Microsoft

#techsummitCH

Microsoft Tech Summit

Build your skills with the latest in cloud technologies

Microsoft

#techsummitCH

Microsoft Tech Summit

28 February – 1 March 2018, Trafo Baden

Microsoft

#techsummitCH

Be a Step Ahead of your Enemy

Daniel von Büren
TSP Threat Management; Microsoft

Ralf Gomeringer
TSP Threat Management; Microsoft

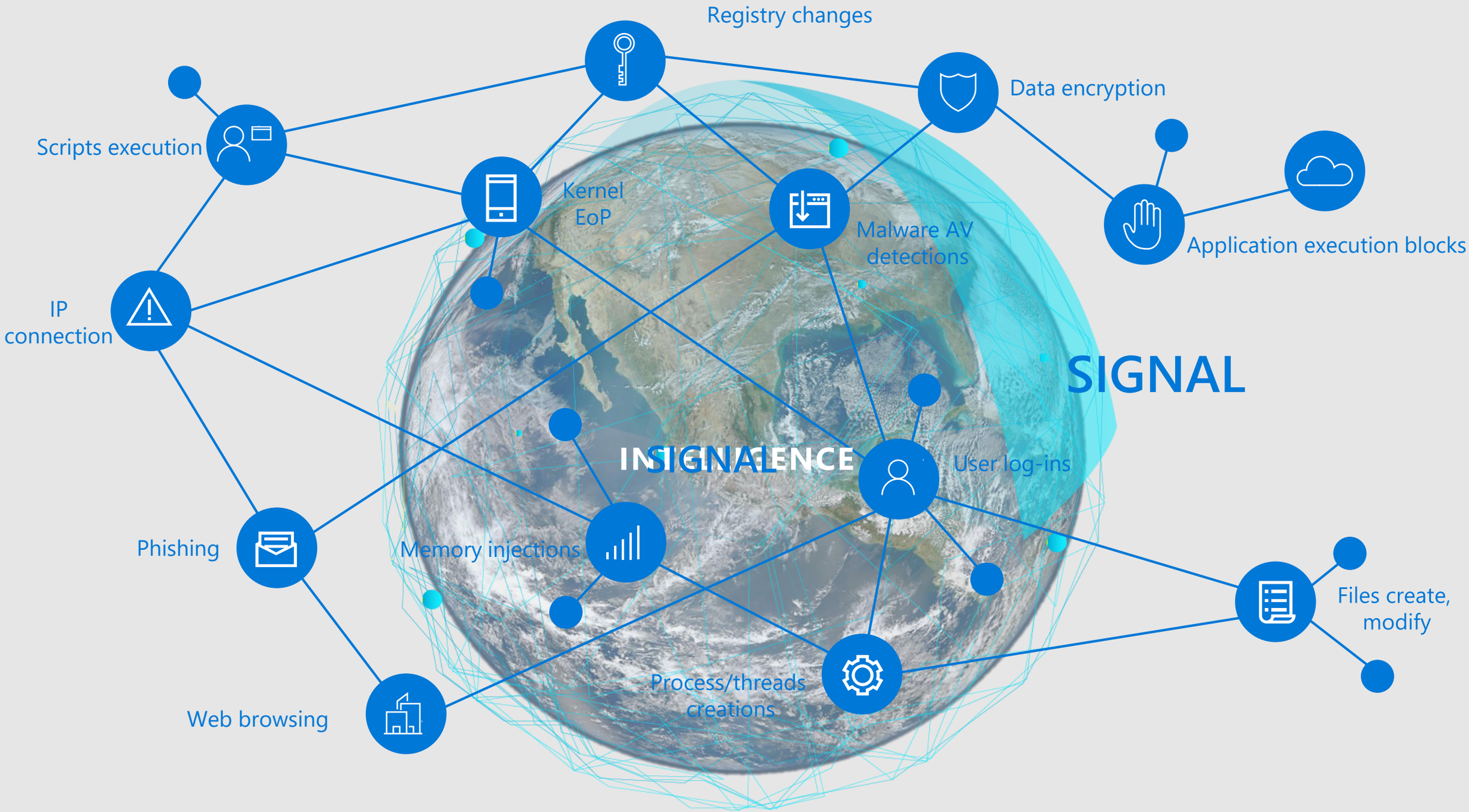
Most criminals are opportunistic and efficient

How to steal a Bike?

