Microsoft

Microsoft Ignite

Microsoft

Modern Malware: Leveraging Its Imperfection to Design Response Methods

Paula Januszkiewicz
CQURE: CEO, Cybersecurity Expert
CQURE Academy: Trainer
Microsoft Regional Director
MVP: Cloud and Datacenter Management
www.cqureacademy.com
paula@cqure.us

CQURE CQURE ACADEMY

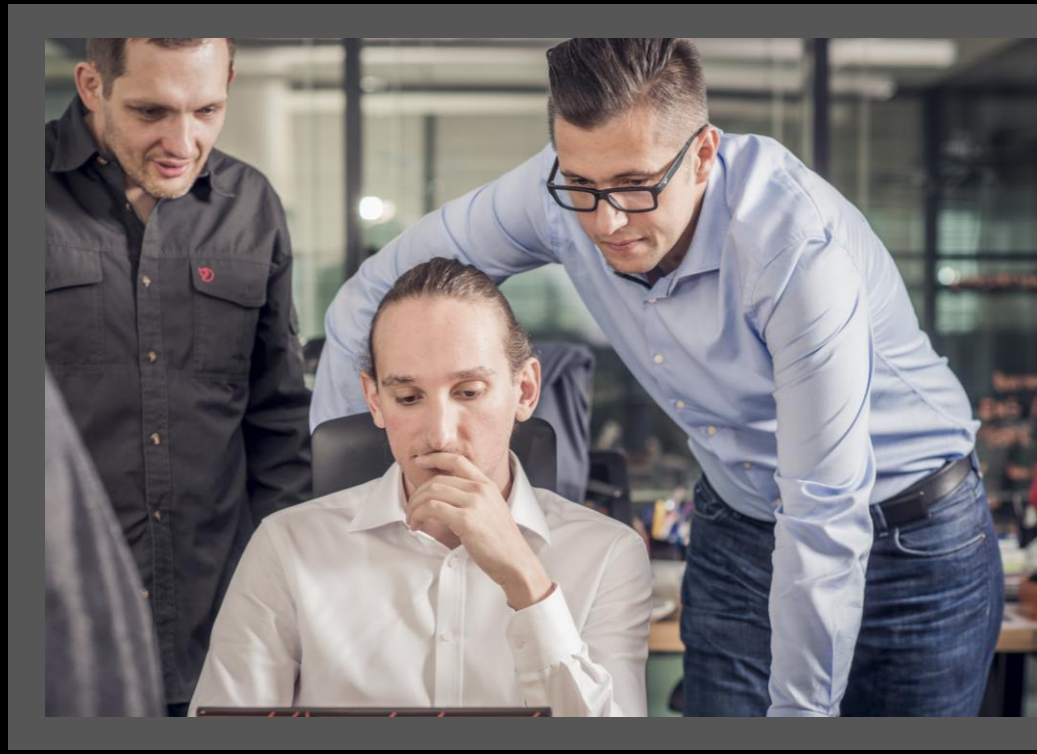
@paulacqure
@CQUREAcademy

What does CQURE do?

1. **Consulting Services:**
   Extensive IT Security Audits and Penetration Tests of all kinds,
   Configuration Audit and Architecture,
   Design Social Engineering Tests,
   Advanced Troubleshooting and Debugging,
   Emergency Response Services.

2. **R&D & CQLabs Tools & Hacks Publications.**

3. **Trainings & Seminars:**
   Offline (mainly in New York or via our partners worldwide),
   Online (you will hear more about it at the end of this Webinar stay with us!).



Doris

Kama

Artur

Liza

Paula

Mike

Krystian

Adrianna

RSA CONFERENCE

HACKER FEST

Microsoft tech·days

Hacker Halted

TecHFuse

Microsoft Technology Summit

black hat

TechEd Microsoft

NIC nordic infrastructure conference

cyberday

Microsoft Ignite

UTmessan.

