

Nabídka testování zabezpečení webové aplikace včetně prověření infrastruktury pro Českomoravskou záruční a rozvojovou banku, a.s

insighti

Platnost nabídky
Předkládá

27.4.2020

Obsah

OBSAH	2
ÚVOD	3
O SPOLEČNOSTI	3
REFERENCE	4
TÝM	5
TESTOVÁNÍ WEBOVÝCH APLIKACÍ	5
A. PENETRAČNÍ TESTY DLE STANDARDU TGV4	5
<i>Shromažďování informací</i>	5
<i>Identifikace potenciálních zranitelností</i>	6
<i>Testování reálných možností zneužití zranitelností</i>	6
B. PENETRAČNÍ TESTY DLE STANDARDU ASVSV4	6
<i>Úroveň testování</i>	6
Level 1 - oportunistický	6
Level 2 - standardní	6
Level 3 – pokročilý	7
<i>Rozsah testů</i>	7
C. VYMEZENÍ ROZSAHU PLNĚNÍ.....	7
TESTOVÁNÍ INFRASTRUKTURY	7
A. <i>Test zabezpečení externí a interní infrastruktury</i>	7
ENUMERACE DOSTUPNÝCH SLUŽEB	7
KONSTRUKCE VEKTORŮ ÚTOKU	8
EXEKUCE ÚTOKU	8
B. VYMEZENÍ ROZSAHU PLNĚNÍ.....	8
ZPRÁVA O PENETRAČNÍM TESTU	8
A. <i>Struktura dokumentu</i>	8
B. <i>Ohodnocení zranitelností</i>	9
C. PEER REVIEW	9
MÍSTO A LHŮTY PLNĚNÍ	10
INFORMACE O ROZSAHU TESTŮ	10
SOUČINNOST OBJEDNATELE	10
REFERENCE NA PODOBNÉ PROJEKTY VE FINANČNÍ ČI VEŘEJNÉ SFÉŘE	10
CENOVÁ NABÍDKA	11
ZÁVĚR	11
PŘÍLOHY	11

Úvod

Na základě emailové poptávky od [REDACTED] Vám předkládáme nabídku, která shrnuje kompetence insighti v oblasti testování webových aplikací a možné přístupy k provedení testů zabezpečení nové webové aplikace pro podávání klientských žádostí podrobněji popsané v poptávce a prověření bezpečnostního návrhu použité infrastruktury.

Nabídka obsahuje specifikaci jednotlivých testů a technický popis realizace. Nabídka obsahuje cenovou kalkulaci.

O společnosti

Společnost insighti vstoupila na trh informační bezpečnosti s cílem přinést nový náhled na bezpečnost korporátních informací. Základním pracovním nástrojem expertů insighti je porozumění nástrahám, kterým musí bezpečná architektura informačního systému odolat. insighti přináší hmatatelné a lehce uchopitelné odpovědi na otázku, jak vytvořit či provozovat bezpečné informační systémy.

Svým klientům a partnerům pomáháme zvládnout výzvy v oblasti informační bezpečnosti vhodným začleněním svých expertních konzultantů do projektových či provozních týmů, kde můžou plnit roli poradenskou a kontrolní, roli bezpečnostních architektů či přímo ověřovat účinnost implementovaných bezpečnostních mechanismů simulací skutečných útoků.

Naší doménou je bezpečnostní architektura komplexních podnikových informačních sítí zahrnující jak vnitropodnikové aplikace, tak i aplikace sdílené s veřejností či obchodními partnery. Realizujeme návrhy architektury síťové infrastruktury, návrhy zabezpečení jednotlivých aplikací, celých informačních systémů či jednotlivých komunikačních kanálů.


Informační bezpečnost pro nás není jen prázdnou frází či snůškou zkratk jako jsou ISO, ISMS a ITIL. insighti bere bezpečnost vážně.

