



«TASDIQLAYMAN»
“Biznesni rivojlantirish banki” ATB
Boshqaruv raisi o'rinbosari v.b.:
B.Sharipov

«13» oktabr 2026 y.
№ 655

TEXNIK TOPSHIRIQ

**“Tenable zaifliklarni boshqarish tizimidan foydalanish litsenziyalarini
uzaytirish”**

Toshkent shahri – 2026-yil

1. Kirish

Ushbu hujjat “Biznesni rivojlantirish banki” aksiyadorlik tijorat banki (keyingi o‘rinlarda Bank deb yuritiladi) uchun Tenable mahsulotlari (Tenable.sc, veb-ilovalarni skanerlash, Nessus va Tenable Agent) asosida zaifliklarni skanerlash va boshqarish yechimi bo‘yicha amaldagi litsenziyani uzaytirish xaridiga qo‘yiladigan texnik talablarni belgilaydi.

Yetkazib beruvchi narx taklifi asosida tanlanadi. Ishtirokchi taklifi ushbu Texnik topshiriq talablariga to‘liq muvofiq bo‘lishi lozim.

2. Xarid maqsadi

Bankning IT infratuzilmasida (serverlar, tarmoq qurilmalari, ishchi stansiyalar va veb-ilovalar) mavjud zaifliklar, konfiguratsiya xatolari hamda xavfsizlik standartlaridan chetlanishlarni markazlashgan holda aniqlash, tahlil qilish va nazorat etish, shuningdek O‘zbekiston Respublikasi Markaziy bankining bank tizimlari axborot xavfsizligiga oid talablariga va PCI DSS standartiga muvofiqlikni ta’minlash.

Texnik talablar

Funksional talablar	
Axborot va telekommunikatsiya muhitida zaifliklarni boshqarish uchun dasturiy ta’minot to‘plami	
Umumiy tizim talablari	Tenable Security Center 500 IP-manzil litsenziyasini 1 yilga uzaytirish (Renewal), Tenable Security Center veb-ilovalarni skanerlash 5 ta veb-ilova litsenziyasini 1 yilga uzaytirish (Renewal). Tizim quyidagilarni ta’minlay olishi kerak: shu jumladan, lekin ular bilan cheklanmagan holda, quyidagi variantlar shaklida: ⌚ VMware yoki Hyper-V uchun tayyor virtual qurilma (VA - Virtual Appliance); ⌚ Linux OS uchun o‘rnatish paketi. Tizim ITSda kamida 500 ta IP-manzil va 5 ta FQDNni skanerlash imkoniyatini ta’minlashi kerak.
Markaziy boshqaruv	Tizim barcha komponentlari va funksiyalarini yagona veb-interfeys orqali markazlashtirilgan boshqarishni ta’minlashi kerak. Tizim hisobot berish va o‘zgarishlar tarixini taqdim etish uchun aktivlarni skanerlash va baholash natijalarini ma’lumotlar bazasida saqlashi kerak. Ma’lumotlar bazasi quyidagi mezonlarga javob berishi kerak: ⌚ Natijalarni saqlash uchun uchinchi tomon ma’lumotlar bazalaridan foydalanishni talab qilmasligi kerak.

