

5th HVM New Materials Conference Summit Cambridge, UK 6-7 November 2019 <u>www.cir-strategy.com/events</u>

Implementing AI and Machine Learning to Support Real-Time Monitoring and Decision Making for IT and OT

Tarne Fidler Industrial Cyber Security Manager

Company Overview



World-leading artificial intelligence for cyber defense

Creator of autonomous response technology

AL CNBC DISRUPTOR 50

FAST@MPANY

THF WORLD'S

COMPANIES 2018

OARKTRACE

TIMES

1000 Europe's Fastest FINANCIAI **Growing Companies**

Headquartered in San Francisco and Cambridge, UK









OT Security Challenge





The Need for Al



- Industrial environments are highly bespoke
- Threats are unpredictable and can't be predefined
- Needs to learn continuously without maintenance
- Baselining lacks context to tell good from bad
- Baselining can't detect existing compromise
- Need to correlate events to reduce number of alerts



Total Coverage for OT & IT



- OT and IT networks are increasingly connected
- o Industry 4.0 IoT and IIoT
- Attacks are hybrid and move between networks
- OT and IT security are only as good as the weakest part
- Security operations and management are converging
- Common security platform encourages skill sharing and reduces team silos



Thousands of Unknown Threats Caught Every Day

- Unusual connections between IT and OT
- Irregular inbound remote connectivity
- Internal reconnaissance
- PLC malfunction
- Advanced malware and ransomware
- Insider threats
- Hacked IoT devices
- Attacks on physical security, such as biometric scanners & badge readers

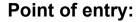


Compromised Equipment on Assembly Line





Industry: Food Manufacturing



Connected manufacturing devices



Apparent objective:

Take control of Industrial IoT to infiltrate information

- Unknown attacker targeted 0 devices on manufacturing assembly line to gain a foothold into the corporate network
- Al identified infected devices, 0 even though security team was unaware they were connected to Internet
- Darktrace identified several issues with the firewall that were then remediated



Thank You