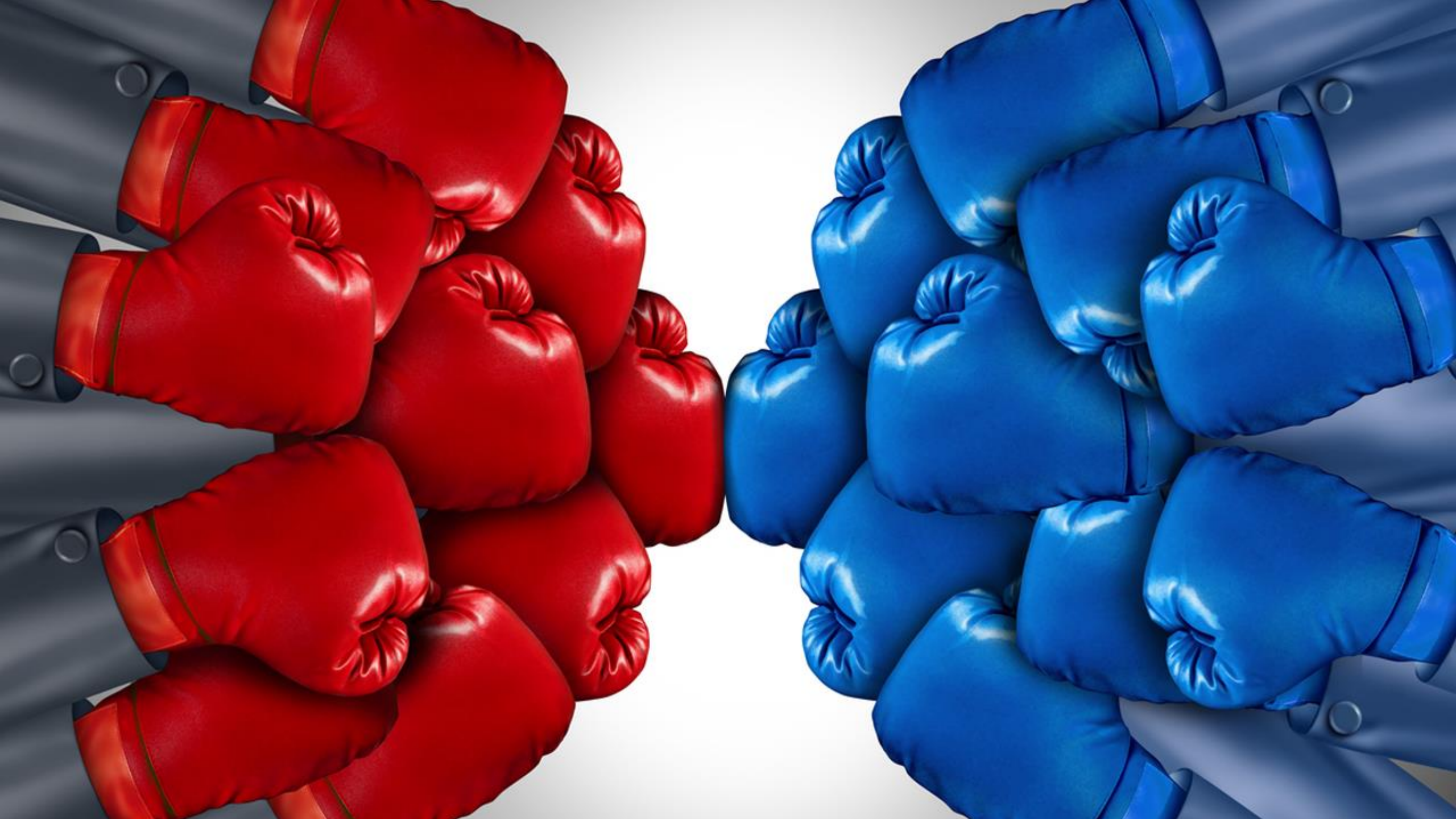
Learning How to Smurf with Honeypots

Emil Tan Chapter Lead, The Honeynet Project (Singapore Chapter)
emiltan@honeynet.sg / @Emil0xA

Who is this for?



