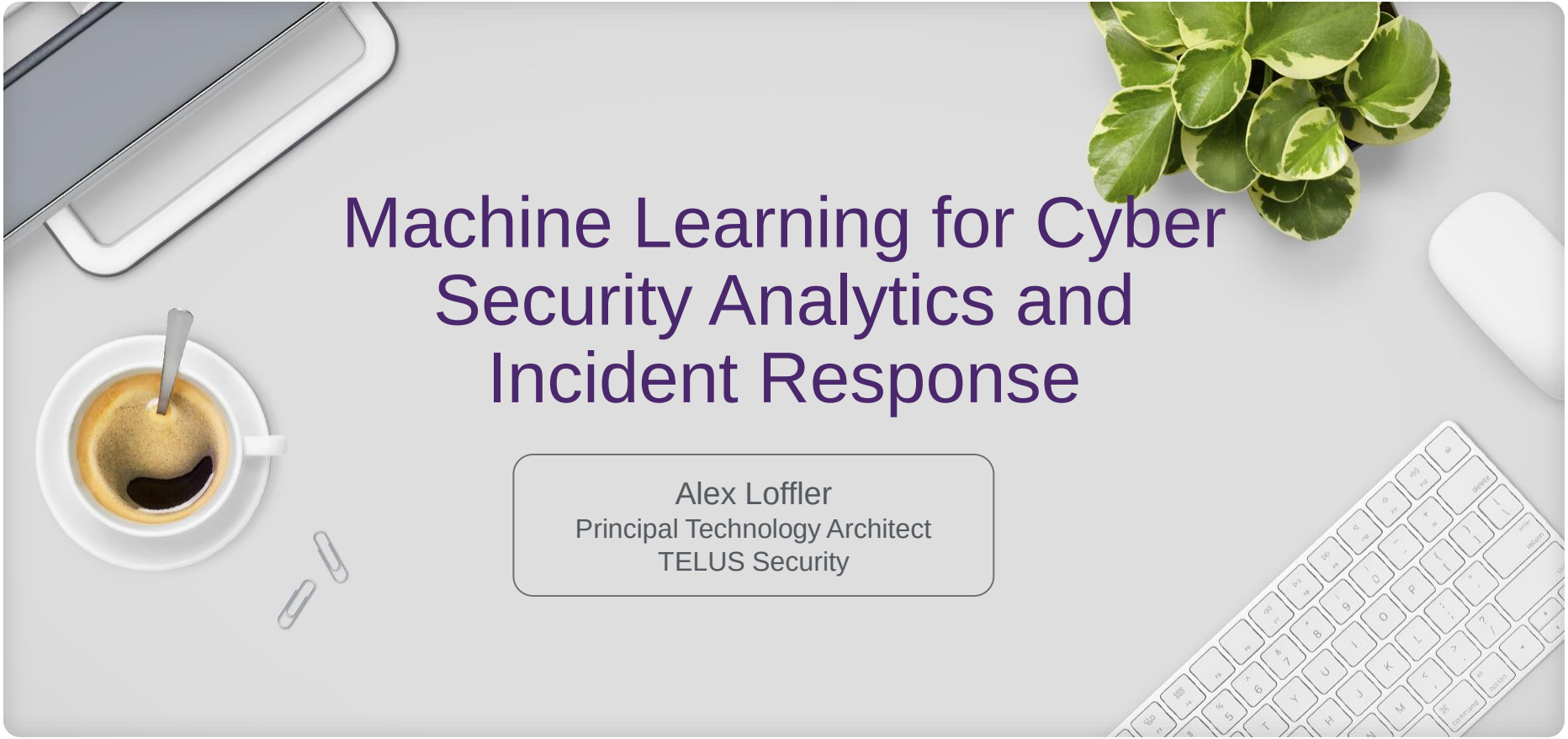


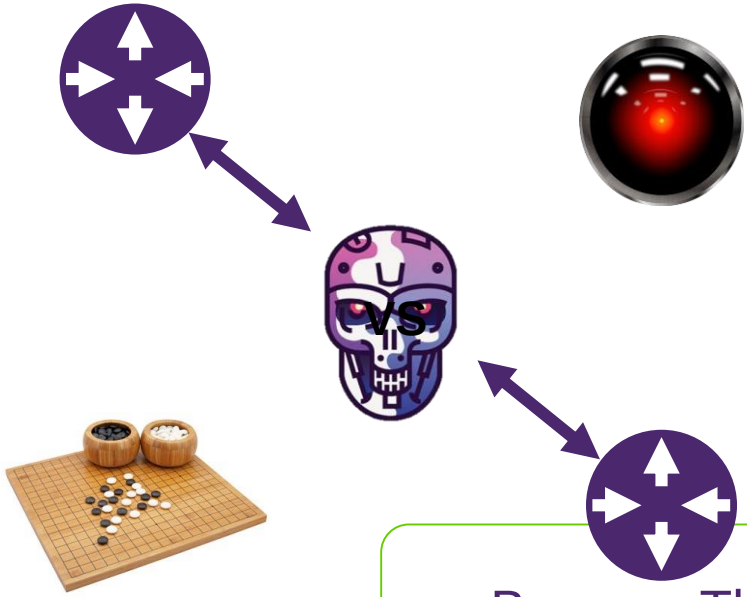
Machine Learning for Cyber Security Analytics and Incident Response

Alex Loffler
Principal Technology Architect
TELUS Security

February 9, 2018

TELUS Business

Broad AI vs Narrow AI



Broad AI

- What every CISO wants
  - Asimov, HAL-9000, Skynet

Narrow AI

- What AI can deliver (today)
  - A step-change in Tool Intelligence

Beware: The Hype Cycle!

