Opis predmetu zákazky

Názov zákazky podľa verejného obstarávateľa: Podpora v oblasti kybernetickej a informačnej bezpečnosti Úradu pre Slovákov žijúcich v zahraničí

Stručný opis predmetu zákazky:

Zákazka je obstarávaná v rámci projektu „Podpora v oblasti kybernetickej a informačnej bezpečnosti Úradu pre Slovákov žijúcich v zahraničí". Opis predmetu zákazky vychádza z implementácie bezpečnostných opatrení v zmysle požiadaviek na odstránenie nálezov auditu kybernetickej bezpečnosti, respektíve samohodnotenia, a z požiadaviek určených zákonom č.69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej ako „zákon o KB"), zákonom č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení zákona č. 301/2023 Z. z. a príslušných vykonávacích právnych predpisov. Ak sa v opise predmetu zákazky odvolávajú technické požiadavky na konkrétneho výrobcu, výrobný postup, obchodné označenie, patent, typ, oblasť alebo miesto pôvodu alebo výroby, tieto môžu byť nahradené ekvivalentným riešením, ktoré musí spĺňať minimálne požadované parametre stanovené verejným obstarávateľom.

Verejný obstarávateľ predpokladá zadanie danej nadlimitnej zákazky postupom verejnej súťaže, zároveň predpokladá, že výsledkom verejného obstarávania bude Zmluva podľa § 269 ods. 2 zákona č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov.

Predpokladaný názov príslušnej časti predmetu zákazky / Predpokladaná lehota na realizáciu danej časti predmetu zákazky:

Časť I: Implementácia centrálneho systému na správu identít, konfigurácia a odladenie / 10 mesiacov od účinnosti zmluvy

Časť II: Implementácia dohľadového systému na sledovanie prevádzkových parametrov siete a systémov / 10 mesiacov od účinnosti zmluvy

Časť III: Implementácia ochrany prístupu k digitálnemu obsahu / 10 mesiacov od účinnosti zmluvy

Časť IV: Implementácia centralizovaného systému ochrany pred škodlivým kódom s monitorovaním detekcie inštalácie nelegálneho obsahu, vrátane automatizovaných nástrojov na detekciu škodlivej komunikácie na koncových staniciach a serveroch / 10 mesiacov od účinnosti zmluvy

Časť V: Implementácia zabezpečeného pripojenia do siete organizácie pomocou VPN a segmentácia siete / 10 mesiacov od účinnosti zmluvy

Časť VI: implementácia MFA pre vzdialený prístup do siete / 10 mesiacov od účinnosti zmluvy

Časť VII: Implementácia nástroja na sledovanie a detekciu prevádzky a neoprávnených spojení na hranici s vonkajšou sieťou / 10 mesiacov od účinnosti zmluvy

Časť VIII: Implementácia centrálneho Log manažment systému / 10 mesiacov od účinnosti zmluvy

Časť IX: Zálohovacie systémy – diskové polia, nástroj na zálohovanie / 10 mesiacov od účinnosti zmluvy

Časť X: Vypracovanie a zvedenie ISMS / 11 mesiacov od účinnosti zmluvy

Časť XI: Testovanie zraniteľností / 12 mesiacov od účinnosti zmluvy

Časť XII: Certifikovaný audit KB / 12 mesiacov od účinnosti zmluvy

1 NÁVRH OPISU ČASTI I. PREDMETU ZÁKAZKY: Implementácia centrálneho systému na správu identít, konfigurácia a odladenie

Implementácia centrálneho systému na správu identít, konfigurácia a odladenie. Produkt musí umožňovať vytváranie, modifikáciu a deaktiváciu používateľských identít, podporovať hromadné operácie a samoobslužné funkcie pre používateľov vrátane resetovania hesla a obnovy účtu. Systém musí podporovať rôzne autentifikačné metódy vrátane hesiel, biometrických údajov, tokenov a viacfaktorovej autentifikácie (MFA), zabezpečiť bezpečný prenos autentifikačných údajov a umožňovať definovanie prístupových práv na základe rolí a skupín používateľov. Produkt musí byť schopný integrovať sa s existujúcimi systémami a aplikáciami v organizácii, podporovať štandardné protokoly a API pre interoperabilitu a umožňovať centralizovanú správu identít a synchronizáciu dát medzi rôznymi systémami. Zabezpečenie dát musí byť zaistené šifrovaním uložených dát a auditovaním prístupov, pričom produkt musí byť v súlade s relevantnými právnymi a regulačnými požiadavkami, ako je GDPR a HIPAA. Administrátorské rozhranie musí byť intuitívne a ľahko použiteľné, rovnako ako užívateľské rozhranie, ktoré musí byť dostupné v rôznych jazykoch vrátane slovenčiny. Systém musí byť škálovateľný na podporu rastúceho počtu používateľov a aplikácií, optimalizovaný pre rýchle spracovanie autentifikačných a autorizačných požiadaviek, a zabezpečiť vysokú dostupnosť služieb.

Správa používateľov
Vytváranie a údržba identít
Produkt musí umožňovať vytváranie, modifikáciu a deaktiváciu používateľských identít.
Produkt musí podporovať hromadné operácie na správu identít (napr. import/export dát, hromadné aktualizácie).

Samoobslužné funkcie pre používateľov
Produkt musí umožňovať používateľom samoobslužné resetovanie hesla a obnovu účtu.
Produkt musí poskytovať používateľom možnosť aktualizovať svoje osobné údaje a nastavenia.

Autentifikácia a autorizácia

Autentifikačné mechanizmy
Produkt musí podporovať rôzne autentifikačné metódy vrátane hesiel, biometrických údajov, tokenov a viacfaktorovej autentifikácie (MFA).
Produkt musí zabezpečiť bezpečný prenos autentifikačných údajov pomocou šifrovania (napr. TLS).

Riadenie prístupu
Produkt musí umožňovať definovanie a spravovanie prístupových práv na základe rolí a skupín používateľov.
Produkt musí podporovať jemnozrnnú kontrolu prístupu k rôznym zdrojom a aplikáciám.

Integrácia a interoperabilita
Integrácia s existujúcimi systémami
Produkt musí byť schopný integrovať sa s existujúcimi systémami a aplikáciami v organizácii (napr. LDAP, Active Directory, cloudové služby).
Produkt musí podporovať štandardné protokoly a API (napr. SAML, OAuth, SCIM) pre interoperabilitu.

Centrálna správa a synchronizácia
Produkt musí umožňovať centralizovanú správu identít a synchronizáciu dát medzi rôznymi systémami.
Produkt musí poskytovať mechanizmy na riešenie konfliktov a konsolidáciu identít.

Bezpečnosť a súlad s predpismi
Ochrana údajov
Produkt musí poskytovať šifrovanie uložených dát a zabezpečenie proti neoprávnenému prístupu.
Produkt musí umožňovať auditovanie prístupov a zmien v identitách.

Súlad s regulačnými požiadavkami
Produkt musí byť v súlade s relevantnými právnymi a regulačnými požiadavkami (napr. GDPR, HIPAA).
Produkt musí umožňovať generovanie reportov pre účely auditu a súladu.

Užívateľské rozhranie a použiteľnosť
Administrátorské rozhranie
Produkt musí poskytovať intuitívne a ľahko použiteľné rozhranie pre správu identít a prístupových práv.
Produkt musí umožňovať administrátorom jednoduché prispôsobenie a konfiguráciu nastavení.

Užívateľské rozhranie
Produkt musí poskytovať prehľadné a priateľské rozhranie pre koncových používateľov pre správu ich identít.
Produkt musí byť dostupný v rôznych jazykoch vrátane slovenčiny.
Škálovateľnosť a výkonnosť

Škálovateľnosť systému
Produkt musí byť škálovateľný na podporu rastúceho počtu používateľov a aplikácií.
Produkt musí podporovať horizontálne škálovanie pre zvýšenie výkonu a dostupnosti.

Výkonnosť
Produkt musí byť optimalizovaný pre rýchle spracovanie autentifikačných a autorizačných požiadaviek.
Produkt musí zabezpečiť minimálnu odozvu a vysokú dostupnosť služieb.

Technická podpora
Produkt musí poskytovať prístup k technickej podpore pre riešenie problémov.
Produkt musí zahrňovať pravidelné aktualizácie a údržbu.

Súčasťou dodávky sú aj implementačné a konfiguračné práce.

