Attack Surface Reduction rules…

your best ally against ransomware!

Ronny de Jong 🇳🇱
Security Technical
Specialist, Microsoft

Pim Jacobs 🇳🇱
Principal Consultant,
InSpark

10TH ANNIVERSARY EDITION

Experts Live Netherlands

Agenda

Introduction

Start with some humor 😃 Understanding the cybercrime economy and ruin their business model

Overview

Defending against ransomware: Moving beyond protection by detection

Proof is in the eating

Prevent common attack techniques used in ransomware attacks

Considerations & next steps

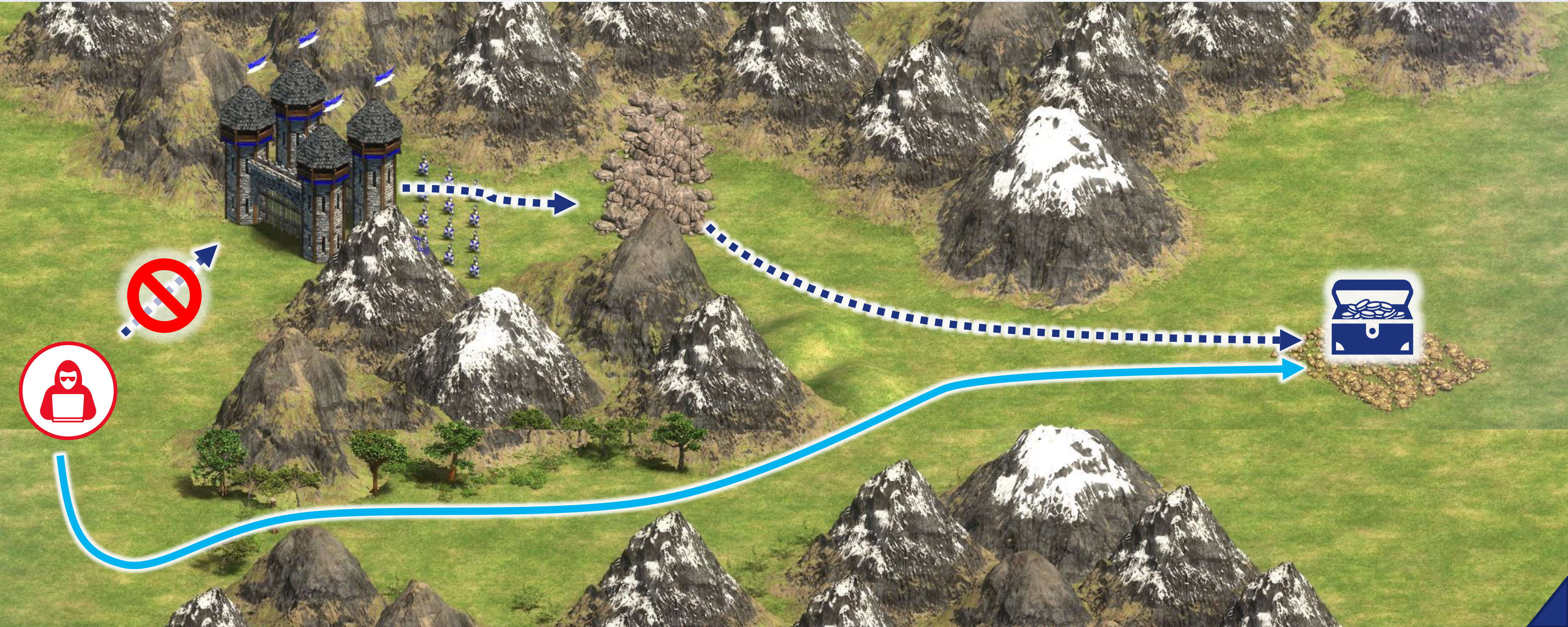
Tips & tricks to get you kick started

Questions

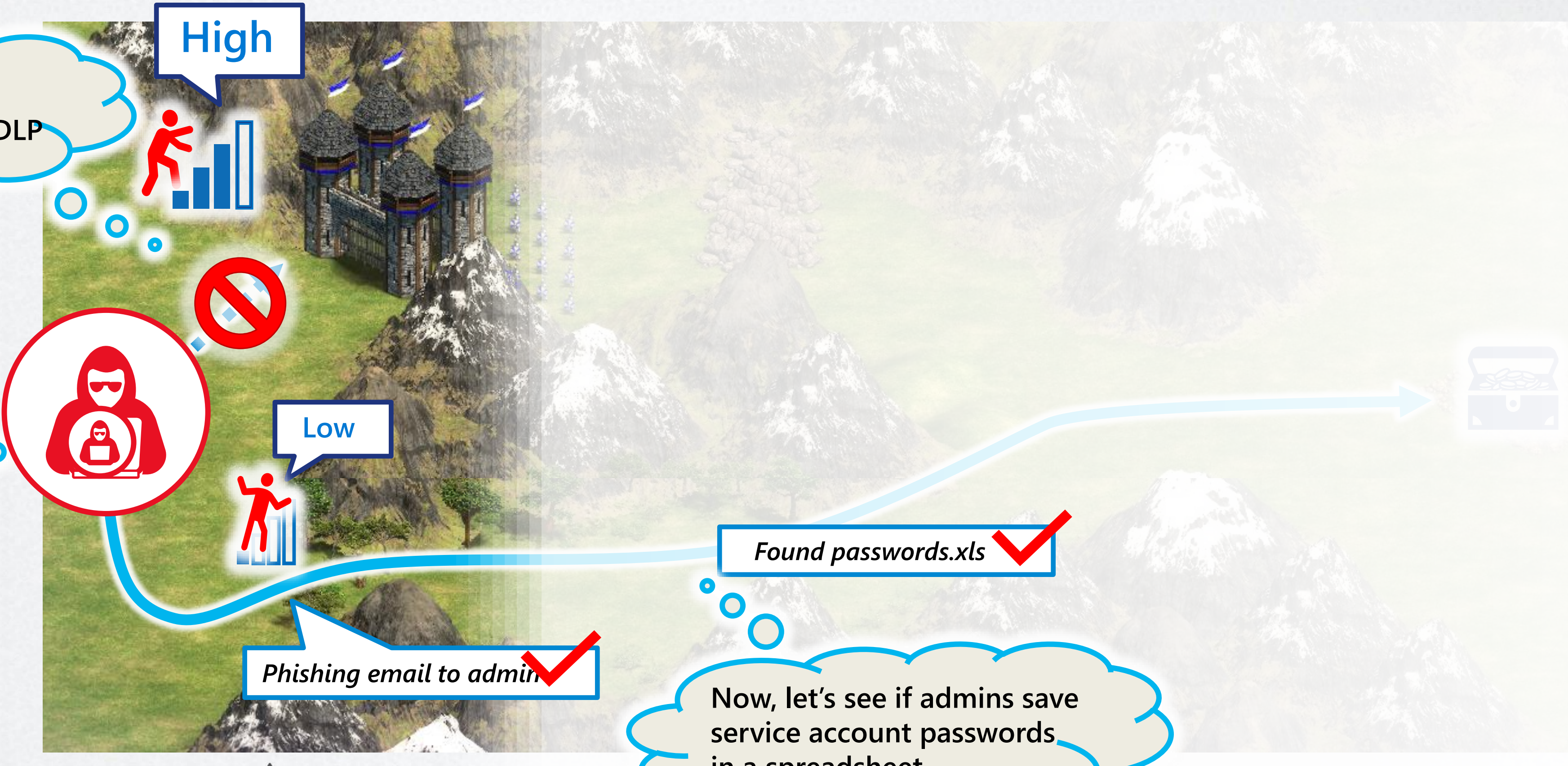
...and hopefully some answers 😉

SECURITY

