SECTOR
Security Education Conference

Hackers' Perspective on Your Infrastructure and How to Keep Them Out of Your Life

October 21st, 2020,

SecTor Conference Keynote Session

CQURE

Hackers' Perspective on Your Infrastructure and How to Keep Them Out of Your Life

PAULA JANUSZKIEWICZ

CQURE: CEO, Penetration Tester; Security Expert

CQURE Academy: Trainer

Microsoft MVP on Cloud and Datacenter Management

Microsoft Regional Director

paula@cqure.us

@PaulaCqure @CQUREAcademy

www.cqureacademy.com **www.cqure.pl**

Adrianna

Doris

Kama

Artur

Liza

Paula

Mike

Krystian

Mariusz

Dominika

Magda

RSA CONFERENCE

HACKER FEST

Microsoft tech·days

Hacker | Halted

TecHFuse

Microsoft Technology Summit

black hat

TechEd Microsoft

NIC nordic infrastructure conference

cyberday

Microsoft Ignite

UT|messan.

SECTOR Security Education Conference

Adrian

Michal

Ken

Antoni

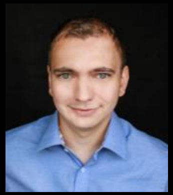
Janusz

Ola

Aga

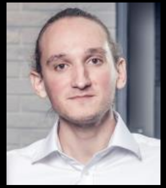
Ula

Grześ


Adrian

Milosz

Michael


Matus

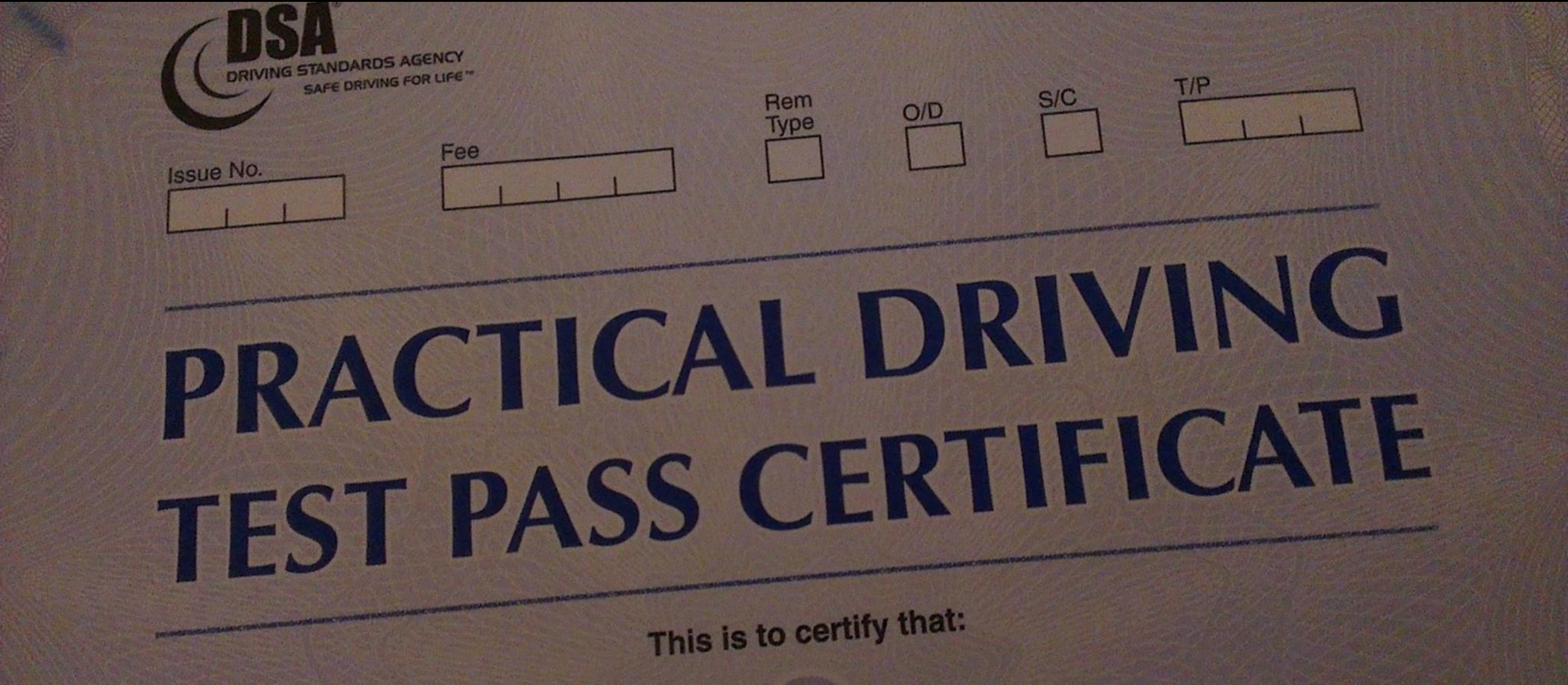
Kamil

Piotr

Awareness >> Behavior >> Culture

Each organization processing sensitive data must aim for a responsible security culture.

Awareness comes with experience



DSA
DRIVING STANDARDS AGENCY
SAFE DRIVING FOR LIFE™

Issue No.	Fee	Rem Type	O/D	S/C	T/P

PRACTICAL DRIVING TEST PASS CERTIFICATE

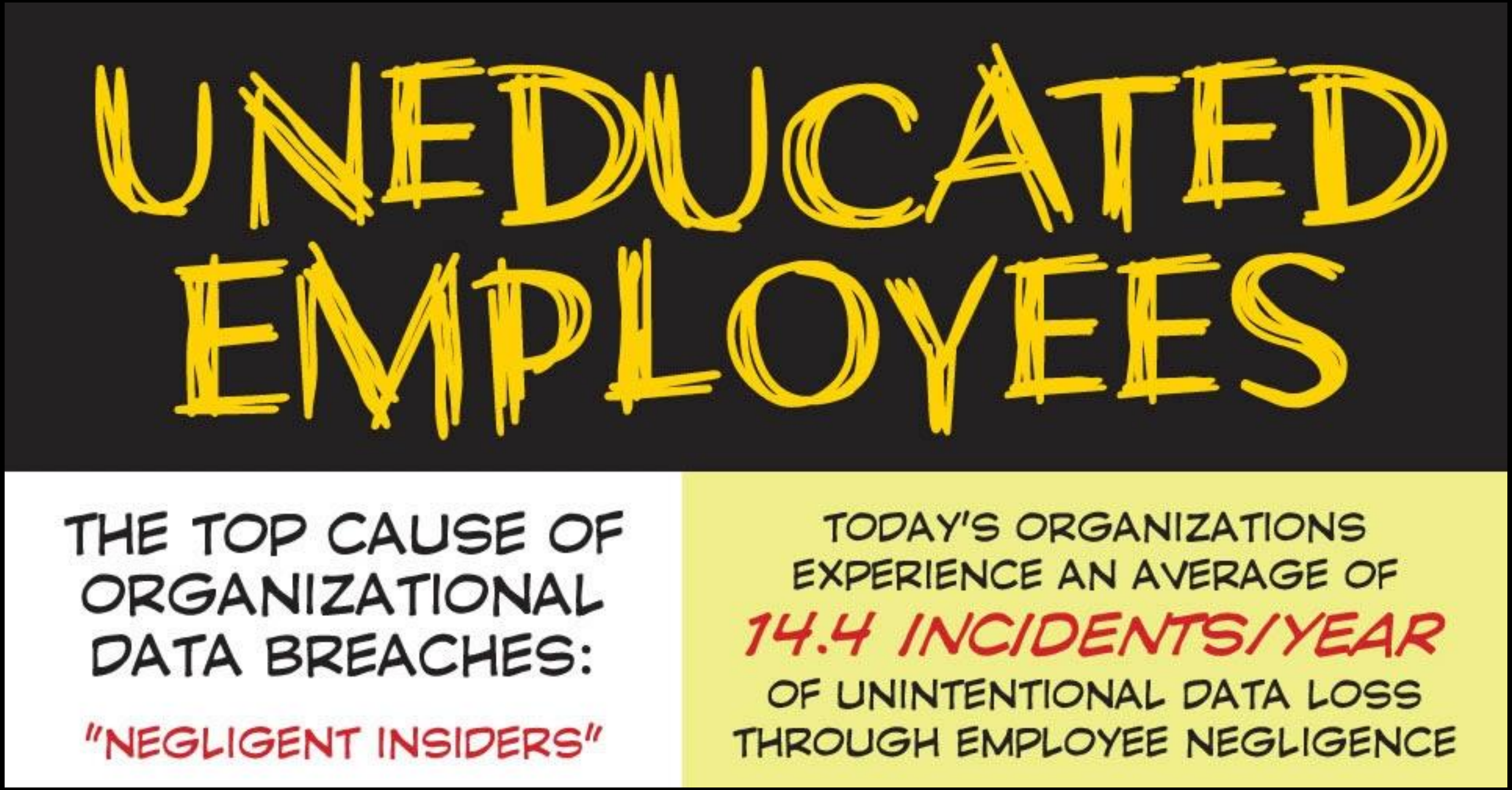
This is to certify that:

Behavior comes with awareness

Culture comes with understanding

Culture comes with understanding

Did you know that one of the main reasons for information loss are…



UNEDUCATED EMPLOYEES

THE TOP CAUSE OF ORGANIZATIONAL DATA BREACHES:

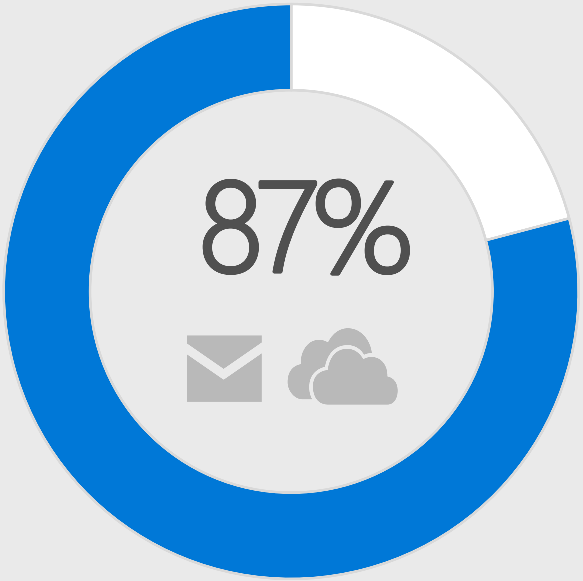
"NEGLIGENT INSIDERS"

TODAY'S ORGANIZATIONS EXPERIENCE AN AVERAGE OF

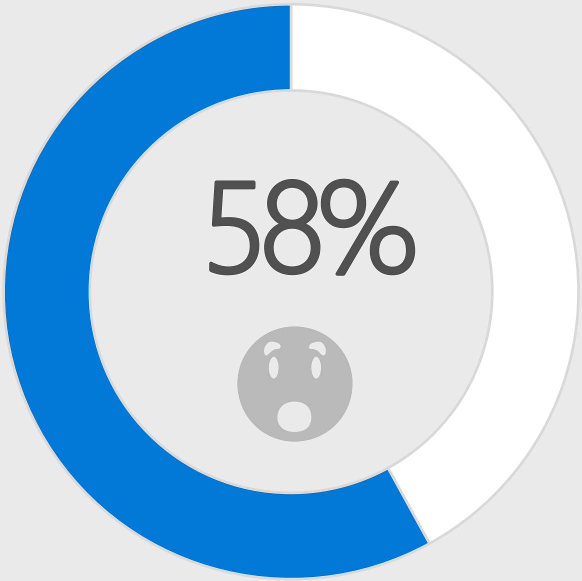
14.4 INCIDENTS/YEAR

OF UNINTENTIONAL DATA LOSS THROUGH EMPLOYEE NEGLIGENCE

Data Leakage



...of senior managers admit to **regularly** uploading work files to a personal email or cloud account[1]



Have accidentally sent sensitive information to the **wrong person**[1]

$240
PER RECORD

Average per record **cost of a data breach** across all industries[2]

[1] Stroz Friedberg, “On The Pulse: Information Security In American Business,” 2013