2 NÁVRH OPISU ČASTI II. PREDMETU ZÁKAZKY: Implementácia dohľadového systému na sledovanie prevádzkových parametrov siete a systémov

Implementácia a konfgurácia monitorovacieho nástroja, ktorý bude monitorovať prevádzkové parametre prevádzkovaných systémov a ktorý bude alertovať v prípade, že dôjde k odchýlke týchto parametrov od bežnej prevádzky. Produkt musí poskytovať monitorovanie rôznych typov zariadení vrátane serverov, sietí, databáz, aplikácií a služieb v reálnom čase a podporovať monitorovanie fyzických, virtuálnych a cloudových prostredí. Produkt musí byť schopný generovať upozornenia na základe definovaných prahových hodnôt a podmienok, podporovať rôzne typy upozornení vrátane e-mailov, SMS a push notifikácií, a umožňovať administrátorom prispôsobiť pravidlá pre upozornenia a eskalačné pravidlá pre kritické incidenty. Škálovateľná architektúra musí podporovať horizontálne škálovanie na monitorovanie veľkých a komplexných infraštruktúr a umožňovať distribúciu monitorovacích agentov na rôzne geografické lokality. Produkt musí byť optimalizovaný pre vysoký výkon, schopný spracovať tisíce monitorovacích metrík za sekundu, podporovať efektívne ukladanie dát a rýchle dotazovanie na veľké objemy dát. Z hľadiska bezpečnosti musí produkt poskytovať šifrovanie dát pri prenose a uložení, umožňovať prístup k monitorovacím dátam iba autorizovaným používateľom prostredníctvom riadenia prístupových práv a podporovať integráciu s inými IT a bezpečnostnými systémami, ako sú SIEM, ITSM a CMDB. Užívateľsky priateľské webové rozhranie musí umožňovať správu a monitorovanie, prispôsobenie dashboardov podľa potrieb používateľov, a poskytovať širokú škálu preddefinovaných reportov a vizualizácií vrátane grafov, tabuliek a máp, ako aj generovanie ad-hoc reportov a export dát do rôznych formátov. Produkt musí poskytovať prístup k technickej podpore a konzultáciám, pravidelné aktualizácie a vylepšenia, komplexnú dokumentáciu vrátane užívateľských príručiek a technických manuálov. Súčasťou dodávky sú aj implementačné a konfiguračné práce.

3 NÁVRH OPISU ČASTI III. PREDMETU ZÁKAZKY: Implementácia ochrany prístupu k digitálnemu obsahu

Implementácia nástroja na ochranu prístupu k emailovej komunikácii, ako aj nástroja na filtrovanie nevyžiadaných správ a phishingových útokov.

Ochrana proti spamom a malvéru
Detekcia spamu
Produkt musí poskytovať pokročilú detekciu a filtrovanie spamu pomocou rôznych techník vrátane analýzy obsahu, blacklistingu, greylistingu a heuristických metód.
Produkt musí umožňovať prispôsobenie antispamových politík podľa potrieb organizácie.

Ochrana proti malvéru
Produkt musí poskytovať viacvrstvovú ochranu proti malvéru vrátane antivírusových skenov, analýzy príloh a behaviorálnej analýzy.
Produkt musí byť schopný detekovať a blokovať phishingové útoky a pokusy o sociálne inžinierstvo.

Bezpečnosť a šifrovanie e-mailov
Šifrovanie e-mailov
Produkt musí podporovať šifrovanie e-mailov pomocou štandardov ako S/MIME a TLS.
Produkt musí poskytovať možnosť automatického šifrovania na základe definovaných politík.

Bezpečnosť komunikácie
Produkt musí zabezpečovať bezpečný prenos dát medzi e-mailovými servermi pomocou protokolu TLS.
Produkt musí podporovať autentizáciu odosielateľa pomocou SPF, DKIM a DMARC.

Centralizovaná správa a monitorovanie
Centrálne rozhranie
Produkt musí poskytovať centralizované rozhranie na správu e-mailovej bezpečnosti, vrátane konfigurácie, monitorovania a reportovania.
Produkt musí umožňovať administrátorom spravovať a monitorovať e-mailovú prevádzku v reálnom čase.

Reportovanie a analýza
Produkt musí poskytovať podrobné reporty o e-mailovej prevádzke, detekcii hrozieb a stave systému.
Produkt musí umožňovať generovanie ad-hoc reportov a export dát pre ďalšiu analýzu.

Doručovanie a dostupnosť e-mailov
Spoľahlivosť doručovania
Produkt musí zabezpečiť spoľahlivé doručovanie e-mailov vrátane mechanizmov pre automatické opätovné doručovanie v prípade dočasných problémov.
Produkt musí podporovať load balancing a vysokú dostupnosť na zabezpečenie kontinuity e-mailovej služby.

Archivácia a zálohovanie

Produkt musí poskytovať funkcie pre archiváciu e-mailov na dlhodobé ukladanie a zabezpečenie súladu s regulačnými požiadavkami.
Produkt musí umožňovať pravidelné zálohovanie e-mailov a konfigurácií pre obnovu v prípade havárie.

Podpora a integrácia
Integrácia s inými systémami
Produkt musí byť schopný integrovať sa s bezpečnostnými riešeniami ako napr. FortiGate, FortiAnalyzer pre konsolidovanú bezpečnosť.
Produkt musí podporovať integráciu s bežnými e-mailovými systémami a službami (napr. Microsoft Exchange, Office 365, G Suite).

Technická podpora
Produkt musí poskytovať prístup k technickej podpore 24/7.
Produkt musí zahrňovať pravidelné aktualizácie a údržbu softvéru na zabezpečenie ochrany proti novým hrozbám.

Užívateľské rozhranie a použiteľnosť
Užívateľské rozhranie
Produkt musí poskytovať intuitívne a užívateľsky priateľské rozhranie pre administrátorov aj koncových používateľov.
Produkt musí podporovať viaceré jazyky vrátane angličtiny, španielčiny, francúzštiny a ďalších.
Užívateľské notifikácie
Produkt musí umožňovať konfiguráciu notifikácií pre používateľov o zablokovaných alebo zadržaných e-mailoch.
Produkt musí poskytovať možnosti pre používateľov na prehliadanie karantény a uvoľňovanie e-mailov podľa potreby.

Súčasťou dodávky sú aj implementačné a konfiguračné práce.

4 NÁVRH OPISU ČASTI IV. PREDMETU ZÁKAZKY: Implementácia centralizovaného systému ochrany pred škodlivým kódom s monitorovaním detekcie inštalácie nelegálneho obsahu, vrátane automatizovaných nástrojov na detekciu škodlivej komunikácie na koncových staniciach a serveroch

Implementácia a konfigurácia EDR/XDR/MDR riešenia na všetky existujúce koncové stanice a servery vrátane správy administrácie nasadeného systému. Funkčné požiadavky na nástroj:

Centralizovaná správa
Produkt musí poskytovať centralizovanú správu všetkých koncových zariadení (počítače, servery, mobilné zariadenia) z jedného rozhrania.
Produkt musí umožňovať spravovanie bezpečnostných politík a konfigurácií naprieč celou sieťou.

Monitorovanie a reportovanie

Produkt musí poskytovať detailné reporty o bezpečnostných udalostiach, stave systémov a ďalších relevantných metrikách.
Produkt musí podporovať real-time monitorovanie a poskytovanie upozornení na bezpečnostné hrozby.

Automatizácia a orchestrácia
Produkt musí umožňovať automatizáciu bežných bezpečnostných úloh a reakcií na incidenty.
Produkt musí podporovať integráciu s ďalšími bezpečnostnými nástrojmi pre orchestráciu komplexných bezpečnostných procesov.

Viacvrstvová ochrana
Produkt musí poskytovať viacvrstvovú ochranu proti malvéru, ransomvéru, phishingu a ďalším typom hrozieb.
Produkt musí zahŕňať funkcie ako firewall, antispam, webový filter a kontrolu zariadení.

Škálovateľnosť a dostupnosť
Produkt musí byť škálovateľný na podporu veľkých podnikových sietí.
Produkt musí poskytovať vysokú dostupnosť a spoľahlivosť, vrátane možnosti zálohovania a obnovenia.

MDR
Monitorovanie a detekcia hrozieb
Produkt musí poskytovať 24/7 monitorovanie a detekciu hrozieb.
Produkt musí zahŕňať pokročilú analýzu správania a detekciu anomálií.