Believing attackers will follow the planned path?



Attacker Perspective: shaped by experience & 'fog of war'



Looks like they have NGFW, IDS/IPS, and DLP

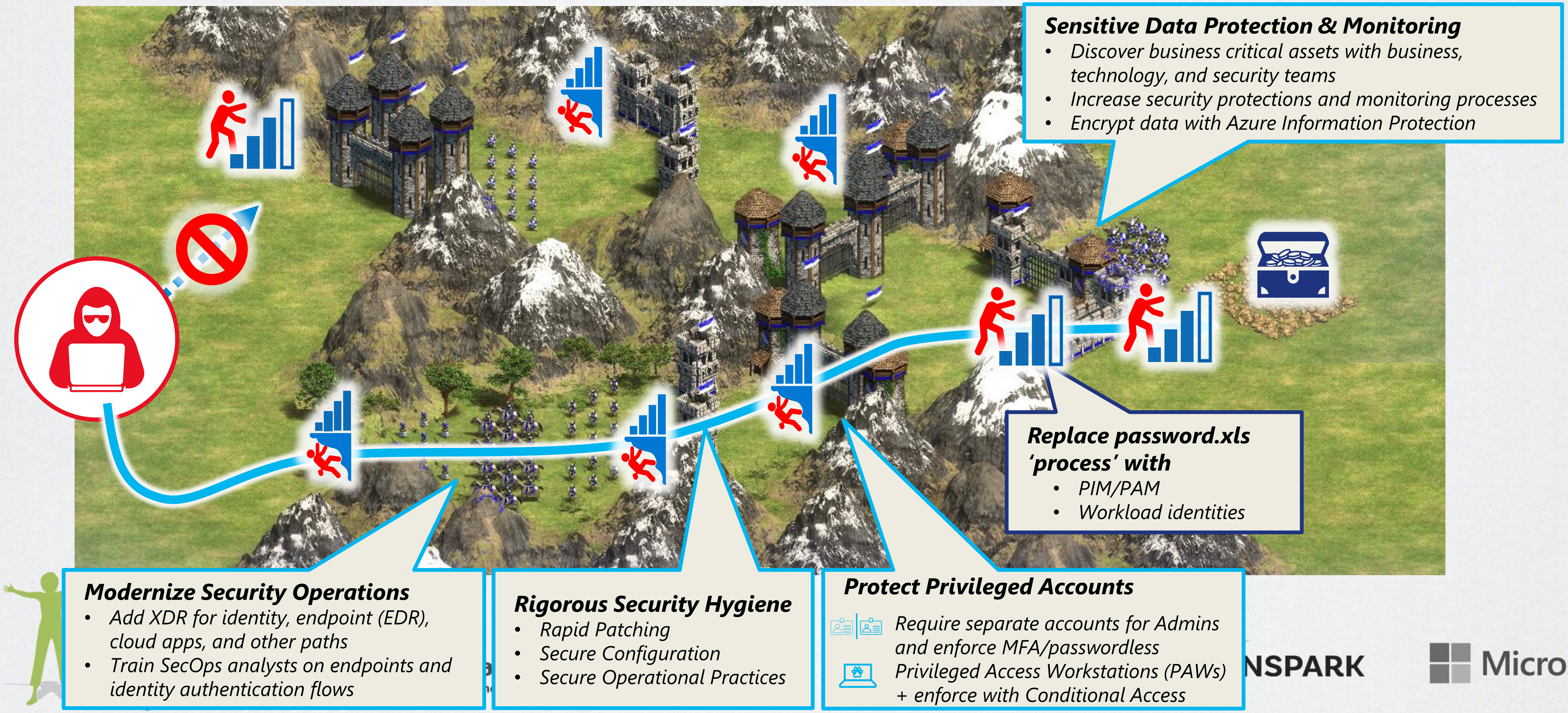
I bet their admins
1. Check email from admin workstations
2. Click on links for higher paying jobs

Phishing email to admin ✓

Found passwords.xls ✓

Now, let's see if admins save service account passwords in a spreadsheet…

Strategically position security investments



Sensitive Data Protection & Monitoring

- Discover business critical assets with business, technology, and security teams
- Increase security protections and monitoring processes
- Encrypt data with Azure Information Protection