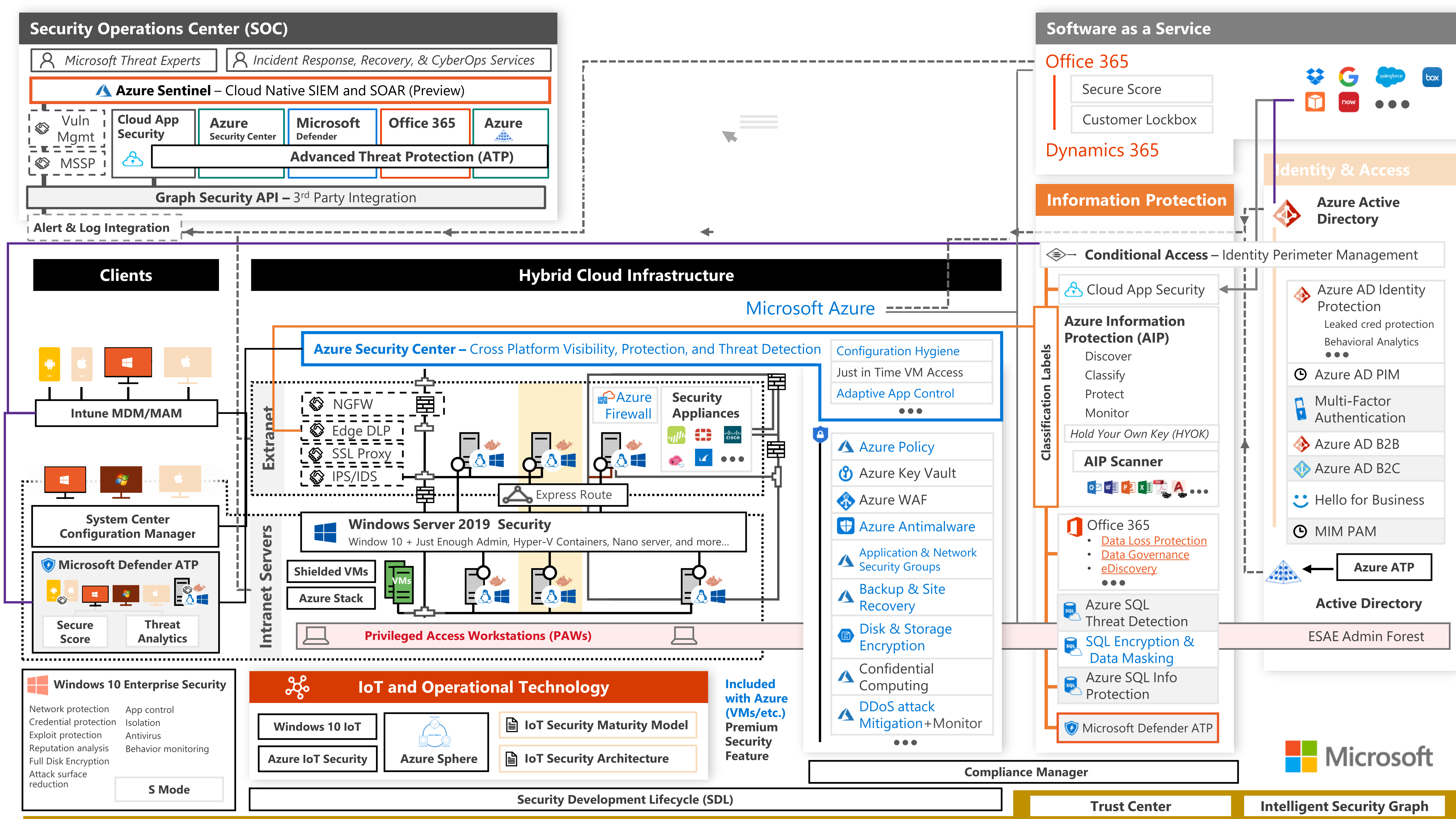
[2] HIPPA Secure Now, “A look at the cost of healthcare data breaches,” Art Gross, March 30, 2012

We have **the best** security solutions…

...but the security landscape has changed.

Cybersecurity Ventures predicts there will be additional 3.5 million cybersecurity job openings by 2021

*Source: Cybersecurity Ventures



Security Operations Center (SOC)

Microsoft Threat Experts

Incident Response, Recovery, & CyberOps Services

Azure Sentinel – Cloud Native SIEM and SOAR (Preview)

Vuln Mgmt

MSSP

Cloud App Security

Azure Security Center

Microsoft Defender

Office 365

Azure

Advanced Threat Protection (ATP)

Graph Security API – 3rd Party Integration

Alert & Log Integration

Software as a Service

Office 365

Secure Score

Customer Lockbox

Dynamics 365

Information Protection

Identity & Access

Azure Active Directory

Conditional Access – Identity Perimeter Management

Cloud App Security

Classification Labels

Azure Information Protection (AIP)

Discover

Classify

Protect

Monitor

Hold Your Own Key (HYOK)

AIP Scanner

•••

Office 365

- Data Loss Protection
- Data Governance
- eDiscovery

•••

Azure SQL Threat Detection

SQL Encryption & Data Masking

Azure SQL Info Protection

Microsoft Defender ATP

Azure AD Identity Protection

Leaked cred protection

Behavioral Analytics

•••

Azure AD PIM

Multi-Factor Authentication

Azure AD B2B

Azure AD B2C

Hello for Business

MIM PAM

Azure ATP

Active Directory

ESAE Admin Forest

Clients

Intune MDM/MAM

System Center Configuration Manager

Microsoft Defender ATP

Secure Score

Threat Analytics

Hybrid Cloud Infrastructure

Microsoft Azure

Azure Security Center – Cross Platform Visibility, Protection, and Threat Detection

Configuration Hygiene

Just in Time VM Access

Adaptive App Control

•••

Extranet

NGFW

Edge DLP

SSL Proxy

IPS/IDS

Azure Firewall

Security Appliances

•••

Express Route

Intranet Servers

Windows Server 2019 Security

Window 10 + Just Enough Admin, Hyper-V Containers, Nano server, and more…

Shielded VMs

VMs

Azure Stack

Privileged Access Workstations (PAWs)

Azure Policy

Azure Key Vault

Azure WAF

Azure Antimalware

Application & Network Security Groups

Backup & Site Recovery

Disk & Storage Encryption

Confidential Computing

DDoS attack Mitigation+Monitor

•••

Included with Azure (VMs/etc.)

Premium Security Feature

Windows 10 Enterprise Security

Network protection

Credential protection

Exploit protection

Reputation analysis

Full Disk Encryption

Attack surface reduction

App control

Isolation

Antivirus

Behavior monitoring

S Mode

IoT and Operational Technology

Windows 10 IoT

Azure IoT Security

Azure Sphere

IoT Security Maturity Model

IoT Security Architecture

Compliance Manager

Security Development Lifecycle (SDL)

Trust Center

Intelligent Security Graph

Microsoft

> "THERE ARE TWO KINDS OF BIG COMPANIES, THOSE WHO'VE BEEN HACKED, AND THOSE WHO DON'T KNOW THEY'VE BEEN HACKED."
>
> -JAMES COMEY, FBI DIRECTOR

200+

Median number of days attackers are present on a victims network before detection

80

Days after detection to full recovery

$3Trillion

Impact of lost productivity and growth

$3.5Million

Average cost of a data breach (15% YoY increase)

7 Security Issues that just should not happen

Here comes the 1st issue…

PASS WORD
WELCOME
Password1
123456

#1: PATHETIC PASSWORDS

15%

IN APPROXIMATELY 15% OF PHYSICAL SECURITY TESTS PERFORMED AT CLIENT SITES WRITTEN PASSWORDS WERE FOUND ON AND AROUND USER WORKSTATIONS

THE MOST COMMON CORPORATE PASSWORD IS Password1 BECAUSE IT JUST BARELY MEETS THE MINIMUM COMPLEXITY REQUIREMENTS OF ACTIVE DIRECTORY FOR LENGTH, CAPITALIZATION AND NUMERICAL FIGURES

#2: PEEPING ROM

WORKERS SURVEYED THAT SAY THEY HAVE BEEN ABLE TO SNEAK A PEEK AT A CO-WORKER'S OR STRANGER'S WORK STATION IN THE WORKPLACE OR A PUBLIC PLACE **71%**

ONE IN THREE WORKERS LEAVE THEIR COMPUTERS LOGGED ON TO NETWORK RESOURCES AND UNLOCKED WHEN THEY ARE AWAY FROM THEIR DESK

26.4% *OF MALWARE* IS KEY LOGGER OR APPLICATION-SPECIFIC — WHICH OFTEN REQUIRES DETAILED KNOWLEDGE OF OR PHYSICAL ACCESS TO A TARGETED SYSTEM

Bootkey:

Class names for keys from HKLM\SYSTEM\CCS\Control\Lsa

Data
GBG
JD
Skew1

SAM/NTDS.dit
(MD4 Hashes)
C:\windows\system32\config
C:\windows\system32\NTDS

LSA Secrets
(Service Accounts)
HKLM\SECURITY\Policy\Secrets

$MACHINE.ACC
(SYSTEM's Clear Text Password)

DPAPI_SYSTEM (Master Keys)
HKLM\SECURITY\Policy\Secrets

MSDCC2
(Cached Logon Data)
HKLM\SECURITY\Cache

More information: http://cqureacademy.com/blog

Classic Data Protection API

- Based on the following components:

Password, data blob, entropy

- Is not prone to password resets!

Protects from outsiders when being in offline access

Effectively protects users data

- Stores the password history

You need to be able to get access to some of your passwords from the past

Conclusion: OS greatly helps us to protect secrets

Classic DPAPI Flow: getting the system's secrets (easy)

Cached Logons: It used to be like this...

Windows 2003 / XP

The encryption algorithm is RC4.
The hash is used to verify authentication is calculated as follows:

```
DCC1 = MD4(MD4(Unicode(password)) .
LowerUnicode(username))
is
DCC1 = MD4(hashNTLM . LowerUnicode(username))
```

Usage in the attack

Before the attacks facilitated by pass-the-hash, we can only rejoice the "salting" by the username.

There are a number pre-computed tables for users as Administrator facilitating attacks on these hashes.

Cached Logons

Windows Vista / 2008 +

The encryption algorithm is AES128.

The hash is used to verify authentication is calculated as follows:

MSDCC2 = PBKDF2(HMAC-SHA1, Iterations, DCC1, LowerUnicode(username))

with DCC 1 calculated in the same way as for 2003 / XP.

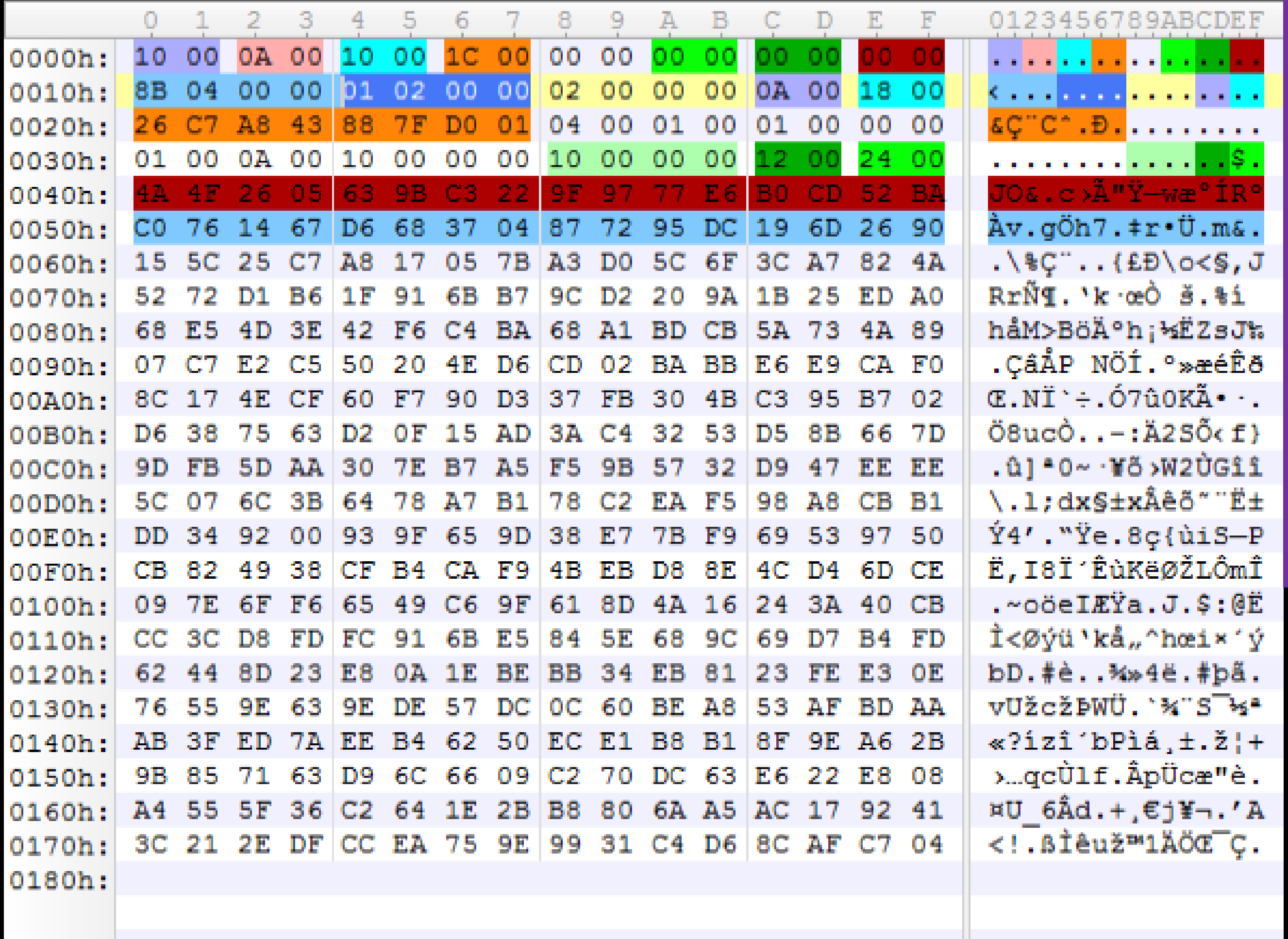
Usage in the attack

There is actually not much of a difference with XP / 2003!
No additional salting.

