Accelerating Responsible Innovation

John Weigelt
Chief Technology Officer
Microsoft Canada

@Thumbtackhead
2020 – Looking backwards
Fourth Session, 41st Parliament (2019)

OFFICIAL REPORT
OF DEBATES
(HANSARD)

Tuesday, October 22, 2019
Afternoon Sitting
Issue No. 278
ISSN 1499-2175
Mind the Tropes

There is no cloud
It’s just someone else’s computer
Machine learning applied to:
• Reduce manual effort
• Reduce wasted effort on false positives
• Speed up detection

5 billion threats detected on devices every month

+1B Windows devices updated & scanned
630 billion monthly authentications
18+ billion web pages scanned
470 billion e-mails analyzed

Unparalleled cybersecurity visibility and insight

The Microsoft Intelligent Security Graph
6.5 trillion diverse threat signals analyzed daily
Cybersecurity Reference Architecture

May 2018 - [https://aka.ms/MCRA](https://aka.ms/MCRA) | Video Recording | Strategies

This is interactive!

1. Present Slide
2. Hover for Description
3. Click for more information

Roadmaps and Guidance

1. Securing Privileged Access
2. Office 365 Security
3. Rapid Cyberattacks
   (Wannacrypt/Petya)

Office 365
- Secure Score
- Customer Lockbox

Dynamics 365
- Identity & Access
- Information Protection
- Conditional Access – Identity Perimeter Management
- Software as a Service
  - Azure Active Directory
  - Azure AD Identity Protection
  - Leaked cred protection
  - Behavioral Analytics
  - Azure AD PIM
  - Multi-Factor Authentication
  - Azure AD B2B
  - Azure AD B2C
  - Hello for Business
  - MIM PAM

Microsoft Azure
- Cloud App Security
- Azure Information Protection (AIP)
- Cloud App Security

Hybrid Cloud Infrastructure

On Premises Datacenter(s) 3rd party IaaS  Microsoft Azure

- Configuration Hygiene
- Just In Time VM Access
- Adaptive App Control

- Windows Server 2016 Security
- Window 10 + Just Enough Admin, HyperV Containers, Nano server, and more...

- Express Route
- Security Appliances
- Enterprise Security
- Network protection
- Credential protection
- Data protection
- Reputation analysis

- DLP
- Confidential Computing
- Azure Stack
- Azure Sphere

- Privileged Access Workstations (PAWs)
- Dynamic Access Workstations

Intranet Servers

- Secure Score
- Threat Analytics
- Windows Defender ATP

Intune MDM/MAM
- Unmanaged & Mobile Devices

Managed Clients
- System Center Configuration Manager

Client

Offices 365
- Dynamics 365

+ Monitor

- Data Loss Protection
- Data Governance
- eDiscovery

Compliance Manager

Security Development Lifecycle (SDL)

Trust Center

Intelligent Security Graph
## Getting Specific on AI

<table>
<thead>
<tr>
<th>Data</th>
<th>Math</th>
<th>Codifying</th>
<th>APIs</th>
<th>Packages</th>
<th>...</th>
<th>Application</th>
<th>Function</th>
<th>Business</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Context of collection</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Unrecognized Bias</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Synthetic data</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Temporal characteristics</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Streaming / static</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## Training

<table>
<thead>
<tr>
<th>Algorithms</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Algorithms</td>
<td></td>
</tr>
<tr>
<td>• Supervised</td>
<td></td>
</tr>
<tr>
<td>• Unsupervised</td>
<td></td>
</tr>
</tbody>
</table>

## Algorithms

<table>
<thead>
<tr>
<th>Algorithms</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Algorithms</td>
<td></td>
</tr>
<tr>
<td>• Locked</td>
<td></td>
</tr>
<tr>
<td>• Trained</td>
<td></td>
</tr>
<tr>
<td>• Evolving</td>
<td></td>
</tr>
</tbody>
</table>

## Security/privacy

<table>
<thead>
<tr>
<th>Safety/privacy</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Safety/privacy</td>
<td></td>
</tr>
<tr>
<td>• Model Theft</td>
<td></td>
</tr>
<tr>
<td>• Model Corruption</td>
<td></td>
</tr>
<tr>
<td>• Faulty training (synthetic data)</td>
<td></td>
</tr>
<tr>
<td>• Adversarial perturbation</td>
<td></td>
</tr>
</tbody>
</table>

## Automation

<table>
<thead>
<tr>
<th>Automation</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Automation</td>
<td></td>
</tr>
<tr>
<td>• Human in the loop</td>
<td></td>
</tr>
<tr>
<td>• Human over the loop</td>
<td></td>
</tr>
<tr>
<td>• Human out of the loop</td>
<td></td>
</tr>
</tbody>
</table>
Microsoft is optimistic about the future of AI systems empowering and augmenting individuals’ and organizations’ abilities to address broad societal issues such as poverty, security, justice, education and healthcare.
The Future Computed: Artificial Intelligence and its role in society
Ethical design and use of automated decision systems

03.100.02; 35.020; 35.240.01
AI Business School

AI Business School: Lead with confidence in the age of AI

Learning paths

Define an AI strategy to create business value
7 MODULES 3 HR 40 MIN  INTERMEDIATE
Learn More

Discover ways to foster an AI-ready culture in your business
6 MODULES 3 HR 10 MIN  INTERMEDIATE
Learn More

Identify guiding principles for responsible AI in your business
3 MODULES 55 MIN  INTERMEDIATE
Learn More
Innovate!