Incorporating Security Intelligence and Automation Into Digital Transformation

Chris Raschke
Advanced Security Architecture – Global Black Belt

Email: chris.raschke@microsoft.com
LinkedIn: www.linkedin.com/in/raschkec
Twitter: @raschkec
Agenda

• Industry trends, Innovations, and Investments
• Notable data breaches, incidents, and attacker techniques, tactics, and procedures (TTPs)
• How are others Evolving Security with the Cloud?
Industry trends, innovations, and investments
Industry trends

Cloud solutions are generally trusted by most companies.

Traditional cybersecurity vendors are struggling.

Identity is a key battleground with intense competition from Okta and others.

Cloud solution providers are investing heavily in security and looking to seek market dominance.
Talent Shortages Exacerbate Cyber Risk

• **1.5 million** unfilled cybersecurity professionals by 2020
• Burnout amongst cybersecurity professionals is extremely high
Major regulatory and legal trends
GDPR gets its teeth

- British Airways faces $183 million fine
- Marriott faces $123 million fine
Notable data breaches, incidents, and attacker techniques, tactics, and procedures (TTPs)
2019
Verizon Data Breach Report

• 52% of breaches featured hacking
• 33% included social attacks
• Errors were causal events in 21% of breaches
• 32% of breaches involved phishing
• 29% of breaches involved use of stolen credentials
• 56% of breaches took months or longer to discover
Microsoft Security Intelligence Report

• Cloud weaponization scenarios on the rise
• Cryptocurrency mining on the rise
• Software supply chains at risk
• Phishing continues to be the preferred attack vector

Source: https://www.microsoft.com/securityinsights/
Timeline of supply chain attacks

2017
- **MAR**: Ask Partner Network (APN) compromised
- **JUN**: Petya ransomware outbreak
- **MAY**: 2 incidents: Operation WilySupply & compromised DVD app for macOS
- **JUL**: ShadowPad backdoor

2018
- **SEPT**: CCleaner compromised
- **OCT**: Compromised media app for macOS
- **MAR**: Dofoil campaign
- **JUL**: Compromised supply chain within a supply chain
- **AUG**: Compromised remote support program
- **OCT**: Compromised hosting control panel
Common attacks against cloud resources

- Exposed endpoints
- Weak passwords
- Exposed and/or stolen credentials
- Improper handling/storage of data

Root cause
Misconfiguration
First American Corporation

850 million files, dating back 16 years, available to view online without authentication
Password spray attacks against cloud services
Ransomware continues to wreak havoc

- City of Riviera Beach, Florida
Nation-states

- Global conflicts and disputes have the potential to accelerate cyber attacks and espionage
- MSTIC Holmium Activity Alert
  - aka APT 33
Attackers Continue to Evolve Techniques

```vba
DTt = Format(Date, "Lon" & "g D" & "ate")
End Function
Function co()
  coo = "MsgBox ("Your Interest to Date is " & int now & ".")": co = Cells
End Function
Function SediR()
  fbb = False
  remmi = "If (pFeatureLayer.FeatureClass.ShapeType = esriGeometryPolygon) Then"
  misR = 19
  trel = ""
  For u = 1 To 4
VBA crafted to evade ML classification engines
```
Evolving Security with Cloud
The intelligent, connected cloud introduces both opportunity and risk.

- 81% of hacking breaches leverage stolen/weak passwords. (Verizon 2017 Data Breach Investigation Report)
- 1,181 cloud apps in the avg. large enterprise, 61% is shadow IT. (Microsoft 2018)
- 90% of the world’s data has been created in the last two years. (IBM Marketing Cloud, “10 Key Marketing Trends For 2017”)

Technology has changed the way we do business. Protecting company assets requires a new approach.
Complexity is the enemy of intelligent security

70 from 35
Security products Security vendors
Is the average for companies with over 1,000 employees

$1.37M
On average that an organization spends annually in time wasted responding to erroneous malware alerts

1.87M
Global cybersecurity workforce shortage by 2022

Nick McQuire, VP Enterprise Research CCS Insight.

“The Cost of Insecure Endpoints” Ponemon Institute© Research Report, June 2017

Global Information Security Workforce Study 2017
# Cloud Redefines Security Responsibilities

<table>
<thead>
<tr>
<th>Responsibility</th>
<th>SaaS</th>
<th>PaaS</th>
<th>IaaS</th>
<th>On-prem</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data governance &amp; rights management</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Client endpoints</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Account &amp; access management</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identity &amp; directory infrastructure</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network controls</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operating system</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical hosts</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical network</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical datacenter</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Always retained by customer

### Varies by Service Type

### Transfers to Cloud Provider
The ‘best-of-breed’ model is broken

- Complex and expensive integration
- Constant training on new tools
- Too many alerts to handle
- Gaps in visibility
Threat Protection

Information Protection

Identity & Access Management

Security Management

Data is your most important company asset

Correlate threat information and automatically respond

Optimize with security insights and configuration tools
Secure identities to reach zero trust

Help stop damaging attacks with integrated and automated security

Protect sensitive information anywhere it lives

Strengthen your security posture with insights and guidance

Intelligent security for the modern workplace
Protection across the attack kill chain

Office 365 ATP
Malware detection, safe links, and safe attachments

Phishing mail
Open attachment
Click a URL
Browse to a website

Exploitation & Installation
Command & Control

Brute force account or use stolen account credentials

User account is compromised
Attacker attempts lateral movement
Privileged account compromised
Domain compromised

Microsoft Defender ATP
Endpoint Detection and Response (EDR) & End-point Protection (EPP)

Exfiltrate data
Attacker accesses sensitive data

Azure AD Identity Protection
Identity protection & conditional access

Microsoft Cloud App Security
Extends protection & conditional access to other cloud apps

Attacker collects reconnaissance & configuration data

Office 365 ATP
Malware detection, safe links, and safe attachments

Azure AD Identity Protection
Identity protection & conditional access

Microsoft Cloud App Security
Extends protection & conditional access to other cloud apps

Azure Sentinel
SIEM + SOAR

Azure ATP
Identity protection

Azure ATP
Identity protection

Microsoft Defender ATP
Endpoint Detection and Response (EDR) & End-point Protection (EPP)
Demo
Session takeaways

• **Phishing** continues to be the primary method for gaining a foothold by attackers

• A significant portion of attacks involve the use of compromised credentials, or successful attacks against weak passwords

• Breaches continue to take months to identify

• Lack of trained and qualified security professionals requires a strategy shift

• Subscribe to and regularly read the MSFT Security Blog and MSFT threat intel

• **Best of Breed** model is broken – must shift to cloud platform solutions.
Thank You!!!