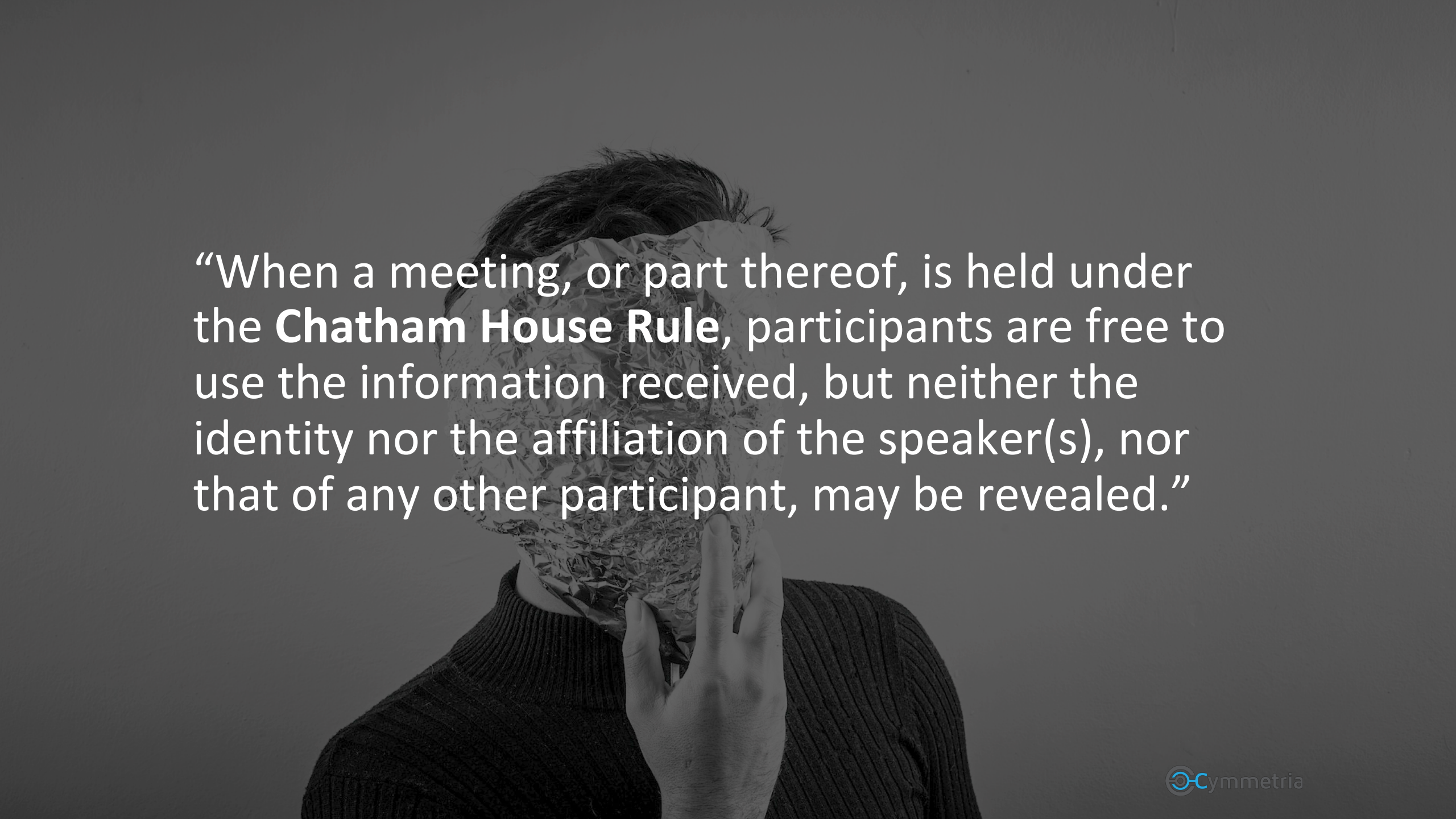
Hunting the Bad Guys: Approaches to Threat Detection

Peter Glock, Managing Director EMEA

Cymmetria


Before we start…
Cymmetria


“When a meeting, or part thereof, is held under the **Chatham House Rule**, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed.”