Replace password.xls 'process' with

- PIM/PAM
- Workload identities

Modernize Security Operations

- Add XDR for identity, endpoint (EDR), cloud apps, and other paths
- Train SecOps analysts on endpoints and identity authentication flows

Rigorous Security Hygiene

- Rapid Patching
- Secure Configuration
- Secure Operational Practices

Protect Privileged Accounts

Require separate accounts for Admins and enforce MFA/passwordless

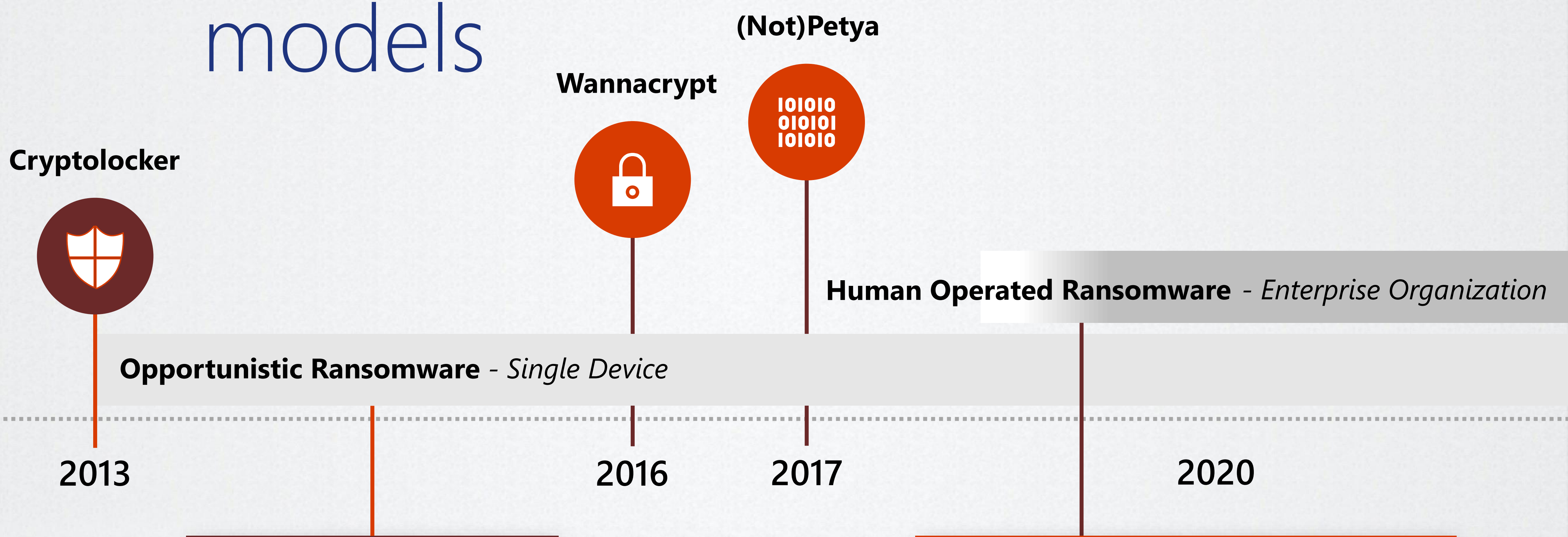
Privileged Access Workstations (PAWs) + enforce with Conditional Access

NSPARK

Microsoft

SECURITY

Evolution of ransomware models

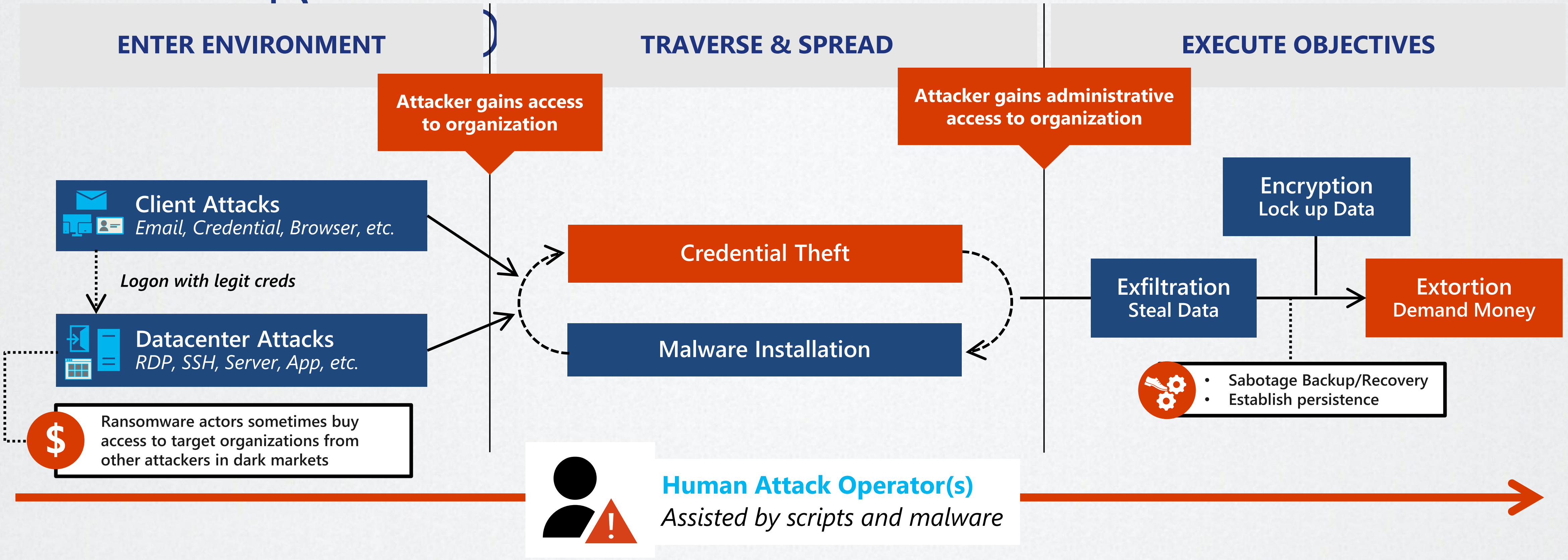

(Not)Petya
Wannacrypt
Cryptolocker
101010
010101
101010
Human Operated Ransomware - *Enterprise Organization*
Opportunistic Ransomware - *Single Device*
2013
2016
2017
2020

2013 - New Business Model
Monetizes by extorting need to access data (single device)

2019 - Vastly Expands Extortion Scope
to enterprise scale attacks (all data & systems), monetizing major business disruption and/or disclosure of confidential data

Delta-N Connecting the Cloud cegeka ARROW LIQUIT INSPARK Microsoft

Pattern – Human Operated



ENTER ENVIRONMENT

TRAVERSE & SPREAD

EXECUTE OBJECTIVES

Attacker gains access to organization

Attacker gains administrative access to organization

Client Attacks
Email, Credential, Browser, etc.