Reakcia na incidenty
Produkt musí umožňovať rýchlu reakciu na bezpečnostné incidenty, vrátane izolácie infikovaných zariadení.
Produkt musí poskytovať podrobný popis incidentov a odporúčania pre ich nápravu.
Analýza a reportovanie
Produkt musí poskytovať pravidelné reporty o bezpečnostných udalostiach a stave ochrany.
Produkt musí umožňovať generovanie ad-hoc reportov na požiadanie.

Podpora a spolupráca
Produkt musí zahŕňať podporu špecialistov na bezpečnosť dostupných 24/7.
Produkt musí umožňovať spoluprácu s internými bezpečnostnými tímami zákazníka.

Premium Support
Technická podpora
Produkt musí poskytovať prístup k technickej podpore 24/7.
Produkt musí zahŕňať prioritný prístup k podpore a riešeniu incidentov.

Aktualizácie a údržba
Produkt musí poskytovať pravidelné aktualizácie a údržbu softvéru.
Produkt musí zahrňovať informácie o nových hrozbách a spôsoboch ich eliminácie.

Školenia a konzultácie
Produkt musí zahŕňať školenia pre administrátorov a používateľov.
Produkt musí poskytovať konzultácie na optimalizáciu bezpečnostných riešení.

Proaktívne služby
Produkt musí poskytovať proaktívne sledovanie bezpečnostných trendov a odporúčania pre zlepšenie ochrany.
Produkt musí umožňovať pravidelné bezpečnostné audity a analýzy.

Deployment and Upgrade
Nasadenie a konfigurácia
Produkt musí zahŕňať služby nasadenia a konfigurácie bezpečnostných riešení ESET v rámci infraštruktúry zákazníka.
Produkt musí poskytovať asistenciu pri prispôsobení nastavení bezpečnosti podľa potrieb zákazníka.

Aktualizácie a migrácie
Produkt musí zahrňovať služby pre aktualizáciu a migráciu na nové verzie softvéru.
Produkt musí zabezpečiť bezproblémový prechod na nové verzie bez prerušenia prevádzky.

Testovanie a overenie
Produkt musí zahŕňať testovanie nasadených riešení a overenie ich funkčnosti.
Produkt musí poskytovať podrobné správy o výsledkoch testovania a odporúčania na zlepšenie.

Dokumentácia a školenia
Produkt musí poskytovať kompletnú dokumentáciu o nasadení a konfigurácii.
Produkt musí zahŕňať školenia pre administrátorov na správne používanie a údržbu nasadených riešení.

Súčasťou dodávky sú aj implementačné a konfiguračné práce.

5 NÁVRH OPISU ČASTI V. PREDMETU ZÁKAZKY: Implementácia zabezpečeného pripojenia do siete organizácie pomocou VPN a segmentácia siete

Konfigurácia perimetrového firewallu za účelom zabezpečenia bezpečného vzdialeného prístupu do siete na základe VPN spojení s overovaním pomocou dvojfaktorovej autentizácie pre všetkých zamestnancov a dodávateľov

Návrh a konfigurácia segmentácie siete s prihliadnutím primárne na bezpečnosť a kategorizáciu využívaných informačných systémov. Súčasťou časti implementácia zabezpečeného pripojenia do siete organizácie pomocou VPN a segmentácia siete je dodávka firewallu pre zabezpečenie vysokej dostupnosti.

Špecifikácia minimálnych požiadaviek Firewall:

Hardvérové Špecifikácie
- GE RJ45 WAN / DMZ Porty: 1
- GE RJ45 Interné Porty: 3
- GE RJ45 FortiLink Porty: 1
- GE RJ45 PoE/+ Porty: Žiadne
- Bezdrôtové Rozhranie: Žiadne
- USB Porty: 1

- Konzola (RJ45): 1
- Interné Úložisko: Žiadne

Výkon Systému — Zmiešaná Prevádzka v Podnikovom Prostredí
- Priepustnosť IPS: 1 Gbps
- Priepustnosť NGFW: 800 Mbps
- Priepustnosť Ochrany Pred Hrozbami: 600 Mbps

Výkon Systému
- Priepustnosť Firewallu (1518 / 512 / 64 byte UDP pakety): 5/5/5 Gbps
- Oneskorenie Firewallu (64 byte UDP pakety): 4 µs
- Priepustnosť Firewallu (Pakety za Sekundu): 7.5 Mpps
- Súbežné Relácie (TCP): 700,000
- Nové Relácie/Sekundu (TCP): 35,000
- Pravidlá Firewallu: 5,000

VPN Výkon
- Priepustnosť IPsec VPN (512 byte): 4.4 Gbps
- IPsec VPN Tunnely medzi Bránami: 200
- IPsec VPN Tunnely Klient-Brána: 250
- Priepustnosť SSL-VPN: 490 Mbps
- Súbežní Používatelia SSL-VPN (Odporúčané Maximum, Tunel Mode): 200

Výkon SSL Inšpekcie
- Priepustnosť SSL Inšpekcie (IPS, priem. HTTPS): 310 Mbps
- CPS SSL Inšpekcie (IPS, priem. HTTPS): 320
- Súbežná Relácia SSL Inšpekcie (IPS, priem. HTTPS): 55,000

Kontrola Aplikácií
- Priepustnosť Kontroly Aplikácií (HTTP 64K): 990 Mbps
- Priepustnosť CAPWAP (HTTP 64K): 3.5 Gbps

Doplnkové Funkcie
- Virtuálne Domény (Štandardné / Maximálne): 10 / 10
- Maximálny Počet Podporovaných FortiSwitchov: 8
- Maximálny Počet FortiAPs (Celkový / Tunelový Režim): 10 / 5
- Maximálny Počet FortiTokenov: 500
- Maximálny Počet Registrovaných FortiClientov: 200
- Konfigurácie Vysokej Dostupnosti: Aktívny / Aktívny, Aktívny / Pasívny, Clustering

6 NÁVRH OPISU ČASTI VI. PREDMETU ZÁKAZKY: implementácia MFA pre vzdialený prístup do siete

Implementácia a konfigurácia multifaktorového overovania pre prístup k zvolených chráneným prostriedkom organizácie.

Autentifikácia používateľa
Produkt musí podporovať viacfaktorovú autentifikáciu (MFA) pomocou jednorazových hesiel (OTP).
Používateľ musí byť schopný prihlásiť sa pomocou biometrickej autentifikácie (odtlačok prsta, rozpoznávanie tváre) v prípade, že to zariadenie podporuje.
Produkt musí podporovať PIN kód ako alternatívny spôsob autentifikácie.

Generovanie jednorazových hesiel (OTP)

Produkt musí generovať časovo obmedzené OTP (Time-based OTP - TOTP) s 30-sekundovým intervalom.
Produkt musí generovať OTP na základe udalostí (Event-based OTP - HOTP) podľa požiadavky používateľa.
Generované OTP musia byť kompatibilné s RFC 6238 a RFC 4226.

Integrácia s Fortinet Security Fabric
Produkt musí byť schopný sa integrovať s Fortinet FortiGate, FortiAuthenticator a ďalšími produktmi Fortinet na poskytovanie MFA.
Produkt musí podporovať integráciu s tretími stranami prostredníctvom štandardných autentifikačných protokolov (napr. RADIUS, LDAP).

Užívateľské rozhranie a použiteľnosť
Aplikácia musí byť dostupná pre platformy iOS a Android.
Užívateľské rozhranie musí byť intuitívne a jednoduché na používanie.
Produkt musí podporovať viaceré jazyky, vrátane angličtiny, španielčiny, francúzštiny, nemčiny a ďalších hlavných svetových jazykov.

Bezpečnosť a ochrana údajov
Všetky uložené autentifikačné údaje musia byť šifrované pomocou AES-256.
Aplikácia musí poskytovať možnosť vzdialeného vymazania v prípade straty alebo krádeže zariadenia.
Produkt musí byť odolný voči rôznym typom útokov, vrátane phishingu, malvéru a man-in-the-middle útokov.

Správa zariadení a tokenov
Administrátori musia byť schopní pridávať, odoberať a spravovať tokeny používateľov prostredníctvom centralizovaného rozhrania.
Produkt musí poskytovať prehľad o aktívnych a neaktívnych tokenoch a generovať reporty pre účely auditu.
Používatelia musia byť schopní jednoducho obnoviť tokeny v prípade straty alebo výmeny zariadenia.

