Conducting Assessments in the Hybrid World of Remote and Onsite

PCI Security Standards Council

PCI Security Standards Council

Presented by Howard Glavin EVP K3DES, LLC

The Hybrid Assessment Environment is a Mix of Onsite and Remote Activities blended into on Reporting Artifact

The Process, Pitfalls, and Saving Graces

PCI Security Standards Council

K3DES, LLC

K3DES, LLC has worked Assessments since 2002 with the start of CISP by VISA and since 2004 has been conducting PCI DSS, PCI-PIN, P2PE, SSF, and 3DS Assessments.

K3DES is a a member of GEAR

Agenda and Takeaways

Agenda

- What is a Remote Assessment
- What is a Onsite Assessment
- How to Conduct a Hybrid or Fully Remote Assessment

Takeaways

- Full understanding of the Pitfalls encountered in a Hybrid Assessment

PCI DSS Assessments

Post Covid businesses have reallocated resources and office space. Assessments, are mostly a blend of onsite and remote or fully remote assessment activities

- PCI SSC Requires Onsite Assessments – Maybe!
  - What is an onsite assessment?
    - You in room with the PCI lead for the company and all others are on the phone or in a remote meeting
    - Many companies have disbanded formal office and work fully remote (Service Providers in general but also ecommerce merchants)
  - What is a remote Assessment?
    - Are you and the PCI lead in a office and all others on the phone or in a teams meeting room an onsite or a remote assessment
  - As you can see, Assessments today are for the most part, a Hybrid of both remote and limited onsite activities

PCI Security Standards Council

Scope Development and Validation is assumed for this Presentation

Remember, Scope is both defined and validated by the Assessed and Assessor.

Scope covers ALL devices used in and to manage the CDE. This covers workstation regardless of Jumpservers or proxy devices when the workstations are used to manage the CDE.

How to Address a Hybrid Assessment

Step 1

The Company's Requirements for Work From Home

You have now found the Haystack in the form of the directives the company you are assessing has for the Work Form Home - Anywhere (WFH) abilities

- Does it permit work from any location?
- Does it permit split tunnels?
- Does it permit others to be in the same are as the work?
- Does it permit BYOD equipment?
- What are the rules of engagement and how is the assessed company enforcing them?

PCI Security Standards Council

PCI SSC Directives for WFH

Step 2

What you can do and what should you do for WFH evidence for the reporting

PCI SSC has established that the WFH environment does not require onsite assessing

How to find the needle in the haystack for WFH interviews

- The evidence you collect is based on the Company's directives for the WFH staff
- Does the interviewee have a camera and if so does the location (laws or regulations) or the company permit the use of these for the interview process?
    - If permitted is the meeting being recorded or how are you going to acquire the evidence you need for observations etc. for reporting purposes

PCI Security Standards Council

Preparing for the Assessment

Step 3

Solving the Puzzle

Preparation for the Interviews in a Hybrid Environment

Developing your questions to gain the evidence you require

- Stay away from Yes No Questions
    - You will get a response but not necessarily the answer to the question
- Develop questions like show me or ‘explain’
- Review each requirement being covered and have your questions drafted so you can cover all topics set for that session

PCI Security Standards Council

Scheduling the Assessment and Interviews

Step 4

Scheduling

Scheduling Interviews and Evidence

- Interview schedules are generally set by the PCI Lead
- Invites go out but attendance is generally not the full invitee list
    - Some invitees do not respond
- Do you have the correct staff to answer the questions?
- Everyone has a hard stop short of the meeting times
- All are multi-tasking during the interviews be it on site or remote attendance
- You only get a portion of what you need

PCI Security Standards Council

Conducting the Assessment and Interviews

Step 5

Conducting the Interviews and Assessment

Do you understand the Questions you Asked?

To gain the information you need for the evidence to prove compliance the form and format of the question is critical.

- Do not speak at 10,000 words a minute in asking questions
- Let the question be understood
- Allow the staff asked to also ask questions as to the intent and meaning of your question
- Be cautious with evidence developed in advance – Better to see it live than in a report
- Be prepared for the “company expert” who has read the requirement in a vacuum at the x.x.x.x level and and does not fully understand the web of cross over for that specific requirement
- The best interviewers are those that listen not talk

PCI Security Standards Council

Sorting the Facts From the Fiction

Step 6

Understanding the data received during the interview and noting the ‘Buts’

While the interviews are underway you need to analyze the data received

Interview techniques require you to wear two hats

1. Interviewee
2. Translator of the responses received

When you can’t see it, how do you know you are getting facts vs I think we are doing x (fiction)