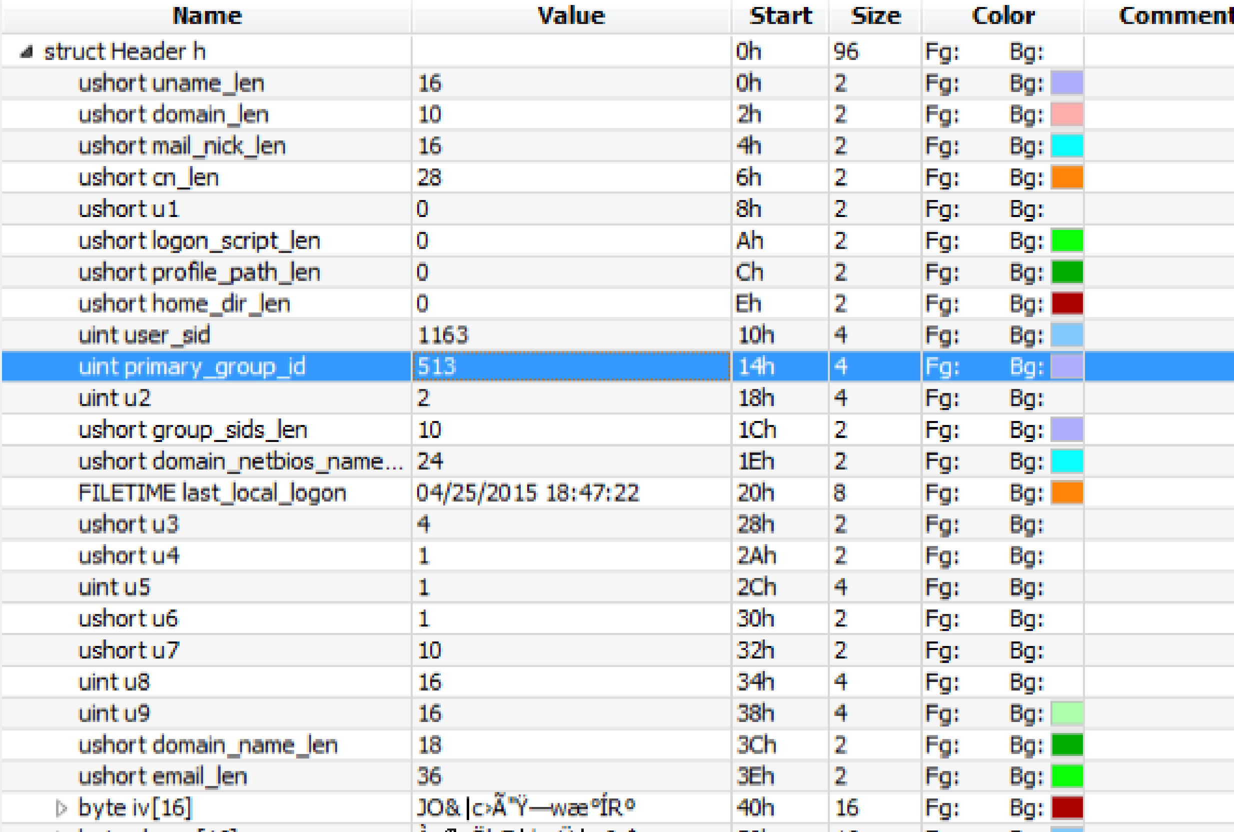
PBKDF2 introduced a new variable: the number of iterations SHA1 with the same salt as before (username).

Sysmon stores a hash base

Encrypted Cached Credentials: Legend



```
        0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
0000h: 10 00 0A 00 10 00 1C 00 00 00 00 00 00 00 00 00  ................
0010h: 8B 04 00 00 01 02 00 00 02 00 00 00 0A 00 18 00  ‹...............
0020h: 26 C7 A8 43 88 7F D0 01 04 00 01 00 01 00 00 00  &Ç¨C^.Ð.........
0030h: 01 00 0A 00 10 00 00 00 10 00 00 00 12 00 24 00  ..............$.
0040h: 4A 4F 26 05 63 9B C3 22 9F 97 77 E6 B0 CD 52 BA  JO&.c›Ã"Ÿ—wæ°ÍRº
0050h: C0 76 14 67 D6 68 37 04 87 72 95 DC 19 6D 26 90  Àv.gÖh7.‡r•Ü.m&.
0060h: 15 5C 25 C7 A8 17 05 7B A3 D0 5C 6F 3C A7 82 4A  .\%Ç¨..{£Ð\o<§‚J
0070h: 52 72 D1 B6 1F 91 6B B7 9C D2 20 9A 1B 25 ED A0  RrÑ¶.‘k·œÒ š.%í 
0080h: 68 E5 4D 3E 42 F6 C4 BA 68 A1 BD CB 5A 73 4A 89  håM>BöÄºh¡½ËZsJ‰
0090h: 07 C7 E2 C5 50 20 4E D6 CD 02 BA BB E6 E9 CA F0  .ÇâÅP NÖÍ.º»æéÊð
00A0h: 8C 17 4E CF 60 F7 90 D3 37 FB 30 4B C3 95 B7 02  Œ.NÏ`÷.Ó7û0KÃ•·.
00B0h: D6 38 75 63 D2 0F 15 AD 3A C4 32 53 D5 8B 66 7D  Ö8ucÒ..-:Ä2SÕ‹f}
00C0h: 9D FB 5D AA 30 7E B7 A5 F5 9B 57 32 D9 47 EE EE  .û]ª0~·¥õ›W2ÙGîî
00D0h: 5C 07 6C 3B 64 78 A7 B1 78 C2 EA F5 98 A8 CB B1  \.l;dx§±xÂêõ˜¨Ë±
00E0h: DD 34 92 00 93 9F 65 9D 38 E7 7B F9 69 53 97 50  Ý4’.“Ÿe.8ç{ùiS—P
00F0h: CB 82 49 38 CF B4 CA F9 4B EB D8 8E 4C D4 6D CE  Ë‚I8Ï´ÊùKëØŽLÔmÎ
0100h: 09 7E 6F F6 65 49 C6 9F 61 8D 4A 16 24 3A 40 CB  .~oöeIÆŸa.J.$:@Ë
0110h: CC 3C D8 FD FC 91 6B E5 84 5E 68 9C 69 D7 B4 FD  Ì<Øýü‘kå„^hœi×´ý
0120h: 62 44 8D 23 E8 0A 1E BE BB 34 EB 81 23 FE E3 0E  bD.#è..¾»4ë.#þã.
0130h: 76 55 9E 63 9E DE 57 DC 0C 60 BE A8 53 AF BD AA  vUžcžÞWÜ.`¾¨S¯½ª
0140h: AB 3F ED 7A EE B4 62 50 EC E1 B8 B1 8F 9E A6 2B  «?ízî´bPìá¸±.ž¦+
0150h: 9B 85 71 63 D9 6C 66 09 C2 70 DC 63 E6 22 E8 08  ›…qcÙlf.ÂpÜcæ"è.
0160h: A4 55 5F 36 C2 64 1E 2B B8 80 6A A5 AC 17 92 41  ¤U_6Âd.+¸€j¥¬.’A
0170h: 3C 21 2E DF CC EA 75 9E 99 31 C4 D6 8C AF C7 04  <!.ßÌêuž™1ÄÖŒ¯Ç.
0180h:
```



Name	Value	Start	Size	Color		Comment
struct Header h		0h	96	Fg:	Bg:	
ushort uname_len	16	0h	2	Fg:	Bg: ■	
ushort domain_len	10	2h	2	Fg:	Bg: ■	
ushort mail_nick_len	16	4h	2	Fg:	Bg: ■	
ushort cn_len	28	6h	2	Fg:	Bg: ■	
ushort u1	0	8h	2	Fg:	Bg:	
ushort logon_script_len	0	Ah	2	Fg:	Bg: ■	
ushort profile_path_len	0	Ch	2	Fg:	Bg: ■	
ushort home_dir_len	0	Eh	2	Fg:	Bg: ■	
uint user_sid	1163	10h	4	Fg:	Bg: ■	
uint primary_group_id	513	14h	4	Fg:	Bg: ■	
uint u2	2	18h	4	Fg:	Bg:	
ushort group_sids_len	10	1Ch	2	Fg:	Bg: ■	
ushort domain_netbios_name...	24	1Eh	2	Fg:	Bg: ■	
FILETIME last_local_logon	04/25/2015 18:47:22	20h	8	Fg:	Bg: ■	
ushort u3	4	28h	2	Fg:	Bg:	
ushort u4	1	2Ah	2	Fg:	Bg:	
uint u5	1	2Ch	4	Fg:	Bg:	
ushort u6	1	30h	2	Fg:	Bg:	
ushort u7	10	32h	2	Fg:	Bg:	
uint u8	16	34h	4	Fg:	Bg:	
uint u9	16	38h	4	Fg:	Bg: ■	
ushort domain_name_len	18	3Ch	2	Fg:	Bg: ■	
ushort email_len	36	3Eh	2	Fg:	Bg: ■	
byte iv[16]	JO& |c›Ã"Ÿ—wæ°ÍRº	40h	16	Fg:	Bg: ■	

Encrypted Cached Credentials
DK = PBKDF2(PRF, Password, Salt, c, dkLen)

Microsoft's implementation: MSDCC2= PBKDF2(HMAC-SHA1, DCC1, username, 10240, 16)

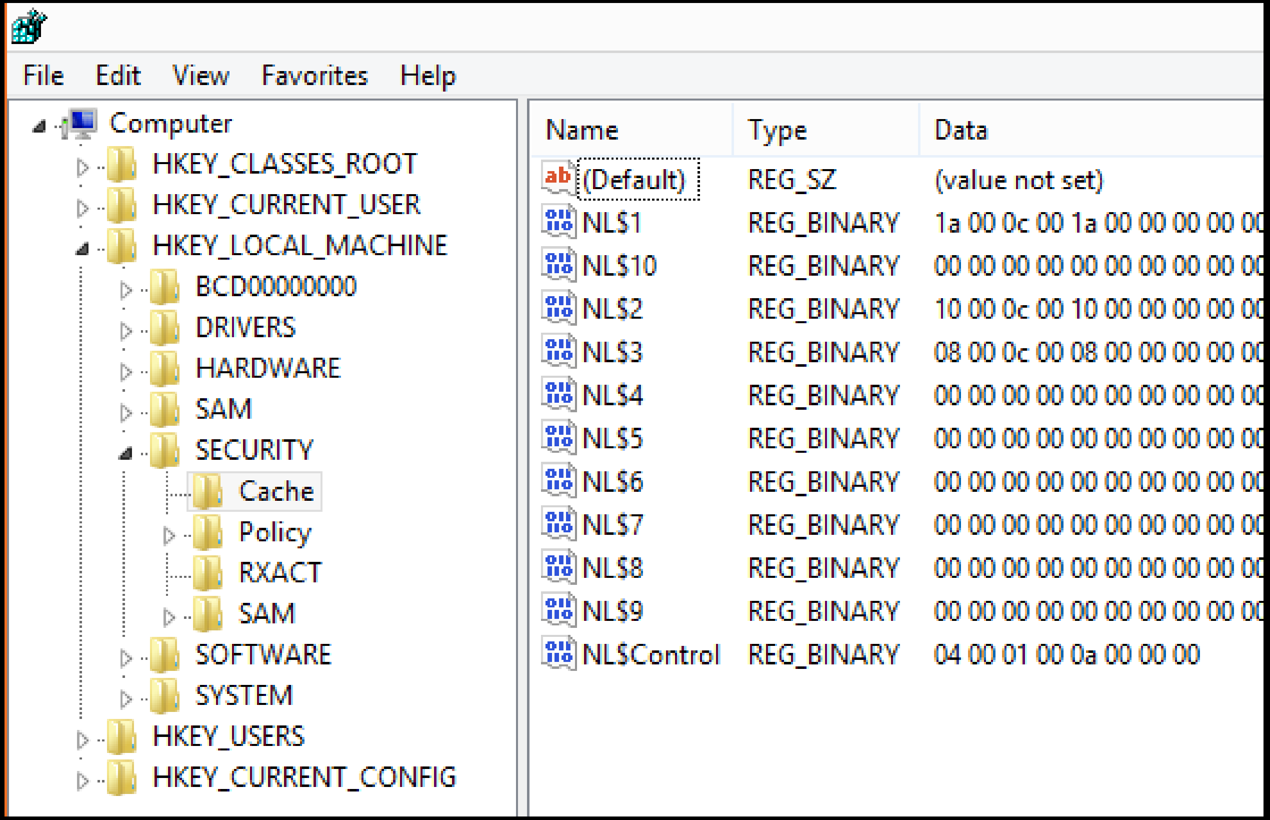
Cached Logons: Iterations

The number of iterations in PBKDF2, it is configurable through the registry:

HKEY_LOCAL_MACHINE\SECURITY\Cache DWORD (32) NL$IterationCount

If the number is less than 10240, it is a multiplier by 1024 (20 therefore gives 20480 iterations)