	Natijaga (zaiflik turlari, resurs guruhlari va boshqalar) qarab, skanerlash ma'lumotlarini ma'lumotlar bazasida alohida saqlashni ta'minlashi kerak va ma'lumotlarni tahlil qilish yoki so'rov qilishda natijalarni istalgan kombinatsiyada birlashtirishi kerak. Ma'lumotlarni belgilangan va sozlanishi mumkin bo'lgan vaqt davomida saqlashi kerak, shundan so'ng ma'lumotlar bazasi avtomatik ravishda eskirgan ma'lumotlardan tozalanadi.
Tizim foydalanuvchilari	Tizim rollarga asoslangan boshqaruv (RBAC) va foydalanuvchilarning kirish huquqlarini granular darajada farqlash imkoniyatini ta'minlashi kerak. Jumladan, quyidagi amallar uchun alohida huquqlarni belgilash imkoniyati mavjud bo'lishi kerak: • Ma'lumotlar bazasi tekshiruvlarini yangilash; • Skanerlash siyosati mavjudligi yoki yo'qligi, har qanday skanerlashni amalga oshirish; • Foydalanuvchi boshqaruvi; • Zaiflik ma'lumotlarini ko'rish uchun kirish; • Aktivlar ro'yxatini aniqlash, yaratish va almashish; • Audit fayllarini qo'shish; • Ogohlantirishlar yaratish; • Taqdim etilgan ma'lumotlarni skanerlash uchun aniqlash va almashish; • Skanerlash siyosatlarini yaratish va almashish; • Ish jarayoni (Workflow) ticketlarini boshqarish; • Foydalanuvchi harakatlarining auditi. Tizim foydalanuvchiga aniqlangan zaiflik bilan bog'liq xavfni qabul qilish, shuningdek, zaiflikning xavf darajasini ishlab chiqaruvchi tomonidan belgilangan qiymatdan qat'i nazar, tashkilot talablariga muvofiq darajaga o'zgartirish imkonini berishi kerak. Tizim zaifliklarni aniqlash, kuzatish va bartaraf etish jarayonlarini boshqarish uchun ish jarayoni (Workflow) ticketlari bilan ishlash imkoniyatini ta'minlashi kerak. Tizim har bir ticketni alohida mas'ul foydalanuvchi yoki guruhga tayinlash imkonini berishi kerak. Tizim har bir ticket bilan bog'liq zaifliklar ro'yxatini yuritishi va ularning holatini kuzatish imkonini berishi kerak. Tizim foydalanuvchiga platformaning asosiy xavfsizlik va kirish parametrlarini sozlash imkonini berishi kerak, jumladan: ⌚ Parol siyosati; ⌚ Sessiyaning amal qilish muddati; ⌚ Autentifikatsiya va kirish nazorati parametrlari.

	Tizim cheklanmagan miqdordagi foydalanuvchi hisoblarini yaratish va boshqarish imkoniyatini ta'minlashi kerak.
Uzatilgan ma'lumotlarni shifrlash	Tizim komponentlari va modullari o'rtasida, shuningdek foydalanuvchi va tizim o'rtasida uzatiladigan ma'lumotlarni TLS 1.2 yoki undan yuqori versiyadagi himoyalangan aloqa protokollari yordamida shifrlashni ta'minlashi kerak. Tizim SSL hamda TLS 1.0/1.1 kabi eskirgan va xavfsizligi yetarli bo'lmagan protokollardan foydalanmasligi kerak.
Tashqi autentifikatsiya va avtorizatsiyani qo'llab-quvvatlash	Tizim foydalanuvchilarni markazlashgan autentifikatsiya va avtorizatsiya qilish uchun LDAP va Microsoft Active Directory (AD) kabi tashqi katalog xizmatlari bilan integratsiyalashish, shuningdek tashqi katalogdagi foydalanuvchi va guruhlariga asoslangan holda tizim rollari va kirish huquqlarini belgilash imkoniyatini ta'minlashi kerak.
Tizim ishlashi	Tizim tarmoq infratuzilmasining kommutatorlar, marshrutizatorlar, xavfsizlik devorlari (Firewall), hujumlarni aniqlash va oldini olish tizimlari (IDS/IPS) hamda boshqa tegishli xavfsizlik vositalaridan ma'lumotlarni yig'ish, qayta ishlash, tahlil qilish va audit qilish imkoniyatini ta'minlashi kerak. Tizim tomonidan yig'ilgan hodisalar, aniqlangan zaifliklar, skanerlash natijalari va shakllantirilgan hisobotlarni kamida 999 kun davomida saqlash imkoniyatini ta'minlashi kerak. Saqlanayotgan ma'lumotlar bo'yicha qidiruv, filtrlash, saralash va belgilangan davrlar kesimida tahlil qilish imkoniyati mavjud bo'lishi kerak.
Aktivlar boshqaruvi	Tizim aktivlarni aniqlash va inventarizatsiya qilish uchun alohida uchinchi tomon skanerlash vositalaridan foydalanishni talab qilmasligi hamda tarmoqdagi aktivlar to'g'risidagi ma'lumotlarni markazlashgan tarzda yig'ish va tahlil qilish imkoniyatini ta'minlashi kerak. Tizim faol yoki agentga asoslangan skanerlashdan tashqari, tarmoqdagi yangi aktivlarning paydo bo'lishini aniqlash va ularni aktivlar inventarizatsiyasiga avtomatik ravishda kiritish imkoniyatiga ega bo'lishi kerak. Tizim kamida quyidagi aktiv turlarini aniqlash va tasniflash imkoniyatini ta'minlashi kerak: 🕒 Serverlar 🕒 Ish stantsiyalari 🕒 Ilovalar 🕒 Operatsion tizimlar 🕒 Tarmoq qurilmalari 🕒 Virtual va bulutli tizimlar 🕒 BYOD qurilmalari 🕒 Mobil telefonlar Tizim tarmoq aktivlarini rejalashtirilgan jadval asosida hamda talab bo'yicha (on-demand) inventarizatsiya qilish va skanerlash imkoniyatini ta'minlashi kerak. Tizim DHCP muhitida IP-manzili o'zgarib turadigan aktivlarni aniqlashi va