Oznámenia a upozornenia
Používateľ musí byť informovaný o každom úspešnom alebo neúspešnom pokuse o prihlásenie prostredníctvom push notifikácií.
Administrátori musia mať možnosť konfigurovať upozornenia pre rôzne bezpečnostné udalosti a anomálie.

Podpora a dokumentácia
Produkt musí byť dodávaný s podrobnou dokumentáciou pre používateľov aj administrátorov.
Musí byť k dispozícii technická podpora a pravidelné aktualizácie pre zabezpečenie kompatibility a bezpečnosti aplikácie.

Škálovateľnosť a výkonnosť
Produkt musí byť schopný zvládnuť veľký počet používateľov a autentifikačných požiadaviek bez zníženia výkonu.
Musí byť možné ľahko rozšíriť kapacitu a funkčnosť produktu v súlade s rastom organizácie.

Súčasťou dodávky sú aj implementačné a konfiguračné práce.

7 NÁVRH OPISU ČASTI VII. PREDMETU ZÁKAZKY: Implementácia nástroja na sledovanie a detekciu prevádzky a neoprávnených spojení na hranici s vonkajšou sieťou

Nástroj na sledovanie a detekciu prevádzky je výkonná platforma na správu logov, analýzu a reportovanie, ktorá poskytuje organizáciám orchestráciu, automatizáciu a reakciu z jedného miesta pre zjednodušené bezpečnostné operácie, proaktívnu identifikáciu a nápravu rizík a kompletnú viditeľnosť celého povrchu útoku.

Tento nástroj, integrovaný s bezpečnostnou infraštruktúrou, poskytne pokročilé schopnosti detekcie hrozieb, centralizovanú bezpečnostnú analýzu a úplnú informovanosť a kontrolu nad bezpečnostným postojom, čo pomáha bezpečnostným tímom identifikovať a eliminovať hrozby skôr, ako dôjde k narušeniu.

Nástroj umožní orchestráciu bezpečnostných nástrojov, ľudí a procesov pre zjednodušené vykonávanie úloh a pracovných postupov, analýzu a reakciu na incidenty a rýchle urýchlenie detekcie hrozieb, tvorby prípadov a vyšetrovania, ako aj zmiernenie a reakciu.

Nástroj umožní automatizáciu pracovných postupov a umožní spúšťanie akcií pomocou konektorov, playbookov a obslužných programov. Reagujte v reálnom čase na útoky na sieťovú bezpečnosť, zraniteľnosti a varovania o potenciálnych kompromitáciách s využitím informácií o hrozbách, korelácie udalostí, monitorovania, upozornenia a reportovania pre okamžitú reakciu.

Kľúčové vlastnosti:

- Analytika bezpečnostnej infraštruktúry s koreláciou udalostí a detekciou v reálnom čase naprieč všetkými logmi, so službou indikátorov kompromitácie (IOC) a detekciou pokročilých hrozieb
- Integrácia bezpečnostnej infraštruktúry s rôznymi bezpečnostnými nástrojmi pre hlbšiu viditeľnosť a kritické poznatky o sieti
- Podniková vysoká dostupnosť na automatické zálohovanie databáz (až štvornódový klaster), ktoré môžu byť geograficky rozptýlené pre obnovu po havárii
- Bezpečnostná automatizácia na zníženie komplexnosti, využívanie REST API, skriptov, konektorov a automatizačných skratiek na urýchlenie bezpečnostnej reakcie a zníženie času na detekciu
- Riešenie pre viac tenantov s riadením kvót, využívanie (ADOMs) na oddelenie údajov zákazníkov a správu domén pre efektívnosť a dodržiavanie predpisov
- Flexibilné možnosti nasadenia ako zariadenie, VM, hostované alebo verejný cloud.

Súčasťou dodávky sú aj implementačné a konfiguračné práce.

8 NÁVRH OPISU ČASTI VIII. PREDMETU ZÁKAZKY: Implementácia centrálneho Log manažment systému

Zaobstaranie, implementácia a konfigurácia centrálneho logovacieho systému, ktorý bude bezpečným spôsobom zbierať, vyhodnocovať, vizualizovať a ukladať systémové logy zo všetkých dôležitých systémov organizácie. Predmetom verejného obstarávania je dodávka a implementácia systému pre centralizované ukladanie a správu logov s integrovaným systémom analýzy a riešenia bezpečnostných udalostí/incidentov zo systémov a aplikácií obstarávateľa a jeho podriadenej organizácie.

Všetky technické parametre/funkcionality, resp. vlastnosti požadovaného predmetu zákazky predstavujú minimálne požiadavky, ktoré musia byť splnené v ponuke uchádzača. V prípade, že by sa záujemca/uchádzač cítil dotknutý vo svojich právach, t.j., že by týmto opisom dochádzalo k znevýhodneniu alebo k vylúčeniu určitých záujemcov/uchádzačov alebo výrobcov, alebo že tento predmet zákazky nie je opísaný dostatočne presne a zrozumiteľne, tak vo svojej ponuke môže uchádzač použiť technické riešenie ekvivalentné, ktoré spĺňa kvalitatívne, technické, funkčné požiadavky na rovnakej a vyššej úrovni, ako je uvedené v tejto časti výzvy, túto skutočnosť však musí preukázať uchádzač vo svojej ponuke.

Všeobecné požiadavky na systém:

- Systém pracuje ako fyzická appliance s jedným uceleným webovým rozhraním pre všetky administrátorské i operátorské činnosti. Nevyžaduje inštaláciu ďalších systémov a aplikácií okrem podpory zberu na iných lokalitách (mimo centrálu) a agenta pro zber Windows logov.
- Konfigurácia systému sa musí vykonávať v grafickom rozhraní jednotnej užívateľskej konzoly, Systém musí poskytovať podporu pre vizuálne programovanie pre všetky kroky spracovania strojových dát. Vo webovom rozhraní nesmie byť povinná konfigurácia s využitím skriptov, makier alebo textových konfiguračných polí, do ktorých sa skripty a makrá vkladajú
- Systém umožňuje doplnenie parseru pre zariadenia, aplikácie alebo systémy mimo uvedeného zoznamu užívateľom bez nutnosti spolupráce s výrobcom alebo dodávateľom ponúkaného systému - užívateľsky definované parsery. Dokumentácia systému musí obsahovať prehľadný návod na vytváranie zákaznických parserov a systém musí obsahovať možnosť testovania a ladenia zákaznickych parserov bez vplyvu na ostatné produkčné funkcie systému. Pre vytváranie nesmie byť použité textové písanie programového kódu, ale tzv. vizuálne programovanie, ktoré automaticky opravuje a upozorňuje na chyby.
- Systém umožňuje v grafickom rozhraní vizuálneho programovacieho jazyka jednoducho vykonávať triedenie a značkovanie vstupných dát pre ich ďalšie spracovanie. Nie je prípustné nastavenie triedenia vstupných dát vo forme skriptu/makra zobrazeného v textovom okne.
- Systém prijíma a spracováva logy, udalosti a ďalšie strojovo generované dáta prostredníctvom minimálne nasledujúcich protokolov: UDP/TCP 514 (SYSLOG), TCP 20514 (RELP, nešifrovane) a TCP 20515 (RELP, šifrovane). Systém musí umožnovať príjem logov i na rozsahu minimálne 50 UDP a TPC portov.
- Prijaté logy systém štandardizuje do jednotného formátu a logy sú rozdeľované príslušných polí podľa ich typu. Systém musí zároveň uchovávať originálne verzie správ.
- Pre hodnoty jednotlivých parsovaných polí je možné v definícii parseru zmeniť typ a štandardizovať minimálne na tieto základné druhy: číslo, IP adresa, MAC adresa, URL. Nad uloženými dátami typu číslo musí byť možné pri vyhľadávaní vykonávať matematické operácie (súčty všetkých hodnôt, priemery, najmenšie/najväčšia hodnota a pod.)
- Systém zachovává pôvodné informácie zo zdroju logu o časovej značke udalosti, ale nedôveruje jej a vytvára vlastné dôveryhodné časové razítko ku každému logu, která vzniká v okamihu prijatia logu systémom a ktorým sa systém riadi.