5 questions to ask before we get to ‘threat detection’

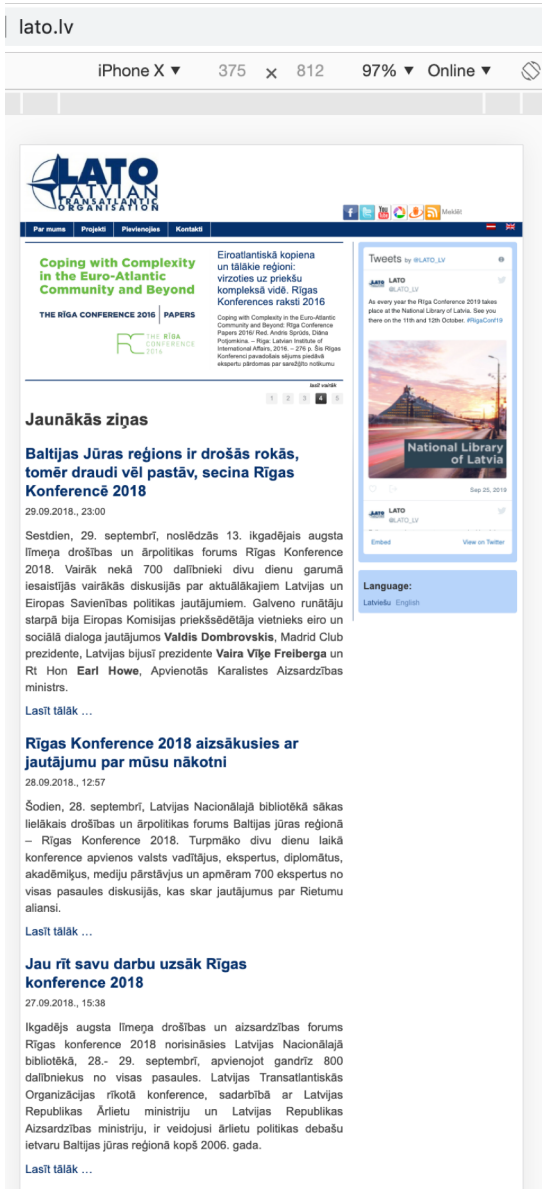
Cymmetria

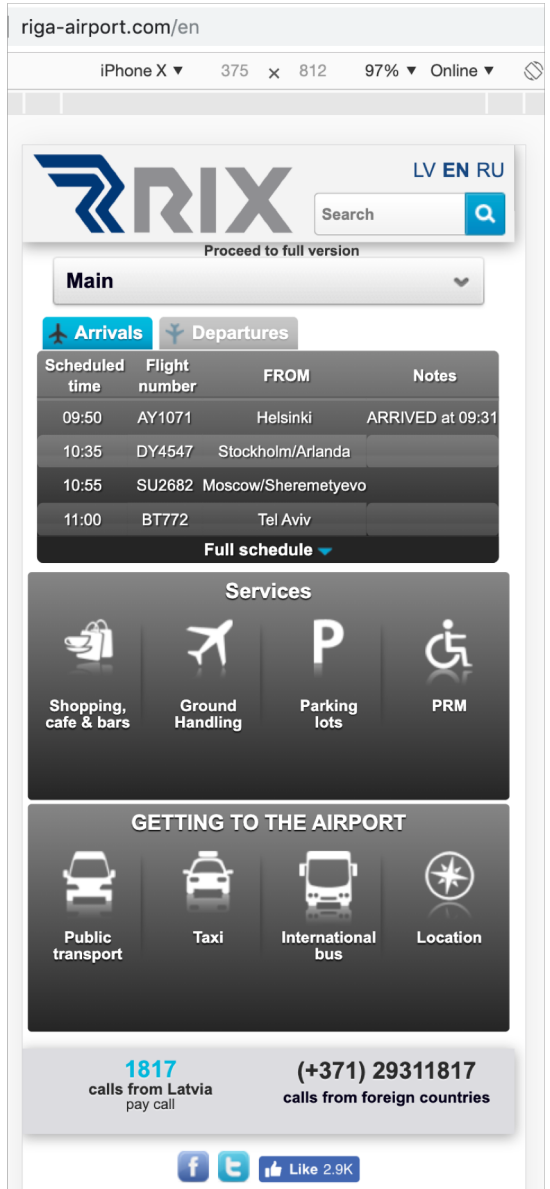
Contents

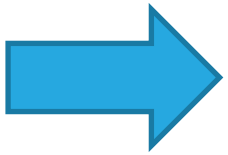
- An exercise in trust and risk