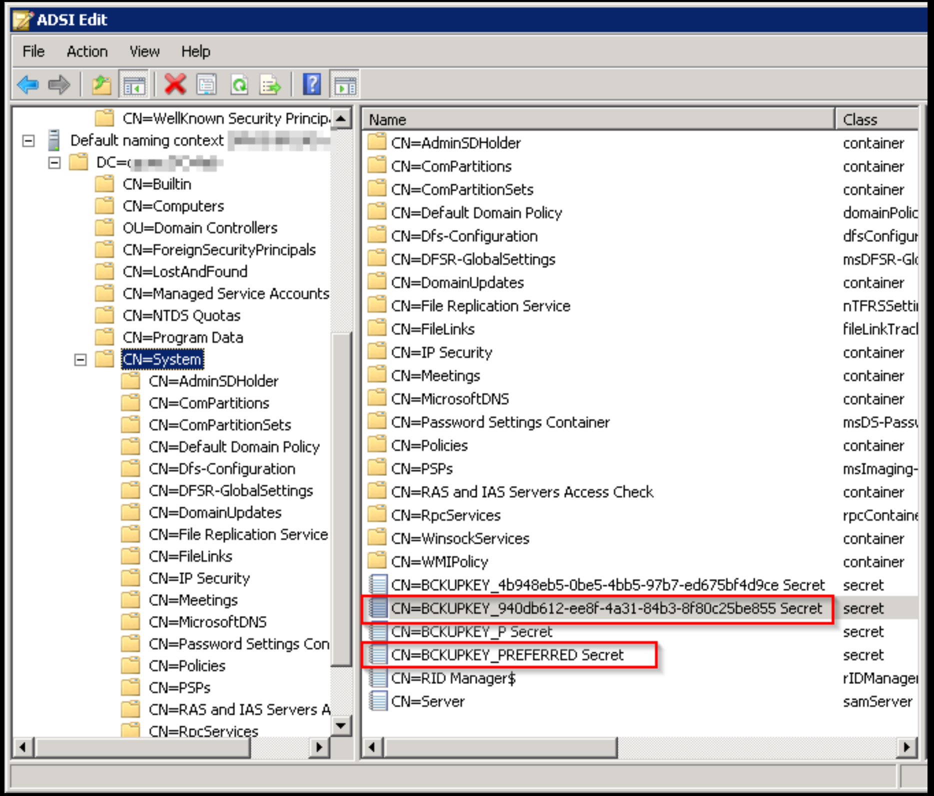
If the number is greater than 10240, it is the number of iterations (rounded to 1024)



Name	Type	Data
(Default)	REG_SZ	(value not set)
NL$1	REG_BINARY	1a 00 0c 00 1a 00 00 00 00 00
NL$10	REG_BINARY	00 00 00 00 00 00 00 00 00 00
NL$2	REG_BINARY	10 00 0c 00 10 00 00 00 00 00
NL$3	REG_BINARY	08 00 0c 00 08 00 00 00 00 00
NL$4	REG_BINARY	00 00 00 00 00 00 00 00 00 00
NL$5	REG_BINARY	00 00 00 00 00 00 00 00 00 00
NL$6	REG_BINARY	00 00 00 00 00 00 00 00 00 00
NL$7	REG_BINARY	00 00 00 00 00 00 00 00 00 00
NL$8	REG_BINARY	00 00 00 00 00 00 00 00 00 00
NL$9	REG_BINARY	00 00 00 00 00 00 00 00 00 00
NL$Control	REG_BINARY	04 00 01 00 0a 00 00 00

Classic DPAPI Flow: getting the user’s secrets

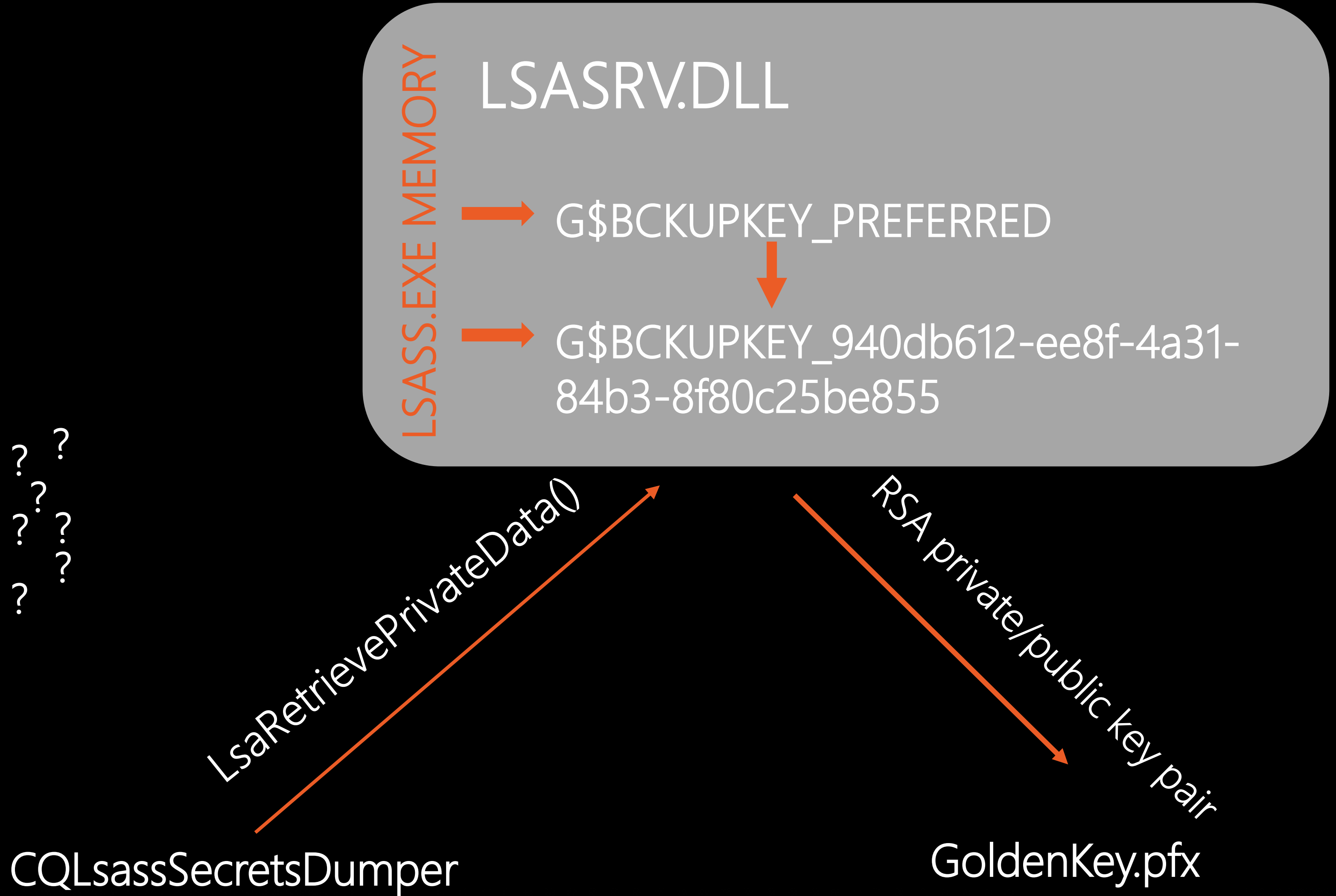
Retrieving Golden Key from LSA – CQURE's way



```
CN=WellKnown Security Princip
⊟ Default naming context [redacted]
  ⊟ DC=[redacted]
      CN=Builtin
      CN=Computers
      OU=Domain Controllers
      CN=ForeignSecurityPrincipals
      CN=LostAndFound
      CN=Managed Service Accounts
      CN=NTDS Quotas
      CN=Program Data
    ⊟ CN=System
        CN=AdminSDHolder
        CN=ComPartitions
        CN=ComPartitionSets
        CN=Default Domain Policy
        CN=Dfs-Configuration
        CN=DFSR-GlobalSettings
        CN=DomainUpdates
        CN=File Replication Service
        CN=FileLinks
        CN=IP Security
        CN=Meetings
        CN=MicrosoftDNS
        CN=Password Settings Con
        CN=Policies
        CN=PSPs
        CN=RAS and IAS Servers A
        CN=RpcServices
```

Name	Class
CN=AdminSDHolder	container
CN=ComPartitions	container
CN=ComPartitionSets	container
CN=Default Domain Policy	domainPolic
CN=Dfs-Configuration	dfsConfigur
CN=DFSR-GlobalSettings	msDFSR-Gl
CN=DomainUpdates	container
CN=File Replication Service	nTFRSSetti
CN=FileLinks	fileLinkTracl
CN=IP Security	container
CN=Meetings	container
CN=MicrosoftDNS	container
CN=Password Settings Container	msDS-Pass
CN=Policies	container
CN=PSPs	msImaging-
CN=RAS and IAS Servers Access Check	container
CN=RpcServices	rpcContaine
CN=WinsockServices	container
CN=WMIPolicy	container
CN=BCKUPKEY_4b948eb5-0be5-4bb5-97b7-ed675bf4d9ce Secret	secret
CN=BCKUPKEY_940db612-ee8f-4a31-84b3-8f80c25be855 Secret	secret
CN=BCKUPKEY_P Secret	secret
CN=BCKUPKEY_PREFERRED Secret	secret
CN=RID Manager$	rIDManager
CN=Server	samServer

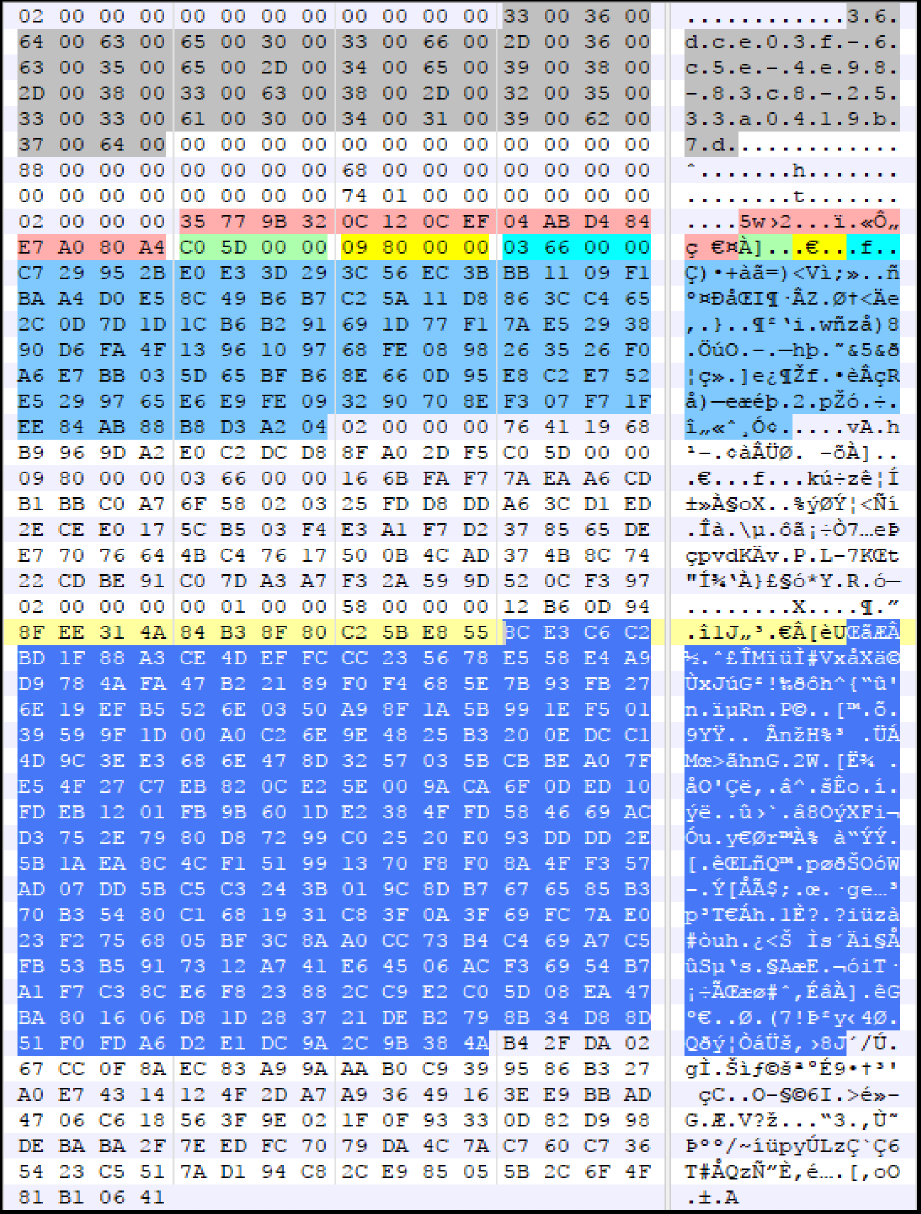
AD secret? HOW?!