Logon with legit creds

Datacenter Attacks
RDP, SSH, Server, App, etc.

Ransomware actors sometimes buy access to target organizations from other attackers in dark markets

Credential Theft

Malware Installation

Encryption
Lock up Data

Exfiltration
Steal Data

Extortion
Demand Money

- Sabotage Backup/Recovery
- Establish persistence

Human Attack Operator(s)
Assisted by scripts and malware

Delta-N Connecting the Cloud   cegeka   ARROW   LIQUIT   INSPARK   Microsoft

Mapping rules to HumOR

LAPS + MFA + RDP lockout polices

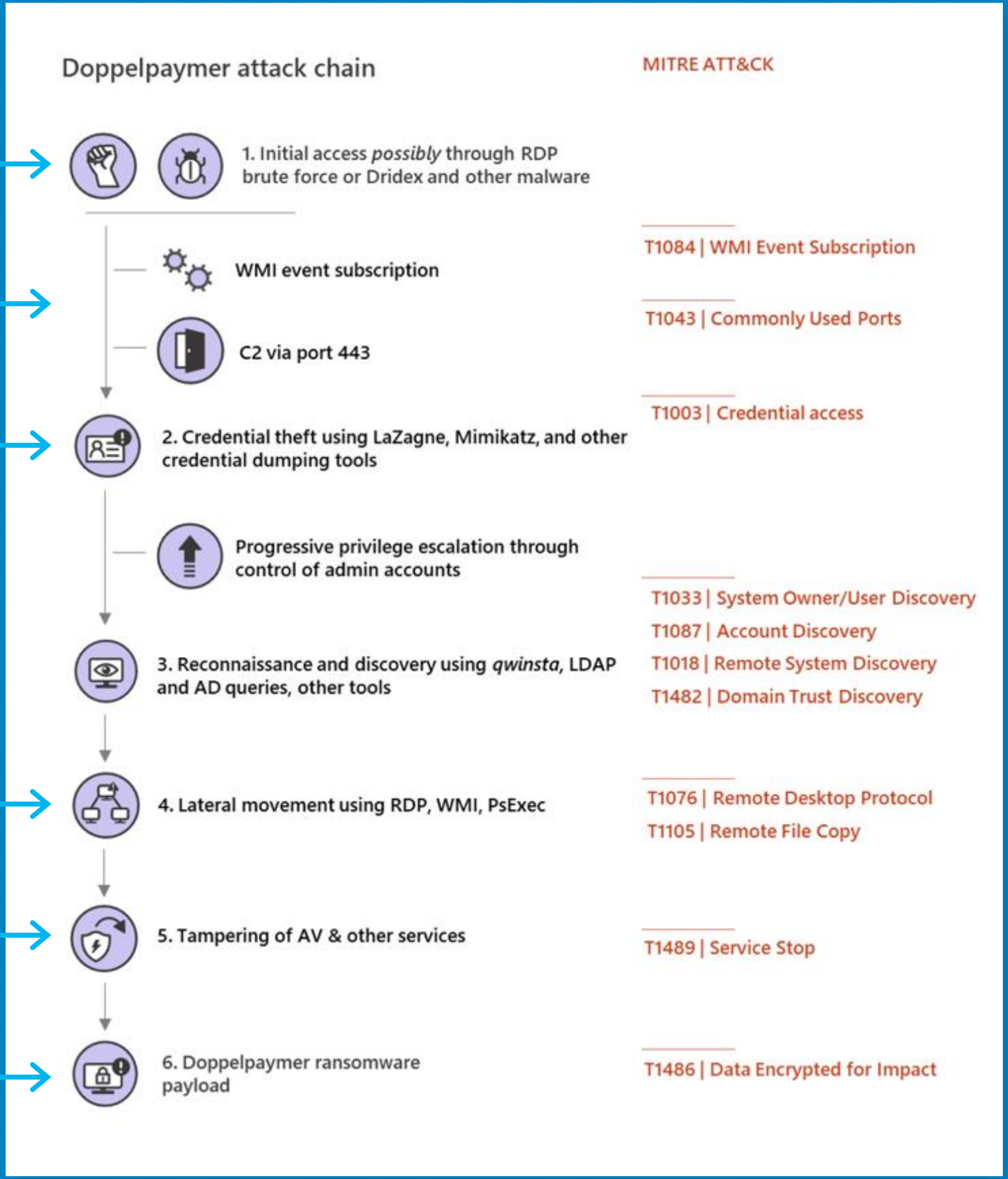
WMI persistence blocking ASR

Cred guard and/or cred theft blocking ASR

Lateral movement blocking ASR

Tamper protection feature

Aggressive ransomware blocking / behavioral monitoring / controlled folder access etc.



