Microsoft
tech·days
Kistamässan Stockholm
22-24 oktober 2019

Hacking Lambada:
Forensic Techniques for Unveiling the Hacker's Forbidden Dance

Paula Januszkiewicz

CQURE: CEO, Cybersecurity Expert
CQURE Academy: Trainer
MVP: Enterprise Security, MCT
Microsoft Regional Director
www.cqureacademy.com
paula@cqure.us

CQURE CONSULTING

CQURE ACADEMY

@paulacqure
@CQUREAcademy


Featured TechEd 2012 Speakers
More featured speakers →
Wally Mead
John Craddock
Mark Russinovich
Paula Januszkiewicz


Microsoft
CQURE ACADEMY©
We are proud to announce that
Paula Januszkiewicz
was rated as
No 1 Speaker
at Microsoft Ignite!!!
May 4-8, 2015
Chicago, IL


TechEd
Learn


black hat
ASIA 2019
SPEAKER
SPEAKER

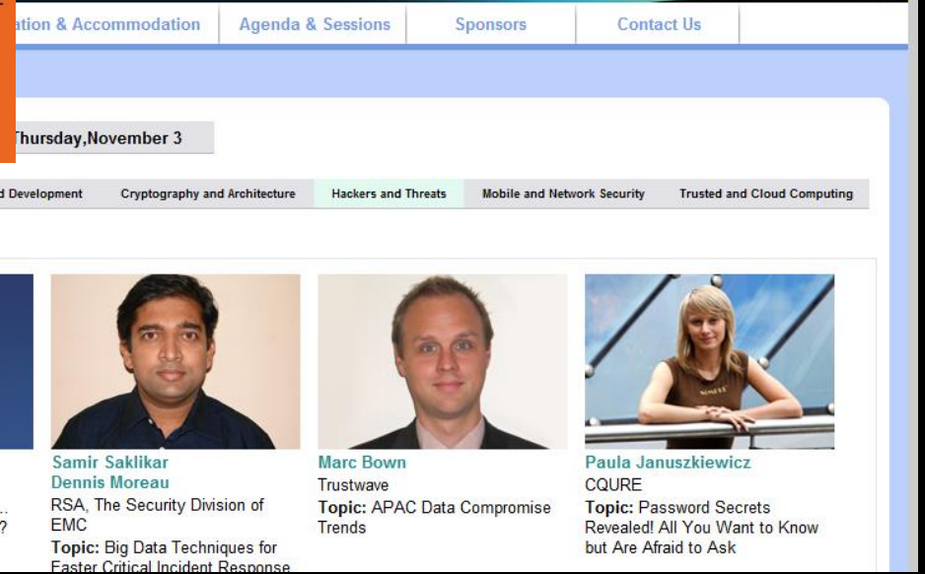

No.1
Speaker
Paula Januszkiewicz
CEO CQURE
She received
a "Best of Briefings" award at her
"CQTools: The New Ultimate Hacking Toolkit"
Black Hat Asia 2019 briefing session
black hat


black hat
USA 2017


ATTEND
TRAININGS
BRIEFINGS
ARSENAL
FEATURES
SCHEDULE
SEE ALL PRESENTERS
SPEAKER
PAULA JANUSZKIEWICZ
CQURE INC.


Brian Keller
Paula Januszkiewicz
Mark Minasi
John Craddock
Scott Woodgate
Marcus Murray


Where The World
Talks Security
November 2 – 3
China World Hotel
Beijing, China
2011
the adventures of
alice & bob


Thursday,November 3
General Sessions
Applications and Development
Cryptography and Architecture
Hackers and Threats
Mobile and Network Security
Trusted and Cloud Computing
Mark Kennedy
Symantec
Topic: Anti-Malware Industry... Cooperating. Are You Serious?
Samir Saklikar
Dennis Moreau
RSA, The Security Division of EMC
Topic: Big Data Techniques for
Marc Bown
Trustwave
Topic: APAC Data Compromise Trends
Paula Januszkiewicz
CQURE
Topic: Password Secrets Revealed! All You Want to Know but Are Afraid to Ask


There is pretty much always something you can find...