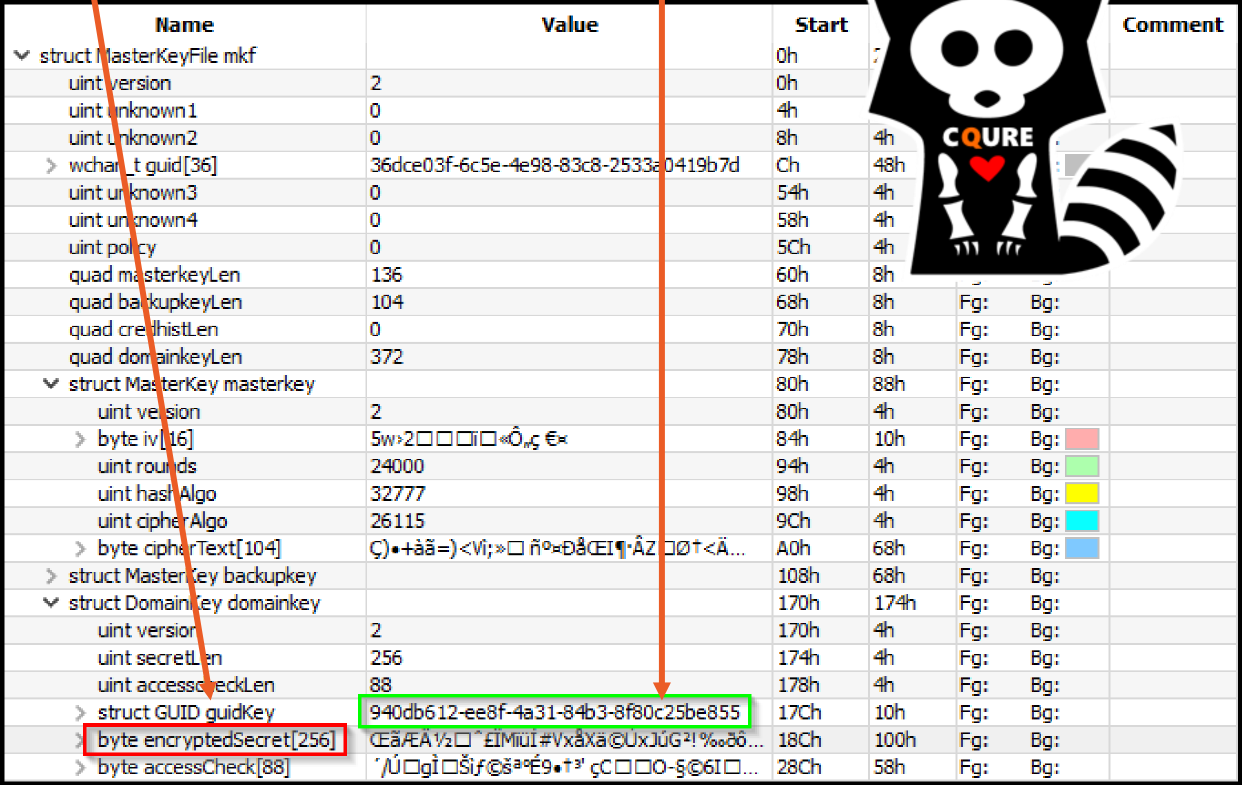
DPAPI-AD: How did we do it?

DomainKey contains some GUID and
256-byte len secret – RSA??

Dude, look in the AD...

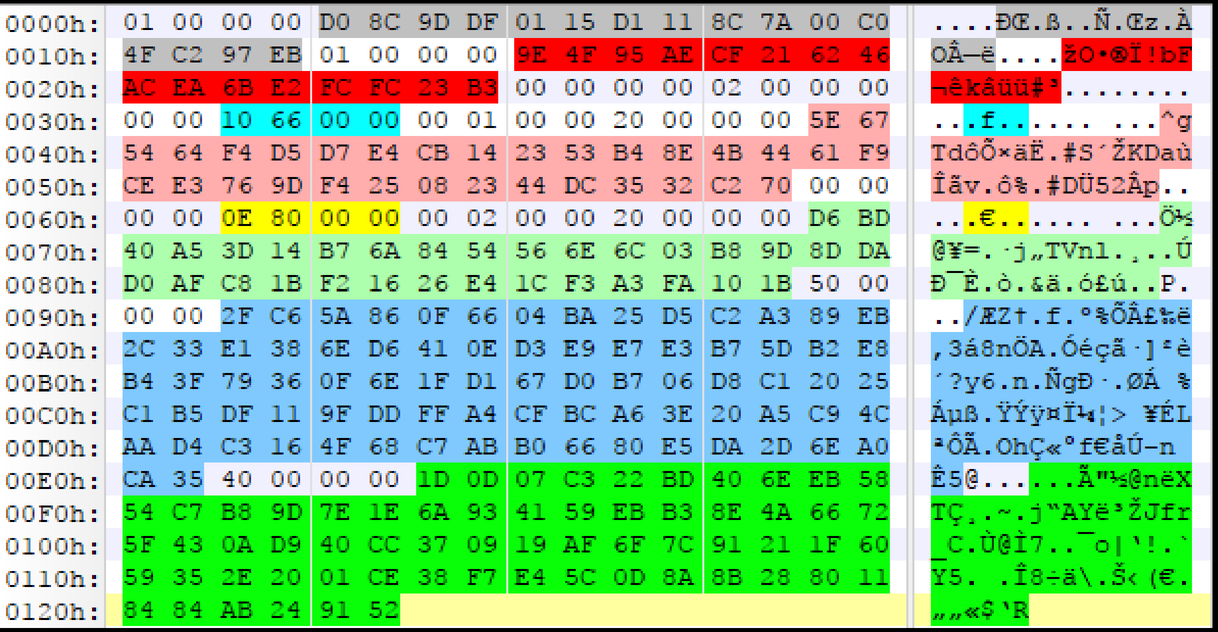


```
02 00 00 00 00 00 00 00 00 00 00 00 33 00 36 00  ............3.6.
64 00 63 00 65 00 30 00 33 00 66 00 2D 00 36 00  d.c.e.0.3.f.-.6.
63 00 35 00 65 00 2D 00 34 00 65 00 39 00 38 00  c.5.e.-.4.e.9.8.
2D 00 38 00 33 00 63 00 38 00 2D 00 32 00 35 00  -.8.3.c.8.-.2.5.
33 00 33 00 61 00 30 00 34 00 31 00 39 00 62 00  3.3.a.0.4.1.9.b.
37 00 64 00 00 00 00 00 00 00 00 00 00 00 00 00  7.d.............
88 00 00 00 00 00 00 00 68 00 00 00 00 00 00 00  ˆ.......h.......
00 00 00 00 00 00 00 00 74 01 00 00 00 00 00 00  ........t.......
02 00 00 00 35 77 9B 32 0C 12 0C EF 04 AB D4 84  ....5w›2...ï.«Ô„
E7 A0 80 A4 C0 5D 00 00 09 80 00 00 03 66 00 00  ç €¤À]...€...f..
C7 29 95 2B E0 E3 3D 29 3C 56 EC 3B BB 11 09 F1  Ç)•+àã=)<Vì;»..ñ
BA A4 D0 E5 8C 49 B6 B7 C2 5A 11 D8 86 3C C4 65  º¤ÐåŒI¶·ÂZ.Ø†<Äe
2C 0D 7D 1D 1C B6 B2 91 69 1D 77 F1 7A E5 29 38  ,.}..¶²'i.wñzå)8
90 D6 FA 4F 13 96 10 97 68 FE 08 98 26 35 26 F0  .ÖúO.–.—hþ.˜&5&ð
A6 E7 BB 03 5D 65 BF B6 8E 66 0D 95 E8 C2 E7 52  ¦ç».]e¿¶Žf.•èÂçR
E5 29 97 65 E6 E9 FE 09 32 90 70 8E F3 07 F7 1F  å)—eæéþ.2.pŽó.÷.
EE 84 AB 88 B8 D3 A2 04 02 00 00 00 76 41 19 68  î„«ˆ¸Ó¢.....vA.h
B9 96 9D A2 E0 C2 DC D8 8F A0 2D F5 C0 5D 00 00  ¹–.¢àÂÜØ. -õÀ]..
09 80 00 00 03 66 00 00 16 6B FA F7 7A EA A6 CD  .€...f...kú÷zê¦Í
B1 BB C0 A7 6F 58 02 03 25 FD D8 DD A6 3C D1 ED  ±»À§oX..%ýØÝ¦<Ñí
2E CE E0 17 5C B5 03 F4 E3 A1 F7 D2 37 85 65 DE  .Îà.\µ.ôã¡÷Ò7…eÞ
E7 70 76 64 4B C4 76 17 50 0B 4C AD 37 4B 8C 74  çpvdKÄv.P.L-7KŒt
22 CD BE 91 C0 7D A3 A7 F3 2A 59 9D 52 0C F3 97  "Í¾'À}£§ó*Y.R.ó—
02 00 00 00 00 01 00 00 58 00 00 00 12 B6 0D 94  ........X....¶."
8F EE 31 4A 84 B3 8F 80 C2 5B E8 55 BC E3 C6 C2  .î1J„³.€Â[èUŒãÆÂ
BD 1F 88 A3 CE 4D EF FC CC 23 56 78 E5 58 E4 A9  ½.ˆ£ÎMïüÌ#VxåXä©
D9 78 4A FA 47 B2 21 89 F0 F4 68 5E 7B 93 FB 27  ÙxJúG²!‰ðôh^{"û'
6E 19 EF B5 52 6E 03 50 A9 8F 1A 5B 99 1E F5 01  n.ïµRn.P©..[™.õ.
39 59 9F 1D 00 A0 C2 6E 9E 48 25 B3 20 0E DC C1  9YŸ.. ÂnžH%³ .ÜÁ
4D 9C 3E E3 68 6E 47 8D 32 57 03 5B CB BE A0 7F  Mœ>ãhnG.2W.[Ë¾ .
E5 4F 27 C7 EB 82 0C E2 5E 00 9A CA 6F 0D ED 10  åO'Çë,.â^.šÊo.í.
FD EB 12 01 FB 9B 60 1D E2 38 4F FD 58 46 69 AC  ýë..û›`.â8OýXFi¬
D3 75 2E 79 80 D8 72 99 C0 25 20 E0 93 DD DD 2E  Óu.y€Ør™À% à"ÝÝ.
5B 1A EA 8C 4C F1 51 99 13 70 F8 F0 8A 4F F3 57  [.êŒLñQ™.pøðŠOóW
AD 07 DD 5B C5 C3 24 3B 01 9C 8D B7 67 65 85 B3  -.Ý[ÅÃ$;.œ.·ge…³
70 B3 54 80 C1 68 19 31 C8 3F 0A 3F 69 FC 7A E0  p³T€Áh.1È?.?iüzà
23 F2 75 68 05 BF 3C 8A A0 CC 73 B4 C4 69 A7 C5  #òuh.¿<Š Ìs´Äi§Å
FB 53 B5 91 73 12 A7 41 E6 45 06 AC F3 69 54 B7  ûSµ's.§AæE.¬óiT·
A1 F7 C3 8C E6 F8 23 88 2C C9 E2 C0 5D 08 EA 47  ¡÷ÃŒæø#ˆ,ÉâÀ].êG
BA 80 16 06 D8 1D 28 37 21 DE B2 79 8B 34 D8 8D  º€..Ø.(7!Þ²y‹4Ø.
51 F0 FD A6 D2 E1 DC 9A 2C 9B 38 4A B4 2F DA 02  Qðý¦ÒáÜš,›8J´/Ú.
67 CC 0F 8A EC 83 A9 9A AA B0 C9 39 95 86 B3 27  gÌ.Šìƒ©šª°É9•†³'
A0 E7 43 14 12 4F 2D A7 A9 36 49 16 3E E9 BB AD   çC..O-§©6I.>é»-
47 06 C6 18 56 3F 9E 02 1F 0F 93 33 0D 82 D9 98  G.Æ.V?ž..."3.,Ù˜
DE BA BA 2F 7E ED FC 70 79 DA 4C 7A C7 60 C7 36  Þºº/~íüpyÚLzÇ`Ç6
54 23 C5 51 7A D1 94 C8 2C E9 85 05 5B 2C 6F 4F  T#ÅQzÑ"È,é….[,oO
81 B1 06 41                                      .±.A
```

