

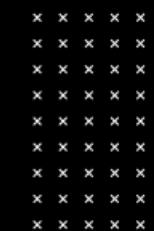
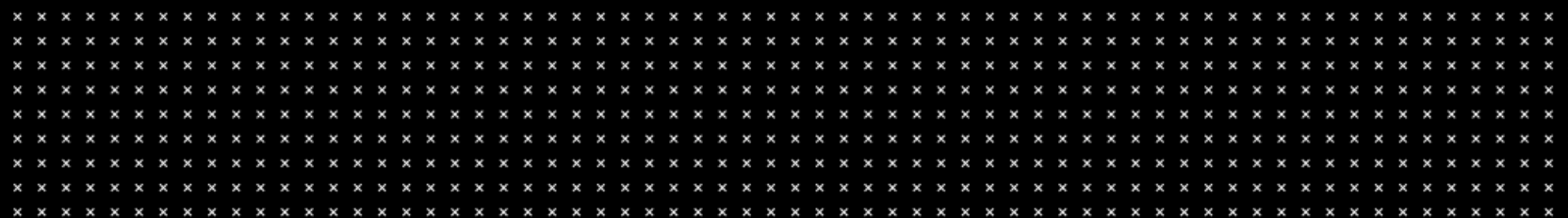
Hacker's Perspective on New Risks:

**Revising the Cybersecurity
Priorities for 2025**

IT-Defense | Leipzig | 12.02.2025



CQURE



Hacker's Perspective on New Risks:

Revising the Cybersecurity Priorities for 2025

Paula Januszkiewicz

CQURE: CEO, Cybersecurity Expert, Penetration Tester

CQURE Academy: Trainer

Microsoft Enterprise Security MVP

Microsoft Regional Director

paula@cquire.us

 @PaulaCquire @CQUREAcademy

www.cquireacademy.com Management



AUSTRALIAN CYBER CONFERENCE

2023

MELBOURNE | 17 - 19 OCTOBER



NIC X edition

May 31st - June 2nd
Oslo Spektrum

June 1st | 10:00 CEST

Adventures in the Underland:
Uncommon Hacker's Persistence Methods
and Countermeasures

June 1st | 16:00 CEST

Hackers' Perspective on Remote Working:
Know the Risks, Fight the Tricks

HACK IN PARIS | 2022

CYBERSECURITY EVENT



We are proud to announce that
Paula Januszkiewicz
was rated as
No 1 Speaker
at Microsoft Ignite!!!

May 4-8, 2015
Chicago, IL

FEATURED SPEAKERS



Professor Brian Cox
CBE FRS

Arguably the UK's best known experimental physicist, Professor Brian Cox's books and TV programmes have been read and watched around the world and credited with making science engaging and accessible...

[READ MORE](#)



Chris Hadfield
ASTRONAUT, ENGINEER AND
MILITARY FIGHTER/TEST PILOT

Referred to as "the most famous astronaut since Neil Armstrong," Colonel Chris Hadfield is a worldwide sensation whose video of David Bowie's 'Space Oddity' - seen by over 75 million people - was call...

[READ MORE](#)



Mikko Hypponen

Mikko Hypponen is cybersecurity research. He has written for the Times, V and lectured at Oxford, S...

[READ MORE](#)



Paula Januszkiewicz

RSAConference

Where the world talks security

I have been awarded
the **RSA Top-Rated Session!**



**Strong Story to Tell:
Top 10 Mistakes
by Administrators
About Remote Work**

Paula Januszkiewicz

CEO, Cybersecurity Expert, CQURE Inc.



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



LEAP

RIYADH FRONT EXPO CENTRE, SAUDI ARABIA

**Keynote: Cyber Attacks & Defense Transformation:
The Look to Past, Present & Future.**

by Paula Januszkiewicz, CEO of CQURE

February 3rd, 2022 | 16:25 AST (GMT +3)



Dr. Makaziwe...
Founder
House of Mandela...



Eugene Kaspersky
CEO & Co-Founder
Kaspersky



Luis Figo
Ballon d'Or winning...



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 via our partners worldwide),
- Online



Get to know us better!



Scan the QR code or visit
<https://cquireacademy.com/it-defense25>
to get access to this presentation and
find out more about CQURE!



The Impact of Cybercrime



There is always something to find...

