THE GAME OF CYBER CAT AND CYBER MOUSE: IMPROVING THE MOUSETRAP

Laurence Pitt
Security Strategy Director

@laurencepitt
lpitt@juniper.net
We grew up watching Tom and Jerry.

There is reality in their situation.

Image: http://www.transparentpng.com
But what if Jerry isn’t even here?

This is how normal looks, it’s important.
Five Common Mousetrap mistakes

...and what we can learn for Cybersecurity
Mistake **Number 1:** Lack of planning; mousetrap strategy fails.

Most **mice** will be **caught** on the first night.
Solution Number 1: Cybersecurity without planning is likely likely to fail.

Partner, do not take the challenge solo
Mistake Number 2: Too many **Mousetraps** or positioned too closely.
Mistake Number 2: Too many Solutions to the same problem.

Organisations today have a multitude of different and similar products on their network.

Old version, failed version, new version

Product Overlap = Security Risk.
Mistake Number 3: Setting mousetraps in all the wrong places.
Mistake **Number 3**: Setting traps but looking at the wrong places.

The focus needs to change as we only look at ‘Human’ interfaced computers.

There is no consistent Security model.
Solution **Number 3:**
Setting traps but looking at the wrong places.

Things are changing, devices, applications, services

Only the network remains consistent

We need to **Leverage the network**
Mistake **Number 4:**
Using the wrong amount or type of bait.

Mice will eat cheese...
But **Mice** prefer **nuts or seeds**
Mistake Number 4: Understand what you need to protect.

For each malware family there are thousands of variants. They in essence, are malware disguises. ‘Shape shifting’ to appear safe to your defences.

And understand what you are protecting it from!
Mistake Number 5: What if it’s not a mouse!!
The Smarter Mouse Trap
Detect problems based on knowledge of what is bad

Time based security models

Detect problems based on knowledge of what is normal

Behaviour based security models
Developing a Threat Management Platform

Ingest
Analyse
Enforce
Automate

Collect Targeted Intelligence
Analytics and Traps
Outcomes and Responses
Integrate and Ingest your Qualitative data

Not all data is created equally
Focus on the quality data first

unlock the combined power and intelligence from multiple security solutions
Analyse and understand Behaviour

Collect the **unique data** available across each business

Model what’s normal within this data to **protect each business**

Leverage deep learning to help identify normal and abnormal behaviour
Just like us, machines need to learn how.

This is NOT artificial intelligence but an essential step towards it.
Reality check

Machine’s don’t know what’s good or bad

Machine learning can be leveraged if the responses are tracked
Teaching machines to think

Data > Analysis > Human Response(s)

Let the machine see what to do in given situations

It is possible to determine how humans ‘typically’ react
You are being watched

Provide the meta
watch what the human does
track what actions are taken

If you react the same way to a certain set of conditions – machines can learn it.
Enforcement...but where?

The network is the only consistent business enforcement point.

Embed and Simplify security policies across the entire business.

Leverage routing, switching, security and third-party technologies.

Leverage that intelligence throughout the network.
Automate it!

Let the machines do what they are good at
Let people do what they are good at

Allow people to focus on improving the security
Juniper Networks Connected Security
‘Mouse Trap’

Integrate intelligence from across the business
Enforce across the entire network
Routing, Switching, Firewalls and integrated 3rd party solutions
Secure the data, the brand, the business, the customers

The Intelligent, Automated Secure Network
THANK YOU