	turli skanerlash natijalarini tegishli aktiv bilan to'g'ri bog'lash imkoniyatiga ega bo'lishi kerak. Tizim aktivlarni turli mezonlar, atributlar va qoidalar asosida qo'lda guruhlash imkoniyatini ta'minlashi kerak. Tizim aktivlarni avtomatik tasniflash va dinamik ravishda teglar (tags) bilan belgilash imkoniyatiga ega bo'lishi kerak. Bunda kamida quyidagi mezonlardan foydalanish imkoniyati mavjud bo'lishi kerak: ⌚ IP quyi tarmog'iga tegishliligi; ⌚ NetBIOS va FQDN nomiga asoslangan; ⌚ Operatsion tizim asosida; ⌚ Ochiq portlar/xizmatlar orqali; ⌚ Muayyan zaiflikning mavjudligiga asoslanib; ⌚ Skanerlash vaqtlariga asoslangan; ⌚ Rejalashtirilgan skanerlashni o'tkazib yuborgan aktivlar va boshqalar. Tizim skanerlash jarayonida tarmoq va mijoz infratuzilmasiga tushadigan yuklamani boshqarish imkoniyatini, jumladan skanerlash tezligi, parallel ulanishlar va boshqa tegishli parametrlarni sozlash imkoniyatini ta'minlashi kerak. Windows tizimlarida imtiyozli skanerlashni amalga oshirishda zarur bo'lgan masofaviy xizmatlarni, jumladan Remote Registry xizmatini, avtomatik ravishda ishga tushirish va skanerlash yakunlangandan so'ng, agar xizmat dastlab ishlamagan bo'lsa, uni avtomatik ravishda avvalgi holatiga qaytarish imkoniyati mavjud bo'lishi kerak.
Skanerlash uchun qo'llab-quvvatlanadigan OS va ma'lumotlar bazalari	Tizim infratuzilmadagi zaifliklarni aniqlash maqsadida quyidagi operatsion tizimlarni agent orqali va/yoki tarmoq orqali masofaviy skanerlash imkoniyatini ta'minlashi kerak, jumladan, lekin ular bilan cheklanmagan holda: • Microsoft Windows; • IBM AIX; • Oracle Solaris; • HP/UX; • Linux; • Tarmoq dasturlari; • MacOS. Tizim ma'lumotlar bazalarining zaifliklarini aniqlash uchun autentifikatsiyalangan (credentialed) skanerlashni qo'llab-quvvatlashi va quyidagi ma'lumotlar bazalarini skanerlash imkoniyatini ta'minlashi kerak, jumladan, lekin ular bilan cheklanmagan holda: ⌚ MS SQL;