Learning How to Smurf with Honeypots

Emil Tan Chapter Lead, The Honeynet Project (Singapore Chapter)
emiltan@honeynet.sg / @Emil0xA

$ whoami

– Chapter Lead, The Honeynet Project, Singapore www.honeynet.sg
– Crew & Co-Founder, Edgis/Div0 www.edgis-security.org / www.meetup.com/div-zero
– Co-Boss & Co-Founder, Infosec in the City www.infosec-city.com

– [redacted], [redacted] ____.___.sg

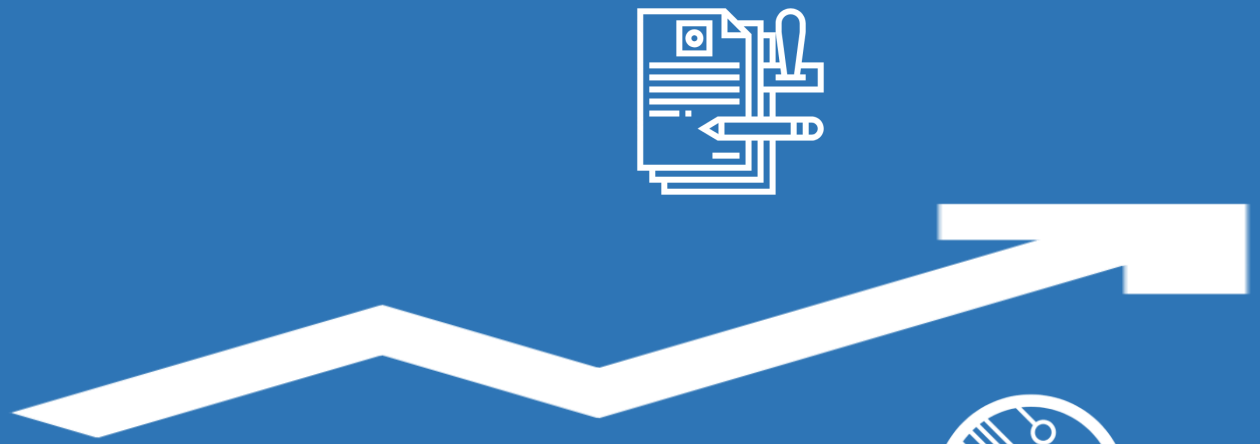
– Advisor, Cortex Insight www.cortexinsight.com
– Advisor, Maddox Technologies www.maddox.sg

What I Used to Do / am Doing

Research
& Development

Cybersecurity
Operations

Governance, Risk,
Compliance (GRC)

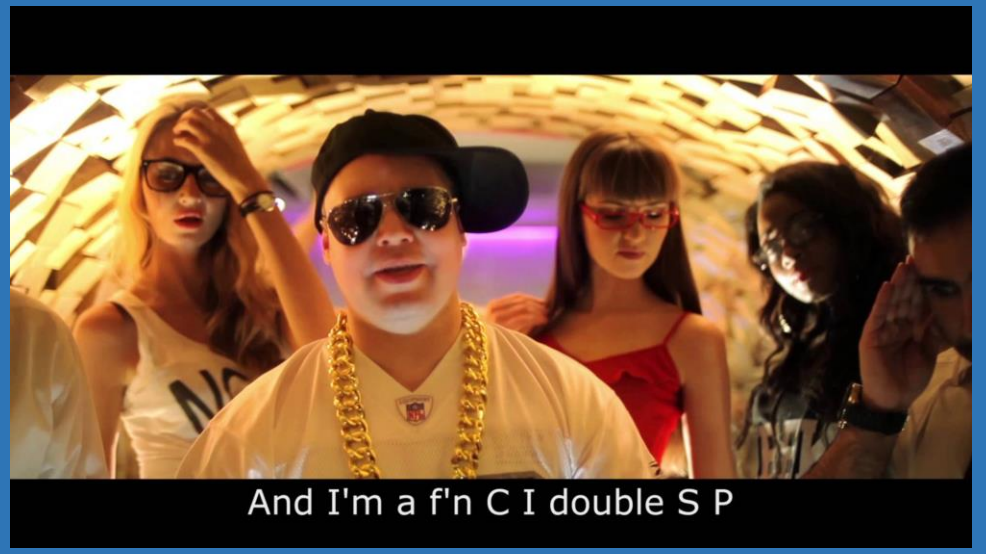


Textbook: Honeypot – The Holy Grail

– Confidentiality, Integrity, Availability
– People, Process, Technology

– Encryption
– Firewall
– Intrusion Detection System (IDS)
  – Network & Host
– Antivirus

– HONEYPOT



Host Unknown: I'm a C I Double S P
https://youtu.be/whEWE6WC1Ew

“We need to build a honeypot!”

