Příloha B smlouvy

Akceptační testy – Etapa I.

Tyto akceptační testy budou provedeny po skončení Etapy I., tedy před integrací Analytického SW na Threat DB server a Intel MG DB server pracoviště GovCERT.CZ.

Test	Splněno
Analytický systém má jednotné grafické rozhraní (webové GUI), přístupné pomocí HTTPS s autentizací do všech svých komponent pomocí AD/LDAP.	ANO / NE
Data lze vyhledávat a agregovat dle zdrojové IP adresy, cílové IP adresy, zdrojového portu, cílového portu, domény, zadaného časového okna, CIDR, ASN, země, geoip, portu, vlastníka, abuse kontaktu, údaje, kdy byla IP adresa poprvé viděna v nějaké databázi, a údaje, kdy byla IP adresa naposledy viděna viděna v některé z externíchdatabází (přes Intel MQ) nebo interních databází připojených do Analytického systému.	ANO / NE
Data lze ručně opatřit libovolnými tagy, přičemž jeden záznam lze označit více tagy najednou.	ANO / NE
Data lze opatřit libovolnými tagy automaticky na základě definovaných pravidel, přičemž při splnění více pravidel zároveň může být jeden záznam označen více tagy najednou.	ANO / NE
Data lze vyhledávat a agregovat podle tagů přidělených v Analytickém systému.	ANO / NE
Data lze opatřit komentáři.	ANO / NE
Data lze vyhledávat a agregovat podle textu v komentářích přidělených v Analytickém systému.	ANO / NE
Data lze zobrazit v podobě: Sankeyův diagram.	ANO / NE
Data lze zobrazit v podobě: Chord diagram.	ANO / NE
Data lze zobrazit v podobě: Sequences sunburst.	ANO / NE
Data lze zobrazit v podobě: SPI graph	ANO / NE
Data lze zobrazit v podobě: Graf spojení.	ANO / NE
Data lze zobrazit v podobě: SPI view.	ANO / NE
Data lze zobrazit v podobě: NFSEN.	ANO / NE
Data lze zobrazit v podobě: IP/CIDR.	ANO / NE
Data lze zobrazit na základě geografických dat dané IP v podobě: zobrazení na mapovém podkladu.	ANO / NE
Data lze zobrazit v podobě: timeline kybernetické bezpečnostní události nebo incidentu.	ANO / NE
Data lze zobrazit v podobě: podíl událostí jednotlivých sítí Partnerů na celkovém počtu událostí.	ANO / NE
Systém umožňuje zobrazení na obrazovce a následný export zdrojových dat, použitých ke konkrétní vizualizaci.	ANO / NE
Systém je schopen zpracovat 2500 EPS kybernetických bezpečnostních událostí za sekundu a více.	ANO / NE

