RSAConference2018
San Francisco | April 16 – 20 | Moscone Center

SESSION ID: HTA-T08

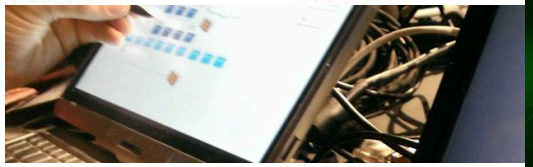
ADVENTURES IN THE UNDERLAND: TECHNIQUES AGAINST HACKERS EVADING THE HOOK

Paula Januszkiewicz

CQURE: CEO, Cybersecurity Expert
CQURE Academy: Trainer
MVP: Enterprise Security, MCT
Contact: paula@cqure.us | http://cqureacademy.com

@paulacqure
@CQUREAcademy

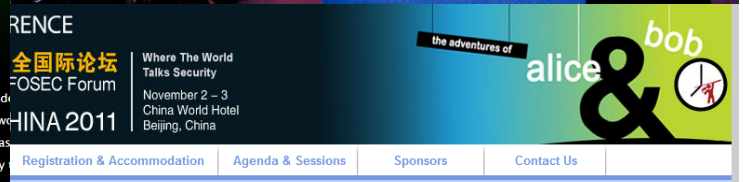

Featured TechEd 2012 Speakers
More featured speakers
Wally Mead
John Craddock



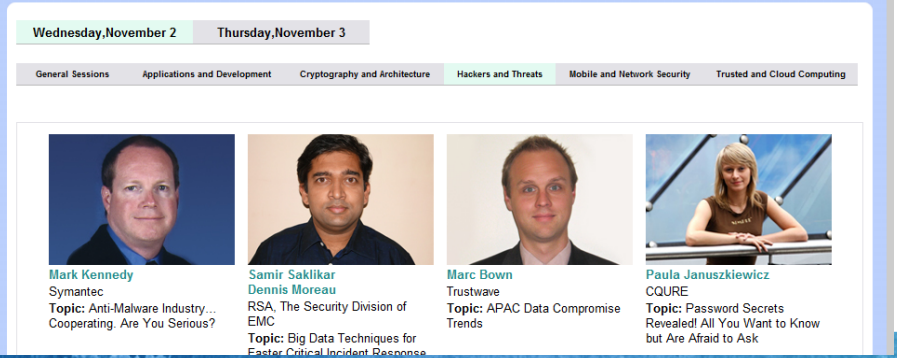

black hat
USA 2017
JULY
ATTEND
TRAININGS
BRIEFINGS
ARSENAL
FEATURES
SCHEDULE
SEE ALL PRESENTERS
SPEAKER
PAULA JANUSZKIEWICZ
COURE INC.


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
Europe 2013
Learn. Co
Join us in Ma


RENCE
全国际论坛
FOSEC Forum
HINA 2011
Where The World Talks Security
November 2 – 3
China World Hotel
Beijing, China
the adventures of
alice & bob
Registration & Accommodation
Agenda & Sessions
Sponsors
Contact Us


Brad Anderson
Jon DeVaan
Mark Russinovich
Brian Keller
Paula Januszkiewicz
Mark Minasi
Jeffrey Snover
John Craddock
Scott Woodgate
Marcus Murray