Reference

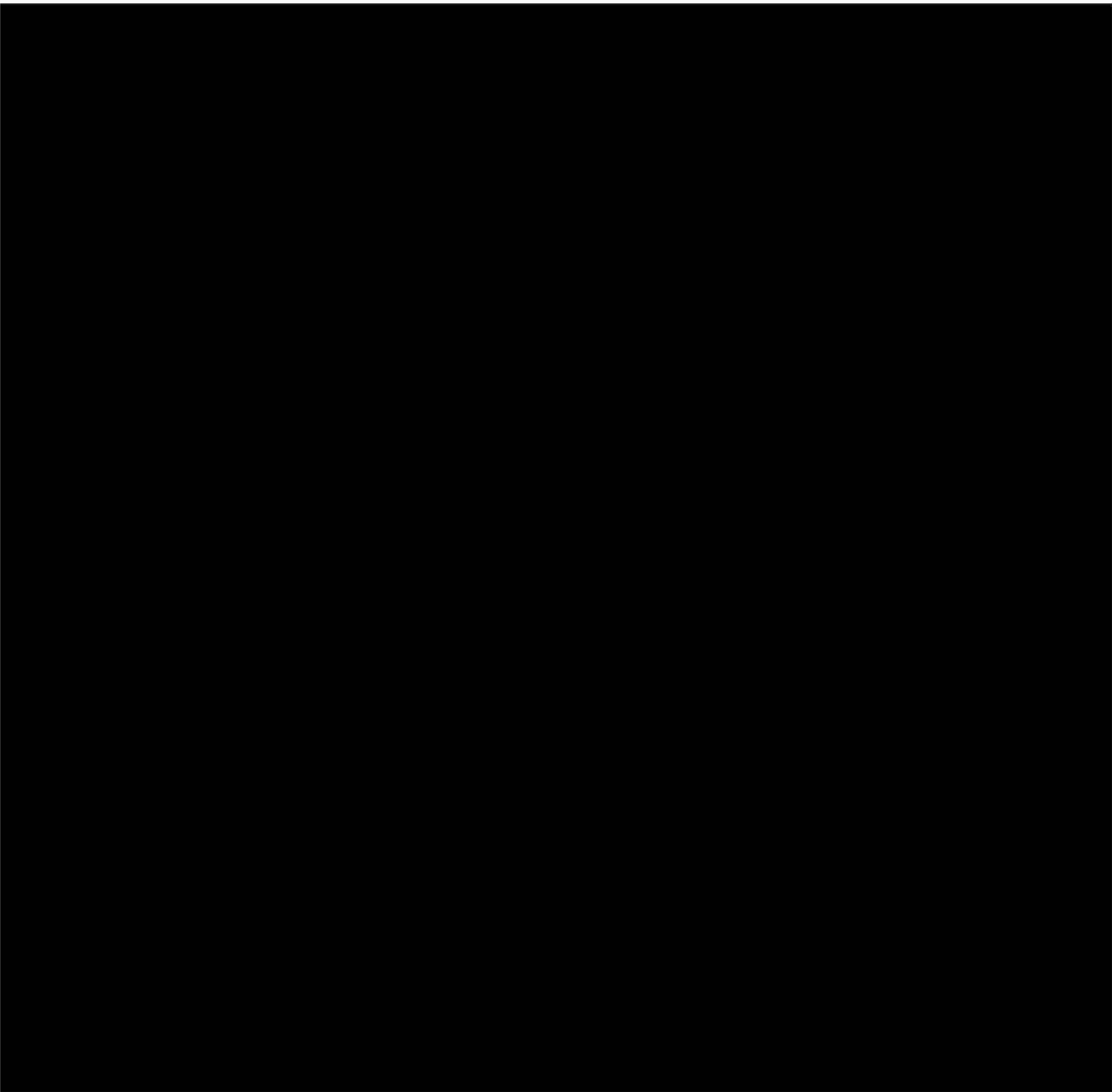


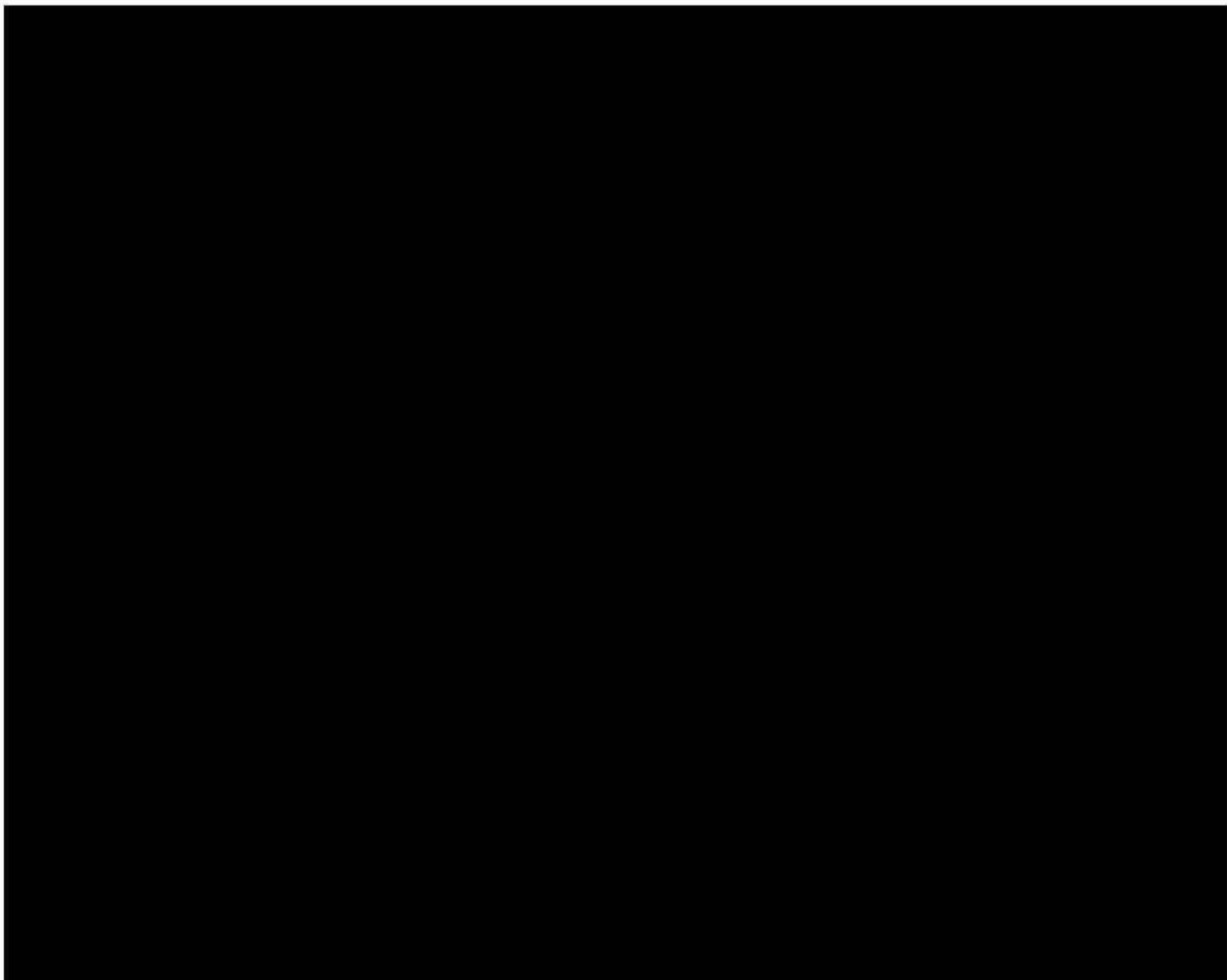
Tým

Členové našeho týmu se mohou pyšnit certifikáty OSCP (<https://www.offensive-security.com/information-security-certifications/oscp-offensive-security-certified-professional/>). Držitelé tohoto certifikátu musí projít náročným 24. hodinovým praktickým testem.