~~Why You Don't Need Honeypots~~

Honeypot is …

“Information system resources which has **no production values**.
Its values lies in unauthorised or illicit use of that resource.
Its **values lies in being probed, attacked, or compromised**.”

Canary / Detection

Decoy / Deception

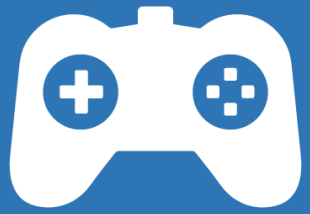
- Architecture
- Analytics
  - Malware, Network, Logs
- Forensics
- Data Science
  - Visualisation No, I'm not talking about pew pew

- Theoretical Skills
- Technical Skills
- Operations Skills

Proof-of-Concept (Theoretical)

DevSecOps Approach to Managing Honeypots

Cyber Threat Intelligence



Honeypots & Game Theory

Attack Model & Deception

Tools Development

IoT Honeypots

State of the Internet Cybersecurity Survey Tool

Web Browser Honeyclient

Sinkhole Honeypot

Exploitation & Contextualisation of Data from Honeypots into Useful Intelligence & Sharing of Cyber Threat Landscape

Threat Intelligence

“**Information** that is **contextualised** and relevant to an organisation or group’s operational environment and their needs, allowing them to properly understand their adversaries and the risks that they may face, in turn **enabling them to act and make better decisions** to secure their operational environment.”

Threat Information v. Intelligence

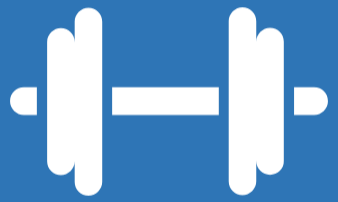
Indicators of Compromise (IOCs)

Tactics, Techniques & Procedures (TTPs)