Insightful Stats for 2025



\$4.88M

Is the global average cost of a data breach in 2024. It increased 10% over the previous year.



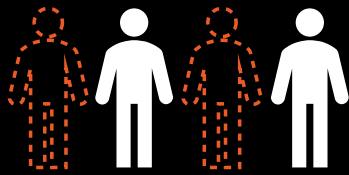
292 Days

That's how long on average it took to identify and contain breaches involving stolen or compromised credentials.



68%

of data breaches involved human error in 2024



>50%

of breached organizations are facing high levels of security staffing shortages. That's a 26.2% increase from the prior year

Source: IBM (2024), Verizon (2024)

Impactful Hacking Stats for 2025



43%

of all cyberattacks are aimed at small businesses.



95%

of data breaches are financially motivated.



83%

of breaches involve external actors.



64%

of organizations do not have a cyber security incident response plan.

Source: Verizon (2023); Accenture (2023), Kroll (2022)

Perspective on new threats

AI-Enhanced
Cyberattacks

Adversarial AI

Deepfakes
and Manipulated
Content

AI-Enabled Social
Engineer

Demo:
Is hacking easy?





Six Priorities to Have Your Infrastructure Prepared for a Battle

01 02 03 04

#1

Monitoring – Priority No 1



What if... hackers takes over AD?



After the AD incident (1)

1. Get a backup of DC prior to incident -> VHD, system state or backup;
2. Get a backup of DC in the current state -> VHD, system state or backup;
3. Reset all user account passwords twice
4. Reset all administrator passwords
5. Reset all service accounts passwords
6. Reset (twice – but bear in mind the issues with replication so there's specific guidance on this) the KRBTGT password
7. Reset all computer account passwords
8. Check the value of the computer account password change value
9. By default, it is 30 days, threat actors can change this to give themselves access using machine hashes for a longer duration.

After the AD incident (2)

1. Reset all LAPS Passwords
2. Reset permissions on AdminSDHolders object
3. Revoke and re-issue all certificates from ADCS
4. Check for malicious scheduled tasks
5. Check for malicious WMI event filters
6. Check for malicious autoruns or other registry-based persistence mechanisms
7. Check for utilman style backdoors
8. Check for malicious printers/printer drivers
9. Review Active Directory Delegated access permissions
10. Rotate ADFS token signing and token decryption certificates
11. Check Service Control Manager (SCM) security descriptors

After the AD incident (3)

1. Check for object changes around initial access/event timescales
2. Validate group memberships against known baselines (replication metadata, backup, AD reporting tools/reports etc.)
3. Harden Active Directory (look at pingcastle and MITRE)
4. Review logon scripts in GPOS and SYSVOL
5. Rotate Group Managed Service Accounts (GMSA)
6. Rotate LAPS credentials
7. Force AZUREADSSOACC\$ password rollover if AAD seamless SSO is used (Seamless SSO allows users on domain-joined devices to automatically sign in to Azure AD. It allows companies to configure SSO between AD and AAD without the need to deploy ADFS)
8. Invoke DC machine account password changes

After the AD incident (4)

1. Change Azure AD Connect-related passwords on both AD Connect servers, as these accounts could have been compromised and have high privileges in the environment.
2. Check all changes to GPO (find all modified files since incident time);
3. Check ASEPs on Domain Controllers with autoruns (important to have cross-check on all DCs)
4. Perform Revoke-AzureADUserAllRefreshToken for all users after password change;
5. Verify newly created accounts and privileged roles assignment in Azure AD;
6. Verify App Registration in Azure AD;
7. If Conditional Access is currently used – please verify all the policies and check the logs for possible changes;
8. For all services within Azure (and any other cloud providers) verify the logs to check all possible changes made by the suspected user;

After the AD incident (5)

1. Check ASEPs on all other servers and machines that might have been compromised;
2. Perform cross-check of all processes running on DCs;
3. Change KDS Root Key;
4. Perform a thorough analysis of all logs on Tier 0 servers;
5. **(Optional)** Run on all machines IOC rules (example: LOKI or THOR or similar);
6. **(Optional)** Perform network dump (through port mirroring) for all DC for 24h;
7. Check all forwarding/redirecting rules in Exchange Online Rules and mailbox level inbox rules;
8. Get the output of the command from DC: `auditpol /get /category:*`
9. PKI if exists:
 1. Check all issued certificates (after the incident)
 2. Check all Templates and permissions on templates
 3. Check all published templates
 4. Check for rouge NTAAuth entries