MODERN SECURITY THREATS

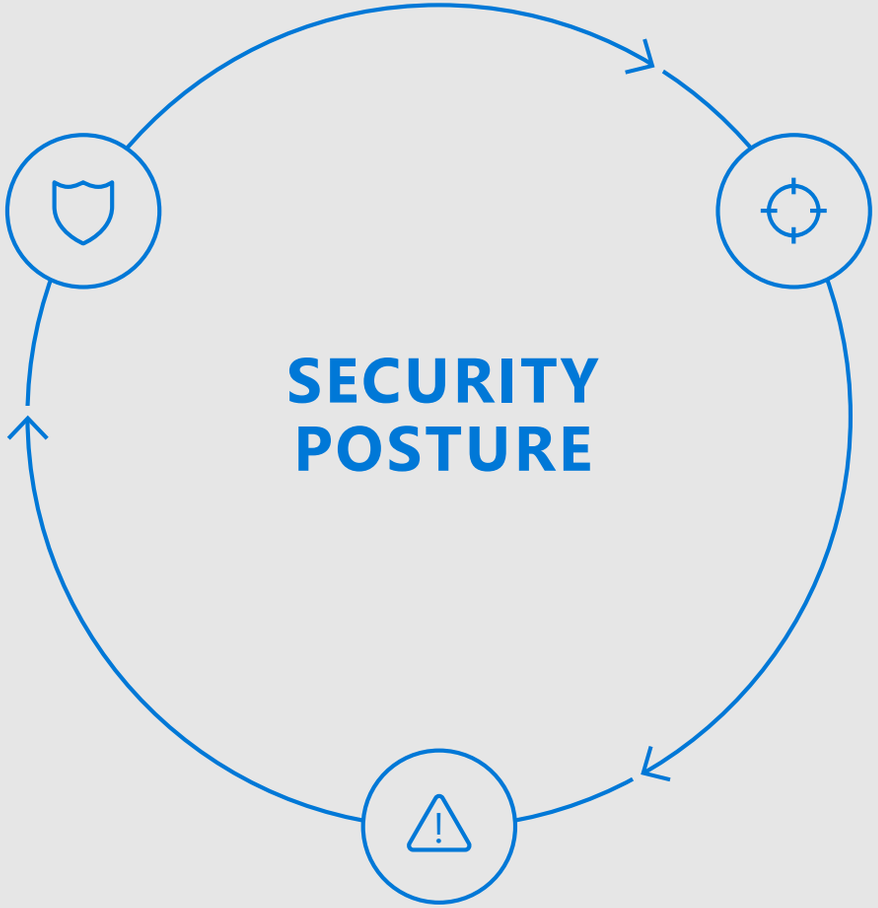
“THERE ARE TWO KINDS OF BIG COMPANIES, THOSE WHO’VE BEEN HACKED, AND THOSE WHO DON’T KNOW THEY’VE BEEN HACKED.”

JAMES COMEY, FORMER DIRECTOR FBI


Registry changes
Data encryption
Scripts execution
Kernel
EoP
Malware AV
detections
Application execution blocks
IP
connection
SIGNAL
INTELLIGENCE
User log-ins
Phishing
Memory injections
Files create,
modify
Process/threads
creations
Web browsing