Threat Alerts

Threat Reports

Discerning Cyber Kill Chain



Strengthen Defences

Improve Incident Response

I4RMHONEY Framework

Objectives

Understanding Adversaries

Understanding Threat Landscape

Improve Defences

Artefacts

Data

Information

Intelligence

Sources of Data

Logs

Correlation Mechanisms

Process & Registry Monitors

Intrusion Detection Systems

Firewall

Production & Sharing of Information & Intelligence

Report

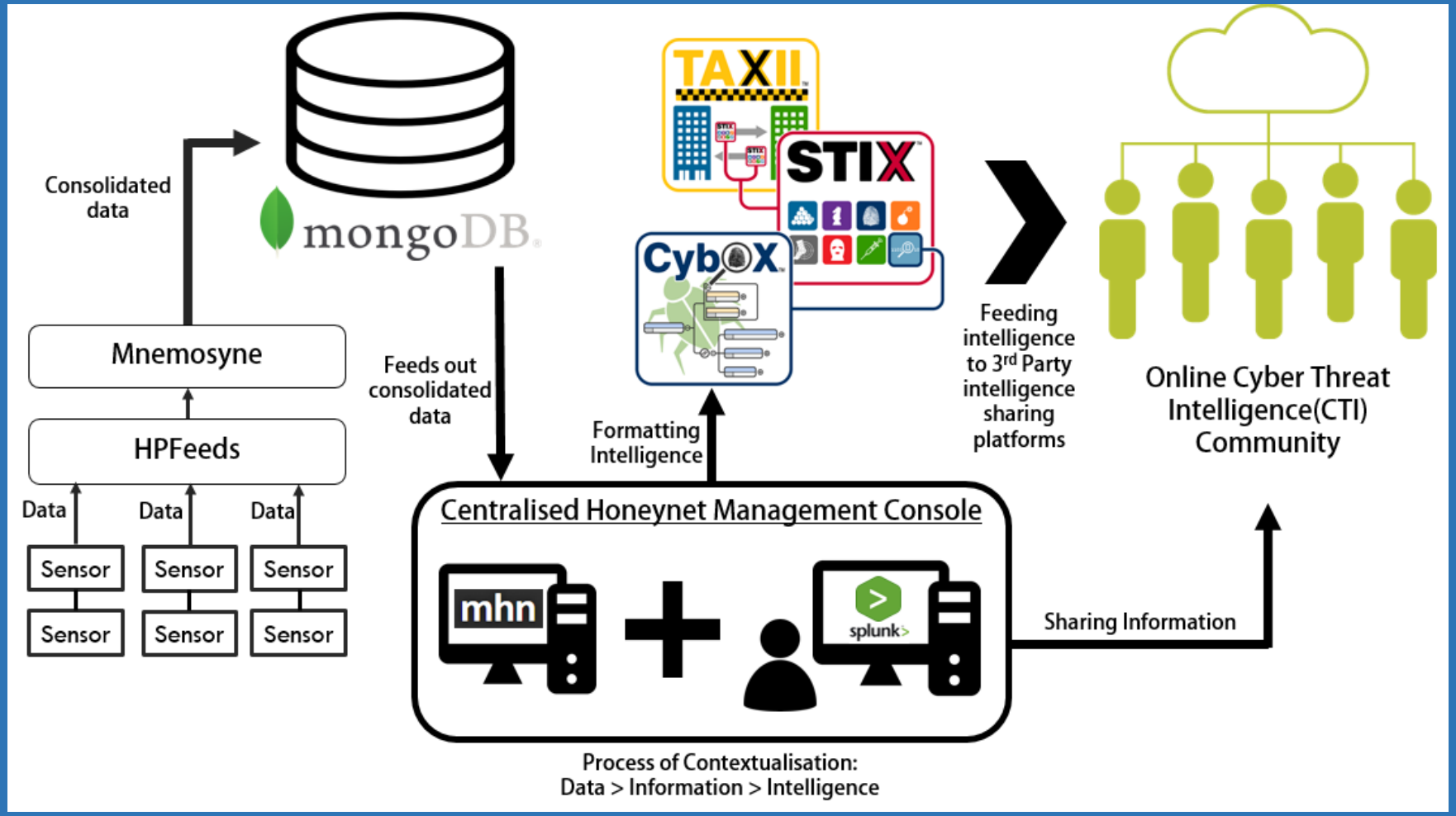
Observable

Indicator

THREAT CONNECT™

MISP Threat Sharing

I4RMHONEY in Action



Honeypots & Game Theories

Application of Game Theory

Data Control

Data Capture