	🕒 IBM DB2; 🕒 Informix/DRDA; 🕒 MySQL; 🕒 Oracle ma'lumotlar bazasi; 🕒 PostgreSQL; 🕒 Sybase ASE.
Ma'lumotlarni vizualizatsiya qilish (boshqaruv paneli)	Tizim zaifliklar, aktivlar, skanerlash natijalari, xavf ko'rsatkichlari va boshqa xavfsizlik ma'lumotlarini vizual ko'rinishda taqdim etish uchun o'rnatilgan boshqaruv panellari (Dashboard) to'plamiga ega bo'lishi kerak. Tizim foydalanuvchiga tashkilot ehtiyojlaridan kelib chiqib maxsus boshqaruv panellarini yaratish, sozlash va saqlash imkoniyatini ta'minlashi kerak. Boshqaruv panellarida aks ettiriladigan ma'lumotlarni avtomatik ravishda yangilash (auto-refresh) imkoniyati mavjud bo'lishi kerak. Tizim boshqaruv panelidagi alohida element yoki ko'rsatkichni batafsil ko'rib chiqish (drill-down) imkoniyatini ta'minlashi kerak. Bu imkoniyat doimiy monitoring, aniqlangan zaifliklarni tahlil qilish va hodisalarni tekshirish uchun qo'llanilishi kerak. Tizim yaratilgan boshqaruv panellarini boshqa vakolatli foydalanuvchilar bilan almashish (share) imkoniyatini ta'minlashi kerak. Tizim boshqaruv panellarida aks ettirilgan ma'lumotlar asosida hisobotlarni shakllantirish, ko'rish, saqlash va yuklab olish imkoniyatini ta'minlashi kerak. Hisobotlarni kamida keng tarqalgan formatlarda, jumladan PDF va CSV formatlarida eksport qilish imkoniyati mavjud bo'lishi kerak.
API qo'llab-quvvatlashi	Tizim boshqa axborot tizimlari, xavfsizlik vositalari va tashqi dasturiy ta'minot bilan integratsiyani ta'minlash uchun hujjatlashtirilgan va standart API (Application Programming Interface) imkoniyatiga ega bo'lishi kerak. API orqali tizimda saqlanadigan va tizim tomonidan qayta ishlanadigan ma'lumotlarga, jumladan aktivlar, zaifliklar, skanerlash natijalari, foydalanuvchilar, teglar, siyosatlar va hisobotlar kabi ma'lumotlarga dasturiy ravishda murojaat qilish imkoniyati mavjud bo'lishi kerak. API orqali boshqa axborot tizimlari bilan ma'lumot almashish, ma'lumotlarni olish va tegishli tizim obyektlarini boshqarish imkoniyati ta'minlanishi kerak. API bo'yicha to'liq texnik hujjatlar, autentifikatsiya va avtorizatsiya mexanizmlari hamda foydalanish bo'yicha yo'riqnomalar taqdim etilishi kerak. API'dan foydalanish uchun asosiy tizim litsenziyasidan tashqari alohida litsenziya yoki qo'shimcha majburiy to'lov talab qilinmasligi kerak.
Avtomatik yangilash	Tizim foydalanuvchi tomonidan doimiy qo'lda aralashuvni talab qilmasdan, tizim konfiguratsiyasi va xavfsizlik komponentlariga tegishli yangilanishlarni avtomatik ravishda aniqlash, yuklab olish va o'rnatish imkoniyatini

	ta'minlashi kerak. Avtomatik yangilanishlar, jumladan, lekin ular bilan cheklanmagan holda, zaifliklar ma'lumotlar bazasi, zaifliklarni aniqlash uchun foydalaniladigan pluginlar/tekshiruvlar, skanerlash komponentlari va boshqa zarur tizim komponentlari yangilanishlarini qamrab olishi kerak. Tizim yangilanishlarni boshqarish uchun quyidagi imkoniyatlarni ta'minlashi kerak: • Rejalashtirilgan yangilanish; • Qo'lda yangilash; • Yangilanishni yuklab olish va kerakli vaqt ichida o'rnatish imkoniyati.
Zaxiralash va tiklash	Tizim konfiguratsiya va tizim sozlamalarining avtomatik zaxira nusxalarini yaratish imkoniyatini ta'minlashi kerak. Tizim konfiguratsiya zaxira nusxalarini asosiy yechimdan alohida va mustaqil saqlash joyiga eksport qilish yoki saqlash imkoniyatini ta'minlashi kerak. Tizim zaxira nusxalarini belgilangan jadval asosida avtomatik ravishda yaratish, shuningdek administrator tomonidan talab bo'yicha (on-demand) zaxira nusxasini yaratish imkoniyatiga ega bo'lishi kerak. Zaxira nusxalari ruxsatsiz kirish, o'zgartirish yoki o'chirishdan himoyalangan bo'lishi kerak.
Masshtablash	Tizim mavjud litsenziyalangan funksional imkoniyatlar doirasida infratuzilma hajmi, aktivlar soni va skanerlash yuklamasi oshib borishi bilan tezkor va moslashuvchan masshtablash imkoniyatini ta'minlashi kerak. Tizim arxitekturasi qo'shimcha skanerlar va boshqa zarur komponentlarni qo'shish orqali funksional imkoniyatlarni kengaytirishni qo'llab-quvvatlashi kerak. Tizim geografik jihatdan turli hududlarda joylashgan skanerlash komponentlari va markaziy boshqaruv komponentlari o'rtasida markazlashgan boshqaruv va xavfsiz o'zaro aloqani ta'minlashi kerak. Geografik jihatdan taqsimlangan komponentlarni boshqarish uchun alohida boshqaruv platformasi yoki ortiqcha qo'lda sozlash talab qilinmasligi kerak. Tizim bir nechta zaiflik skanerlaridan foydalanilganda skanerlash yuklamasini dinamik ravishda taqsimlash (load balancing) imkoniyatini ta'minlashi kerak. Tizim skanerlash vazifalarini mavjud skanerlarning yuklamasi, mavjudligi va holatiga qarab tegishli skanerga avtomatik ravishda taqsimlashi kerak. Tizim alohida skaner yoki skanerlash komponenti ishlamay qolganda skanerlash vazifalarini mavjud boshqa skanerlarga avtomatik qayta taqsimlash (failover) imkoniyatini ta'minlashi kerak. Tizim skanerlarning holati, mavjudligi, yuklamasi va bajarilayotgan skanerlash vazifalarini markazlashgan boshqaruv interfeysi orqali monitoring qilish imkoniyatini ta'minlashi kerak.
Skanerlash	Tizim zaifliklarni aniqlash va baholash uchun quyidagi skanerlash imkoniyatlarini ta'minlashi kerak:

- ⌚ Jadval bo'yicha skanerlash;
- ⌚ Belgilangan skanerlash vazifalarida kerakli testlarni yoqish/o'chirish;
- ⌚ Vazifani kerakli vaqt davomida to'xtatib turish;
- ⌚ Agar muhim resurslar xizmat ko'rsatish jarayonlari bilan band bo'lsa, jadvalga muvofiq ularni avtomatik ravishda skanerlashdan chiqarib tashlash imkoniyatiga ega bo'lish;
- ⌚ Izolyatsiya qilingan tarmoq segmentini skanerlash va keyinchalik natijalarni bitta konsolga yuklash;
- ⌚ Tekshirish uchun zaifliklarni tanlash;
- ⌚ Muayyan portlarni skanerlash;
- ⌚ Hisoblardan foydalanish.

Tizim skanerlash vaqtida quyidagi autentifikatsiya mexanizmlaridan foydalanishni qo'llab-quvvatlashi kerak.

- ⌚ Windows operatsion tizimi uchun: login va parol, Kerberos, CyberArk Vault, Lieberman, Thycotic Secret Server, Arcon, Centrify, BeyondTrust, Hashicorp Vault, NTLM Hash, LM Hash;
- ⌚ Unix tizimlari uchun: login va parol, Kerberos, CyberArk Vault, Lieberman, Thycotic Secret Server, Arcon, Centrify, BeyondTrust, Hashicorp Vault, Certificate, Public Key;
- ⌚ Tarmoq uskunalari uchun – SNMP;

Tizim skanerlash maqsadlarini turli formatlarda qabul qila olishi kerak: aktivlar, IP manzillar, IP tarmoqlari, nomlar.

Skanerlash moduli kamida quyidagi operatsion tizimlarga o'rnatilgan bo'lishi kerak:

- ⌚ Windows;
- ⌚ MacOS;
- ⌚ Amazon Linux 2;
- ⌚ Red Hat Enterprise Linux;
- ⌚ Fedora.

Veb-ilova zaifliklarini aniqlash tizimi (DAST) quyidagi funktsiyalarni bajarishi kerak:

- Veb-ilovalarni vakolatli yoki vakolatsiz zaifliklarni tekshirish;
- Konfiguratsiya xatolarining ko'rsatkichi;
- REST API zaifliklarini skanerlashni amalga oshirish;
- SSL/TLS auditini o'tkazish

Tizim veb-ilovalarni SQL in'ektsiyasi, saytlararo skriptlash (Cross-Site Scripting), HTTP sarlavha in'ektsiyasi, katalogni aylanib chiqish (Directory Traversal), masofaviy fayllarni kiritish, buyruqlarni bajarish kabi keng