- Example: Does everyone in the office wear their badge all the time
    - The building walk through will generally show a wallet swipe and this is not wearing the badge in plan view

PCI Security Standards Council

Sorting the Facts From the Fiction

Step 7

Understanding the data received during the interview and do not accept hearsay evidence

While the interviews are underway you need to analyze the date received

- Look for the evidence that is pre-packaged and ask to see the source – Show Me Please
    - Example:
        - Firewall rules review: Go to the live rules and review do not rely on the “output file” as the only source of the evidence
        - Vulnerability Scans: Do not accept summary reports look at the raw scan data and have the person responsible for the scanning explain the output

PCI Security Standards Council

Solving the Puzzle

Step 8

Controlling the data received to ensure you get the evidence you require

Who is answering the Questions and How

General Observations from Hybrid Assessment Questions

- The PCI project lead wants to answer all questions
- The Head of departments like development or network will answer in deference to his team and this gives a one-sided view
- Do not get roped into a rabbit hole with discussions that are ancillary to the question being asked
- Be cautious when told the tool X cannot meet the requirement and thus it is “Risk Accepted”
    - Generally Risk Acceptance does not meet PCI requirements

PCI Security Standards Council

Your Assumptions of the Data Received

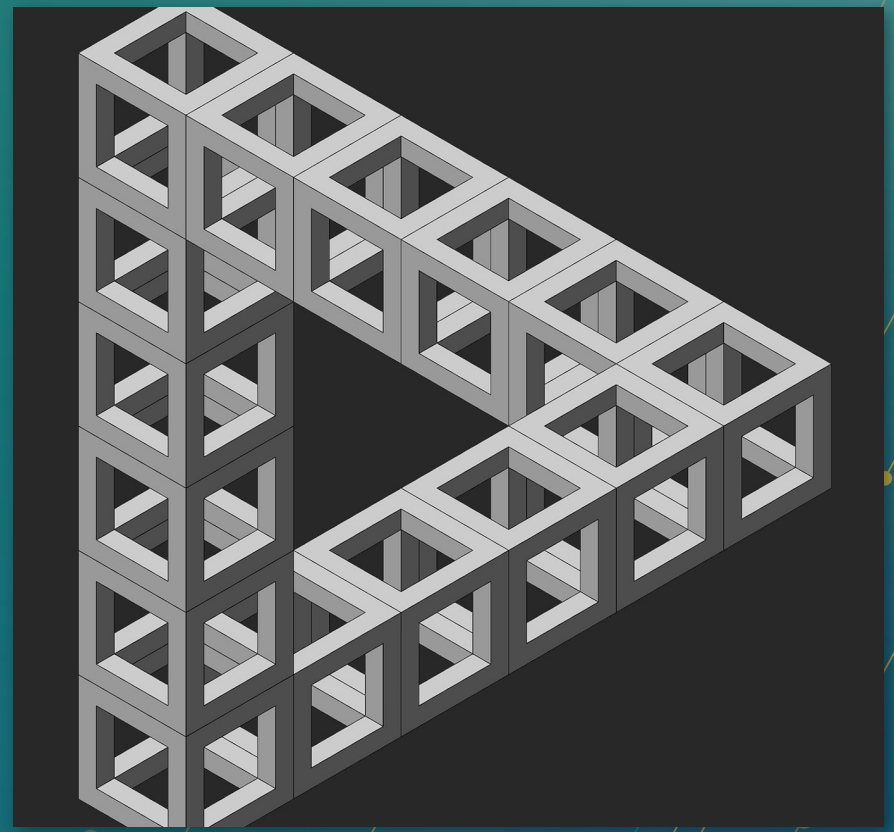
Step 9

How do you sort out what is evidence and what is missing in the evidence

Be Careful Do not fall into the Rabbit Hole

Drawing conclusions without the facts is easy

- Example
  - Entry to the MDF room or Data Center is by Card Key
    - You conclude this card key data can be used for logging in and out.
      - Is this a valid conclusion
        - No as you do not know if it meets all of the data required for in and out.
        - How are visitors logged in and out



PCI Security Standards Council

Trust But Verify

Step 10

Verify everything to the degree you are willing to use it as evidence in the court room

Do not approach the assessment using Blinders

Tunnel Vision or viewing through blinders causes you to miss the evidence behind you or offered in a manner you may neglect it

- Like the graphic what is happening behind you on site?
- How to you get this degree of acceptance when working remotely?
- Do you trust everything given to you?
  - No
- Verify everything given to you
  - Ask clarification questions. Do not challenge responses. This is not an adversarial process. We are the companies advocate

PCI Security Standards Council

Europe Community Meeting 2023

PCI Security Standards Council