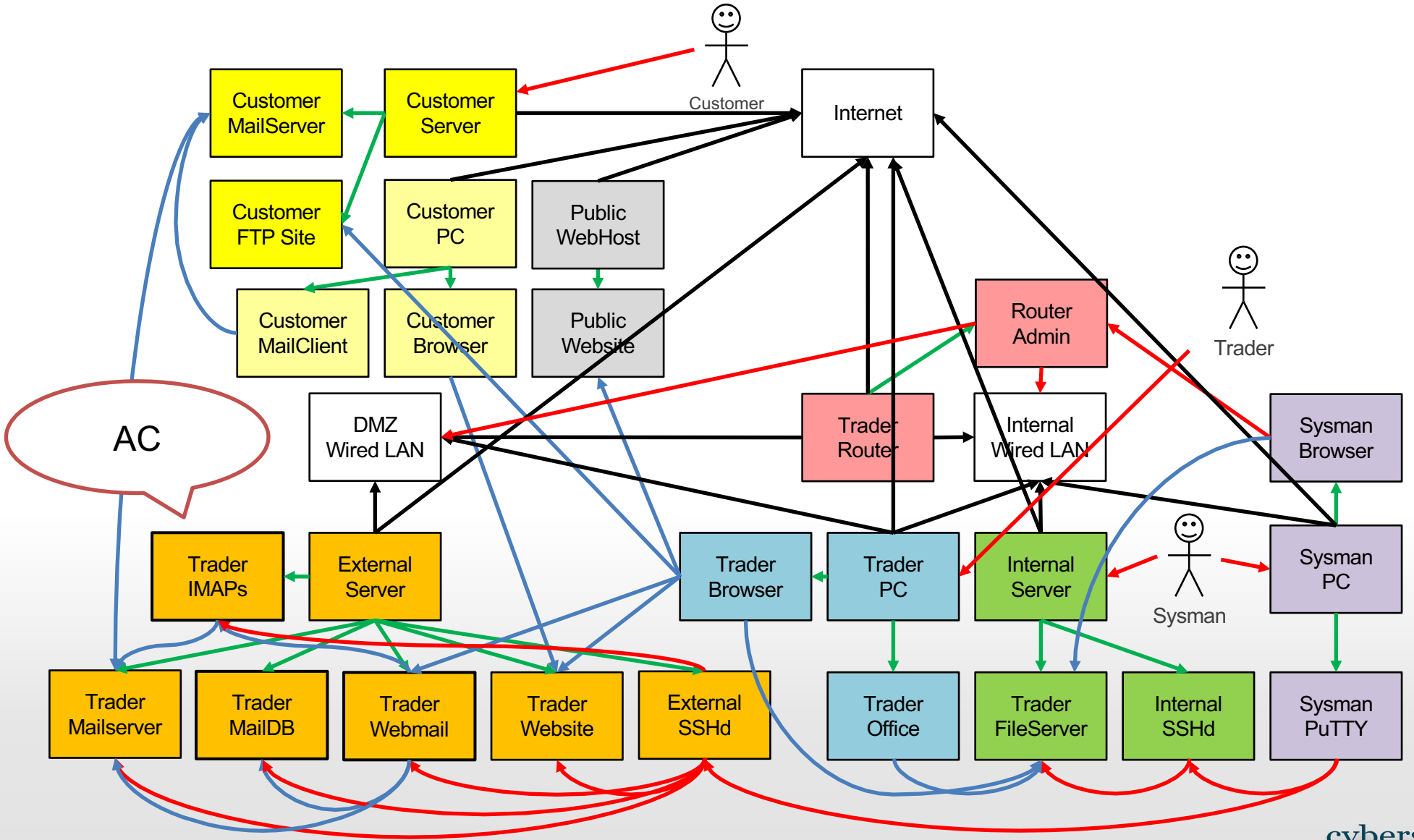
in-house SME network



in-house SME network



in-house SME network



Cyber Essentials does address around 80% of common threats in traditional SME networks with well-defined perimeters

Cyber Essentials is less effective for SMEs that use Clouds and/or have mobile workers

- these networks have fewer threats, but a higher percentage are missed by Cyber Essentials

Cyber Essentials could be improved by

- guidelines on how to choose Cloud services based on their security measures
- guidelines on communication security
- guidelines on training users against impersonation attacks
- tools supporting SME's IT configuration self assessment, impact and cost of alternative controls

- Investigating areas where Cyber Essentials fell short: use of cloud services and mobile (and BYOD) devices
  - a follow-up study on BYOD devices has been started
- Establishing a threat classification schema based on this approach
  - distinguished from the CVE/CWE approach by being machine understandable and based on how threats affect a network
  - could be used to (automatically) assess control strategies against the range of threats addressed
  - can be updated whenever new threats are identified
- Using automated methods to reduce the cost of security analysis, especially for SMEs