	tarqalgan veb-ilova zaifliklarini tekshirish imkoniyatiga ega bo'lishi kerak. Aniqlangan zaifliklar uchun OWASP TOP 10 reytingi qo'llanilishi kerak.
Zaiflikni aniqlash	Tizim muammolar, xavflar va zaifliklarni aniqlashi va tasniflashi kerak. Shuningdek, u xavfning mohiyati va uni kamaytirish bo'yicha tavsiyalar haqida batafsil ma'lumot berishi kerak. Tizim xavfsizlik bo'yicha maslahat tashkilotlari tomonidan aniqlangan aktivdagi ma'lum zaifliklar haqida xabar berishi kerak (masalan, Umumiy zaifliklar va ta'sirlar ma'lumotlar bazasi (CVE) yoki Umumiy zaifliklar ro'yxati (CWE) yoki SecurityFocus Bugtraq (BID) yoki ularning har qanday kombinatsiyasi). Mahsulot zaifliklari ma'lumotlar bazasi quyidagilarni tekshirishni o'z ichiga olishi kerak: ⌚ CISCO; ⌚ Xavfsizlik devorlari; ⌚ DNS; ⌚ FTP; ⌚ SMTP; ⌚ RPC; ⌚ SNMP; ⌚ LDAP; ⌚ SMB; ⌚ CGI; ⌚ Veb-serverlar; ⌚ Ma'lumotlar bazalari; ⌚ Backdoors; ⌚ Denial of Service; ⌚ Default accounts; ⌚ Peer-To-Peer; ⌚ Remote Shell; Tizim quyidagilarga qodir bo'lishi kerak: • nostandart portlarda ishlaydigan xizmatlarni aniqlash. • ulanish bannerlarini ko'rsatish uchun sozlanmagan xizmatlarni aniqlash. • turli portlarda ishlaydigan bir xil xizmatning bir nechta nusxalarini sinab ko'rish. • "o'lik tugunlar" (dead hosts)ni (ping buyrug'iga javob bermaydigan

	qurilmalar) skanerlash.
Audit	Tizim Windows va Unix/Linux tizimlarida patchlarning konfiguratsiyasi va mavjudligini tekshirish imkoniyatini ta'minlashi kerak. Tizim Windows, Unix/Linux, ilovalar, Cisco qurilmalari, ma'lumotlar bazalari uchun audit siyosatini taqdim etishi kerak, maxsus konfiguratsiyalardan foydalanish imkoniyati bilan.
Ustuvorlik	Tizim qo'shimcha aqlli ustuvorlik berish imkoniyatlariga ega bo'lishi kerak, bu zaifliklarning hujum paytida har birining ekspluatatsiya qilinish ehtimoliga qarab ustuvorlik beradi va yaqin kelajakda eng ko'p ekspluatatsiya qilinishi mumkin bo'lgan zaifliklarni aniqlash uchun mulkiy mashina o'rganish algoritmidan foydalangan holda mustaqil ma'lumot manbalarini, jumladan, sotuvchi zaiflik ma'lumotlari va uchinchi tomon zaifliklari va tahdid ma'lumotlarini birlashtiradi. Ushbu funksiya internetga ulanishni talab qilmasdan ichki ishlashi kerak.
Ogohlantirishlar va bildirishnomalar	Tizim zaifliklarni skanerlash yoki konfiguratsiya auditlari natijalariga asoslangan ogohlantirishlarni qo'llab-quvvatlashi kerak. Bildirishnoma harakatlari quyidagilarni o'z ichiga olishi kerak: Kontekst o'zgaruvchilaridan foydalanish imkoniyatiga ega sozlanishi mumkin bo'lgan elektron pochta manzillari: ⌚ Chiptalar yaratish; ⌚ Skanerlashni boshlash; ⌚ Syslog hodisasini yo'naltirish.
Hisobot berish	Tizim barcha hodisalar bo'yicha hisobotlarni taqdim etishi kerak, hisobotlarga veb-interfeys orqali kirish mumkin bo'lishi kerak. Tizim hisobotlarni mustaqil ravishda sozlash va o'z hisobotlarini yaratish imkoniyatini ta'minlashi kerak. Tizim so'rov bo'yicha hisobotlarni yaratish imkoniyatiga ega bo'lishi kerak. Tizim foydalanuvchiga yangi hisobotlarni yaratish va ulardan foydalanishni osonlashtirish uchun yaratilgan hisobotlarning namunalarini taqdim etishi kerak. Tizimda o'rnatilgan hisobotlar bo'lishi kerak. Tizimda eng yaxshi amaliyot hisobotlarining o'rnatilgan yoki osongina mavjud bo'lgan tayyor paketlari (NIST, CIS, ISO) bo'lishi kerak. Tizim tarmoqdagi turli segmentlar va tizimlar bo'yicha ma'lum bir vaqt oralig'ida hisobotlarni taqdim etishi kerak. Tizim tomonidan yaratilgan hisobotlarda kamida quyidagi ma'lumotlar bo'lishi kerak: ⌚ Zaiflikning nomi va uning sotuvchi shkalasi va CVSS ga muvofiq jiddiylik darajasi; ⌚ Zaif tizimlar yoki xizmatlar ro'yxati;