- What do I want to protect?
- Defining and discovering assets
- Threats, risks and security controls
- Smoke alarms for security and privacy

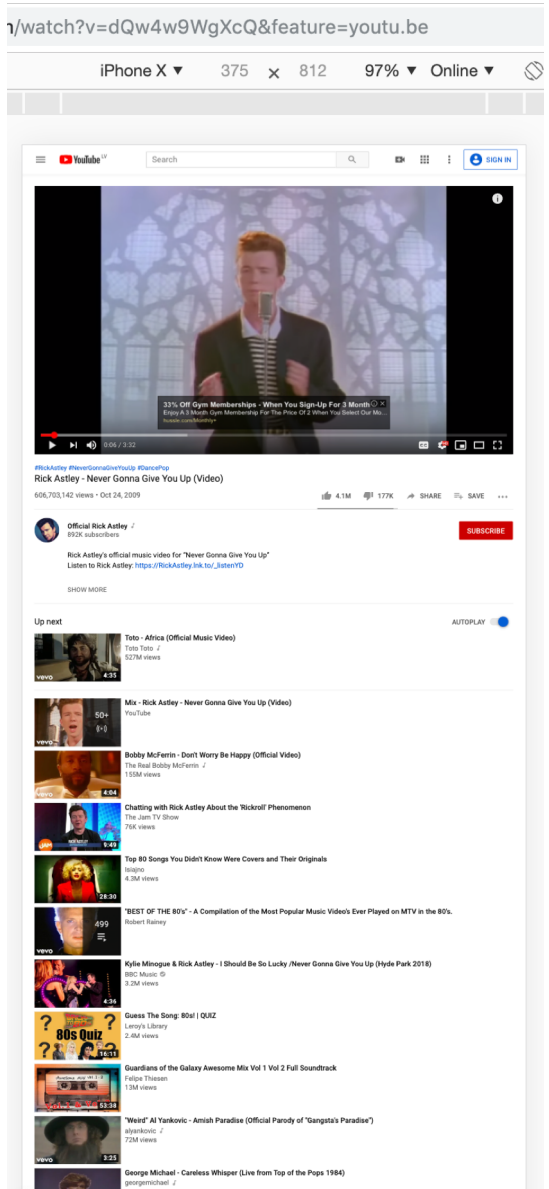
Cymmetria

Who and what do you trust?