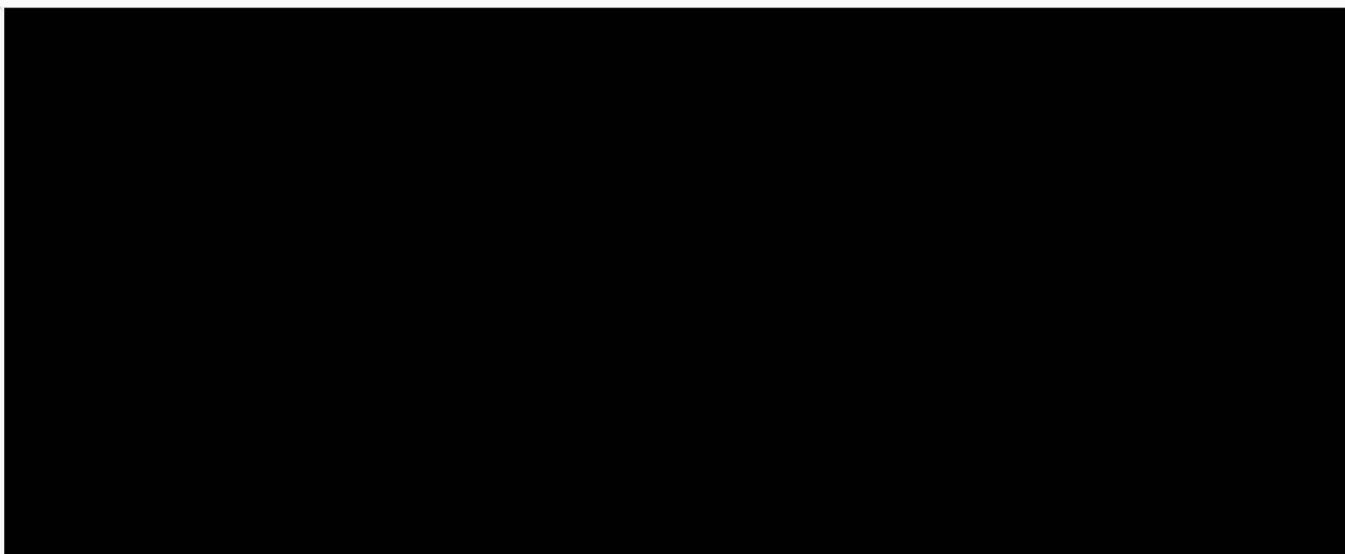


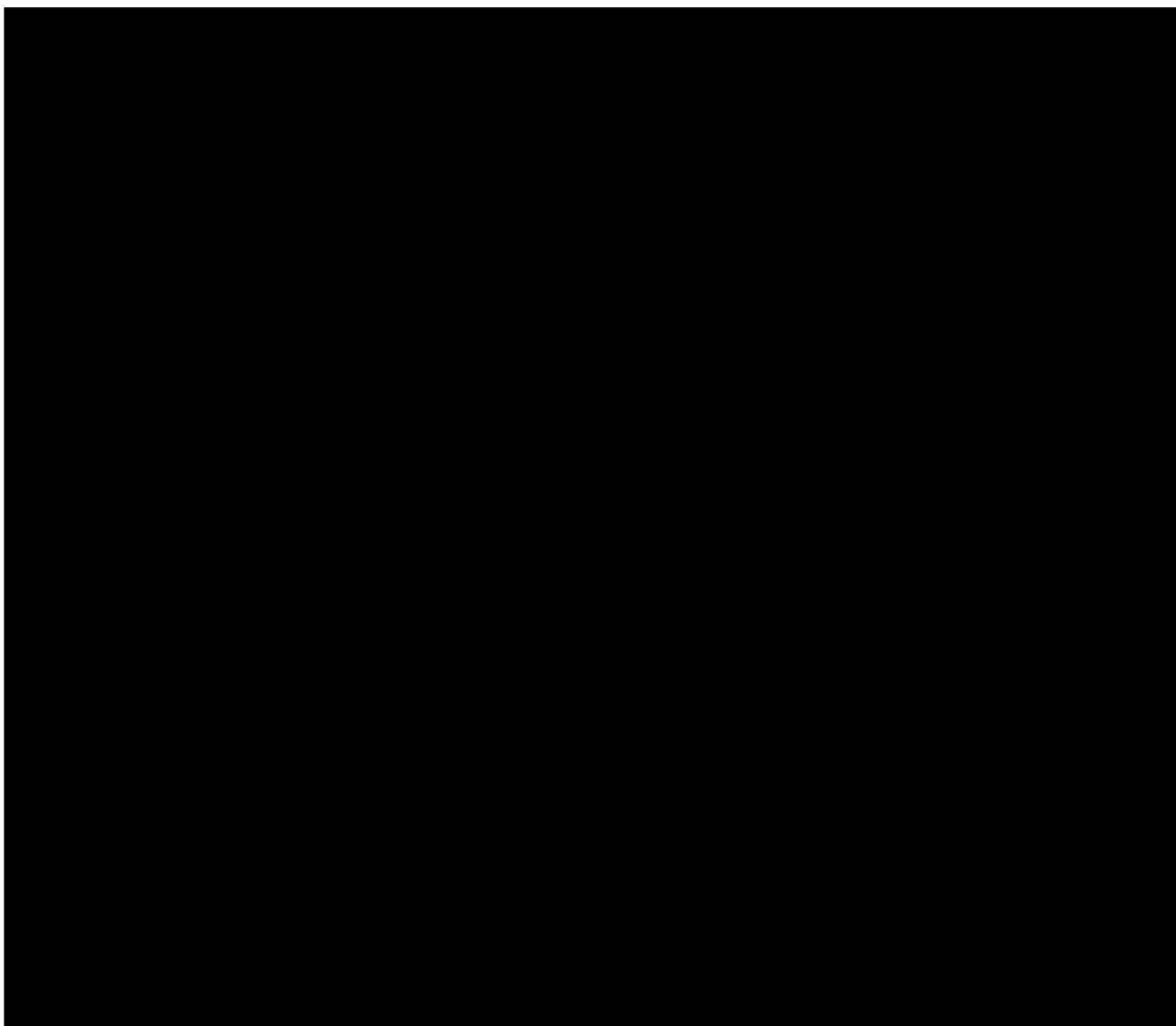
Testování webových aplikací



