

TURNING THE TABLES



Dean Iacovelli

Director, Secure Enterprise



Microsoft State and Local Government

deaniac@microsoft.com

Asymmetrical: this is not a fair fight

SLG 2nd lowest preparedness, 2nd most attacked by industry ₁

You are facing a profit-motivated human adversary

76% of breaches financially motivated ₂

They use your transparency against you

90% of attacks begin with phishing email ₃

Attacks are now automated, response is not

One bank: 62,000 devices encrypted in 1 hr by Petya ₄

You can't just throw people at the problem

1.8M global unfilled cyber jobs by 2022 ₅

Complexity is the chief enemy of security

Managing 20-30 tools = 5% alert investigation rate ₆

Breach costs can be enormous and are asymmetrical to org size

See OPM ₇

CYBERSECURITY BY THE NUMBERS

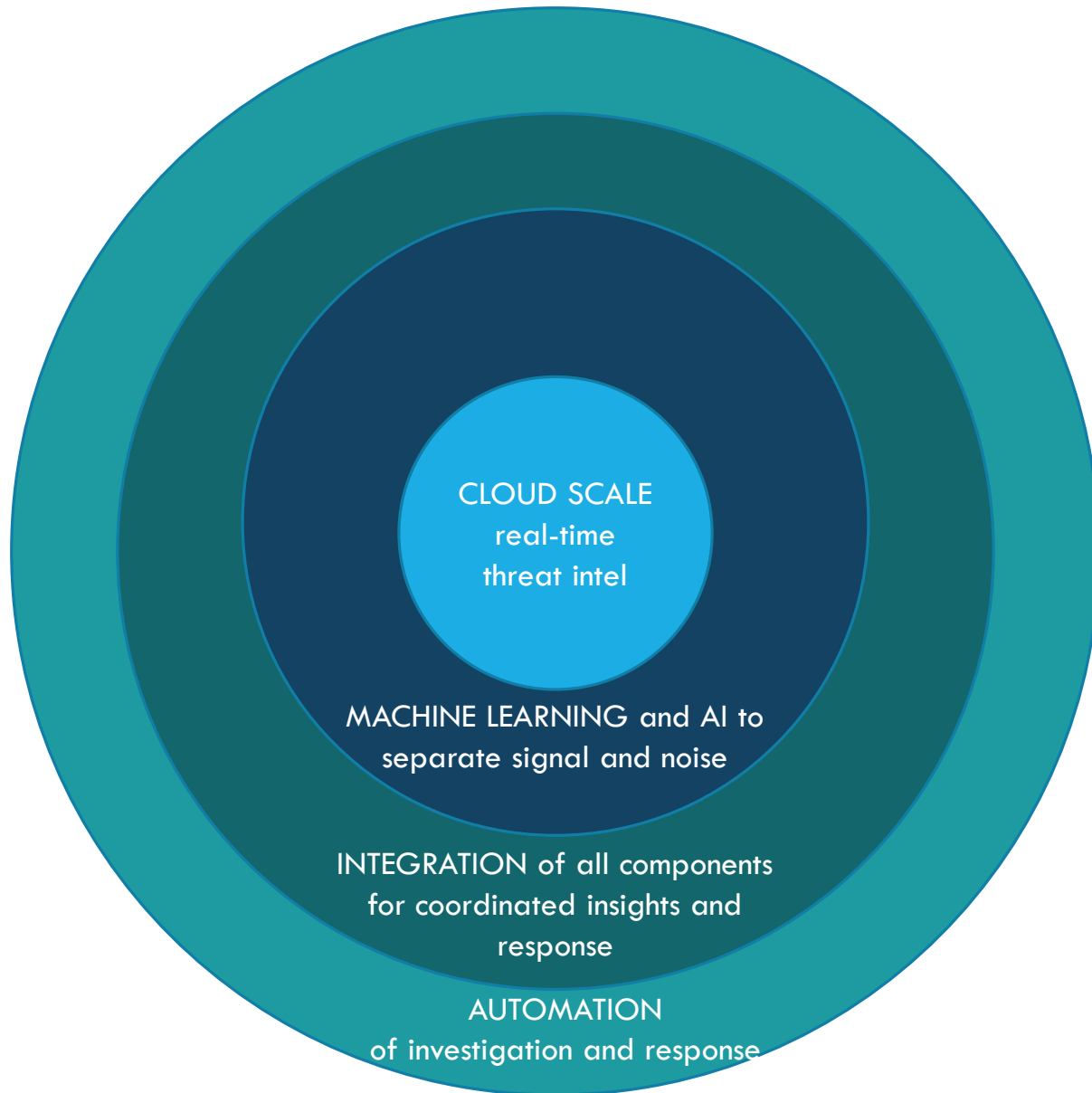
“Best of breed” approach can no longer keep up with rate and sophistication of attacks.

“Going it alone” as an individual org with individual org resources is a losing battle.

POTENTIAL CONCLUSIONS ?

Basically, all roads lead to **CLOUD** and **AUTOMATION**.

FOUNDATIONS OF A MODERN SECURITY PLATFORM



“By 2020, **30%** of security spending will be on vendors that provide an integrated platform approach to security”
– 2017 IDC FutureScape report

AN ARGUMENT FOR UTILITY COMPUTING IN THE CYBER FIGHT

Hyperscale cloud vendors will far outspend even the Fortune 5 on security because their business model is TRUST.

Radically different economics - customers get access to 1 B in cyber spend, only pay for a “slice”.