Systém umožňuje detekovat posloupnost událostí, tedy časovou souslednost jednotlivých bezpečnostních událostí.	ANO / NE
Systém umožňuje nacházet shodu v různých druzích dat podle zadaných vstupních parametrů, např. podle manuálně zadaných seznamů IP adres/domén.	ANO / NE
Systém umožňuje detekovat komunikaci na blacklistovanou IP adresu v rámci interní ThreatDB.	ANO / NE
Systém umožňuje jako reakci na korelační pravidlo vygenerovat korelovanou událost a vytvořit návrh na bezpečností incident pro operátora Analytického systému, který bude obsahovat všechny bezpečností události a související záznamy, které vedly k pozitivní detekci.	ANO / NE
Systém umožňuje jako reakci na korelační pravidlo automaticky blacklistovat IP adresu (vytvořit záznam v ThreatDB).	ANO / NE
Systém umožňuje schopnost blacklistovat IP adresu manuálně (zadat do ThreatDB) v rámci práce v GUI.	ANO / NE
Systém s pomocí metod síťové behaviorální analýzy (NBA) detekuje anomálně dlouhé spojení z jedné organizace na jednu IP adresu.	ANO / NE
Systém s pomocí metod síťové behaviorální analýzy (NBA) detekuje anomálně dlouhé spojení z více organizací na jednu IP adresu.	ANO / NE
Systém s pomocí metod síťové behaviorální analýzy (NBA) detekuje spojení z jedné organizace na jednu IP či doménu, která je blacklistovaná (integrace s interní ThreatDB).	ANO / NE
Systém s pomocí metod síťové behaviorální analýzy (NBA) detekuje spojení z více organizací na jednu IP či doménu, která je blacklistovaná (integrace s interní ThreatDB).	ANO / NE
Systém v rámci metod síťové behaviorální analýzy (NBA) umožňuje definovat prahové hodnoty při nalézání statistických anomálií v provozu jednotlivých organizací.	ANO / NE
Systém umožňuje v rámci NBA funkcionality v případě *„false-positive“* detekce vytvořit whitelist podle IP adresy, domény, portu a jejich libovolné kombinace.	ANO / NE
Systém je schopen zpracovat příchozí NetFlow/IPFIX údaje v objemu 250 000 NetFlow/s a více.	ANO / NE
Jako reakci na anomálii nalezenou pomocí NBA Systém generuje událost a vytváří návrh na bezpečností incident pro operátora Analytického systému, včetně záznamu o všech bezpečnostních událostech a souvisejících záznamech, které vedly k pozitivní detekci.	ANO / NE
Systém generuje výstupní XML soubor obsahující signaturu.	ANO / NE
Je požadována funkcionalita generovat alerty na základě korelačních nebo NBA funkcí Analytického systému a tyto alerty zasílat standardizovaným protokolem do externího ticketovacího systému GovCERT.CZ.	ANO / NE
Systém automaticky odmazává data podle objemového klíče, tedy při přiblížení se maximální velikosti ukládaných dat odmazává nejstarší záznamy.	ANO / NE
Systém automaticky odmazává data podle časového klíče, tedy odmazává položky starší určeného data, nebo odmazává položky starší než operátorem určený časový úsek.	ANO / NE
Jednotlivé detekované události i události vyhodnocené jako pravděpodobné incidenty jsou za specifikované časové období automaticky ukládány pro další využití v nadřazeném systému využívaném GovCERT.CZ.	ANO / NE
Systém umožňuje dodatečně označit dříve detekované události či skupinu událostí jako	ANO / NE

incidenty, pokud bude na základě dodatečných analýz tato skutečnost zjištěna.	
Operátor může na základě nahlášeného incidentu z jedné instituce vyhledat podobné události z jiných institucí, a to na základě společných charakteristik, zejména množství dat/paketů/spojení přenesených v časovém okně, použitých portů nebo TCP flagů.	ANO / NE
Webové rozhraní je přístupné z prohlížečů Firefox 50+, Chrome 54+, Safari 10+ a Edge 38+, a to bez externích pluginů nebo doplňků typu Flash, Silverlight anebo Java.	ANO / NE
Analytický systém je v jakémkoliv daném bodě schopen obnovit jednu z pěti posledních záloh pro obnovení systému obsahující zálohy konfigurací a základních indexů.	ANO / NE
Všechny komponenty systému zaznamenávají své auditní logy v souladu s vyhláškou 316/2014, §21.	ANO / NE
Analytický systém nabízí REST API schopný na dotaz vystavit aktuální blacklist IP adres/domén, kybernetické bezpečnostní incidenty za určité časové období, kybernetické bezpečnostní incidenty za konkrétní subjekt a kybernetické bezpečnostní incidenty v rámci určeného IP rozsahu.	ANO / NE
Řešení zahrnuje neomezenou výhradní licenci pro provoz celého Analytického systému po neomezenou dobu.	ANO / NE
Analytický systém má prostředí v českém nebo anglickém jazyce.	ANO / NE
Analytický systém umožňuje založení až 100 rozdílných uživatelských profilů/účtů.	ANO / NE
Analytický systém umožňuje souběžnou práci 10 fyzických uživatelů.	ANO / NE

Akceptační testy – Etapa II

Tyto akceptační testy budou provedeny po skončení Etapy II. , tedy po integraci Analytického SW na Threat DB server a Intel MG DB server pracoviště GovCERT.CZ.

Test	**Splněno**
Systém vystaví XML soubor obsahující signaturu, který je úspěšně vložen do Threat DB updatovacího serveru (Threat DB server není součástí tohoto VŘ).	ANO / NE
Jako reakci na anomálii nalezenou pomocí korelace různých zdrojů dat Analytický systém automaticky blacklistuje IP adresu (nebo doménu), a vystaví aktualizovaná data do Threat DB updatovacího serveru (Threat DB server není součástí tohoto VŘ).	ANO / NE
Systém pro analýzu čerpá blacklisty IP adres a domén z Intel MQ pracoviště GovCERT.CZ.	ANO / NE
Analytický systém prošel penetračními testy.	ANO / NE