Data Collection

Data Analysis

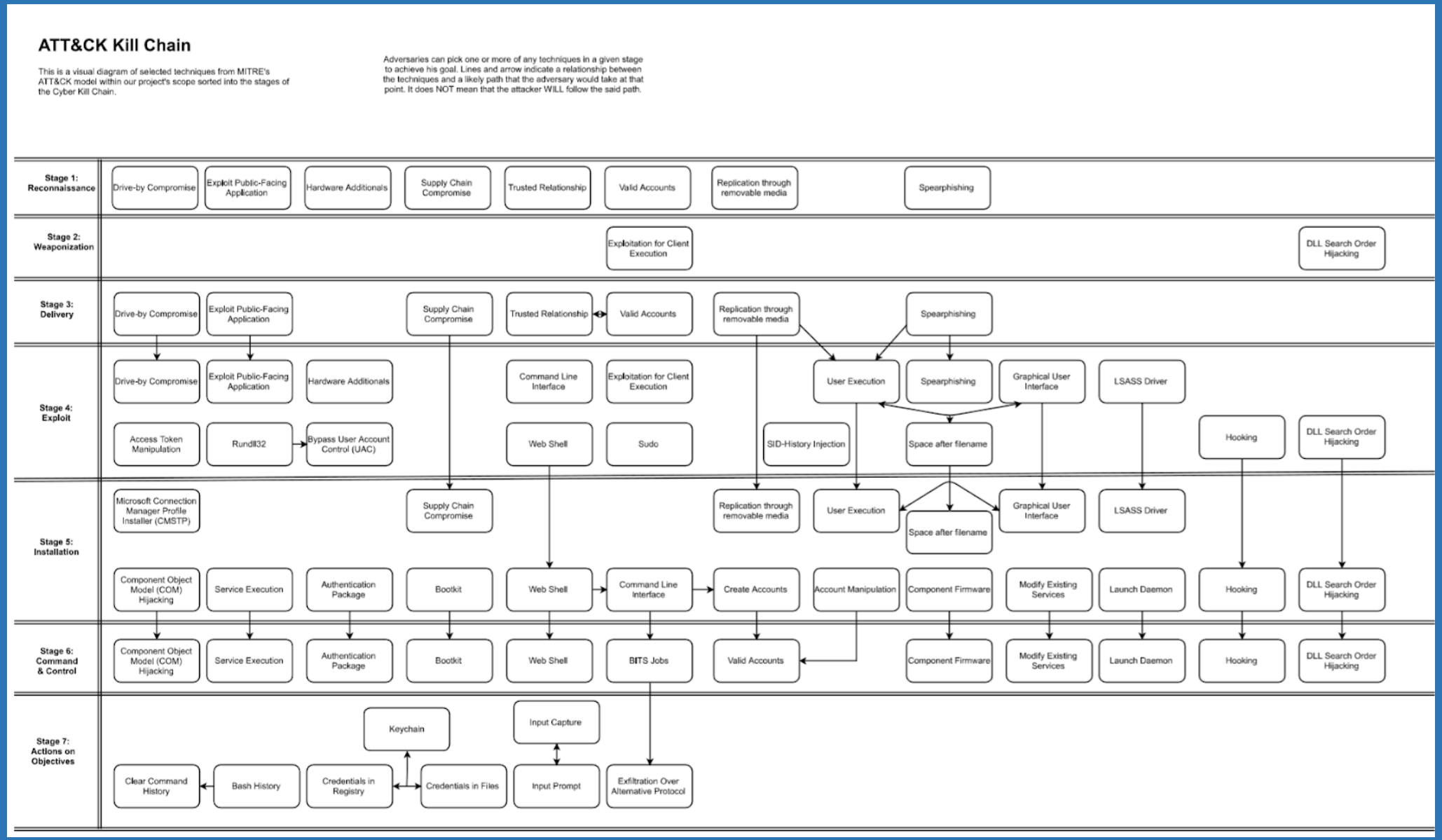
Mixed Strategy Nash Equilibrium

– Strategies are chosen with a probability

– Sequential Move Games

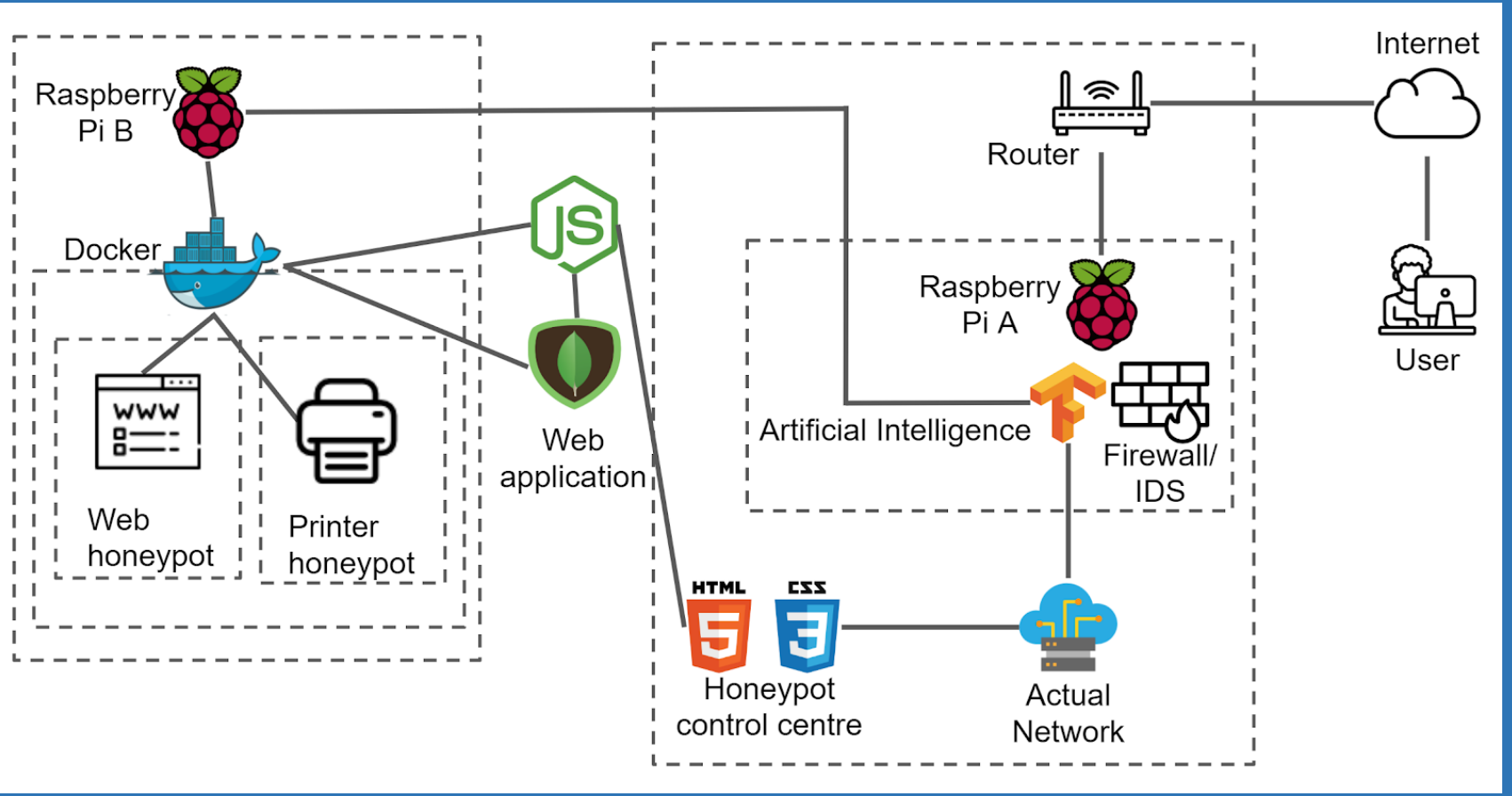
Attack Model & Deception

ATT&CK Kill Chain



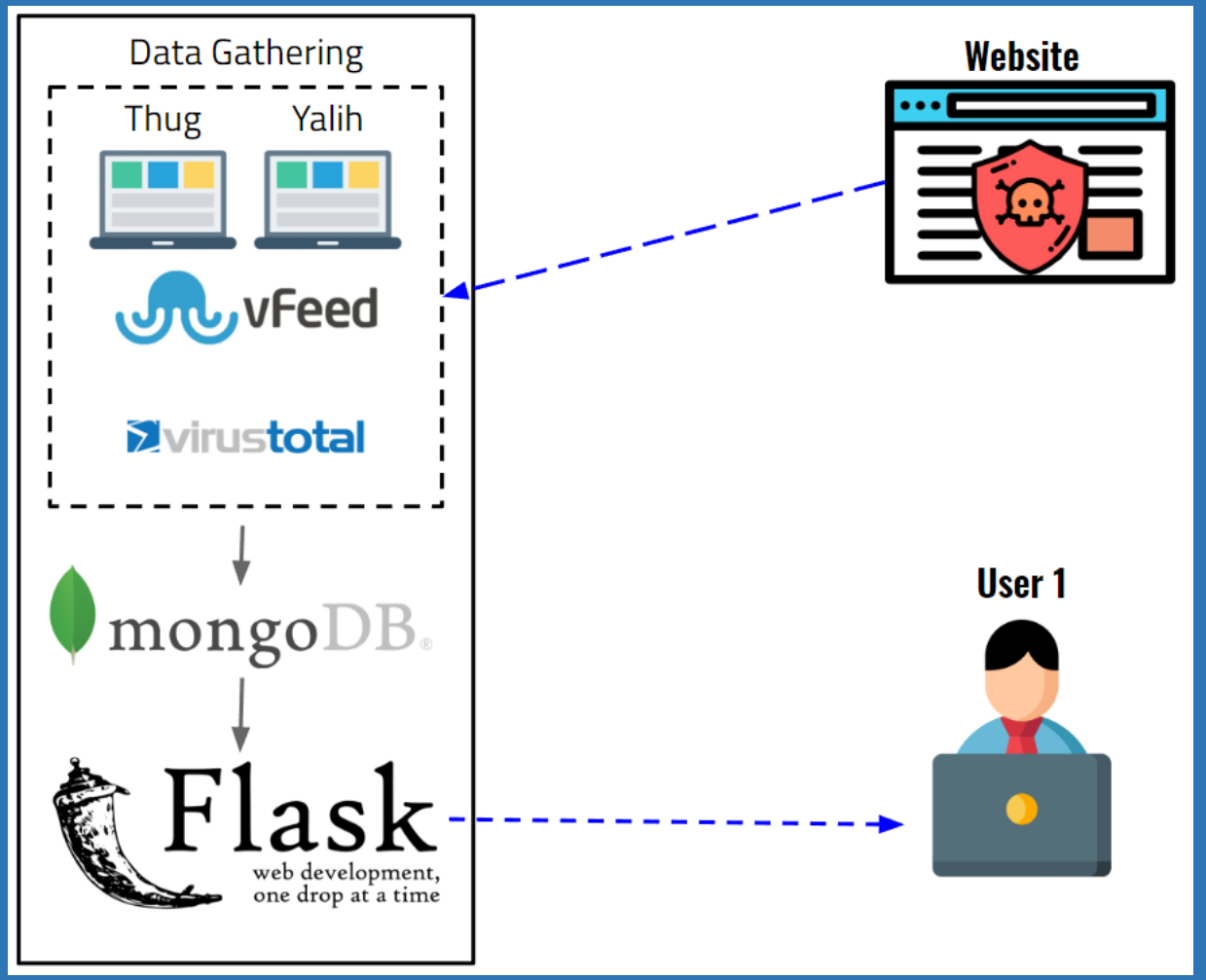
IoT Honeypots

BeeTrace


Raspberry
Pi B
Docker
WWW
Web
honeypot
Printer
honeypot
Web
application
Router
Internet
User
Raspberry
Pi A
Artificial Intelligence
Firewall/
IDS
HTML
CSS
Honeypot
control centre
Actual
Network

Web Browser Honeyclient

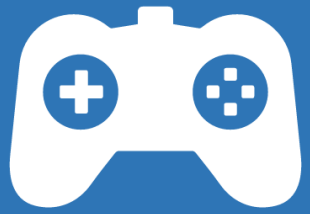
Beeware


Data Gathering
Thug
Yalih
vFeed
virustotal
mongoDB