Move to cloud is part of a sound risk management strategy
— i.e. transferring risk

Cloud helps you stay continually patched and compliant

Certs AND a track record

TOP 10 THINGS YOU SHOULD DO RIGHT NOW

Action	How We Can Partner				
	Self-service	Fast Track	Premier	MCS	Partner
10. Deploy Azure Backup and Recovery services	●	●	●	●	●
9. Move doc stores to OneDrive for Business	●	●	●	●	●
8. Automate info protection and classification	●	●	●	●	●
7. Deploy Win 10 and Cred Guard to all clients.	●		●	●	●
6. Deploy Endpoint Protection with automated investigation/remediation.	●		●	●	●
5. Monitor and reduce time-to-patch	●		●	●	●
4. Deploy next gen Security Information and Event Management tools	●		●	●	●
3. Deploy behavior-analysis content scanning	●		●	●	●
2. Leverage Microsoft Secure Score best practices across Identity, Office 365, Windows clients and servers.	●		●	●	●
1. Deploy phishproof identities for all users, including Just-In-Time and Just-Enough admin accounts.	●		●	●	●

FINALLY, PLEASE REMEMBER...



BRAKES ARE WHAT ALLOW THE CAR TO GO FASTER.

Q & A

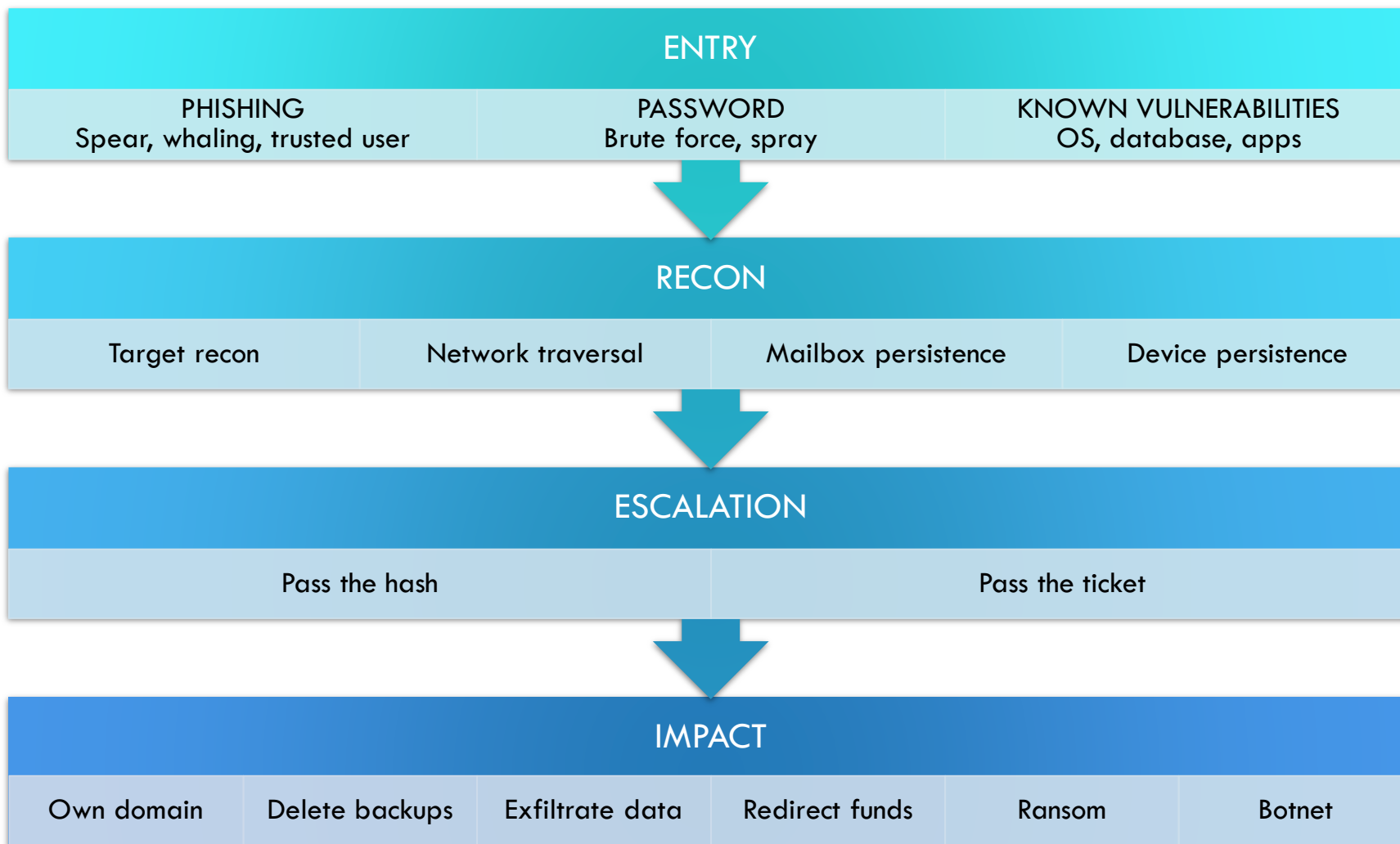
THANK YOU !

Dean Iacovelli
deaniac@microsoft.com



APPENDIX

“WHAT HAPPENED AT THE CITY OF XXX ?”



[Video](#)

INTELLIGENT SECURITY GRAPH

Our most unique global asset in the fight, informed by trillions of feeds. Machine learning helps sort the signal from the noise. This signal is leveraged across all of Microsoft's security services.