After the AD incident (5)

1. ADFS or similar if exists:
 1. Check all IDP
 2. Check all RPs
 3. Check all authorization policies
 4. Force ADFS urgent token signing cert rollover
2. PAM if exists:
 1. All logs
 2. All changes in secrets protected by PAM
 3. All internal accounts
 4. Check for additional access accounts
3. SCCM or similar:
 1. Check all task sequences
 2. Check all scheduled tasks
 3. Check all new/modified packages

#2

Check for Legacy Configuration or Misconfiguration



Decommission of old solutions or their default settings

- ⌵ Key learning points:
 - ⌵ Certificate Services are often misconfigured:
 - ⌵ Default certificate request website should be removed
 - ⌵ Review of templates and template permissions
 - ⌵ Regular audits of identity services (Active Directory etc.) are necessary
 - ⌵ SQL issues – TDS provides by default a lack of encryption
 - ⌵ ODBC Driver – check if it has a secure networking layer built into it



Demo:
Password Spray
Escalates



#3

Absence of Insight: Look for Persistence



Persistence Through Misconfiguration

⌵ Key learning points:

- ⌵ The best approach is to avoid using a solution until we know when it fails (time matters too)
- ⌵ Solution may have some 'backdoor weakness'
- ⌵ Some antivirus solutions can be stopped by SDDL modification for their services
- ⌵ Passwords are stored in various configuration files/places
- ⌵ Lack of monitoring adds up -> Golden Ticket etc.
- ⌵ Privilege Access Management not in place
- ⌵ Example: How to get access to the password management portal?



Persistence Used by Malware

Key learning points:

- Persistence through Windows mechanisms (services, task scheduler, etc.)
- Autoruns / FRST are very helpful
- Malware payload (e.g. PowerShell script) may be stored in the registry
- Malware as a debugger for other apps
- Extension hijacking (e.g. *.txt files are opened with malware by default)
- DLL hijacking attacks
- Callback on shutdown
- Adding entries to Group Policy
- WMI repository
- Domain persistence, like AdminSDHolder, etc.



Demo:
Persistence



#4

The Lack of Threat Hunting Skills



Demo:
dfsCoerce



Recycle Bin desktop.ini

Untitled3.ps1

cert.txt tools.msc

Google Chrome

desktop.ini PuTTY (64-bit)

Microsoft Edge



W10

Logon Domain:	RACCOONS
User Name:	jbond
IP Address:	(none) 10.1.1.100
Subnet Mask:	(none) 255.255.255.0
Default Gateway:	0.0.0.0
DNS Server:	(none) 10.1.1.1

CQURE



#5

Define Incident Response Readiness



77%



More than 77% of organizations do not test their incident response plan.

54 days



Organizations with both an IR team and IR plan testing identified breaches 54 days faster than those with neither.

26.1 days



The average time to investigate an incident is approximately 26.1 days, and the time to resolve incidents is an additional 17.1 days.

19%



19% of companies highlight managing the complexities of having too many tools as a significant challenge in their digital forensics and incident response activities.

32%



On average, SOC Team Members spend one-third of their typical workday investigating/validating incidents that are not a real threat.

Sources: IBM Security (2023), ThriveDX (2022), IDC (2023), Morning Consult (2023)

Demo:
Incident Ready?



Demo:

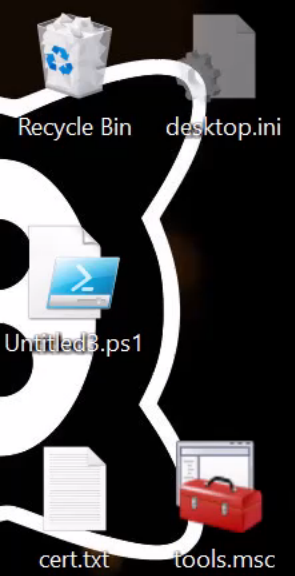
NGC



W10

Logon Domain:	RACCOONS
User Name:	jbond
IP Address:	(none) 10.1.1.100
Subnet Mask:	(none) 255.255.255.0
Default Gateway:	0.0.0.0
DNS Server:	(none) 10.1.1.1

CQURE



#6

Support Yourself with AI



How can you use a KQL Query to prove or refute a hypothesis?