SC MAGAZINE

Adrian

Michal

Ken

Aga

Ula

Grzegorz

Adrian

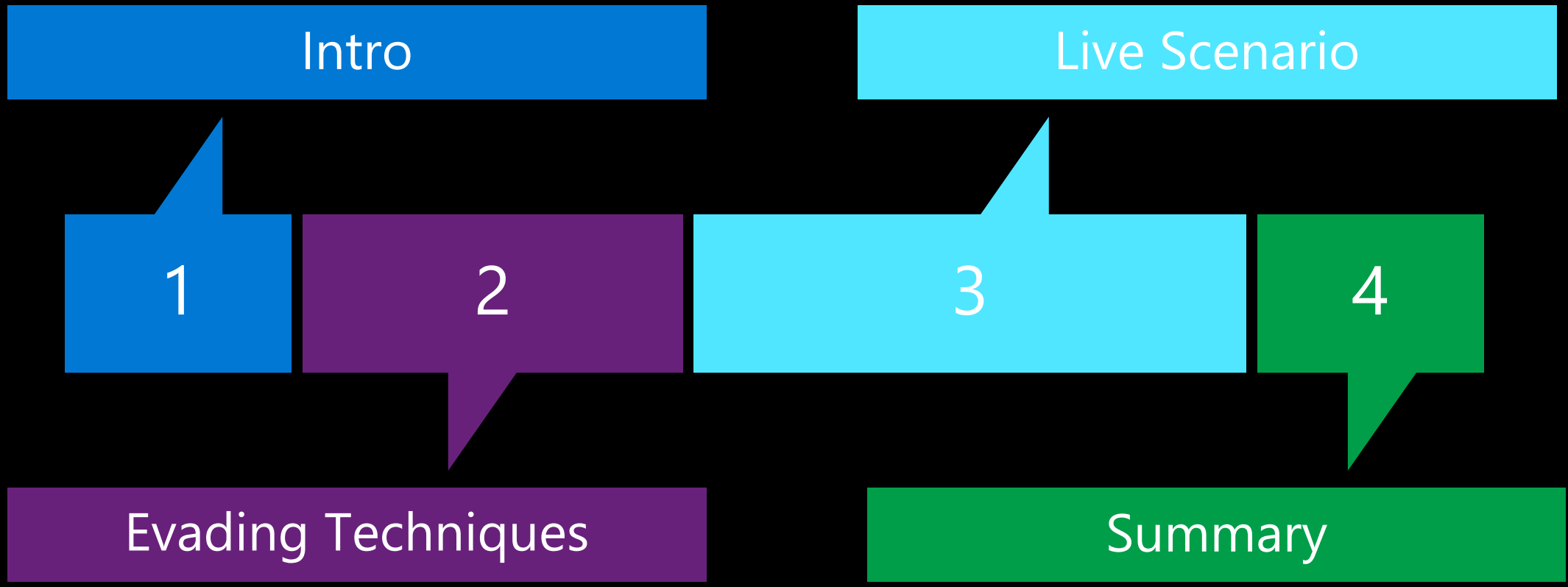
Milosz

Michael

Matus

Kamil

Agenda




We have the best security solutions...


...but the security landscape has changed.

Demo:

SDDL - Can antivirus be stopped?

Techniques for malware discovery

Signature-based

Can rely on the imphash" (uses library/API names and their specific order within the executable)

Behavior-based

Attempts to open, view, delete, and/or modify files
Attempts to format disk drives and other unrecoverable disk operations
Modifications to the logic of executable files, scripts of macros
Modification of critical system settings, such as start-up settings
Scripting of e-mail and instant messaging clients to send executable content
Initiation of network communications

1- Evasion Techniques Used by Malware

Packers and Encryptors

Tools used to compress and encode binary files. Packer will "unpack" the payload into memory and execute it.