- Všechny polia a položky prijaté systémom sú automaticky indexované. Nad všetkými položkami je možné ihneď vykonávať vyhľadávanie bez nutnosti dodatočného ručného indexovania administrátorom.
- Možnost zberu událostí minimálne vo formátoch RAW, Syslog, CEF, LEEF, JSON RFC7159.
- Systém nesmie umožniť mazanie alebo modifikovanie uložených logov ani konfiguračnou zmenou administrátorovi systému s najvyššími oprávneniami. Každý log musí mať unikátny identifikátor, ktorý umožní jeho jednoznačnú identifikáciu.
- Systém musí umožňovať konfiguráciu filtrácie nerelevantných správ
- Systém vykonáva konsolidáciu logov na vlastnom storage priestore.
- Systém umožňuje jednoduché vyhľadávanie udalostí a okamžité vytváranie grafických reportov (ad hoc) bez nutnosti dodatočného programovania alebo aplikovania dopytov v SQL jazyku. Reportovací nástroj musí byť integrálnou súčasťou navrhovaného systému a byť súčasťou jednotného rozhrania
- Systém vykonáva ucelenú vizualizáciu logov, udalostí a strojových dát (grafy udalostí). Vizualizácia musí byť dynamická, t.j. voľbou v jednom grafe sa ostatné príslušné grafy v pohľade na dáta upravia podľa požadovanej voľby automaticky.
- Systém umožňuje jednoducho vytvárať grafické znázornenie udalostí nad všetkými uloženými dátami za ľubovoľné časové obdobie bez nutnosti modifikácie konfigurcie systému alebo parametrov uložených dát.Historické dáta v požadovanej dĺžke retencie uložené v systéme j možné prehľadávať okamžite bez časových strát opätovného importu alebo dekomprimácie starších dát, prehľadávanie nesmie vyžadovať manuálnu konfiguráciu a zásahy používateľa
- Systém vykonáva automatické doplňovanie reverzných DNS záznamov a GeoIP informácií k udalostiam a v prípade GeoIP ich grafické znázornenie na mape bez nutnosti využívať služby tretích strán či externé aplikácie.
- Systém musí podporovať natívne získavaie logov z Office365.
- V prípade krátkodobého preťaženia systému nesmie dôjsť k strate logov. Všetky prijaté nespracované logy/udalosti musia byť ukladané do vyrovnávacej pamäte.
- Systém musí umožňovať unifikované vyhľadávanie naprieč všetkými typmi dát a zariadení podľa normalizovaných polí
- Systém musí spĺňať požadavky normy STN/ISO 27001:2013 pre získavanie auditných záznamov. Toto potvrdenie nie je možné nahradiť certifikátom na společnosť dodávateľa (subdodávateľa) alebo výrobcu ponúkaného systému. Nie je ho možné nahradiť ani čestným vyhlásením.
- Systém musí mať možnosť uloženia užívateľom vytvorených pohľadov na dáta (dashboardov) pre budúce spracovanie. Výrobcom dodané typy pohľadov nesmie byť možné nevratne modifikovať
- Systém obsahuje reportovací nástroj s prednastavenými najbežnejšími reportami a možnosťou vlastných úprav a vytváranie nových pohľadov. Pre vytváranie nových pohľadov na dáta nie je prípustné používať povinne SQL jazyk.
- Systém obsahuje predpripravené pohľady na uložené dáta podľa jednotlivých kategórií zdrojových zariadení i podľa logického členenia.
- Na základe pohľadu na uložené dáta je možné vykonať export dát v štruktúrovanom formáte tak, ako sú v pohľade skutočne zobrazené
- Konfiguračné a systémové rozhranie a dokumentácia musia byť identické v anglickom i v slovenskom alebo českom jazyku. Nepripúšťa sa obmedzená dokumentácia v slovenskom alebo českom jazyku.
- Systém musí umožňovať kapacitnú i výkonovú škálovatelnosť.

- Monitoring stavu systému - alertovanie pri prekročení prahových hodnôt alebo chybe systému, preposlanie upozornenia pomocou SMTP nebo Syslog.
- Systém musí obsahovať REST-API pre integráciu s externým monitorovacím systémom (Zabbix, Nagios, PRTG a pod.)
- Jednotná centrálna webová konzola pre prístup k logom, alertom, reportom a pre správu systému. Z tejto konzoly sa vykonáva kompletná konfigurácia, správa a analýza logov. Nie je prípustné, aby dodaný systém mal viacero konzol pre jednotlivé časti systému.
- Systém musí umožňovať jednoduché vytváranie užívateľských rolí definujúcich prístupové práva k uloženým udalostiam a jednotlivým ovládacím komponentom systému.
- Systém musí vykonávať parsovanie a normalizáciu prijatých udalostí bez nutnosti inštalovať externé aplikácie alebo systémy a to priamo vo svojom rozhraní. Jedinou prípustnou výnimkou je monitorovanie systémov Windows, ktoré cez WMI protokol neumožňujú monitorovať textové logy.
- Systém musí podporovať overovanie užívateľa systému na externom LDAP serveri. V prípade výpadku externého LDAP systému musí podporovať overenie z lokálnej databázy. Systém musí automaticky zaznamenávať užívateľské meno ku každej prevedej akcii užívateľom.

Výkonnostné a SW parametre systému

- Systém funguje formou HW appliance (všetkych časti systému je možné nastavit v centrálnej webovej konzole a nie je potrebné upravovať žiadne konfiguráčné súbory, scripty, alebo makra v príkazovom riadku).
- Aktualizácie systému sú distribuované v jednotnom balíku a ich inštalácia je vykonávaná cez centrálnu správcovskú konzolu. Všetky aktualizácie sú vykonávané z webového rozhrania systému bez potreby asistencie výrobcu/dodávateľa.
- Systém musí podporovať downgrade, napríklad pri problémoch s novou verziou systému po upgrade.
- Priemerný trvalý príjem min. 2000 udalostí za sekundu pri priemernej veľkosti jednej udalosti
- 700Byte. Systém musí preukázateľne kompletne spracovať prijaté udalosti vrátane vytvorenia očakavaných metadát (DNS-PTR, čisla a mená ASN, geolokácie), zaisťovanie
- Normalizácie, zamedzovania straty prijatých udalostí, alebo posunutiu dôverychodného časového razítka udalosti.
- Špičkový príjem minimálne 4000 udalostí za sekundu po dobu najmenej 10 minút pri priemernej veľkosti jednej udalosti 700Byte. Systém musí pri špičkovom príjme preukázateľne kompletne spracovať prijaté udalosti vrátane vytvorenia očakavaných metadát (DNS-PTR, čisla a mená ASN, geolokácie), zaisťovanie normalizácie, zamedzovania straty prijatých udalostí, alebo posunutiu dôverychodného časového razítka udalosti.
- Licenčne neobmezený počet zariadení pre príjem zasielaných udalostí. Licenčne neobmezený počet udalostí v GB za deň alebo licencia na minimálne 200GB uložených udalostí za deň. Integrovaná databáza musí mať čistú veľkosť najmenej 12 TB a musí podporovať kompresiu ukladaných dát
- Užívateľská konfigurácia vlastných parserov pomocou vizuálneho programovacieho jazyka v centrálnej správcovskej webovej konzole. Vizuálny programovací jazyk musí užívateľovi umožniť písať vlastné parsery bez nutnosti znalosti programovania (napr. Node-RED, Microsoft VPL, Blockly apod). Vizuálny programovací jazyk nie je prezentovaný textovo, ale graficky formou blokov, ktoré obsahujú aplikačnú logiku.