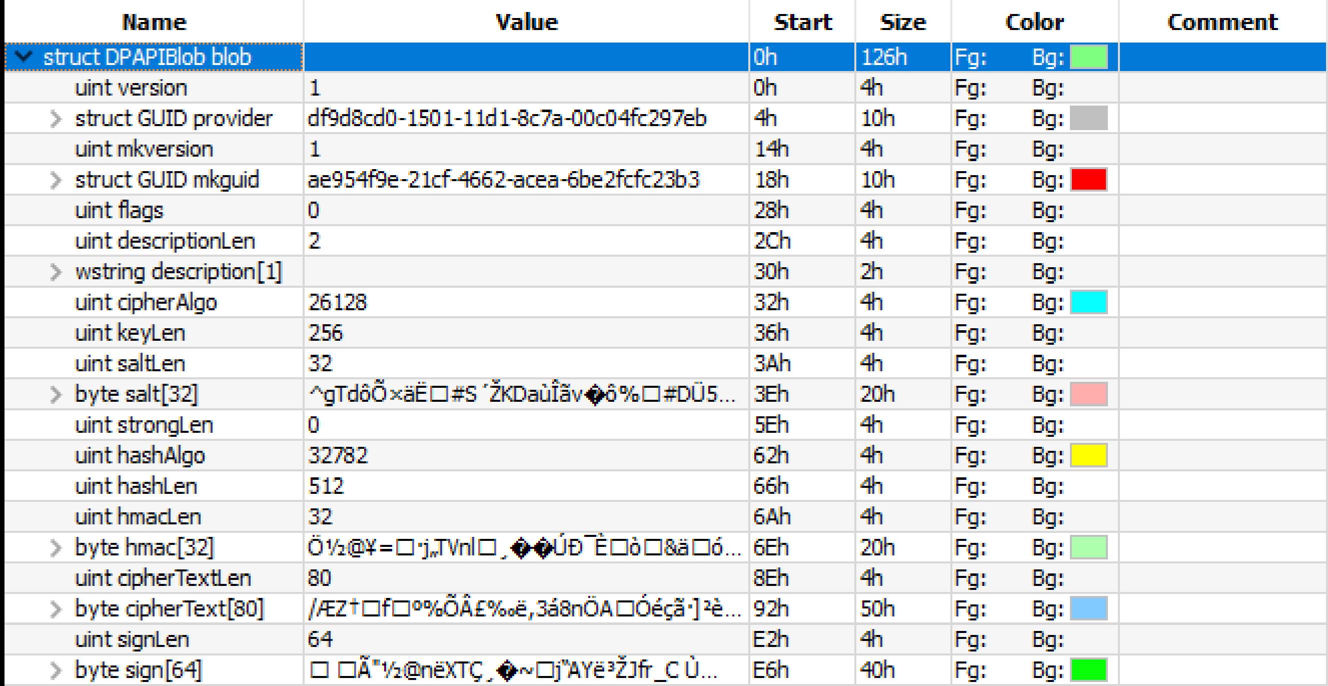


Name	Value	Start			Comment
struct MasterKeyFile mkf		0h			
uint version	2	0h			
uint unknown1	0	4h			
uint unknown2	0	8h	4h		
wchar_t guid[36]	36dce03f-6c5e-4e98-83c8-2533a0419b7d	Ch	48h		
uint unknown3	0	54h	4h		
uint unknown4	0	58h	4h		
uint policy	0	5Ch	4h		
quad masterkeyLen	136	60h	8h		
quad backupkeyLen	104	68h	8h	Fg: Bg:	
quad credhistLen	0	70h	8h	Fg: Bg:	
quad domainkeyLen	372	78h	8h	Fg: Bg:	
struct MasterKey masterkey		80h	88h	Fg: Bg:	
uint version	2	80h	4h	Fg: Bg:	
byte iv[16]	5w›2□□□ï□«Ô„ç €¤	84h	10h	Fg: Bg: 🟥	
uint rounds	24000	94h	4h	Fg: Bg: 🟩	
uint hashAlgo	32777	98h	4h	Fg: Bg: 🟨	
uint cipherAlgo	26115	9Ch	4h	Fg: Bg: 🟦	
byte cipherText[104]	Ç)•+àã=)<Vì;»□ ñº¤ÐåŒI¶·ÂZ □Ø†<Ä...	A0h	68h	Fg: Bg: 🟦	
struct MasterKey backupkey		108h	68h	Fg: Bg:	
struct DomainKey domainkey		170h	174h	Fg: Bg:	
uint version	2	170h	4h	Fg: Bg:	
uint secretLen	256	174h	4h	Fg: Bg:	
uint accessCheckLen	88	178h	4h	Fg: Bg:	
struct GUID guidKey	940db612-ee8f-4a31-84b3-8f80c25be855	17Ch	10h	Fg: Bg:	
byte encryptedSecret[256]	ŒãÆÂ½□ˆ£ÎMïüÌ#VxåXä©ÙxJúG²!‰ðô...	18Ch	100h	Fg: Bg:	
byte accessCheck[88]	´/Ú□gÌ□Šìƒ©šª°É9•†³' çC□□O-§©6I□...	28Ch	58h	Fg: Bg:	

DPAPI in pictures Example: KeePass ProtectedUserKey.bin



```
0000h: 01 00 00 00 D0 8C 9D DF 01 15 D1 11 8C 7A 00 C0  ....ÐŒ.ß..Ñ.Œz.À
0010h: 4F C2 97 EB 01 00 00 00 9E 4F 95 AE CF 21 62 46  OÂ—ë....žO•®Ï!bF
0020h: AC EA 6B E2 FC FC 23 B3 00 00 00 00 02 00 00 00  ¬êkâüü#³........
0030h: 00 00 10 66 00 00 00 01 00 00 20 00 00 00 5E 67  ...f.... ....^g
0040h: 54 64 F4 D5 D7 E4 CB 14 23 53 B4 8E 4B 44 61 F9  TdôÕ×äË.#S´ŽKDaù
0050h: CE E3 76 9D F4 25 08 23 44 DC 35 32 C2 70 00 00  Îãv.ô%.#DÜ52Âp..
0060h: 00 00 0E 80 00 00 00 02 00 00 20 00 00 00 D6 BD  ...€.... ...Ö½
0070h: 40 A5 3D 14 B7 6A 84 54 56 6E 6C 03 B8 9D 8D DA  @¥=.·j„TVnl.¸..Ú
0080h: D0 AF C8 1B F2 16 26 E4 1C F3 A3 FA 10 1B 50 00  Ð¯È.ò.&ä.ó£ú..P.
0090h: 00 00 2F C6 5A 86 0F 66 04 BA 25 D5 C2 A3 89 EB  ../ÆZ†.f.º%ÕÂ£‰ë
00A0h: 2C 33 E1 38 6E D6 41 0E D3 E9 E7 E3 B7 5D B2 E8  ,3á8nÖA.Óéçã·]²è
00B0h: B4 3F 79 36 0F 6E 1F D1 67 D0 B7 06 D8 C1 20 25  ´?y6.n.ÑgÐ·.ØÁ %
00C0h: C1 B5 DF 11 9F DD FF A4 CF BC A6 3E 20 A5 C9 4C  Áµß.ŸÝÿ¤Ï¼¦> ¥ÉL
00D0h: AA D4 C3 16 4F 68 C7 AB B0 66 80 E5 DA 2D 6E A0  ªÔÃ.OhÇ«°f€åÚ-n 
00E0h: CA 35 40 00 00 00 1D 0D 07 C3 22 BD 40 6E EB 58  Ê5@.......Ã"½@nëX
00F0h: 54 C7 B8 9D 7E 1E 6A 93 41 59 EB B3 8E 4A 66 72  TÇ¸.~.j“AYë³ŽJfr
0100h: 5F 43 0A D9 40 CC 37 09 19 AF 6F 7C 91 21 1F 60  _C.Ù@Ì7..¯o|'!.`
0110h: 59 35 2E 20 01 CE 38 F7 E4 5C 0D 8A 8B 28 80 11  Y5. .Î8÷ä\.Š‹(€.
0120h: 84 84 AB 24 91 52                                „„«$'R
```



Name	Value	Start	Size	Color	Comment
struct DPAPIBlob blob		0h	126h	Fg: Bg: 🟩	
uint version	1	0h	4h	Fg: Bg:	
struct GUID provider	df9d8cd0-1501-11d1-8c7a-00c04fc297eb	4h	10h	Fg: Bg: ⬜	
uint mkversion	1	14h	4h	Fg: Bg:	
struct GUID mkguid	ae954f9e-21cf-4662-acea-6be2fcfc23b3	18h	10h	Fg: Bg: 🟥	
uint flags	0	28h	4h	Fg: Bg:	
uint descriptionLen	2	2Ch	4h	Fg: Bg:	
wstring description[1]		30h	2h	Fg: Bg:	
uint cipherAlgo	26128	32h	4h	Fg: Bg: 🟦	
uint keyLen	256	36h	4h	Fg: Bg:	
uint saltLen	32	3Ah	4h	Fg: Bg:	
byte salt[32]	^gTdôÕ×äË□#S´ŽKDaùÎãv�ô%□#DÜ5...	3Eh	20h	Fg: Bg: 🟪	
uint strongLen	0	5Eh	4h	Fg: Bg:	
uint hashAlgo	32782	62h	4h	Fg: Bg: 🟨	
uint hashLen	512	66h	4h	Fg: Bg:	
uint hmacLen	32	6Ah	4h	Fg: Bg:	
byte hmac[32]	Ö½@¥=□·j„TVnl□¸��ÚÐ¯È□ò□&ä□ó...	6Eh	20h	Fg: Bg: 🟩	
uint cipherTextLen	80	8Eh	4h	Fg: Bg:	
byte cipherText[80]	/ÆZ†□f□º%ÕÂ£‰ë,3á8nÖA□Óéçã·]²è...	92h	50h	Fg: Bg: 🟦	
uint signLen	64	E2h	4h	Fg: Bg:	
byte sign[64]	□ □Ã"½@nëXTÇ¸�~□j"AYë³ŽJfr_C Ù...	E6h	40h	Fg: Bg: 🟩	

The master password for KeePass files encrypted & stored as cipherText (80 bytes)

DPAPI blob: Legend

Solution: Privileged Access Management

Administrative / power user access

A privileged user is someone who has administrative access to critical systems

Privileged users have sometimes more access than we think (see: SeBackupRead privilege)

Privileged users have possibility to read SYSTEM and SECURITY hives from the registry

Domain Admins should log on only to the Domain Controllers

Access Monitoring / Effective Access

We need to know about who and where has access to

Access should be role driven

#3: USB STICK UP

60% OF USERS WHO FIND RANDOM USB STICKS IN A PARKING LOT WILL PLUG THEM INTO THEIR COMPUTERS

LOGO

ADD THE COMPANY LOGO, AND THAT NUMBER INCREASES TO **90%**

35% OF USERS REPORT HAVING EXPERIENCED A VIRUS INFECTION THROUGH A USB DEVICE

Solution: Whitelisting

Code execution prevention

It is an absolute necessity taking into consideration the current security trends

PowerShell is a new hacking tool

Scripting languages are the biggest threat

Ransomware can be in a form of PowerShell script

Just Enough Administration: PowerShell should be blocked for users and limited for helpdesk to use the necessary commands

It is necessary to know what executes on your servers

Sysmon is perfect for this

AppLocker / DeviceGuard in the audit mode

Scenario

You receive the email about the new voice mail:

You received a voice mail : VOICE548-457-6638.wav (27 KB)
Caller-Id: 548-457-6638
Message-Id: S5VAAC
Email-Id: paula.j@gmail.com

Download and extract the attachment to listen the message.
We have uploaded fax report on dropbox, please use the following link to download your file:

https://www.dropbox.com/meta_dl/eyJzdWJfcGF0aCI6ICIiLCAidGVzdF9saW5rIjogZmFsc2UsICJzZXJ2ZXIiOiAiZGwuZHJvcGJveHVzZXJjb250ZW50LmNvbSIsICJpdGVtX2lkIjogbnVsbCwgImlzX2RpciI6IGZhbHNlLCAidGtleSI6ICJueGxzcWh0MDF5ZnloOHMifQ/AAPQJWOgwKVSIAJCmizztc3dqjAIfdlgyD87Cw0mgJOIxw?dl=1
Sent by Microsoft Exchange Server

What do you do?

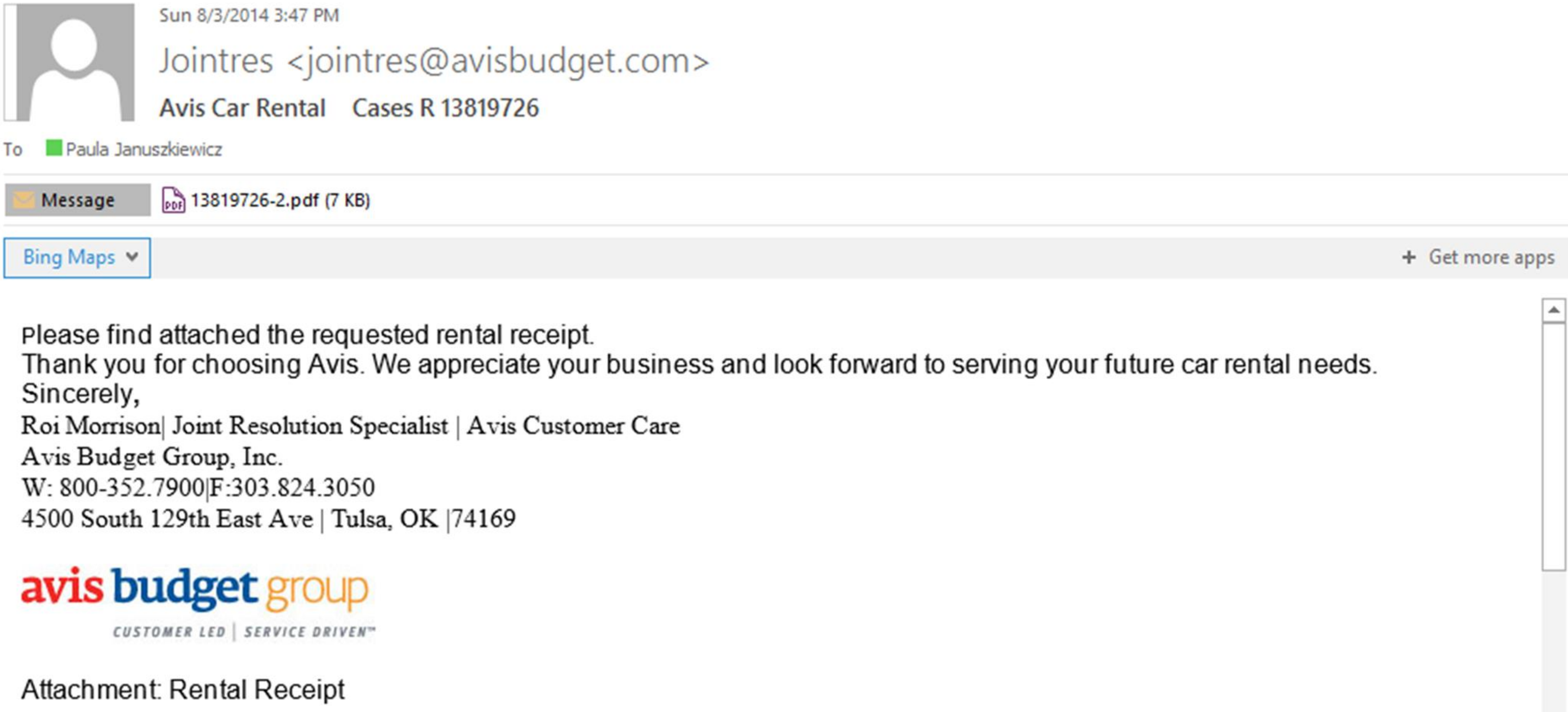
#4: PHISH BITING

69% OF IT SECURITY PROS SAY THEY COME ACROSS PHISHING MESSAGES THAT GET PAST SPAM FILTERS

27% OF IT ORGANIZATIONS HAVE TOP EXECUTIVES OR PRIVILEGED USERS WHO HAVE FALLEN FOR MALICIOUS EMAIL ATTACKS

USERS TRAINED IN AVOIDING PHISHING AND SCAM EMAILS FELL FOR THESE MALICIOUS EMAILS 42% LESS THAN THOSE WITHOUT TRAINING

Question: Is this a phishing email?