Searching for a Trace: Disk

Disk

Profile, NTUSER
Run dialog
Most Recently Used (MRU), Management Console (MMC)
Remote Desktop connections
Prefetch files
Recent documents
Automatic Destinations (LNK)
Security Log
RDP Operational Log
Application Logs
Temporary Internet Files
Deleted files – recoverable from the disk
NTFS Structures
Hiberfil.sys
Memory dumps

Demo: Data on Disk

Analysis

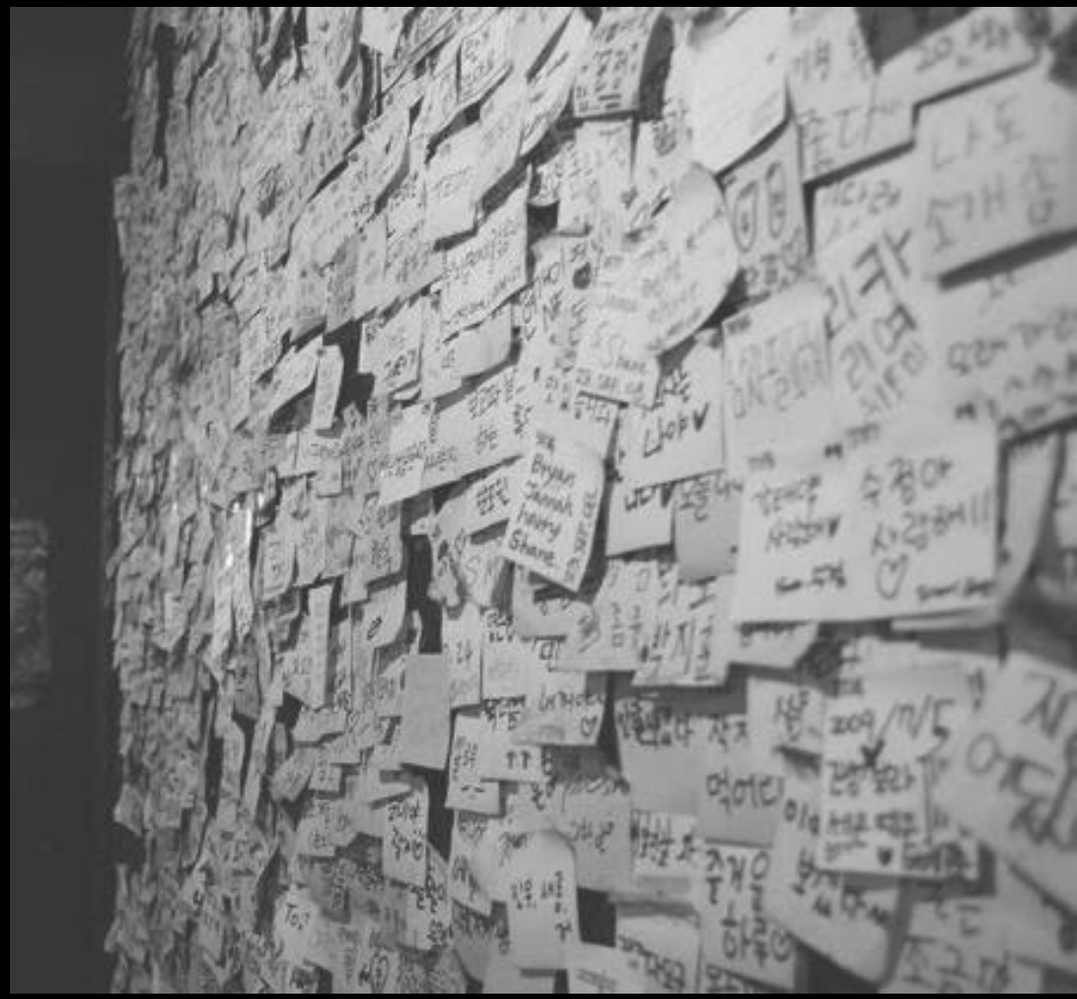
Techniques for Hiding vs. Recovering Data

File Level Games

Extension change
Joining files
Alternative data streams
Embedding
Playing with the content
Steganography
Deletion