- Konfigurácia užívateľských parserov musí umožňovať automatické doplňovanie DNS reverzných záznamov, GeoIP informácie a identifikáciu výrobcu zariadenia podľa MAC adresy.
- Systém musí podporovať doplňovanie správ o statické informácie z textových tabuliek, napríklad k užívateľskému menu doplniť informáciu o jeho emailovej adrese, členstve v AD skupinách a pod. Pre automatickú aktualizáciu takto uložených doplnkových informácií musí byť možné tieto textové tabuľky doplniť pomocou REST API systému a modifikovateľné cez webové rozhranie systému.
- Možnosť on-line ladenia užívateľsky definovaných parserov - pri ich vytváraní je možné vložiť vlastné testovacie správy, pri zmene je okamžite zobrazená výsledná podoba rozparsovaných dát a prípadné chybové hlásenia.
- V centrálnej správcovskej konzole je možné pridávať k jednotlivým zdrojom dát, aplikáciám, zariadeniam alebo IP subnetom tzv. značky, označujúce napríklad umiestnenie zariadenia, typ zariadenia, kritickosť zariadenia a pod. Systém musí obsahovať preddefinované značky, ktoré automaticky pridáva k prijímaným správam (napríklad konfiguračná zmena, úspešné overenie užívateľa, neúspešné overenie užívateľa, správa z Windows, správa generovaná firewallom a pod.)
- Všetky pridávané značky sú ukladané s každou prijatou udalosťou, na základe značky je možné filtrovať dáta alebo obmedzovať oprávnenia užívateľov systému k jednotlivým udalostiam.
- Systém musí byť predpripravený pre zrkadlenie a clustrové zapojenie – 2 nody.
- V prípade zapojenia ako dvojnodový cluster sa systém správa ako jeden celok.
- V prípade využitia dvoch nodov v clustri sa zrýchľuje vyhľadávanie a sú automaticky prehľadávané všetky dáta na všetkých zariadeniach v clustri.
- V prípade rozšírenia systému na cluster musí navrhovaný systém zaistiť bezvýpadkovosť zberu logov.
- Systém musí umožňovať export dát ve formáte vhodnom pre ďalšie strojové spracovanie bez dodatočných obmedzení na časové obdobie, množstvo, alebo obsah exportovaných dát.
- Podpora zálohovania alebo obnovy konfigurácie v jednom kroku a jednom súbore pre celý systém.
- Podpora zálohovania dát na externý systém, požadované je plánované aj ad-hoc zálohovanie.

Alerty
- Systém je schpný na základe zadaných podmienok splnených v prijatých dátach vygenerovať alert.
- Text emailu vygenerovaného alertom môže byť užívateľsky definovaný s premennými z prijatej rozparsovanej udalosti.
- Systém musí obsahovať výrobcom predpripravené sety/vzory alertov a korelácií
- Užívateľská konfigurácia alertov pomocou vizuálneho programovacieho jazyka v centrálnej správcovskej konzole. Vizuálny programovací jazyk nie je prezentovaný čisto textovo, ale textovo-grafickou formou, ktorá vizualizuje aplikačnú logiku. Konfigurácia alertu alebo korelácie musí umožňovať okamžitú kontrolu
- Ako výstupné pravidlo alertu musí systém vedieť odoslať udalosť, ktorá alert vyvolala na externý systém minimálne prostredníctvom SMTP alebo Syslog cez TCP protokol. Pre Syslog protokol je poadovaná možnosť definície formátu dát pre jednoduchšiu integráciu so systémami tretích strán.
- V alertoch je možné využívať značky (napríklad: pošli alert iba v prípade, že sa udalosť stala na kritickom serveri, ktorý beží v určitej lokalite).

- Systém podporuje funkcie SIEM - korelácie udalostí a upozornenia s hraničnými limitmi. Definícia korelačných pravidiel musí mať možnosť vloženia testovacej správy a výsledku testu vykonanej akcie

Zber udalostí v prostredí Microsoft
- Udalosti z Microsoft prostredí sú získavané pomocou agenta inštalovaného priamo na koncovom Windows systéme. Windows agent musí súčasne podporovať ako monitoring interných windows logov, tak i monitoring textových súborových logov.
- Agent zaisťuje zber nemodifikovaných udalostí a detailné spracovánie auditných informácií.
- Agent podporuje nastavenie filtrácie odosielaných udalostí pomocou centrálnej správcovskej konzoly
- Filtrácia odosielaných udalostí agentom sa konfiguruje pomocou vizuálneho programovacieho jazyka v centrálnej správcovskej konzole. Nerelevantné logy sú filtrované na strane windows agenta a nie sú odosielané po sieti. Vizuálny programovací jazyk nie je prezentovaný textovo, ale textovo-grafickou formou, ktorá vizualizuje aplikačnú logiku.
- Windows agent nevyžaduje administrátorské zásahy na koncovom systéme – je centrálne spravovaný a automaticky aktualizovaný priamo z centrálnej správcovskej konzoly systému.
- Správa a aktualizacia Windows agenta sa nevykonáva z Group Policy.
- Komunikácia Windows agenta a centrálného systému musí být šifrovaná.
- Windows agent musí podporovať zber nielen zo základných systémových logov (Aplikácie, Zabezpečenie, Inštalácie, Systém), ale je možné z centrálnej správcovskej konzoly nastaviť i zber všetkých ostatných logov v zložke Protokoly aplikácií a služieb. Windows agent musí podporovať centralizované nastavenie z administrátorskej konzoly systému pre zber textových logov vrátane možnosti výberu ich formátu.
- Windows agent musí automaticky dopĺňať ku všetkým odosielaným udalostiam ich textový popis tak, ako je zobrazený v Prohliadači udalostí (Event Viewer) na koncovom systéme.
- Počet inštalácií Windows agenta nesmie byť licenčne ani časovo obmedzený.

Podpora pre zber udalostí z pobočiek
- Systém musí obsahovať centrálne spravované riešenie, ktoré zbiera udalosti na pobočkách alebo v záložnom datacentre a umožňuje ich odoslanie po saturovanej linke bez straty dát.
- Systém musí podporovať centralizovanú správu pre zber udalostí z viacerých lokalít priamo z centrálneho úložiska dát vrátane požiadaviek na virtualizáciu a komunikačnú maticu pre šifrovaný prenos dát
- Riešenie pre zber udalostí z iných lokalít musí byť schopné automaticky nadviazať spojenie s centrálnym úložiskom dát a prenášané dáta šifrovať. V prípade výpadku spojenia medzi inou lokalitou a centrálou musí spojenie automaticky obnoviť.
- Riešenie musí komunikovať po definovanom IP protokole, aby mohla byť centrálne nastavená kvalita služby (QoS) pre prenos udalostí.
- Riešenie musí poskytovať kapacitu vyrovnávacej pamäte pre minimálne 100GB udalostí, ktoré na inej lokalite môžu vzniknúť počas výpadku spojenia medzi inou lokalitou a dátovým centrom.
- Riešenie pre zber udalostí z iných lokalít musí mať výkon minimálne 5 tisíc udalostí /s. a to i pri trvalej záťaži.
- Riešenie pre zber udalostí z iných lokalít musí poskytovať podporu na identických UDP i TCP portoch ako hlavný systém a pre aktívny zber z lokálnych Windows agentov.

- Riešenie pre zber udalostí z iných lokalít musí byť poskytované ako fyzický systém aj ako virtuálny systém pre VMware ESXi a Hyper-V. Výber fyzického alebo virtuálneho riešenia je voliteľný na základe možností dostupných na predmetnej vzdialenej lokalite podľa voľby obstarávateľa.
- Riešenie pre zber udalostí z iných lokalít musí byť schopné komunikovať s centrálou i skrze viacnásobný preklad adries (NAT).

Súčasťou dodávky sú aj implementačné a konfiguračné práce.

9 NÁVRH OPISU ČASTI IX. PREDMETU ZÁKAZKY: Zálohovacie systémy – diskové polia, nástroj na zálohovanie

Implementácia zabezpečeného systému zálohovania vo fyzicky oddelenej budove za účelom zabezpečenia kópie dôležitých systémov a dát v prípade zlyhania alebo zničenia primárnej serverovne. Systém zálohovania by mal mať ochranu pred zmazaním a prepísaním uložených dát a mal by uchovávať zálohy v šifrovanej podobe.
Požiadavky na zálohovací systém alebo ekvivalent:
NAS Storage
1 x Synology RS2423RP+
4 x Synology Enterprise 3.5" 16 TB, 7.2K SAS 3 - HAS5300-16T
1 x Posuvne lyziny - RKS-02
SW pre zálohovanie buď aktuálne využívaný, alebo Veeam B&R Free (10 VMs

Súčasťou dodávky sú aj implementačné a konfiguračné práce.