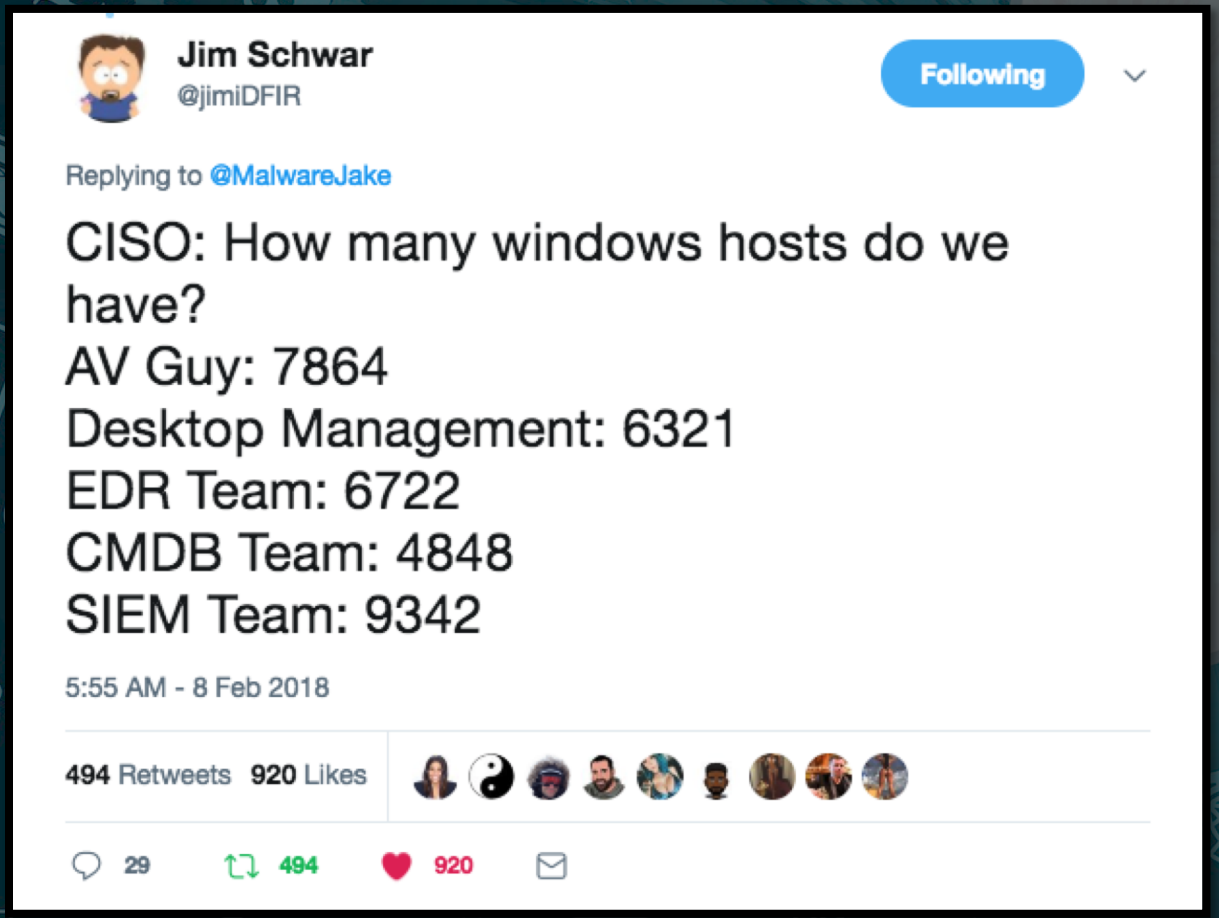


Demonstration – wireless insecurity

Cymmetria


What do you want to protect?
Cymmetria

Information Assets



And what about?:

- Client data
- Personnel files
- Supply chain details
- …

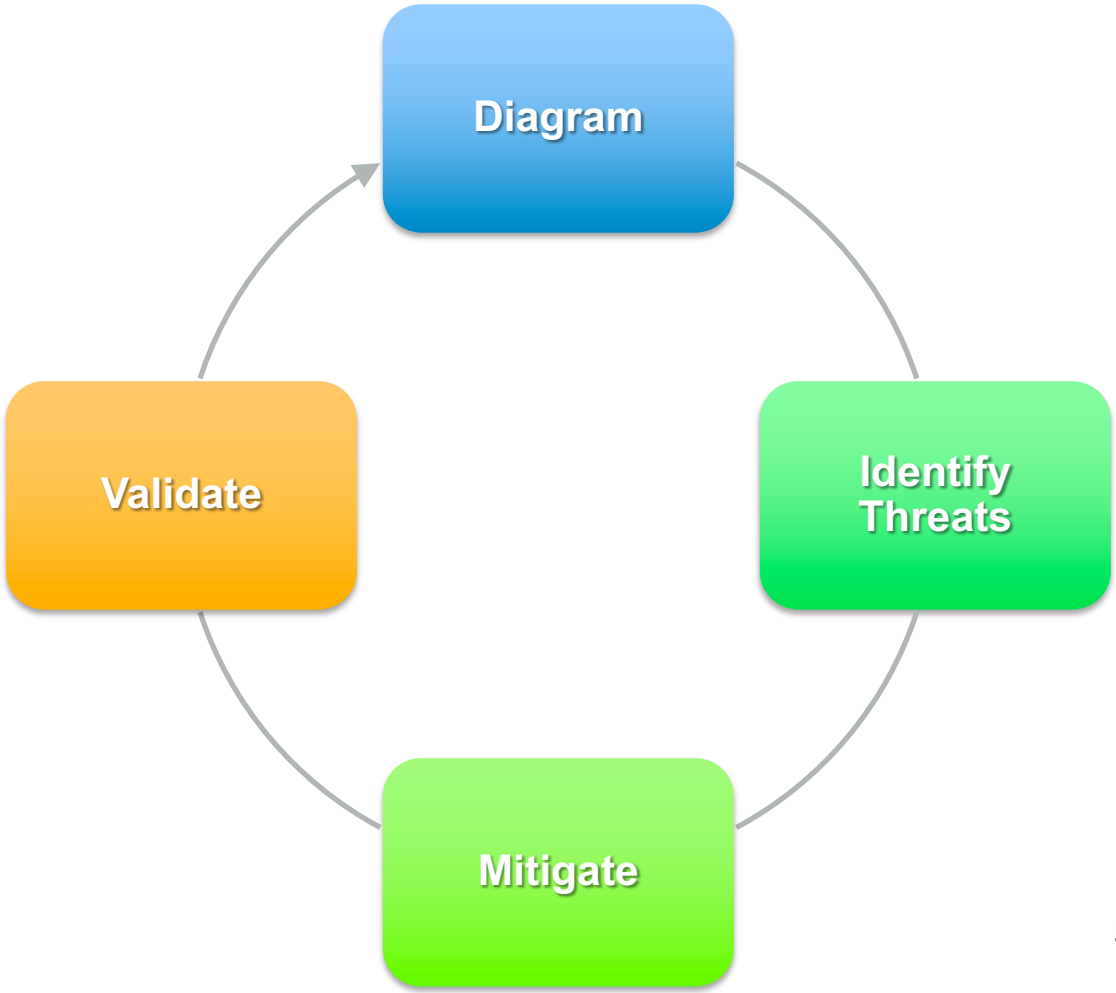
Demonstration – unsexy asset management

Cymmetria

Threats, risks, security controls

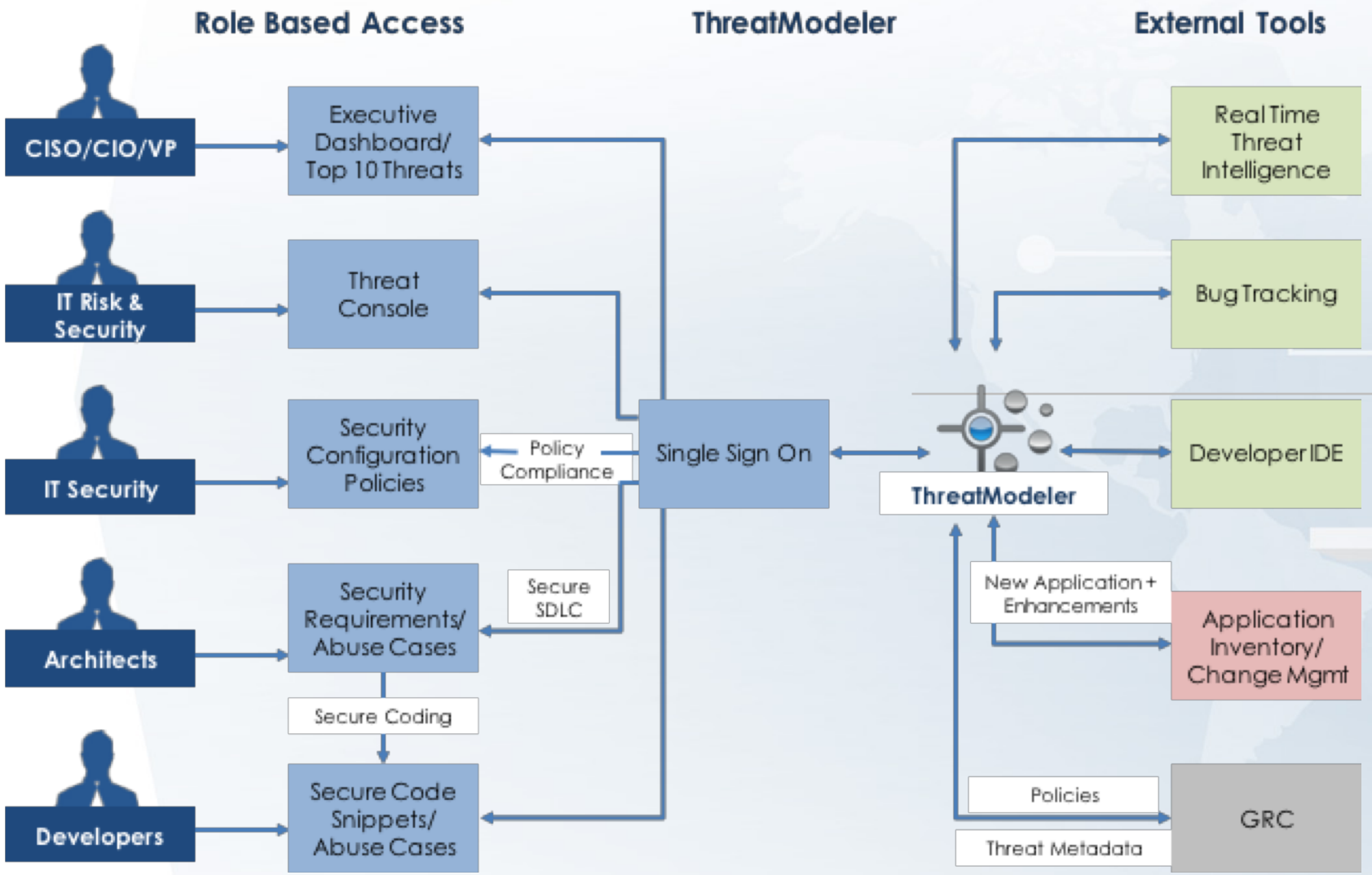
Cymmetria

The Process in a Nutshell



Source: Microsoft

Architecture and Integration



ThreatModeler
Security Starts Here

Source: ThreatModeler

Demonstration – VAST Threat Modelling

Cymmetria

Smoke alarms

A word about supply chains

