DFN Cloud Workshop
Microsoft

Helge Schroda
Cybersecurity Solutions Group

Susann Hüttner
Forschung und Lehre
54 Azure regions
Microsoft Intelligent Security Graph

Unique insights, informed by trillions of signals

- 400B emails analyzed
- 6.5T threat signals analyzed daily
- 200+ global cloud consumer and commercial services
- 5B threats detected on devices every month
- 450B monthly authentications
- 18B+ Bing web pages scanned
- 1B+ Azure user accounts
- Shared threat data from partners, researchers, and law enforcement worldwide

Outlook
OneDrive
Windows
Azure
Bing
Xbox Live
Botnet data from Microsoft Digital Crimes Unit
Microsoft accounts
Maximize Detection During Attack Stages

1. User browses to a website
2. Phishing mail opens attachment
3. Clicks on a URL
4. Exploitation & Installation
5. Command & Control
6. User account is compromised
7. Attacker attempts lateral movement
8. Privileged account compromised
9. Domain compromised
10. Attacker accesses sensitive data
11. Exfiltrate data

Azure AD Identity Protection
- Identity Protection & Conditional access
- Brute force account or use stolen account credentials

Cloud App Security
- Extends Protection & Conditional Access to other Cloud Apps

Azure Information Protection
- Label & Protect sensitive Files

Office 365 ATP
- Email and Content Protection

Microsoft Defender ATP
- Endpoint Protection

Azure ATP
- Identity protection

Azure ATP
- Identity protection

Microsoft Defender ATP
- Endpoint Protection
Cloud is a Security Imperative
**The deepest and most comprehensive compliance coverage in the industry**

<table>
<thead>
<tr>
<th>GLOBAL</th>
<th>ISO 27001</th>
<th>ISO 27018</th>
<th>ISO 27017</th>
<th>ISO 22301</th>
<th>ISO 9001</th>
<th>SOC 1 Type 2</th>
<th>SOC 2 Type 2</th>
<th>SOC 3</th>
<th>CSA STAR Self-Assessment</th>
<th>CSA STAR Certification</th>
<th>CSA STAR Attestation</th>
</tr>
</thead>
<tbody>
<tr>
<td>US GOV</td>
<td>FedRAMP</td>
<td>FedRAMP</td>
<td>DoD DISA SRG Level 2</td>
<td>DoD DISA SRG Level 4</td>
<td>DoD DISA SRG Level 5</td>
<td>NIST</td>
<td>FIPS 140-2</td>
<td>Section 508 VPAT</td>
<td>ITAR</td>
<td>CJIS</td>
<td>IRS 1075</td>
</tr>
<tr>
<td>INDUSTRY</td>
<td>PCI DSS Level 1</td>
<td>CDSA</td>
<td>MPAA</td>
<td>FACT UK</td>
<td>Shared Assessments</td>
<td>FISC Japan</td>
<td>HIPAA / HITECH Act</td>
<td>HITRUST</td>
<td>GxP 21 CFR Part 11</td>
<td>MARS-E</td>
<td>IG Toolkit UK</td>
</tr>
<tr>
<td>REGIONAL</td>
<td>Argentina PDPA</td>
<td>EU Model Clauses</td>
<td>UK G-Cloud</td>
<td>China DSCP</td>
<td>China TRUCS</td>
<td>Singapore MTCs</td>
<td>Australia IRAP/CCSL</td>
<td>New Zealand GCEO</td>
<td>Japan My Number Act</td>
<td>ENISA</td>
<td>Japan CS Mark Gold</td>
</tr>
</tbody>
</table>