Doppelpaymer attack chain

MITRE ATT&CK

1. Initial access *possibly* through RDP brute force or Dridex and other malware

WMI event subscription — T1084 | WMI Event Subscription

C2 via port 443 — T1043 | Commonly Used Ports

2. Credential theft using LaZagne, Mimikatz, and other credential dumping tools — T1003 | Credential access

Progressive privilege escalation through control of admin accounts

3. Reconnaissance and discovery using *qwinsta*, LDAP and AD queries, other tools — T1033 | System Owner/User Discovery; T1087 | Account Discovery; T1018 | Remote System Discovery; T1482 | Domain Trust Discovery

4. Lateral movement using RDP, WMI, PsExec — T1076 | Remote Desktop Protocol; T1105 | Remote File Copy

5. Tampering of AV & other services — T1489 | Service Stop

6. Doppelpaymer ransomware payload — T1486 | Data Encrypted for Impact

SECURITY

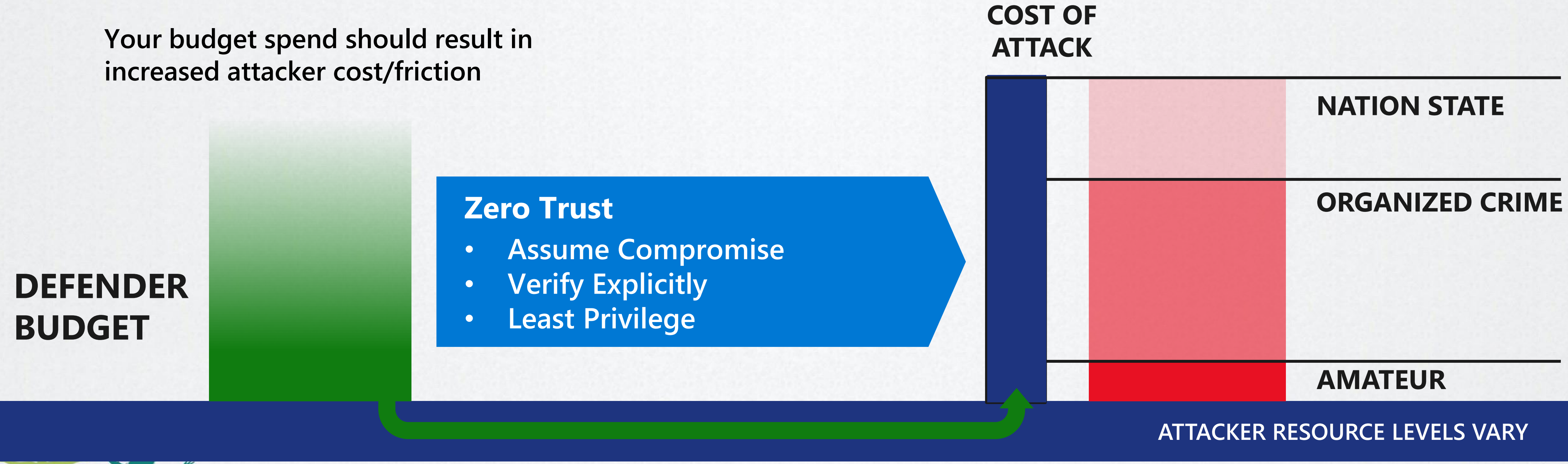
Ruin their Business Model

NOTE: Cost of attack is continuously changing with technical advancement + business model evolution

ATTACKERS:
MAXIMIZE RETURN ON INVESTMENT (ROI)
(return may be monetary/political/etc.)

DEFENDERS:
RUIN ATTACKER ROI
by raising attack cost with protection + rapid response/recovery

ZERO TRUST:
PRIORITIZE AND SIMPLIFY
with a strategy that combines advanced techniques with security fundamentals



Your budget spend should result in increased attacker cost/friction

DEFENDER BUDGET

Zero Trust
- Assume Compromise
- Verify Explicitly
- Least Privilege

COST OF ATTACK

NATION STATE

ORGANIZED CRIME

AMATEUR

ATTACKER RESOURCE LEVELS VARY

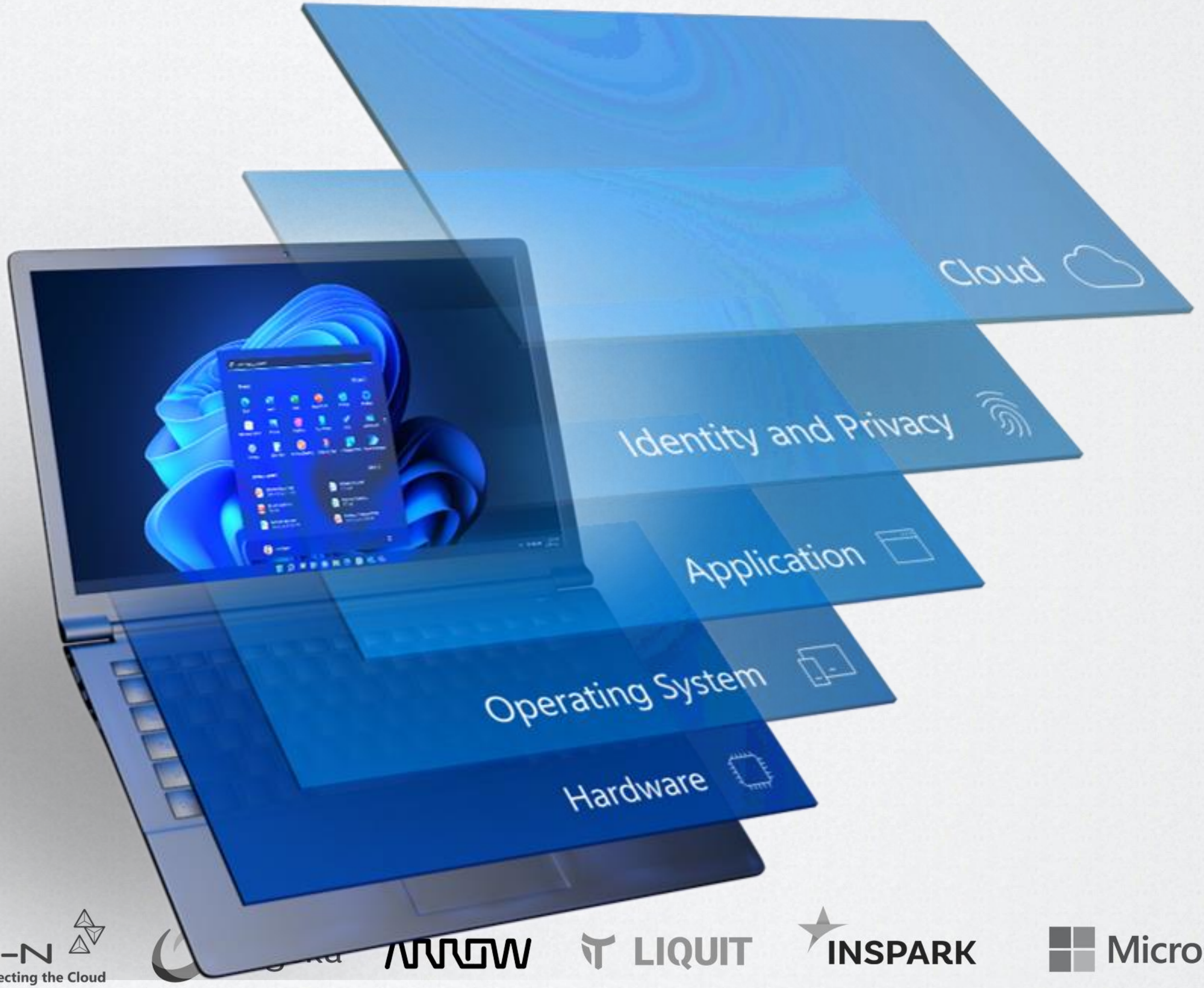
Delta-N Connecting the Cloud cegeka ARROW LIQUIT INSPARK Microsoft