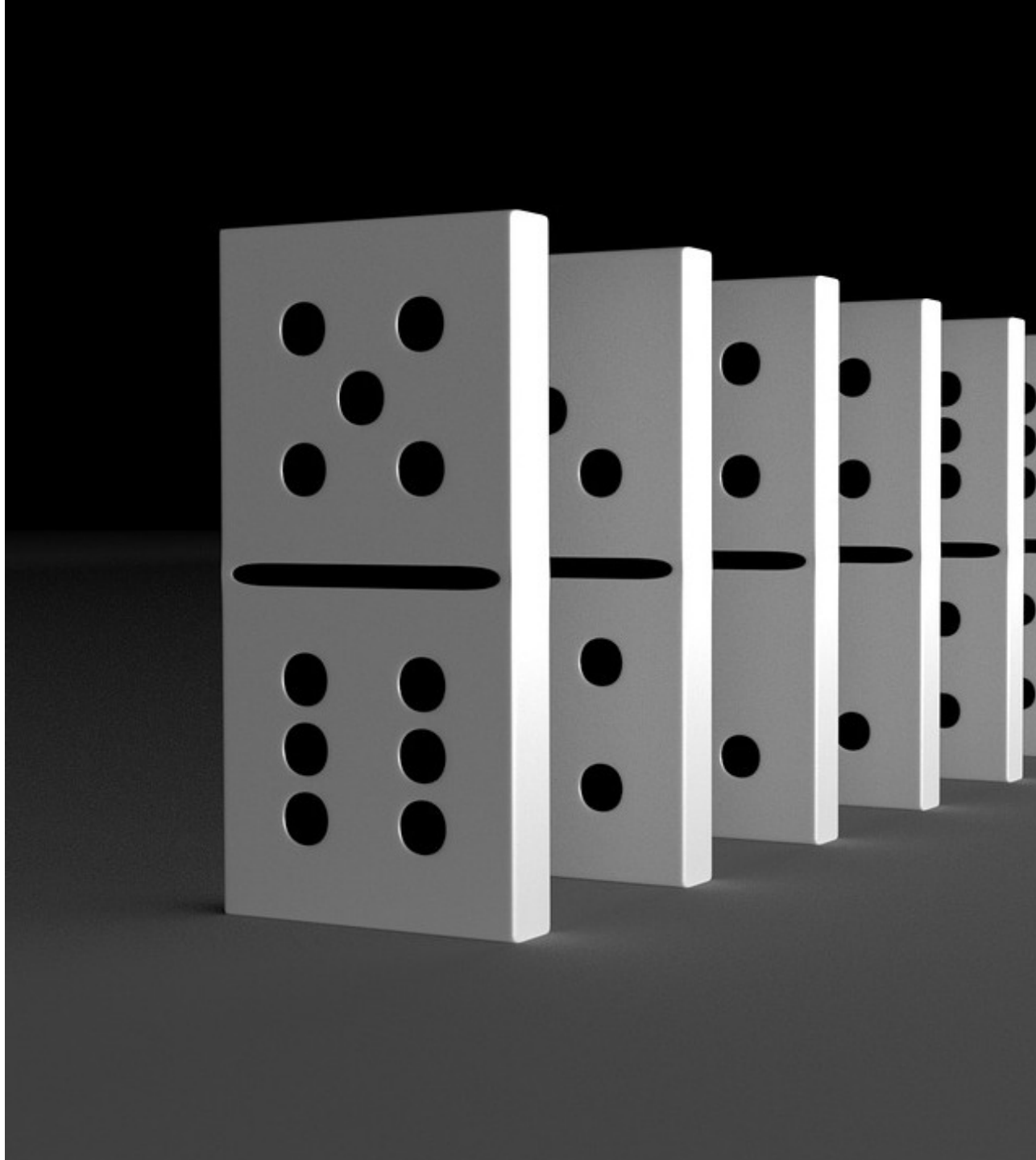
Your data is spread throughout your supply chain

- Github
- Unprotected network shares (s3, DropBox…)
- Shadow IT

…and maybe by the bad guys

- Pastebin
- Dark Web

You need a ‘smoke alarm’ for the supply chain



Smoke Alarm – a breach of your own defenses

Leverage the fact attackers are predictable

```
// start with spearphishing, and
then …

while ( !TargetFound )
{
/* compromise endpoint →
escalate privileges → recon
(mimikatz, net use, etc.) →
lateral movement */
}
```

Cymmetria

Controlling the attackers

Attackers use **information they find in our networks** to make lateral movement and attack targets in the organization.

Deception feeds them **real-looking information** that causes them to follow a **defender-controlled path**.

Once they hit a **deception target**, their *modus operandi* is exposed and their attacks are **detected and prevented**.