	⌚ Zaiflik holati; ⌚ Zaiflikni yoki agar mavjud bo'lsa, patchga havolani bartaraf etish bo'yicha tavsiyalar; ⌚ Zaifliklarni ustuvorlashtirish uchun qo'shimcha mezonlar: eksplloit, zararli kod va boshqalarning mavjudligi.
Zaifliklarni boshqarish	Tizim zaiflik infratuzilmada mavjud bo'lgan vaqt bo'yicha hisobotlarni filtrlash va yaratish uchun zaiflikni aniqlash sanasini va oxirgi aniqlash sanasini kuzatishi kerak. Tizim patchlarning yo'qligini, xizmatlarning mavjudligini tekshirishni, audit fayllariga muvofiqligini tekshirishni va boshqalarni qo'llab-quvvatlashi kerak. Tizim tarmoq ichida va tashqarisida resurslarni agentlar yordamida va agar kerak bo'lsa, agentlarsiz skanerlash imkoniyatini ta'minlashi kerak.
Tahdid haqida ma'lumot	Tizim ma'lum zaifliklar haqidagi ma'lumotlarni ko'rish imkoniyatini taqdim etishi kerak, ular haqidagi ma'lumotlar ishlab chiqaruvchining ma'lumotlar bazasidan olinishi kerak. Sotuvchining ma'lumotlar bazasi ichki tajriba, sotuvchi tavsiyalari, GitHub maslahat ma'lumotlar bazasi va Milliy zaiflik ma'lumotlar bazasi kabi manbalarga asoslangan bo'lishi kerak. Tizim eng muhim zaifliklarni aniqlash uchun ma'lum xavf ko'rsatkichlarini sotuvchining tadqiqot guruhining topilmalari bilan birlashtirgan zaiflik tasnifini taqdim etishi kerak. Zaifliklarni tasniflash funksiyasi sotuvchining ma'lumotlar bazasidagi asosiy zaifliklarni, jumladan, quyidagi toifalarni tasniflash imkoniyatini beradi: ⌚ Rivojlanayotgan tahdidlar; ⌚ Yaqinda faol ravishda ekspluatatsiya qilingan; ⌚ To'lov dasturi (Ransomware); ⌚ Yangiliklarda. Tizim quyidagilarni ta'minlashi kerak: ⌚ ishlab chiqaruvchining zaiflik ma'lumotlar bazasini qidirish; ⌚ zaifliklarni profilash; ⌚ Tashkilotning zaifliklarini ma'lum zaifliklar bilan taqqoslash. Sotuvchining zaiflik ma'lumotlar bazasida qidiruv CVE ID orqali qidiruv imkoniyatlarini ta'minlashi kerak. Zaiflik profili zaiflikni batafsil tahlil qilish imkoniyatini berishi va voqealar xronologiyasini, ta'sirlangan infratuzilma aktivlari va mahsulotlarini, kelib chiqish manbalarini va xavf profili va jiddiyligi kabi ko'rsatkichlarni o'z ichiga olishi kerak. Zaifliklarni taqqoslash funksiyasi ma'lum bir toifadagi zaifliklar ro'yxatini muhitda aniqlanganlar bilan taqqoslash imkoniyatini ta'minlashi kerak.