SECURITY

Introduction of Attack Surface Reduction rules

Reducing the attack surface…

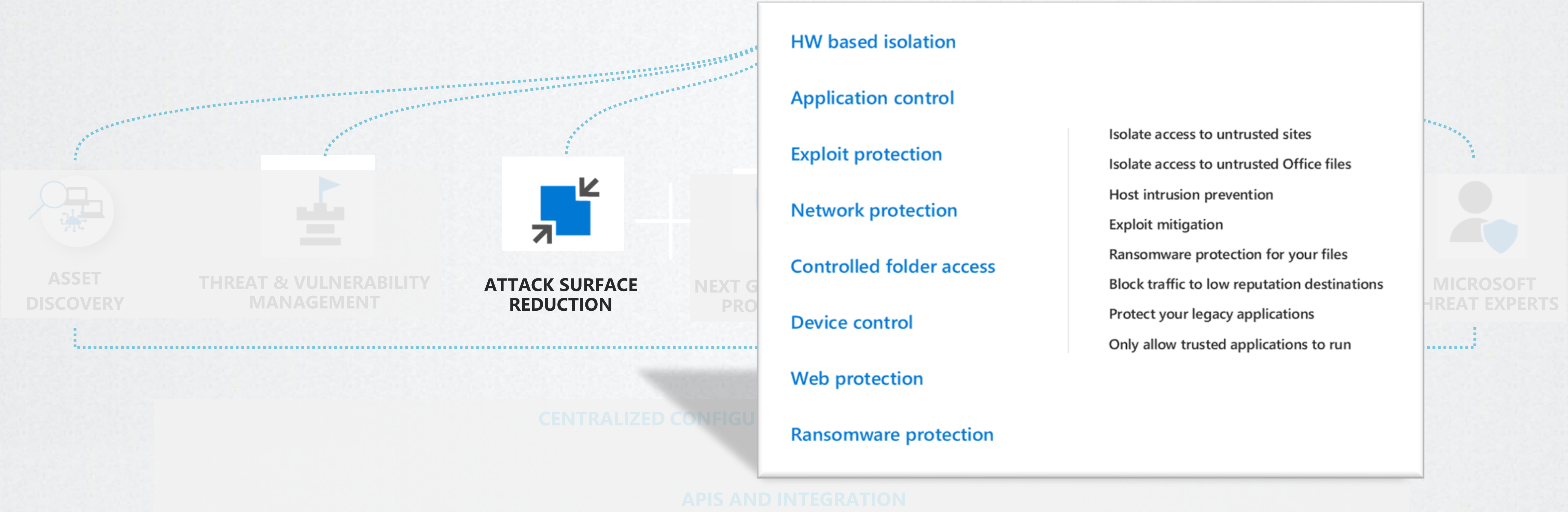
SECURITY


Cloud
Identity and Privacy
Application
Operating System
Hardware

SECURITY

Microsoft Defender for Endpoint

Threats are no match.



- HW based isolation
- Application control
- Exploit protection
- Network protection
- Controlled folder access
- Device control
- Web protection
- Ransomware protection