PROTECT

across all endpoints, from sensors to the datacenter

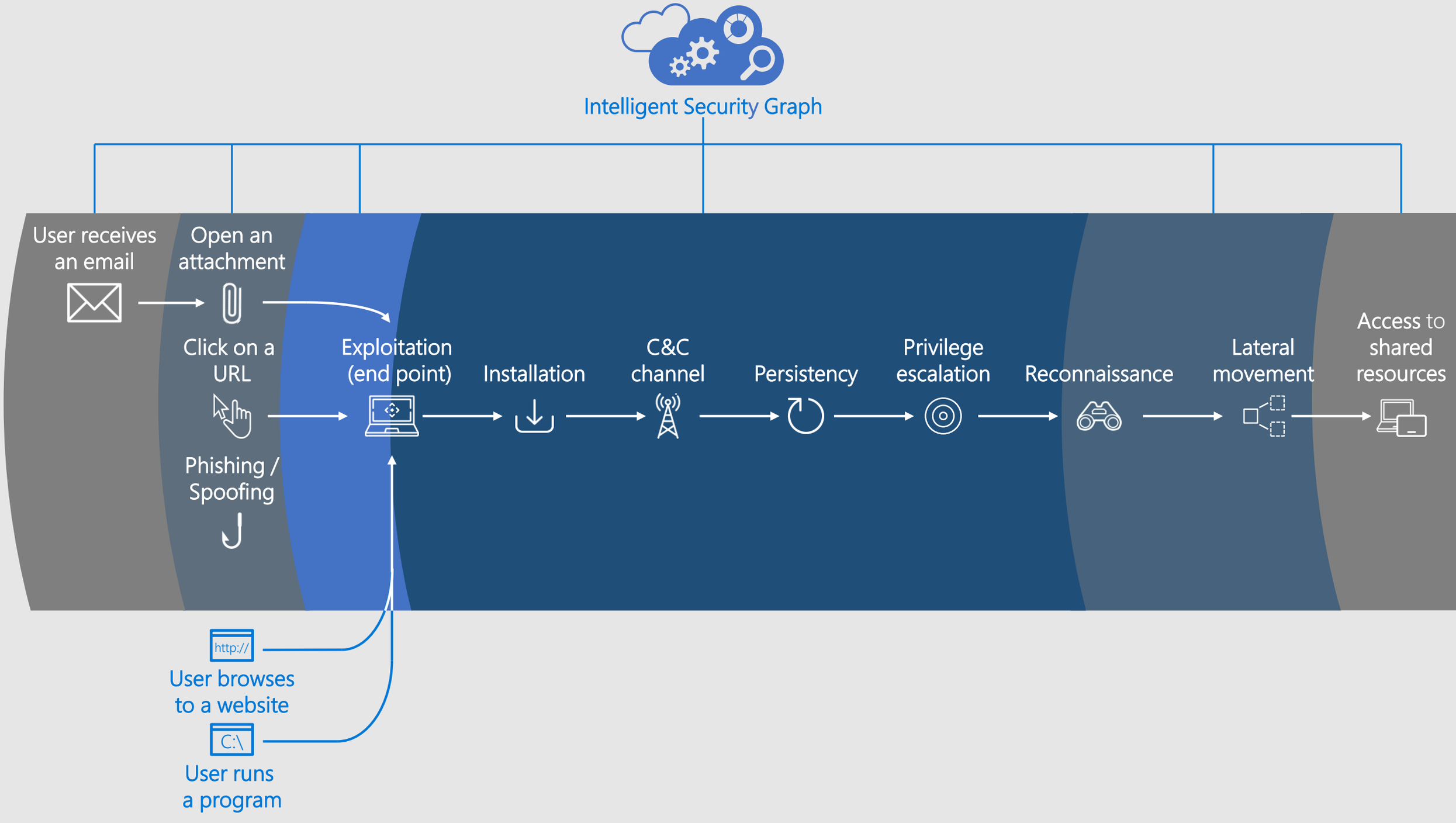


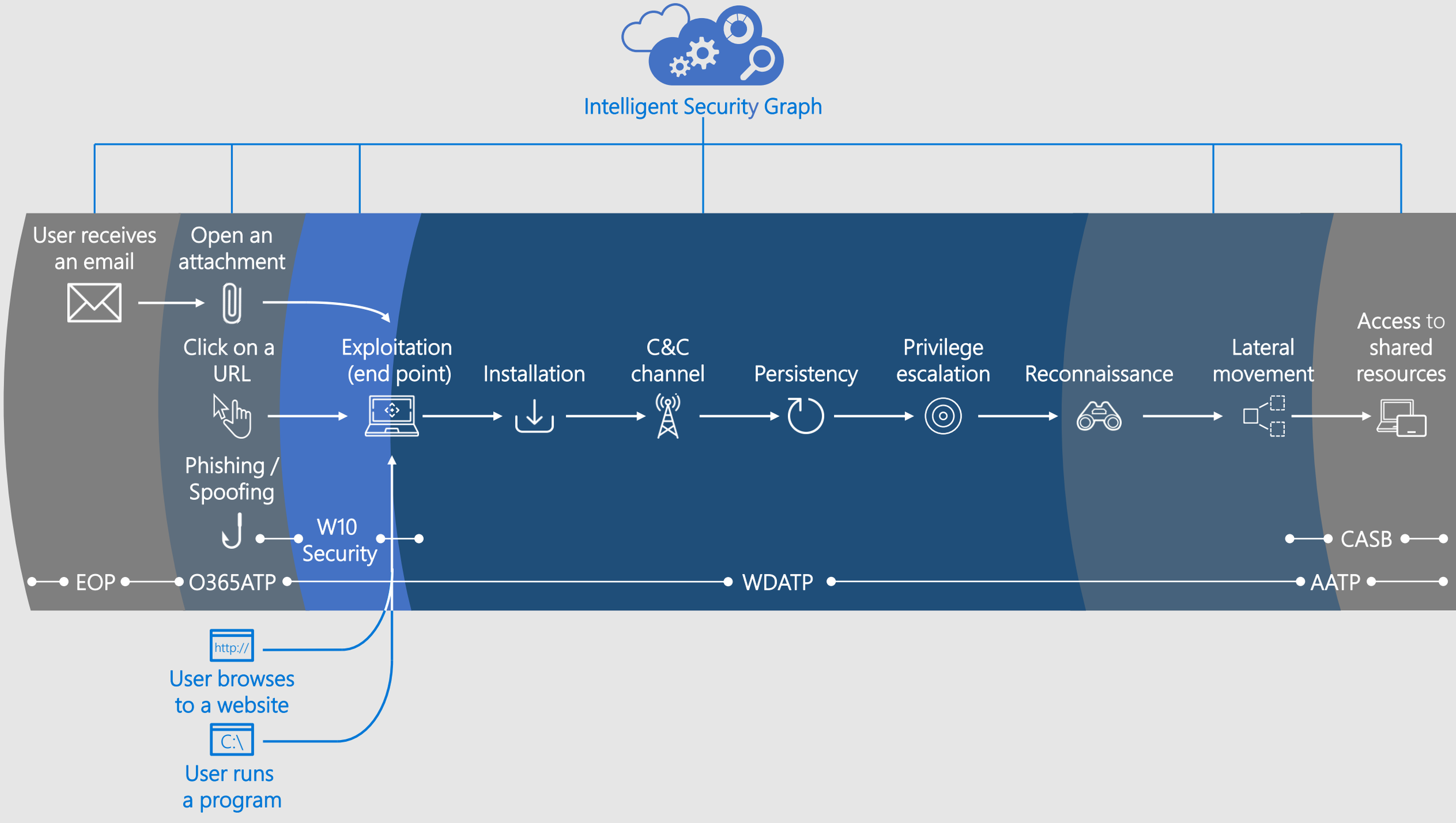
DETECT

using targeted signals, behavioral monitoring, and machine learning

RESPOND

closing the gap between discovery and action


Intelligent Security Graph
User receives an email
Open an attachment
Click on a URL
Phishing / Spoofing
Exploitation (end point)
Installation
C&C channel
Persistency
Privilege escalation
Reconnaissance
Lateral movement
Access to shared resources
http://
User browses to a website
C:\
User runs a program


Intelligent Security Graph
User receives an email
Open an attachment
Click on a URL
Phishing / Spoofing
Exploitation (end point)
Installation
C&C channel
Persistency
Privilege escalation
Reconnaissance
Lateral movement
Access to shared resources
W10 Security
CASB
EOP
O365ATP
WDATP
AATP
http://
User browses to a website
C:\
User runs a program

Abbreviations & Links for reference

- AATP: Azure Advanced Threat Protection
- MCAS: Microsoft Cloud App Security
- O365ATP: Office 365 Advanced Threat Protection
- WD: Windows Defender
  - SmartScreen
  - WDATP: Windows Defender Advanced Threat Protection
  - WDAV: Windows Defender AntiVirus
  - WDAC: Windows Defender Application Control
  - WDAG: Windows Defender Application Guard
- WDEG: Windows Defender Exploit Guard
  - WDEG ASR: Attack Surface Reduction
  - WDEG NP: Network Protection
  - WDEG CFA: Controlled Folder Access

Resources

Exchange Online Protection (EOP)

- EOP resources for malware prevention
  https://blogs.technet.microsoft.com/eopfieldnotes/2017/05/25/eop-resources-for-malware-prevention/

Windows Defender Antivirus (WDAV)

- How artificial intelligence stopped an Emotet outbreak
