Minimální požadavek na testování systému

SSH relace

1.1. Přístup do uživatelského rozhraní prostřednictvím SSH klienta – Zobrazení přístupných aktiv dle autorizací.
1.2. Možnost zobrazení přizpůsobitelné zprávy pro uživatele řešení – Informace o monitoringu aktivit atd.
1.3. Využití MFA v rámci SSH relace (soft token / push notifikace).
1.4. Navázání SSH relace prostřednictvím webového prohlížeče.
1.5. Navázání SSH relace prostřednictvím běžně využívaných klientů, např.:
    1.5.1. OpenSSH,
    1.5.2. PuTTY,
    1.5.3. Cygwin (+ Xming pro X11 forwardování),
    1.5.4. FileZilla,
    1.5.5. WinSCP.

RDP relace

1.6. Přístup do uživatelského rozhraní prostřednictvím běžně využívaných klientů, např.:
    1.6.1. MSTSC,
    1.6.2. rdesktop,
    1.6.3. FreeRDP,
    1.6.4. Remmina.
1.7. Navázání relace prostřednictvím staženého .rdp souboru.
1.8. Navázání RDP relace prostřednictvím webového prohlížeče.
1.9. Ověření funkčnosti znaků typických pro češtinu.
1.10. Využití MFA v rámci RDP relace (soft token / push notifikace).
1.11. Zobrazení přístupných aktiv dle autorizací.

Audit a monitoring

1.12. Zobrazení všech uskutečněných relací včetně doplňujících informací – Uživatel, cílové aktivum, čas a trvání, metoda ukončení relace.
1.13. Ověření vytvoření zápisu metadat / textových záznamů o:
    1.13.1. aktivních oknech,
    1.13.2. vstupech z klávesnice,
        1.13.2.1. cenzura / anonymizace vstupů při zadávání hesel či OTP,
    1.13.3. aktivitách clipboardu,
        1.13.3.1. vkládání textu do relace,
        1.13.3.2. kopírování textu z relace,
        1.13.3.3. vkládání souborů do cílového zařízení, včetně jejich SHA256 otisku,
        1.13.3.4. kopírování souborů z cílového zařízení, včetně jejich SHA256 otisku,
    1.13.4. zaznamenání uživatelských akcí – Zavření / minimalizace okna,
    1.13.5. identifikace běžících procesů, včetně cesty k jejich zdrojům a parametrům, se kterými byly spuštěny.
1.14. Vyhledávání aktivit napříč všemi relacemi.
1.15. Ukončení relace dozorujícím pracovníkem.

1.16. Automatické ukončení na základě provedení nepovolených aktivit.
1.17. Notifikace v případě provedení nepovolených aktivit.
1.18. Real-time monitoring aktivní relace.

Řízení a schvalování relací

1.19. Žádost o schválení přístupu v rámci RDP relace.
1.20. Žádost o schválení přístupu v rámci SSH relace.
1.21. Žádost o schválení přístupu skrze webové prostředí PAM.
1.22. Provedení schválení přístupu oprávněným pracovníkem.
1.23. Umožnění přístupu v rámci definovaných časových rámců.
1.24. Zamezení „bočního pohybu“ – blokace odchozích TCP spojení ze spravovaných aktiv.
1.25. Zamezení spuštění procesu v prostředí Windows.
1.26. Zamezení spuštění procesu v prostředí Linux.

SCP/SFTP

1.27. Přenos souboru s použitím SCP/STFP.
1.28. Demonstrace možnosti napojení na ICAP server.
1.29. Ukázka možných pravidel pro notifikace / blokace na základě vyhodnocení:
    1.29.1. Antivirem,
    1.29.2. DLP.

Správa hesel

1.30. Uživatelské zobrazení hesla z šifrovaného úložiště.
1.31. Změna hesla Linux.
1.32. Změna hesla AD.
1.33. Změna hesla lokálního účtu na platformě Windows.