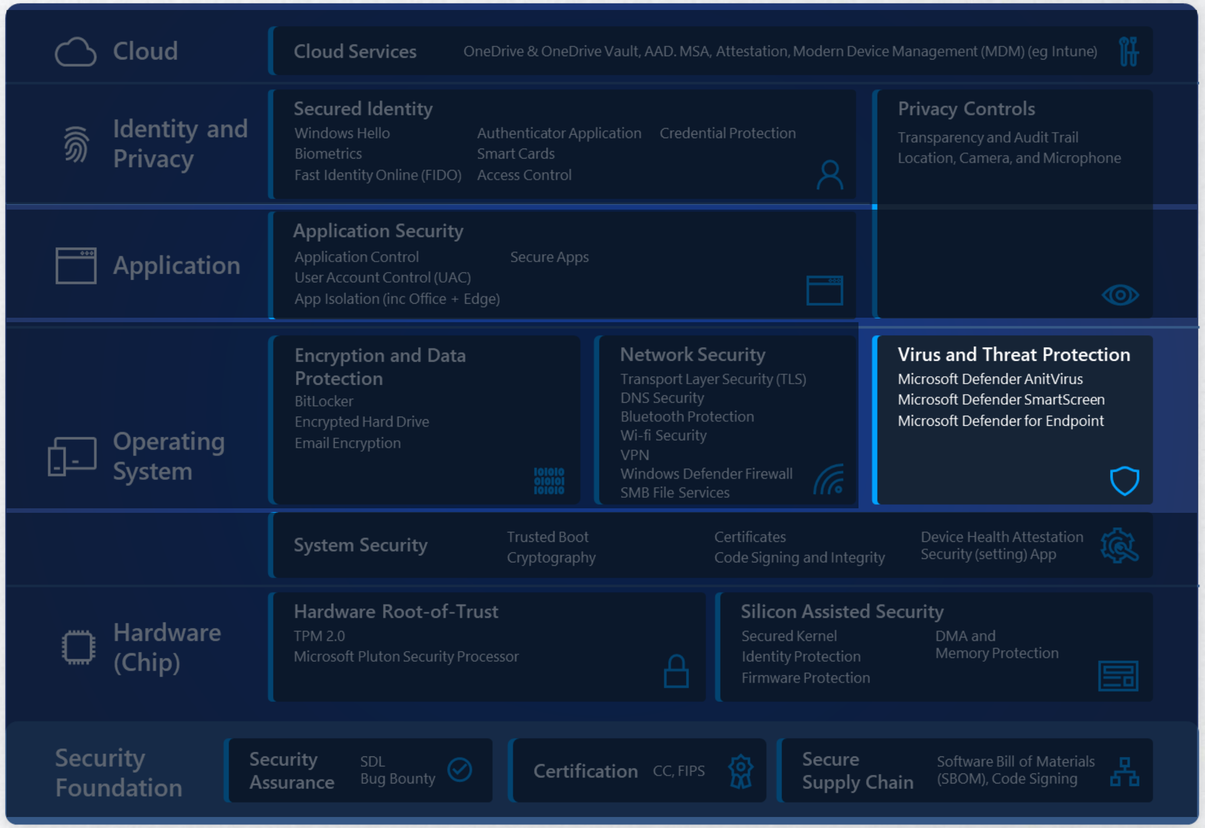
- Isolate access to untrusted sites
- Isolate access to untrusted Office files
- Host intrusion prevention
- Exploit mitigation
- Ransomware protection for your files
- Block traffic to low reputation destinations
- Protect your legacy applications
- Only allow trusted applications to run

Delta-N Connecting the Cloud cegeka ARROW LIQUIT INSPARK Microsoft

What are Attack Surface Reduction rules?

Attack Surface Reduction rules are meant to resist attacks and exploitations on endpoints.

- Attack surface reduction rules target certain software behaviors, such as:
  - Launching executable files and scripts that attempt to download or run files
  - Running obfuscated or otherwise suspicious scripts
  - Performing behaviors that apps don't usually initiate during normal day-to-day work



Cloud

Cloud Services OneDrive & OneDrive Vault, AAD. MSA, Attestation, Modern Device Management (MDM) (eg Intune)

Identity and Privacy

Secured Identity
Windows Hello
Biometrics
Fast Identity Online (FIDO)
Authenticator Application
Smart Cards
Access Control
Credential Protection

Privacy Controls
Transparency and Audit Trail
Location, Camera, and Microphone

Application

Application Security
Application Control
User Account Control (UAC)
App Isolation (inc Office + Edge)
Secure Apps

Operating System

Encryption and Data Protection
BitLocker
Encrypted Hard Drive
Email Encryption

Network Security
Transport Layer Security (TLS)
DNS Security
Bluetooth Protection
Wi-fi Security
VPN
Windows Defender Firewall
SMB File Services

Virus and Threat Protection
Microsoft Defender AnitVirus
Microsoft Defender SmartScreen
Microsoft Defender for Endpoint

System Security
Trusted Boot
Cryptography
Certificates
Code Signing and Integrity
Device Health Attestation
Security (setting) App

Hardware (Chip)

Hardware Root-of-Trust
TPM 2.0
Microsoft Pluton Security Processor

Silicon Assisted Security
Secured Kernel
Identity Protection
Firmware Protection
DMA and
Memory Protection

Security Foundation

Security Assurance SDL
Bug Bounty

Certification CC, FIPS

Secure Supply Chain Software Bill of Materials
(SBOM), Code Signing

Rules by category

Productivity apps rules

- Block Office apps from creating executable content
- Block Office apps from creating child processes
- Block Office apps from injecting code into other processes
- Block Win32 API calls from Office macros
- Block Adobe Reader from creating child processes

Email rule

- Block executable content from email client and webmail
- Block Office communication apps from creating child processes
- Block only Office communication applications from creating child processes

Misc rule

- Block abuse of exploited vulnerable signed drivers

Script rules

- Block obfuscated JS/VBS/PS/macro code
- Block JS/VBS from launching downloaded executable content

Polymorphic threats

- Block executable files from running unless they meet a prevalence (1000 machines), age (24hrs), or trusted list criteria
- Block untrusted and unsigned processes that run from USB
- Use advanced protection against ransomware

Lateral movement & credential theft

- Block process creations originating from PSExec and WMI commands
- Block credential stealing from the Windows local security authority subsystem (lsass.exe)
- Block persistence through WMI event subscription

Operating modes

Disabled (default)

- The rule is not enforced.
- No processes or activity is blocked by the rule.

Audit mode

- An ASR Audit Event is generated every time the targeted activity occurs on the protected device.
- The activity in question is NOT really blocked; only logged.
- Useful for evaluating impact of the rule, before enabling in Block Mode.

Block mode

- The targeted activity is blocked by the rule.
- An ASR Block Event is generated for every Block (some exceptions/optimizations/suppressions apply).

Warn mode (added this year)

- The targeted activity is blocked by the rule. However, user gets and option to exclude for 24h.
- An ASR Block Event is generated for every Block (some exceptions/optimizations/suppressions apply).