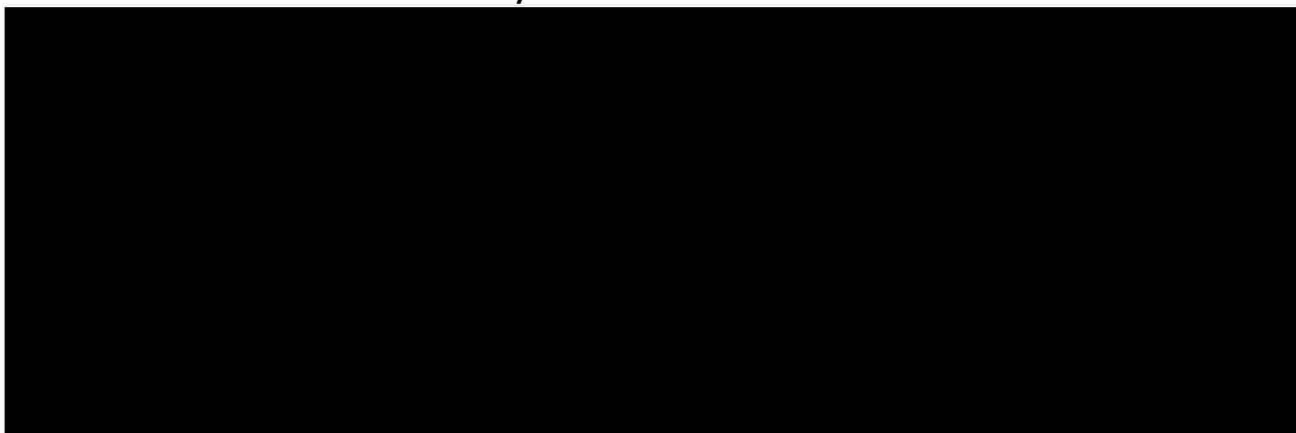


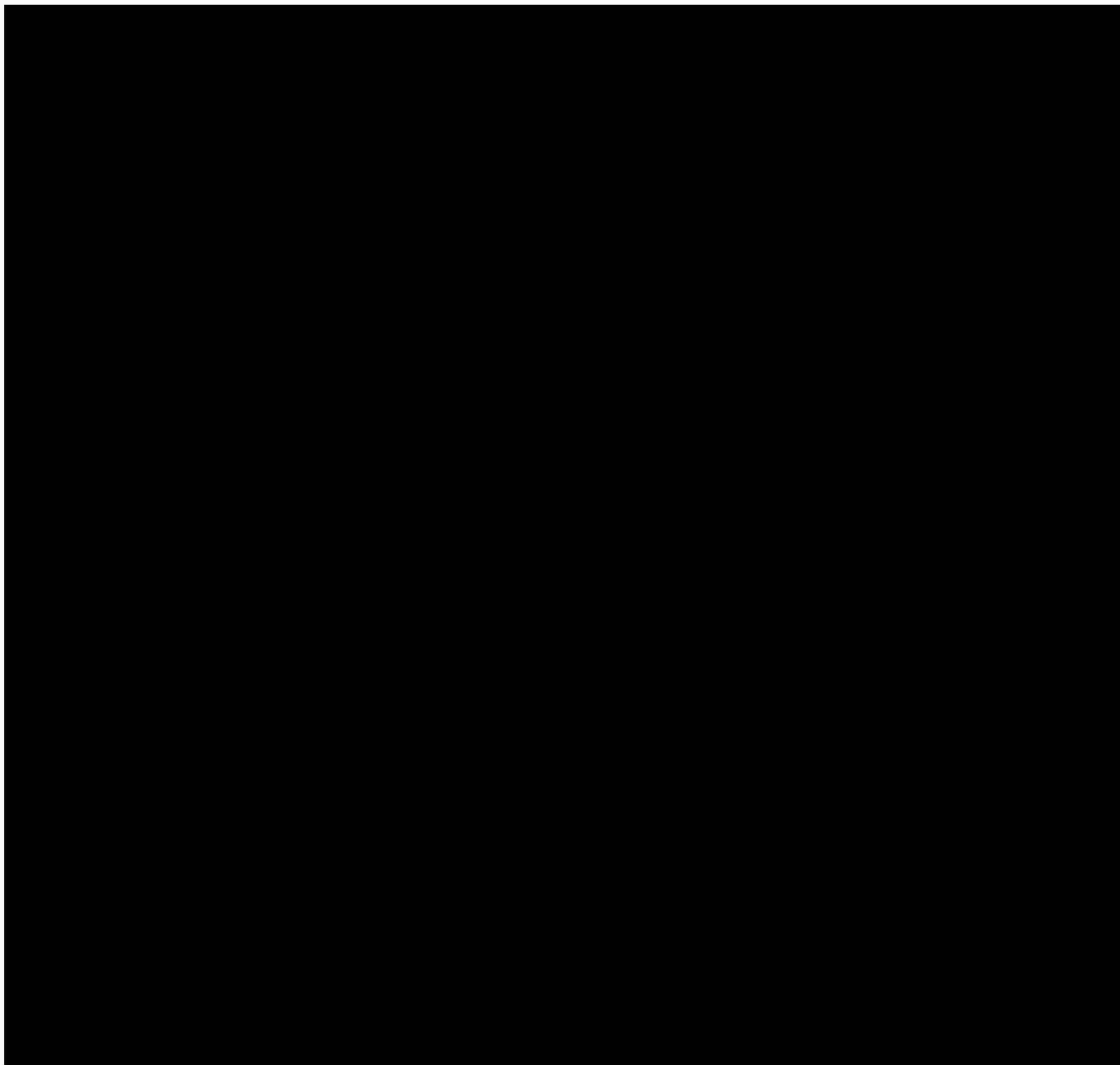
B. Penetrační testy dle standardu ASVSv4