Threat Hunting - the surgical approach

Surgical approach – as opposed to “spray and pray”

- Better at catching attackers, including advanced attackers
- Lower friction with IT, as well as lower total cost (compared to other deception approaches)

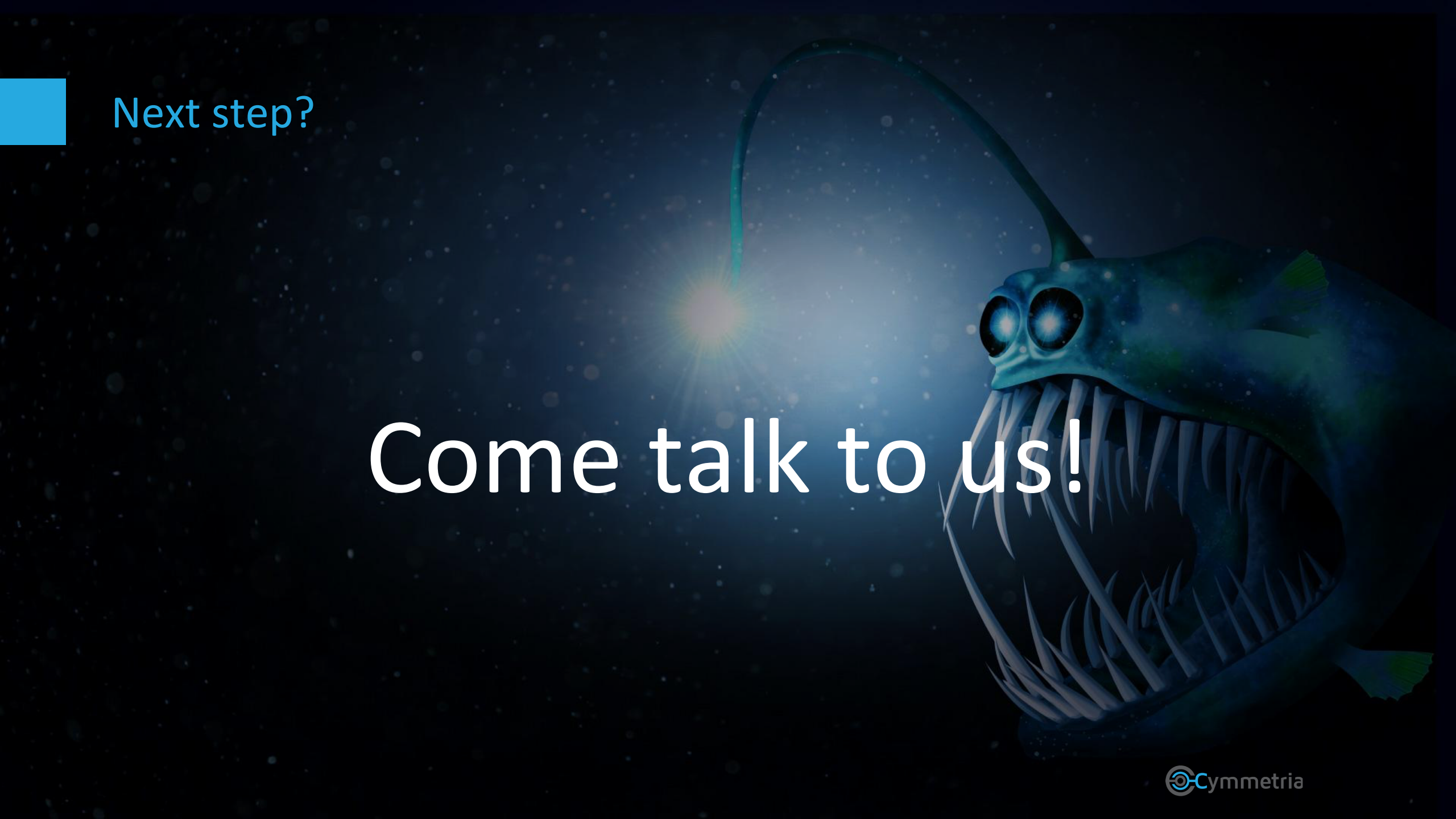
Conclusion – detect threats throughout the SDLC

- It’s much more efficient to build security controls and mitigate threats during development
- Test the effectiveness of your security controls at each step (Red Teams…)
- Don’t trust your own controls, set up some smoke alarms for breaches

5 questions to ask

Cymmetria

Next step?



Come talk to us!

Cymmetria