Test v rámci sítě zapojeného Partnera

Tento test se vztahuje na sítě všech tří partnerů.

SW kontroly

Test	Splněno
Jsou analyzovány/detekovány toky směrované z privátního IP rozsahu na veřejné rozsahy.	ANO/NE
Jsou analyzovány toky obsahující veřejnou IP zadavatele (IP bude dodána při testování) a libovolnou veřejnou adresou.	ANO/NE
Generované NetFlow/IPFIX záznamy jsou ze sond exportovány na kolektor.	ANO/NE
Generované události jsou exportovány do nadřazeného kolektoru (pokud je architektura nasazení hierarchická).	ANO/NE
Obsahují zpracované NetFlow/IPFIX záznamy informace z L7 vrstvy požadované v rámci zadávací dokumentace (http-metoda, http-user-agent, http-hostname, http-url, DNS request, detaily protokolu SMB).	ANO/NE
Sonda umožňuje zachytávat vybraný provoz do PCAP souboru (filtr specifikující požadovaný provoz bude dodán při testování) a to na základě manuálního zadání.	ANO/NE
Sonda umožňuje zachytávat vybraný provoz do PCAP souboru (filtr specifikující požadovaný provoz bude dodán při testování) a to na základě automatického triggeru (událost, na základě které se záchyt spustí, bude zvolena při testování).	ANO/NE
Zadavatelem bude proveden vertikální scan port v rámci infrastruktury Partnera. Tato událost bude detekována a zobrazena softwarem analyzátoru .	ANO/NE
Zadavatelem bude proveden horizontální scan port v rámci infrastruktury Partnera. Tato událost bude detekována a zobrazena softwarem analyzátoru .	ANO/NE
Zadavatelem bude proveden přenos anomálně velkého objemu dat ven z infrastruktury Partnera. Tato událost bude detekována a zobrazena softwarem analyzátoru .	ANO/NE

Zadavatelem bude proveden slovníkový útok v rámci interní sítě Partnera na službu SSH. Tato událost bude detekována a zobrazena softwarem analyzátoru.	ANO/NE
Zadavatelem bude proveden realistický DoS útok v rámci interní sítě Partnera. Tato událost bude detekována a zobrazena softwarem analyzátoru.	ANO/NE
Zadavatelem bude proveden realistický DoS útok z vnějšku. Tato událost bude detekována a zobrazena softwarem analyzátoru .	ANO/NE
Zadavatelem bude provedeno spojení na veřejnou IP adresu z blacklistu GovCERT.CZ. Tato událost bude detekována a zobrazena softwarem analyzátoru.	ANO/NE
Zadavatelem bude proveden DNS-enumeration (Reverse lookup) na nejméně 1000 IP adres v rámci infrastruktury dodavatele, směrované na lokální DNS server. Tato událost bude detekována a zobrazena softwarem analyzátoru.	ANO/NE
Zadavatelem bude změněna MAC adresa na serveru. Tato událost bude detekována a zobrazena softwarem analyzátoru (bude poskytnut nezbytný časový prostor pro *„naučení se“* systému).	ANO/NE
Je možné se přihlásit na administrativní rozhraní analyzátoru pomocí https.	ANO/NE
Je možné se přihlásit na administrativní rozhraní kolektoru pomocí https.	ANO/NE
K události (detekované nebo uměle vytvořené dodavatelem) lze zobrazit oba směry síťového toku.	ANO/NE
V administrativním rozhraní analyzátoru je možné vytvořit filtr pro zobrazení/nezobrazení provozu (pravidlo bude dodáno v rámci testu podle dostupných dat v analyzátoru)	ANO/NE
Je možné v administrativním rozhraní analyzátoru označit jakoukoliv událost jako False-Positive a zajistit tak aby se daná událost již nezobrazovala provozu, nebo byla zobrazena s nejnižší kritičností (událost bude vybrána v rámci testu podle dostupných dat v analyzátoru)	ANO/NE
Je možno na kolektoru vytvořit report a zaslat ho šifrovaným emailem podepsaným pomocí PGP.	ANO/NE

Systém sond a kolektorů umožňuje filtrovat NetFlow/IPFIX záznamy pouze externí komunikace (procházející perimetrem) a tyto odesílat z vybraného kolektoru do GovCERT.CZ	ANO/NE
Kolektor umožňuje přijímat NetFlow/IPFIX ze sond a z jiných kolektorů, do GovCERT.CZ směřují přes zabezpečenou komunikační linku pouze záznamy externí komunikace.	ANO/NE
Kolektor umožňuje přijímat syslog z jiných kolektorů a modulů a směrovat ho do GovCERT.CZ (přes zabezpečenou komunikační linku)	ANO/NE
Kolektor obsahuje rozhraní pro konfiguraci a zpracování cílených záchytů do PCAP.	ANO/NE
Modul detekce DDoS vytváří signaturu útoku pro mitigaci útoku: modul detekce DDoS vytvoří a zadá BGP Flowspec pravidlo včetně signatury útoku.	ANO/NE
Modul detekce DDoS umoňuje jako reakci na probíhající útok spustit libovolný script na základě triggeru.	ANO/NE

HW kontroly

Test	Splněno
TAP je zapojen a zrcadlí data.	ANO/NE
TAP neomezuje prostupnost sítových toků, které jím prochází. Tedy byly nastaveny správné rychlosti portů 1000/100/10 Mb/s full nebo half duplex.	ANO/NE
TAP je odpojen od napájení. Data se nezrcadlí, v sítí není detekován významný výpadek provozu.	ANO/NE
TAP nemodifikuje data.	ANO/NE

Test – komunikace systému do GovCERT.CZ

Tento test se vztahuje na sítě všech tří partnerů.

SW kontroly

Test	Splněno

NetFlow/IPFIX data ze sond jsou přes zabezpečenou komunikační linku doručena do GovCERT.CZ.	ANO/NE
Syslog data ze sond jsou přes zabezpečenou komunikační linku doručena do GovCERT.CZ.	ANO/NE
Všechny instalované sondy upravují svá pravidla podle dat odebraných z Aktualizačního serveru GovCERT.CZ.	ANO/NE
Je dostupné rozhraní pro monitorování stavu běhu a funkce tunelu.	ANO/NE
V rámci přípojného bodu na straně GovCERT.CZ je možno konfigurovat přesměrování příchozích paketů na cílové IP adresy v rámci sítě GovCERT.CZ (routing, port forwarding)	ANO/NE
V případě výpadku/nevydařeného připojení na primární lokalitu je automaticky sestaveno spojení na záložní lokalitu.	ANO/NE
Klíče pro sestavení zabezpečené linky je možno dodat zadavatelem.	ANO/NE

HW kontroly

Test	Splněno
Aktualizační server v infrastruktuře NCKB běží.	ANO/NE
Aktualizační server v infrastruktuře NCKB lze konfigurovat prostřednictvím příkazové řádky a/nebo jednoduchého GUI	ANO / NE