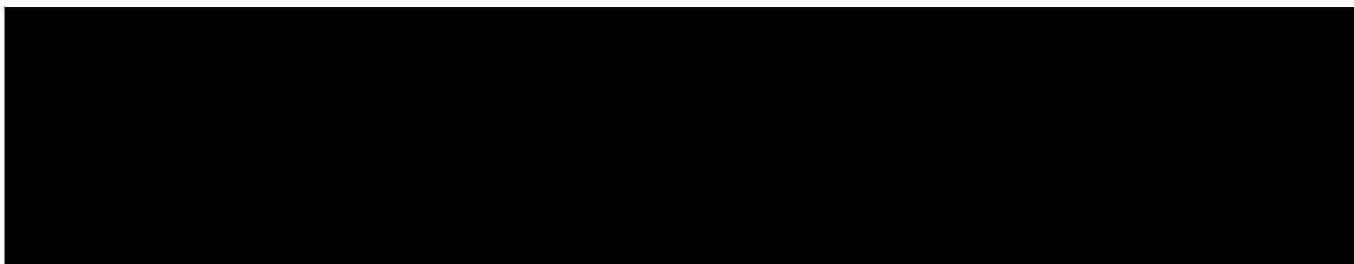


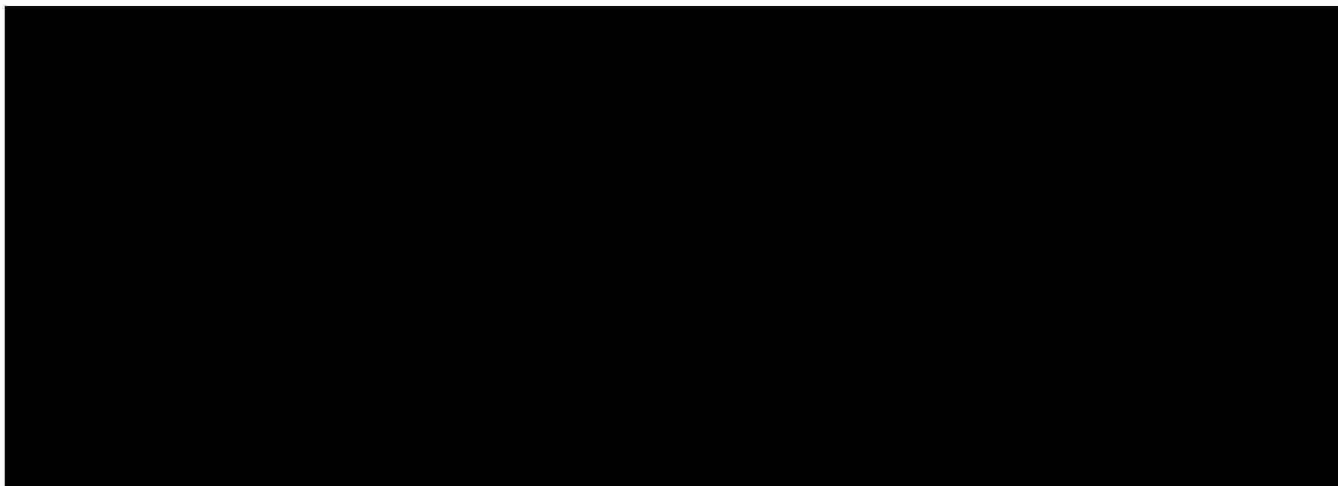
Testování infrastruktury



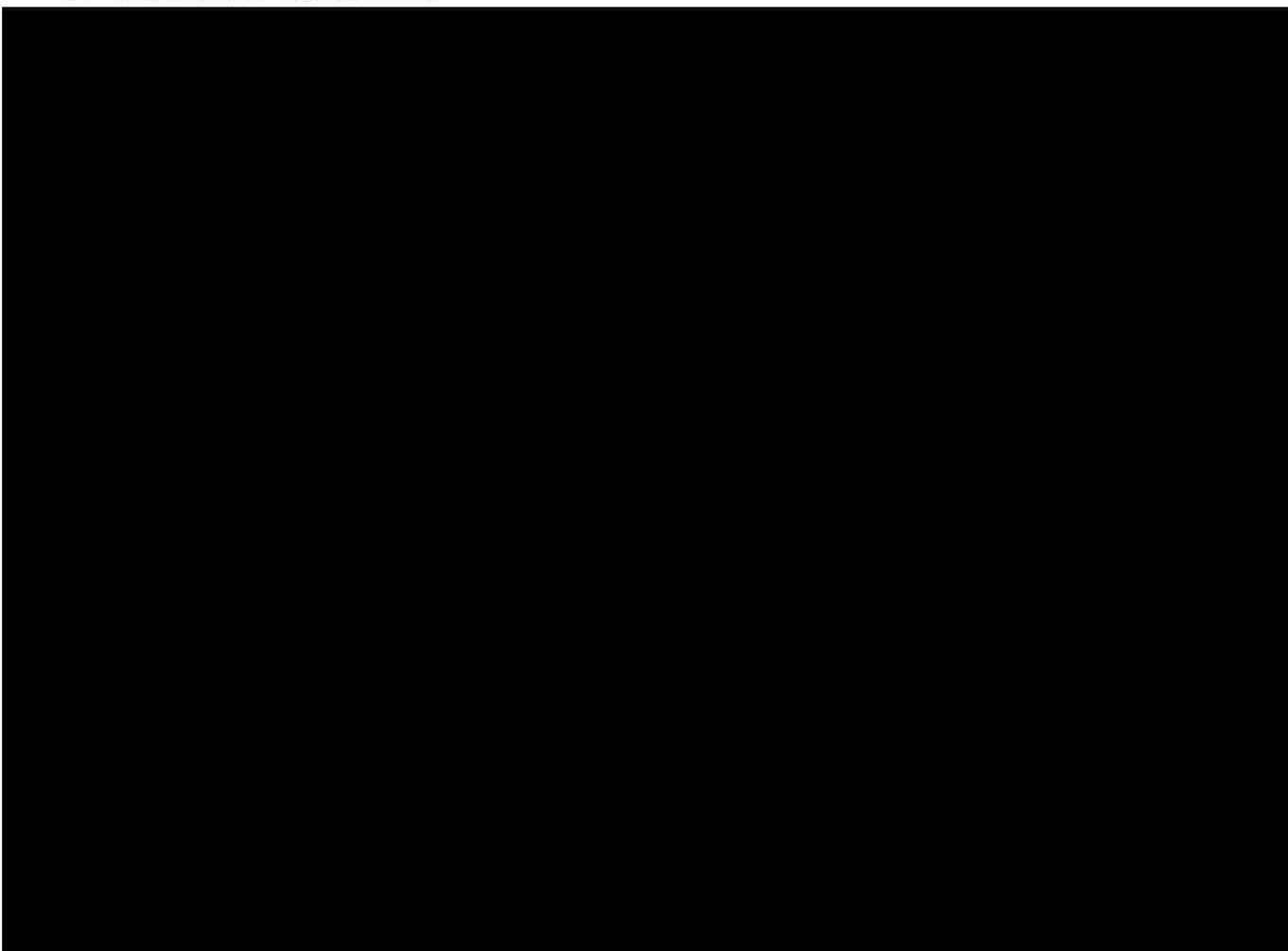


Zpráva o penetračním testu