Disk Level Games

Hiding data
Encryption



Demo: Data Recovery

Searching for a Trace: Memory

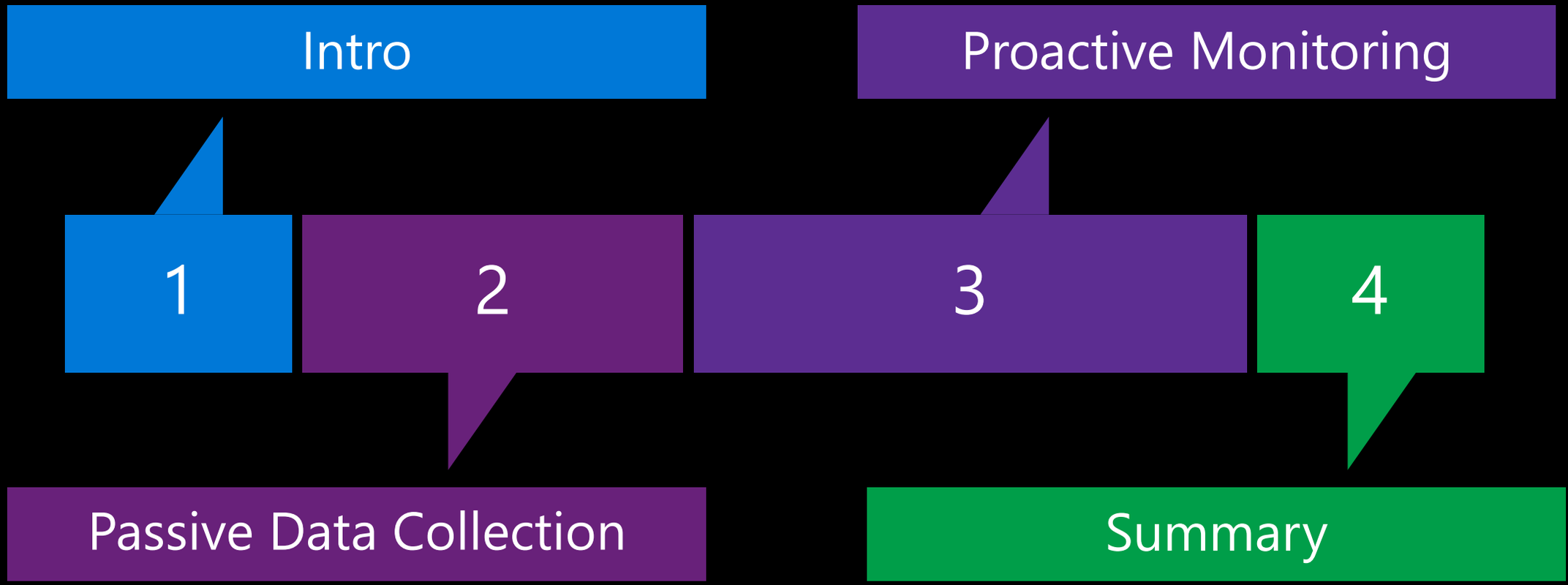
Memory

Handles
Processes
Hidden Processes (ActiveProcessLinks)
Files that can be extracted
Threads
Modules
Registry
API Hooks
Services
UserAssist
Shellbags
ShimCache
Event Logs
Timeline

Demo: Extracting Logs from Memory

Demo: Dump Analysis

Agenda


Intro
Proactive Monitoring
1
2
3
4
Passive Data Collection
Summary

Sysmon

Entry Information

Allows to build an attack timeline
Allows to define an entry point and anomalies
Collects and records system events to the Windows event log
It is free and easy to set up

Good practices

Filter out uninteresting events (image loads etc.)
Make sure event log is big enough
Centralize the events in a separate server

You can download Sysmon from Sysinternals.com

Demo: Sysmon in Action

Sysmon: Events and Filtering Examples

Filtering Rules

Include thread injections into lsass:

```
<CreateRemoteThread onmatch="include">
        <TargetImage condition="image">lsass.exe</TargetImage>
</CreateRemoteThread >
```

Exclude all Microsoft-signed image loads:

```
<ImageLoad onmatch="exclude">
        <Signature condition="contains">Microsoft</Signature>
        <Signature condition="contains">Windows</Signature>
</ImageLoad>
```

Recorded Events

Event ID 1: Process creation
Event ID 2: A process changed a file creation time
Event ID 3: Network connection
Event ID 4: Sysmon service state changed
Event ID 5: Process terminated
Event ID 6: Driver loaded
Event ID 7: Image loaded
Event ID 8: CreateRemoteThread
Event ID 9: RawAccessRead
Event ID 10: ProcessAccess

Demo: Sysmon Customized

- \+ getting info about the IP addresses

Demo: Sysmon and Network

Forensics adventures: Summary

→ Make sure all tracing features on the drive and in the system are enabled: USN, Prefech etc.