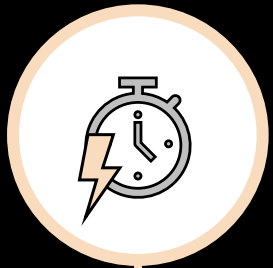
By writing custom KQL queries, cybersecurity professionals can create **targeted searches** to identify **specific threat indicators** and potentially stop attacks before they can cause significant damage.

How to create good KQL Queries?

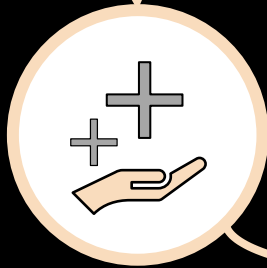
- Use time filters first
- Use 'has' instead of 'contains'
- Don't filter on a calculated column
- Select the table with the fewest rows to be the first one (left-most in query)

What does AI bring to threat hunting?

Speeds up hypothesis verification



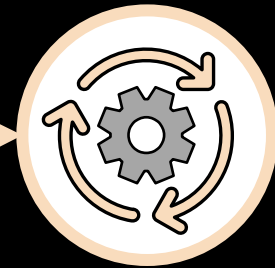
Offers support in information enrichment



Creates KQL queries and combines them with additional insights



Allows for automation and faster response



ChatGPT: The Power of AI

- Advanced conversational AI by OpenAI
- Understands complex queries
- Built on GPT-4 architecture for superior language comprehension

How ChatGPT and KQL can be used?

- ChatGPT helps refine queries for non-experts
- KQL extracts precise data from large datasets
- Their combined power enables accurate and efficient threat detection
- Automated threat detection using ChatGPT-guided KQL queries

Demo:
ChatGPT + KQL



Shared Chat • Default



please show me kql query for sentinel which will search for teamviewer on all devices



Certainly! In Azure Sentinel, you can use Kusto Query Language (KQL) to search for specific data across your data sources. If you want to search for TeamViewer-related information on all devices, you might need to have the relevant data source configured, such as Windows Security Events or any other relevant logs. Here's a general example of a KQL query that you could use as a starting point:

```
kql Copy code  
  
// Search for events related to TeamViewer on all devices  
SecurityEvent  
| where EventID == 4688 // This event ID corresponds to process creation events  
| where CommandLine contains "teamviewer" // Adjust the keyword if needed  
| project TimeGenerated, ComputerName, SubjectUserName, CommandLine  
| order by TimeGenerated desc
```

Please note that the above query assumes that you have security event logs collected in Azure Sentinel and that the EventID 4688 corresponds to process creation events on your systems. You might need to adapt the query to match the specifics of your environment and data sources.

Also, the keyword `"teamviewer"` in the `CommandLine` filter is used as a simple example. Depending on how TeamViewer appears in the logs, you might need to adjust this keyword or use additional filters to narrow down the search.

Remember to refer to the documentation for Azure Sentinel and your data sources to ensure you're using the correct event IDs, field names, and other specifics for your environment.

[Continue this conversation](#)



Summary

Summary



#1
Monitoring



#4
**Build the Threat
Hunting Skills**



#2
**Check for Legacy
Configuration or
Misconfiguration**



#5
**Define Incident
Response Readiness**



#3
**Absence of Insight:
Look for Persistence**



#6
Support Yourself with AI

Q&A



DOWNLOAD THE TOOLS

<https://resources.cquireacademy.com/tools/>

Username: student

Password: CQUREAcademy#123!

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

<https://cquireacademy.com/blog>



Get to know us better!



Scan the QR code or visit
<https://cquireacademy.com/it-defense25>
to get access to this presentation and
find out more about CQURE!

Hacker's Perspective on New Risks:

Revising the Cybersecurity Priorities for 2025

Paula Januszkiewicz

CQURE: CEO, Cybersecurity Expert, Penetration Tester

CQURE Academy: Trainer

Microsoft Enterprise Security MVP

Microsoft Regional Director

paula@cquire.us

 @PaulaCquire @CQUREAcademy

www.cquireacademy.com Management



Hacker's Perspective on New Risks:

**Revising the Cybersecurity
Priorities for 2025**

IT-Defense | Leipzig | 12.02.2025



CQURE