Wednesday,November 2
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

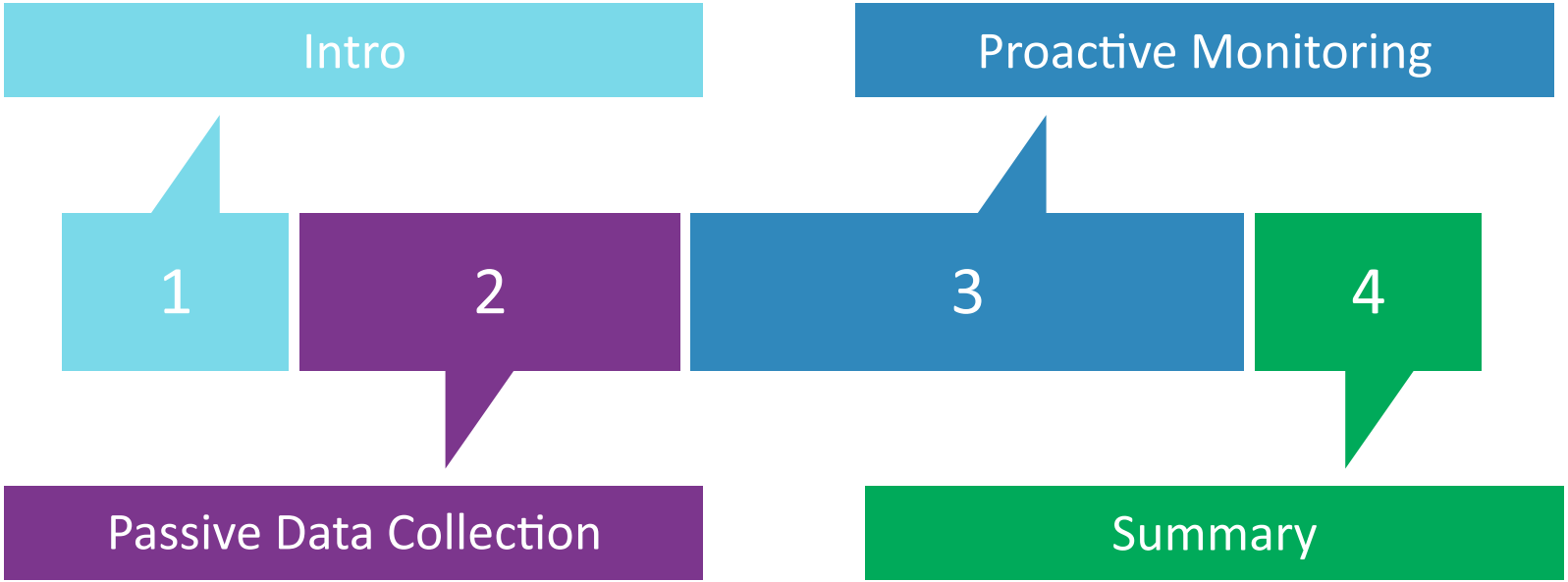
Handles
Processes
Hidden Processes (ActiveProcessLinks)
Files that can be extracted
Threads
Modules
Registry
API Hooks
Services
UserAssist
Shellbags
ShimCache
Event Logs
Timeline

DEMO: EXTRACTING LOGS FROM MEMORY

DEMO: DUMP ANALYSIS

DEMO: MEMORY ANALYSIS FROM THE SNAPSHOT

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
And more

DEMO: SYSMON CUSTOMIZED

DEMO: SYSMON AND NETWORK

+ getting info about the IP addresses

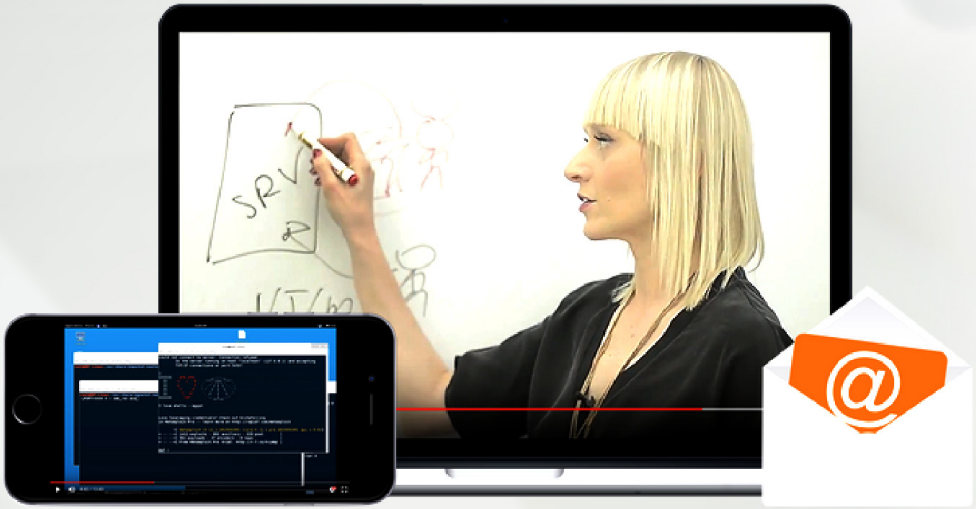
Apply: Adventures Summary

→ 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 ☺)

To get **SLIDES & TOOLS** (and not to miss out on my WEEKLY video tutorials):



Sign up for our weekly 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.)

CQURE
ACADEMY

IMPORTANT UPDATE If You Want To *Seriously* Level Up In This Area...

Test Yourself Against **Me** And See How Much You *Really* Know About Windows Security:

cqureacademy.com/QUIZ