TELUS Business

Machine Learning vs Deep Learning

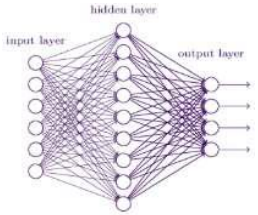
Machine Learning

Input

Log Events
Flows/PCAP

Feature Extraction

Classification



Output

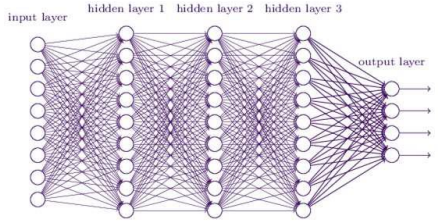
Good or Bad

Deep Learning

Input

Log Events
Flows/PCAP

Feature Extraction & Classification



Output

Good or Bad

There's a problem: Ground Truth

input = 

output = 'Bus' | 'Not Bus'

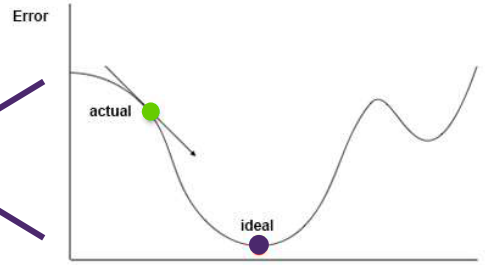
f() =  ?

Bus Classifier

output = f(input)

0 = | f(input) – output |

Error = | f(input) – output |



Incident Classifier

input = ?

output = 'Good' | 'Bad'

f() =  ?

What is our input?

- A single event (aka 'the smoking gun' event)?
- A set of events/conditions?
- Some complex sequence of events?

We need lots of event level examples of both 'good' and 'bad' event sequences aka Ground Truth

Some early results

Incident Response Feedback Loop (Gathering Ground Truth)

- Gather feedback (true/false positives) from the IR team
- Maintain the links between inputs, features and incidents

Mitigation Recommendation

- Gather historical mitigation actions for future recommendations
- Improves response speed, consistency & accuracy

Active Defense

- As performance increases, take the human out of the loop

Event classification without parsers

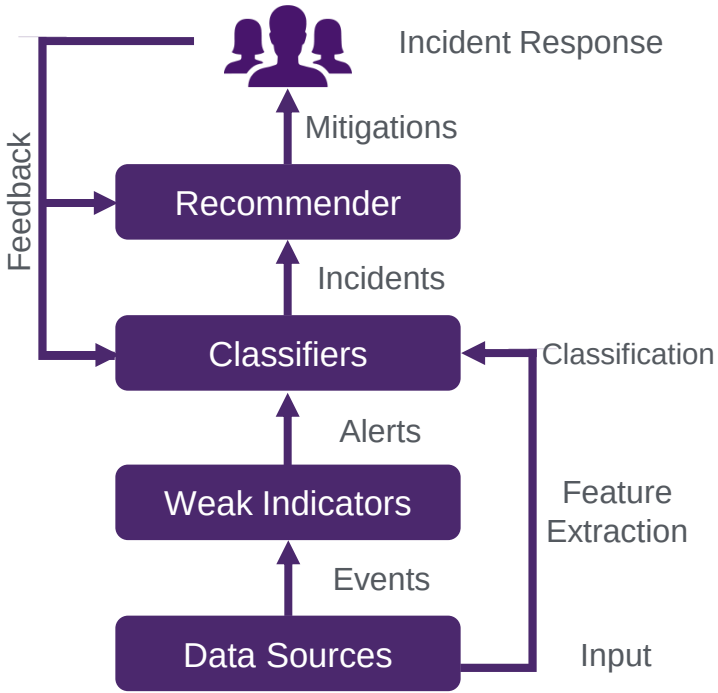
- >80% accuracy rate across >100 device types