Tools and techniques: UPX, PECompact, Armadillo, Encoders (Metasploit), Hyperion

Wrapping

Attaches the malicious payload (the installer or the malware itself) to a legitimate file.

Tools:

2- Evasion Techniques Used by Malware

Obfuscation

Modifies high level or binary code it in a way that does not affect its functionality, but changes its signature.

Tools:

Anti-debugging

Prevents a binary from being analyzed in an emulated environments such security sandbox etc.

Examples: ZeroAccess, sleep function.

Reflective PE Loader

- Custom code
- User Mode Loaders

Executable is extracted and decrypted in memory

Code is loaded and executed dynamically

In Powershell.exe – not every module is embedded – they can be created and loaded during the execution

In Win32API: Custom code mimics LoadLibrary()

Interesting: During the compilation, that's what helps us:

```
CompilerParameters.CompilerOptions =
"/platform:x64";
```

Demo:

Custom Reflective PE Loader - CQPELoader

Demo:

Execution through the debugger

3- Evasion Techniques Used by Malware

Targeting

Used to:

Attack a specific part of a system (IE, Firefox etc.), and act as one (Create Remote Thread etc.)

Detect specific settings (VMWare, Process Explorer running etc.) to prevent analysis.

Typical examples are:

Do not run if network card is Microsoft Corporation

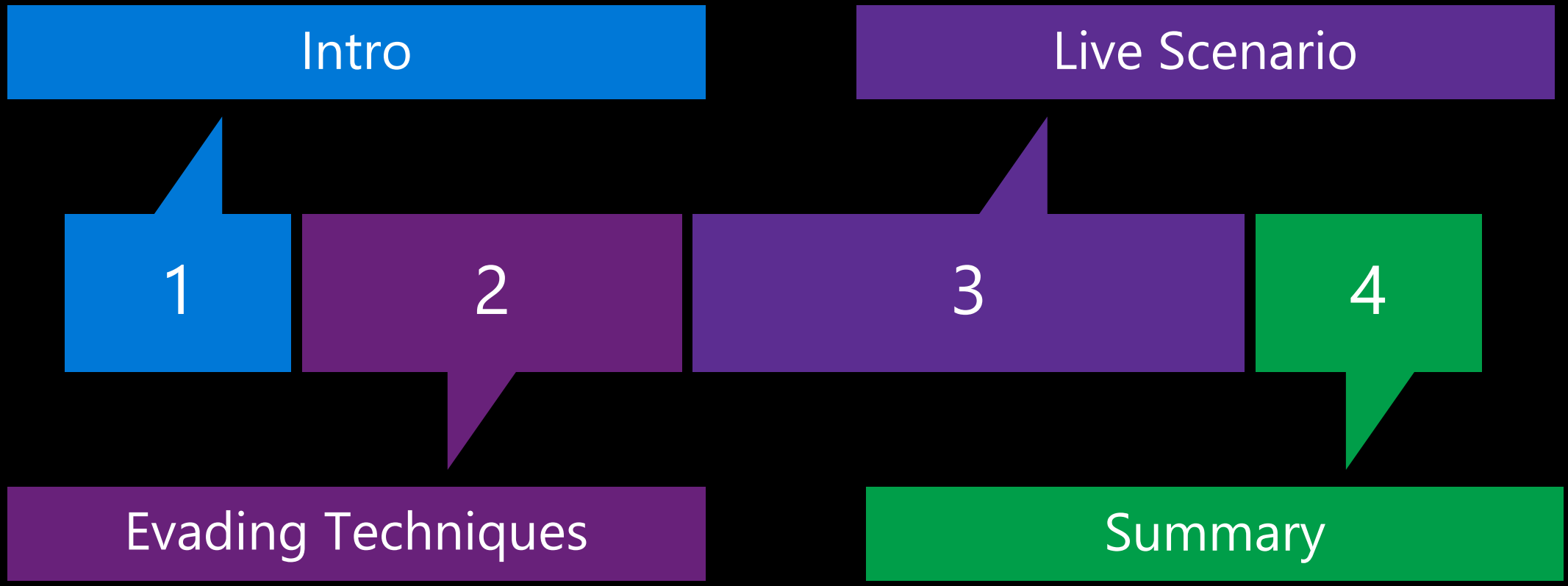
Do not run if wireshark.exe is working

Do not run if windbg.exe is running

Demo:

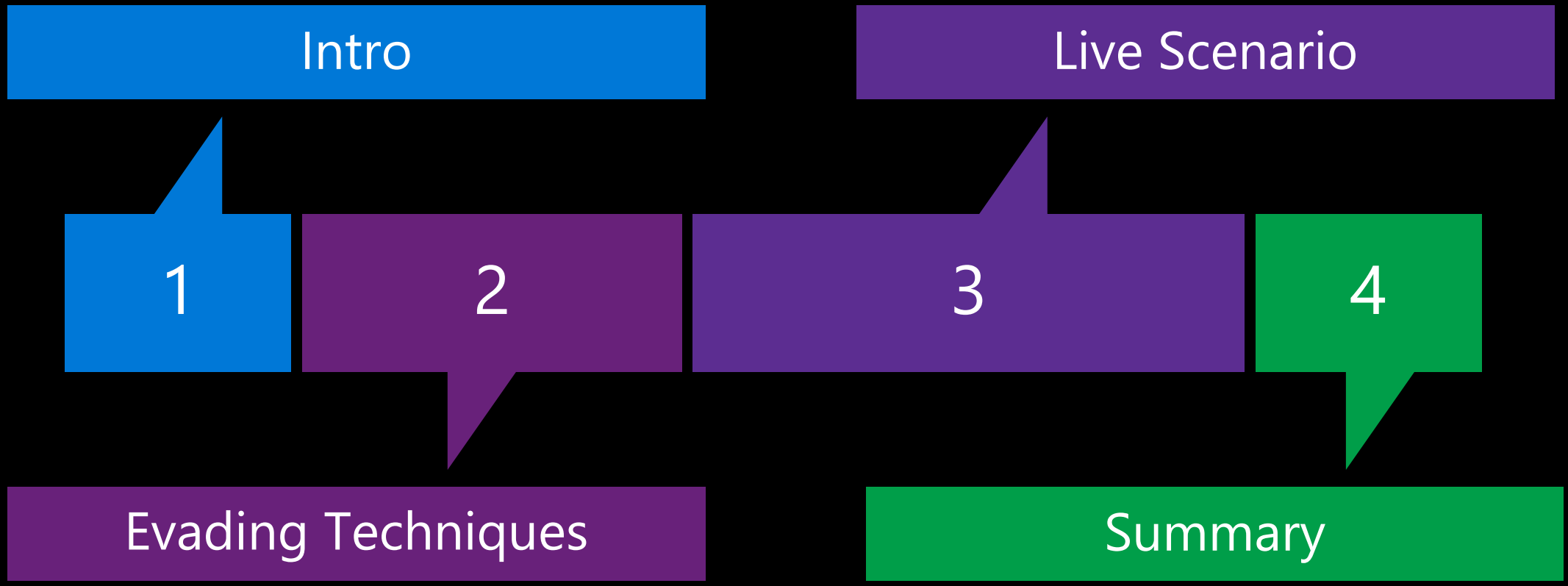
Sample malware analysis

Agenda



Demo:
Life scenario

Agenda



Summary: Bypassing techniques and mitigations

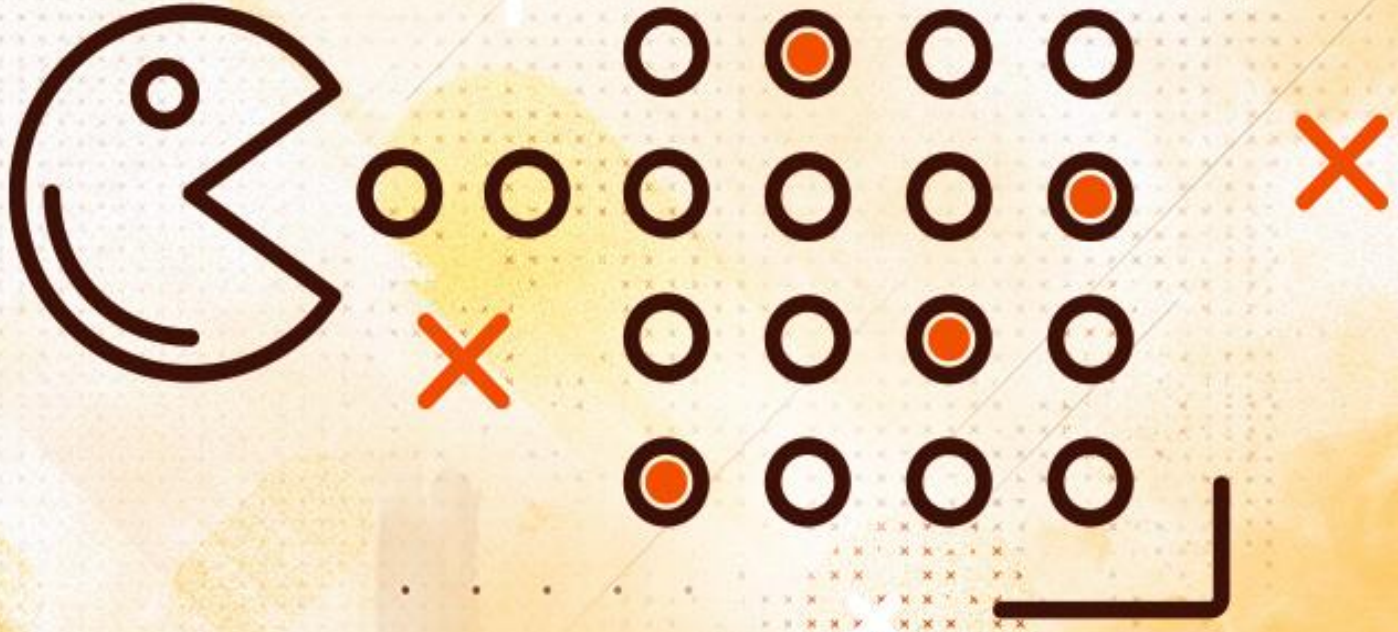
1. The only cure is a **_complete_** code execution prevention
2. Anti-Exploit solutions make a lot of sense
3. Sysmon
4. At the end it is a matter of budged and price
5. Code execution prevention solutions are often misconfigured

CQURE

Hardcore Cyber Security QUIZ 4.0

by CQURE Experts

Take the Quiz!



https://cqu.re/quiz

To get SLIDES & TOOLS

(and not to miss out on CQLabs video tutorials):

Sign up for our Newsletter
Cqureacademy.com/newsletter

Like CQURE Academy on Facebook
Facebook.com/CQURE

Follow us on Twitter
@PaulaCqure @CQUREAcademy

The best option – all of the above!
We won't think you're a stalker, promise!


Advanced Windows Security Course 2020
6 weeks, 12 LIVE modules
Full of surprises + certificate
Paula Januszkiewicz
and Security Experts
CQURE
CQURE

Microsoft

Modern Malware: Leveraging Its Imperfection to Design Response Methods

Paula Januszkiewicz
CQURE: CEO, Cybersecurity Expert
CQURE Academy: Trainer
Microsoft Regional Director
MVP: Cloud and Datacenter Management
www.cqureacademy.com
paula@cqure.us

CQURE CQURE ACADEMY

@paulacqure
@CQUREAcademy

Microsoft

Microsoft Ignite

THANK YOU!