10 NÁVRH OPISU ČASTI X. PREDMETU ZÁKAZKY: Vypracovanie ISMS

Vytvorenie systému riadenia informačnej bezpečnosti vrátane metodiky riadenia aktív a rizík v súlade so zákonom 69/2018 Z. z. a vyhláškou 362/2018 Z. z. Spolupráca pri zavádzaní systému riadenia informačnej bezpečnosti do praxe. Táto činnosť bude zahŕňať:

Názov podaktivity		**Bližšie činnosti v zmysle výzvy**	**Požadované činnosti**
a)	Organizácia kybernetickej a informačnej bezpečnosti	Vypracovanie bezpečnostnej dokumentácie vrátane rozsahu a spôsobu plnenia všeobecných bezpečnostných opatrení;	Bezpečnostná stratégia kybernetickej bezpečnosti; Bezpečnostná politika kybernetickej bezpečnosti a informačnej bezpečnosti; Deklarácia a záväzok vedenia; Štatút bezpečnostného výboru; Vypracovanie bezpečnostného projektu ISVS;
		Vypracovanie štatútu bezpečnostného výboru;	
		Vypracovanie bezpečnostného projektu informačného systému verejnej správy;	
b)	Riadenie rizík	Identifikácia všetkých aktív súvisiacich so zariadeniami na spracovanie informácií a centrálne zaznamenávanie inventáru týchto aktív podľa ich hodnoty vrátane	Identifikácie všetkých aktív; Inventarizácia aktív; Katalóg aktív; Riadenie rizík;

		určenia ich vlastníka, ktorý definuje požiadavky na ich dôvernosť, dostupnosť a integritu;	Smernica pre riadenie bezpečnostných rizík; Metodika pre riadenie bezpečnostných rizík; Implementácia predmetných IRA;
		implementáciu systému pre inventarizáciu aktív;	
		Riadenie rizík pozostávajúce z identifikácie zraniteľností, identifikácie hrozieb, identifikácie a analýzy rizík s ohľadom na aktívum, určenie vlastníka rizika, implementácie organizačných a technických bezpečnostných opatrení, analýzy funkčného dopadu a pravidelného preskúmavania identifikovaných rizík v závislosti od aktualizácie prijatých bezpečnostných opatrení;	
		Vypracovanie a implementácia interného riadiaceho aktu riadenia rizík kybernetickej a informačnej bezpečnosti;	
c)	Personálna bezpečnosť	Vypracovanie postupov pri zaradení osoby do niektorých z bezpečnostných rolí; Zavedenie plánu rozvoja bezpečnostného povedomia a vzdelávania; Vypracovanie spôsobov hodnotenia účinnosti plánu rozvoja bezpečnostného povedomia; Určenie pravidiel a postupov na riešenie prípadov porušenia bezpečnostnej politiky; Zavedenie postupov pri skončení pracovnoprávneho vzťahu alebo iného obdobného vzťahu; Zavedenie postupov pri porušení bezpečnostných politík;	Plán rozvoja bezpečnostného povedomia vrátane spôsobov hodnotenia účinnosti plánu, vrátane určenia pravidiel a postupov na riešenia prípadov porušenia bezpečnostnej politiky; Zavedenie postupov pri skončení pracovnoprávneho vzťahu alebo iného obdobného vzťahu, zavedenie postupov pri porušení bezpečnostných politík; Smernica pre používateľov; Riadenie personálnej bezpečnosti;
		Vypracovanie alebo aktualizácia interného riadiaceho aktu s bezpečnostnými zásadami pre koncových používateľov;	
		Vypracovanie a implementácia postupov a procesov upravujúcich personálnu bezpečnosť organizácie prostredníctvom interného riadiaceho aktu;	

d)	Riadenie prístupov	Vypracovanie a implementácia zásad riadenia prístupov osôb k sieti a informačnému systému; vypracovanie a implementácia postupov a procesov upravujúcich riadenie prístupov organizácie;	Riadenie prístupových práv; Zapracovanie a implementácia postupov a procesov napr. prostredníctvom RACI matice v nadväznosti na implementované technické riešenie; Pravidlá pre oddelenie právomocí;
e)	Riadenie kybernetickej a informačnej bezpečnosti vo vzťahoch s tretími stranami	Vypracovanie analýzy rizík tretích strán a celého dodávateľského reťazca, vrátane analýzy politických rizík; Analýza a posúdenie súladu všetkých aktuálnych zmlúv s tretími stranami so zákonom o KB a dobrou praxou; Vypracovanie návrhov dodatkov zmlúv s treťou stranou spolu s návrhom potrebných úprav na zabezpečenie súladu so zákonom KB; Vypracovanie a implementácia interného riadiaceho aktu upravujúceho zásady kybernetickej a informačnej bezpečnosti vo vzťahoch s tretími stranami;	Metodika pre riadenie bezpečnostných rizík vo vzťahu k tretím stranám; Analýza a posúdenie súladu vypracovanie návrhov dodatkov zmlúv; Smernica riadenie tretích strán; Smernica požiadavky pre tretie strany;
f)	Bezpečnosť pri prevádzke informačných systémov a sietí	Zavedenie opatrení a interného riadiaceho aktu v oblasti riadenia zmien, riadenia kapacít, inštalácie softvéru v sieťach a informačných systémoch, inštalácia zariadení v sieťach a informačných systémoch, zaznamenávanie bezpečnostných záznamov a zaznamenávanie a vyhodnocovanie prevádzkových záznamov;	Smernica pre riadenie zmien; Smernica správa a prevádzka IS a služieb;
g)	Hodnotenie zraniteľností a bezpečnostné aktualizácie	Vypracovanie a implementácia interného riadiaceho aktu upravujúceho proces riadenia implementácie bezpečnostných aktualizácií a záplat;	Smernica riadenie a implementácia bezpečnostných záplat a bezpečnostných aktualizácií;
h)	Ochrana proti škodlivému kódu	Vypracovanie interného riadiaceho aktu s požiadavkami na určenie zodpovednosti používateľov, pravidiel pre inštaláciu a monitorovania potenciálnych ciest prieniku škodlivého kódu Vypracovanie a implementácia pravidiel súvisiace s ochranou proti škodlivému kódu	Smernica pre ochranu proti škodlivému kódu a inštaláciu a hardening IS; Vypracovanie a implementácia postupov a procesov v nadväznosti na technické riešenie;

i)	Sieťová a komunikačná bezpečnosť	Vypracovanie a implementácia interného riadiaceho aktu upravujúceho pravidlá sieťovej a komunikačnej bezpečnosti;	Smernica pre pravidlá sieťovej a komunikačnej bezpečnosti;
j)	Akvizícia, vývoj a údržba informačných technológií verejnej správy	Vypracovanie metodiky softvérového vývoja v podobe interného riadiaceho aktu, definujúce bezpečnostné požiadavky na všetky fázy životného cyklu vývoja SW (SSDLC);	Metodika Požiadavky pre bezpečný vývoj SSDLC;
k)	Zaznamenávanie udalostí a monitorovanie	Vypracovanie interného riadiaceho aktu, ktorý obsahuje a upravuje povinnosti definované platnou legislatívou;	Smernica o bezpečnostnom monitoringu IS a sietí;
l)	Riešenie kybernetických bezpečnostných incidentov	Vypracovanie štandardov a postupov riešenia kybernetických bezpečnostných incidentov, vrátane definovania zodpovedností zamestnancov a ďalších povinností;	Vypracovanie štandardov a postupov riešenia kybernetických bezpečnostných incidentov - Súčasť smernice a metodiky pre riešenie bezpečnostných incidentov; Smernica pre riešenie bezpečnostných incidentov; Metodika pre riešenie bezpečnostných incidentov;
		Vypracovanie interného riadiaceho aktu obsahujúceho a upravujúceho povinnosti týkajúce sa riešenia kybernetických bezpečnostných incidentov;	
		Vypracovanie plánov a spôsobov riešenia kybernetických bezpečnostných incidentov.	
m)	Kryptografické opatrenia	Vypracovanie a implementácia interného riadiaceho aktu upravujúceho používanie kryptografických prostriedkov a šifrovania;	Smernica Riadenie kryptografických opatrení; Metodika pre Riadenie kryptografických opatrení; Metodika pre správu kryptografických kľúčov a certifikátov;
		Definovanie pravidiel využitia kryptografických prostriedkov používajúcich dostatočne odolné kryptografické mechanizmy na ochranu údajov pri ich prenose alebo uložení v rámci sietí a informačných systémov;	
		Vypracovanie a dokumentácia systému správy kryptografických kľúčov a certifikátov;	
n)	Kontinuita prevádzky	Vypracovanie stratégie a krízových plánov prevádzky na základe analýzy vplyvov kybernetického bezpečnostného incidentu na základnú službu;	Stratégia Riadenie kontinuity prevádzky vypracovanie analýzy dopadov (BIA); Vypracovanie BCP (plánov kontinuity prevádzky);