Predicting victims of cyber-attack

- >74% accuracy with <4% error rate

Command history analysis

- >85% identification of individual user

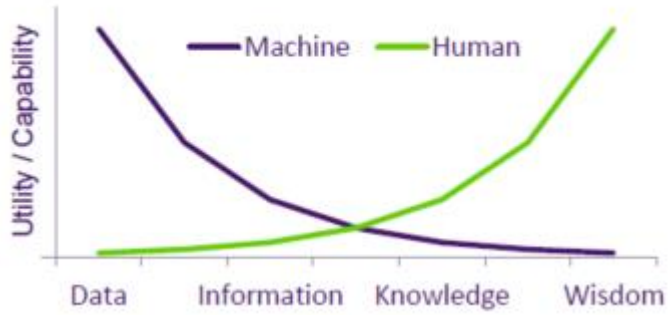


TELUS Business

Conclusions

Narrow AI

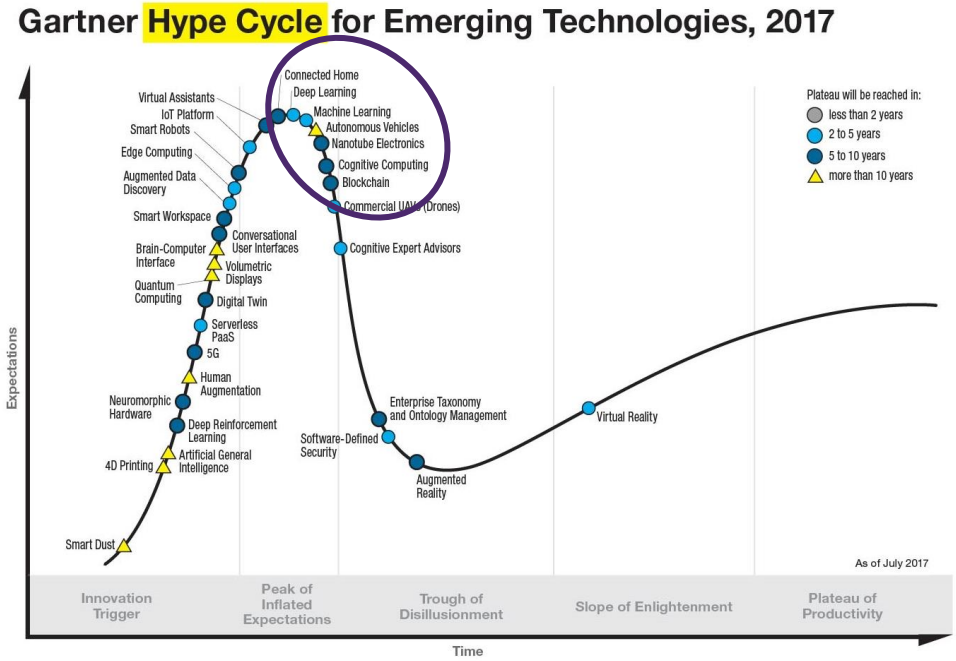
- Is disrupting the cyber security industry
- Is being used by both sides
- Acts as a force multiplier
  - As event volumes & data sharing standards evolve
- Will augment but not replace the Incident Responder



TELUS Business


TELUS
Business

Beware: the Hype Cycle



Gartner Hype Cycle for Emerging Technologies, 2017

Security analytics: Industry stats

88% Utilize analytics to some degree in their prevention programs

33% Integrate analytics functions with SIEM systems for incident response

66% Utilize in-house developed analytics systems of various types

4% Consider their analytics automated (10% “highly” automated)

44% Able to quantify improvements in detection & response through the use of analytics

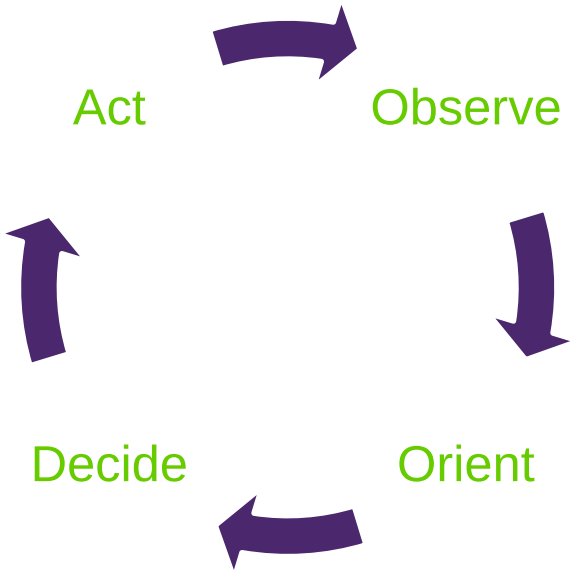
TELUS Business

Incident Response: The OODA Loop

Execution Phase

Act
- Mitigation & Remediation
- Deny, Disrupt, Degrade, Deceive
- Asset Inventory

Decide
- Triage (Crown Jewels)
- Unplug vs Observe & Learn
- Major Incident Declaration



Intelligence Phase

Observe
- Network & Platform Topology
- Log & Network Telemetry
- Asset Inventory

Orient
- Threat Modelling
- Baselining & anomaly detection
- Correlation/application of Threat Intelligence

OODA Loop – Developed by military strategist and United States Air Force Colonel John Boyd

TELUS Business


TELUS
Business