

5th HVM New Materials Conference Summit
Cambridge, UK 6-7 November 2019

www.cir-strategy.com/events

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

Headquartered in **San Francisco and Cambridge, UK**

1.65 BN
VALUATION

3000
CUSTOMERS

1000
EMPLOYEES

40
OFFICES

Forbes 
THE
2018 Cloud100

 **DISRUPTOR/50**
2018

FT | **1000**
FINANCIAL | Europe's Fastest
TIMES | Growing Companies

FASTCOMPANY
**THE WORLD'S
MOST INNOVATIVE
COMPANIES 2018**

 **DARKTRACE**

OT Security Challenge



Critical
Systems



Difficult to
secure



Increasing
connectivity



Rising
threat

The Need for AI

- Industrial environments are highly bespoke
- Threats are unpredictable and can't be predefined
- Needs to learn continuously without maintenance
- Baselineing lacks context to tell good from bad
- Baselineing 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
- 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



Point of entry:

Connected manufacturing devices



Apparent objective:

Take control of Industrial IoT to infiltrate information

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

Thank You