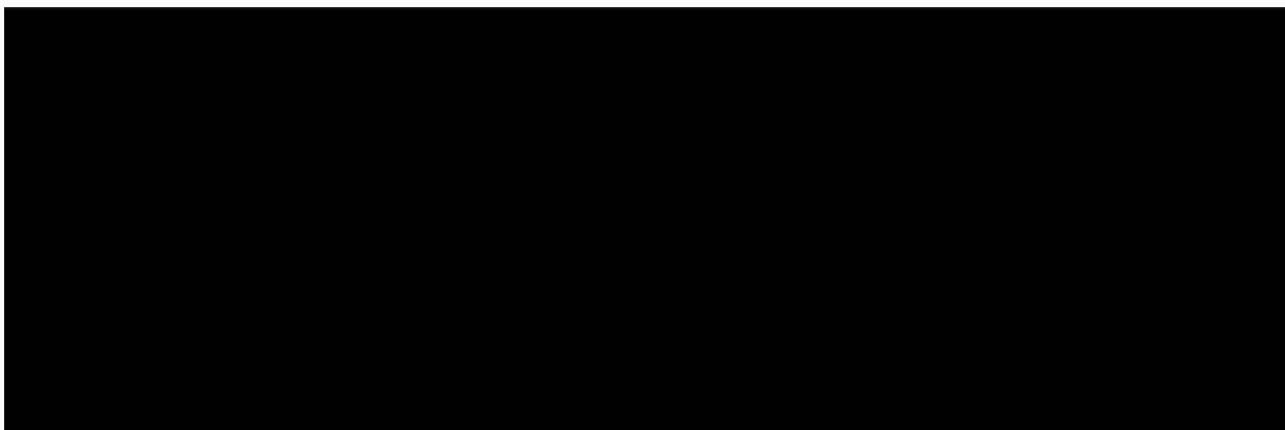


B. Ohodnocení zranitelností



C. Peer review





Místo a lhůty plnění

Penetrační test bude proveden prostřednictvím sítě Internet z lokality zcela oddělené od sítě objednatele.