*Windows 10, Windows Server, version 1809 or higher
*Microsoft Defender Antivirus must be running with real-time protection in Active mode

SECURITY

Demo

Proof is in the eating…

- Determine your security posture by Secure Score and unleash your ASR potential
- Understand user impact recommendations in practice with Vulnerability Management
- Configure Attack Surface Reduction rules Endpoint Manager

Attack Surface Reduction rules

What’s new in ASR rules

- Indicator based exclusions
- Vulnerable driver rule
  - The rule is designed to block the known vulnerable drivers from being dropped on the machine.
  - [Attack surface reduction rules reference | Microsoft Docs]
- ASR rules support for Windows Server 2012 R2/2016 with the new Unified MDE client.

Demo scenarios to validate Defender for Endpoint, SmartScreen and Attack Surface Reduction*

https://demo.wd.microsoft.com/Page/ASR

Requirements

- Windows 10/11 Pro/Enterprise/Education
- Windows 10, versions 1709 and later, Windows Server version 1803 (Semi-Annual Channel or later) and Windows Server 2019
- Microsoft Defender Antivirus as primary AV (real-time protection on)
- Cloud-Delivery Protection (aka MAPS)

Warn mode exceptions*

- Block JavaScript or VBScript from launching downloaded executable content
- Block persistence through WMI event subscription
- Use advanced protection against ransomware

Attack Surface Reduction rules

What's to check when having false positives?

- Cloud Protection is set to "High +" (normal or high)
- Make sure that "Cloud Protection" (aka MAPS) is working (MpCmdRun.exe –ValidateMapsConnection)
- Make sure that 'Security Intelligence Updates' (aka signatures, definitions) is up to date
- Make sure that 'Platform Update' is up to date.

What type of exclusions work for ASR rules?low

- Indicators – Certificate – Allow
- Indicators – File hash – Allow
- MDAV exclusions except for AMSI detections (e.g. PoSh/js, etc…)
- ASR Rules exclusions

What type of wildcards work with ASR Rules exclusions?

- You can use the asterisk *, question mark ?, or environment variables (such as %ALLUSERSPROFILE%) as wildcards when defining items in the file name or folder path exclusion list.

C:\MyData\*.txt includes C:\MyData\notes.txt
C:\MyData\my?.zip includes C:\MyData\my1.zip
C:\Serv\**\Backup includes any file in C:\Serv\Primary\Denied\Backup and its subfolders, and C:\Serv\Secondary\Allowed\Backup and its subfolders

SECURITY

Demo

Proof is in the eating…

- Attack Surface Reduction in action from a user perspective
- Gain insights and fine tune your ASR deployment using reports
- Use Advanced Hunting to get detailed information with a little help of KQL

SECURITY

Tips & Tricks

Attack Surface Reduction rulezzz…

How & where to start tomorrow?

- Make sure **Cloud Protection** and **MAPS** are **enabled**
- Create **individual policies** for each of the ASR Rules (audit/warn/block) and deploy
- Audit for a period between 1 to 7** days. Repeat for 3-4 weeks
- Have at least **some ASR rules enabled** in **block mode** while working on others
- Start **mitigation from least amount audit detections** to the greatest number of detections
- Use **Advanced Hunting** queries **to find** apps/scripts/docs that might have **compatibility issues**
- Standardize on **Endpoint Security (ASR) policy templates**
- Think **defense-in-depth**! Do not rely on ASR rules solely

SECURITY

Resources

Blog posts in Microsoft Defender for Endpoint Tech Communities

Demystifying ASR rules

Use attack surface reduction rules to prevent malware infection

Use attack surface reduction rules to prevent malware infection - Windows security | Microsoft Docs

Enable attack surface reduction rules

Enable attack surface reduction rules - Windows security | Microsoft Docs

Power BI Power BI Report templates

GitHub - microsoft/MDE-PowerBI-Templates: A respository for MDATP PowerBI Templates

Customize attack surface reduction rules

Customize attack surface reduction rules - Windows security | Microsoft Docs

View attack surface reduction events

View attack surface reduction events - Windows security | Microsoft Docs

Attack surface reduction policy for endpoint security in Endpoint Manager

Manage attack surface reduction settings with endpoint security policies in Microsoft Intune | Microsoft Docs

Demo scenarios to validate Defender for Endpoint, SmartScreen and Attack Surface Reduction*

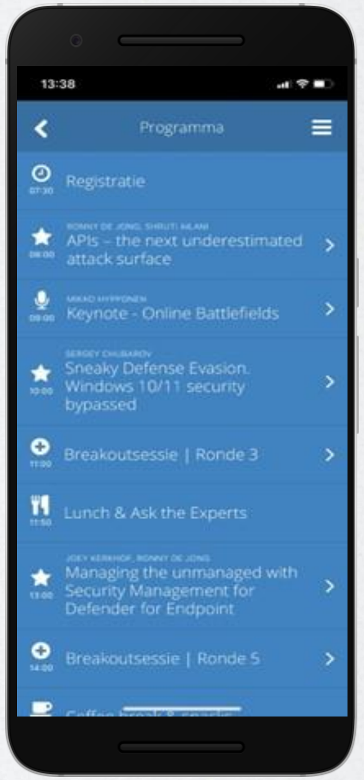
https://demo.wd.microsoft.com/Page/ASR

*After listening to feedback, we have decided to delay the retirement of this site until 09/30/2022. You have more time to let us know about the features you are using and how you are using them. To contact us, email mdedemositefeedback@microsoft.com.

Delta-N Connecting the Cloud   cegeka   ARROW   LIQUIT   INSPARK   Microsoft

Questions?

Thank you!



13:38

Programma

07:30 Registratie

08:00 RONNY DE JONG, SHRUTI AILANI
APIs – the next underestimated attack surface

09:00 MIKKO HYPPONEN
Keynote - Online Battlefields

10:00 SERGEY CHUBAROV
Sneaky Defense Evasion. Windows 10/11 security bypassed

11:00 Breakoutsessie | Ronde 3

11:50 Lunch & Ask the Experts

13:00 JOEY KERKHOF, RONNY DE JONG
Managing the unmanaged with Security Management for Defender for Endpoint

14:00 Breakoutsessie | Ronde 5

Coffee break & snacks

Pim Jacobs
pim.jacobs@inspark.nl

Ronny de Jong
ronnydejong@microsoft.com