Litsenziyalash	Tizimni litsenziyalash, tizimning alohida komponentlarini litsenziyalashdan qat'i nazar, IP-manzillar soniga asoslanishi kerak. Litsenziya quyidagilarni o'z ichiga olishi kerak: ⌚ Cheksiz miqdordagi skanerlar; ⌚ Nessus Agentlari soni IP manzillari soniga teng; ⌚ Tizimning xalqaro standartlarga muvofiqligini audit qilish siyosati (DISA STIG, CIS, MSCT va boshqalar); ⌚ REST API.
Integratsiyalar	Tizim quyidagi yechimlar bilan integratsiyani qo'llab-quvvatlashi kerak: ⌚ APCON - Tarmoq monitoringi; ⌚ Aruba, Hewlett Packard Enterprise kompaniyasi – NAC; ⌚ Axonius – CMDB; ⌚ Atlassian - Xavfsizlik operatsiyalari; ⌚ BeyondTrust - Imtiyozli Kirish Boshqaruvi; ⌚ BMC – Patchlarni boshqarish; ⌚ Brinqa – TVM; ⌚ Cisco – NAC; ⌚ CyberArk - Imtiyozli Kirish Boshqaruvi; ⌚ Simulation – Attack Simulation; ⌚ Dell - Patchlarni boshqarish; ⌚ ForeScout – NAC; ⌚ Garland Technology – Tarmoq; ⌚ Gigamon – Tarmoq; ⌚ Blackberry tomonidan ishlab chiqarilgan Good – MDM; ⌚ HCL BigFix - Patchlarni boshqarish; ⌚ IBM – SIEM; ⌚ Infoblox - IP manzilini boshqarish; ⌚ Kenna – TVM; ⌚ LogRhythm - SIEM; ⌚ Microsoft – SIEM; ⌚ Red Hat - Patchlarni boshqarish; ⌚ RedSeal – TVM; ⌚ ServiceNow - Xavfsizlik operatsiyalari;

	⌚ Splunk – SIEM; ⌚ Symantec - Patchlarni boshqarish; ⌚ Thycotic - Imtiyozli hisoblarni boshqarish. Barcha ro'yxatdagi integratsiyalar Tizim ishlab chiqaruvchisi tomonidan qo'llab-quvvatlanishi kerak.
Joylashtirish	Tizimning barcha komponentlari internetga ulanmasdan mahalliy darajada o'rnatilishi va qo'llab-quvvatlanishi kerak. Tizim oflayn faollashtirishni qo'llab-quvvatlashi kerak. Tizim internetga ulanishni talab qilmasdan tizim yangilanishlari va zaiflik ma'lumotlarini qo'llab-quvvatlashi kerak.

1. Uskuna kafolati va xizmat ko'rsatishni qo'llab-quvvatlash

Dasturiy ta'minot ishlab chiqaruvchining kafolati va kamida 12 oylik xizmat ko'rsatish xizmati bilan ta'minlanishi kerak.

Xizmat ko'rsatish shartlari xizmat ko'rsatish holatlarini 24x7x365 rejimida ro'yxatdan o'tkazish, tizim mikrokodini va o'rnatilgan dasturiy ta'minot versiyalarini yangilash imkoniyatini o'z ichiga olishi kerak.

2. Pudratchi uchun talablar

2.1. Pudratchi uchun boshqa talablar

Ajratilgan byudjet doirasida Pudratchi quyidagi talablarga javob berishi kerak:

- ⌚ Yetkazib berish to'liq hajmda Mijozga (Mijoz vakiliga) amalga oshiriladi;
- ⌚ Pudratchi ishlab chiqaruvchining vakolatli vakilidan O'zbekiston Respublikasi hududida tovarlarni yetkazib berish huquqini tasdiqlovchi vakolatnoma xatini (Ishlab chiqaruvchining vakolatnoma shakli, MAF) taqdim etishi shart;

3. Qo'shimcha talablar

3.1. WAS modulini sozlash va ishga tushirish

Yetkazib beruvchi Tenable Security Center tarkibidagi WAS (Web Application Scanning) modulini to'liq sozlashi, mavjud infratuzilmaga moslashtirishi, veb-ilovalarni skanerlash uchun zarur konfiguratsiyalarni amalga oshirishi hamda modulning to'liq va barqaror ishlashini ta'minlashi shart.

WAS modulining ishlashi amaliy skanerlash orqali tekshirilishi va ishga tushirilgan holatda buyurtmachiga topshirilishi shart.

3.2. Tenable Agentlarni o'rnatish va sozlash

Yetkazib beruvchi mavjud Tenable Agentlarni tegishli server va ishchi stansiyalarga o'rnatishi, sozlashi va Tenable Security Center bilan integratsiyasini amalga oshirishi shart.

Agentlarni ro'yxatdan o'tkazish, zarur konfiguratsiyalarni amalga oshirish, agentlar va Tenable Security Center o'rtasidagi ma'lumot almashinuvini ta'minlash hamda agentlarning to'g'ri ishlashini amaliy tekshirish yetkazib beruvchi tomonidan bajarilishi shart.

kelishuvchilar: I.Mamajanov, F.Turgunbayev, B.Shamsiev, Z.Orifkhojayev

<https://hujjat.brb.uz/?pin=yG78dK16&id=ce13c061-0783-48c6-a1f4-68b6e3667ad4>