Sun 8/3/2014 3:47 PM

Jointres <jointres@avisbudget.com>

Avis Car Rental Cases R 13819726

To Paula Januszkiewicz

13819726-2.pdf (7 KB)

Please find attached the requested rental receipt.
Thank you for choosing Avis. We appreciate your business and look forward to serving your future car rental needs.
Sincerely,
Roi Morrison| Joint Resolution Specialist | Avis Customer Care
Avis Budget Group, Inc.
W: 800-352.7900|F:303.824.3050
4500 South 129th East Ave | Tulsa, OK |74169

Attachment: Rental Receipt

Attacks happen FAST and are HARD to stop

If an attacker sends an email to 100 people in your company…

…23 people will open it…

…11 people will open the attachment…

…and six will do it in the first hour.

Source: VerizoData Breach Investigations Report

#5: Reckless Abandon

70%

OF USERS DO NOT PASSWORD PROTECT THEIR SMARTPHONES

89%

OF PEOPLE WHO FIND LOST CELL PHONES RUMMAGE THROUGH THE DIGITAL CONTENTS TO LOOK AT SENSITIVE INFORMATION

Classic Data Protection API

- Based on the following components:

Password, data blob, entropy

- Is not prone to password resets!

Protects from outsiders when being in offline access

Effectively protects users data

- Stores the password history

You need to be able to get access to some of your passwords from the past

Conclusion: OS greatly helps us to protect secrets

Solution: Incident Response Plan

Action list

In case of emergency situation: allows to act reasonably and according to the plan

Increases chances that evidence is gathered properly

Allows to define responsibilities for recovery

Discussions provide management with understanding of security

Recovery plan

Centralization of the event logs

BYOD management strategy

'Connect and go' approach for better efficiency

#6: HOOKING UP WITH ANOTHER MAN'S WI-FI

BY 2015, THE NUMBER OF WIFI HOTSPOT DEPLOYMENTS WILL INCREASE BY 350%

ONLY 18 PERCENT OF USERS USE A VPN TOOL WHEN ACCESSING PUBLIC WI-FI

FBI

THE FBI RECENTLY RELEASED AN ALERT TO TRAVELERS WARNING AGAINST AN UPTICK IN MALWARE PASSED OFF AS SOFTWARE UPDATES ON HOTEL INTERNET CONNECTIONS

Lack of SMB Signing (or alternative)

Key learning points:

✓ Set SPNs for services to avoid NTLM:

SetSPN –L <your service account for AGPM/SQL/Exch/Custom>

SetSPN –A Servicename/FQDN of hostname/FQDN of domain domain\serviceaccount

✓ Reconsider using Kerberos authentication all over

https://technet.microsoft.com/en-us/library/jj865668.aspx

✓ Require SPN target name validation

Microsoft network server: Server SPN target name validation level

✓ Reconsider turning on SMB Signing

✓ Reconsider port filtering

✓ Reconsider code execution prevention but do not forget that this attack leverages administrative accounts

SMB2/3 client and SMB2/3 server signing settings

Setting	Group Policy Setting	Registry Key
Required *	Digitally sign communications (always) – Enabled	RequireSecuritySignature = 1
Not Required **	Digitally sign communications (always) – Disabled	RequireSecuritySignature = 0

* The default setting for signing on a Domain Controller (defined via Group Policy) is “Required”.

** The default setting for signing on SMB2 Servers and SMB Clients is “Not Required”.

Effective behavior for SMB2/3:

	Server – Required	Server – Not Required
Client – Required	Signed	Signed
Client – Not Required	Signed*	Not Signed**

* Default for Domain Controller SMB traffic.

** Default for all other SMB traffic.

Allowing unusual code execution

Key learning points:

Common file formats containing malware are:

- ✓ .exe (Executables, GUI, CUI, and all variants like SCR, CPL etc)
- ✓ .dll (Dynamic Link Libraries)
- ✓ .vbs (Script files like JS, JSE, VBS, VBE, PS1, PS2, CHM, BAT, COM, CMD etc)
- ✓ .docm, .xlsm etc. (Office Macro files)
- ✓ *.other (LNK, PDF,* PIF, *etc.)*

If SafeDllSearchMode is enabled, the search order is as follows:

1. The directory from which the application loaded
2. The system directory
3. The 16-bit system directory
4. The Windows directory
5. The current directory
6. The directories that are listed in the PATH environment variable

Old protocols or their default settings

Key learning points:

- ✓ **SNMPv3 addresses: user-based system for access control, a means to properly authenticate users, and a method for encrypting SNMP traffic between agent and host**
- ✓ **SQL issues – TDS provides by default lack of encryption**
- ✓ **ODBC Driver – check if it has a secure networking layer built into it**

NTLMv1 / NTLMv2

- ✓ Security Options in GPO allow to monitor where NTLM is used
- ✓ General direction is to get rid of NTLM

SSL / TLS

- ✓ **TLS v1.3 is still an Internet Draft**
- ✓ **SSL 2.0 and 3.0 have been deprecated by the IETF (in 2011 and 2015)**
- ✓ **Disable SSL 2.0 and 3.0, leaving only TLS protocols enabled**

Solution: Machine Learning for Threat Protection

- Antivirus solution is not enough
  - Signature and behavioral recognition is not enough too
  - In most cases it is possible to run an unknown code
  - … if not then it is possible to run PowerShell
  - Windows Defender ATP – have a look!

- Modern solutions
  - Are capable of machine learning but it takes time
  - Are quire easy to implement bur require a lot of understanding of what do they actually do

For example: What if we use a custom reflective PE Loader to create and run custom code?

#7: A LITTLE TOO SOCIAL

facebook
Error
HECK, YES!
No.

The super-cool video from your digital penpal failed to load due to a video codec error. Click here to download virus...err, new video codec.

67% OF YOUNG WORKERS THINK CORPORATE SOCIAL MEDIA POLICIES ARE OUTDATED

70% REGULARLY IGNORE IT POLICIES

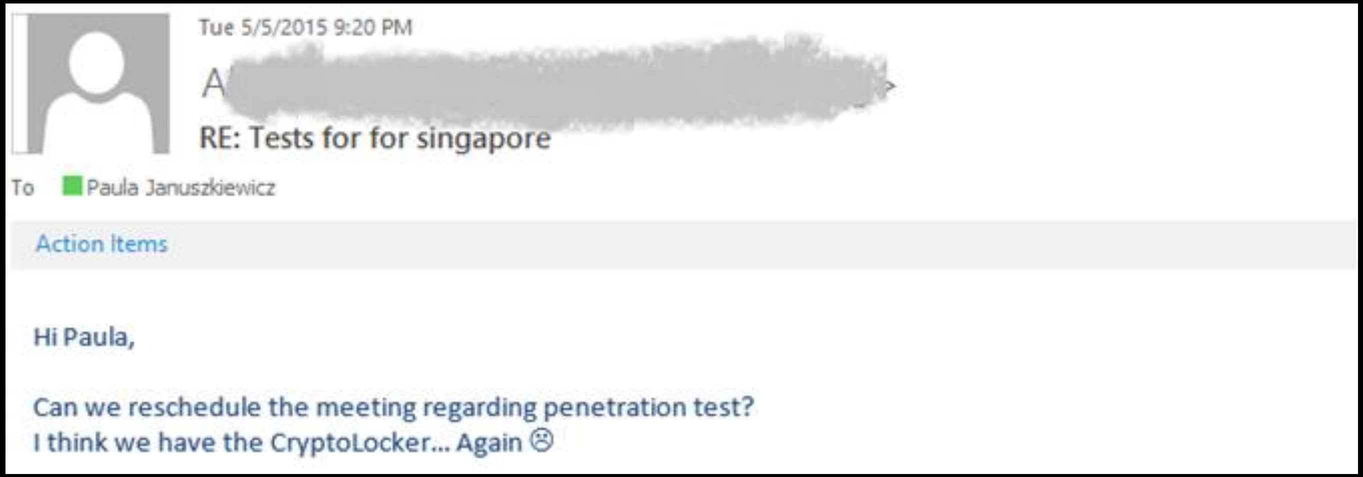
52% OF ENTERPRISES HAVE SEEN AN INCREASE OF MALWARE INFECTIONS DUE TO EMPLOYEES' USE OF SOCIAL MEDIA

Solution: Talk *Security* to Employees

Sad facts

Most of the companies we deal with did not have security policies in place that included security awareness education programs.

Management understands risk. IT also understands it. This can be nicely combined together when we use appropriate language.



Tue 5/5/2015 9:20 PM

[redacted]

RE: Tests for for singapore

To 🟩 Paula Januszkiewicz

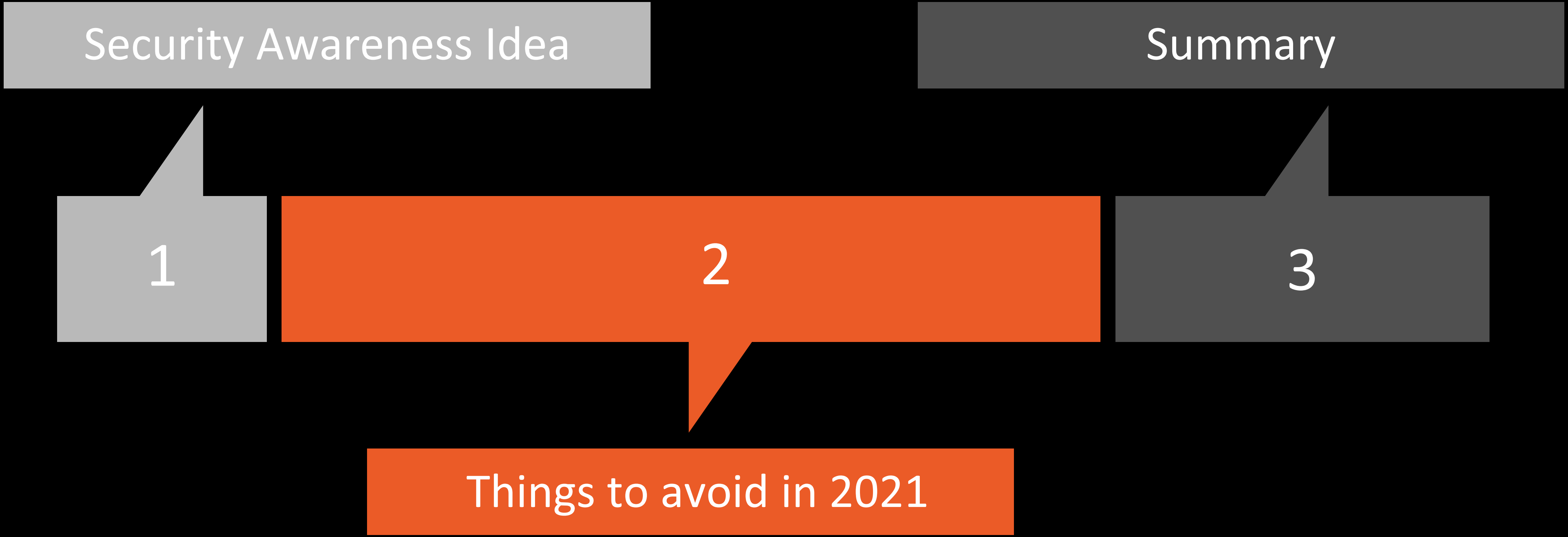
Action Items

Hi Paula,

Can we reschedule the meeting regarding penetration test?
I think we have the CryptoLocker... Again ☹

Photo: the New York Times Magazine

Agenda



1 Security Awareness Idea

2 Things to avoid in 2021

3 Summary

Why human factor is so important?