→ Image first then play

→ Create Incident Response Procedure (most of the Customers we start the adventure with do not have it…)

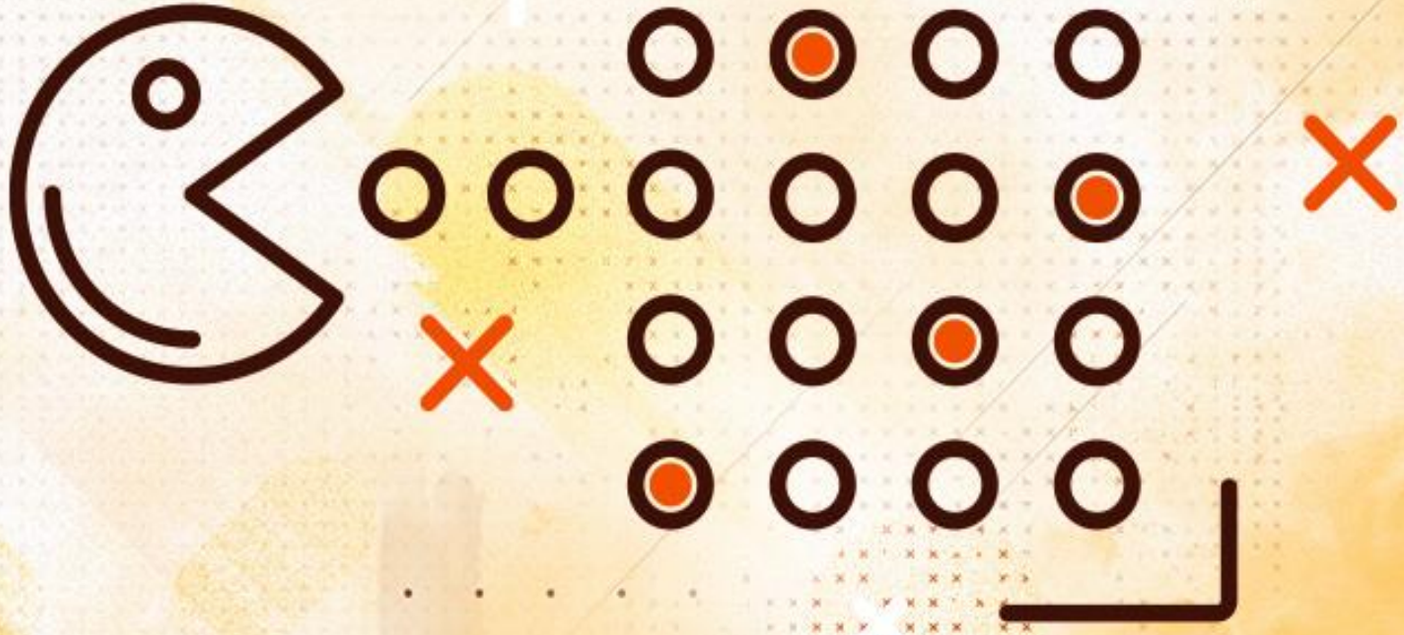

CQURE
Last call to register
with Paula Januszkiewicz
& Mike Jankowski-Lorek
ANALYSIS OF THE
POINTS OF ENTRY TO
YOUR INFRASTRUCTURE
Sign up

CQURE

Hardcore Cyber Security QUIZ 4.0

by CQURE Experts

Take the Quiz!



https://cqu.re/quiz

Advanced Windows Security Course 2020

6 weeks, 12 LIVE modules
Full of surprises + certificate

Paula Januszkiewicz
and Security Experts

CQURE

30-day Windows Security Crash Course

Get Security Professional Certification in 30 Days Online

Boost Your Career

Join Now!

https://cqu.re/30dayWindowsSecurity

CQURE

To get SLIDES & TOOLS

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

Sign up for our Newsletter
Cqureacademy.com/newsletter

Like CQURE Academy on Facebook
Facebook.com/CQURE

Follow me on Twitter
@PaulaCqure

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

DOWNLOAD THE TOOLS

https://resources.cqureacademy.com/tools/

Password: CQUREAcademy#123!