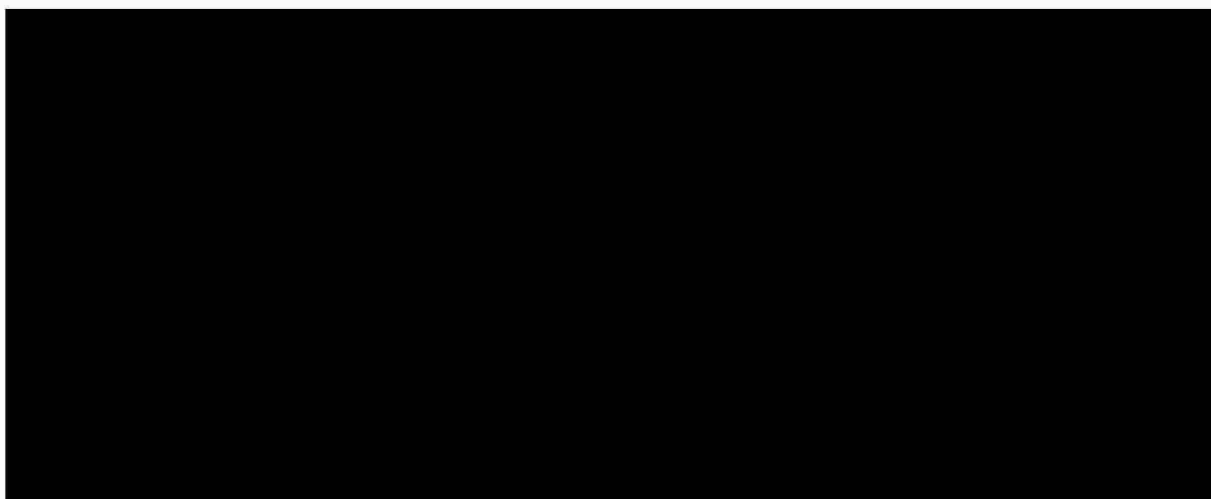
Předpokládaný termín započetí prací bude dle harmonogramu a poskytnutí potřebné součinnosti objednatele nevyhnutelné k zahájení testu.

Informace o rozsahu testů

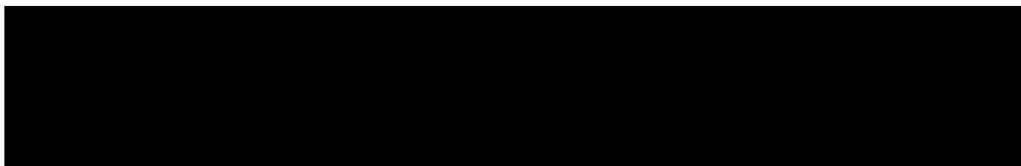
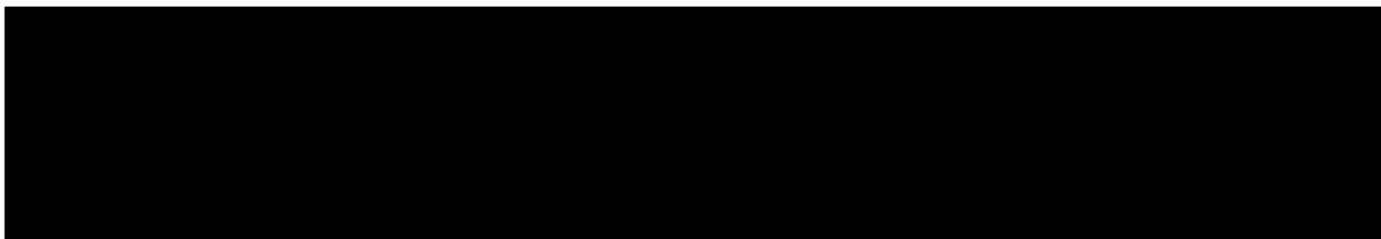
Předmětem testu je 7MD práce.

Součinnost objednatele

Pro řádné splnění nabízených činností je po objednateli požadováno:



Reference na podobné projekty ve finanční či veřejné sféře



Závěr



Přílohy