Reason 1: Security is both a Reality and Feeling

For Security Practicioners

Security is a reality based on the mathematical probability of risks

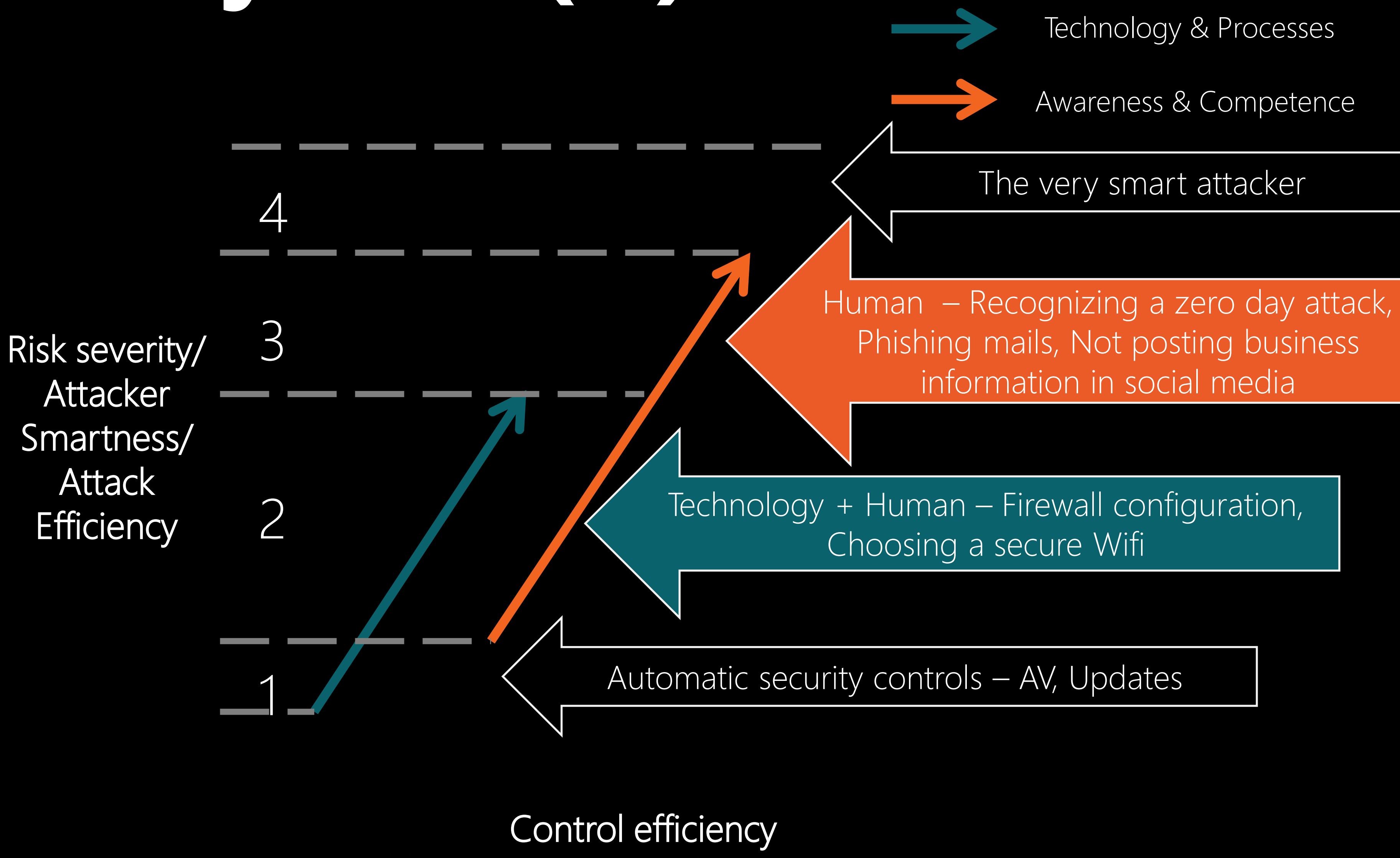
For End User

Security is a feeling

Success lies in influencing the “feeling” of security

Reason 2: Not every attack(er) is that smart

People exaggerate risks that are spectacular or uncommon



→ Technology & Processes

→ Awareness & Competence

Risk severity/ Attacker Smartness/ Attack Efficiency

4

3

2

1

The very smart attacker

Human – Recognizing a zero day attack, Phishing mails, Not posting business information in social media

Technology + Human – Firewall configuration, Choosing a secure Wifi

Automatic security controls – AV, Updates

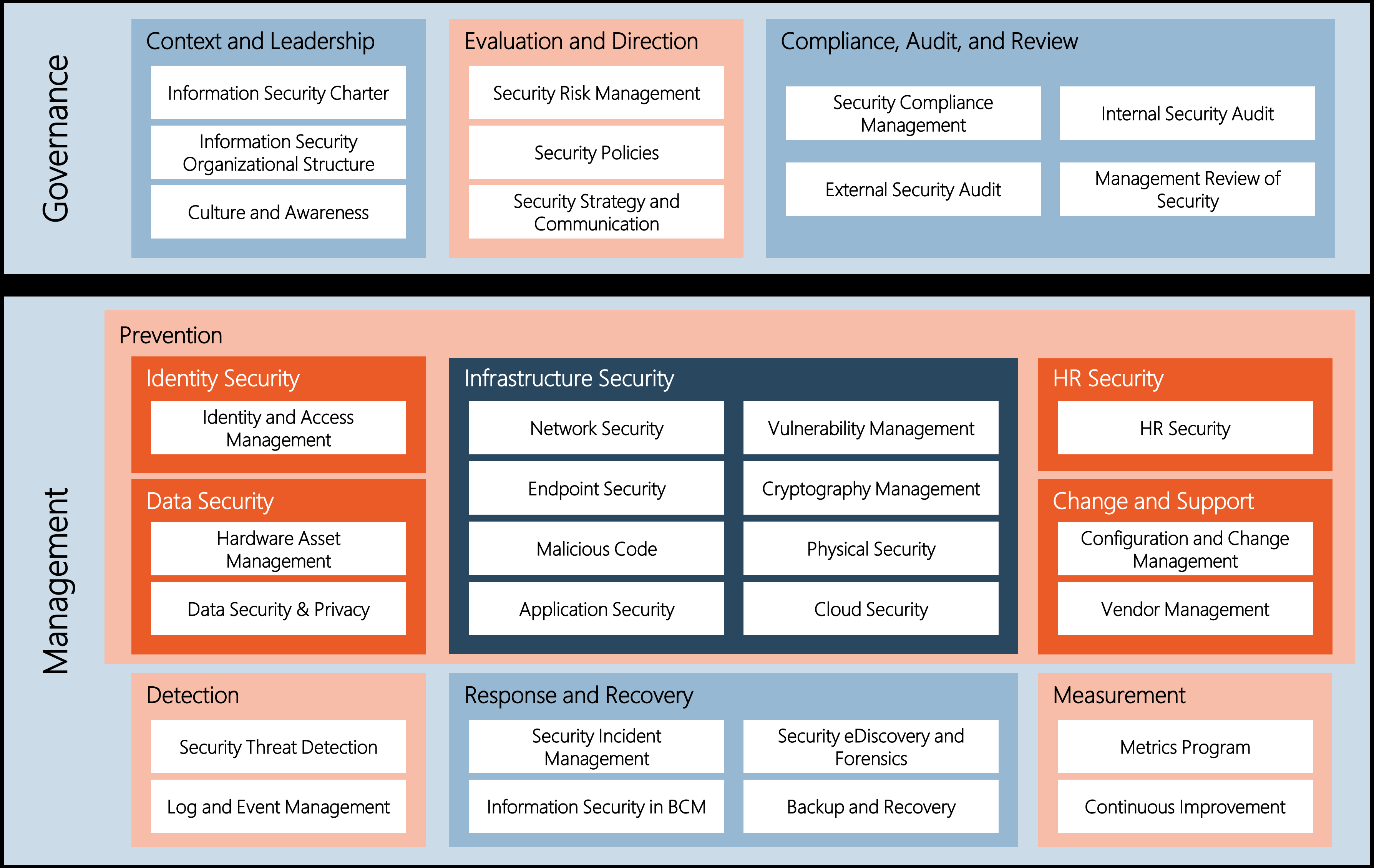
Control efficiency

Reason 3: Technology…yes, but humans… of course!

Aircrafts have become more advanced, but does it mean that pilot training requirements have reduced?

Medical technology has become more advanced, but will you choose a hospital for it’s machines or the doctors?

A best-of-breed security framework



Governance

Context and Leadership

- Information Security Charter
- Information Security Organizational Structure
- Culture and Awareness

Evaluation and Direction

- Security Risk Management
- Security Policies
- Security Strategy and Communication

Compliance, Audit, and Review

- Security Compliance Management
- Internal Security Audit
- External Security Audit
- Management Review of Security

Management

Prevention

Identity Security

- Identity and Access Management

Data Security

- Hardware Asset Management
- Data Security & Privacy

Infrastructure Security

- Network Security
- Vulnerability Management
- Endpoint Security
- Cryptography Management
- Malicious Code
- Physical Security
- Application Security
- Cloud Security

HR Security

- HR Security

Change and Support

- Configuration and Change Management
- Vendor Management

Detection

- Security Threat Detection
- Log and Event Management

Response and Recovery

- Security Incident Management
- Security eDiscovery and Forensics
- Information Security in BCM
- Backup and Recovery

Measurement

- Metrics Program
- Continuous Improvement

CQURE

The 11 key cyber security questions

1. Do we treat cyber security as a business or IT responsibility?
2. Do our security goals align with business priorities?
3. Have we identified and protected our most valuable processes and information?
4. Does our business culture support a secure cyber environment?
5. Do we have the basics right? (For example, access rights, software patching, vulnerability management and data leakage prevention.)
6. Do we focus on security compliance or security capability?
7. Are we certain our third-party partners are securing our most valuable information?
8. Do we regularly evaluate the effectiveness of our security?
9. Are we vigilant and do we monitor our systems and can we prevent breaches?
10. Do we have an organized plan for responding to a security breach?
11. Are we adequately resourced and insured?

Summary: Best Practices

Understanding is the key to security

Continuous vulnerability discovery

Context-Aware Analysis

Prioritization

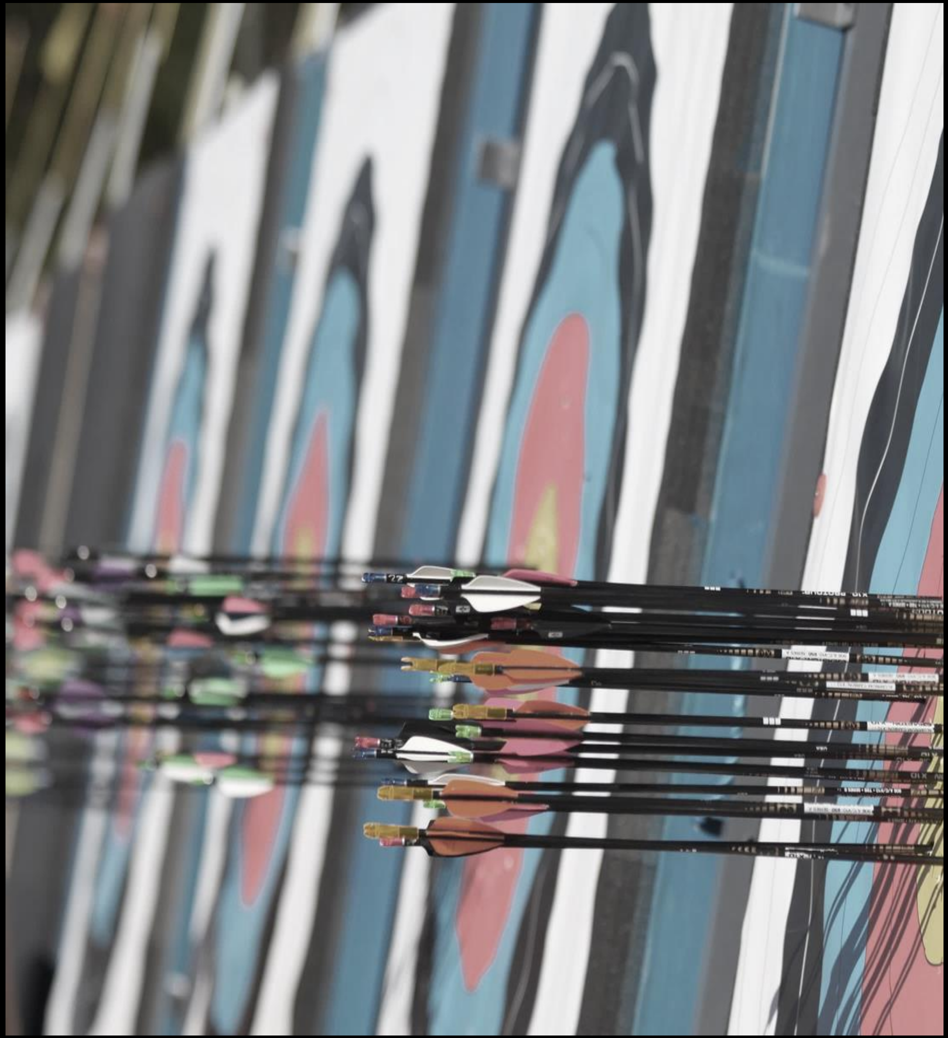
Remediation and Tracking

Configuration reviews

Put on the Hacker's Shoes

Prevention is the key to success

How can we know what to prevent if we do not know what is the threat?



Additional Resources

Websites

Ars Technica
The Register
The Hacker News
Dark Reading
Krebs on Security
Computer World
Threat Post
Beta News
Tech News World
Tech Crunch
ZDNetSecurity Affairs
Computer Weekly
Network World

SC Magazine
Wired
Schneier on Security

Q&A

Visit our BLOG and discover more about cybersecurity solutions & tools:

https://cqureacademy.com/blog

If you want level up your Windows Cybersecurity Skills

JOIN OUR ONLINE TRAININGS

CQURE

Advanced Windows Security Course 2021

Online certified course for intermediate and advanced professionals.

START: NOVEMBER 2020

CQURE

Hackers' Perspective on Your Infrastructure and How to Keep Them Out of Your Life

PAULA JANUSZKIEWICZ

CQURE: CEO, Penetration Tester; Security Expert

CQURE Academy: Trainer

Microsoft MVP on Cloud and Datacenter Management

Microsoft Regional Director

paula@cqure.us

@PaulaCqure @CQUREAcademy

www.cqureacademy.com

SECTOR
Security Education Conference

Hackers' Perspective on Your Infrastructure and How to Keep Them Out of Your Life

October 21st, 2020,

SecTor Conference Keynote Session

CQURE