		Vypracovanie plánov kontinuity prevádzky a ich prvotné otestovanie v reálnom prostredí organizácie a zapracovanie nedostatkov z výsledkov testovania;	Vypracovanie DRP (plánov obnovy prevádzky IS); Testovanie BCP a DRP; Smernica Riadenie kontinuity prevádzky; Metodika Riadenie kontinuity prevádzky; Zálohovacie politiky;
		Vypracovanie interného riadiaceho aktu obsahujúceho a upravujúceho kontinuitu prevádzky následkom kybernetického bezpečnostného incidentu alebo inej krízovej situácie;	
		Vypracovanie postupov zálohovania na obnovu siete a informačného systému po jeho narušení alebo zlyhaní v dôsledku kybernetického bezpečnostného incidentu alebo inej krízovej situácie;	
o)	Audit a kontrolné činnosti	Vypracovanie programu posúdenia bezpečnosti na definované informačné technológie verejnej správy, hodnotenia zraniteľností a penetračných testov;	Vypracovanie programu posúdenia bezpečnosti na definované informačné technológie verejnej správy;

11 NÁVRH OPISU ČASTI XI. PREDMETU ZÁKAZKY: Testovanie zraniteľností

Vykonanie testov zraniteľností verejných IP adries a aj interných systémov. Vypracovanie výslednej správy s ohodnotením nájdených zraniteľností a s návrhom nápravy jednotlivých zraniteľností.

Pentest externého perimetra:

- Reconnisaince
- Service discovery
- Overenie bezpečnosti VPN
- Externý sken IPs vystavených do internetu
- Manuálna analýza:
- Service version discovery
- Vulnerability discovery
- Manuálne overenie zraniteľností
- Exploitácia
- Reporting

Report:

- Executive summary
- Krátky zoznam zraniteľností s ich hodnotením podľa impact-severity
- Popis jednotlivých identifikovaných zraniteľností
- Umiestnenie zraniteľností

- Odporúčania na odstránenie
- Popis vykonaného testovania spolu s dátumami

Interný infraštruktúrny test:
- Reconnisaince
- Service discovery
- Overenie bezpečnosti VPN
- Externý sken IPs vystavených do internetu
- Manuálna analýza:
- Service version discovery
- Vulnerability discovery
- Manuálne overenie zraniteľností
- Exploitácia
- Reporting

Report:
- Executive summary
- Krátky zoznam zraniteľností s ich hodnotením podľa impact-severity
- Popis jednotlivých identifikovanách zraniteľností
- Umiestnenie zraniteľností
- Odporúčania na odstránenie
- Popis vykonaného testovania spolu s dátumami

Webové služby informačných systémov :
- Mechanizmy autentikácie
- Kontroly autorizácie
- Validácia údajov a filtrovanie vstupov
- Session management
- Spracovanie chýb
- Riadenie konfigurácie
- Šifrovanie a ochrana údajov
- Bezpečnosť API (ak je to relevantné)
- Dodržiavanie zvolených bezpečnostných metód OWASP API TOP 10 2019

Predmet dodávky:
- Výkon penetračného testu
- Dodávka reportu popisujúceho jednotlivé nálezy s najmenej nasledujúcim obsahom:
    - Manažérsky sumár
    - Krátky zoznam zraniteľností s ich hodnotením podľa impact-severity
    - Popis jednotlivých identifikovanách zraniteľností
    - Umiestnenie zraniteľností
    - Odporúčania na odstránenie
    - Popis vykonaného testovania spolu s dátumami

12 NÁVRH OPISU ČASTI XII. PREDMETU ZÁKAZKY: Certifikovaný audit KB

Vykonanie auditu kybernetickej bezpečnosti podľa § 29 zákona č. 69/2018 Z. z. zahŕňa posúdenie stavu prijatia a dodržiavania všeobecných bezpečnostných opatrení vo forme úloh, procesov, rolí a technológií v organizačnej, personálnej a technickej rovine. Vykonanie auditu kybernetickej bezpečnosti Objednávateľa podľa zákona č.69/2018 v súlade s vyhláškou Národného bezpečnostného úradu č. 493/2022 Z. z. o audite kybernetickej bezpečnosti a znalostnom štandarde audítora (ďalej len „vyhláška o audite“) s cieľom overiť plnenie povinností podľa zákona a posúdiť zhodu prijatých bezpečnostných opatrení s požiadavkami podľa zákona a súvisiacich osobitných predpisov vzťahujúcich sa na bezpečnosť sietí a informačných systémov, s cieľom zabezpečiť požadovanú úroveň kybernetickej bezpečnosti a predchádzať kybernetickým bezpečnostným incidentom. Auditom sa identifikujú nedostatky pri zabezpečovaní kybernetickej bezpečnosti prevádzkovateľom informačných systémov verejnej správy s cieľom prijať opatrenia na ich odstránenie a nápravu a na predchádzanie kybernetickým bezpečnostným incidentom.

Poskytovateľ sa v rámci auditov kybernetickej bezpečnosti (ďalej len „audit“) zaväzuje zabezpečiť výkon auditu prostredníctvom certifikovaného audítora kybernetickej bezpečnosti (ďalej len „audítor kybernetickej bezpečnosti"), ktorý spĺňa všetky požiadavky na výkon auditu podľa vyhlášky o audite. Poskytovateľ uvedie meno a priezvisko osoby, ktorá bude pre Objednávateľa zabezpečovať výkon auditu, číslo jej platného certifikátu podľa vyhlášky o audite, dátum vydania a dobu platnosti certifikátu. Ak sa na výkone auditu budú podieľať aj iné osoby, Poskytovateľ uvedie ich mená. Audítor kybernetickej bezpečnosti sa v rámci auditu kybernetickej bezpečnosti zaväzuje poskytnúť služby v súlade s požiadavkami zákona, vyhlášky o audite a vyhlášky o bezpečnostných opatreniach výkonom auditu kybernetickej bezpečnosti, a teda vykonanie auditu sietí a informačných systémov objednávateľa ako prevádzkovateľa informačných systémov verejnej správy s cieľom preveriť účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek zákona a vyhlášky o bezpečnostných opatreniach, ktoré definujú príslušné požiadavky na prevádzkovateľa informačných systémov verejnej správy. Audit kybernetickej bezpečnosti zahŕňa tieto požiadavky: Posúdenie prijatia a dodržiavania všeobecných bezpečnostných opatrení vo forme úloh, procesov, rolí a technológií v organizačnej, personálnej a technickej rovine v oblastiach:

a) organizácie kybernetickej bezpečnosti a informačnej bezpečnosti,
b) riadenia rizík kybernetickej bezpečnosti a informačnej bezpečnosti,
c) personálnej bezpečnosti,
d) riadenia prístupov,
e) riadenia kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahoch s tretími stranami,
f) bezpečnosti pri prevádzke informačných systémov a sietí,
g) hodnotenia zraniteľností a bezpečnostných aktualizácií,
h) ochrany proti škodlivému kódu,
i) sieťovej a komunikačnej bezpečnosti,
j) akvizície, vývoja a údržby informačných sietí a informačných systémov,
k) zaznamenávania udalostí a monitorovania,
l) fyzickej bezpečnosti a bezpečnosti prostredia,
m) riešenia kybernetických bezpečnostných incidentov,
n) kryptografických opatrení,

o) kontinuity prevádzky

Vyhodnotenie auditných zistení, oboznámenie objednávateľa so zistenými nedostatkami, zostavenie a odovzdanie odporúčaných opatrení na ich odstránenie v písomnej a elektronickej forme. Vypracovanie a predloženie výstupu auditu kybernetickej bezpečnosti, a to záverečnej správy o výsledkoch auditu kybernetickej bezpečnosti v slovenskom jazyku (ďalej aj ako „správa"), ktorá bude vypracovaná v súlade s požiadavkami § 2 vyhlášky o audite. Preskúmanie bezpečnostnej dokumentácie a vyhodnotenie bezpečnostných opatrení. Vypracovanie kontrolného záznamu auditovaných bezpečnostných opatrení podľa Prílohy č. 3 vyhlášky o audite. Vyhodnotenie auditných zistení, oboznámenie prevádzkovateľa základnej služby so zistenými nedostatkami a zostavenie odporúčaných opatrení na ich odstránenie v písomnej forme. Vypracovanie a predloženie záverečnej správy o výsledkoch auditu v rozsahu podľa § 2 vyhlášky o audite.