Flask
web development,
one drop at a time
Website
User 1

Proof-of-Concept (Theoretical)

DevSecOps Approach to Managing Honeypots

Cyber Threat Intelligence



Honeypots & Game Theory

Attack Model & Deception

Tools Development

IoT Honeypots

State of the Internet Cybersecurity Survey Tool

Web Browser Honeyclient

Sinkhole Honeypot

Talent for Hire

Jordan Yeo
Bryan Lim
David Choong
Goh Soon Teck

Jared Tan
Terence Chan
Muhammad Fairuz
Lim Chun Ann
Juve Wong

Benjamin Khong
Chew Tian-Le
Aloysius Lee
Yea Jie Xuan
Koh Tar Yen

Teng Yan Hao
Chua Yi Xuan
Ong Chee Xian
Chen Yan Jiun
Yap Bing Xun

Daryl Lim
Lim Chun Yu
Chng Wei Cheng
Jonathan Wong
Joshua Soh

Darren Ang
Chua Ming Kiang
Leyong Lee
Chen QiuRong

Hong Shibao
Sng Yong Chai
Siti Nur Hadirah
Nadiah

Ng Zi Kai
Leonard Leow
Alison Mak
Barnabas Tan

Conclusion

Honeypot is …

“Information system resources which has **no production values**.
Its values lies in unauthorised or illicit use of that resource.
Its **values lies in being probed, attacked, or compromised**.”


"That's all Folks!"


AND THAT'S MY PRESENTATION. WHAT DO YOU THINK?
Dilbert.com @ScottAdamsSays
I DIDN'T UNDERSTAND A WORD OF IT.
10-18-17 © 2017 Scott Adams, Inc./Dist. by Andrews McMeel
YOU COULD HAVE MEN-TIONED THAT AN HOUR AGO.
DIDN'T WANT TO BE RUDE.