  https://cloudblogs.microsoft.com/microsoftsecure/2018/02/14/how-artificial-intelligence-stopped-an-emotet-outbreak/
- Windows Defender Antivirus cloud protection service: Advanced real-time defense against never-before-seen malware
  https://blogs.technet.microsoft.com/mmpc/2017/07/18/windows-defender-antivirus-cloud-protection-service-advanced-real-time-defense-against-never-before-seen-malware/
- Detonating a bad rabbit: Windows Defender Antivirus and layered machine learning defenses
  https://blogs.technet.microsoft.com/mmpc/2017/12/11/detonating-a-bad-rabbit-windows-defender-antivirus-and-layered-machine-learning-defenses/

Windows Defender Advanced Threat Protection (WDATP)

- Windows Defender ATP thwarts Operation WilySupply software supply chain cyberattack
  https://blogs.technet.microsoft.com/mmpc/2017/05/04/windows-defender-atp-thwarts-operation-wilysupply-software-supply-chain-cyberattack/
- Detecting stealthier cross-process injection techniques with Windows Defender ATP: Process hollowing and atom bombing
  https://blogs.technet.microsoft.com/mmpc/2017/07/12/detecting-stealthier-cross-process-injection-techniques-with-windows-defender-atp-process-hollowing-and-atom-bombing/

Microsoft Cloud App Security (MCAS)

- Cloud App Security Threat Protection just got better
  https://cloudblogs.microsoft.com/enterprisemobility/2018/02/08/cloud-app-security-threat-protection-just-got-better/
- Protect multiple cloud app instances using Microsoft Cloud App Security
  https://cloudblogs.microsoft.com/enterprisemobility/2018/02/26/protect-multiple-cloud-app-instances-using-microsoft-cloud-app-security/

Microsoft

#techsummitCH

Please Complete your Session Evaluations

Get your cool IoT Dev Kit!

Fill out your feedback form and turn it in before you leave.

Microsoft